МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

IX Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 30 березня 2018 року)

Електронна версія

Київ
2018

УДК 341.123(045)(0.034.2PDF)

Організаційний комітет конференції:

Кудінов С.С. – голова організаційного комітету конференції, ректор Національної академії СБ України, кандидат юридичних наук, доцент; ***Золотухін Д.Ю.*** – співголова, заступник Міністра інформаційної політики України; ***Пилипчук В.Г.*** – співголова, директор Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України; ***Спірін О.М.*** – співголова, в.о. директора Інституту модернізації змісту освіти Міністерства освіти і науки України, доктор педагогічних наук, професор; ***Фальченко С.Л.*** – проректор з наукової роботи Національної академії Служби безпеки України, кандидат юридичних наук, доцент; ***Довгань О.Д.*** – перший заступник директора Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, старший науковий співробітник; ***Чорний Р.Л.*** – директор науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук, старший науковий співробітник; ***Мамченко С.М.*** – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор; ***Муратов О.Є.*** – заступник директора центру – начальник організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; ***Панченко В.М.*** – заступник директора інституту (з навчальної і наукової роботи) Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; ***Дашковська О.В.*** – старший науковий співробітник відділу модернізації вищої освіти Інституту модернізації змісту освіти Міністерства освіти і науки України, кандидат хімічних наук, доцент; ***Макобрій О.О.*** – головний спеціаліст сектору стратегічних комунікацій Міністерства інформаційної політики України; ***Давидова Т.О.*** – старший науковий консультант організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук

Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – Київ : Нац. акад. СБУ, 2018. – 408 с.

У збірнику висвітлюються актуальні проблеми забезпечення інформаційної та кібернетичної безпеки України та науково-практичні підходи до їх вирішення. Розглядаються питання формування системи забезпечення кібернетичної безпеки України, розвитку стратегічних комунікацій в Україні, удосконалення вітчизняного законодавства у сфері охорони державної та службової інформації, шляхи оновлення змісту вищої освіти фахівців з інформаційної безпеки держави.

Для працівників органів державної влади, науковців, викладачів, фахівців з інформаційної безпеки, широкої громадськості.

Тези доповідей публікуються в авторській редакції. Організаційний комітет залишає за собою право не поділяти думку авторів.

певні засоби захисту інформації, а також визначити основні пріоритети витрачання коштів, передбачених у бюджеті на забезпечення інформаційної безпеки (якщо підприємство практикує виділення фіксованих сум на ці цілі).

Література

1. Анисимов А.А. Менеджмент в сфере информационной безопасности М.: БИНОМ, 2009.

2. Основи управления информационной безопасностью / А.П.Курило, Н.Г.Милославская, М. Ю.Сенаторов и др. – М.: Горячая линия-Телеком, 2012.

3. Петренко С.А. Управление информационными рисками. Экономически оправдання безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, ДМК-Пресс, 2004.

4. Артемов В.Ю. Основи менеджменту для інформаційних аналітиків: курс лекцій / В.Ю.Артемов. – К.: КНТ, 2007.

УДК 004.56

Гулак Г.М.
кандидат технічних наук, доцент
Національна академія СБ України
Кащук В.І.
Національна академія СБ України
Складанний П.М.
Київський університет ім. Б. Грінченко

УТОЧНЕНА МОДЕЛЬ ПОРУШНИКА ТА МОДЕЛЬ РЕАЛІЗАЦІЇ КІБЕРАТАК В СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Реалізація ефективного кіберзахисту (включаючи, криптографічний захисту інформації (КЗІ)), в системах управління технологічними процесами (СУТП) потребує побудови адекватної моделі загроз, що в умовах постійного вдосконалення методів та засобів нападу [1] вимагає постійного уточнення моделі потенційного порушника системи захисту [2].

Аналіз повідомлень про кібератаки дає змогу визначити мету його злочинних дій, а саме нанесення суттєвих збитків власнику системи, мінімізуючи при цьому власні фінансові, матеріальні та інші витрати. Для цього, по-перше, він має достатньо високу кваліфікацію та необхідний фінансовий ресурс, технічне і програмне оснащення, які дозволяють йому створювати складні програмні комплекси для реалізації кібератак.

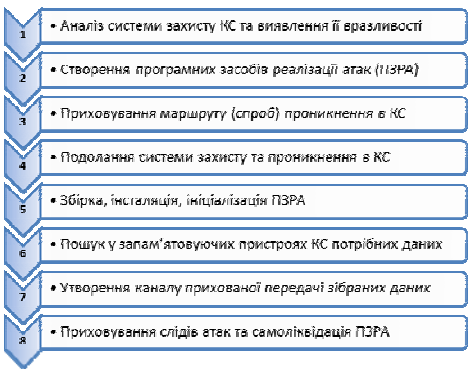
По-друге, згідно з принципом Керкхофса, він знає алгоритми функціонування засобів захисту, включаючи засоби КЗІ, але до початку атаки не знає діючих ключів. По-третє, для досягнення поставлених цілей порушник має можливість перехоплення будь якої інформації у транспортній мережі, модифікацію або створення неприпустимої команди за відносно невеликий час.

Виходячи з викладеного, можливо передбачити наступні варіанти його зловмисних дій (потенційних загроз) стосовно СУТП в цілому: 1) модифікація дійсної команди або реальної інформації про внутрішній стан системи; 2) формування та надсилання керованому об'єкту неприпустимої команди або фальшивих даних про внутрішній стан СУТП; 3) перехоплення в транспортній мережі окремих команд або частки інформації щодо внутрішніх станів задля їх вилучення; 4) крадіжка конфіденційної інформації щодо сервісів, які надаються; 5) модифікація або руйнування програмного коду СУТП.

Щодо програмних реалізацій засобів КЗІ, які використовуються в СУТП, можливо вважати, що метою дій порушника може бути: 1) зміна, знищення або крадіжка критичних параметрів CSP; 2) модифікація програмного коду (криптосхеми) засобу КЗІ.

На підставі аналізу наукових публікацій щодо реалізації кібератак у поєднанні з відомими методами криптоаналізу на основі побічних каналів [3] була сформована наступна модель кібератак в СУТП, яка включає вісім фаз активних дій порушника (рис.):

1. Розвідка. На першому етапі порушник, використовуючи всі доступні методи, здійснює приховане вивчення вразливостей комп'ютерної системи (КС), яка є технологічною базою функціонування СУТП, а також виявлення слабких місць наявної системи захисту [4].



2. Розробка. На цьому кроці, здійснюється вивчення отриманої інформації та розробка програмних засобів для реалізації атак (ПЗРА).

3. Маскування. Порушник здійснює заходи щодо усунення ознак, які пов'язують ПЗРА та спосіб його застосування з реальним розробником, та/або створює фіктивні ознаки, що ототожнюються з непричетними до кібератаки суб'єктами. Також він визначає тактику приховування реального маршруту (адрес проміжних вузлів глобальної мережі) спроб проникнення в КС.

4. Проникнення. Використовуючи створені засоби і технології, а також можливості інсайдерського впливу порушник забезпечує подолання системи захисту та проникнення ядра ПЗРА в програмне середовище КС.

5. Підготовка. Далі в автоматичному або автоматизованому режимі реалізується збирання ПЗРА з окремих модулів, його інсталяція та ініціалізація.

6. Реалізація. Ініціалізоване ПЗРА на основі певної апріорної інформації про підсистеми (елементи) КС, що виконують конкретні функції СУТП, а також про потрібні порушнику дані, зокрема, чутливі параметри безпеки криптографічних модулів SSP виявляє та ідентифікує зазначені об'єкти у запам'ятовуючих пристроях КС. У якості відповідної апріорної інформації можуть виступати розмір файлів, формати даних, певні ключові слова, програмні переривання/звернення до деяких ресурсів системи тощо. Залежно від цілей кібератаки виявлені ресурси можуть бути знищені, модифіковані або використані для розкриття конфіденційної інформації.

7. Витік. За необхідності, створюється канал прихованої передачі зібраних даних з використанням методів стеганографії, процедури стискання даних з наступним шифруванням, фізичного переносу під час підключення зовнішніх пристроїв тощо.

8. Самоліквідація. На завершальному етапі ПЗРА включає механізми самознищення та приховування слідів кібератаки. Цей етап реалізується автоматично, в разі настання в КС певних обставин (наприклад, визначеного часу), або автоматизовано на підставі отримання команди ззовні.

Література

1. Бурячок В.Л. Завдання форми та способи ведення воєн у кібернетичному просторі / В.Л.Бурячок, Г.М.Гулак, В.О.Хорошко // Науково-технічний журнал «Наука та оборона»,2011. – № 3. – С. 35-42.

2. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, в редакції Наказу Адміністрації ДССЗЗІ від 14.12.2015 № 767.

3. J. Kelsey Side Channel Cryptanalysis of Product Ciphers / J. Kelsey, B. Schneier, D. Wagner, C. Hall // 5th European Symposium on Research in Computer Security Louvain-la-Neuve, Belgium September 16–18, 1998 Proceedings, Berlin, Springer, 1998, 97-111 pp.

4. Гулак Г.М. Забезпечення безпеки засобів КЗІ у кіберпросторі / Г.М.Гулак // Матеріали науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» – Т. ІУ Сучасні технології інформаційної безпеки. – К., 2015. – С. 100-102.

ЗМІСТ

РОЗВИТОК СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЯК ПЕРЕДУМОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ УЧЕНИХ І СТУДЕНТІВ

Наукове видання

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

IX Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 30 березня 2018 року)

Електронна версія

Авторська редакція

Технічне редагування, макетування *Т. О. Коркач*

Формат 60x84/16.
Ум. друк. арк. 24,03. Обл.-вид. арк. 23,71.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 22, Київ, 03022
факс: (044)257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб'єкта видавничої справи ДК № 99 від 23.06.2000