Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

магістр
(освітній рівень)

на тему: **Аналіз проблем безпеки в розподілених інформаційних системах на прикладі протоколу автентифікації KERBEROS**

Виконав: студент 6 курсу, групи СБм-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

(підпис) Леньо В.М.
(прізвище та ініціали)

Керівник (підпис) Александер М.Б..
(прізвище та ініціали)

Нормоконтроль (підпис) Кареліна О.В.
(прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

м. Тернопіль – 2019

РЕФЕРАТ

"Аналіз проблем безпеки в розподілених інформаційних системах на прикладі протоколу автентифікації KERBEROS ” Леньо Вікторія Михайлівна // Тернопільський національний технічний університет ім. І.Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // с. – , рис. – , табл. – , ілюстр. – , джерел – .

Ключові слова: АВТЕНТИФІКАЦІЯ, ШИФРУВАННЯ, ДОВІРЕНИЙ КОРИСТУВАЧ, KERBEROS, СЕРВЕР, ПРОТОКОЛ.

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності комп'ютерних мереж на основі авторизації користувачів з використанням віддаленого сервера Kerberos. Здійснено огляд принципів авторизації та аутентифікації.

В дипломній роботі показано актуальність оцінювання рівня захищеності комп'ютерних систем з на основі ОС Windows з використанням служби автентифікації Kerberos. Проаналізовано основні механізми авторизації та принципи роботи такої системи з виділеним сервером Kerberos.

ANNOTATION

"Analysis of security problems in distributed information systems (KERBEROS authentification protocol as a case of study) " // Diploma paper of Master degree level // Lenio Viktoria Mykhailivna// Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Cybersecurity Department // Ternopil, 2019 // p. – , Fig. – , Tables – , Posters – , Refence. – .

Key words: AUTHENTIFICATION, ENCRYPTION, TRUSTED USER, KERBEROS, SERVER, PROTOCOL.

The master's thesis investigates how to provide the necessary level of security of computer networks based on user authorization using a remote Kerberos server. Authorization and authentication principles are reviewed.

The diploma thesis shows the relevance of assessing the security level of computer systems based on Windows using Kerberos authentication service. The basic authorization mechanisms and principles of operation of such a system with a dedicated Kerberos server are analyzed.

ЗМІСТ

ВСТУП .....

РОЗДІЛ 1. ПРОБЛЕМИ БЕЗПЕКИ В РОЗПОДІЛЕНИХ СИСТЕМАХ .....

1.1 Ризики розподілених систем, пов'язані з безпекою .....

1.2 Переваги розподілених систем з точки зору безпеки .....

1.3 Цілі забезпечення безпеки розподілених систем .....

1.4 Архітектурні рівні служб безпеки .....

1.5 Механізми апаратної безпеки .....

1.6 Механізми електронної безпеки .....

1.7 Автентифікація .....

1.8 Логічне управління доступом .....

1.9 Механізми безпеки комунікації .....

1.10 Політика безпеки .....

1.11 Управління безпекою .....

1.12 Управління ризиками .....

1.13 Стандарти безпеки .....

1.14 Сервіс віддаленої автентифікації Kerberos як частина розподілених систем .....

РОЗІДЛ 2. ОСНОВИ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ВІДДАЛЕНОГО СЕРВЕРА .....

2.1 Вимоги, як основа проектування архітектури сервера віддаленої автентифікаці.....

2.2 Модель для аутентифікації та авторизації Kerberos.....

2.3 Стандарти розробки сервера Kerberos .....

2.4 Масштабованість сервера.....

2.5 Вибір механізмів аутентифікації.....

2.6 Системні актори реалізації протоколу.....

2.7 Екологічні припущення.....

2.8 Перехресна автентифікація.....

РОЗІДЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ.....

3.1 NTP та синхронізація часу .....
3.2 Попередня аутентифікація .....
3.3 Квитки аутентифікації протоколу .....
3.4 Служба аутентифікації .....
3.5 Обмін послуг з надання квитків .....
3.6 Обмін зі службою додатків .....
3.7 Архітектура програмної системи автентифікації в ОС Windows на основі Kerberos .....
3.8 Домени Windows .....
3.9 Приклад розгортання системи з сервером віддаленого доступу для домену Windows .....
РОЗІДЛ 4. РОБОТА З ПРОГРАОЮ ЗАХВАТУ TCP-ПАКЕТІВ WIRESHARK .....
4.1 Загальні відомості про програму захоплення пакетів .....
4.2 Установка Wireshark .....
4.3 Робота з програмою .....
5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ
5.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР .....
5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи .....
5.3 Розрахунок матеріальних витрат .....
5.4 Розрахунок витрат на електроенергію .....
5.5 Розрахунок суми амортизаційних відрахувань .....
5.6 Обчислення накладних витрат .....
5.7 Складання кошторису витрат та визначення собівартості НДР .....
5.8 Розрахунок ціни проекту .....
5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень .....
6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ ....

6.1 Оцінка стійкості роботи об’єкту економіки до впливу вражаючих факторів при надзвичайних ситуаціях .....
6.2 Організація робіт і заходів для дослідження стійкості об’єкту економіки .....
6.2.1 Проведення дослідження стійкості роботи об’єкту економіки .
6.2.2 Параметри об’єктів економіки, котрі враховуються при визначенні оцінки інженерного захисту робітників і службовців .....
6.3 Розрахунок штучної вентиляції .....
6.4 Пожежна безпека .....
7 ЕКОЛОГІЯ .....
7.1 Енергозбереження і його роль у вирішенні екологічних проблем .....
7.1.1 Складова енергозабезпечення .....
7.1.2 Складова енергетичної незалежності .....
7.1.3 Складова екологічної прийнятності .....
7.1.4 Складова соціальної стабільності .....
7.2 Застосування екологічних знань у різних галузях соціально-політичного життя .....
ВИСНОВОК .....
ПЕРЕЛІК ПОСИЛАНЬ .....
ДОДАТКИ

ВСТУП

Актуальність теми. Сучасні комп'ютерні розподілені системи характеризуються високим рівнем інтегрованості функціональних можливостей, підтримкою взаємодії декількох апаратних та програмних платформ, часто з використанням принципів розподіленості та паралельної роботи користувачів. Цей факт обумовлює високу складність проектованих систем та необхідність керування доступом до спільних ресурсів. Керуаання доступом – це механізм авторизації, який базується на автентифікації користувачів розподіленої системи.

Отже, автентифікація користувачів – важлива частина забезпечення інформаційної безпеки. Одним з методів автентифікації є використання протоколу Kerberos, з доступом до відповідного сервера. Тому тема роботи є актуальною.

Мета роботи. Метою роботи є аналіз методів і засобів автентифікації користувачів комп'ютерної розподіленої системи на основі сервера Kerberos.

Для досягнення вказаної мети в рамках дипломної роботи було сформульовано та розв’язано наступні задачі:

– дослідити сучасний стан технологій автентифікації користувачів;

– розробити модель бізнес процесу автентифікації з використанням віддаленого сервера;

– проаналізувати потенційні ризики методу автентифікації з використанням віддаленого сервера;

– запропонувати типове рішення для розподіленої комп'ютерної системи для авторизації її користувачів на основі віддаленого сервера.

Об’єкт дослідження: процеси забезпечення, контролю та управління безпекою у комп'ютерних системах.

Предмет дослідження: протокол авторизації на основі виділеного сервера Kerberos.

Методи дослідження. Для досягнення мети дипломної роботи використовувались:

– методи узагальнення та аналізу – при проведенні огляду стану механізмів автентифікації;

– формалізації та математичного моделювання – при аналізі методу стійкості шифрування паролів.

Наукова новизна отриманих результатів. Наукова новизна полягає у вирішенні задачі забезпечення захищеності особистих даних користувача розподіленої комп'ютерної системи. При цьому було отримано такі результати:

– систематизовано моделі автентифікації користувачів;

– запропоновано практичний приклад налаштування процесу автентифікації користувачів розподіленої системи.

Практичне значення отриманих результатів. Всі проаналізовані методи та засоби автентифікації можуть використовуватись практично при вивченні відповідних дисциплін, що стосуються адміністрування розподілених комп'ютерних систем, а також при побудові розподілених систем, для котрих критичним параметром є процес надійної автентифікації користувачів з використанням виділеного сервера.

Апробація результатів та особистий внесок здобувача. Основні положення роботи доповідались, розглядались та обговорювались на науковій конференції Тернопільського національного технічного університету. Результати дипломної роботи опубліковані у тезах студентської наукової конференції, яка проводились у ТНТУ.

РОЗДІЛ 1
ПРОБЛЕМИ БЕЗПЕКИ В РОЗПОДІЛЕНИХ СИСТЕМАХ

Термін Розподілені системи (Distributed systems) ще не набув повністю усталеного значення та змісту. У цій роботі визначаємо, що це така система, у якій кілька автономних процесорів і сховищ даних, підтримуючих процеси та / або бази даних, взаємодіють для досягнення загальної цілі. Процеси координують свою оперування та обмінюються інформацією за допомогою комунікаційної мережі.

В якості ілютсрації розглянемо розподілену систему для гіпотетичного бізнесу. У економічному відділі є власна мережа робочих станцій із засобами зберігання даних та друку звітів. Він пов’язаний з виробничими підрозділами, деякі з яких можуть знаходитись на віддалених майданчиках, які мають здійснювати спеціалізований контроль виробництва. Існують системи складів для ведення товарних запасів, відділи продажу, які генерують рахунки-фактури тощо. Усі ці окремі частини організації перебувають у взаємодії з корпоративним центром. Їх інформація сприяє палнуванню корпоративного бізнесу, а їх дії реагують на корпоративну політику. Це ілютсрація системи, яка виконує життєво важливу роль у функціонуванні та управлінні сучасним бізнесом. Тому її потрібно забезпечити.

1.1 РИЗИКИ РОЗПОДІЛЕНИХ СИСТЕМ, ПОВ'ЯЗАНІ З БЕЗПЕКОЮ

У розподілених системах існують спеціальні фактори ризику. Існуючі розподілені системи пропонують значні можливості для впровадження небезпечного чи шкідливого програмного забезпечення. Вони також дозволяють злом і перегляд. Навіть ті розподілені системи, які призначені для підтримки бізнесу з низьким або середнім рівнем ризику, все ж повинні бути обережними сьогодні, щоб не залишати себе повністю незахищеними. Потрібне пильне відстежування усіх спроб щодо атак, що призводять до відмови у наданні послуги. Навіть якщо ці напади не ставлять під загрозу цілісність даних , вони можуть бути

як незручними, так і дорогими. Досвід людей, постраждалих від «Інтернет-хробака» (Spafford, 1988), це ілютсрує це. Навмисно створена програма розповсюджувалася в кількох мережах, особливо в США. Хоча вона сама по собі не заподіює ніякої шкоди, вона постійно відтворюється до тих пір, поки не поглинає всі ресурси комп'ютерів, на яких вона вторглась, і не зупинила їх. Вартість відновлення оцінювалася в мільйони доларів. Інші ризики такого роду описані в [1].

Подібні ефекти можуть бути викликані випадково. Зокрема, неправильне поводження з повідомленнями про помилки в системах електронної пошти може спричинити "поштові бурі", які загрожують мережею. Це можливо буде спричинено, якщо меседж, що містить помилки, транслюється на кілька сайтів. Якщо кожен приймальний сайт повідомляє про помилку джерела помилки і окремо викликає повторне повторення всієї трансляції, кількість меседжів зростає експоненціально, поки мережа не зупиниться.

Інший ризик полягає в тому, що незахищені системи можуть використовуватися як точка входу до інших недостатньо захищених, але чутливих систем. Цей випадок ілютсрував випадок німецьких хакерів, які отримали доступ до багатьох чутливих систем [2]. Вони використовували незахищені системи як майданчики, з яких систематично досліджували недоліки безпеки в інших більш чутливих системах, і робили це з надзвичайно високим рівнем успіху. Це призвело не лише до розкриття конфіденційної інформації, але й до додаткових витрат на кілька сайтів, які виявили лише те, що в них потрапили, коли їхні рахунки за комунікацію стали несподівано високими.

Існує прямий ризик виявлення конфіденційної інформації при неконтрольованому, незахищеному використанні публічних мереж між вузлами системи для передачі інформації. Є багато можливостей для персоналу мережі отримати доступ до переданої інформації, але, крім того, будь-яка супутникова радіозв'язок або точка-точка можливо буде перехоплена відповідним обладнанням. Якщо потрібна захищена мережа, потрібне забезпечення зашифровування та контролю доступу.

Поширення не лише вводить додаткові ризики в комп'ютерні системи, але й ускладнює поводження з ризиками. Наприклад:

– комунікація може спричинити значні часові затримки в системі стосовно інформації, що стосується безпеки; це може ускладнити систему управління безпекою співвіднесення інформації, яка, разом узяте, вказувала б на порушення безпеки;

– розбиття системи на різні географічні, політичні, технічні чи адміністративні сфери ускладнює встановлення та управління узгодженою політикою безпеки; це також додає труднощів відслідковувати порушення безпеки, які ініціюються з іншого домену.

1.2 ПЕРЕВАГИ РОЗПОДІЛЕНИХ СИСТЕМ З ТОЧКИ ЗОРУ БЕЗПЕКИ

Однак, на додаток до зниження ризиків, у розподілених системах є компенсуючі фактори, які можна використовувати для підвищення безпеки системи.

Несанкціонований доступ до корпоративних даних може надати зловмиснику цінну стратегічну інформацію. Перевага розподілу в цьому випадку полягає в тому, що він дозволяє поширювати чутливі дані по всій системі. Таким чином, лише знаючи спосіб розповсюдження та доступ до нього у всіх місцях, зловмисник може отримати повну інформацію.

Збиток, який може призвести при порушенні можливостей обробки системи, можливо буде дуже високим, особливо коли висока премія надається здатності обробляти інформацію. Поширення може забезпечити альтернативні місця, з яких можна придбати ресурси для обробки. Випадкові збої, як правило, трапляються на одному сайті одночасно, і навмисні спроби зірвати надання послуги вимагатимуть втручання на декілька сайтів одночасно.

У розподіленій системі можуть бути різні вимоги безпеки. Однією з переваг розповсюдження є те, що воно не обмежує всі компоненти системи приймати один і той же режим безпеки. Якщо оточення розділено на окремі домени безпеки,

кожен домен може відображати різний аспект політики організації щодо безпеки. Загальний контроль отримують або шляхом узгодженої політики взаємодії між менеджерами доменів, або шляхом ієрархічної структуризації доменів, при цьому один менеджер бере на себе відповідальність за координацію взаємодії всіх.

Цілі безпеки в розподілених системах можна визначити на кількох різних рівнях, від цілі високого рівня, таких як "захист активів організації", до низького рівня, наприклад "гарантувати, що слова словника не використовуються як паролі", з ієрархією цілей між ними. Кожен рівень допомагає досягти цілей більш високого рівня. Ці цілі можуть бути досягнуті механізмами на декількох різних архітектурних рівнях в межах розподіленої системи. Прикладом цього є захист даних при передачі. Це можливо буде досягнуто шляхом захисту ліній зв'язку, захистом від кінця до кінця або на проміжному рівні. Поєднання цілей безпеки та архітектурних рівнів, на яких вони можуть підтримуватися, утворюють рамку, в якій можна описати безпеку.

Міжнародна організація стандартів (ISO) Відкриті системи взаємодії відкритих систем (OSI) Архітектура безпеки [3] визначає набір служб безпеки на основі загально узгоджених цілей та встановлює варіанти архітектурних рівнів, на яких вони можуть надаватися. Цілі більш детально описані в Огляді систем безпеки OSI [4].

1.3 ЦІЛІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗПОДІЛЕНИХ СИСТЕМ

Корисно розрізняти первинні та вторинні цілі безпеки. Основні цілі відповідають таким загрозам, як розголошення, корупція, втрата, відмова в наданні послуг, себе за себе, відмову. Вторинні цілі призводять до конкретизації послуг для підтримки первинних.

Є три основні цілі безпеки, які стосуються як збережених даних, так і меседжів, які перебувають у дорозі. Вони є:

Конфіденційність – збереження конфіденційності інформації, що зберігається в системах або передається між ними. Зазвичай це означає запобігання несанкціонованого доступу до збережених файлів даних та

запобігання підслуховування меседжів у передачі. Однак у додатках підвищеної безпеки також можливо буде вимога щодо захисту найвищої інформації, яка може виводитися виключно з того, що дані передаються, а не з їх вмісту. Цю інформацію можна отримати з аналізу трафіку, аналізу джерела, місця призначення та обсягу зв'язку.

Цілісність – підтримка цілісності даних, що зберігаються в системах або комунікаційних між ними системах. Це запобігає втраті чи зміні інформації через, наприклад, несанкціонований доступ, збої компонентів або помилки зв'язку. У передачі даних можливо буде важливим також запобігання повторення меседж. Наприклад, меседж в системі електронних переказів коштів, що санкціонує переказ коштів з одного рахунку на інший, не повинно надсилатися та діяти двічі. Захист від цього ризику відомий як запобігання відтворення. Цілісність можливо буде досягнута двома різними способами : або взагалі запобігаючи виникненню збоїв, або виявляючи виникнення і відновлюючись після нього. Профілактика можливо буде досягнута рядом засобів; фізичним захистом, контролем доступу від несанкціонованих дій та процедурними заходами для запобігання помилок. Виявлення та відновлення потребують своєчасного виявлення в поєднанні з резервними засобами, які дозволяють знову почати ситуацію з відомою цілісністю.

Доступність – підтримка доступності інформації, що зберігається в системах або передається між системами, гарантуючи, що служби, що надають доступ до даних, є доступними та дані не втрачаються. Загрози наявності можуть існувати на кількох рівнях. Файл даних недоступний для юзера, якщо комп'ютер, який надає послугу, апаратно знищений вогнем, або якщо файл було безповоротно видалено, або якщо зв’язок між юзерем та комп'ютером не відбувся. Як і щодо цілісності, доступні два різні способи захисту: запобігання; виявлення та відновлення за допомогою засобів резервного копіювання.

Дві інші основні цілі безпеки застосовуються спеціально для спілкування між юзерами та / або програмами:

Автентифікація – автентифікація особи, яка спілкується з партнерами, та автентичність походження та цілісності даних, що передаються між ними. Це

важливо для кількох цілей. Ідентифікація особи, яка створює меседж, надає в електронних поштових системах конфіденційність того , що меседж є справжніми. Він також забезпечує основу для аудиту та бухгалтерського обліку. Це вимога до систем контролю доступу, заснованих на особі юзерів системи. Автентифікація вмісту меседж дозволяє знайти збої цілісності в повідомленнях.

Неприйняття – це запобігання юзереві неправильно заперечувати надсилання або отримання меседж. Перший з них відомий як доказ походження, а другий як доказ доставки. Неприйняття чинності є важливим у будь-якій ситуації, коли інтереси сторін, що надсилають та приймають, можуть конфліктувати. Наприклад, у системі передачі акцій було б у економічних інтересах відправника відмовитись від замовлення на продаж, якщо вартість запасу внаслідок цього зростає, а в інтересах отримувача – відмовити його у випадку невдачі. Це є ключовим питанням для контрактних систем, заснованих на EDI (Електронний обмін даними), наприклад, системи придбання та постачання.

Вторинні цілі безпеки, визначені Архітектурою безпеки, є такими:

Управління доступом – надання контролю доступу до служб або їх компонентів для забезпечення доступу юзерів лише до служб та доступу до даних, на які вони мають право. Управління доступом – це один із засобів, який використовується для досягнення конфіденційності, цілісності та доступності. Це може забезпечуватися фізичними та / або логічними механізмами.

Несанкціонованому доступу до персонального комп’ютера можна запобігти дезактивацією клавіатури. Доступ до спільної системи може контролюватися логічною системою контролю доступу, використовуючи правила доступу, засновані на автентифікованій особі юзерів.

Аудиторський слід – надання аудиторського сліду оперування в системі для забезпечення підзвітності юзерів. Аудиторський слід містить свідчення того, хто що робив і коли. Важливий особливий випадок аудиту систем контролю доступу обговорюється в розділі VB

Сигналізація безпеки – виявлення подій, що вказують на фактичну або потенційну помилку безпеки, повинно викликати тривогу і призвести до того, що система працюватиме в режимі безвідмовної роботи. Деякі збої в безпеці не

виявляються в той час і про них не можливо буде повідомлено, як, наприклад, невдача системи контролю доступу знайти несанкціонований доступ через власну слабкість. Інші види оперування можуть свідчити про можливі збої в безпеці та потребують розслідування; наприклад, змінений шаблон доступу юзерем. Завданням у цій ситуації є одночасно звести до мінімуму ризик втрати, якщо дійсно є збій безпеки та незручності для юзера , якщо помилкова тривога.

Викладені вище цілі безпеки є взаємозалежними і не повинні прийматися окремо. Автентифікація є основою для досягнення багатьох інших цілей. Автентифіковані унікальності юзерів потрібні для контролю доступу, заснованого на унікальності, нерозподілу та аудиту, але для автентифікації на основі пароля потрібен як управління доступом, щоб захистити файл пароля, так і конфіденційність на основі зашифровування для подальшого захисту, якщо управління доступом не виконаний. Управління доступом, крім того, що вимагає та підтримує автоматичну перевіряння, є основою для конфіденційності, цілісності та доступності. Аудиторські шляхи та сигналізація про безпеку залежать від інших цілей та підтримують їх.

1.4 АРХІТЕКТУРНІ РІВНІ СЛУЖБ БЕЗПЕКИ

Архітектура безпеки ISO визначає можливі рівні протоколу зв'язку базової моделі взаємозв’язку відкритих систем, на якій могла б покластися кожна служба безпеки. Служба безпеки, така як конфіденційність, може застосовуватися для спілкування на різних рівнях моделі, але застосовувати службу на всіх рівнях недоцільно. Наприклад, юзереві, який отримує конфіденційність від кінця до кінця за допомогою зашифровування на шарі презентації, також не потрібно зашифровування даних для передачі даних. Подальша робота зі стандартів дозволить визначити відповідні профілі служб безпеки для конкретних програм.

Для досягнення цілей безпеки використовується низка різних механізмів. Вони включають:

- фізична та електронна безпека компонентів системи;
- механізми автентифікації;

– механізми контролю доступу;

– механізми захисту зв'язку.

Вони коротко описані тут. Зацікавлені читачі перейдуть до подальшого читання для більш детальної інформації.

1.5 МЕХАНІЗМИ АПАРАТНОЇ БЕЗПЕКИ

Механізми апаратної безпеки використовуються для захисту обладнання та для контролю доступу поза межами логічного контролю доступу або зашифровування. Вони потрібні для захисту від ризиків, таких як пожежа, буря, терористичні атаки та випадкові або зловмисні збитки з боку юзерів та технічних працівників. Фізична безпека вимагає різноманітних механізмів:

– Превентивна безпека – міцна конструкція, замки на дверях, вогнестійкість та гідроізоляція;

– Виявлення та стримування – сповіщувачі руху та дверні вимикачі, пов'язані з сигналізаціями, освітленням безпеки та телевізором із замкнутим контуром;

– Відновлення – надання резервного веб-сайту з альтернативними схемами обчислень та комунікацій.

Базовий рівень апаратної безпеки завжди потрібний навіть за умови логічного контролю доступу та зашифровування. У деяких ситуаціях апаратний захист можливо буде простішим та безпечнішим, ніж логічне рішення; наприклад, керуючи фізичним доступом до терміналів та персональних комп'ютерів та їх даних та зберігаючи конфіденційні дані на знімних носіях.

Фіг.3 ілютсрує ситуацію, коли зашифровування потрібно доповнити фізичним захистом лінії, якщо потрібно повністю захистити від кінця до кінця . Це потрібно, оскільки блок зашифровування не є невід'ємною частиною захищеного терміналу.

1.6 МЕХАНІЗМИ ЕЛЕКТРОННОЇ БЕЗПЕКИ

Можуть знадобитися електронні механізми захисту для захисту від перешкод від статичної електрики та радіочастотних перешкод, що може призвести до несправності комп'ютерного та комунікаційного обладнання. Вони також потрібні для радіаційної безпеки, щоб уникнути пасивного підслуховування електромагнітного випромінювання від візуальних дисплеїв, принтерів та процесорних систем . Модульовані сигнали можуть бути виявлені сусідніми радіоприймачами та проаналізовані для виявлення даних, що відображаються, друкуються або обробляються. Профілактичні пристрої є у продажу, а також існують військові стандарти захисту (так звана "захист від шкідників").

1.7 АВТЕНТИФІКАЦІЯ

Метою особистої автентифікації в комп'ютерних системах є перевіряння заявленої особи людини. Для цього існує ряд різних механізмів, які базуються на одному або декількох принципах наступних крил:

– особиста характеристика юзера (відбиток пальців, геометрія руки, підпис тощо), яка є унікальною для людини;

– володіння юзера, наприклад, магнітно або електронно кодована картка, яка є унікальною для цієї особи;

– інформаційний іон, відомий лише юзереві, наприклад, секретний пароль або ключ зашифровування.

Секретні особисті паролі – це найпростіший і найдешевший спосіб втілення, і вони забезпечують належний рівень захисту для додатків середнього та низького рівня безпеки. Їм потрібен ряд підтримуючих заходів, якщо їх не підірвати. Заходи включають: регулярну зміну юзерем, одностороннє зашифроване сховище, мінімальну довжину та керований формат (наприклад, слова без словника), обмежена кількість дозволених спроб, а також перевіряння та перевіряння всіх збоїв. Їх можна посилити, обмеживши юзерів входити в конкретні апаратно

захищені термінали; наприклад, службовці з оплати праці можуть входити в цю службу лише за допомогою одного з терміналів, розміщених в конкретному офісі.

Застосування паролів через відкриті канали зв'язку в розподілених системах є особливою проблемою, оскільки пароль можна знайти, підслухавши канал, а потім використати його для себе. Одним з варіантів цього є застосування одноразових паролів, створених смарт-картами (див. Нижче).

Картки з магнітним кодом мають деякі переваги перед паролями – їх неможливо скопіювати так легко і їх менш легко забути. Однак вони також страждають від можливої експозиції свого вмісту у відкритих каналах комунікації.

Смарт-карти пропонують підвищену безпеку, оскільки їх можна запрограмувати для надання змінної інформації. Існує кілька режимів, в яких їх можна використовувати для особистої автентифікації. Дві з них:

– Генератори одноразових паролів, які генерують інший paSword кожен раз, коли вони використовуються. Один комерційний продукт щомісяця змінює пароль. У всіх випадках обчислювальна служба повинна синхронізуватися з генератором паролів.

– Пристрої реагування на виклики Хост надсилає номер виклику та смарт-карту h для обчислення правильної відповіді, включаючи вхід від юзера.

Смарт-карти стають дешевшими та простішими у використанні, і вони обіцяють забезпечити задовільний спосіб подолання проблем особистої автентифікації в розподілених системах. Однак система автентифікації повинна вирішувати проблему захисту захищеної інформації, на якій вона ґрунтується. Це аспект управління безпекою (див. Розділ VA).

Метою автентифікації меседжів у комп'ютерних та комунікаційних системах є перевіряння того, що меседж надходить від заявленого джерела і що воно не було змінено при передачі. Це особливо потрібно для EFT (Електронний переказ коштів). Механізм "p rotection" – це генерування коду автентифікації меседж (MAC), приєднаного до меседж, який можливо буде перерахований отримувачем і знайде будь-які зміни на шляху. Див. Рисунок 4. Один

уніфікований спосіб описаний у (ANSI, X9.9). Механізми автентифікації Messa можуть також використовуватися для досягнення неповернення меседжів.

1.8 ЛОГІЧНЕ УПРАВЛІННЯ ДОСТУПОМ

Логічний управління доступом повинен використовуватися, коли апаратний управління доступом неможливий, як це має місце в системах з багатьма юзерами. Модель управління логічним доступом надається Довідковим монітором, який перехоплює всі спроби доступу та дозволяє їх лише у випадку дозволу доступу. В іншому випадку доступ заблокований, юзереві повертається меседж про помилку та вживаються відповідні реєстраційні та тривожні дії .

Існує дві основні форми логічного контролю доступу: обов'язковий управління доступом, заснований на фіксованих правилах; та дискреційний управління доступом, який дозволяє юзерам ділитися та контролювати доступ (див. розділ VI.A). Рекомендований дискреційний підхід до контролю доступу

Ідентифікація / авторизація. Система забезпечує автентифікацію ідентифікацій юзерів під час входу в систему, а контрольний монітор приймає рішення на основі правил доступу, що стосуються юзера, сутності, до якої звертаються, та операції, яку юзер намагається здійснити.

Є дві основні реалізації правил доступу:

– До цільових об'єктів додається Список контролю доступу (ACL), який визначає юзерів, які мають право доступу до них та операції, які вони можуть виконувати;

– Юзері отримують автентифіковані можливості, які діють як квитки, що дозволяють їм отримувати доступ до визначених ресурсів.

Багато персональних обчислювальних систем забезпечують лише управління доступом на основі паролів файлів. Вони забезпечують мінімальний, простий у використанні рівень захисту, який є адекватним для систем із низьким рівнем безпеки.

1.8 МЕХАНІЗМИ БЕЗПЕКИ КОМУНІКАЦІЇ

Існує два основних механізми забезпечення безпеки зв'язку, крім апаратного захисту ліній та обладнання: зашифровування; і прокладка руху.

Зашифровування – один з найважливіших прийомів захисту комп'ютера та зв'язку. Криптографія означає буквально «таємне написання». Зашифровування перетворює (шифрує) звичайний текст у шифротекст, який неможливо прочитати, а дезашифровування знову перетворює його на читабельний звичайний текст (розшифровує його). Криптографією займаються тисячі років, але поява алгоритмів зашифровування на основі комп’ютера змінило її з важкої та ненадійної на просту та потужну. Алгоритми, такі як Стандарт зашифровування Da ta, описаний нижче, легко доступні, прості у використанні та забезпечують високий ступінь захисту від загроз конфіденційності та цілісності комунікацій.

Тут буде розглянуто лише короткий пробіг. Його ціль – приховати існування меседжів на лінії зв'язку, вставляючи фіктивні меседж на лінію, щоб забезпечити рівномірний рівень трафіку в усі часи. В основному це цікавить військовий рівень безпеки.

Зашифровування можна використовувати для декількох цілей: запобігання підслуховуванню; виявлення зміни меседжів; і, у поєднанні з застосуванням унікальних ідентифікацій меседжів, виявлення видалення та повторного відтворення меседж.

Зашифровування може використовуватися на окремих повідомленнях або в кінці. Зашифровування меседжів охоплює лише комунікаційні зв'язки. На відміну від цього, кінцеве зашифровування проводиться безпосередньо між ініціюючою та цільовою системами. Проміжний рівень – це мережеве зашифровування, де зашифровування охоплює всю мережу, але не шлюзи між мережами. У всіх випадках, коли зашифровування здійснюється окремим апаратним блоком, зв'язок між терміналом і блоком зашифровування не охоплюється, а додатково потрібний апаратний захист. Дивіться рисунок 3.

Існує два основних типи зашифровування:

Зашифровування з секретним ключем, яке використовує єдиний секретний ключ, що ділиться між відправником та отримувачем.

Зашифровування з відкритого ключа, яке використовує пов'язану пару ключів. Один ключ є загальнодоступним і може використовуватися для зашифровування меседжів, тоді як інший ключ є секретним, відомим лише отримувачу, і він можливо буде використаний для розшифровки меседжів.

1.9 ПОЛІТИКА БЕЗПЕКИ

Політика – це плани організації щодо досягнення її цілей. У контексті безпеки політика безпеки визначає загальні цілі організації щодо ризиків для безпеки та плани поводження з ризиками відповідно до цих цілей. Політика зазвичай є ієрархічною; плани політики високого рівня – це цілі, які повинні вирішувати політики нижчого рівня.

Усі організації повинні проводити політику безпеки на високому рівні, визначаючи загальні цілі безпеки організації та встановлюючи рамки планів для досягнення цілей. Ці цілі на високому рівні істотно відрізняються від організації до організації. Військові організації приділяють велику цінність таємниці на відміну від академічних установ, які пропонують відкритість інформації. Економічні установи переймаються насамперед збереженням цілісності даних та меседжів, які представляють гроші. За замовчуванням для простих соціальних організацій взагалі немає політики безпеки.

Політики безпеки не завжди точно сформульовані або записані, але ефективна політика комп'ютерної безпеки вимагає відповіді на наступні питання:

- Які активи слід захищати та яка їхня вартість?
- Які загрози цим активам?
- Яку загрозу слід усунути та якими засобами?

Політика безпеки для розподіленої системи повинна відображати очікування вищих керівників щодо цілей безпеки організації. Часто так само, як цілі безпеки організації можуть бути не чітко визначені, ті, що знаходяться в розподіленому середовищі обробки, залишаються незмінними, і їх слід

витягувати з інших документів або ідентифікувати та узгоджувати шляхом переконання та обговорення з працівниками відповідної організації.

Політика безпеки на високому рівні може зробити загальну заяву про цілі організації, але для її ефективності потрібно провести аналіз ризиків, щоб зрозуміти вразливість організації та наслідки порушень безпеки. Управління ризиками, про які йдеться нижче у розділі VC, потрібне через можливі компроміси між передбачуваною вартістю загроз та фактичними витратами на заходи безпеки. Заходи безпеки, що вживаються для протидії загрозі, повинні бути співмірними із самою загрозою. Th Результати е аналізу ризику може допомогти переглянути або зосередитися політики на високому рівні, а також визначити політику нижнього рівня для управління системою в безпечному режимі.

Вибір служб безпеки повинен узгодити низку конфліктуючих цілей, які включають наступне.

Політика безпеки часто визначається централізовано, але застосовується локально або в кожній програмі, а також у багатьох точках втручання в комунікацію між кожним юзерем. Тому існують практичні труднощі у забезпеченні дотримання політики безпеки.

Дизайн існуючих уніфікованих комунікаційних продуктів та багатьох операційних систем дозволяє уникнути чи нехтувати міркуваннями безпеки. Тому вимоги безпеки повинні узгоджуватись окремо з постачальниками системи, що вимагає великих затрат на реалізацію закупівель, ніж якщо б вони були визначені як частина уніфікованої або невід'ємної частини операційної системи.

Можна створити розподілену систему, в якій всі аспекти безпеки централізовано управляються загальним стандартом. Оскільки розподілена система, швидше за все, розвивається федерацією ряду існуючих різних (і неоднорідних) систем, можливо, раніше вони застосовували різні політики безпеки. Завжди можливо, що вони можуть бути несумісними або тому, що політики систем відрізняються рівнем безпеки, яку вони надають, або терплять, або тому, що існує технічна несумісність, наприклад, тому, що були обрані різні алгоритми зашифровування.

ISO визнали цю проблему і ввели концепцію політики взаємодії з безпекою як частину рамок безпеки. Це політика, яка приймається всіма учасниками взаємодії. Це має бути домовлено між ними, перш ніж вони зможуть спілкуватися. У питаннях , які повинні бути вирішені між ними як рівень безпеки і технічної сумісність їх механізмів безпеки. Що стосується рівня безпеки, це не обмежується параметрами безпеки, що стосуються їх зв'язку. Політика безпеки однієї організації може наполягати на тому, що сумісні стандарти безпеки діють на комп'ютерних підприємствах іншої організації до того, як буде дозволена взаємодія.

Міжорганізаційна політика взаємодії з безпекою, узгоджена та дотримана всіма сторонами, можливо буде складною для ведення переговорів через потрібність більш широкої сумісності, ніж просто стандартів безпеки зв'язку . Наприклад, можуть бути несумісності в рівнях безпеки їх операційних систем. Якщо не можна погодити загальну політику безпеки, можливо, буде прийнято рішення відмовитись від спілкування або через те, що ризик є неприйнятним, або недійсним накладенням неприйнятних чи неконфесійних практик безпеки. Наприклад, більшість організацій, які працюють за своїми установками відповідно до державних стандартів військової безпеки, не дозволяють електронній пошті працювати на будь-якому з їх комп'ютерних мереж через відомі експозиції, пов’язані з цим. Вони повинні використовувати спеціальну вільну електронну пошту, відключену або завантажену від інших систем.

Політика взаємодії з безпекою в розподіленій системі повинна призвести до створення загальноприйнятого розкладу потрібних служб безпеки та їх механізмів підтримки.

Для ілютсрації практичного застосування політик безпеки інформаційних технологій (IT) в середовищі розподіленої обробки описуються деякі політики, які можуть застосовуватися до типової компанії. Вони поділяються на такі напрямки:

- політика управління безпекою;
- рівні безпеки;
- безпека зв'язку;
- системний управління доступом;

- управління доступом до даних;
- палнування катастроф;
- аудиторність системи;
- правова та регуляторна політика, що стосується безпеки.

Зверніть увагу насамперед на масштаби та межі цих політик. Вони включають сфери, потрібні для забезпечення конфіденційності, цілісності та доступності інформації, з двома помітними винятками. По-перше, вони не охоплюють процедури резервного копіювання та відновлення, які є частиною звичайних ІТ-операцій на сьогодні. Передбачається, що крім Політики безпеки ІТ, організація має Політику роботи з комп'ютером ІТ, яка охоплює щоденні процедури керування комп'ютером, включаючи відновлення після інцидентів, таких як збої системи та збої дисків; а також Політика управління інформаційними комунікаціями, що охоплює такі процедури, як чергування у випадку відмов лінії. Виключення цих областей із політики безпеки є певною мірою довільним, але є загальним для багатьох організацій, які вважають за краще їх розглядати як аспекти системних та комунікаційних операцій. Звичайно, важливо забезпечити, щоб ці теми були охоплені тим чи іншим політичним документом.

По-друге, ці політики безпеки також виключають контроль змін системи. Це теж може розглядатися як довільне, але знову ж таки виправданням є те, що воно повинно бути охоплено в іншій політиці. Ці аспекти контролю змін, що стосуються реконфігурації системи шляхом зміни апаратних компонентів, таких як системи обробки та мережі, повинні охоплюватися інформаційними політиками комп'ютерних операцій та управління комунікаціями. Контроль за зміною програмного забезпечення повинен охоплюватися правилами з управління та розвитку комп'ютерних технологій.

У типовій комерційній організації безпека не зробить незначного або взагалі ніякого прямого внеску у досягнення своїх найближчих цілей (поки щось не піде не так) , витрачаючи при цьому значну кількість зусиль і коштів. Тому, якщо політика безпеки має бути ефективною, їх потрібно затвердити на найвищому рівні управління, як правило, на рівні Ради та включати в цілі, які встановлюються

для кожного відділу. Тільки тоді менеджери підприємств розглядають їх як невід'ємну частину своїх цілей.

Далі, вони повинні ефективно повідомлятися. Багато організацій мають неофіційну політику безпеки, яку можна вивести з інших політичних документів та з управлінських рішень, які можуть бути поховані у внутрішніх меморандумах та їх важко знайти. Ефективні політики безпеки повинні бути окремо і чітко задокументовані, бажано як документ Політики безпеки або як розділ у документі Політики ІТ. Тоді можливість ІТ та персоналу юзерів легко дізнатись, що таке політика; немає можливості ефективного здійснення політики, про яку ніхто не знає.

Отже, перша рекомендація компанії полягає в тому, щоб директор, відповідальний за ІТ, отримував схвалення Правління на створення та впровадження політики безпеки ІТ, як це викладено в документі Політики безпеки ІТ.

Основою політики безпеки організації буде ефективної організаційної структури. Хоча обробка інформації централізована, достатньо поставити когось, відповідального за забезпечення безпеки ІТ у всій організації. Однак , як тільки він розповсюджується, потрібно мати дворівневу організаційну структуру: центральний координатор безпеки; та Адміністратори безпеки, що охоплюють кожен відділ організації. Для дотримання самостійності розподілених систем відповідальний за безпеку в кожній системі повинен нести її адміністратор безпеки, але для того, щоб рівень безпеки був узгодженим у всій організації, Координатор безпеки повинен мати мету забезпечити, щоб кожна s ystem працює над сумісними стандартами та процедурами. Зазвичай Координатор безпеки має два завдання: забезпечення того, щоб кожен адміністратор безпеки знав про стандарти та процедури; і допомагати керівникам відомчих підприємств у забезпеченні їх дотримання.

Основна проблема компанії, окрім створення своєї організації ІТ-безпеки, повинна полягати у забезпеченні поширення мережі досить широко; кожна незалежна система, яка ухиляється від контролю зв'язку або управління системами, є потенційним ризиком для безпеки. Персональні комп’ютери, які

стали «незалежними», можуть бути або не працювати відповідно до стандартів безпеки компанії. Кожен повинен бути внесений під парасолькою відповідного адміністратора безпеки.

1.10 РІВЕНЬ БЕЗПЕКИ

Політики управління повинні здійснюватися щодо груп об'єктів, а не окремих осіб. Більшість організацій повинні також застосувати цю концепцію до заходів безпеки. Якщо можна визначити лише кілька рівнів безпеки та встановити пакет заходів безпеки для кожного рівня, то детальних рішень щодо окремих об'єктів можна уникнути.

Комерційні організації, ймовірно, визначають два типи рівня безпеки: для даних та для юзерів. Більшість прагнуть забезпечити однаковий рівень захисту всіх своїх даних, щоб був лише один рівень безпеки для даних. Це набагато простіше в управлінні, ніж на декількох рівнях, і відповідає звичайній вимозі, що обмін та мобільність даних повинні бути включені, але контролюватися. Однак може виникнути вимога обробляти такі дані мені особливо безпечно, або тому, що її конфіденційність має вирішальне значення для успіху бізнесу, або, звичайно, через умови урядового контракту.

З іншого боку, досить часто хочеться робити розрізнення між категоріями юзерів, особливо коли стороннім особам надається обмежений доступ до системи для спеціальних цілей або коли дозволений безпечний набір номера дозволений. Таким чином, може існувати політика, що стосується трьох категорій юзерів по-різному: звичайних юзерів, які мають найменший доступ до розширеного відпочинку ; тих самих юзерів, коли вони набирають номер, яким повинен бути дозволений доступ до конкретно заздалегідь визначених даних; та сторонніх людей із подібним обмеженням. Зауважимо, що це поняття рівнів безпеки має схожість із рівнями безпеки військового типу для m та обов'язкової безпеки. Але формально визначене значно менше.

Фізична безпека є основою всієї безпеки системи. Повинна бути політика, яка вимагає відповідного рівня апаратного захисту всіх фізичних активів, що знаходяться під її контролем.

Політика безпеки зв'язку зазвичай визначає потрібні рівні конфіденційності, цілісності та доступності. Вони поділяються на дві категорії: безпека корпоративних мереж; а також критерії для додатків для забезпечення вищого рівня безпеки на завершення. Виходячи з сучасних технологій, політика, ймовірно, вимагає впевненої цілісності та визначеного відсотка доступності в мережі, але не наполягати на забезпеченій конфіденційності мережі. Протягом кількох років із збільшенням доступності дешевих продуктів зашифровування політика, ймовірно, буде вдосконалена, щоб також наполягати на конфіденційності мережі.

Припускаючи відносно слабку політику безпеки мережі, потрібна додаткова політика для того, щоб додатки, що потребують більш високого рівня безпеки, забезпечувались нею за допомогою заходів безпеки на рівні додатків. Зауважте, що політики автентифікації юзерів розглядаються нижче.

Часто найбільш важливі заходи безпеки повинні бути прийняті в організаціях з відкритими розподіленими системами робити з контролем доступу юзерів до системи. Тому потрібно розробити політику щодо контролю доступу до системи з двома основними частинами. У першій частині зазначено вимогу до унікальних ідентифікаторів юзерів та потрібність їх поваги. Друга визначає силу автентифікації, яку потрібно застосувати до юзерів, які намагаються увійти в систему. Зазвичай є два рівні автентифікації.

Звичайні юзері входять із терміналів та робочих станцій у приміщеннях ABC. У політиці будуть вказані стандарти для паролів, наприклад мінімальна довжина та потрібний формат, а також частота змін.

Юзері, незалежно від персоналу компанії чи зовнішні, які здійснюють реєстрацію за межами приміщень ABC. Буде набагато вищий рівень автентифікації, ймовірно, використовуючи смарт-карти чи інші генератори одноразових паролів.

Політика контролю доступу до даних містить такі елементи. Належить визначити право власності на всі елементи даних організації, при цьому власник несе відповідальність за рішення щодо застосування даних.

Усі дані повинні бути захищені, а доступ повинен бути дозволений лише за дозволу власника.

У всіх системах повинні бути системи управління процесом, які захищають дані до визначеного стандарту.

1.11 Управління безпекою

Управління безпекою – це активність управління функціями та механізмами, які використовуються різними службами в розподіленій системі для реалізації політики безпеки. Основні функції управління безпекою включають:

Керування ключами зашифровування (ANSI, X9.17) та іншими артефактами, таким як паролі. Це включає генерацію ключів у міру потрібності та розподіл ключів до відповідних компонентів системи, зберігання ключів та ключів архівації. Клавіші повинні мати обмежений термін експлуатації, і тому їх слід регенерувати в регулярні періоди.

Керування реєстрацією юзерів та інформацією, що використовується для перевірки їхньої унікальності (загальнодоступний ключ або пароль зашифровування).

Керування інформацією про управління доступом, що стосується юзерів та сервісів. Сюди входять списки контролю доступу, можливості, привілеї та багаторівневі мітки безпеки.

Забезпечення слідів аудиту безпеки. Вони фіксують усі виняткові події (спроби несанкціонованого доступу тощо) та вибрані звичайні події, такі як вхід у систему та доступ до файлів. Їх ціль – дозволити розслідування порушень безпеки та аудит дій адміністратора безпеки.

Практично неможливо гарантувати, що самовільний доступ чи перегляд чутливих матеріалів ніколи не відбуватиметься. У кращому випадку можливо обмежити потенційний розмір дозволеної групи доступу та розмістити її членів

під юридичними чи договірними обмеженнями щодо застосування чи розкриття інформації. Якщо застосування законодавства серйозно розглядається як варіант, важливо підтримувати ефективний аудит доступу. Це само по собі означає потрібність високого рівня безпеки для механізму контролю доступу та пов’язаного з ним аудиту. Їх слід підтримувати за рахунок продуктивності та у випадку декількох відмов, якщо від них потрібно отримати якусь реальну цінність. Однак забезпечення запису є недостатнім; також повинен бути доступний швидкий та ефективний механізм аудиту.

1.12 УПРАВЛІННЯ РИЗИКАМИ

Термін ризик часто застосовується стосовно інформаційних систем. Для розподілених систем потрібно з’ясувати як важливість ризику, так і актуальність управління ризиками . Потрібно розрізняти дві досить різні форми ризику; ризик безпеки та бізнес- ризик. Ризик безпеки пов'язаний з майбутніми подіями, в яких подія призводить лише до втрат. Прикладами є ризик втрати через шахрайство, порушення впевненості в собі та несправність обладнання. Цей тип ризику розглядається тут. Діловий ризик може спричинити за собою збиток або виграш і виникає в результаті звичайних управлінських рішень бізнесу. Ця стаття не висвітлена

Оцінка та управління ризиками – це оперування, яка раціонально враховує активи організації та ризики, з якими вони стикаються, а потім приймає рішення про захист, який їм слід надавати. Важливим елементом рішень є те, що витрати на захист повинні відповідати очікуваним витратам, що виникають внаслідок втрат безпеки. Існує кілька методологій управління ризиками безпеки, пов'язаних з комп'ютером [5]. Всі вони мають спільні завдання:

– ідентифікація та оцінка активів;

– проти нитку до сценаріїв загроз безпеки;

– оцінка ймовірності сценаріїв та втрат, які можуть бути наслідком;

– визначення та вартість можливих заходів безпеки для кожного сценарію;

– вибір портфоліо заходів безпеки.

Аналіз ризиків є найбільш ефективним, коли він проводиться під час специфікації та проектування розробленої розподіленої системи. На цих етапах можуть бути встановлені ризикові наслідки проектних рішень (визначення місця, де проект показує найменш надійні характеристики) та вимоги безпеки та встановлення їх наслідків. Однак ця ідеальна політика рідко практична для розподілених систем, оскільки однією з їх характеристик є те, що вони часто виникають шляхом еволюційного процесу.

1.13 СТАНДАРТИ БЕЗПЕКИ

Існує три основні категорії стандартів безпеки, що стосуються розподілених систем. Перші – це стандарти, що стосуються безпеки окремих комп'ютерів, які існують певний час і є досить зрілими. Другі – це стандарти захисту передачі зв'язку та віддаленої автентифікації. Вони теж досить зрілі. По-третє, в процесі розробки – це ті, які інтегрують стандарти комп'ютерної та комунікаційної безпеки для забезпечення стандартів безпеки розподілених систем.

Стандарти, як правило, не передбачають фізичних чи процедурних механізмів, а також не встановлюють процедур управління ризиками чи оцінки ризиків або вимог щодо їх застосування. Це всі потрібні елементи, які слід врахувати та вирішити для ресурсів, що містять всю розподілену систему. Тому, хоча стандарти безпеки є важливою підтримкою політики безпеки розподіленої системи, їх слід розглядати в контексті загальної політики безпеки, яка також використовує інші заходи.

Критерії оцінювання довірених комп'ютерних систем Міністерства оборони США (TCSEC – помаранчева книга) (Міністерство оборони (США), 1985), займається контролем доступу до окремих систем. Він визначає низку можливих рівнів, які можуть бути розміщені в системі, починаючи від сертифікованого високого рівня безпеки рівня A1 до низького рівня неофіційно визначеного рівня безпеки на рівні C1. Він зазвичай використовується як засіб індикації рівня безпеки, потрібного або забезпеченого в комп'ютерних системах.

Управління доступом поділяється цим стандартом на дві категорії: обов'язковий та дискреційний управління доступом. Попередні правила застосування, які вбудовані в дизайн системи і не можуть бути змінені, крім встановлення нової версії системи. Прикладом може слугувати політика, згідно з якою дані в багатошарових системах безпеки не можуть бути прочитані юзерем із нижчою класифікацією безпеки, ніж призначена для даних. Дискреційні механізми контролю доступу визначаються як такі, які дозволяють юзерам визначати та контролювати обмін ресурсами з іншими юзерами. Наприклад, дискреційна політика контролю доступу на рівні С2 визначається як вимагає механізмів, які забезпечують захист інформації та ресурсів від несанкціонованого доступу, а дозвіл на доступ призначається лише авторизованим юзерам.

Трактована мережева інтерпретація критеріїв оцінювання довіреної комп'ютерної системи (Міністерство оборони (США), 1987) (Червона книга) розширює критерії Червоної книги до мереж. Це головне питання щодо критеріїв безпеки, яким слід дотримуватися під час доступу до віддалених хостів.

Червона книга зараз досить стара, і вона завжди була більш орієнтована на безпеку військового типу, ніж на комерційну безпеку. Зараз впроваджуються уніфіковані критерії – критерії оцінювання інформаційної безпеки інформаційних технологій (ITSEC) (CEC, 1991). Це спільне зобов'язання урядів Великобританії, Нідерландів, Франції та Німеччини. Її метою є врахування потреб комерційних юзерів та вдосконалення Червоної книги шляхом відокремлення узгоджень щодо рівнів безпеки від способу оцінювання безпеки. У Великобританії Департамент торгівлі та промисловості та Група безпеки та зв’язку-електроніки створили Британську схему оцінювання та сертифікації безпеки IT (CESG, 1991), яка оцінює та сертифікує продукцію за критеріями ITSEC. Подібні зусилля ведуться і в інших країнах.

Стандарти безпеки передачі в основному стосуються методів зашифровування. Зокрема, один із алгоритмів став предметом уніфікованих зусиль: алгоритм DES для зашифровування секретного ключа, який є американським, але не міжнародним, стандартом. З іншого боку, алгоритм RSA для зашифровування відкритих ключів є предметом патентів США. Це стало

фактичним стандартом криптографії з відкритим ключем, але через його запатентований статус наразі не визначається як національний або міжнародний стандарт. Ці два алгоритми були коротко описані у розділі II.E.2, вище.

Зашифровування залежить від його міцності від безпеки захищеного обладнання, яке використовується, і (BSI, 86/67937) описує стандарти апаратної безпеки криптографічного обладнання.

Основним стандартом для DES є (NBS, 46), доповнений (ANSI , X3.92). Існують додаткові стандарти, що описують його режими роботи (NBS, 81) та Керівні принципи встановлення та застосування (NBS, 74). Управління ключами в банківських додатках описано в (ANSI, X9.17), але цей стандарт досить виражений узагальнено і застосовуватиметься також і до інших програм. Детальне обговорення стандартів DES знаходиться в (Davies & Price, 1989).

Розроблено низку стандартів для банківських програм для однорангового спілкування та автентифікації меседжів. Вони теж досить загальні за форматом і можуть бути використані для інших цілей. Вони включають (ANSI, X9.19) для автентифікації меседж та (ANSI, X3.118) для особистої автентифікації, використовуючи персональний ідентифікаційний номер (PIN).

Безпека мережі не викликала першочергових проблем, коли вперше почалися зусилля з відкритого системного взаємозв'язку (OSI) наприкінці 1970-х. Однак зараз розробляється низка стандартів ISO, які спрямовані на підвищення безпеки в ОС I. Стандарти визначають служби безпеки, з якими партнери в спілкуванні могли б погодитись, і протоколи, які будуть використовуватися для встановлення безпечної взаемодії.

Служби безпеки, які можуть знадобитися для засобів зв'язку, були визначені в ISO 7498-2 Архітектура безпеки (ISO, 7498-2). Протоколи їх надання досі знаходяться на стадії розробки та ще не доступні в продуктах OSI.

Багато інших заходів із стандартизації мають наслідки для безпеки, а отже, мають стандарти, пов'язані з безпекою, наприклад, в областях Каталог OSI, Управління системою OSI та Електронний обмін даними (EDI). Проводиться кілька подібних та пов’язаних із цим зусиль, включаючи профілі для опису характеристик безпеки вибраних програм.

1.14 СЕРВІС ВІДДАЛЕНОЇ АВТЕНТИФІКАЦІЇ KERBEROS ЯК ЧАСТИНА РОЗПОДІЛЕНИХ СИСТЕМ

Kerberos був спочатку розроблений для розподіленого обчислювального оточення, яке MIT розгорнуло у 1980-х роках як Project Athena. Понад два десятиліття Kerberos, згідно з Інтернет-стандартами, є старшою технологією. Щоб поставити речі в перспективу, Kerberos і DNS з'явилися приблизно в один і той же час. Що стосується безпеки, то зрілість є надзвичайно бажаною: відкриті, широко використовувані та широко вивчені технології є найбільш передбачуваними безпечними і найменш схильні до нових подвигів.

Як і DNS, Kerberos вийшов із чіткої уваги на чітко визначене завдання. У таких оточеннях, як Ath ena, що є звичним сьогодні, але новим часом, від окремого юзера можна очікувати застосування багатьох різних робочих станцій (і багатьох різних сервісів, таких як доступ до файлів та друк, розміщених на багатьох різних сервісах).

Оригінальним питанням, що постало перед розробниками Kerberos-a, було те, як забезпечити єдиний вхід : дозволити юзерам отримувати доступ до різноманітних систем і служб, не потребуючи введення свого ідентифікатора юзера та пароля неодноразово (або, що ще гірше, без потрібності запам’ятовувати та надавати різні ідентифікатори юзерів та паролі для кожної з різних систем та сервісів, які вони використовують).

Хоча оригінальний Kerberos був розроблений для єдиного оточення, він базувався на чіткій архітектурній моделі, застосовній до інших середовищ. Через цю міцну архітектурну основу, Kerberos, як і DNS, міг зростати та підтримувати масштаб та широту функцій, які мало можна уявити під час свого первісного створення. Сьогодні Kerberos забезпечує не тільки єдиний вхід, він також забезпечує надійну загальну основу f або безпечну автентифікацію у відкритих розподілених системах.

Криптографічно безпечний, архітектурно звуковий і легко інтегрується як компонент в інші системи, Kerberos широко сприймається як спосіб надання

основного набору служб безпеки для багатьох розроблених системних проектів і розробок, і сьогодні є невід'ємною частиною багатьох обчислювальних середовищ. Майже у всіх популярних операційних системах (ОС) вбудований Kerberos, як і у багатьох важливих програм, і він широко використовується постачальником мережевого обладнання. Як і DNS, Kerberos – це сервіс, який більшість юзерів навіть не розуміють, що вони користуються, але він дозволяє багато взаемодій, що відбуваються в сучасних корпоративних мережах.

РОЗДІЛ 2
ОСНОВИ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ВІДДАЛЕНОГО СЕРВЕРА

Kerberos – це технологія, яка дозволяє зробити сильну аутентифікацію у відкритих, розподілених мережах. Це надійне рішення щодо безпеки з чотирьох основних причин:

1. Керберос зрілий. Він широко застосовується і широко вивчається протягом тривалого часу. Що стосується безпеки, то це дуже важливо.

2. Kerberos відповідає вимогам сучасних розподілених систем. Він був розроблений у відповідь на чітко визначений і чітко продуманий набір вимог щодо безпечної автентифікації у відкритому середовищі з незахищеними комунікаційними зв’язками; виявилося, що ці вимоги тісно відповідають вимогам сучасних розподілених систем, що працюють по мережах на основі Інтернет-протоколів.

3. Керберос є архітектурно здоровим. Він розроблений навколо чіткого набору архітектурних та функціональних абстракцій; що архітектурна обґрунтованість дозволила йому розвиватися з часом, і полегшує інтеграцію його в інші системи. Ця ж архітектурна міцність дозволяє легко проаналізувати, як поводитиметься Керберос.

4. Kerberos вже інтегрований у найпопулярніші операційні системи та багато широко використовувані програмні програми. Це невід'ємна частина сьогоднішньої IT-інфраструктури.

2.1 Вимоги, як основа проектування архітектури сервера віддаленої автентифікації

Запорукою успішної розбудови системи є чітке розуміння вимог – як функціональних вимог, що описують, що система повинна робити, так і нефункціональних вимог, що описують, серед іншого, середовище, в якому вона повинна працювати. Як і у більшості технічних рішень, правильне отримання

вимог на самому початку є найважливішим кроком. Широко оприлюднені недоліки деяких сучасних мережевих сервісів (наприклад, NFS, WEP, взаємодія веб-браузера / сервера) часто є наслідком невдавання правильних вимог.

Що характерно для Кербероса, це не лише те, що оригінальні архітектори проникливо розуміли відповідні вимоги, але й тому, що вони залишаються віддані всім необхідним крокам для повного їх вирішення, багато з яких на той момент здавалися «надмірними». Оскільки багато характеристик середовища Афіни стосуються також сучасних Інтернет та корпоративних інтранет, цей підхід залишається принципово надійним і сьогодні.

Основні вимоги, на яких базується Керберос, включають:

– Єдиний вхід для користувачів: В Діві lopers з Kerberos зрозуміла, що користувачі не повинні приймати постійні проблеми аутентифікації від кожної служби вони доступ. Сучасна павутина наочно ілюструє безліч головних болів, які виникають через невиконання цієї основної вимоги. Що характерно для Kerberos, це те, що він фактично дозволяє взаємну аутентифікацію для кожного сеансу зв'язку, який користувач встановлює за допомогою сервісів, але він управляє цими процедурами аутентифікації "під кришками", коли користувач спочатку успішно аутентифікується через систему Kerberos.

– Робота в розподілених системах на основі відкритої моделі Інтернету: Project Athena була новим академічним обчислювальним середовищем, заснованим повністю на розподілених робочих станціях та серверах, що працюють через відкритий Інтернет з кількома, якщо такі є, зовнішніми або внутрішніми межами безпеки. У цьому сенсі це було так, як сьогодні є загальнодоступний Інтернет, зі студентським органом, відомим своєю майстерністю та творчістю у використанні будь-яких вад у будь-якій системі.

– Інтеграція з існуючою технологією: Однак, як системна вимога, Kerberos повинен був співіснувати та підтримувати широкий спектр стандартних та користувацьких послуг, використовуючи стек протоколів IP.

– Взаємна автентифікація сторін повинна відбуватися до обміну будь-якою інформацією: Сервер повинен бути не лише переконаний у справжності клієнта, але й клієнт повинен бути впевнений у достовірності сервера. У

відкритому середовищі шахрайські сервери, що крадуть дані клієнтів, є настільки ж загрозою, як і самозванець, що представляє реальних клієнтів. Багато систем аутентифікації схильні зосереджуватись на автентифікації користувачів, що залишає користувачів, що піддаються атакам зловмисних служб, що представляють собою послугу, на яку користувач покладається. Наприклад, сьогоднішні фішинг-атаки, як правило, використовують слабку аутентифікацію служб, щоб захопити користувачів і захопити облікові дані для входу або іншу інформацію про чутливість. На думку Кербероса, він повністю підтримує взаємну аутентифікацію, хоча автентифікація послуги клієнтом не є обов'язковою.

– Паролі ніколи не слід виставляти під час аутентифікації: пароль, який ніколи не розголошується та не надсилається по мережі, зловмиснику набагато складніше зламати. Отже, автентифікація користувачів Kerberos не вимагає надання паролів службі аутентифікації. Натомість сервіс аутентифікації Kerberos використовує криптографічні протоколи, за допомогою яких користувач може доводити володіння паролем, фактично не перекриваючи його.

– Центральне адміністрування секретів аутентифікації: У розповсюдженому середовищі було б незручно в крайньому випадку підтримувати спільні секрети, такі як паролі на кожному клієнті та сервері, які потребують аутентифікації запитів. Крім того, розповсюдження загальних секретів у багатьох системах збільшує потенційні вразливості прямо пропорційно кількості систем – проблема, що посилюється явищем «найслабшого зв’язку». Kerberos вирішує цю вимогу, підтримуючи централізовану базу даних, яка розповсюджується лише на декілька серверів аутентифікації. Хоча загальна безпека критично залежить від захисту цієї центральної бази даних, набагато простіше загартувати кілька серверів спеціального призначення від атак, ніж захистити багато систем загального призначення. Центральний контроль за секретами аутентифікації також полегшує видачу нових облікових даних, анулювання існуючих та вилучення з компрометованих облікових даних.

– Використання криптографічних заходів: У той час, коли Керберос був спочатку розроблений, криптогрудні заходи рідко використовувалися як засіб для досягнення безпеки, і насправді вважалося радикальним вимагати використання

шифрування. На щастя, розробники Kerberos визнали, що криптографія – це не просто розумна математика; це було еззе ntial для запобігання розголошенню інформації аутентифікації у відкритому середовищі, в якій ворожі сторони мають доступ. Незважаючи на численні нетехнічні виклики, розробники Kerberos дотримувались цієї вимоги, і їх переконання витримали тест часу і багатьох противників на цьому шляху. Скориставшись новішими криптографічними алгоритмами, коли вони з'явилися, Керберос зберіг цю основну перевагу.

– Підтримуйте довільний розподіл сервісів та користувачів: Kerberos не встановлює обмежень щодо взаємодії користувачів із службами в розподіленому середовищі або навіть того, як служби взаємодіють між собою, але це дозволяє кожному взаємодії передувати сильну аутентифікацію сторін та взаємну аутентифікація за потребою. Щоб проілюструвати цю точку, модель афіни передбачала, що користувачі можуть зайти на будь-яку наявну робочу станцію, підтвердити автентифікацію, а робоча станція буде кешувати інформацію ("квитки"), яка може бути використана для аутентифікації всіх служб, з якими згодом взаємодіяли. Коли вони закінчать користуватися робочою станцією, вони вийдуть локально, що очистить усі встановлені сеанси та квитки, тим самим дозволивши іншому користувачеві взяти на себе використання робочої станції, не маючи доступу до будь-якої інформації, яку наші сервіси пов’язані з пріоритетним користувачем. Хоча подальша наявність недорогих персональних комп’ютерів, як правило, застаріла дана модель, сьогодні аспекти оригінальної моделі знову з'являються, оскільки користувачі схильні переходити зі своїми комп’ютерами до різних підмереж та гарячих точок Інтернету Wi-Fi.

– Не довіряйте жодній стороні до отримання автентичності: в академічних мережах зазвичай застосовується базова політика "дозволяти все, крім того, що явно заборонено", тоді як неакадемічні мережі починаються з протилежної політики "заборонити все, окрім того, що прямо не дозволено". Незважаючи на своє академічне походження, Керберос насправді наближений до неакадемічного режиму політики, оскільки він передбачає, що жодній стороні не можна довіряти, поки не засвідчити автентичність. Розробники Kerberos зрозуміли, що їм потрібно підтримувати автентифікацію, авторизацію та контроль

доступу у ворожій обстановці, що ґрунтувалася на політичному режимі "дозволити все". Вони розробили компромісний підхід, який дозволив користувачам і службам вирішити, чи потрібно довіряти іншій стороні, і, якщо це так, довіру буде надано лише сторонам, які могли пройти автентифікацію за допомогою сервісів Kerberos.

– Розробники Kerberos припускали, що будь-хто може підслухати мережевий трафік, може претендувати на будь-якого користувача та може налаштувати шахрайські сервери, здатні використовувати будь-яку законну послугу, включаючи самі сервіси Kerberos. Шифрування використовувалося для запобігання атак підслуховування, а ключі сеансу були введені разом із мітками часу для запобігання повторних атак. Коли користувачі (або хости / послуги) підтверджують автентифікацію до служби аутентифікації Kerberos, служба аутентифікації, у свою чергу, автентифікує себе користувачеві (або хосту / службі), підтверджуючи, що він знає раніше встановлений загальний секрет. Побічним продуктом цих контрзаходів є те, що Керберос забезпечує протидію атакам між людьми в середині, які, як правило, вважалися нездійсненними на той час, і протягом більше десяти років після того, як Керберос був початково розгорнутий. На жаль, напади людини в середині вже не є просто вигадкою, і вони надто поширені в сьогоднішній Інтернет-Інтернеті, який не був розроблений з вражаючим оточенням.

2.2 Модель для аутентифікації та авторизації Kerberos

Kerberos – це більше, ніж набір протоколів – він пропонує системну модель для аутентифікації та подальшої авторизації у орієнтованому на однорангових, розподіленому обчислювальному середовищі. Важливими аспектами моделі є:

1. Він характеризує середовище та взаємодію між агентами таким чином, що сумісний з більшістю розповсюджених системних підходів, полегшуючи інтеграцію Kerberos в додатки та системи.

2. Він концентрує підтримку секретів (тобто збережених паролів) у невеликій кількості місць (що може бути відповідним чином загартовано), а не розповсюдження їх по всій системі.

3. Kerberos відокремлює автентифікацію від самих сервісів. Наприклад, файловий сервер не знає і не запитує пароль користувача. Натомість він делегує цю роботу Керберосу та покладається на інформацію, надану Керберосом, щоб визначити достовірність запиту.

4. Він не вимагає, щоб усі сторони, що спілкуються, мали попередні стосунки між собою, а також раніше не ділилися між собою будь-якою інформацією для аутентифікації. Натомість усі сторони встановлюють попередні зв'язки зі службою Kerberos і покладаються на неї для перевірки облікових даних та авторизації сесій.

Повна архітектура і протокол буде описано далі. Цей навмисне спрощений опис підкреслює яскраві моменти (рис. 2.1).

Архітектура Kerberos розроблена навколо повідомлень, що обмінюються між трьома видами сутностей:

1. Клієнти, які бажають користуватися послугами,

2. Сервери, які надають послуги (зауважте, що клієнти та сервери спільно називаються директорами)

3. Сервери, які керують самим протоколом Kerberos. Ці сервери часто називають "KDC" (ключові центри розподілу) і насправді містять кілька модульних сервісів.

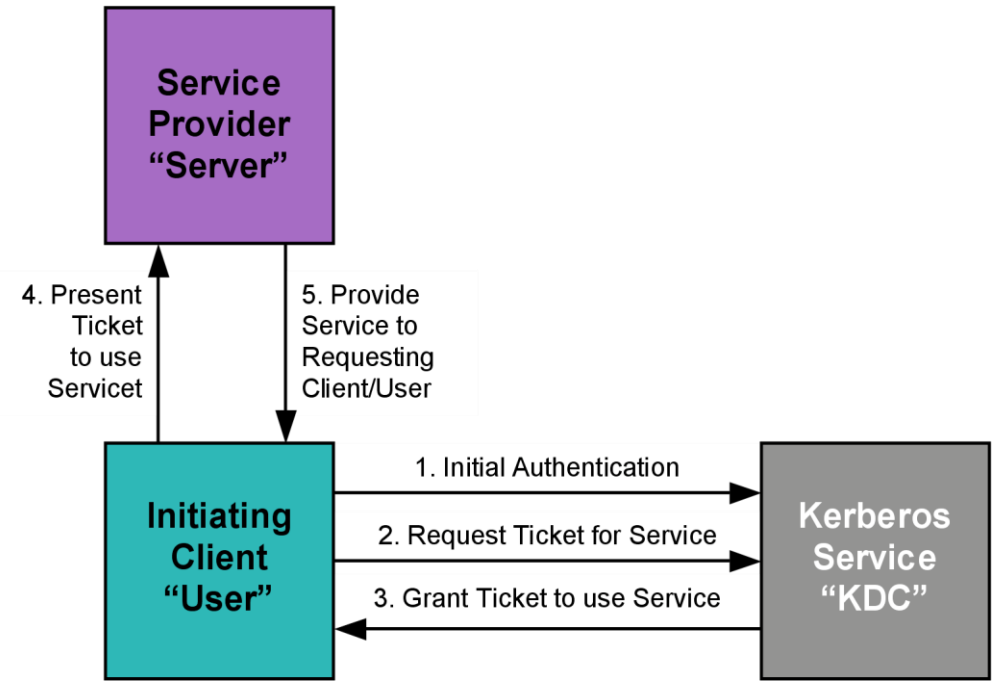


Рисунок 2.1 – Спрощена модель Kerberos із спрощеної моделі

Клієнти та сервери аутентифікують один одного за допомогою протоколу, що включає обмін квитками: криптографічно захищені структури часу з печаткою часу, що містять інформацію про автентифікацію та інші деталі щодо конкретного запропонованого видалення між клієнтом та сервером.

– Коли в систему додається новий головний (клієнт або сервер) або при зміні облікових даних, секретар (наприклад, пароль) ділиться між головним і сервером Kerberos. Цей етап налаштування – це єдиний час, коли секрети потрібно обміняти.

– Згодом, коли клієнт бажає увійти в систему, він отримує квиток від сервера Kerberos. Клієнт не розкриває свою таємницю під час отримання квитка. Натомість квиток побудований таким, коли розшифрувати та використовувати його може лише той, хто володіє клієнтською таємницею.

– Коли клієнти хочуть отримати доступ до серверів, вони аутентифікують себе на серверах, представляючи квитки. Ще раз, ніяких секретів не обмінюються; сервісний квиток шифрується та доставляється таким чином, що його міг отримати лише законний клієнт, і лише законний сервер може розшифрувати його.

– Зауважте, що між сервером та інфраструктурою Kerberos немає зв'язку в режимі реального часу.

За останні два десятиліття модель Кербероса добре піднялася. Що ще важливіше, ця модель дозволила протоколам Kerberos та системним специфікаціям розвиватися для задоволення нових вимог без необхідності зміни базової архітектури. Чинні стандарти (звані «версія 5») представляють третє покоління еволюції Kerberos, але залишаються надзвичайно узгодженими з оригінальною моделлю. Це дозволило відбутися значні зміни "під кришкою", не змінюючи істотної форми та функції служб Kerberos. Сьогоднішні протоколи Kerberos є розширюваними, підтримують декілька криптографічних алгоритмів, дозволяють альтернативні механізми аутентифікації, підтримують масштабовані системи та дозволяють проходити автентифікацію та авторизацію через організаційні межі, але істотна модель взаємодій залишається тією ж.

2.3 Стандарти розробки сервера Kerberos

Той факт, що модель системи Kerberos залишилася неушкодженою протягом декількох десятиліть еволюції, говорить про основну силу підходу. Не менш важливим є ступінь, в якому Kerberos був стандартизований та інтегрований в інфраструктуру мереж підприємств.

Хоча деякі стандарти просто намагаються відобразити деталі конкретної реалізації, стандарти Kerberos фактично використовуються для керівництва декількома незалежними реалізаціями – як у межах спільнот з відкритим кодом, так і від основних постачальників, таких як Apple, Cisco, Google, Intel, Oracle, Microsoft та Sun. Kerberos є дещо унікальним як відкритий стандарт, для якого існують як відкриті, так і фірмові реалізації. Крім того, еволюція Kerberos була керована як розробниками з відкритим кодом, так і основними постачальниками.

IETF слугує платформою, де спочатку норми Kerberos були стандартними, і вона продовжує залишатися спільнотою, де еволюціонували стандарти Kerberos. Робоча група Kerberos в IETF (krb-wg) активно працює над подальшими

доопрацюваннями та розширеннями специфікацій Kerberos, тобто еволюція триває.

Kerberos також використовував і використовував інші стандарти для полегшення інтеграції з новими технологіями та додатками. Наприклад, Kerberos тепер підтримує стандарт шифрування AES (FIPS 197) і працює над підтримкою вдосконалених хеш-алгоритмів hms, визначених FIPS 180. На передній панелі програми було прийнято Інтерфейс прикладного програмування служб безпеки IETF (GSS-API). розробниками Kerberos на ранніх термінах як засіб для полегшення інтеграції Kerberos у додатки. На початку 1990-х The Open Group прийняла Kerberos як основну технологію аутентифікації для використання в їх сімействі специфікацій розподіленого обчислювального середовища (DCE), що згодом вплинуло на багато інших продуктів.

Комерційна продукція всіх типів продовжує сприймати Керберос, і тепер вона вбудована у безліч загальних пропозицій товарів. Наприклад, Kerberos – це технологія аутентифікації за замовчуванням у сімействі Microsoft Windows операційних систем клієнта та сервера з часу впровадження Windows 2000 Professional та Windows 2000 Server. Аналогічно, він є продуктом аутентифікації за замовчуванням у сімействі Mac OS X Apple і відіграє розширену роль в останньому випуску 10.5 (він же "Leopard"). Sun Microsystems давно використовує Kerberos в рамках Solaris та інших програмних продуктів Sun, включаючи Java, як загальну платформу аутентифікації. Постачальники мережевих технологій, такі як Cisco та TeamF1, також застосували Kerberos як переважну технологію аутентифікації для адміністрування системи та інших вимог контролю доступу. Intel навіть використовує Kerberos для автентифікації доступу до функцій віддаленого адміністрування системи, вбудованих в останнє сімейство мікропроцесорів.

На передній панелі Unix / NetBSD / Linux Kerberos ретельно інтегрований і поставляється як схема автентифікації за замовчуванням для багатьох популярних дистрибутивів. Він також включений у безліч вбудованих ароматів Linux, а тому знаходить свій шлях у мережевих приладах усіх типів.

Справжня заслуга стандарту полягає не в тій чи іншій структурі органу зі стандартів, який видає технічні характеристики, ані в різноманітності та широті прийняття, а в здатності різних систем взаємодіяти. У цьому плані Керберос надзвичайно успішний. У багатьох сучасних корпоративних мережах Kerberos покладається на створення загального рішення для аутентифікації та авторизації, яке дозволяє кінцевим користувачам та системним адміністраторам отримувати перевагу від єдиного входу на все: від серверів баз даних до електронних служб до принтерів до мережевих пристроїв. Nextmor e, не має значення, на якій ОС працює платформа користувача або на якій ОС працює служба.

Будь-яка технологія безпеки, яка має намір надати сильну аутентифікацію та авторизацію в розповсюдженому середовищі Інтернет-протоколів, буде ретельно перевірена в реальному світі. Безумовно, Керберос пережив незліченні напади протягом тривалого періоду в багатьох дуже ворожих умовах. На нього було піддано всі форми атаки, часто зловмисники, що знають, як налаштовані служби Kerberos. Хоча ідеальної безпеки немає, консенсус полягає в тому, що Керб ерос добре витримав ці виклики. Якби цього не було, воно, безумовно, отримало б багато негативного розголосу.

Крім того, Kerberos був розгорнутий у багатьох різних середовищах. Це розширило коло загроз далеко за межі того, що може виникнути в академічному чи підприємницькому середовищі. Наприклад, Керберос використовувався для захисту інформаційних активів урядових установ, у тому числі агентств, які стикаються з державними нападами на інформацію. Kerberos також, як правило, використовується для управління захоплюючим доступом до цілей високої якості, знайдених у кожній мережі, таких як брандмауері, маршрутизатори, комутатори, сервери та послуги DNS / каталогів. Цей розширений контекст загрози призвів до кращого розуміння того, як Керберос може поводитися з широким спектром загроз.

Протягом свого життя Kerberos був широко проаналізований дослідниками безпеки та тестувальниками проникнення, які прагнули виявити вразливості, які потрібно виправити. Здебільшого цей аналіз призвів до виявлення та виправлення проблем до розгортання життєздатних подвигів у природі. Знову ж таки, жодна

система не може бути захищеною від усіх форм нападу, але широкий аналіз широкої спільноти, що включає розробників, користувачів, системних адміністраторів та дослідників безпеки, допомагає зменшити ризики. Інакше кажучи, Керберос був ретельно перевірений як друзями, так і ворогами, і він тримався досить добре.

Чому Kerberos варто враховувати сьогоднішні системи?

Будучи зрілим широко розповсюдженим рішенням безпеки, відкритого стандарту, Kerberos користується широкою спільнотою розробників, яка включає декілька ініціатив з відкритим кодом, які працюють паралельно комерційним розробкам від основних постачальників. Взаємодія спільноти розвитку Kerberos через органи галузевих стандартів, консорціум MIT Kerberos та взаємодію продуктів у виробничих середовищах. Оскільки такі постачальники, як Apple, Microsoft і Sun, розробили розширення до протоколів Kerberos, тенденція полягала в тому, щоб ці розширення стали частиною "стандарту" і включалися в інші реалізації Kerberos.

Широке співтовариство розробників, що працює з Kerberos, також призвело до інтеграції з іншими технологіями, такими як служби каталогів, управління політикою, багатофакторна автентифікація, Java та послуги файлів / баз даних. У багатьох випадках ці зусилля щодо інтеграції Кербероса з іншими технологіями привели до нового розуміння того, як поліпшити та розширити Керберос. Результатом став сприятливий цикл розвитку та інтеграції, який дав багато синергетичних результатів.

Kerberos також може бути безпосередньо інтегрований у додатки, які працюють у розподіленому або транзакційному контексті, де автентифікація та авторизація є життєво важливими для забезпечення операційних середовищ. Наприклад, основні платформи бази даних мають вбудовану підтримку для Kerberos. Зважаючи на труднощі в отриманні автентичності / авторизації «правильно», Kerberos також є розумним способом для нових додатків, включаючи власні власні додатки, додати нові вимоги безпеки. Крім того, додатки на базі Kerberos також виграють від централізованого управління політикою та встановленого режиму управління та аудиту системи.

API загальних служб безпеки (API GSS) був представлений на початку 1990-х, і Kerberos був однією з перших служб безпеки, яка підтримала цей важливий галузевий стандарт для інтеграції додатків. Оскільки всі основні постачальники ОС, які також підтримують Kerberos у самому світі, сьогоднішні розробники додатків мають численні можливості для інтеграції підтримки Kerberos таким чином, щоб принести користь користувачам та операторам.

2.4 Масштабованість сервера

Керберос, що має однакове значення, виявив здатність до масштабування найбільших організацій. Він також підтримує окремі адміністративні сфери послуги, які можна використовувати для розширення автентифікації та авторизації через межі організації. Це може допомогти полегшити взаємодію між діловими партнерами та клієнтами у сучасних дедалі більш об'єднаних моделях взаємодії.

Оригінальна модель Curberos була розроблена для задоволення потреб цілого університетського містечка з тисячами користувачів та систем. Ця модель також добре працювала для багатьох підприємств та державних установ. Однак, оскільки масштаби Інтернету зросли разом з багатьма внутрішньомережевими мережами – мережами, що працюють в межах великих глобальних організацій – модель Кербероса потрібно було розширити, щоб забезпечити достатню масштабованість.

Це було досягнуто, ввівши Kerberos "царства", які працюють автономно, але розширюють автентичні послуги і служби авторизації з однієї сфери в іншу. Наприклад, велика корпорація може розміщувати окремі царини Kerberos на кожному з своїх основних сайтів, але користувачі все одно зможуть використовувати серверні сервіси для аутентифікації та отримання доступу до сервісів у всій корпорації.

Це аналогічно тому, що служби Microsoft Windows розгортаються як взаємопов’язані «домени», а насправді домен Windows, по суті, також є цариною Kerberos. Подібні стратегії також використовуються для масштабування служб

каталогів у великій організації, а домен Windows надасть сферу Kerberos, яка використовує службу каталогу Windows для адміністрування облікових записів користувачів. Використовуючи підхід інтегрованого сервісу, сучасні розподілені системи, що використовують Керберос, можуть бути розгорнуті в глобальному масштабі, але дозволяють користувачам працювати по всьому підприємству, в той час як системні адміністратори можуть керувати дотриманням політики як на місцевому, так і на глобальному рівні. Apple і Sun, поряд з дистрибутивом з відкритим кодом, використовують подібні стратегії інтеграції царств Kerberos з службами каталогів для спрощення загальної системи розгортання та адміністрування.

Зростання Інтернету також призвело до зростання потреб користувачів до доступу до послуг за межами одного підприємства. eCommerc e, аутсорсинг та галузь "екстранети" сприяли зростаючій потребі в аутентифікації та авторизації для переходу організаційних меж. Одним із підходів до вирішення цього виклику, що набуває прийняття, є "федеративна модель" аутентифікації, згідно з якою встановлюється правова та технічна база, яка дозволяє одній організації розраховувати на іншу для аутентифікації сторін, незалежно від того, що це окремі користувачі чи послуги.

Розроблена розширена модель Kerberos, яка включає сфери з аутентифікацією міжреальними сферами, також була розроблена для вирішення потреби в аутентифікації між організаціями і по суті є ранньою реалізацією федеральної моделі. Враховуючи зрілість і широке прийняття Kerberos, він вже відіграє значну роль у системах автентифікації / авторизації у федеральному світі.

Kerberos вже давно використовується для централізованого адміністрування політик щодо використання паролів, реєстрації користувачів та серверів, а також скасування облікових записів. По мірі того, як у багатьох регуляторних та псевдорегулюючих органів з'явилася політика, що надана зовнішнім законодавством, управління політикою набуває все більшого значення. Інструменти адміністрування політики в Керберосі розвивалися протягом багатьох років і були доповнені численними розробками. Адміністрація Kerberos часто інтегрується з іншими системними службами, такими як служби каталогів

та адміністрація користувачів. Це допомагає уникнути дублювання зусиль у встановленні та застосуванні політик на системному рівні.

Відворотним боком адміністрування політики є можливість аудиту системи на предмет дотримання політики. Модель Kerberos, яка використовується разом з іншими інструментами, такими як реєстрація в центральній системі, забезпечує поглиблену підтримку аудиту систем, а також механізми f або вжиття коригувальних заходів при виявленні порушень політики. Є навіть ThirdParty розробників (наприклад, Centrify), які надають кошти для систем аудиту Kerberos на основі і інтегроване управління політикою для систем, які включають в себе Kerberos поряд з іншими заходами безпеки.

Стара приказка про стандарти – у нас їх так багато для вибору – стає з кожним роком все більш вірною. Незважаючи на те, що стандарти необхідні, на сьогодні дійсно важливим є взаємодія між продуктами та послугами багатьох постачальників. Для служб аутентифікації та авторизації необхідна також сумісність у різних класах систем, починаючи від мережевих пристроїв до мейнфреймів, від портативних комп'ютерів до робочих станцій або від локального додатку до програми «Програмне забезпечення як послуга» («SaaS»). Керберос вирішує всі ці проблеми інтероперабельності сьогодні і відіграє більшу роль у нових стандартах, які намагаються поєднати все більш різноманітні нитки інформаційних технологій.

Іншим аспектом взаємодії, який іноді не помічається, є необхідність співіснування з альтернативними рішеннями. З добрих і поважних причин, а тому, що саме так воно є, існує і буде існувати безліч методологій вирішення проблем аутентифікації та авторизації. Будучи зрілим рішенням, яке тривалий час знаходилося в "наборі" для IT, Kerberos вплинув на інші рішення безпеки та на нього вплинули інші розробки в галузі безпеки. Це дало змогу створити різні стратегії співіснування альтернативних підходів до безпеки в одному середовищі.

Однією з цих ілюстрацій є пропозиції в ОС від великих гравців, таких як Apple, Microsoft та Sun. Кожен з цих постачальників ОС ретельно інтегрував Kerberos у свої програмні пропозиції, але вони також підтримують альтернативні підходи та надають розробникам додатків інструменти для підтримки бажаних

користувачами заходів аутентифікації. У багатьох випадках програми можуть бути вбудовані в API (включаючи API GSS), що дозволяє користувачам визначати, як слід виконувати аутентифікацію та авторизацію для цієї програми в їх оточенні. Відкриті джерела Linux та NetBSD також застосовують аналогічні підходи до забезпечення співіснування.

Іншим аспектом співіснування є підтримка різних схем надання багатофакторної аутентифікації. Хоча Kerberos спочатку був розгорнутий за допомогою підходу до автентифікації, який базується на паролях, сьогодні він підтримує багато популярних багатофакторних схем, включаючи токени одноразового пароля (OTP), смарт-карти та різні біометричні сканери.

2.5 Вибір механізмів аутентифікації

Окрім підтримки цифрових сертифікатів та інфраструктури відкритих ключів (PKI) для аутентифікації, до Kerbero s були адаптовані багато інших технологій аутентифікації, включаючи різні багатофакторні рішення. Наприклад, смарт-карти та інші пристрої, які покладаються на серти, як правило, працюють «поза коробкою» з Kerberos, і вони підтримуються великими постачальниками.

Різні схеми одноразового пароля (OTP) також були пристосовані для роботи з Kerberos, включаючи популярні "ключі", які відображають унікальні коди для кожної операції аутентифікації. Крім того, Kerberos був інтегрований із загальними біометричними сканерами, тим самим забезпечуючи подальші варіанти багатофакторної аутентифікації.

Інтеграція нових технологій аутентифікації в Kerberos є простою розробкою, яка використовує перевагу послідовної моделі Kerberos, щоб дозволити розробникам вдосконалити прийняття за рахунок використання широкої встановленої бази Kerberos. Оскільки K erberos ізолює програми та послуги від початкового процесу автентифікації користувачів, переваги нових технологій багатофакторної аутентифікації можна легко поширити на багато існуючих додатків чи служб.

У технологічній базі, яка поставляється інтегрована з багатьма поза-шельфових платформ, Kerberos може бути більш економічно ефективним для використання по порівнянні з іншими технологіями, які повинні бути «болтах на.» Системні адміністратори, як правило, мати справу з Kerberos в рамках всієї системи вони вже керують, а нові розгортання або оновлення включають Kerberos як частину загального пакету. У той же час, якщо необхідно запровадити нові технології аутентифікації (наприклад, у відповідь на нові нормативні вимоги), Kerberos може надати готові «розетки», до яких ці нові технології можуть бути включені.

Підтримка Kerberos зазвичай також є частиною "пакетної угоди". Існуючі договори на підтримку та внутрішня підтримка персоналу є попередніми зобов'язаннями ресурсів, тому використання технології аутентифікації, яка включена до таких механізмів підтримки, допомагає уникнути накопичення нових витрат на підтримку.

Там, де Керберос часто виплачує дивіденди, – це його здатність розширювати автентифікацію та авторизацію на різних платформах. Для ілюстрації, якщо організація розгортає первинну платформу, що включає Kerberos, інтегрований з додатковим набором служб каталогів та інструментів системного адміністрування, ці послуги можуть бути застосовані до інших платформ, мережевого обладнання, управління об'єктами та в терапії з клієнтами або бізнесом партнери. У змішаних середовищах платформи це може означати значне зниження витрат на підтримку, полегшуючи роботу користувачів та системних адміністраторів на змішаних платформах.

Як відкритий стандарт, який підтримується декількома спільнотами з розробленим відкритим кодом, технологія Kerberos доступна для всіх, щоб використовувати, вдосконалювати або інтегрувати їх у свої програми чи продукти. Технічно спроможні організації можуть повністю підтримувати власне використання Kerberos, оскільки вони мають повний доступ до технології, а також доступ до спільнот розвитку. Вони можуть навіть розробити власні розширення до Керберосу.

Організації, які інтегрують Kerberos у додатки чи програми, також мають доступ до спеціальних фірм, що підтримують, які можуть надати досвід інтеграції та тестування. Крім того, багато інших продуктів та інструментів вже інтегровано з Kerberos, що може ще більше зменшити зусилля з розвитку. Коли додатки доставлятимуться користувачам або клієнтам, навантаження на підтримку також зменшиться, оскільки Kerberos, ймовірно, вже використовується в цільовому середовищі.

Однак більшість організацій не хочуть підтримувати Kerberos на рівні вихідного коду. Зазвичай вони отримуватимуть підтримку від своїх існуючих постачальників платформ та додатків, і навіть не можуть вважати Kerberos як позицію у своїх контрактах на підтримку.

Kerberos передує протоколам SSL / TLS. Отже, його творцям довелося реалізувати захищений протокол автентифікації, який не мав доступу до всюдисущої технології шифрування транспортного рівня, доступної сьогодні.

2.6 Системні актори реалізації протоколу

Спочатку опишемо кілька акторів Кербероса, які нам потрібно знати.

Область: набір мережевих вузлів (хостів, робочих станцій, VM, серверів тощо), які мають спільну базу даних Kerberos. Мені подобається думати про це як про всі ці вузли плюс KDC (і пов'язану з ним базу даних). Це приводить його у відповідність до визначень, які я дав для подібних концепцій в інших протоколах ідентичності.

Принцип: унікальна особа, якій можна присвоїти квитки на Kerberos. Це може бути клієнт, користувач або сервер, який надає послугу. Основна назва е в Kerberos v5 має форму первинний / екземпляр @ REALM.

Хости / Клієнти: Процес, хост, сервер, VM або інший мережевий вузол, який використовує мережевий сервіс (який розуміє Kerberos і є частиною того ж Царства або Царства, яким довіряється) від імені користувача.

Сервер (іноді його називають Сервером сервісів – SS): Конкретний Принцип, який надає ресурс мережевим Клієнтам. Сервер також іноді називають сервером прикладних програм.

Сервіс: ресурс, що надається мережевим клієнтам. Як правило, надається більш ніж одним сервером.

Центр розподілу ключів (KDC): послуга мережі, яка постачає квитки та тимчасові ключі сеансу; або екземпляр тієї служби або хоста, на якому вона працює. KDC обслуговує як початковий, так і запит на отримання квитків. До його складу входить Служба аутентифікації та сервер надання квитків (див. Нижче).

Сервер аутентифікації (AS): компонент KDC, який обробляє початковий запит і видає TGT. AS несе відповідальність за підтримку бази даних про принципалів (користувачів та серверів) та пов'язані з ними секретні ключі.

Сервер надання квитків (TGS): компонент KDC, який обробляє етап надання квитка протоколу Kerberos. Це видає квитки на запитувані послуги.

2.7 Екологічні припущення

Специфікація Kerberos v5 робить такі припущення:

Атаки "відмови в обслуговуванні" не вирішуються за допомогою Curb eros. Хоча розширення та впровадження створили механізми, які захищають від таких атак.

Елементи мережі (комп'ютери) обов'язково зберігають свої секретні ключі в секреті. Якщо пароль порушений, система не настільки захищена.

Керберос не вирішує атаки "вгадування паролем". Знову ж таки, розширення та впровадження встановили механізми, які захищають від цього.

Кожен хост у мережі обов'язково має мати годинник, який "слабко синхронізований" з часом інших хостів. Більшість протоколів ідентичності, які часто використовуються сьогодні, мають цю вимогу.

Основні ідентифікатори не переробляються короткочасно. Не використовуйте повторно імена користувачів та серверів.

2.8 Перехресна автентифікація

Kerberos v5 підтримує аутентифікацію та взаємодію між суб'єктами в різних сферах Kerberos. Щоб все було просто, ми будемо вважати, що всі актори знаходяться в одній царині Керберос для цієї дискусії.

Підпротоколи.

Протокол аутентифікації Kerberos визначає три підпротоколи (або повідомлення виключення повідомлень). До них належать:

- Служба обміну аутентифікацією.
- Обмін сервісами Token.
- Обмін клієнтом / сервером.
- На діаграмах протоколів, наведених нижче, всі три описані.

РОЗІДЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 NTP та синхронізація часу

Усі учасники Kerberos повинні синхронізувати час до джерела поточного часу – як і більшість протоколів ідентичності. Зазвичай це робиться за допомогою мережевого протоколу часу (NTP). Якщо часи не синхронізовані, то виникнуть дивні проблеми.

TCP проти UDP.

Протокол Kerberos використовує порт 88 (UCP або TCP, обидва повинні підтримуватися) на KDC при використанні в мережі IP. Spec підтримує альтернативні порти; особливо для підтримки декількох областей Kerberos на одному сервері. Клієнти повинні підтримувати використання TCP, але можуть використовувати UDP. Деякі розширення до специфікації Kerberos v5 не вдасться застосувати, якщо TCP не використовується. Клієнт може надсилати декілька повідомлень із запитом до того, як отримає відповідь – однак, щоб це спростити, ми не будемо намагатися цього робити.

Оскільки Kerberos може працювати на ненадійних транспортних протоколах, таких як UDP, учасники Kerberos повинні бути готові до повторної передачі повідомлень, які, можливо, були втрачені в цьому сценарії. Або ще краще, просто використовуйте TCP.

3.2 Попередня аутентифікація

Попередня автентифікація забезпечує механізм для сервера аутентифікації, щоб визначити, хто головний (користувач або система, яка автентифікується), перш ніж він видає повідомлення KRB_AS_RSP. Це запобігає певним видам відомих атак на Керберос.

З RFC 6113 (Узагальнена рамка для попередньої автентифікації Kerberos),

Основна специфікація Kerberos (RFC4120) розглядає дані попередньої аутентифікації як непрозорий набраний отвір у повідомленнях до центру розподілу ключів (KDC), який може впливати на ключ відповіді, який використовується для шифрування відповіді KDC. Ця спільність була корисною: дані попередньої аутентифікації використовуються для різних розширень протоколу, багато за межами очікувань початкових розробників.

За замовчуванням для доменів Windows потрібні дані попередньої аутентифікації, які потрібно надати у повідомленнях KRB_AS_REQ. Отже, ми маємо наступне.

За замовчуванням KDC вимагає, щоб усі облікові записи використовували попередню аутентифікацію. Це функція безпеки, яка пропонує захист від атак нападів пароля. Запит AS ідентифікує клієнта до KDC у простому тексті. Якщо ввімкнено попередню автентифікацію, часова марка буде зашифрована, використовуючи хеш пароля користувача як ключ шифрування. Якщо KDC зчитує дійсний час, використовуючи хеш пароля користувача, який доступний в Active Directory для дешифрування часової позначки, KDC знає, що запит не є повтором попереднього запиту.

Попередня автентифікація забезпечує механізм, який потрібно багатьом розширенням Kerberos інтегрувати з тими "несподіваними" випадками використання, для яких Kerberos не був спочатку призначений. Сама специфікація Kerberos використовує заголовок попередньої аутентифікації для передачі даних аутентифікації на етапі TGS-REQ.

3.3 Квитки аутентифікації протоколу

З RFC 4120, квиток є «запис, який допомагає клієнту аутентифікувати себе на сервері; він містить особу клієнта, ключ сесії, часову позначку та іншу інформацію, запечатану за допомогою секретного ключа сервера. Він служить лише для аутентифікації клієнта, коли він представлений разом із свіжим аутентифікатором.

Існують різні типи квитків, включаючи квиток на видачу квитків (TGT) та службовий квиток.

TGT – квиток, призначений для TGS, який можна використовувати для отримання квитків на додаткові послуги без необхідності оригінального пароля користувача або секретного ключа.

Сервісний квиток – це квиток, виданий TGS, який можна використовувати для аутентифікації на потрібну послугу.

Квитки можна поновити. Протокол надає механізми для запиту на поновлюваний квиток та певні властивості для поновлення.

Квиток містить таку інформацію високого рівня:

- білетні прапори;
- ім'я користувача;
- область видимості;
- назва послуги;
- IP-адреса клієнта;
- мітка часу;
- час життя квитка;
- ключ сесії;

На початку дослідження деталей Кербероса на низькому рівні мене розчарувала детальна інформація про те, які саме поля знаходяться у кожному повідомленні, наведеному у звичайних зверненнях у верхній частині Google по цій темі. Очевидно, RFC 4120 має цю інформацію, але більшість параметрів є необов'язковими. Отже, розглядаючи приклади функціонування протоколу Kerberos – це найбільш життєздатний спосіб отримання деталей. У наступних пунктах роботи ми розглянемо приклади реального застосування Kerberos та деталі повідомлень.

Аутентифікатор.

Аутентифікатором є інформація, що надсилається разом із квитком у запиті Кербероса, щоб довести, що повідомлення походить від довірителя, якому було видано квиток. Аутентифікатор шифрується ключем сеансу (ключ сеансу клієнта t-to-TGS або ключ сесії клієнт-сервер (сервіс)); це доводить, що аутентифікатор

був згенерований стороною, яка має сеансовий ключ (який повинен бути в основному, описаних в квитку). Аутентифікатор також містить часову позначку, яка не підтверджує, що повідомлення було створене нещодавно і не перехоплене та відтворене.

Аутентифікатор містить такі дані:

- відмітка часу
- ідентифікатор клієнта
- спеціальна контрольна сума
- початковий номер послідовності повідомлень KRB_SAFE або KRB_PRIV)
- під-ключ сесії (використовується для переговорів щодо ключа сесії, унікального для даної сесії)

Делегація

Іноді клієнту може знадобитися надати віддаленій службі повноваження діяти від імені клієнта, щоб не посилатися на інші послуги. Це називається делегуванням. Делегування тягне за собою службу, яка має особу (або облікові дані) клієнта, який викликав її, щоб здійснити іншу дію, таку як виклик іншої послуги (з тим самим доступом, який мали і інші клієнти). Протокол Kerberos v5 визначає два механізми делегування облікових даних до сервісу: проксі-квиток або пересланий TGT. Механізми протоколу посвідчення особи, які диктують, як актор повинен дозволити іншому акторові безпечно використовувати свої повноваження, є захоплюючою темою, про яку я розповім набагато детальніше в майбутній публікації. Тим часом зауважте, що Керберос забезпечує підтримку делегування через два механізми, які коротко описані нижче.

Проксі-квитки.

Перший тип делегації, визначений специфікацією Kerberos, називається проксі-білетом. Повинно бути можливість контролювати, які саме дії дозволено виконувати службі за допомогою наданих облікових даних. Проксі-квиток дозволяє довірителю, який описує квиток, точно визначати, що може зробити послуга від її імені. Або, використовуючи термінологію в специфікації, довіритель може надати сервіс-проксі. Це робиться з допомогою проксі і

PROXIABLE прапорів в квитку. Ці прапори дозволяють довірителю надати облікові дані, які можна використовувати з певними службами.

З специфікації, прапор PROXIABLE у квитку, як правило, тлумачиться лише службою надання квитків. Його можуть ігнорувати сервери додатків. Якщо його встановлено, то цей прапор повідомляє серверу видачі квитків, що для видачі нового квитка (але не TGT) нема перешкод з іншою мережевою адресою на основі цього квитка. Цей прапор встановлюється за запитом клієнта при початковій автентифікації.

Отже, важливим кроком тут є те, що видається квиток, який посилається на мережеве доповнення, відмінне від того, де розташований клієнт. Зокрема, він має адресу служби, якій дозволено використовувати делеговану особу.

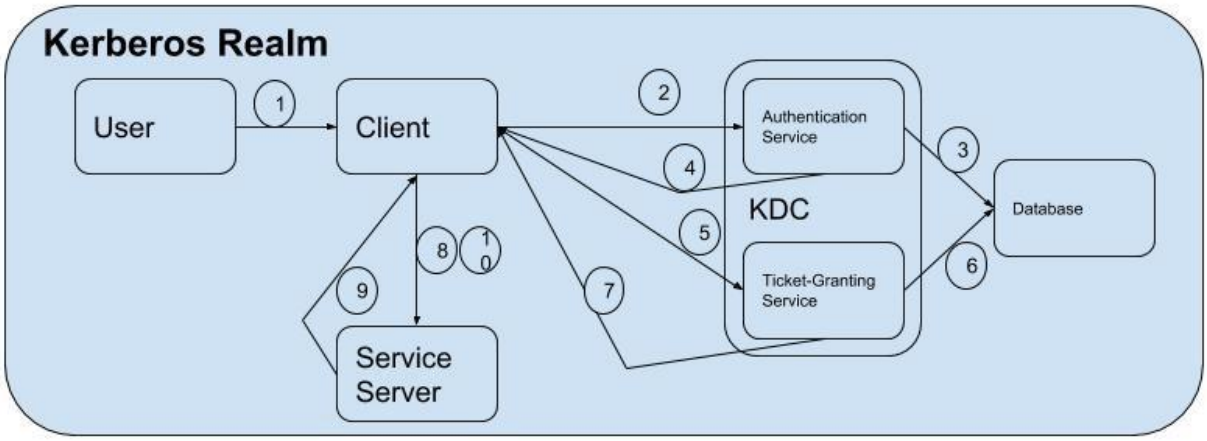
Специфікація передбачає можливість сервера додатків вимагати від служби виклику надавати інформацію про себе для цілей журналу аудиту.

Форвардні квитки.

Переадресація квитка або переадресація автентифікації – це проксі-білет, де сервісу, якому дозволено використовувати проксі, надається повна свобода використовувати ідентифікацію з будь-яким віддаленим сервісом, до якого інакше можна було б отримати доступ.

Ця концепція реалізована шляхом видачі квитка, який не посилається на будь-яку мережеву адресу, звідки дозволено надходити запит.

На наступній діаграмі (рисунок 3.1) показано високоефективну взаємодію акторів Кербероса.



1. User enters credentials (username + password).
2. Send KRB_AS_REQ.
3. Lookup user (and password) in database.
4. Send KRB_AS_RSP.
5. Send KRB_TGS_REQ.
6. Lookup service (and password) in database.
7. Send KRB_TGS_RSP.
8. Send KRB_AP_REQ.
9. Send KRB_AP_RSP.
10. Send service request to Service Server.

Рисунок 3.1 – Взаємодія ролей в протоколі аутентифікації

Наступна схема (рисунок 3.2) описує детальний обмін повідомленнями між учасниками.

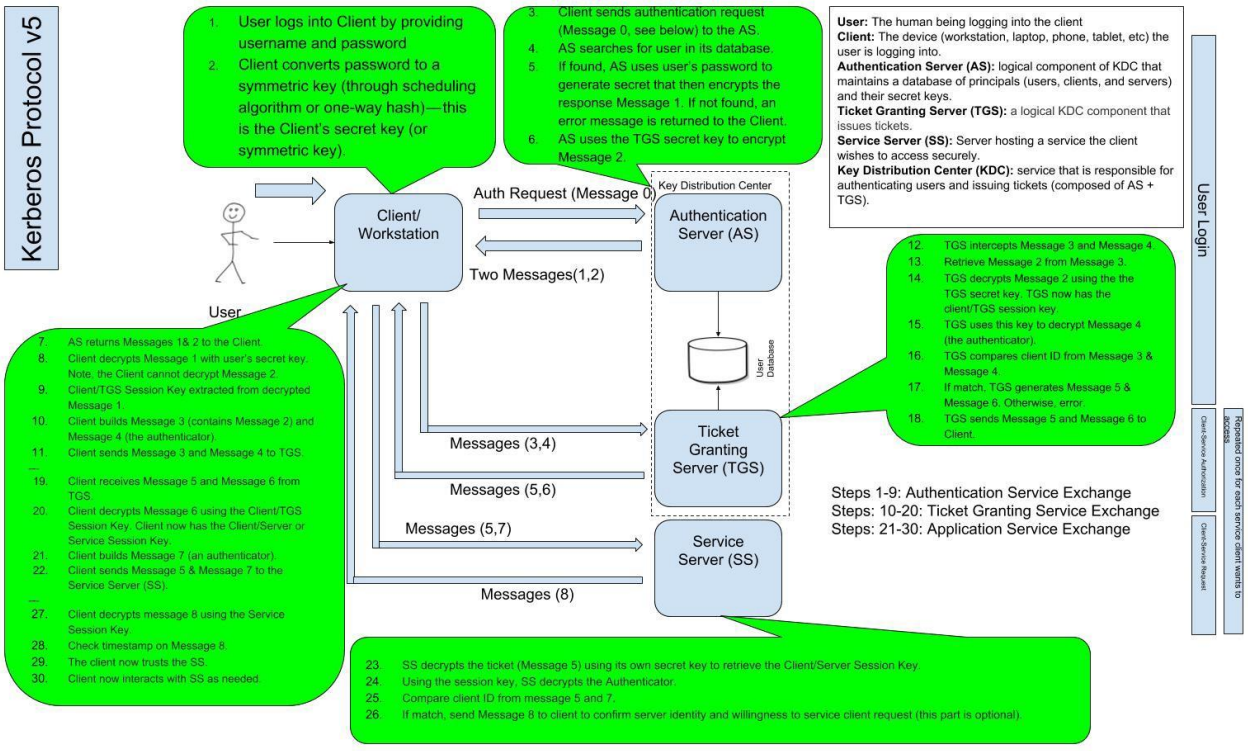


Рисунок 3.2 – Деталізована схема представлення протоколу

3.4 Служба аутентифікації

Наступні кроки реалізують в протоколі процес засвідчення користувача.

1. Користувач здійснює вхід в Клієнтську машину, надаючи ім'я користувача та пароль.

2. Клієнтська машина перетворює пароль в симетричний ключ (за допомогою алгоритму планування або одностороннього хешу) – це секретний ключ Клієнта (або симетричний ключ).

3. Клієнт надсилає запит на аутентифікацію (повідомлення 0, див. рисунок 3.3 нижче) до служби уатентифікації – Authentication Service (AS).

4. AS шукає користувача у своїй базі даних.

5. Якщо його знайдено, AS використовує пароль користувача для створення секрету, який потім шифрує відповідь Повідомлення 1. Якщо його не знайдено, повідомлення про помилку повертається Клієнту.

6. AS використовує секретний ключ TGS для шифрування повідомлення 3.

7. AS повертає Клієнту повідомлення 1 та 3.

8. Клієнт розшифровує Messag e 1 секретним ключем користувача. Зауважте, Клієнт не може розшифрувати Повідомлення 3.

9. Ключ сесії клієнт / TGS, вилучений із розшифрованого повідомлення 1.

Деякі примітки:

– У цей момент пароль, який користувач спочатку ввів, підтверджується, і користувач може вважатися аутентифікованим.

– З RFC 4120, "Цей обмін зазвичай використовується при ініціюванні сеансу входу для отримання облікових даних для сервера надання квитків, який згодом буде використовуватися для отримання облікових даних для інших серверів (див. Розділ 3.3), не вимагаючи подальшого використання клієнтських секретний ключ ».

– З RFC 4120, “Без попередньої аутентифікації сервер автентифікації не знає, чи є клієнт насправді основним, вказаним у запиті. Він просто надсилає відповідь, не знаючи і не піклуючись, чи однакові вони. Це прийнятно, оскільки ніхто, крім довірителя, особа якого було вказано у запиті, не зможе використовувати відповідь. "

– Якщо не зазначено інше, інформація передається чітким текстом.

– Секретний ключ комп'ютера не кешований.

3.5 Обмін послуг з надання квитків

1. Клієнт створює повідомлення 3 (містить повідомлення 2) та повідомлення 4 (автентифікатор).
2. Клієнт відправляє Повідомлення 3 та d Повідомлення 4 TGS.
3. TGS перехоплює повідомлення 3 та повідомлення 4.
4. Отримайте повідомлення 2 із повідомлення 3.
5. TGS розшифровує повідомлення з допомогою 2 секретний ключ TGS. Тепер у TGS є ключ сеансу клієнт / TGS.
6. TGS використовує цей ключ для розшифрування повідомлення 4 (автентифікатор).
7. TGS відповідає ідентифікатору клієнта з повідомлення 3 та повідомлення 4.
8. Якщо збігається, TGS генерує Повідомлення 5 та Повідомлення 6. В іншому випадку помилка.
9. TGS надсилає Клієнту повідомлення 5 та повідомлення 6.
10. Клієнт створює повідомлення 3 та повідомлення 4.
11. Клієнт надсилає Повідомлення 3 та Повідомлення 4 TGS.
12. Клієнт отримує Мед мудрець 5 та Повідомлення 6 від TGS.
13. Клієнт розшифровує Повідомлення 6 за допомогою ключа клієнта / TGS сесії. Тепер у клієнта є ключ клієнта / сервера або сервісний сеанс обслуговування.

Деякі примітки:

– TGT зберігається в кешеному режимі протягом усього життя та використовується для запиту кожного нового квитка на обслуговування, який потрібен Клієнту.

– Cl Key дієнт до TGS Session також кешуються клієнтом.

3.6 Обмін зі службою додатків

1. Клієнт будує Повідомлення 7 (автентифікатор).
2. Клієнт надсилає Повідомлення 5 та Повідомлення 7 на Сервер обслуговування – Service Server (SS).
3. SS розшифровує квиток (Повідомлення 5), використовуючи власний секретний ключ, щоб отримати ключ для сеансу клієнт / сервер.
4. Використовуючи сесійний ключ, SS розшифровує Генератор.
5. Порівняйте ідентифікатор клієнта з повідомлень 5 та 7.
6. Якщо це відповідає, надішліть повідомлення 8 клієнту, щоб підтвердити ідентифікацію сервера та готовність обслуговувати запит клієнта (ця частина є опцією l).
7. Клієнт розшифровує повідомлення 8 за допомогою ключа сеансу обслуговування.
8. Перевірте позначку часу на повідомленні 8.
9. Клієнт тепер довіряє SS.
10. Клієнт тепер взаємодіє з SS за потребою.

Слід зауважити, що відповідь SS, повідомлення 8, необов’язковий. Це потрібно лише в тому випадку, якщо клієнт хоче, щоб SS пройшов автентифікацію (тобто потрібна взаємна аутентифікація. Цікаво відзначити, що компонент аутентифікації TLS розглядає взаємну аутентифікацію і включає аутентифікацію клієнта (навпаки Kerberos).

Ці всі етапи представлені на наступній діаграмі послідовностей (рисунок 3.3).

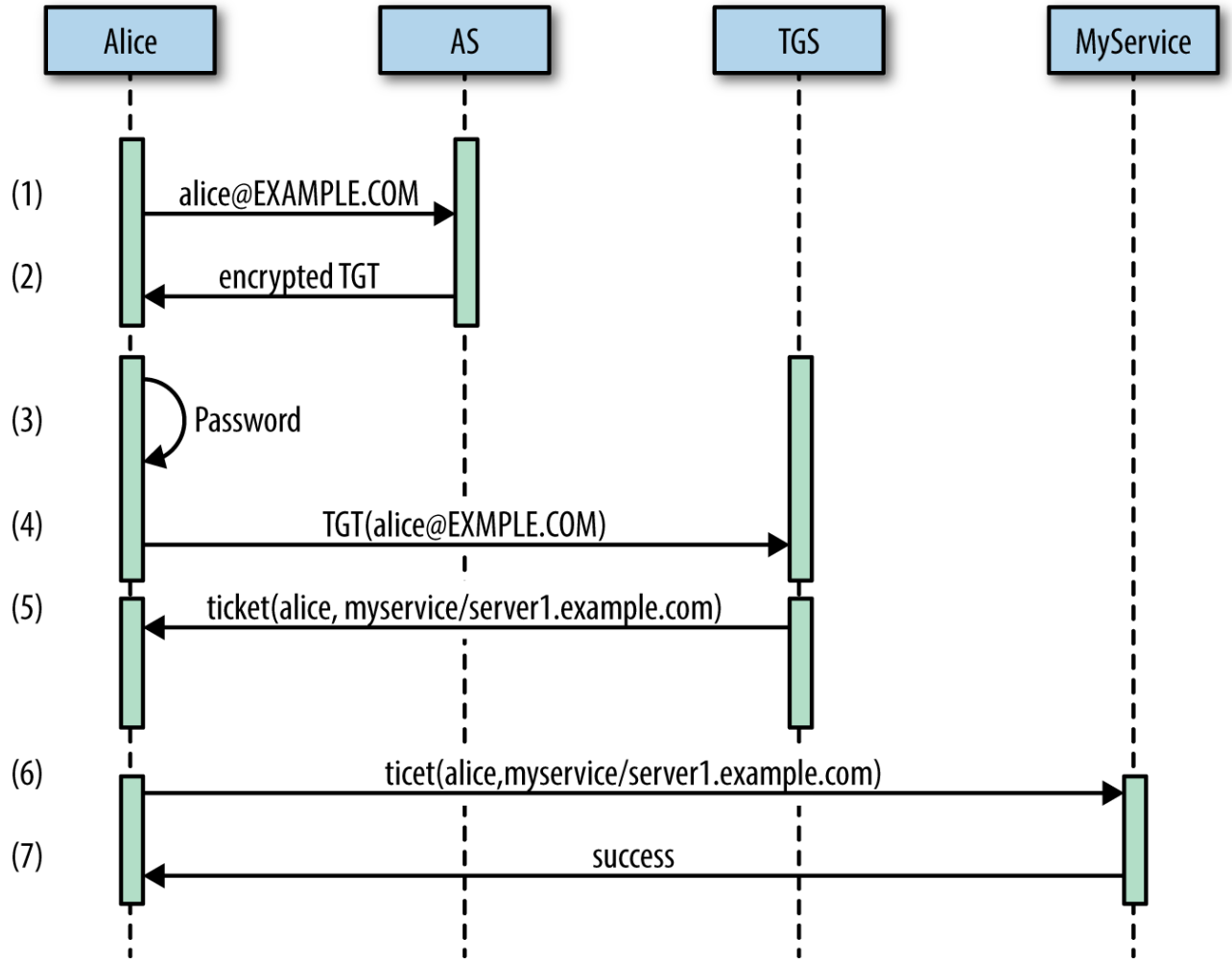


Рисунок 3.3 – Діаграма послідовності обміну повідомленнями в протоколі аутентифікації

Формати повідомлень

Далі описані всі поля у форматах повідомлень Kerberos v5, які використовуються на діаграмах та описі вище.

Повідомлення 0: KRB_AS_REQ

Дані попередньої аутентифікації (якщо вони використовуються) – в Windows це буде містити зашифровані часові позначки

– Основне ім’я клієнта

– Адреса клієнта

– Nonce (генерується випадковим чином клієнтом, використовується для виявлення повторів та узгодження відповіді із запитом)

– Запитаний час закінчення повідомлення.

– Запрошений час поновлення (необов’язково, використовується при запиті на поновлення).

– Запитаний час після дати (необов’язково, використовується для пост-дати запитів).

– Бажаний тип шифрування (необов’язково)

Параметри:

– Чи це початковий квиток (тобто, чи були надані облікові дані)?

– Чи проводиться попередня аутентифікація?

– Потрібно поновлювати квиток?

– Запрошений квиток доступний ?

– Потрібний квиток для повернення?

– Дозволено розміщення публікацій?

– Дозволено розміщення похідних квитків?

– Відновлюваний квиток дозволений замість невідновлюваного квитка

KRB_AS_REP

Різні метадані (див. Приклади в наступних публікаціях)

Повідомлення 1: KRB_AS_REP (зашифроване секретним ключем клієнта)

– Назва TGS

– Відмітка часу

– Час життя

– Ключ сесії TGS

Повідомлення 2: KRB_AS_REP (TGT, зашифрований секретним ключем TGS)

– Ім'я користувача

– Назва TGS

– Відмітка часу

– IP-адреса клієнта

– Життя квитка

– Ключ сесії TGS

– KRB_TGS_REQ

– Метадані

Повідомлення 3: KRB_TGS_REQ

- Назва запитуваної послуги.
- TGT (повідомлення 2 зверху)

Повідомлення 4: KRB_TGS_REQ

- Аутентифікатор (див. Попередній опис)
- KRB_TGS_REP
- Метадані

Повідомлення 5: (Сервісний електронний квиток, зашифрований секретним ключем служби)

- Ім'я користувача
- Назва послуги
- Відмітка часу
- IP-адреса клієнта
- Життя квитка
- Ключ сесії клієнт-сервер (або сервіс)

Повідомлення 6: KRB_TGS_REP (зашифроване ключем сесії Client-TGS)

- Ключ сеансу обслуговування
- KRB_AP_REQ
- Метадані

Повідомлення 5: KRB_TGS_REP (службовий квиток, зашифрований службовим секретним ключем)

- Ім'я користувача
- Назва послуги
- Відмітка часу
- IP-адреса клієнта
- Життя квитка
- Ключ сесії клієнт-сервер (або сервіс)

Повідомлення 7: KRB_AP_REQ

- Аутентифікатор
- KRB_AP_RES
- Метадані

Повідомлення 8: KRB_AP_REP

- Відмітка часу від автентифікатора (зашифрована ключем сесії клієнт-сервер (служба). Ключ сесії)

Існує багато інших деталей у базовій специфікації Kerberos, а ще більше – у родині розширень та RFC разом з власними функціями, які були додані за час використання сервера.

3.7 Архітектура програмної системи автентифікації в ОС Windows на основі Kerberos

Рзглянемо використання Kerberos в Microsoft Windows (Microsoft Kerberos). Зрештою, Kerberos з Windows більше-менш такий же, як і Kerberos де-небудь ще; однак є декілька фірмових розширень, які впроваджено Microsoft. Ці власні розширення обмежені полями, які специфікація Kerberos відкладає для таких розширень. Таким чином, це не обов'язково порушує взаємодію.

Kerberos складний. Windows приховує багато такої складності. Це дозволяє легко розкручувати домени Windows, але може стати кошмаром для адміністратора Windows Server, коли все не працює – ця посада зазвичай не передбачає бути експертом з посвідчення особи.

Якщо ви входите в екземпляр Windows (сервер або робочу станцію, апаратне забезпечення або віртуальну машину), який не підключений до домену, ви виконуєте локальний вхід (використовуючи NTLM та автентифікуючись на локальну базу даних користувачів). Якщо він підключений до домену, то виконується вхід домену (він використовує Kerberos, за замовчуванням). Для входу в систему доменна база даних знаходиться на контролері домену. Навіть якщо примірник Windows приєднаний до домену, все ж є можливість увійти в локальну ОС – ми вважатимемо типові випадки використання, як описано в цьому пункті.

Коли користувач заходить у Windows, існує декілька підсистем, які взаємодіють одна з одною для надійної автентифікації користувача. Деталі дещо відрізняються залежно від того, чи локальний користувач або користувач домену

входить у систему. Припустимо, для цього обговорення надається ім’я користувача та пароль. Існує багато інших способів аутентифікувати користувача в Windows, і є специфікації Kerberos, які підтримують багато з цих методів, але одночасно.

Ми розглянемо, як спочатку працює процес входу в локальну систему. На діаграмі нижче (рисунок 3.3) описано процес локального входу та архітектуру безпеки Windows. Тут ми припускаємо, що SPI для переговорів вибирає NTLM.

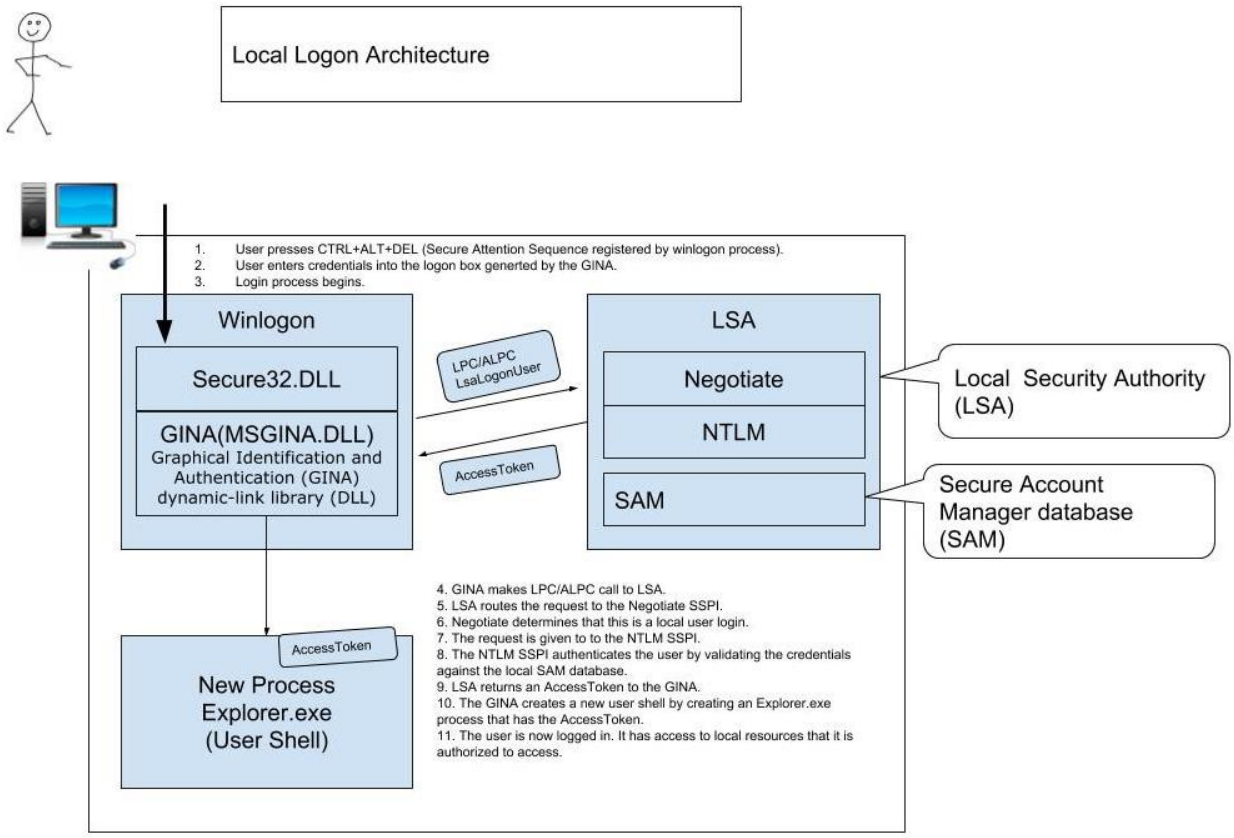


Рисунок 3.4 – Процес входу в систему для локальних користувачів

На наступній схемі (рисунок 3.5) описаний процес входу в домен користувача та архітектура безпеки Windows при підключенні до домену. Тут ми припускаємо, що SPI для переговорів вибирає Kerberos, а не інший варіант.

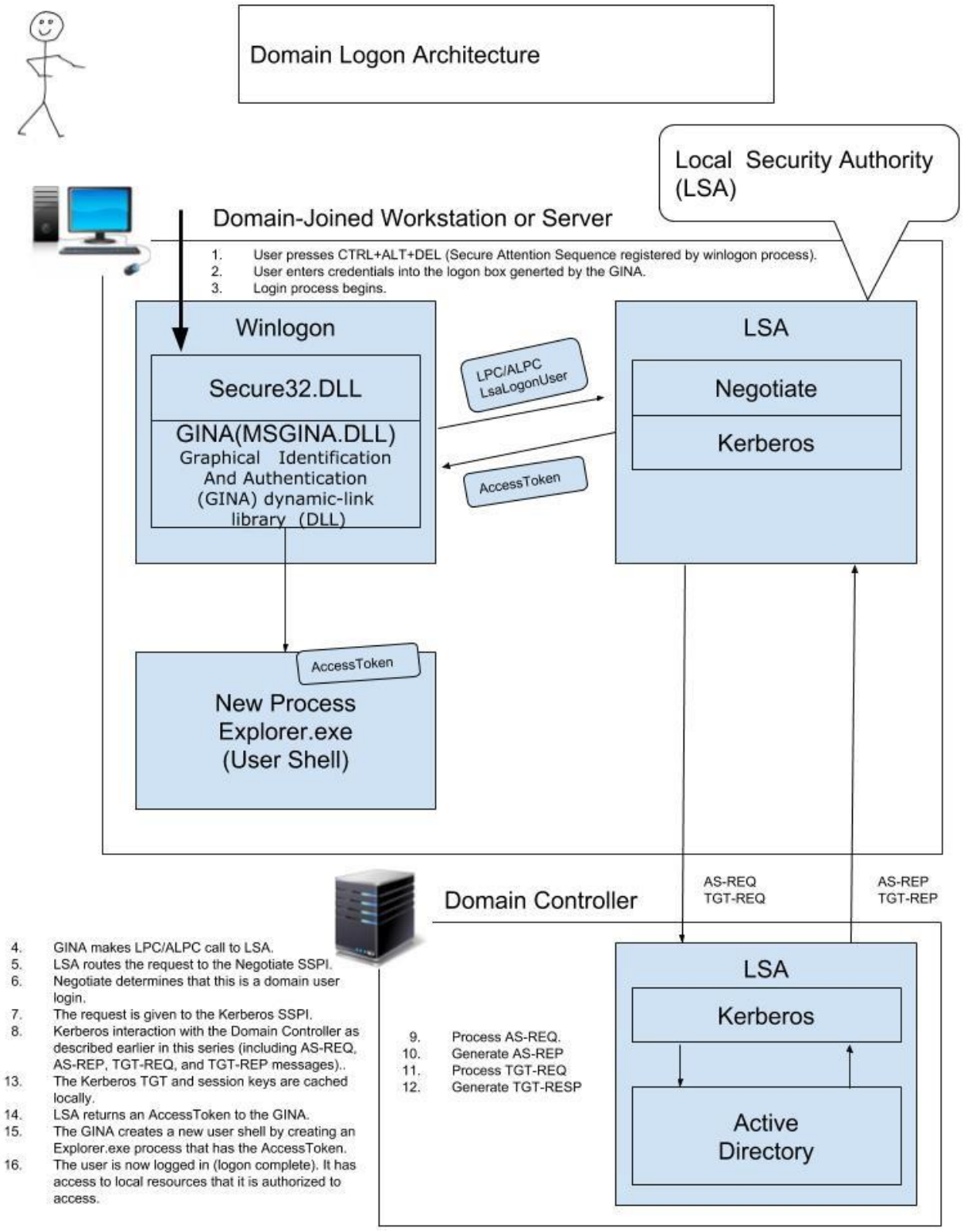


Рисунок 3.5 – Процес входу користувачів домену

Архітектура Windows SSPI (впровадження Microsoft GSS-API) виглядає наступним чином (див. рис. 3.6).

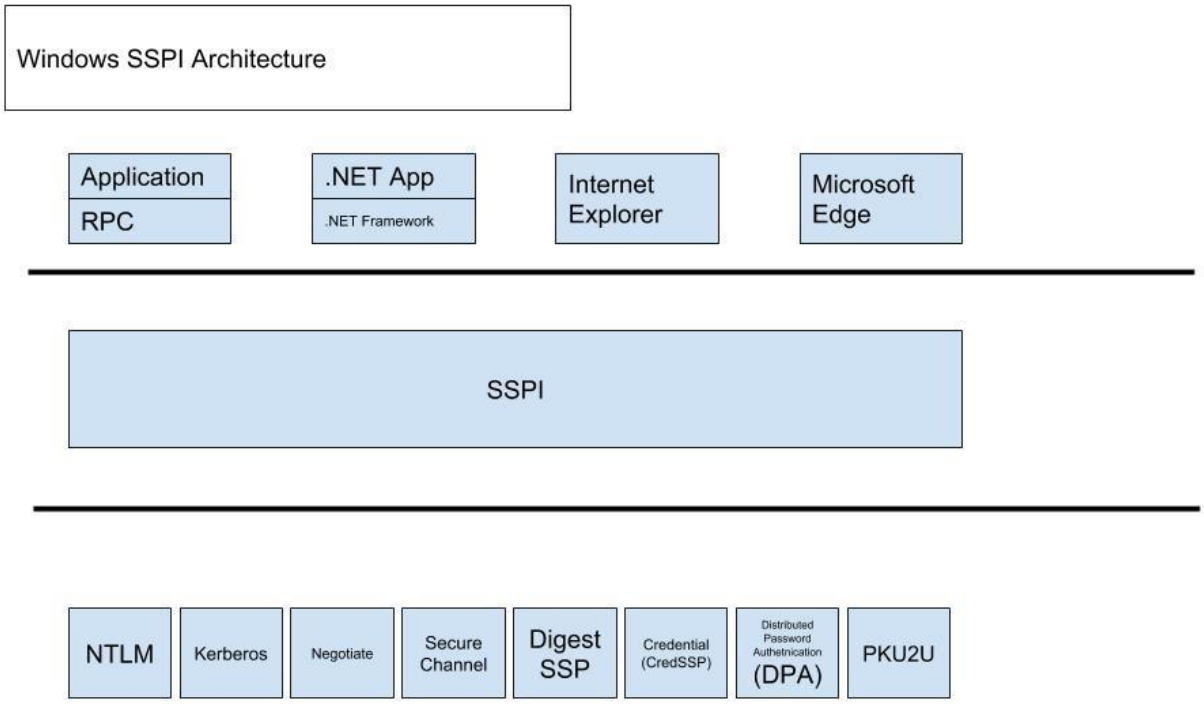


Рисунок 3.6 – Архітектура Windows SSPI

Microsoft вирішила не використовувати RFC1964 (GSS-API) в оригінальній реалізації Kerberos; їх реалізація, Інтерфейс постачальника підтримки безпеки (SSPI), використовує аналогічний набір функцій GSS-API, але з розширеннями та типовими даними для Windows. Усі протоколи Windows використовують API автентифікації Windows (SSPI). У Microsoft Windows доступні наступні SSP (провайдер підтримки безпеки) :

- NTLM (NT Manager)
- Керберос
- Ведіть переговори
- Безпечний канал (SChannel)
- Дайджест SSP
- Акредитив (CredSSP)
- Розподілена автентифікація пароля (DPA)
- Криптографія з відкритим ключем користувач-користувач (PKU2U)

Після завершення обміну Kerberos дані сертифіката привілейованих атрибутів (PAC) в полі даних про авторизацію, що входить до повідомлення TGT_REP, використовуються для створення маркера доступу (не плутати з

маркером доступу OAuth2) зображений на схемі вище. Поле даних авторизації також включає:

– Довідкова інформація: Інформація про квиток та клієнта.

– Інформація про клієнта: підтвердьте, що квиток належить клієнту, який його подає.

– Додаткові облікові дані: Повернено службою KDC, щоб увімкнути PKINIT.

– Підписи. Дані авторизації Microsoft містять два цифрові підписи: один для контролера домену та один для сервера, що пропонує послугу. Ці підписи використовуються для запобігання клієнтам або ненадійним службам генерувати власні підроблені дані авторизації Microsoft.

– Дані попередньої автентифікації PAC-запиту: Зазвичай дані авторизації Microsoft включаються у кожен попередній аутентифікаційний квиток, отриманий від запиту AS. Однак клієнт також може явно вимагати – за допомогою сертифіката атрибутів привілею (PAC) – запитувати поле даних про попередню автентифікацію – включати або не включати SID. Якщо це поле є, SID облікового запису буде включено. Якщо цього поля немає, SID не включатимуться.

Після того, як (Kerberos) облікові дані дістаються до екземпляра Windows (де ініційовано вхід), процес створення токенів багато в чому такий же, як і для інших методів аутентифікації. Маркер доступ в поступовим зниженням дози є об'єктом (Microsoft Windows патентованої конструкції, яка не залежить від Kerberos), який описує контекст безпеки у вигляді нитки або процесу. Кожен процес, породжений оболонкою користувача (Explor.exe, швидше за все) або будь-яким із його дітей, успадковує маркер доступу, який спочатку видається в оболонку користувача. Інформація в токені включає інформацію про особу та атрибути безпеки цієї особи, включаючи:

– ідентифікатор безпеки (SID) для облікового запису користувача;

– SID для груп, учасником яких є користувач;

– SID входу в систему, який ідентифікує поточний сеанс входу в систему;

– перелік привілеїв, якими користуються або користувач, або групи користувачів;

– власник SID;

– SID для первинної групи;

– DACL за замовчуванням, який система використовує, коли користувач створює об'єкт, що захищається, без вказівки дескриптора безпеки;

– джерело маркера доступу;

– незалежно від того, маркер є первинним або імперсональним ознакою;

– необов’язковий список обмежуючих SID;

– інша статистика.

Система використовує маркер доступу, пов'язаний з потоком або процесом, для ідентифікації користувача, коли він взаємодіє з об'єктами, що захищаються, або виконує завдання, яке вимагає привілеїв.

LSA кешує хешований пароль користувача; однак хеші паролів для комп’ютера та служб зберігаються у захищеній області реєстру комп'ютера. Цей захищений ділянку реєстру також використовується для зберігання хешів паролів локальних облікових записів.

3.8 Домени Windows

Концепція домену еволюціонувала з Windows NT в кінці 1990-х. Домен Windows надає адміністраторам спосіб централізовано керувати багатьма робочими станціями, ноутбуками та іншими пристроями. Один (або більше) серверів (контролерів домену) в домені керує доменом і комп'ютерами в ньому.

Контролер домену – це екземпляр Windows Server, на якому запущені служби доменних служб Active Directory. Він обробляє запити на аутентифікацію (входи, перевірки дозволів, оновлення токенів тощо) у домені Windows. У домені буде один або кілька контролерів домену. З практичної точки зору, їх зазвичай більше.

Центр розподілу ключів Kerberos (KDC) – служба домену, що працює на одному або декількох контролерах домену. Microsoft реалізує KDC як єдиний

процес, який надає дві послуги: Служба аутентифікації та Служба надання квитків. KDC працює на кожному контролері домену.

В основі Windows Kerberos – Active Directory (AD). Active Directory – це програмні компоненти, що працюють на контролері домену Windows, який реалізує:

– базу даних облікових записів Kerberos, яка містить користувачів, користувачів комп'ютерів та паролі;

– сервер LDAP;

– деякі інші речі, які зараз не важливі.

Підтримка LDAP в AD – це лише інтерфейс, який приховує набагато більш багатий набір функціональних можливостей. Хоча для більшості цілей, пов’язаних із автентифікацією імені користувача + паролем та авторизацією RBAC, LDAP стане набагато простішим способом інтеграції з AD, ніж Kerberos.

Клієнти Active Directory ніколи не отримують доступ до сховища даних безпосередньо, як і в будь-якій іншій системі баз даних підприємства. Клієнт, який хоче прочитати або записати дані каталогів, використовує один із підтримуваних інтерфейсів служби Active Directory (ADSI) для підключення до агента служб каталогів (DSA) та пошуку цих даних.

Об'єкти Active Directory мають списки контролю доступу (ACL) так само, як файли та папки файлової системи NTFS. Атрибути в об’єктах AD також мають ACL; Таким чином, атрибути, що містять конфіденційну інформацію облікового запису, можуть бути додатково обмежені, ніж інші атрибути.

Учасники домену: Сервери Windows.

Екземпляр Windows Server, який є членом домену, який не працює доменними службами (і Active Directory), є членом домену. Такий сервер, як правило, працює з певними службами (можуть надаватися в Windows, можуть бути сторонніми), які надають загальну функцію для інших членів домену. Все це може бути або клієнтом Kerberos, або сервером / послугами. Ймовірно, вони діють як обидва одночасно в різних контекстах.

Учасники домену: Робочі станції / ноутбуки Windows

Це по суті те саме, що було описано вище, але вони працюють з різними смаками Windows (орієнтовані на настільні ПК, ноутбуки та інші пристрої). Замість того, щоб використовувати загальні сервіси, це запущені програми / сервіси, які використовуються для підтримки поточної роботи користувача одного домену.

Ресурси Windows.

Ресурс Active Directory – це спільний ресурс у мережі (домен), такий як принтер або спільна файлова система (до нього можна отримати відповідні дозволи). Реєструючи ресурс в AD, користувачеві не потрібно входити на окремі сервери, щоб знайти та отримати доступ до цих ресурсів. Натомість AD може надавати інформацію про зареєстровані ресурси в центральному місці – подумайте про те, коли останній раз ви шукали мережеві принтери на роботі, всі вони були перераховані в одному місці (ми вважаємо, що подібні речі є належними в наші дні).

Вихід з системи.

Коли користувач виходить із системи, кеш даних облікових записів видаляється, а всі службові квитки – як і всі сеансові ключі – знищуються. Оболонка користувача сеансу припиняється і всі дочірні процеси коректно зупиняються.

3.9 Приклад розгортання системи з сервером віддаленого доступу для домену Windows

На щастя, протокол Kerberos здебільшого незашифрований (за винятком квитків, автентифікаторів та деяких інших реквізитів), які покладаються на шифрування повідомлень та полів. Це полегшує фіксацію мережевих знімків (за допомогою Wireshark або подібних інструментів) Kerberos, ніж деякі інші протоколи ідентичності. Звичайно, багато інших протоколів ідентичності побудовані поверх HTTP (S), а такі інструменти, як Chrome Developer Tools або подібні, можуть використовуватися в браузері.

У цій публікації ми будемо використовувати Wireshark v2.6.0. Сліди були зафіксовані на контролері домену Windows, який обробляв запити Kerberos.

Як завжди, ми почнемо з припущень. Пропустимо більшість деталей того, що виконує кожен актор в процесі автентифікації і натомість зосереджуюсь на повідомленнях, якими обмінюється протокол тут.

Знімки мережевої активності, захоплені для цієї роботи, були створені за допомогою Windows Server 2016, що працює на AWS.

Структура Кербероського квитка.

Квиток Kerberos включає таку інформацію.

Нешифрована частина:

- номер версії формату квитка.
- сфера обслуговування
- головний сервіс

Зашифрована частина:

- Білетні прапори
- ключ сеансу
- Real Клієнтська сфера
- Principal Клієнт (ім'я користувача)
- Список царств Kerberos, які брали участь в автентифікації користувача, якому виданий цей квиток.
- Мітка часу та інші метадані про останній початковий запит.
- час клієнт був ідентифікований.
- початок Термін дії часу (по бажанню).
- Термін дії кінцевого часу.
- квитків Надання сервера (TGC) Назва / ID
- Відмітка часу
- Клієнт (робоча станція) Адреса
- Термін експлуатації
- Authorization-дані – використовуються для передачі даних авторизації від принципала , від імені якого квиток був виданий служба додатків

У квитку можна використовувати такі прапори:

– зарезервовано (0)

– для переадресування (1)

– переслано (2)

– близький (3)

– проксі (4)

– травень – поле дати (5)

– відкладено (6)

– недійсним (7)

– відновлювані (8)

– початковий (9)

– попередня аутентифікація (10)

– hw- Authent (11)

– транзит-дирек- перевіряється (12)

– нормально- делегат (13)

На цьому прикладі ми побачимо два квитки: квиток на видачу квитків (TGT) та службовий квиток.

Структура автентифікатора Kerberos.

Аутентифікатор Kerberos містить таку інформацію (зашифровану):

– мітка часу

– ідентифікатор клієнта

Checks контрольна сума, що стосується додатків

– початковий номер послідовності повідомлень KRB_SAFE або KRB_PRIV)

– сесія під-ключ (використовується в переговорах для ключа сеансу унікальною для цієї конкретної сесії)

Аутентифікатори не повинні використовуватися повторно. Сервер, який стикається з перезапущеним автентифікатором, повинен відхилити повідомлення.

У цьому запиті ми побачимо одного автентифікатора: автентифікатор, надісланий із повідомленням TGT-REQ.

Вхід користувачів домену.

На наступному скріншоті показано початкове TCP-з'єднання між сервером Windows, що приєднався до домену, і контролером домену, коли користувач "RCBJ \ rcbj " намагався увійти через RDP. Зауважте, домен, про який йдеться, називається RCBJ (його DNS ім'я – rcbj.net); користувач домену, за яким ми відстежуємо вхід, називається rcbj . Так, мені подобається називати речі після себе, і належним чином зазначається, що це дещо зайве.

Служба обміну аутентифікацією.

Перші три пакети є типовим рукостисканням SYN-SYNACK-ACK, яке відбувається для будь-якого TCP-з'єднання (рисунок 3.7).

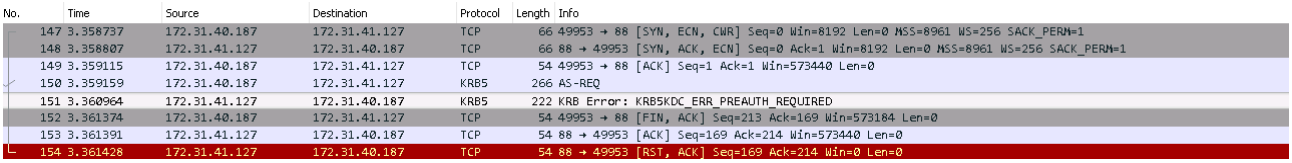


Рисунок 3.7 – Знімок мережевого трафіку з пакетами Kerberos

Четвертий пакет, який надсилається з Windows-сервера (Клієнта) на контролер домену (KDC / Служба автентифікації) – це повідомлення AS-REQ (це тип повідомлення KRB_KDC_REQ). Повідомлення AS-REQ виглядає наступним чином (див. рис. 3.8):

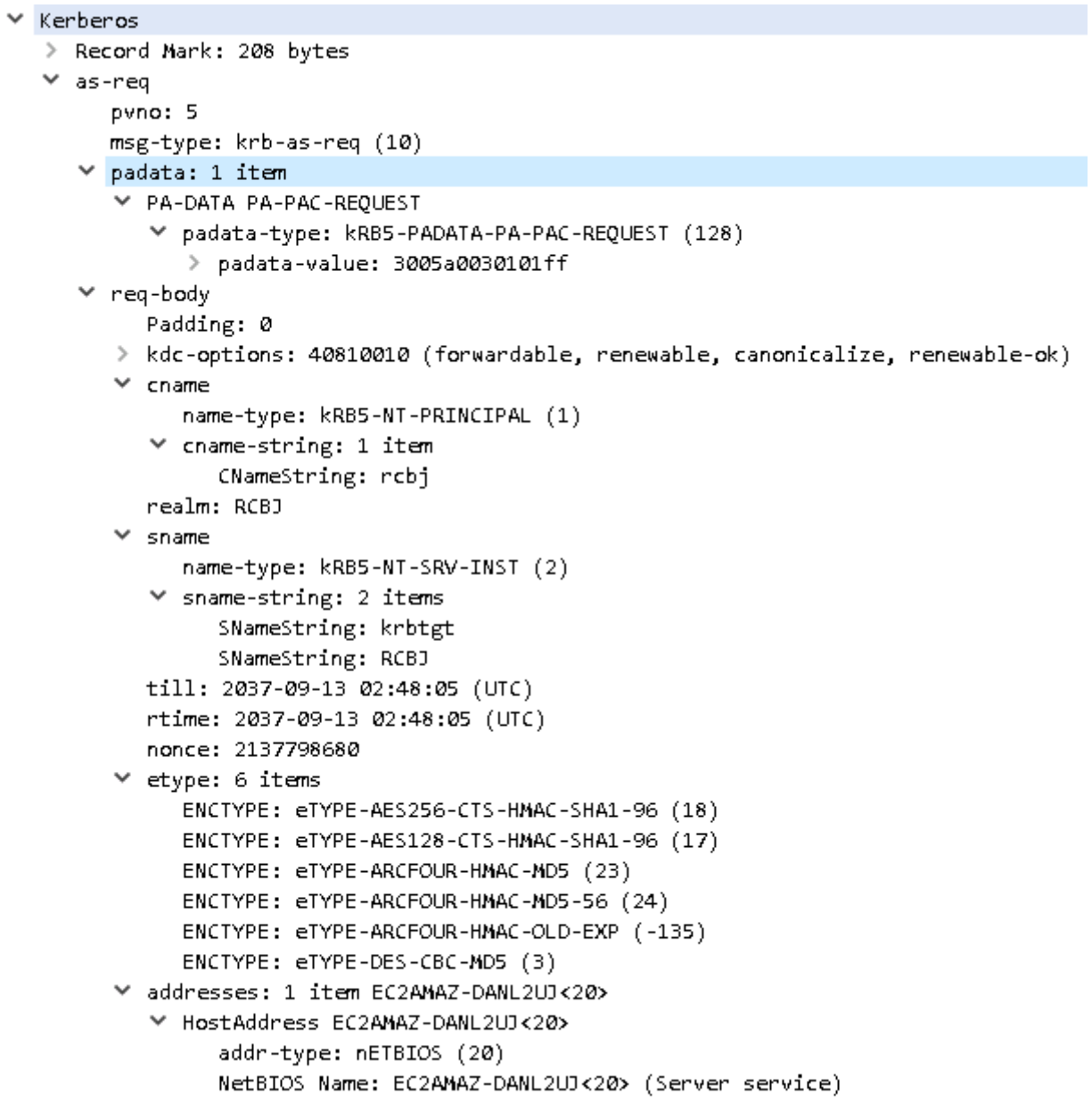


Рисунок 3.8 – Структура пакету протоколу Kerberos

Це Повідомлення 0. Можете побачити наступні поля на скріншоті вище:

– pvno – версія протоколу Kerberos (5).

– msg-type – номер тегу класу програми (10)

– padata – дані попередньої аутентифікації, що містять структуру PA-PAC-REQUEST . Про це коротко згадується у RFC4120.

– KDC-options – прапори , запитані для результуючого квитка (пересилається, поновлювані джерела, КаноніческаяФорм, поновлюваний ОК).

– CNAME – містить ім'я користувача аутентифицирующей

– царство – містить сферу Kerberos (також ім'я домену Windows)

– SNAME – ім'я служби запитується (в даному випадку, це знову вікна доменне ім'я)

– до – запитуваний термін дії квитка, який запитується.

– RTIME – Якщо поновлюваний квиток був запропонований, це поле містить бажане абсолютне час закінчення для квитка

– nonce – повідомлення nonce

– etype – запитувані типи шифрування

– адреси – IP-адреса клієнта

Контролер домену (служба аутентифікації) хоче надати дані попередньої аутентифікації. Отже, він повертає таку помилку Kerberos (рис. 3.9):

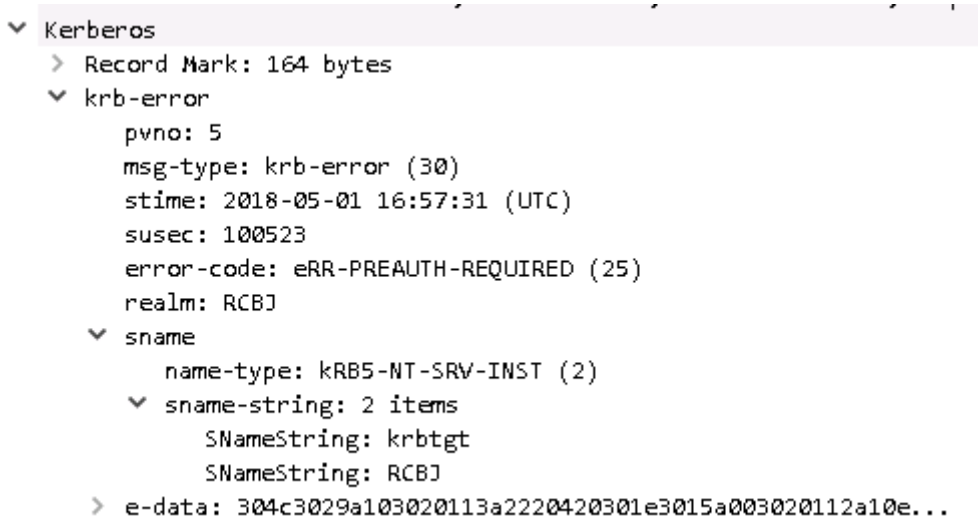


Рисунок 3.9 – Структура пакету попередньої аутентифікації

Повідомлення про помилки Kerberos визначені в RFC 4120. Поля, що містяться в цьому повідомленні:

– pvno – номер версії протоколу Kerberos (5)

– msg-type – номер тегу класу програми (30)

– stime – Поточний час на сервері в момент створення цього повідомлення.

– susec – це поле містить мікросекундну частину часової позначки сервера.

– код помилки – помилка , що сталося (необхідні дані попередньої аутентифікації, в даному випадку)

– сфера – сфера , в якій ця помилка сталася .

– SNAME – ідентифікатор служби (KRBTGT @ RCBJ , в цьому випадку квиток видачі квитків)

– електронні дані – додаткові дані про помилку, яку використовує додаток, щоб допомогти їй відновитись або виправити помилку.

У цей момент з'єднання TCP закрите.

Використовуючи секретний ключ користувача, отриманий із пароля Windows, клієнт (робоча станція або сервер Windows) зашифровує поточну часову позначку та використовується для заповнення даних попередньої автентифікації повідомленням KRB5-PADATA-ENC-TIMESTAMP у запиті нижче.

Встановлено новий зв'язок. Нове повідомлення AS-REQ надсилається до служби аутентифікації KDC.

По суті це саме те саме повідомлення, яке надійшло вперше, але тепер дані попередньої аутентифікації заповнюються. Я не збираюся переробляти всі поля – див. рис. 3.8 вище.

Після обробки повідомлення про запит служба аутентифікації повертає KRB_AS_REP клієнту (робочій станції).

У повідомленні KRB_AS_REP наявні такі поля:

– pvno – номер версії протоколу Kerberos (5)

– msg-type – номер тегу класу програми (10)

– padata – дані попередньої аутентифікації (у цьому випадку з RFC4120, Розділ 5.2.7.5, він "надасть клієнтові інформацію про те, яку ключову сіль використовувати для того, щоб клієнт використовував строку до ключа для отримання ключ для розшифрування зашифрованої частини AS-REP. ")

– креальм – царство Керберос (у цьому випадку RCBJ.NET)

– CNAME – клієнт / ім'я користувача (rcbj в даному випадку).

– квиток – Квіток на видачу Кербероса на цей сеанс.

– ticket-> tkt-vno – Номер версії формату квитка (5).

– ticket-> realm – Ділянка, на яку цей квиток видається (у цьому випадку RCBJ.NET).

– ticket-> SNAME – ім'я служби цей квиток належить, на KDC Ticket Грейнінг служби. (krbtgt@RCBJ.NET)

– ticket-> enc-part – Частина квитка, зашифрована секретним ключем TGS.

– enc-part – ключ клієнта / TGS сесії (зашифрований секретним ключем користувача)

Ці поля даних представляють Повідомлення 1 (поле частини коду, яке зашифроване із секретом користувача, що походить від пароля) та Повідомлення 2 (поле квитка, що містить TGT). Також є кілька метаданих, включених у повідомлення KRB_AS_REP.

Отже, на даний момент у клієнта є сесійний ключ, який він розшифрував за допомогою секретного ключа користувача та TGT (який містить той самий ключ сеансу, серед іншого, зашифрований секретним ключем TGS). На наступному кроці TGS також матиме доступ до ключа клієнта / TGS сесії.

Обмін сервісами Token.

Далі клієнт (робоча станція) встановлює нове підключення до сокета і надсилає повідомлення TGS-REQ. Структура повідомлення TGT-REQ схожа на повідомлення AS-REQ, яке ми розглянули раніше, що має сенс, враховуючи, що обидва ці повідомлення мають загальне визначення KRB_KDC_REQ.

Запит TGT-REQ містить:

– PVNO : версія протоколу область Kerberos (5).

– msg-type: номер тегу класу програми (12).

– pa-data: поле даних попередньої аутентифікації, яке містить заголовок аутентифікації (див. Нижче).

– REQ тіла: тіло запиту.

У наведеному вище прикладі повідомлення ми бачимо, що поле даних про попередню автентифікацію заповнене заголовком аутентифікації типу PA-TGS-REQ (див. RFC 4120, розділ 5.2.7.1) структури даних – воно містить TGT та автентифікатор для цей крок і має тип AP-REQ. PA-TGS-REQ містить такі поля:

– pvno – номер версії протоколу Kerberos

– msg-type – номер тегу класу програми (14)

– padata – Дані попередньої аутентифікації.

– crealm – ім'я клієнтської області (в даному випадку ім'я домену Windows).

– cname – ім'я користувача (у цьому випадку rcbj).

– квиток – структура квитка (TGT з повідомлення 2)

– ticket-> tkt-vno – Номер версії формату квитка.

– ticket-> realm – царство, для якого був виданий квиток.

– Білет-> ім'я – послуга, на яку цей квиток був виданий (krbtgt@rcbj.net)

– ticket-> enc-part – Зашифрована частина квитка.

– аутентифікатор – Аутентифікатор, зашифрований за допомогою ключа клієнта / TGS сесії

Сюди входить Повідомлення 3 (TGT з повідомлення 2 та ідентифікатор запитуваної послуги, krbtgt@rcbj.net для нашого входу в домен Windows) та повідомлення 4 (аутентифікатор, зашифрований за допомогою ключа клієнта / TGS сесії) з нашого попереднього опису.

У цей момент TGS використовує свій секретний ключ для розшифрування TGT. Потім він може отримати ключ клієнта / TGS сесії з розшифрованого квитка. Потім він може використовувати сесійний ключ для розшифрування автентифікатора (поле enc-part). Тепер TGS може порівняти ім'я користувача в автентифікаторі з іменем у TGT. Якщо обидва імена збігаються, TGS продовжується, як описано нижче; в іншому випадку помилка буде повернута.

Орган запиту TGS-REQ містить такі поля:

– прапори: прапори, що описують тип службового квитка, який потрібно повернути (у такому випадку квиток повинен бути поновлюваним, переоформленим та канонізованим.

– царство: доменне ім'я, на яке видається квиток (rcbj.net, в даному випадку).

– ім’я : послуга, для якої повинен бути виданий Сервісний квиток (тут, host@domain.net).

– до: Запитаний час закінчення терміну дії квитка для видачі цього запиту.

– одноразового значення: одноразове значення для цього запиту.

– ETYPE : Необхідний алгоритм шифрування (и) , які будуть використовуватися у відповіді.

Служба надання квитків KDC відповідає на відповідь TGS-REP. Поля, що входять до поля відповіді:

– pvno – номер версії протоколу Kerberos (5).

– msg-type – номер тегу класу програми (13).

– crealm – ім'я реальності (ще раз, ім'я домену Windows , RCBJ.NET).

– CNAME – ім'я користувача.

– квиток – Структура квитків (Клієнт-серверний квиток, зашифрований за допомогою секретного ключа служби. Квиток називається Сервісним квитком. У цьому прикладі послуга є службою реєстрації локальної робочої станції.

– ticket-> tkt-vno – Номер версії формату квитка.

– ticket-> царство – царство, для якого цей квиток був виданий.

– ticket-> SNAME – ім'я служби якою цей квиток був виданий (ec2amaz-danl2uj.rcbj.net).

– квиток-> enc-part – Зашифрована частина квитка від клієнта до сервера (або послуги).

– enc-частина – сесійний ключ клієнта / сервера (або послуги), зашифрований ключем сесії Client-TGS.

Сюди входить Повідомлення 5 (клієнт-сервер або службовий квиток, зашифрований за допомогою секретного ключа служби або в цьому випадку секретний ключ облікового запису комп’ютера робочої станції) та Повідомлення 6 (ключ сеансу клієнт-сервер, зашифрований ключем сеансу клієнт-TGS). Щоб додатково уточнити, який секретний ключ використовується для розшифровки службового квитка у повідомленні 5, пам’ятайте, що на кожній робочій станції та сервері, зареєстрованих у домені Windows, визначено обліковий запис комп’ютера, з яким пов’язаний секретний ключ (пароль).

Після отримання клієнт може розшифрувати ключ сеансу клієнт-сервер, який йому необхідний для наступного кроку, і зашифрований квиток клієнт-сервер буде доступний для подання в потрібну послугу. Незважаючи на те, що сервер Сервісу, названий у щойно отриманому нам квитку клієнт-сервер, – це локальний сервер, на який ми входимо, що робить цей конкретний приклад дещо дивним щодо стандартного випадку використання Kerberos – немає віддаленого сервера компонент, до якого здійснюється доступ. Принаймні, поки що. Зважаючи на достатньо часу, типовий користувач Windows зробить щось, що передбачає доступ до віддаленої послуги (мережева файлова система, принтер, електронна пошта тощо).

4 СПЕЦІАЛЬНА ЧАСТИНА
РОБОТА З ПРОГРАОЮ ЗАХВАТУ TCP-ПАКЕТІВ WIRESHARK

4.1 Загальні відомості про програму захоплення пакетів

Навіть поверхневе знання програми Wireshark і її фільтрів на порядок заощадить час при усуненні проблем мережевого або прикладного рівня. Wireshark корисний для багатьох завдань в роботі мережевого інженера, фахівця з безпеки або системного адміністратора. Ось кілька прикладів використання:

Усунення неполадок мережного підключення:

- Візуальне відображення втрати пакетів
- Аналіз ретрансляції TCP
- Графік по пакетам з великою затримкою відповіді

Дослідження сесій прикладного рівня (навіть при шифруванні з допомогою SSL / TLS, см. Нижче)

- Повний перегляд HTTP- сесій, включаючи всі заголовки і дані для запитів і відповідей
- Перегляд сеансів Telnet, перегляд паролів, введених команд і відповідей
- Перегляд трафіку SMTP і POP3, читання листів

Усунення неполадок DHCP з даними на рівні пакетів

- Вивчення трансляцій широковещательного DHCP
- Другий крок обміну DHCP (DHCP Offer) з адресою та параметрами
- Клієнтський запит по запропонованим адресою
- Ack від сервера, що підтверджує запит

Витяг файлів з сесій HTTP

- Експорт об'єктів з HTTP, таких як JavaScript, зображення або навіть виконувані файли

Витяг файлів з сесій SMB

- Аналогічно опції експорту HTTP, але витяг файлів, переданих по SMB, протоколу загального доступу до файлів в Windows

Виявлення і перевірка шкідливих програм

- Виявлення аномального поведінки, яке може вказувати на шкідливе ПЗ
- Пошук незвичайних доменів або кінцевих IP
- Графіки введення-виведення для виявлення постійних з'єднань (маячків) з керуючими серверами
- Отфільтровка « нормальних » даних і виявлення незвичайних
- Витяг великих DNS- відповідей і інших аномалій, які можуть вказувати на шкідливе ПЗ

Перевірка сканування портів та інших типів сканування на уразливості

- Розуміння, який мережевий трафік надходить від сканерів
- Аналіз процедур по перевірці вразливостей, щоб розрізняти хибнопозитивні і помилково негативні спрацьовування

Ці приклади - лише вершина айсберга. У керівництві ми розповімо, як використовувати настільки потужний інструмент.

4.2 Установка Wireshark

Wireshark працює на різних операційних системах і його нескладно встановити. Згадаємо лише Ubuntu Linux, Centos і Windows.

Установка на Ubuntu або Debian

Apt-get update

Apt-get install wireshark tshark

Установка на Fedora або CentOS

Yum install wireshark-gnome

Установка на Windows

На сторінці завантаження лежить виконуваний файл для установки. Досить просто ставиться і драйвер захоплення пакетів, з допомогою якого мережева карта переходить в «нерозбірливий» режим (promiscuous mode дозволяє приймати всі пакети незалежно від того, кому вони адресовані).

4.3 Робота з програмою

З першим перехопленням ви побачите в інтерфейсі Wireshark стандартний шаблон і подробиці про пакет. Як тільки захопили сесію HTTP, зупиніть запис і пограйте з основними фільтрами і настройками Analyze | Follow | HTTP Stream. Назви фільтрів говорять самі за себе. Просто вводите відповідні вирази в рядок фільтра (або в командну рядок, якщо використовуєте tshark). Основне перевага фільтрів - в видаленні шуму (трафік, який нам не Інтерест). Можна фільтрувати трафік по MAC-адресу, IP-адресою, підмережі або протоколу. Самий простий фільтр - ввести http, так що буде відображатися тільки трафік HTTP (порт tcp 80).

Приклад фільтру по IP-адресах

```
ip.addr == 192.168.0.5
! (ip.addr == 192.168.0.0/24)
```

Приклад фільтру по протоколу

```
tcp
udp
tcp.port == 80 || udp.port == 80
http
not arp and not (udp.port == 53)
```

Спробуйте зробити комбінацію фільтрів, яка показує весь вихідний трафік, крім HTTP і HTTPS, який прямує за межі локальної мережі. Це хороший спосіб виявити програмне забезпечення (навіть шкідливе), яке взаємодіє з інтернетом по незвичайним протоколам.

Як тільки ви захопили кілька HTTP- пакетів, можна застосувати на одному з них пункт меню Analyze | Follow | HTTP Stream. Він покаже цілком сесію HTTP. У цьому новому вікні ви побачите HTTP- запит від браузера і HTTP- відповідь від сервера.

За замовчуванням Wireshark налаштований перетворювати мережеві адреси в консолі. Це можна змінити в настройках. Edit | Preferences | Name Resolution | Enable Network Name Resolution Як і в разі tcpdump, процедура резолвінг сповільнить відображення пакетів. Також важливо розуміти, що при оперативному захопленні пакетів DNS- запити з вашого хоста стануть додатковим трафіком, який можуть перехопити.

Якщо Wireshark скомпільовано з підтримкою GeoIP і у вас є безкоштовні бази Maxmind, то програма може визначати місце розташування комп'ютерів по їх IP-адресами. Перевірте в About | Wireshark, що програма скомпільована з тієї версією, яка у вас в наявності. Якщо GeoIP присутній в списку, то перевірте наявність на диску баз GeoLite City, Country і ASNum. Вкажіть розташування баз в меню Edit | Preferences | Name Resolution. Перевірте систему на дампі трафіку, вибравши опцію Statistics | Endpoints | IPv4. В колонках праворуч повинна з'явитися інформація про місцезнаходження та ASN для IP-адреси. Інша функція GeoIP - фільтрація трафіку по місцю розташування з допомогою фільтра ip.geoip. Наприклад, так можна виключити трафік з конкретної ASN. Нижчезазначених команда виключає пакети від мережевого блоку ASN 63949 (Linode).

Один з способів розшифровки сесій SSL / TLS - використовувати закритий ключ з сервера, до якого підключений клієнт. Звичайно, у вас не завжди є доступ до приватного ключу. Але є інший варіант простого перегляду трафіку SSL / TLS на локальній системі. Якщо Firefox або Chrome завантажуються з допомогою спеціальної змінної середовища, то симетричні ключі окремих сеансів SSL / TLS записані в файл, який Wireshark може прочитати. З допомогою цих ключів Wireshark покаже повністю розшифровану сесію.

5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від розробки, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільність впровадження відповідної розробки.

Передбачається, що описаний в роботі підхід буде імплементовано у вигляді спеціальної СППР, яка представляє собою програмний продукт. Розробка такого продукту вимагатиме певних затрат. Тому розрахуємо ці затрати.

Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції.

5.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час їх виконання

№	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Витрати праці на підготовку опису задачі	інженер	9
2.	Витрати праці на розробку проекту	інженер	18
3.	Витрати праці на розробку структури системи	інженер	11
4.	Витрати праці на створення системи по вибраному проекту та структурі	інженер	74
5.	Витрати праці на підготовку документації	інженер	15
6.	Витрати праці на відлагодження роботи зпроектованої системи при комплексній відладці	інженер	42
Разом			169

Загальні затрати на дипломний проект становить 169 годин.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2018 рік», зокрема Статтею восьмою мінімальна заробітна плата у погодинному розмірі встановлена у розмірі 22,41 грн. Рекомендовані тарифні ставки: керівник дипломної роботи – 30,00...50,00 грн./год., інженер – 22,41...30,00 грн./год., консультант – 22,41...30,00 грн./год., технік – 22,41...30,00 грн./год., лаборант – 22,41...25,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (5.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в даному проекті виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 30 \cdot 169 = 5070 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \qquad (5.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод.} = 5070 \cdot 0{,}15 = 760{,}50 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.}. \qquad (5.3)$$

$В_{о.п.}$=5070+760,50 = 5830,50 грн.

Крім того, слід визначити відрахування на соціальні заходи:

1) ЄСВ + ПДФО 22 %;
2) військовий збір – 1,5 %.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{с.з.} = Ф_{оп} \cdot 0{,}235, \qquad (5.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$B_{с.з.} = 5830{,}5 \cdot 0{,}235 = 1370{,}05 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 5.2.

Таблиця 5.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівник-ків	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн. *6=3+4+5*
		Тарифна ставка, грн.	К-сть відпра-цьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	інженер	30	169	5070	760,5	1370,05	7200,55

Загальні витрати на оплату праці становить 7200,55 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{в\,i} = q_i \cdot p_i, \qquad (5.5)$$

де: q_i – кількість витраченого матеріалу *i*-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{B\,i}. \qquad (5.6)$$

Проведені розрахунки занесемо у таблицю 5.3. Для розробки ПЗ передбачається покупка Microsoft Visual Studio Professional 2017, вартість якого на сьогодні становить 74400 грн.

Таблиця 5.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транспортно-заготівельні витрати, грн	Загальна сума витрат на матеріали, грн
1. Основні матеріали						
Програмне забезпечення	комп.	1	74400,00	74400,00	–	74400,00
2. Допоміжні матеріали						
Папір формату А4	шт.	200	0,18	36	–	36
Разом:						74436,00

Загальні матеріальні затрати становлять 74436,00 гривень.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \qquad (5.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютера для створення проекту – 550 Вт, кількість годин роботи обладнання згідно таблиці 5.1 – 169 годин.

Тоді, $З_е = 0,55 \cdot 169 \cdot 2,42 = 224,94$ грн.

5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Для даного проекту засобом розробки є комп'ютер. Його сума становить 7335 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{7335 \cdot 5\%}{100\%} = 366,75 \text{ грн.}$$

Оскільки робота виконувалась 169 годин, то амортизаційні відрахування будуть становити:

$$A = \frac{366{,}75 \cdot 169}{150} = 413{,}21 \text{грн.}$$

5.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (5.9)$$

де $H_В$ – накладні витрати.

Отже, накладні витрати:

$H_В$ = 5830,5· 0,2 = 1166,10 грн.

5.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	5830,5	7,1%
Відрахування на соціальні заходи	370,05	0,4%
Матеріальні витрати	74436	90,3%
Витрати на електроенергію	224,94	0,3%
Амортизаційні відрахування	413,21	0,5%
Накладні витрати	1166,1	1,4%
Собівартість	82440,8	100,0%

Собівартість (C_B) проекту розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + А + Н_в. \quad (5.10)$$

Отже, собівартість проекту дорівнює:

$С_в$ = 5830,50 + 370,05 + 74436 + 224,94 + 413,21 + 1166,10 = 82440,80 грн.

5.8 Розрахунок ціни проекту

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + К \cdot B_{н.і.}}{К} \cdot (1 + ПДВ), \quad (5.11)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

$К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

$ПДВ$ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти $К$ та $B_{і.н}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.12)$$

Звідси ціна на проект складе:

Ц = C_B · (1+0,3)(1+0,2) = 128607,65 грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = П / C_B \,, \tag{5.13}$$

де $П$ – прибуток;

C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_B \,. \tag{5.14}$$

Розраховуємо плановий прибуток:

$П_{пл}$ = 128607,65 – 82440,8 = 46166,85 грн.

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_p = \frac{П_{пл}}{Св} \,. \tag{5.15}$$

Тоді, E_p = 46166,85 / 82440,8 = 0,56

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = 1 / E_p \,, \tag{5.16}$$

Термін окупності дорівнює:

T_p = 1/0,56 = 1,8 роки.

В цьому розділі дипломної роботи було розраховано основні техніко-економічні показники проекту (див. таблицю 5.5).

Розраховане значення економічної ефективності становить 0,42 що є високим значенням.

Так само нормальним є термін окупності. Для даного продукту він становить 2,4 роки.

Таблиця 5.5 – Техніко-економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	82440,8
2.	Плановий прибуток, грн.	46166,85
3.	Ціна, грн.	128607,65
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Отже, даний проект може бути впроваджений та мати подальший розвиток, оскільки він є економічно вигідним за всіма основними техніко-економічними показниками.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Оцінка стійкості роботи об’єкту економіки до впливу вражаючих факторів при надзвичайних ситуаціях

В наш час стрімкого розвитку техніки ростуть і загрози різноманітних техногенних аварій, які можуть завдати значної шкоди як економічному потенціалу окремого регіону чи цілої країни. Актуальною, особливо в останній час, є також проблема тероризму.

Здатність підприємств протидіяти таким шкідливим впливам та аваріям характеризується стійкістю роботи об’єкту в надзвичайних ситуаціях.

Зрозуміло, що збереження обладнання підприємства та його будівель має значення тільки тоді, коли в надзвичайних ситуаціях буде збережено також персонал, який зможе працювати на цьому обладнанні. Тому інженерний захист населення та персоналу займає важливе місце серед заходів по забезпеченню стійкості підприємства в надзвичайних ситуаціях. Підтвердження цій думці знаходимо і в літературі з цивільної оборони.

Принципами стійкості роботи промислових підприємств в надзвичайних ситуаціях є єдина нормативна директивна база, яка включає:

– Конституцію України;

– Закон про цивільну оборону України;

– Закон України про захист населення і території від надзвичайних ситуацій техногенного та природного характеру;

– Положення по цивільній обороні;

– нормативні документи про стійкість роботи об’єктів;

– директиви начальника штабу цивільної оборони України.

Під стійкістю роботи промислових підприємств розуміють їх можливість в умовах надзвичайних ситуацій мирного і воєнного часу виробляти продукцію в запланованому обсязі і номенклатурі, а при слабких пошкодженнях відновлювати виробництво в мінімальні терміни.

Стійкість роботи промислового підприємства складається з:

– стійкості інженерно-технічного комплексу (будівель, споруд, систем енерго-, газо-, водозабезпечення, технічного обладнання і т.п.) до дії зовнішніх факторів при аваріях, катастрофах, стихійному лиху, а також при застосуванні щодо них сучасної зброї;

– стійкості виробничої діяльності (захист виробничого персоналу, надійність систем управління, постачання, поновлення роботи в найкоротші терміни).

Під стійкістю роботи об’єктів, які не виробляють матеріальних цінностей, розуміють їх можливість виконувати свої функції в умовах надзвичайних ситуацій.

Фактори, від яких залежить стійкість роботи об’єктів в надзвичайних ситуаціях мирного і воєнного часу:

– надійність захисту робітників і службовців;

– безпечність розташування об’єкту відносно зон можливих руйнувань;

– можливість інженерно-технічного комплексу протистояти ударній хвилі будь-якого вибуху і уражаючим діям ядерної зброї;

– безперервність постачання електроенергією, паливом, сировиною, газом і всім необхідним для впуску продукції;

– надійність керування виробництвом, силами і засобами цивільної оборони;

– підготовленість підприємства до поновлення виробництва та проведення РіІНР.

Із перерахованих факторів випливають такі шляхи і засоби підвищення стійкості роботи промислових підприємств і галузей господарства України:

– нагромадження фондів захисних споруд і засобів індивідуального захисту;

– будівництво важливих підприємств за межами зон можливих руйнувань;

– будівництво підприємств-дублерів;

– розширення шляхів сполучення і розвиток всіх видів транспорту;

– підсилення і дублювання енергетичних потужностей;
– розширення зв’язків між галузями промисловості і підприємствами;
– утворення матеріально-технічних резервів;
– підтримування сил цивільної оборони в постійній готовності.

6.2 Організація робіт і заходів для дослідження стійкості об’єкту економіки

Основою для проведення заходів по підвищенню стійкості роботи промислових підприємств надзвичайних ситуаціях є вимоги норм інженерно-технічних заходів цивільної оборони.

З метою підвищення стійкості роботи підприємств в надзвичайних ситуаціях мирного і воєнного часу проводяться дослідження по оцінці стійкості. Внаслідок дослідження повинні бути вивчені наступні питання:

– захист виробничого персоналу;
– захист засобів виробництва;
– стійкість виробничої діяльності при стихійному лиху, аваріях, катастрофах, а також при застосуванні противником сучасної зброї;
– готовність до відновлення порушеного виробництва.

Головна мета дослідження втому, щоб на основі вивчення всіх умов, які визначають виробничу діяльність підприємства в надзвичайних ситуаціях, виробити заходи, які сприяли б підвищенню стійкості його роботи.

Оцінка стійкості підприємства має на меті:

– визначення стійкості його роботи до уражаючих дій сучасної зброї, стихійного лиха, аварій, катастроф;
– визначення можливості виникнення вторинних уражаючих факторів і оцінка характеру ураження від цих факторів;
– аналіз надійності систем управління, постачання і промислових зв’язків.

6.2.1 Проведення дослідження стійкості роботи об’єкту економіки

Дослідження стійкості роботи в надзвичайних ситуаціях здійснюється штабом цивільної оборони підприємства і розрахунково-дослідними групами, які створюються з інженерно-технічного персоналу підприємства. Для роботи в цих групах можуть залучатись працівники науково-дослідних і проектно-конструкторських організацій.

На промисловому підприємстві можна утворювати такі розрахунково-дослідні групи:

- головного технолога;
- головного механіка;
- головного енергетика;
- відділу капітального будівництва;
- заступника директора з постачання і збуту і інші.

Кожна група проводить дослідження підвідомчого їй господарства (елементів об’єкту), оцінює їх стійкість і планує інженерно-технічні заходи в умовах надзвичайних ситуацій мирного і воєнного часу.

Для загального керівництва і координації роботи розрахунково-дослідних груп утворюється група керівництва на чолі з головним інженером.

Робота по дослідженню стійкості планується за трьома етапами:

- підготовчий – 10–15 днів;
- період досліджень – 1–2 місяці;
- заключний – 7–10 днів.

За висновками досліджень і пропозиціями керівництво цивільної оборони підприємства складає звіт з висновками, рекомендаціями і планами заходів по підвищенню стійкості роботи в надзвичайних ситуаціях мирного і воєнного часу, пересилає в штаб цивільної оборони для узгодження і затвердження.

6.2.2 Параметри об’єктів економіки, котрі враховуються при визначенні оцінки інженерного захисту робітників і службовців

Забезпечення надійного захисту робітників і службовців об’єкту в надзвичайних ситуаціях – один із основних шляхів підвищення стійкості роботи.

В комплексі заходів по реалізації цього шляху важливе місце займають заходи по інженерному захисту робітників і службовців.

Інженерний захист робітників і службовців – це захист з використанням інженерних споруд: сховищ, ПРУ, простіших укриттів. Він досягається шляхом завчасного проведення інженерних заходів по будівництву і обладнанню захисних споруд з врахуванням умов розташування об’єкту і вимог будівельних норм і правил.

Успішне виконання завдань інженерного захисту можливе при дотриманні таких умов:

– загальна місткість захисних споруд дозволяє сховати найбільшу працюючу зміну;

– захисні властивості споруд відповідають потребам (забезпечують захист людей від надлишкового тиску ударної хвилі і радіоактивного випромінювання, які очікуються);

– фільтровентиляційне обладнання захисних споруд забезпечує життєдіяльність людей протягом встановленого терміну безперервного перебування їх в захисних спорудах;

– розміщення захисних споруд відносно місця роботи.

З перерахованого випливає, що оцінка інженерного захисту робітників і службовців підприємства полягає у визначенні показників, які характеризують можливість інженерних споруд забезпечити ці умови.

На основі висновків оцінки інженерного захисту робітників і службовців підприємства визначають заходи по підвищенню надійності захисту, а, відповідно, і по підвищенню стійкості роботи підприємства в надзвичайних ситуаціях.

6.3 Розрахунок штучної вентиляції

Загальнообмінна вентиляція застосовується для видалення надлишкового тепла при відсутності токсичних виділень, а також у випадках, коли характер технологічного процесу та особливості виробничого устаткування виключають можливість використання місцевої витяжної вентиляції.

В умовах промислового виробництва найбільш розповсюджена припливно-витяжна система вентиляції із загальним припливом в робочу зону та місцевою витяжкою шкідливих речовин безпосередньо з місць їх утворення.

Місцева витяжна вентиляція здійснюється за допомогою місцевих витяжних зонтів, всмоктуючих панелей, витяжних шаф, бортових відсмоктувачів.

Основне завдання розрахунку загальнообмінних систем штучної вентиляції – визначити кількість повітря, що необхідно подати і вилучити з приміщення.

Для приміщень, де немає шкідливих виділень (або кількість їх незначна) приплив (витяжку) повітря можна визначити за кратністю повітрообміну (k) – відношенням об'єму вентиляційного повітря L ($м^3$/год) до об'єму приміщення V ($м^3$):

$$k = \frac{L}{V_п}. \qquad (6.1)$$

Для нашого випадку при розмірах приміщення 3м · 6м · 3 м маємо об’єм приміщення $V_п$=54 $м^3$. Об’єм повітря на одного працівника при трьох працюючих становить 18 $м^3$.

Для приміщень без шкідливих виділень та надлишкового тепла можна використати формулу:

$$L = l \times n, \qquad (6.2)$$

де l – мінімальне подання повітря на одного працівника відповідно до санітарних норм (при об'ємі приміщення, що припадає на одного працівника, до 20 $м^3$ – 30 $м^3$/год, а при об'ємі більше 20 $м^3$ – 20 $м^3$/год);

n– кількість працівників в приміщенні.

Отже, для трьох працюючих в приміщенні згідно (6.2) L=30·3 = 90$м^3$.

Тепер кратність повітрообміну згідно (6.1) становить 90/54=1,67.

Використовуючи спеціальну довідникову літературу [ ], можна встановити для даного значення кратності повітрообміну об’єм припливного повітря. Схему вентиляції зображено на рисунку 6.1.

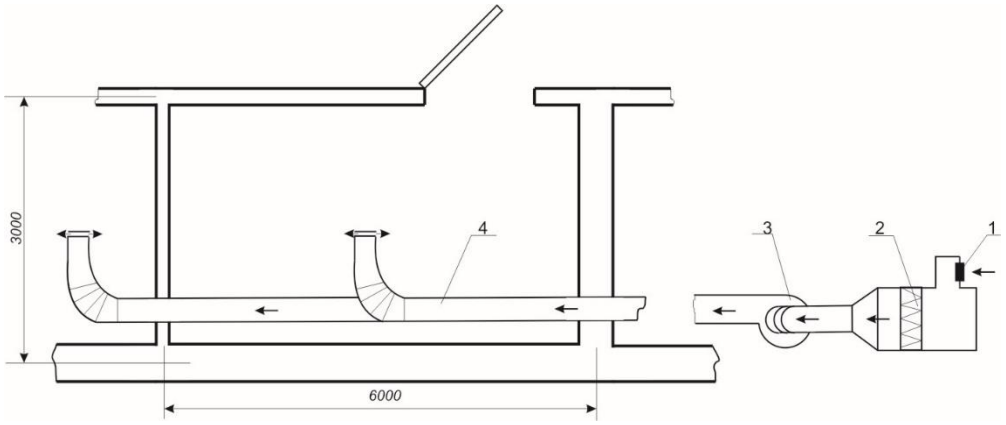


Рисунок 6.1 – Схема вентиляції приміщення:
1 – повітрозабірний пристрій; 2 – очисний фільтр; 3 – вентилятор;
4 – система повітропроводів та припливних патрубків

6.4 Пожежна безпека

Горіння – це швидка хімічна реакція окислення горючої речовини киснем повітря або іншим окислювачем, під час якої виділяється тепло і світло. При повному згорянні вуглецю, що становить більшу частину палива, утворюється вуглекислий газ. Якщо кисню не вистачає, крім вуглекислого газу утворюватиметься окис вуглецю, який ще може горіти. Для горіння потрібно, щоб швидкість його забезпечувала перевищення кількості тепла, яке виділяється, у порівнянні з теплом, що розсіюється в навколишньому просторі, і температура в зоні горіння була достатньою для підготовки горючої речовини до займання дедалі нових її частин. Для займання горючої рідини вона повинна мати таку температуру, щоб концентрація її парів у повітрі над її поверхнею була достатньою. Деревина або кам'яне вугілля спочатку розкладаються під дією нагрівання з утворенням горючих газів.

Запалювання – це стійке загоряння горючої речовини (парів і газів над ними) від місцевого нагрівання. Запалювання може спричинитися дотиком полум'я або розпеченого предмета.

Спалах – швидке згоряння суміші парів горючої речовини з повітрям або киснем. Виникає він внаслідок зіткнення суміші з полум'ям, електричною іскрою або нагрітим предметом. Найменша температура, за якої пари утворюють з повітрям займисту суміш, називається температурою спалаху. За високої температури замість короткочасного спалаху може зайнятися горюча речовина.

Вибух – дуже швидке перетворення речовини (вибухове горіння), що супроводиться виділенням великої кількості енергії й утворенням великої кількості газів, які своїм тиском можуть спричинити руйнування. Гарячі газоподібні продукти вибуху, стикаючись із повітрям, часто займаються, що може призвести і до пожежі.

Найменшу і найбільшу концентрацію горючих парів, газів або пилу в повітрі, що утворюють вибухову суміш, називають відповідно нижньою і верхньою межами вибуховості. За більшої, ніж верхня межа вибуховості, концентрації парів вибух не виникне через нестачу кисню.

Приміщення, в котрому працюють оператори ЕОМ по розробці даної теми роботи, згідно ОНТП 24 відноситься до категорії В, класу П-IIа ПУЕ 76/87 по пожежній небезпеці. В приміщенні є горючі речовини: волокнисті (папір), тверді (дерево).

Пожежа в приміщенні представляє особливу небезпеку, так як пов’язана з значними матеріальними втратами. Як відомо, пожежа може виникнути при взаємодії горючих речовин, окислювача і джерела запалювання.

Горючими речовинами являються будівельні матеріали для акустичної обробки приміщення, перегородки, двері, підлога, папір для принтеру, корпуса ПЕОМ і принтерів, ізоляція кабелів. Особливістю сучасних ПЕОМ являється дуже висока щільність розміщення елементів електронних схем.

При проходженні електричного струму по провідниках і деталях виділяється тепло, що в умовах їх високої щільності може привести до перегріву. Надійна робота окремих елементів і електричних схем в цілому забезпечується тільки в визначених інтервалах температури, вологості і при заданих електричних параметрах.

При відхиленні реальних умов експлуатації від розрахункових може виникнути пожежонебезпечна ситуація.

Кабельні лінії зв’язку являються найбільш пожежонебезпечним місцем. Для зниження загоряння і здатності розповсюдження вогню кабелі покривають вогнетривким покриттям.

Для гасіння пожежі на початковій стадії її виникнення в приміщенні встановлені 30 вуглекислотних вогнегасники ВВ-2.

Для передбачення пожежі в приміщені прийняті такі міри:

– передбачений вільний доступ до мережевих рубильників і вимикачів;

– на випадок короткого замикання передбачені запобіжники і автоматичне відключення мережі;

– в наявності є вогнегасники ВВ-2 для гасіння електрообладнання і ВХП-10 для гасіння об’єктів, що не знаходяться під напругою з розрахунку 1 вогнегасник на 12 м^2;

– вхідні двері приміщення відкриваються назовні;

– ширина дверей не менше 0,8 м, а висота проходу більше 1 м;

– в приміщенні є план евакуації людей;

– у приміщенні знаходиться 10 пожежних кранів;

– ширина загального коридору, ширина дверей, висота дверей відповідають нормативним значенням, що наведені й таблиці 6.2:

Таблиця 6.2 – Нормативні та існуючі параметри дверей та коридору

	Нормативні значення, м	Існуючі значення, м
Ширина коридору	> 2,0	2,5
Ширина дверей	> 0,8	1,2
Висота дверей	> 2,0	2,5

7 ЕКОЛОГІЯ

7.1 Енергозбереження і його роль у вирішенні екологічних проблем

Енергоефективність та енергозбереження є пріоритетними напрямами енергетичної політики більшості країн світу. Це обумовлено вичерпанням невідновлювальних паливно-енергетичних ресурсів, відсутністю реальних альтернатив їх заміни, наявністю ризиків при їх виробництві і транспортуванні. В останній час ці чинники набувають все більшого значення у зв'язку із загальною нестабільністю у регіонах видобутку паливно-енергетичних ресурсів (ПЕР), напругою на паливно-ресурсних ринках та несприятливими прогнозами щодо подальшого зростання цін на енергоресурси. Розвинені країни світу, у першу чергу, країни ЄС, які вже досягли значних успіхів у вирішенні проблем енергоефективності, продовжують пошук нових джерел енергозабезпечення та розробку заходів щодо енергозбереження, що є позитивним прикладом для України.

З огляду на ситуацію, що сьогодні складається, вирішення цих проблем буде відбуватися в умовах загальної нестабільності в світі, у тому числі і на паливно-ресурсних ринках, несприятливих прогнозів щодо подальшого зростання цін на енергоресурси та незначних іноземних інвестицій у вітчизняну економіку.

Досвід розвинутих країн і власний досвід України вказує на необхідність державного регулювання процесами енергозбереження та проведення цілеспрямованої державної політики. Тільки держава шляхом виваженої законодавчої, гнучкої цінової, тарифної та податкової політики може забезпечити дієздатність фінансового механізму енергозбереження.

Основними принципами такої політики повинні стати:

– пріоритет підвищення ефективності використання паливно-енергетичних ресурсів над зростанням обсягів їх видобутку й виробництва теплової та електричної енергії;

– відповідність політики загальним ринковим перетворенням в країні;

– пріоритетність забезпечення безпеки здоров'я людини, соціально-побутових умов її життя, охорони навколишнього середовища при видобутку, виробництві, переробці, транспортуванні та використанні паливно-енергетичних ресурсів та (або) енергії;

– здійснення державного регулювання у сфері енергозбереження, в першу чергу, контролю виконання законів, нормативів та прийнятих рішень;

– необхідність економічної підтримки енергозбереження, стимулювання використання відновлювальних джерел енергії;

– обов'язковість вірогідного обліку паливно-енергетичних ресурсів, що виробляються та споживаються;

– системний підхід в енергозбереженні;

– реалізація інформаційної, освітньої та науково-дослідницької діяльності у сфері енергозбереження.

З результатів розрахунків проведених на базі прогнозних даних проекту енергетичної стратегії України до 2030 року виходить, що в країні за рахунок енергозбереження до 2020 року можна досягти економії енергоносіїв у загальному обсязі порядку 470 млн. т у.п., що відповідає зменшенню витрат на їх імпорт близько 38 млрд. дол.

Чиста економія (із врахуванням витрат на енергозбереження) може скласти у 2020 році близько 15 млрд. дол. Такі переваги відповідають зниженню енергоємності ВВП більш ніж у 4,8 рази.

Інші переваги енергозбереження складаються у зменшенні техногенного навантаження на навколишнє середовище: зменшення обсягів викидів CO_2 у 2020 році може досягти 207 млн. т, що поліпшить умови життя населення країни, а також забезпечить можливість торгувати квотами і одержувати додаткові дивіденди на впровадження новітніх технологій і взагалі на соціально-економічний розвиток країни.

Крім того, енергозбереження в енергетиці дозволить зекономити у 2020 році близько 323 млрд. кВт год. електроенергії, що дозволить не вводити в експлуатацію електрогенеруючих потужностей у 37 ГВт і зменшити потреби в інвестиціях для галузі на 74 млрд. дол.

Таким чином, проведення нової політики енергозбереження забезпечить для країни такі дивіденди:

1. Знизяться обсяги необхідного імпорту енергоносіїв (це особливо важливо, бо при зростанні економіки потреби в енергоносіях будуть зростати).
2. За рахунок економії коштів на імпорті енергоносіїв з'явиться можливість оновлення основних фондів та впровадження нових технологій.
3. Технологічне переоснащення виробництв призведе до зменшення обсягів шкідливих викидів у навколишнє середовище (це взагалі є дуже важливим при нинішній екологічній ситуації в країні, окрім того при відповідному розвитку подій може з'явитися можливість торгівлі квотами).
4. Підвищиться конкурентоспроможність вітчизняних товарів, бо зменшиться частка енергії в собівартості продукції.
5. Буде відбуватися відстрочка термінів вичерпання вітчизняних не відновлювальних енергоносіїв
6. З'являться також інші переваги, що пов'язані із соціальними стандартами, з поліпшенням міжнародного іміджу країни.

Все це дасть додаткові можливості країні щодо досягнення європейського рівня соціально-економічного розвитку і забезпечення у прогнозований період її повноправного членства у європейському співтоваристві.

Забезпечення енергетичної безпеки є одним із найбільш важливим питань, які визначають можливість сталого розвитку суспільства в країнах світу в тому числі і в Україні. Проблема забезпечення енергетичної безпеки стоїть в центрі уваги енергетичної політики майже для всіх країн світу.

Енергетична безпека держави – це стан готовності паливно-енергетичного комплексу країни щодо максимально надійного, технічно безпечного, екологічно прийнятного, економічно ефективного та обґрунтовано достатнього енергозабезпечення економіки держави й населення, а також щодо гарантованого забезпечення можливості керівництва держави у формуванні і здійсненні політики захисту національних інтересів у сфері енергетики без зовнішнього і внутрішнього тиску.

Виходячи з такого визначення енергетичної безпеки можна виділити наступні її складові: енергозабезпечення, енергетичну незалежность, екологічну прийнятність та соціальну стабільність. Необхідно зазначити, що характер поділу на складові є дещо умовним, тому деякі механізми та стратегічні пріоритети забезпечення енергетичної безпеки будуть загальними для різних її складових. Це цілком зрозуміло в зв'язку із багатоплановістю самого поняття енергетичної безпеки, тісним зв'язком та взаємним впливом різних її складових.

На сучасному етапі основними реальними та потенційними загрозами енергетичній безпеці України є неефективність використання паливно-енергетичних ресурсів, відсутність активної політики енергозбереження, недостатні темпи диверсифікації джерел постачання енергоносіїв, низький рівень екологічної прийнятності енергетичного виробництва та соціальні конфлікти в сфері енергетичного виробництва та енергопостачання населення.

Сучасний стан енергетичної безпеки в Україні є незадовільним. Однією із основних причин цього є низька ефективність виробництва, транспортування та споживання ПЕР, відсутність активної політики енергозбереження в країні. Вплив заходів енергоефективності на енергетичну безпеку є багатоплановим та значним, що позначається на стані енергетичної безпеки з усіх її складових.

7.1.1 Складова енергозабезпечення

Не визиває сумнівів що визначальним фактором впливу на цю складову буде рівень енергоємності споживання. Необхідність стабільного, максимально надійного та якісного забезпечення енергетичними ресурсами потреб національного господарства і населення як головної складової енергетичної безпеки залежить від реалізації цілої низки заходів з підвищення енергетичної ефективності.

Як показують результати розрахунків, динаміка росту показника енергозабезпечення на період до 2020 року спостерігається для всіх варіантів, в яких реалізуються заходи щодо енергозбереження. Ці заходи дозволяють значно (у 2,5-4 рази) підвищити рівень показника енергозабезпечення.

7.1.2 Складова енергетичної незалежності

Україна є енергодифіцитною державою яка на сьогодні лише на половину задовольняє потреби в паливі та енергії, що є негативним чинником впливу на її енергетичну безпеку. Головними чинниками, які впливають на енергетичну незалежність є відносний рівень імпорту енергоносіїв та рівень його диверсифікації. Зниження рівня енергетичної залежності як складової енергетичної безпеки залежить, в першу чергу, від заходів щодо зменшення частки загального імпорту паливно-енергетичних ресурсів, яке повинно здійснюватися за рахунок збільшення рівня та ефективності власного виробництва ПЕР та за рахунок підвищення ефективності їх використання.

Враховуючи можливості країни щодо нарощування власного видобутку ПЕР і нарощування потужностей ПЕК та існуючий значний потенціал енергозбереження особлива увага повинна приділятися заходам енергоефективності. При цьому головним механізмом для запобігання можливому зростанню собівартості власного видобутку (виробництва) енергоносіїв повинно бути технологічне переозброєння галузі за рахунок впровадження інновацій.

Аналіз результатів розрахунків впливу різних варіантів розвитку ПЕК України показує на їх значну залежність саме від рівня енергетичної ефективності.

Так у варіанті збереження енергоємності на рівні 2000р., як показують розрахунки, буде спостерігатися зменшення показника імпорту з часом, що пояснюється ростом частки імпорту нафти і газу пов'язане зі зростанням економіки і таким же зростанням енергоспоживання, а також обмеженими можливостями власного видобутку цих енергоносіїв та прогнозованим зростанням цін на імпортовані ПЕР. Економічне ж зростання дає більше можливостей для диверсифікації постачання енергоносіїв які імпортуються, що позитивно позначається на показнику монопольного імпорту, який зростає практично для всіх розглянутих варіантів.

Зменшення енергоємності ВВП, як показують результати розрахунків на всьому розглянутому періоді часу (2000-2020р.р.), дозволяє значно підвищити значення показників енергетичної незалежності. Це відбувається за рахунок

зменшення енергетичних потреб економіки в результаті впровадження енергозберігаючих заходів. До того ж, ці енергоносії є більш дорогими відносно вугілля, частка ж власного видобутку якого в Україні зостається великою на весь розглянутий період часу.

7.1.3 Складова екологічної прийнятності

Складна екологічна ситуація в Україні, яка зумовлена значною мірою шкідливими викидами підприємств традиційної енергетики також вимагає широкого впровадження енергозберігаючих заходів. Існує певна залежність між послідовним проведенням політики підвищення енергоефективності (реалізацією енергозберігаючих заходів) у всіх сферах національного господарства та охороною навколишнього середовища (позитивним впливом на довкілля). Ефективне енергоспоживання в галузях економіки та населенням зменшить загальне використання енергоресурсів, що відповідно, призведе до зменшення забруднення довкілля, зокрема, до скорочення викидів в атмосферу антропогенних газів, що виникають у промислових процесах виробництва енергоносіїв. Покращенню екологічного стану довкілля будуть також сприяти впровадження енергоефективних технологій, устаткування, обладнання, побутових енергетичних пристроїв; використання нетрадиційних поновлюваних джерел енергії, альтернативних видів палива, що забезпечать економію або заміщення енергоресурсів, технології видобутку, виробництва та використання яких є екологічно неприйнятними. Тому при плануванні і проведенні політики енергозбереження та підвищення енергоефективності виробництва в Україні необхідно поєднувати ці питання з проблемами екології в єдину державну політику розвитку економіки держави.

Енергозберігаючі заходи повинні мати позитивний екологічний вплив на довкілля і, навпаки, при оцінці витрат на зменшення шкідливих викидів необхідно враховувати економічні вигоди від енергозбереження, тобто окупність цих витрат.

Для оцінки екологічної прийнятності енергетичного виробництва використано показники, які враховують рівень викидів у відносному вигляді у порівнянні з викидами у 1990р. (прийнятими Україною за Кіотською згодою) та

вартість ліквідації наслідків від впливу основних забруднювачів (SO2, NO2, золи і парникових газів). Результати розрахунків показують, що рівень екологічної прийнятності зменшується з часом для всіх варіантів крім варіанту де рівень енергоємності ВВП поступово наближається до рівня енергоємності розвинутих країн. Для базового варіанту економічного розвитку, який був прийнятий у проекті "Енергетичної стратегії...2030р..." це зниження є незначним на ~ 5% у 2020 році, а для варіанту де енергоємність ВВП залишається на рівні 2000 р. – дуже значним, що пояснюється як темпами нарощування виробництва і споживання електроенергії, так і темпами введення обладнання для уловлювання забруднювачів. Варіант підвищення енергетичної ефективності є превалюючим, бо веде до зменшення виробництва електроенергії для потреб економіки і майже пропорціонального зменшення викидів парникових газів, які у вартості викидів дають найбільший вклад, але найменше піддаються очищенню. Інші забруднювачі можуть очищуватись більш ефективно. Зростання економіки дає більше можливостей для оновлення обладнання електростанцій та впровадження технологій очищення шкідливих викидів, таких як: SO_2, NO_2 та попіл.

Загалом реалізація енергоефективних варіантів дозволить значно збільшити значення показника екологічної прийнятності відносно варіанту незмінної енергоємності, в тім, тільки варіант де енергоємність ВВП поступово наближається до рівня розвинутих країн дає можливість забезпечити збільшення рівня екологічної прийнятності у 2020 році відносно рівня 2000 року.

7.1.4 Складова соціальної стабільності

Енергозбереження є довгостроковою, стратегічно важливою складовою державної політики, яка містить значні резерви впливу на соціально-економічні перетворення в країні, а тобто на соціальну стабільність в суспільстві.

Соціальний фактор є достатньо значущим в забезпеченні енергетичної безпеки, навіть у відносно благополучних економічно розвинутих країнах. Проблеми виникнення загроз енергетичної безпеки в цих країнах пов'язуються, в першу чергу, із зростаючим попитом на бензин та ціновою політикою щодо нього.

Ця ситуація змушує країни змінювати політику управління попитом, зокрема політику підвищення енергетичної ефективності.

В Україні соціальні загрози, пов'язані з енергетичною сферою, є гострішими, що пояснюється як значною кількістю факторів впливу на них, так і економічним становищем в країні, яке ще не дозволяє ефективно зменшувати рівень цих загроз.

Серед найбільш значущих факторів впливу слід відзначити: значний рівень енергетичної складової в собівартості продукції, низька платоспроможність населення, в тому числі, щодо енергетичних послуг, а також екологічний фактор. В самій енергетичній галузі факторами впливу є: невиплата заробітної плати, зростання рівня безробіття, аварії та травматизм на виробництві (особливо у вугільній галузі). Можна зробити припущення, що внаслідок економічного зростання в країні, вплив зазначених факторів в енергетичній галузі буде значно зменшуватися. Заходи найбільш ефективного використання енергоресурсів (реалізація найбільших обсягів потенціалу енергозбереження) за рахунок впровадження новітніх технологічних процесів та інноваційних перетворень будуть найкраще сприяти покращенню екології, умов та охорони праці, зниженню травматизму та смертності на виробництві.

Значний вплив на рівень соціальної напруги, пов'язаний з цінами на енергоресурси (що прямо пов'язано із споживчими цінами) буде залишатися ще достатньо довго у термін часу, що розглядається. Значні коливання цін на нафту у світі будуть збільшувати економічні ризики, що буде позначатися і на соціальній сфері.

Для стимулювання виконання накреслених заходів з енергозбереження та зниження витрат необхідні стабілізація фінансового стану підприємств енергетичної галузі і відповідна тарифна стратегія, яка передбачала би врахування фактичних витрат за постачання енергії споживачам, відсутність перехресних субсидій і бартерних взаєморозрахунків, мінімізацію комерційних втрат, механізми подолання неплатежів, соціальні інтереси споживачів енергії.

Для ілюстрації розглянемо показник, який характеризує співвідношення вартості енергетичних ресурсів (яка є також складовою собівартості цін для

споживачів) та рівня заробітної плати в Україні відносно цих показників для країн ЄС. Ці результати є ще одним із аргументів на користь підвищення рівня енергетичної ефективності, що значно впливає на рівень соціальної стабільності, особливо в період 2015-2020 рр.

Таким чином, необхідність сталого енергопостачання населення і економіки країни, зниження рівня енергетичної залежності, зниження техногенного навантаження на довкілля, зниження соціальної напруги у сфері енергетики, загальне підвищення рівня енергетичної безпеки України потребують вирішення проблем, пов'язаних з низькою енергетичною ефективністю економіки країни, значними витратами суспільства на своє енергозабезпечення. Тобто, реалізація заходів енергетичної ефективності, покликаних забезпечити реалізацію одних із головних задач енергетичної стратегії держави, є переважним фактором підвищення рівня енергетичної безпеки України.

Різні фактори впливу (економічні, екологічні, соціальні) рівня енергетичної ефективності на енергетичну безпеку, які були розглянуті вище, хоча і в різному ступені, але однозначно показують на позитивну роль підвищення рівня енергетичної ефективності в забезпеченні енергетичної безпеки країни.

7.2 Застосування екологічних знань у різних галузях соціально-політичного життя

У перекладі з грецького слово "політика" означає мистецтво управління державою. Серед багатьох напрямків політика (оборонна, економічна, культурна тощо) все більшого значення набуває екологічна політика держави і людського суспільства в цілому. Всі напрямки політики тісно пов'язані між собою та взаємозалежні і визначаються мстою, яка може бути поточною чи довгостроковою стратегічною. Для людства стратегічною метою є забезпечення сталого розвитку, головною рисою якого є гармонійні взаємовідносини між людством і природою. Саме цим пояснюється невпинне зростання важливості екологічної міжнародної і державної політики.

Досвід країн, яким вдалося стримати погіршення чи навіть покращити стан природного середовища (Канада, Японія, Фінляндія та інші) показує, що екологічна політика повинна ґрунтуватися на таких принципах:

1) побудова практичних заходів на найновітніших досягненнях науки і технологій;

2) виділення на природоохоронну діяльність необхідних матеріально-фінансових ресурсів;

3) раціональне поєднання примусових, економічних та моральних важелів у системі управління природокористуванням;

4) динамічне правове екологічне забезпечення;

5) високий рівень екологічної освіти і культури населення;

6) активна участь громадськості.

Документи ООН (Порядок денний XXI століття, Конвенція про охорону біологічного різноманіття, Рамкова конвенція ООН про зміну клімату, Про контроль суднових баластних вод й осадів та управління ними та ін.) враховують усі шість принципів у рекомендаціях державам і в програмах дій людства в цілому. В "Порядку денному на XXI століття" підкреслюється: "Дуже важливо, щоб всі – від політичних діячів до широкої громадськості – усвідомили ту провідну роль, котру повинна відігравати наука і техніка в охороні довкілля і розвитку людства. Вчені і спеціалісти повинні розробити кодекс дій і керівні принципи для узгодження потреб людини та інтересів захисту навколишнього середовища. Ці кодекси допоможуть оцінити цілісність системи, яка підтримує життя на нашій планеті". Серед першорядних наукових проблем вказуються такі: раціоналізація управління природокористуванням і розвитком з метою сьогоденного виживання і задоволення майбутніх проблем людства:

– з'ясування взаємодії між атмосферою, водою і сушею, які утворюють єдину екологічну систему;

– поглиблення знань щодо таких явищ, як зміна клімату, ріст споживання природних ресурсів, демографічні тенденції, деградація природного середовища;

– оцінка стану довкілля на місцевому, регіональному і глобальному рівнях та визначення національних і регіональних напрямків сталого розвитку;

– розробка показників якості життя, що охоплюють соціальне забезпечення, здоров'я, освіту і стан природного середовища та економіки;

– обґрунтування методів оцінки екологічної чистоти нових технологій.

Незважаючи на відсутність координації дій вчених-екологів у планетарному масштабі, розрізнені дослідження в окремих країнах постійно доповнюють і поновлюють людські уявлення про природні процеси і явища.

Брюссельська школа І. Пригожина на базі аналізу історичних перетворень у науці дійшла висновку, що історія науки – це не лінійна серія послідовних наближень до істини. Запропоновано нову всеохоплюючу теорію змін, згідно з якою саморегульоване перетворення природних і штучних систем здійснюється за рахунок взаємного впливу і доповнення хаотичних і детермінованих процесів.

Існує думка, що традиційний шлях від індивідуальних змін до розвитку цілого виявляється недостатнім і веде до помилкових висновків. Також сучасна людська індивідуалістична філософія протирічить основному принципу біології, за яким головне – це вид, а інтереси особини другорядні.

Наші дії по збереженню біосфери науково недостатньо обґрунтовані. Треба з'ясувати, які елементи в біосфері і в кліматичній системі є критичними з точки зору впливу людини. Додатково оцінка можливих змін клімату стримується відсутністю кількісних оцінок внеску антропогенного фактора в формування клімату.

Для реалізації програм сталого розвитку потрібні значні кошти. В матеріалах ООН головними фінансовими джерелами передбачаються розвинені країни та приватний сектор. Плануються витрати на вказані цілі в розмірі 0,7 відсотка ВНП цих країн. Для країн, що розвиваються, необхідні витрати складають близько 8 млрд. дол. США щорічно.

У галузі управління "Порядок денний на XXI століття" передбачає посилення ролі держав шляхом більш цілеспрямованого адміністративного керівництва з використанням економічних стимулів, законів і норм. Звертається

увага на важливість використання етичних принципів у поведінці ділових і промислових кіл.

Згідно з позицією ООН міжнародне право повинно сприяти проведенню єдиної політики як в галузі охорони природи, так і в галузі розвитку. Для цього необхідно переглянути і вдосконалити існуюче законодавство, вирішуючи такі головні завдання:

– підготовка угод до вдосконалення міжнародних норм по охороні середовища з урахуванням різного стану і можливостей різних країн;

– оцінка можливості встановлення загальних прав і обов'язків держав у питаннях сталого розвитку;

– розробка заходів щодо запобігання чи вирішення міжнародних суперечок в питаннях сталого розвитку.

Підкреслюється, що законодавча політика в питаннях довкілля повинна бути спрямована на ліквідацію основних причин, що викликають погіршення стану природного середовища і не повинні використовуватися для введення непотрібних обмежень у міжнародній торгівлі.

Важливе значення в документах ООН приділяється питанням екологічної просвіти. Звертається увага на те, що багато людей не розуміють тісного зв'язку між діяльністю людини і станом довкілля, тому що не мають точної і достатньої інформації. Підкреслюється, що освіта повинна давати уяву не тільки про фізичне і біологічне довкілля, але і сприяти розумінню соціально-економічного стану і проблем розвитку людини. В галузі освіти та інформації головними вважаються наступні задачі:

– забезпечення просвіти щодо питань розвитку і збереження довкілля для людей різного віку;

– включення концепції розвитку та охорони навколишнього середовища у всі навчальні програми з аналізом причин. Особливу увагу приділити підготовці майбутніх керівників;

– залучення школярів до місцевих і регіональних досліджень стану природного середовища, включаючи питання безпечної питної води, санітарії, харчових продуктів та наслідків використання природних ресурсів;

– заохочення урядів, промисловості, навчальних закладів, недержавних громадських організацій до підготовки кадрів в області раціонального використання навколишнього середовища;

– забезпечення місцевих громад підготовленими з числа жителів спеціалістами для вирішення проблем охорони довкілля;

– робота з засобами масової інформації, рекламної індустрії, мистецтва для заохочування більш активної участі населення в обговоренні проблем навколишнього середовища.

ООН визнала велике значення неурядових організацій (НО) у процесі досягнення мети, яка поставлена в "Порядку денному на XXI століття", внаслідок таких причин:

– незалежність від державних і інших секторів суспільства;

– володіння різноманітними знаннями в галузях, котрі необхідні для забезпечення екологічно безпечного і соціально надійного сталого розвитку;

– спроможність допомогти суспільству досягти згоди з питань, яким шляхом перейти від нестійкого розвитку до стійкого.

Внаслідок цього рекомендовано як підрозділам ООН, так і окремим урядам запрошувати НО до участі в формуванні політики і прийнятті рішень, що спрямовані на досягнення сталого розвитку. Доцільно також заохочувати сумісну діяльність НО і місцевих органів влади.

У розвиток рекомендацій ООН на Четвертій конференції міністрів Комітету з екологічної політики Європейської економічної комісії (Оргус, Данія, 1998) було прийнято Конвенцію "Про доступ до інформації, участі громадськості в прийнятті рішень і доступ до правосуддя з питань, що стосуються навколишнього середовища". Мета Конвенції – сприяння захисту права кожної людини нинішнього і прийдешніх поколінь жити в навколишньому середовищі, сприятливому для здоров'я та добробуту. Відповідно до Оргуської (Орхуської) Конвенції європейські держави (і Україна в тому числі) мають забезпечити наступне:

– розвиток законодавчо-правового поля, яке сформує мотивації та процедури для ефективної участі громадськості у вирішенні екологічних проблем;

– розвиток нових інфраструктурних можливостей, які б створили умови для посилення громадської екологічної активності;

– створення умов щодо активного включення судової гілки влади як дієвого механізму вирішення екологічних суперечок та конфліктів;

– створення та розвиток прозорої, доступної системи комунікацій та інформаційних зв'язків, які забезпечили б повний, достовірний, оперативний обмін екологічною інформацією.

Екологічна політика держави чи місцевої автономії будується з урахуванням міжнародних рекомендацій і оформляється у вигляді документів різного рівня та довгостроковості. У 1998 році Верховна Рада України затвердила "Основні напрямки державної екологічної політики у галузі охорони довкілля, використання природних ресурсів та забезпечення екологічної безпеки", в яких викладена стратегія екологічної політики нашої держави. В 1999 році Верховною Радою було ухвалено Закони України "Про загальнодержавну програму поводження з токсичними відходами" та "Про загальнодержавну програму формування національної екомережі на 2000-2015 роки".

Територіальні адміністративні одиниці (області, райони, міста) розробляють свої Програми, Плани дій, Концепції щодо охорони природного середовища, покращення природокористування та інших питань екологічної політики в межах своєї території.

ВИСНОВОК

У магістерській роботі виконано дослідження способів забезпечення автентифікації користувачів розподіленої комп'ютерної системи на основі протоколу Kerberos.

Основні наукові та практичні результати полягають в наступному.

1. Проведено аналіз наукових публікацій, протоколів та практичних рішень в області реалізації методів автентифікації користувачів розподіленохї комп'ютерної системи.

2. Проаналізовано можливості протоколу на основі віддаленого сервера автентифікації.

3. Здійснено аналіз ризиків при використанні методу автентифікації з віддаленим сервером.

4. Запропоновано практичну реалізацію методу для операційної системи Windows.

ПЕРЕЛІК ПОСИЛАНЬ

1. Denning, P. J. (Ed.). (1990). Computers Under Attack: Intruders, Worms and Viruses. Addison-Wesley Paper, 592 pp.

2. Stoll, C. (1989). The cuckoo's egg: tracking a spy through a maze of computer espionage. New York: Doubleday.

3. ISO 7498-2 (1988). Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. International Standards Organisation.

4. ISO 10181-1 (1991). Open Systems Interconnection - Security Frameworks - Part 1: Overview. International Standards Organization.

5. Gilbert, I. E. (1989). Guide for Selecting Automated Risk Analysis Tools (NIST Special Publication 500-174).

6. Методичні вказівки по виконанню організаційно-економічної частини дипломних проектів науково-дослідницького характеру для студентів спеціальності 7.080401 “Інформаційні управляючі системи та технології” / Кирич Н.Б., Зяйлик М.Ф., Брощак І.І., Шевчук Я.М – Тернопіль, ТНТУ, – 2009. –11 с.

7. Основы охраны труда: учебник / А. С. Касьян, А. И. Касьян, С. П. Дмитрюк. – Дн-ськ : Журфонд, 2007. – 494 с.

8. Безпека життєдіяльності: Навч. посібник./ За ред. В.Г. Цапка. 4–те вид., перероб. і доп. – К.: Знання, 2006. – 397 с.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 грудня 2019 року

ТЕРНОПІЛЬ
2019

М. Садівник
МАШИННЕ НАВЧАННЯ У БРАУЗЕРІ З ВИКОРИСТАННЯМ TENSORFLOW.JS 89
Р. Самець
ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ОЗОНОГЕНЕРАТОРІВ ДЛЯ МЕДИЧНИХ ОЗОНОТЕРАПЕВТИЧНИХ СИСТЕМ 90
Я. Самиця, М. Горалечко, Ю. Дзига
ІЄРАРХІЧНА СТРУКТУРА МОДЕЛЕЙ ЯКОСТІ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ 91
Я. Самиця, С. Магула
ПРИНЦИПИ ІНТЕГРАЛЬНОЇ ОЦІНКИ РІВНЯ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ 93
Т. Сачик, Н. Загородна
ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ В ЗАДАЧАХ АНАЛІЗУ ТА ОБРОБКИ ВЕЛИКИХ ДАНИХ 95
Д. Северин
ПРОГРАМНИЙ ЗАСІБ ДЛЯ УПРАВЛІННЯ ПРОЦЕСОМ МІГРАЦІЇ ВІРТУАЛЬНИХ МАШИН В ОБЧИСЛЮВАЛЬНІЙ ХМАРІ 96
О. Ситник, А. Лазорко
МЕТОД РЕПЛІКАЦІЇ ДАНИХ З ВИКОРИСТАННЯМ NFC-ТЕХНОЛОГІЇ 97
Т. Склярова, О. Палка
ІСТОРІЯ РОЗВИТКУ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ 98
В. Соборук, Л. Матійчук
ЗАДАЧІ ТЕСТУВАННЯ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 99
А. Тарапата, М. Іваник
ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ ДЛЯ ОЦІНЮВАННЯ ЯКОСТІ ПРОЕКТУ КОМП`ЮТЕРНИХ МЕРЕЖ 100
А. Тарапата, А. Гулик
ВИКОРИСТАННЯ МОДЕЛЕЙ ЯКОСТІ ДЛЯ РОЗРОБКИ ВИМОГ 101
П. Телевяк, Л. Матійчук
АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЇХ КЛАСИФІКАЦІЯ 102
О. Топчак, Н. Кунанець
РЕКОМЕНДАЦІЙНА СИСТЕМА РЕАБІЛІТАЦІЇ ХВОРИХ З ПРОБЛЕМАМИ ОПОРНО-РУХОВОГО АПАРАТУ 103
Б. Тригубець
РОЗРОБКА CMS ТА МЕТОДІВ ЗАХИСТУ WEB-САЙТІВ НА ЇЇ ОСНОВІ 104
Л. Тучапський, М. Поліщук
ЦИФРОВА ФІЛЬТРАЦІЯ РАДІОСИГНАЛІВ 105
М. Шмигельський, В. Ліщинський
ОСНОВНІ МЕТОДИ І ПРИЙОМИ ПОРУШЕННЯ БЕЗПЕКИ СУЧАСНИХ БЕЗДРОТОВИХ МЕРЕЖ 106
А. Шум'як, О. Палка, І. Пятківський
АНАЛІЗ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМ 107
Р. Яворський, В. Амбок, В. Леньо
ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ 108

УДК 004.056
Р. Яворський, В. Амбок, В. Леньо
Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

UDC 004.056
R. Yavorskii, V. Ambok, V. Lenio
(Ternopil Ivan Puluj National Technical University, Ukraine)

INFORMATION SECURITY CHALANGES FOR DEPLOYMENT OF INTRUSION DETECTION SYSTEMS

Розглянемо основні класи небезпек, характерних для розгортання систем виявлення вторгнень на основі віртуальних машин – Virtual Machines (VM), оскільки саме вони є основним елементом побудови інформаційної інфраструктури організації у хмарних сервісах [1].

VM image sharing. Вважається, що існує репозиторій образів різних VM, а користувач на їх основі може сконфігурувати потрібний образ. Таке використання образів з репозиторію може спричинити появу вразливостей у системі [2]. Зловмисник може знайти вразливості в існуючому образі або завантажити у репозиторій власний, шкідливий, образ VM.

VM isolation. З іншого боку проблему становить використання VM в ізоляції від інших віртуальних машин, що працюють на тому ж комп'ютері. Очевидно, що вони мають бути ізольовані одна від одної. Попри логічну ізоляцію існує проблема доступу до спільних ресурсів (пам'яті, дискового простору). Через що виникає проблема крос-VM атак.

VM escape. Це ситуація, коли зловмисник обходить систему управління VM [3]. В цьому випадку зловмисник отримає доступ до інших VM, що може спричинити також неавторизований доступ до файлів на жорстких дисках. До таких вразливостей в основному схильні системи
IaaS [4].

VM migration. Під час міграції весь інформаційний контент VM стає відкритим при передачі даних по мережі [5]. На додачу модуль міграції може бути скомпрометований атакуючим зловмисником для переміщення VM на сторонній сервер. Тому критично важливим є виконання операції міграції VM з дотриманням всіх заходів безпеки.

Безпечне управління образами забезпечується за допомогою спеціально розробленого фреймворку, згідно якого кожну операцію може виконувати тільки авторизований користувач. Крім того рекомендується використовувати журналювання всіх операцій.

Література

1. F. Sabahi, “Secure Virtualization for Cloud Environment Using Hypervisor-based Technology,” Int. Journal of Machine Learning and Computing, vol. 2, no. 1, 2012.
2. S.-F. Yang, W.-Y. Chen, and Y.-T. Wang, “ICAS: An inter-VM IDS Log Cloud Analysis System,” in 2011IEEE International Conference on Cloud Computing and Intelligence Systems, 2011, pp. 285–289.
3. S. L. and Z. L. and X. C. and Z. Y. and J. Chen, S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, “Virtualization security for cloud computing service,” in International Conference on Cloud and Service Computing (CSC), 2011, pp. 174–179.
4. M. Ibrahim, A.S. and Hamlyn-Harris, J. and Grundy, J. and Almorsy, “CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model,” in 5th International Conference on Network and System Security (NSS), 2011, pp. 113–120.
5. J. Sedayao, S. Su, X. Ma, M. Jiang, and K. Miao, “A Simple Technique for Securing Data at Rest Stored in a Computing Cloud,” in Proceedings of the 1st International Conference on Cloud Computing, 2009, pp. 553–558.