МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Черкаський національний університет
імені Богдана Хмельницького
Черкаський інститут банківської справи
Чорноморський державний університет імені Петра Могили

Всеукраїнська науково-практична
Інтернет-конференція

Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку

11-21 березня 2021 року

м. Черкаси

При шифруванні повідомлення M перетворюється в ціле число m так, щоб $0 \leq m < n$ за допомогою узгодженого оберненого протоколу. Зашифрований текст c формується через використання відкритого ключа e за допомогою рівняння:

$$c = m^e \,(mod\, n). \quad (1)$$

Для розшифрування повідомлення m використовується рівність:

$$m = c^d \,(mod\, n) \quad (2)$$

Після шифрування повідомлення його потрібно сховати в контейнер – зображення. Суть методу LSB (Least Significant Bits) полягає в приховуванні інформації шляхом зміни останніх бітів зображення, які кодують колір на біти приховуваного повідомлення. Нижче наведений приклад (рис. 2) показує, як повідомлення може бути приховано в перших восьми байтах, що відносяться до трьох пікселів 24-бітного зображення.

```
Pixels: (00100111 11101001 11001000)
        (00100111 11001000 11101001)
        (11001000 00100111 11101001)
A: 01000001
Result: (00100110 11101001 11001000)
        (00100110 11001000 11101000)
        (11001000 00100111 11101001)
```

Рис.2. Приклад роботи методу LSB

Список використаних джерел

1. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А.Ю. Пузиренко. – М: МК-Пресс, 2006 .– С. 315–318.

Слюсарь І.І., к.т.н., доцент
Полтавська державна аграрна академія, Полтава

МЕХАНІЗМИ ЗАХИСТУ УНІФІКОВАНИХ КОМУНІКАЦІЙ

Одною з основних складових уніфікованих комунікацій (Unified Communications, UC) є IP-телефонія [1]. Вона може реалізовуватись на базі програмних IP-АТС або хмарних рішень на їхній основі. При реалізації корпоративних інформаційних систем [2], іноді, не

приділяють необхідної уваги захисту VoIP від зловмисників. На сьогодні, слід виділити кілька основних зовнішніх впливів.

1. Перехоплення телефонних розмов. Що стосується IP-телефонії, то зловмиснику не обов'язково мати фізичний доступ до локальної мережі. Основне джерело небезпеки – Інтернет. Виходячи з цього, переговори, які проводять співробітники компанії між собою та із клієнтами можуть бути джерелом для витоку корпоративної інформації.

2. Відмова в обслуговуванні. Також для злому телефонної системи або для виводу її з ладу може використовуватись flood-трафік. Цьому явищу характерні затримки передачі та прийому корисного голосового трафіка, та/або відсутність фрагментів мови співрозмовника. Крім цього, зломщики можуть відправляти на АТС велику кількість підроблених запитів на телефонне обслуговування. Подібні дії спричиняють надмірне навантаження на IP АТС, і вона не в змозі обслуговувати запити, що надходять від справжніх абонентів.

3. Злом системи для здійснення дзвінків. Це найпоширеніша причина атак на АТС. Вона ж є й самою дорогою для власника телефонії. Він базується на підборі параметрів викликів. Зловмисник знаходить помилки в конфігураціях телефонії. Після цього він має можливість здійснювати дзвінки. У підсумку, компанія одержує рахунок із кругленькою сумою, яку необхідно виплатити провайдеру послуг.

Для протидії цим негативним чинникам в найбільш відомих системах на базі IP-АТС FreePBX (Asterisk) [3] і 3CX [1] реалізовано кілька механізмів: застосування технологій шифрування для захищеної передачі голосових пакетів; правильна організація мережної топології; забезпечення контрольованого доступу. Їхню деталізацію можна розглянути на аналізі 3CX.

1. Захист телефонних розмов. 3CX містить наступні інструменти по безпеці телефонних переговорів і шифруванні голосового трафіку: SIP TLS – шифрований протокол обміну сигнальним трафіком; SIP SRTP – безпечний протокол обміну голосом; WebRTC SSL – безпечний метод для організації робочого місця у веб-браузері; 3CX-Tunel – вбудований в 3CX-клієнти пропістарний протокол, що забезпечує шифрування в 3CX iOS, Adnroid, Windows-софтфон; 3CX SBC Tunel – вбудований в 3CX SBC протокол, що забезпечує шифрування

віддалених пристроїв, підключених через 3CX SBC. Слід зазначити, що в рекомендованих 3CX IP-телефонах, може використовуватися комбінація TLS + SRTP. Все це знижує ймовірність прослуховування розмов, навіть у випадку перехоплення мережного трафіку. З іншого боку, при організації веб-конференцій на основі технології WebRTC через VPN можливе визначення публічної IP-адреси.

2. Захист від несанкціонованого підключення. Будь-яка редакція 3CX містить наступний набір функціоналу для власної безпеки IP-АТС: білий список IP-адрес, з яких дозволений доступ в інтерфейс адміністратора; обмеження підключення SIP-пристроїв без використання шифрування з публічних мереж; Обмеження роботи без використання 3CX Tunel; чорний список IP-адрес, у тому числі «глобальний» список від 3CX з відомими зловмисниками; алгоритм захисту підключень від «підозрілих» SIP User Agent; алгоритм захисту від перебору паролів і автоматичного блокування на 24 год.; алгоритм безпечних паролів користувачів, що не дозволяє використовувати прості та короткі паролі.

3. Захист міжнародних дзвінків передбачає: вбудований механізм «що не дозволене явно, те заборонене»; закриті за-замовчанням міжнародні дзвінки; коди всіх країн миру з можливість відкриття напрямку для певних груп користувачів.

4. Внутрішня безпека містить: заборону записи розмов вибіркових користувачів або груп користувачів; права доступу до записів розмов на основі групових політик безпеки; керування «видимістю» співробітників на основі групових політик безпеки.

Таким чином, компетентне використання розглянутих рішень дозволить підвищити рівень безпеки корпоративних інформаційних систем.

Список використаних джерел

1. URL: https://unified.com.ua.
2. Слюсарь І.І., Слюсар В.І., Дегтярьова Л.М., Курчанов В.М. Інструментарій віддаленого доступу до ресурсів інформаційних управляючих систем. Проблеми інформатизації: тези доп. 8-ої міжнародної науково-технічної конференції (Черкаси – Харків – Баку – Бельсько-Бяла, 26-27 лис. 2020 р.). Черкаси, 2020. Т. 3. С. 43.
3. URL: https://www.freepbx.org.