КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.145158
УДК 004.056

Гулак Геннадій Миколайович
доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0001-9131-9233h.
hulak@kubg.edu.ua

Жданова Юлія Дмитрівна
канд. ф.-м. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Складанний Павло Миколайович
канд. тех. наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Гулак Євген Геннадійович
аспірант
Інститут проблем математичних машин і систем НАН України, м. Київ
ORCID ID: 0000-0003-4984-686X
evgeniygulak@email.com

Корнієць Віктор Анатолійович
аспірант
Інститут проблем математичних машин і систем НАН України, м. Київ
ORCID ID: 0000-0002-4967-8395
viktorkorniets@email.com

УРАЗЛИВОСТІ ШИФРУВАННЯ КОРОТКИХ ПОВІДОМЛЕНЬ В МОБІЛЬНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті розглянуто можливості реалізації атак на інформаційний обмін в мобільних інформаційно-комунікаційних системах (ІКС), що захищені за допомогою практично стійких криптографічних перетворень. Інформаційний обмін в ІКС об'єктів критичної інфраструктури нерідко реалізується шляхом передачі, прийому і оброки відносно коротких повідомлень. Такі повідомлення можуть містити формалізовані команди управління і дані про поточний стан керованих об'єктів, сигнали оповіщення, відомості про підозрілу активність в комп'ютерних мережах або вихідні дані для формування спільних секретів (ключів) в системах кіберзахисту. Для швидкого обміну відносно короткими повідомленнями широко використовуються служби коротких повідомлень (Short Message Service – SMS) або додатки на мобільних платформах – месенджери Проаналізовано останні публікації щодо захисту інформації в мобільних мережах, включаючи стійкі криптографічні перетворення. Узагальнені відомості щодо розподілу довжин коротких повідомлень в чатах на підставі чого визначені можливі атаки на криптографічні системи з метою визначення поточного стану об'єкту критичної інфраструктури та способи їхньої реалізації. Сформульовані практичні рекомендації щодо протидії визначеним атакам, а також визначені напрями подальших досліджень.

Ключові слова: стійка криптосистема, розподіл довжин повідомлень, критична інфраструктура, мобільний пристрій, криптоаналітична атака.

ВСТУП

Постановка проблеми. Інформаційний обмін в інформаційно-комунікаційних системах (ІКС) об'єктів критичної інфраструктури, включаючи комплекси керування виконавчими механізмами і обладнанням, системи інформування (циркулярного оповіщення) про надзвичайні ситуації, промислові комп'ютеризовані системи пожежної безпеки, охорони і дистанційного контролю територій та об'єктів, інформаційно-діагностичні системи в технологіях IoT та «Smart House», системи дистанційного обліку спожитих енергоресурсів та інші, часто реалізується шляхом передачі, прийому і обробки відносно коротких повідомлень.

Такі повідомлення можуть містити формалізовані команди управління і дані про поточний стан керованих об'єктів, сигнали оповіщення, відомості про підозрілу активність в комп'ютерних мережах або вихідні дані для формування спільних секретів (ключів) в системах кіберзахисту.

Аналіз останніх досліджень і публікацій. Окремо слід виділити нову критичну галузь - сферу повсюдних обчислень (*ubiquitous computing*) [1], яка останнім часом швидко розвівається та включає, зокрема, повсюдну робототехніку, що заснована на логічному поєднанні роботизованих технологій, хмарних обчислень, сенсорних систем і нейронних мереж.

При цьому досить часто виникають ситуації коли такі дані необхідно передавати та отримувати за допомогою мобільних пристроїв відповідальних посадових осіб. В певних умовах, в разі виникнення проблем із службовим зв'язком, персонал об'єктів критичної інфраструктури іноді вимушений для координації дій з ліквідації наслідків надзвичайних ситуацій використовувати незахищені комерційні системи телекомунікацій. Трагічні події останніх місяців на полях битв із окупантами, свідчать про необхідність вирішення подібних проблем з комунікаціями також і для систем бойового управління силами та засобами, хоча б на рівні підрозділів територіальної оборони, які не мають штатних засобів захищеного зв'язку.

Зазначимо, що на поточний час для швидкого обміну відносно короткими повідомленнями широко використовуються служби коротких повідомлень (Short Message Service – SMS) або додатки на мобільних платформах – месенджери. Їх застосування не потребує швидкісних каналів зв'язку або оренди виділених IP-адрес, але при цьому для SMS стандартні механізми захисту не передбачені, а механізми забезпечення безпеки месенджерів приховані за завісою комерційного «ноу-хау».

Таким чином постає актуальне питання підвищення кіберзахисту мобільних пристроїв, що взаємодіють з АС об'єктів критичної інфраструктури.

Зауважимо, що захищені інформаційні технології спеціального призначення можуть становити інтерес також ї для звичайних громадян в плані їх використання для захисту персональних даних, приватної інформації про особисте життя, реквізитів банківських карт, даних медичних обстежень тощо.

Актуальність цієї тези підтверджується результатами досліджень використання месенджера WhatsApp [2], на підставі якого можна зробити висновок, що близько 50% користувачів використовують цей месенджер не для утворення великих чатів, а для спілкування «têt à têt».

В переважної більшості наведених випадків існують реальні загрози порушення конфіденційності чутливих даних або їх підробки (несанкціонованої модифікації) з

метою порушення сталого функціонування відповідних АС та нанесення значних збитків або шкоди власнику комп'ютерної системи і, навіть, державі. Тому існує нагальна потреба аналізу методів протидії загрозам та забезпечення безпеки коротких повідомлень та визначення шляхів її розв'язання.

В науково-практичних публікаціях для забезпечення конфіденційності та цілісності такої інформації запропоновано декілька рішень, на яких зупинимось більш детально.

В [3] в рамках проекту «Defense against cyberattacks using steganogaphy techniques» спеціалістами департаменту наукових досліджень національного університету оборони Кореї проаналізовано побудову ботнет на основі відео контейнерів для стеганографічного контенту на платформах SNS (Social Network Service). Показано, що запропонована модель може бути реалізована в додатку Telegram SNS. Слід зазначити, що цей метод потребує суттєвих витрат пропускної здатності системи, зважаючи на те, що розмір контейнеру має бути досить великим, оскільки у випадку малого розміру контейнеру порівняно з довжиною повідомлення факт його приховування ефективно виявляється за допомогою методів математичної статистики.

В [4] запропоновано новий підхід для приховування факту відправлення коротких повідомлень на основі створення секретного IP-каналу. Замість шифрування повідомлення або його вбудовування в мультимедійний контейнер, як у класичній комп'ютерній стеганографії, для приховування секретного повідомлення обробляються всі повідомлення та генерується декілька IP-пакетів різних типів для переносу даних. Зауважимо, що надійне приховування факту передачі унеможливлює атаку зловмисника, що спрямована на підробку повідомлення. Також відмітимо, що запропонований метод працює виключно у випадку форматів подання у мережах пакетної передачі даних. Згадана проблема узгодження методу захисту коротких повідомлень з форматом подання даних на рівні застосувань розглядається в [5] відносно служби коротких повідомлень SMS [6,7].

Застосування методів симетричної криптографії, на відміну від стеганографічного захисту, дозволяє забезпечити конфіденційність повідомлень без збільшення навантаження на канал зв'язку, оскільки шифроване і відкрите повідомлення мають однакову довжину. Зокрема, в [8,9] міститься огляд швидких ефективних криптографічних методів забезпечення безпеки SMS і порівняльний аналіз їх швидкодії, включаючи потоковий шифр RC4, стандарти блокового шифрування DES, 3DES, Blowfish і AES. Зауважимо, що швидкість у випадку симетричного шифрування коротких повідомлень не має суттєвого значення, більшої уваги потребує аналіз криптографічних якостей.

Зокрема, запропонований до використання в [6,10] алгоритм RC4 має вразливості, які утворюють підґрунтя для проведення ефективних криптоаналітичних атак [11].

Аналогічно, виходячи з результатів криптоаналізу швидкого алгоритму потокового шифрування A5/1 [12], дослідження з його модифікації [13,14], не зважаючи на певні успіхи практичної реалізації, не можна вважати перспективними для його застосування для захисту коротких повідомлень

Стосовно запропонованих в [6,15] блокових алгоритмів 3DES і TEA, що реалізують загально відому схему Фейстеля, можливо зазначити, що їх криптографічна стійкість і достатня швидкодія реалізацій поки ще відповідають сучасним вимогам. У той же час, з урахуванням перспектив зростання потужності комп'ютерних систем, які використовуються для криптоаналітичних атак, довжина їх ключів (168 біт у 3DES і 128

біт у TEA) викликає певний сумнів щодо доцільності застосування цих алгоритмів в новітніх системах захисту.

Сучасний алгоритм симетричного шифрування AES [6] має високі криптографічні якості і швидкодію. Водночас, слід звернути увагу на те, що його застосування в режимах ECB або CBC потребує довжини короткого повідомлення кратної 64 біт, В загальному випадку довільної довжини повідомлення воно потребує розширення, Саме з метою уникнення вказаної проблеми в [16] пропонується модифікація алгоритму AES – шифр AESw – що придатний для шифрування повідомлень довжини кратної 32-бітам без розширення даних. З точки зору безпеки шифрування в режимі ECB ця модифікація викликає сумнів, зважаючи на те, що максимальне значення порядку будь-якої точки векторного простору суттєво зменшується:

$$\left(AESw(\bar{x})\right)^n = \bar{x}, \qquad \bar{x} \in V_2^{32} \Rightarrow n \le 2^{32},$$

$$\left(AES(\bar{x})\right)^n = \bar{x}, \qquad \bar{x} \in V_2^{64} \Rightarrow n \le 2^{64}.$$

Запропонована в [17] для шифрування коротких повідомлень комбінація симетричного шифру Віжинера і криптосистеми з відкритими ключами RSA не містить обґрунтування щодо безпеки її застосування. Більш ефективним уявляється запропонована в [18] побудова шифру багато алфавітної заміни з псевдо випадковою управляючою послідовністю.

Слід мати на увазі, що підчас передачі по каналам зв'язку пакети даних можуть бути піддані атакам, внаслідок чого їх відхилить шифратор, а це може призведе до часткового блокування функцій АС. Для уникнення подібної ситуації в [19] запропоновано метод на основі кодів сімейства Ріда-Соломона, який забезпечить доставку коротких важливих повідомлень при дотриманні балансу швидкості обслуговування (SOS) і пропускної здатності мережі. При цьому для забезпечення доставки відповідно до вимог SOS додається мінімальна кількість надлишкових пакетів. За висновками цього дослідження зроблено висновок, що навіть в умовах кібератак важливі повідомлення, такі, як сигнал тривоги постачаються своєчасно по захищеній завдяки шифруванню безпровідної мережі.

Асиметричні шифри (криптосистеми з відкритим ключем) використовуються для вирішення різних задач кіберзахисту, а саме: управління сеансовими ключами симетричних криптосистем, автентифікації, формування і перевірки цифрових підписів. При цьому слід згадати, що в асиметричних системах результат шифрування звичайно обчислюється по модулю деякого великого простого числа, тому запис результатів в двійковому вигляді може мати довжину бітового запису цього числа.

Це означає, що довжина результату зашифрування відносно короткого двійкового числа порядку 2^8 за допомогою асиметричної криптосистеми може досягати кількох тисяч бітів, а саме: для класичних алгоритмів RSA або Диффі-Хеллмана довжина шифротексту може становити до 2048 біт і більше.

В [20] на основі криптосхеми ЄльГамаля запропоноване компактне асиметричне шифрування безпечне щодо атак з обраним шифрованим текстом [21]. Нагадаємо, що схема шифрування ЄльГамаля з відкритим ключем працює в групі G простого порядка q с генератором $g \in G$. Для секретного навмання вибраного елемента $x \in \mathbb{Z}_q$ обчислюється відкритий ключ $y = g^x$. Якщо H – криптографічна стійка хеш-функція, тоді процедура шифрування відкритого повідомлення задається рівнянням:

$$c = m \oplus H(y^r), r \in \mathbb{Z}_q.$$

Відмітимо, що: 1) в запропонованій схемі випадкове значення r використовується одноразово після чого знищується; 2) довжина відкритого і шифрованого повідомлень визначається розміром дайджеста, що утворюється функцією хешування.

Фактично ж, отримувачу надсилається кортеж $\langle z, c \rangle$, де $z = g^r$, який розшифровується:

$$m = c \oplus H(z^x), \text{тому як } z^x = g^{rx} = y^r.$$

Також слід зазначити, що в сучасних умовах для уникнення реалізації в даної схемі атак за методом «грубої сили» порядок випадкового числа, що найменш, має бути

$$r \sim 2^{64} \approx 10^{19}.$$

Змістовна інформація щодо безпеки застосування асиметричних криптосистем для шифрування відносно коротких повідомлень, за суттю під якими маються на увазі сеансові ключі для симетричних шифрів, надана в дослідженні [22] і стандарті [23].

У загальному випадку для безпечного зашифрування будь якого повідомлення за допомогою асиметричних криптосистем необхідно мати сертифікат відкритого ключа, а це може бути у цілому ряді випадків суцільною проблемою.

Вирішенню вказаної проблеми може сприяти використання методу шифрування, що оснований на ідентифікації користувача [24] – *IBE* (*Identity Based Broadcast Encryption*). В [25] запропонована повнофункціональна схема *IBE*, в якій безпека зашифрованого повідомлення в моделі випадкового оракула заснована на обчислювальної складності в задачі Діффі-Хеллмана та використанні білінійних карт між групами. Прикладом такого відображення є спарювання Вейля на еліптичних кривих.

Інша проблема асиметричних шифрів, як відмічене в [26], полягає в площині можливого довготривалого застосування секретного (приватного) ключа. У випадку компрометації цього ключа розшифрування всіх повідомлень, які зашифровані за допомогою відповідного відкритого ключа та перехоплені зловмисником раніше. Це стосується також і майбутніх повідомлень, якщо не будуть вжиті заходи щодо зміни ключової пари. Саме тому для підвищення безпеки інформаційного обміну у вказаній статті запропонований протокол, що забезпечує можливість використання пар приватний – публічний ключ протягом певного короткого терміну.

Загалом, підсумовуючи огляд систем кіберзахисту на мобільних пристроях можливо зробити висновок про недостатню увагу питанням уразливості відповідних криптосистем, що обумовлені особливостями інформаційних потоків.

Мета статті. Метою пропонованої статті є висвітлення питань, пов’язаних з уразливістю систем кіберзахисту на мобільних пристроях

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розподіл довжин повідомлень в чатах

Спочатку уявляється доцільним з’ясувати зміст поняття, яке винесено у назву статті, а саме: що вважати коротким повідомленням (КП) і у чому полягають особливості захисту КП в кіберпросторі? Зважаючи на певні обмеження в плані доступу до відомостей про обмін інформацією (трафік) і заходи щодо її захисту в приватних та державних комунікаційних системах наше дослідження базується виключно на офіційних джерелах та науково-практичних публікаціях.

На поточний час соціальні мережі в Інтернеті дозволяють швидко обмінюватися текстом, зображеннями, аудіо- та відеофайлами. В кіберпросторі поширюється використання месенджерів (зокрема, WhatsApp, Viber, Telegram, Signal) різними суспільними і професійними групами, включаючи чати територіальних громад, державних і комунальних установ, професійних об'єднань, навчальних груп, власників багатоквартирних будинків тощо.

В чатах, у випадках, що не суперечать законодавству, відбувається голосування з різних питань, включаючи організаційні, фінансові, господарські тощо, а також приймаються певні рішення і надаються відповідні доручення. За необхідності обмеження доступу до окремих питань доручення адресуються безпосередньо виконавцю. Перелічені факти свідчать про певний управлінський аспект застосування чатів в суспільстві. А це дає логічні підстави для застосування результатів досліджень таких систем в інтересах вирішення поставленої задачі – оцінки довжини таких повідомлень.

Зокрема, на підставі результатів оцінки довжини повідомлень в рамках демографічних досліджень, що отримані в [2, 27], створена діаграма (рис. 1), з якої неважко бачити, що з ймовірністю більше 0,95 довжина повідомлень в досліджуваних чатах WhatsApp не перевищувала 100 символів (літер) англійської мови.

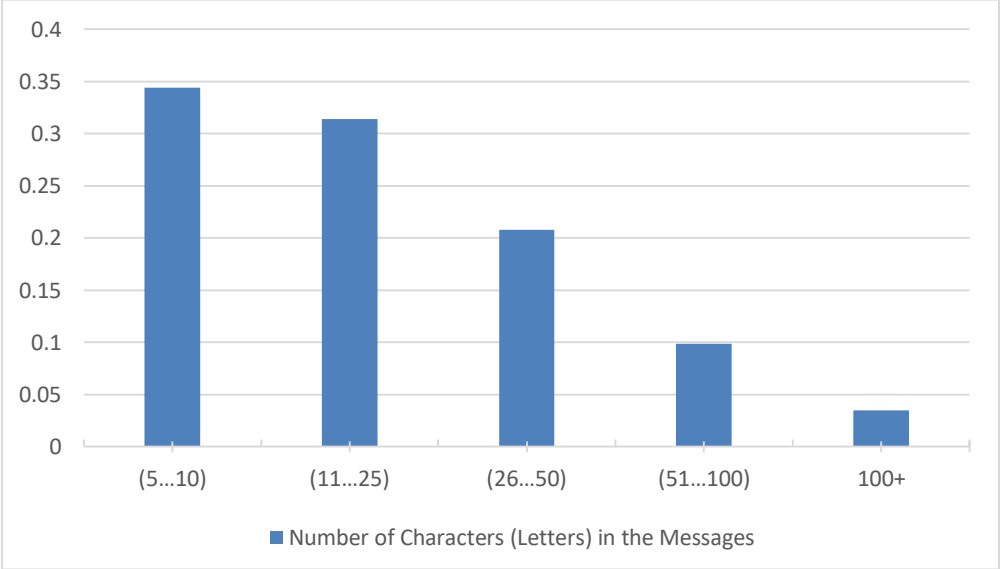

Рис. 1. Розподіл ймовірностей довжин повідомлень англійської мови в чатах месенджера WhatsApp

Зазначимо, що в цьому випадку вихідні дані щодо розподілу довжин в чаті були наведені авторами досліджень у словах досліджуваної мови. Підчас перерахунку в діаграмі рис. 1, використана оцінка середньої довжини слова англійської мови в 5 букв [28]. Водночас відмітимо, що середня довжина слова російський мові сягає 6-7 букв, тобто різниця з англійською мовою становить порядку 20 відсотків.

Виходячи з наведених в [29] даних про автоматизований переклад повідомлень в чатах (пост або коментар до нього) в мішаних кодах (мови хінді + англійська) можливо побудувати дещо іншу діаграму (рис. 2). При цьому використана типова процедура перетворення даних статистичного спостереження в гістограму [30].

Коментуючи цю діаграму, слід відмітити, що можлива зміна мови і тематики досліджуваних постів і коментарів вплинула на їх розподіл довжин повідомлень. Зокрема, мода розподілу зсунулася вбік довжин з інтервалу (51,100), а також з ймовірністю більше 0.96 довжина навмання обраного повідомлення належить інтервалу (1,150). Інші довжини спостерігаються з ймовірністю меншою за 0,04.

Слід звернути увагу, що в [29] наведені дані щодо розподілу довжин повідомлень (речень) після їх коректного перекладу на англійську мову, при цьому візуально суттєвої різниці не спостерігається. Надати математичну оцінку цьому факту не вдалося внаслідок різних інтервалів спостережень, а також відсутності точних числових даних спостереження та обсягу вибірки.

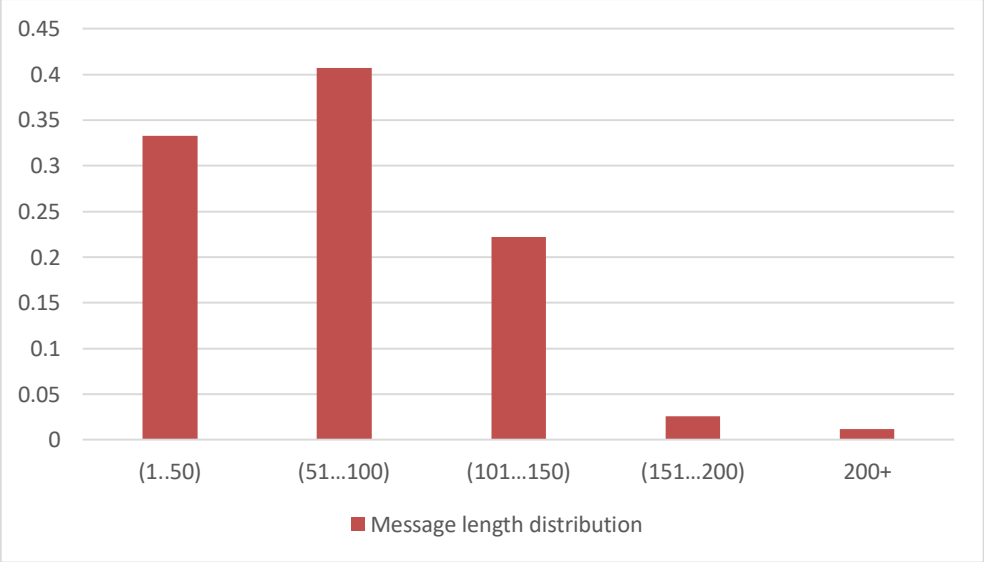

Рис. 2. Розподіл довжин повідомлень в індійських чатах

Слід звернути увагу, що результати двох незалежних досліджень [2,27] та [29], які переслідували різні цілі в різних галузях знань, надали достатньо близькі за суттю результати.

Якщо в зазначених роботах вивчались виключно емпіричні результати, то в [31] і [32] були визначені гіпотези щодо розподілу довжин повідомлень, що становить окремий науковий інтерес. Зважаючи на те, що дослідження в [32] стосується невідомого нам характеристик інформаційного обміну в рамках Центру зарубіжних комунікаційних послуг (Бомбей, Індія) залишимо ці результати для вивчення і аналізу у подальшому.

Щодо результатів в [31] відмітимо, що авторами перевірено гіпотезу відносно розподілу довжин повідомлень в соціальних мережах згідно логнормальному закону, а саме факту, що функція розподілу має вигляд:

$$f_{LN}(L) = \frac{1}{\sqrt{2\pi\sigma}}\frac{1}{L}exp(-(\ln(L)-\mu)^2/2\sigma^2), \qquad (1)$$

де L – це довжина коментаря, а μ та σ – змінні параметри. Цей розподіл має моду $c = \exp(\mu-\sigma^2)$, середнє $\bar{f} = \exp(\mu+\frac{\sigma^2}{2})$ та медіану $m = \exp(\mu)$.

У підсумку дослідження відмічений хороший збіг теоретичних і практичних даних для відносно великих значень довжини повідомлень і дещо гірший результат отриманий для коротких повідомлень.

В нашому випадку становить інтерес саме питання відносно максимальних довжин, тому відмітимо, що максимальне значення функції розподілу довжин за даними в [31] для форуму BBC (*British Broadcasting Corporation*) і польських форумів досягається приблизно для 60 байт, але внаслідок великого значення дисперсії σ^2 середня довжина повідомлення для форуму BBC і польського форуму ставлять 434 і 257 байтів відповідно. Якщо порівнювати ці результати з даними на діаграмах рис.1 і рис. 2 можливо висунути гіпотезу, що збільшення довжин повідомлень у цьому випадку скоріш за все обумовлене політичною та культурологічною тематикою інформаційного обміну, яка потребує в чаті більш розгорнутого доведення власних думок учасників дискусій.

Крім того, в [31] для довжини повідомлень у веб ресурсах YouTube та MySpace отримані оцінки середніх значень 104 і 124 байти відповідно.

Звернемо також увагу, що стандартна довжина інформаційної частини SMS становить 1120 біт [6,7], що надає можливість передати в одному повідомленні до 160 символів англомовного повідомлення, або до 70 символів у випадку використання в якості алфавіту кирилиці. SMS більшої довжини для передачі поділяються на частини.

Підсумовуючи вище викладене, в разі використання в службових цілях в якості інформаційно-комунікаційних платформ короткими доцільно вважати повідомлення довжиною до 150 байтів (до 1200 біт).

Атаки на захищений обмін з метою розпізнавання стану об'єкту

Нехай шифроване повідомлення $C = E(M, K)$ створене за допомогою криптографічного перетворення E з відкритого повідомлення M довжини $|M|$ допомогою ключа K. В загальному випадку метою проведення атак на криптографічну систему може бути часткове дешифрування повідомлення, безключове розкриття повідомлення або розкриття одночасно повідомлення і ключу. В випадку практично стійкого криптографічного перетворення, безпечної реалізації та безпомилкового застосування засобу шифрування зазначені цілі недосяжні.

В той самий час, переважна більшість сучасних систем потокового і блокового шифрування, призначених для забезпечення конфіденційності даних в ІКС, не змінюють довжини файлів у результаті їх шифрування. Для таких систем $|C| = |M|$.

Несуттєвим доповненням довжини файлу можуть бути декілька байтів вектору ініціалізації або посилання на діючий комплект ключів шифрування. Внаслідок цього, розподіл частот зустрічаємості довжин шифрованих повідомлень буде або повністю співпадати з відповідним розподілом відкритих повідомлень (рис. 1, 2), або несуттєво відрізнятися. Останній факт створює потенційну загрозу для реалізації атак на систему захисту.

Нехай H – деякий стан об'єкта критичної інфраструктури, M – повідомлення. Якщо умовна ймовірність $P(H/M) \neq P(H)$, то повідомлення M будемо називати характеристичним для стану H.

Нехай невідомі $M_{H1}, \dots, M_{Hk}$ є характеристичними повідомленнями для стану H, а серед множини шифрованих повідомлень $\mathcal{C} = \{C_i, i = 1,2, \dots\}$ є, зокрема, зашифровані характеристичні повідомлення. Якщо існує поліноміальний алгоритм $\mathcal{A}$, який дозволяє з використанням множини $\mathcal{C}$ оцінити умовну ймовірність $P(H/\mathcal{C})$ стану H, тоді будемо говорити про потенційну загрозу атаки на захищений обмін з метою розпізнавання стану об'єкту на основі зашифрованих повідомлень.

Звернемо увагу на те, що часткове дешифрування може розглядатись як загроза вказаної атаки.

Внаслідок специфіки інформаційного обміну в рамках окремих об'єктів згідно змін розподілу довжин повідомлень без застосування процедур криптоаналізу можна виділити наступні варіанти оцінювання змін станів:

1. Оцінювання різниці середньої довжини повідомлень в звичайному стані L_{mid} та середньої довжини повідомлень в стані H: L_{midH}, при цьому в разі незміни стану виконується нерівність Чебишова:

$$P(|L_{midH} - L_{mid}| \geq t) \leq \frac{\sigma^2}{t^2}.$$

Більш точна оцінка може бути отримана з використанням логнормального розподілу довжин повідомлень, що заданий рівнянням (1).

2. Враховуючи, що внаслідок усереднення довжини може втрачатись суттєва інформація про застосування в ІКС характеристичних повідомлень, для розпізнавання зміни стану об'єкту може бути застосована статистика χ^2 узгодження Пірсона, а саме:

$$\chi^2 = \sum_{i=L_{min}}^{L_{max}} \frac{(\mu_{iH} - \mu_i)^2}{\mu_i},$$

де $\{\mu_i,\ i = \overline{L_{min}, L_{max}}\}$ – сукупність частот довжин повідомлень від мінімальної (L_{min}) до максимальної (L_{max}), $\{\mu_{iH},\ i = \overline{L_{min}, L_{max}}\}$ – сукупність частот довжин повідомлення відносно яких висувається гіпотеза про перехід досліджуваного об'єкту до стану H. Вказана гіпотеза відхиляється, якщо розраховане значення статистики перевищує значення квантиля з відповідним рівнем надійності.

Протидіяти реалізації відповідних атак можливо шляхом:

- зміни випадковим чином довжин відкритих повідомлень до початку їх шифрування шляхом їх дроблення на частини;
- надсилання випадковим чином фіктивних повідомлень з спеціально обраним розподілом їх довжин;
- обрання однакової (максимальної) довжини всіх повідомлень;
- використання створення захищених VPN з'єднань.

Кожен з варіантів має власні переваги та недоліки, тому доцільність їх застосування може бути визначена в конкретних умовах функціонування ІКС.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведений огляд наукових публікацій із захисту коротких повідомлень та узагальнення даних досліджень розподілу довжин коротких повідомлень в чатах сучасних комунікаційних додатків надалі дасть можливість визначити потенційну ймовірність проведення зловмисником атак на мобільні захищені ІКС об'єктів критичної інфраструктури з метою визначення стану цих об'єктів, а також сформулювати рекомендації по протидії їх реалізації.

За рамками статті залишилось питання дослідження умов проведення таких атак та оцінки їх ефективності. Саме на цих питаннях уявляється доцільним у подальшому сфокусувати увагу, а також на методах підвищення захищеності месенджерів мобільних пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Alomair, B., Poovendran, R. (2014). Efficient Authentication for Mobile and Pervasive Computing. *IEEE Transactions on Mobile Computing*, *13*(3), 469–481. https://doi.org/10.1109/tmc.2012.252

2 Rosenfeld, A., Sina, S., Sarne, D., Avidov, O., Kraus, S. (2018). WhatsApp usage patterns and prediction of demographic characteristics without access to message content. *Demographic Research*, *39*, 647–670. https://doi.org/10.4054/demres.2018.39.22.

3 Kwak, M., Cho, Y. (2021). A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger. *Symmetry*, *13*(1), 84. https://doi.org/10.3390/sym13010084.

4 Trabelsi, Z., El-Sayed, H., Frikha, L., Rabie, T. (2006). Traceroute Based IP Channel for Sending Hidden Short Messages. In *Advances in Information and Computer Security* (с. 421–436). Springer Berlin Heidelberg. https://doi.org/10.1007/11908739_30.

5 Zhang, T., Jin, Y. C., Sun, Z. X. (2015). A Lightweight Encoding Mechanism for Encrypted User Notification on Mobile Device in Power Grid System. In *International Conference on Computer Information Systems and Industrial Applications*. Atlantis Press. https://doi.org/10.2991/cisia-15.2015.140.

6 GSM 03.38 (ETSI 300 628): Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information.

7 GSM 03.40 (ETS 300 536): European digital cellular telecommunication system (Phase 2); Technical realization of the Short Message Service (SMS) Point to Point (PP).

8 Karale, S. N., Pendke, K., Dahiwale, P. (2015). The survey of various techniques & algorithms for SMS security. In *2015 International Conference on Innovations in Information,Embedded and Communication Systems (ICIIECS)*. IEEE. https://doi.org/10.1109/iciiecs.2015.7192943.

9 Makala, R., Bezawada, V., Ponnaboyina, R. (2017). A fast encryption and compression technique on SMS data. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE. https://doi.org/10.1109/wispnet.2017.8299956.

10 Aung, T. M., Myint, K. H., Hla, N. N. (2018). A Data Confidentiality Approach to SMS on Android. In *Intelligent Computing & Optimization* (с. 505–514). Springer International Publishing. https://doi.org/10.1007/978-3-030-00979-3_53

11 Attacking SSL when using RC4 // *Hacker Intelligence Initiative*, March 2015/ Imperva. 10P. https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

12 Ekdahl, P., Johansson, T. (2003). Another attack on A5/1. *IEEE Transactions on Information Theory*, *49*(1), 284–289. https://doi.org/10.1109/tit.2002.806129

13 Pan, J., Ding, Q., Qi, N. (2012). The Research of Chaos-based SMS Encryption in Mobile Phone. In *2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC)*. IEEE. https://doi.org/10.1109/imccc.2012.124

14 Pan Jing, Qi Na, Xue Bing-Bing Ding Qun. (2012). Field programmable gate array-based chaotic encryption system design and hardware realization of cell phone short message. *Acta Physica Sinica*, *61*(18), 180504. https://doi.org/10.7498/aps.61.180504

15 Novelan, M. S., Husein, A. M., Harahap, M., Aisyah, S. (2018). SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. *Journal of Physics: Conference Series*, *1007*, 012037. https://doi.org/10.1088/1742-6596/1007/1/012037

16 Lu, E.H., Huang, K.T., Chiu, J.H. (2016). Word-Based AES Encryption Without Data Expansion. *Journal of Information Science and Engineering*, *32*(4), 849-861.

17 Ahamed, B. B., Krishnamoorthy, M. (2020). SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm. *Journal of the Operations Research Society of China*. https://doi.org/10.1007/s40305-020-00320-x

18 Гулак, Г.М., Складанний, П.М. (2017). Забезпечення гарантоздатності автоматизованих систем управління та передачі даних безпілотних літальних апаратів. *Математичні машини та системи*, 3, 154 161.

19 Grushevsky, Y., Elmasry, G., Argentieri, S., Lussier, R. (2006). Adaptive RS Code for Message Delivery Over Encrypted Military Wireless Networks. In *MILCOM 2006*. IEEE. https://doi.org/10.1109/milcom.2006.302323.

20 Asbullah, M.A, Ariffin, M.K. A Proposed CCA-secure Encryption on an ElGamal Variant. 2012 7th International Conference on Computing and Convergence Technology (ICCCT2012), 499-503.

21 Гулак, Г.М., Мухачов, В.А., Хорошко, В.О., Яремчук, Ю.Є. (2011). Основи криптографічного захисту інформації. ВНТУ.

22 Bresson, E; Chevassut, O. Pointcheval, D. New security results on encrypted key exchange. 7th International Workshop on Theory and Practice in Public Key Cryptography 2004 | Public Key Cryptography - PKC 2004, Proceedings 2947, 45-158
23 (IEEE Std 1363-2000) IEEE Standard Specifications for Public-Key Cryptography.
24 Mishra, P. Renuka, Verma, V. (2020). Identity Based Broadcast Encryption Scheme with Shorter Decryption Keys for Open Networks. *Wireless Personal Communications, 115*(2), 961-969
25 Boneh, D. Franklin, M.·(2003) Identity-Based Encryption from the Weil Pairing. *SIAM J. of Computing, 32*(3), 586-615
26 Schneier, B., Hall, C. An improved e-mail security protocol. In *13th Annual Computer Security Applications Conference*. IEEE Comput. Soc. https://doi.org/10.1109/csac.1997.646194
27 Rosenfeld, A. Sina, S. Sarne, D. Avidov, O. Kraus, S. WhatsApp Usage Patterns and Prediction Models. https://www.researchgate.net/publication/299487660
28 Jaglom, A.M., Jaglom, I.M. (2007). Probability and information.
29 Srivastava, V., Singh, M. (2020). PHINC: A Parallel Hinglish Social Media Code-Mixed Corpus for Machine Translation. In *Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020)*. Association for Computational Linguistics. https://doi.org/10.18653/v1/2020.wnut-1.7
30 Cramér, H. (1999). *Mathematical Methods of Statistics. Princeton Landmarks in Mathematics*. Princeton University Press.
31 Sobkowicz, P., Thelwall, M., Buckley, K., Paltoglou, G., Sobkowicz, A. (2013). Lognormal distributions of user post lengths in Internet discussions - a consequence of the Weber-Fechner law? *EPJ Data Science, 2* (1). https://www.researchgate.net/publication/257868097_Lognormal_distributions_of_user_post_lengths_in_Internet_discussions_-_a_consequence_of_the_Weber-Fechner_law
32 Kekre, H.B., Saxena, C.L. (1979). An estimate of the distribution of message lengths in overseas communications. *Computers & Electrical Engineering*, 6(2), 79-92.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Hennadii M. Hulak
Doctor of Technical Sciences, Associate Professor,
Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCIDID: 0000-0001-9131-9233h.
hulak@kubg.edu.ua

Yuliia D. Zhdanova
PhD, Associate Professor, Associate Professor of the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Pavlo M. Skladannyi
PhD, Associate Professor, Head of the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Yevhen H. Hulak
postgraduate
Institute of Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine, Kyiv
ORCID ID 0000-0003-4984-686X
evgeniygulak@email.com

Viktor A. Korniiets
postgraduate
Institute of Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine, Kyiv
ORCID ID 0000-0002-4967-8395
viktorkorniets@email.com

VULNERABILITIES OF SHORT MESSAGE ENCRYPTION IN MOBILE INFORMATION AND COMMUNICATION SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS

Abstract. The article considers the possibility of implementing attacks on information exchange in mobile information and communication systems (ICS), which are protected for additional practical cryptographic transformations. Information exchange in the ICS of critical infrastructure objects is often implemented by means of transmission, receiving and paying fees of apparently short notices. Such improvements can be used to formalize control commands and data on the flow mill of objects, alert signals, alerts about suspected activity in computer networks or data for the formation of multiple secrets (keys) in cyber defense systems. Short message services (Short Message Service - SMS) or add-ons on mobile platforms - messengers are analyzed for the exchange of apparently short notifications. Informed about the possibility of an attack on cryptographic systems with a method of designating a streaming station, the object of critical infrastructure and methods of its implementation. Formulated practical recommendations about how to prevent significant attacks, as well as direct further charges.

Keywords: strong cryptosystem, message length distribution, critical infrastructure, mobile device, cryptanalytic attack.

REFERENCES

1 Alomair, B., Poovendran, R. (2014). Efficient Authentication for Mobile and Pervasive Computing. *IEEE Transactions on Mobile Computing*, *13*(3), 469–481. https://doi.org/10.1109/tmc.2012.252

2 Rosenfeld, A., Sina, S., Sarne, D., Avidov, O., Kraus, S. (2018). WhatsApp usage patterns and prediction of demographic characteristics without access to message content. *Demographic Research*, *39*, 647–670. https://doi.org/10.4054/demres.2018.39.22.

3 Kwak, M., Cho, Y. (2021). A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger. *Symmetry*, *13*(1), 84. https://doi.org/10.3390/sym13010084.

4 Trabelsi, Z., El-Sayed, H., Frikha, L., Rabie, T. (2006). Traceroute Based IP Channel for Sending Hidden Short Messages. In *Advances in Information and Computer Security* (c. 421–436). Springer Berlin Heidelberg. https://doi.org/10.1007/11908739_30.

5 Zhang, T., Jin, Y. C., Sun, Z. X. (2015). A Lightweight Encoding Mechanism for Encrypted User Notification on Mobile Device in Power Grid System. In *International Conference on Computer Information Systems and Industrial Applications*. Atlantis Press. https://doi.org/10.2991/cisia-15.2015.140.

6 GSM 03.38 (ETSI 300 628): Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information.

7 GSM 03.40 (ETS 300 536): European digital cellular telecommunication system (Phase 2); Technical realization of the Short Message Service (SMS) Point to Point (PP).

8 Karale, S. N., Pendke, K., Dahiwale, P. (2015). The survey of various techniques & algorithms for SMS security. In *2015 International Conference on Innovations in Information,Embedded and Communication Systems (ICIIECS)*. IEEE. https://doi.org/10.1109/iciiecs.2015.7192943.

9 Makala, R., Bezawada, V., Ponnaboyina, R. (2017). A fast encryption and compression technique on SMS data. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE. https://doi.org/10.1109/wispnet.2017.8299956.

10 Aung, T. M., Myint, K. H., Hla, N. N. (2018). A Data Confidentiality Approach to SMS on Android. In *Intelligent Computing & Optimization* (c. 505–514). Springer International Publishing. https://doi.org/10.1007/978-3-030-00979-3_53

11 Attacking SSL when using RC4 // *Hacker Intelligence Initiative*, March 2015/ Imperva. 10P. https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

12 Ekdahl, P., Johansson, T. (2003). Another attack on A5/1. *IEEE Transactions on Information Theory*, *49*(1), 284–289. https://doi.org/10.1109/tit.2002.806129

13 Pan, J., Ding, Q., Qi, N. (2012). The Research of Chaos-based SMS Encryption in Mobile Phone. In *2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC)*. IEEE. https://doi.org/10.1109/imccc.2012.124

14 Pan Jing, Qi Na, Xue Bing-Bing Ding Qun. (2012). Field programmable gate array-based chaotic encryption system design and hardware realization of cell phone short message. *Acta Physica Sinica*, *61*(18), 180504. https://doi.org/10.7498/aps.61.180504

15 Novelan, M. S., Husein, A. M., Harahap, M., Aisyah, S. (2018). SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. *Journal of Physics: Conference Series*, *1007*, 012037. https://doi.org/10.1088/1742-6596/1007/1/012037

16 Lu, E.H., Huang, K.T., Chiu, J.H. (2016). Word-Based AES Encryption Without Data Expansion. *Journal of Information Science and Engineering*, *32*(4), 849-861.

17 Ahamed, B. B., Krishnamoorthy, M. (2020). SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm. *Journal of the Operations Research Society of China*. https://doi.org/10.1007/s40305-020-00320-x

18 Hulak, H.M., Skladannyi, P.M. (2017). Zabezpechennia harantozdatnosti avtomatyzovanykh system upravlinnia ta peredachi danykh bezpilotnykh litalnykh aparativ. Matematychni mashyny ta systemy, 3, 154-161.

19 Grushevsky, Y., Elmasry, G., Argentieri, S., Lussier, R. (2006). Adaptive RS Code for Message Delivery Over Encrypted Military Wireless Networks. In *MILCOM 2006*. IEEE. https://doi.org/10.1109/milcom.2006.302323.

20 Asbullah, M.A, Ariffin, M.K. A Proposed CCA-secure Encryption on an ElGamal Variant. 2012 7th International Conference on Computing and Convergence Technology (ICCCT2012), 499-503.

21 Hulak, H.M., Mukhachov, V.A., Khoroshko, V.O., Yaremchuk, Yu.Ie. (2011). Osnovy kryptohrafichnoho zakhystu informatsii. VNTU.

22 Bresson, E; Chevassut, O. Pointcheval, D. New security results on encrypted key exchange. 7th International Workshop on Theory and Practice in Public Key Cryptography 2004 | Public Key Cryptography - PKC 2004, Proceedings 2947, 45-158
23 (IEEE Std 1363-2000) IEEE Standard Specifications for Public-Key Cryptography.
24 Mishra, P. Renuka, Verma, V. (2020). Identity Based Broadcast Encryption Scheme with Shorter Decryption Keys for Open Networks. *Wireless Personal Communications, 115*(2), 961-969
25 Boneh, D. Franklin, M.·(2003) Identity-Based Encryption from the Weil Pairing. *SIAM J. of Computing, 32*(3), 586-615
26 Schneier, B., Hall, C. An improved e-mail security protocol. In *13th Annual Computer Security Applications Conference*. IEEE Comput. Soc. https://doi.org/10.1109/csac.1997.646194
27 Rosenfeld, A. Sina, S. Sarne, D. Avidov, O. Kraus, S. WhatsApp Usage Patterns and Prediction Models. https://www.researchgate.net/publication/299487660
28 Jaglom, A.M., Jaglom, I.M. (2007). Probability and information.
29 Srivastava, V., Singh, M. (2020). PHINC: A Parallel Hinglish Social Media Code-Mixed Corpus for Machine Translation. In *Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020)*. Association for Computational Linguistics. https://doi.org/10.18653/v1/2020.wnut-1.7
30 Cramér, H. (1999). *Mathematical Methods of Statistics. Princeton Landmarks in Mathematics*. Princeton University Press.
31 Sobkowicz, P., Thelwall, M., Buckley, K., Paltoglou, G., Sobkowicz, A. (2013). Lognormal distributions of user post lengths in Internet discussions - a consequence of the Weber-Fechner law? *EPJ Data Science, 2* (1). https://www.researchgate.net/publication/257868097_Lognormal_distributions_of_user_post_lengths_in_Internet_discussions_-_a_consequence_of_the_Weber-Fechner_law
32 Kekre, H.B., Saxena, C.L. (1979). An estimate of the distribution of message lengths in overseas communications. *Computers & Electrical Engineering*, 6(2), 79-92.