надійності продукції, що випускається;

- реєстрацію подій;
- обмеження, контроль і облік доступу;
- архівацію й резервування, використання для цього надійних засобів зберігання даних;
- тестування й перевірку програмного забезпечення на стійкість до збоїв;
- резервне живлення.

Отже, істотне збільшення використання бездротових мереж призвело до розробки механізмів безпеки, які спочатку були подолані зловмисниками, тому необхідне комплексне рішення для захисту мережі. Для цього доцільно впровадити технологію WPA2 в усіх типах бездротових мереж з використанням методології, яка включає в себе: створення пароля, створення плану забезпечення безпеки і захисту програмного забезпечення, що дозволяє більшу складність і безпеку бездротової мережі.[2]

Список використаних джерел

1. Матеріали V Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій – Тернопіль 17-18 листопада 2016 [Електронний ресурс] – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/20131/2/ConfATMT_2016vII_Kovalenko_V_S-Methods_of_protecting_wireless_53.pdf

2. Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв [Електронний ресурс] – http://ena.lp.edu.ua/bitstream/ntb/21459/1/36-192-197.

УДК 004.056.5

АНАЛІЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕФОННИХ МЕРЕЖАХ

Васильєва С. П., студ. гр КБ-161
Науковий керівник: **Гур'єв В. І.,** к.т.н., доцент
Національний університет «Чернігівська політехніка»

На даний момент до складу телекомунікаційних систем входять телефонні мережі, основою яких є телефонні станції. Сучасні телефонні станції за архітектурою схожі на комп'ютери й сервери. Тому захисту мереж телефонного зв'язку необхідно приділити не менше уваги, ніж забезпечення безпеки комп'ютерних мереж.

Телефонні мережі являють собою сукупність кінцевих пристроїв (терміналів) телефонних станцій, ліній і каналів телефонної мережі, транзитних вузлів комутації.

Об'єкти телефонної мережі (АТС, телефонні апарати) можуть піддаватися таким атакам:

- несанкціонований доступ до програмних портів АТС;
- несанкціоноване використання послуг телефонних переговорів.

Несанкціонований доступ до програмних портів АТС. Джерелом загрози є зовнішній порушник і програмно-апаратна закладка. Засоби поширення – електромагнітні хвилі, радіоефір та наведення в провідниках, що виходять за межі контрольованої зони. Загроза реалізується через активацію закладок в програмному забезпеченні телефонних станцій за допомогою використання спеціалізованого цифрового термінала. Внаслідок такого несанкціонованого доступу може відбутися порушення конфіденційності або цілісності. Наприклад, замаскована передача даних з телефонної бази по службовому каналу, прослуховування переговорів абонентів або повне блокування роботи телефонної станції.

Несанкціоноване використання послуг телефонних переговорів. Джерело загрози – зовнішній порушник. Поширюється шляхом використання сервісної функції DISA, яка дозволяє забезпечити прямий доступ віддалених користувачів до їх внутрішніх сервісних послуг. Зловмисник здійснює з'єднання з номером УВАТС (установчої виробничої АТС)

організації, на якій відкрито сервіс DISA. Мовний інформатор видає голосове привітання і запит на введення додаткового номера внутрішнього абонента. Замість додаткового номера проводиться набір міжміського / міжнародного номера. Наслідок – УВАТС встановлює транзитне міжміське / міжнародне з'єднання, причому, рахунки за дзвінки будуть приходити організації, що володіє телефонною станцією.

Характер походження загроз поділяється на 3 типи: антропогенний (кримінальні структури, окремі фізичні особи та персонал), техногенний (злам в ліній і каналів передачі даних, недостатня захищеність апаратури передачі даних і несанкціоноване підключення до лінії зв'язку), а також природний (стихійні лиха). Основними причинами витоку інформації є недотримання персоналом норм, вимог, правил експлуатації АС, що функціонують в рамках АТС, помилки в проектуванні систем захисту програмного забезпечення мережі АТС і отримання інформації, що захищається розвідками.

Для здійснення захисту інформації телефонної мережі необхідна реалізація таких вимог:

— мінімальна кількість декларованих можливостей (закладок) програмного забезпечення телефонної станції;

— використання аутентифікації користувачів для доступу до програмного забезпечення телефонних станцій;

— моніторинг ліній і каналів зв'язку на наявність розривів, за якими може здійснюватися несанкціонований з'їм інформації, що передається;

— відсутність в телефонному обладнанні абонентів апаратних закладок.

На рівень захисту інформації впливають такі фактори:

— Ступінь секретності – висока, оскільки по лініях телефонного зв'язку може передаватися інформація, що має високу державну, комерційну або іншу важливість.

— Обсяг – високий, через те, що по лініях телефонного зв'язку передається найбільший обсяг переданої інформації, в порівнянні з іншими способами комунікації.

— Інтенсивність обробки – висока, бо високий обсяг переданої інформації, а також частота передачі інформації.

Отже, необхідно забезпечувати високий ступінь захисту інформації, що передається по лініях телефонного зв'язку.

Для забезпечення захисту інформації, яка проходить по телефонних лініям та каналам зв'язку можна використовувати такі технічні засоби, призначені для захисту окремого приймального пристрою: фільтр «Граніт-8», приглушувач мобільних телефонів «Жезл» та блокатор мобільних телефонів «Завіса».

Фільтр «Граніт-8» призначений для забезпечення захисту мовної інформації від витоку шляхом акустоелектричних перетворень через двопровідні лінії: відкриті телефонні мережі, мережі радіотрансляції, системи директорського та диспетчерського зв'язку. Призначення фільтру – пропускати сигнали в мовному діапазоні частот при нормальному режимі роботи телефонної лінії та затримувати високочастотні сигнали, які подаються в лінію при високочастотному нав'язуванні.

Приглушувач мобільних телефонів «Жезл» використовується для блокування несанкціонованої роботи мобільних телефонів, що працюють в наступних стандартах: CDMA-450, GSM-900, GSM-1800, 3G (UMTS-2100).

Блокатор мобільних телефонів «Завіса» призначений для блокування несанкціонованої роботи мобільних телефонів, що працюють в наступних стандартах: GSM-900, GSM-1800, DAMPS, CDMA DAMPS, CDMA-2000. Блокування здійснюється одночасно у всіх піддіапазонах перерахованих вище стандартів, що значно збільшує ймовірність блокування.

Список використаних джерел

1. Климчук В. Інформаційні технології та тенденції розвитку міжнародної інформації [Текст] / В.Климчук // Вісн. Кн. Палати.– 2006.–№6.– С.15-18.

2. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посібник / Кормич Б. А. – К. : Кондор, 2004.

3. Александр Зайцев, Роман Мещеряков Технические средства и методы защиты информации. - 7 изд. Горячая линия-Телеком, 2012.

УДК 004.056.5

ЗАГРОЗА ЗМІНИ ВМІСТУ БУФЕРУ ОБМІНУ ЗА ДОПОМОГОЮ PASTEJACKING

Бойко К. В., студ. гр КБ-161,
Ткач Ю. М., д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Зазвичай, дія ***копіювати*** і ***вставити*** - це дуже проста дія, яку може виконати будь-який користувач, але час від часу веб браузер може не дозволити користувачеві копіювати і вставляти текст з певних веб-сайтів. Крім того, браузер може навіть не дати вибрати вміст з веб-сторінки, таким чином обмеживши можливість копіювання користувача.

Це може стати досить проблематичним, особливо якщо цільовим користувачеві потрібні великі шматки тексту з сайту для дослідницьких цілей.

Майже всі веб-браузери дозволяють веб-сайтам виконувати JavaScript команди на комп'ютерах користувачів для виконання обчислень інтерфейсу і бізнес логіки веб додатків. Ця функція може дозволити шкідливим веб-сайтам захопити буфер обміну користувача комп’ютера. Тобто, коли ви щось копіюєте і вставляєте його у буфер обміну, веб-сайт може запустити одну або кілька команд за допомогою вашого браузера. Метод може бути використаний для зміни вмісту буфера обміну для виконання атаки в операційній системі користувача.

Веб-сайти виконують команди, коли користувач виконує якусь дію, - наприклад, під час натискання певної клавіші або клацання правою кнопкою миші. Коли ви натискаєте CTRL + C на клавіатурі, він запускає режим командування веб-сайту. Після невеликого очікування, скажімо, 800 мс, він вставляє щось шкідливе у ваш буфер обміну. Очікування користувача такі, що після використання CTRL + V для вставки оригінального тексту, який було скопійовано, але замість нього буде вставлено те, що було потрібно зловмиснику. Деякі веб-сайти можуть відстежувати CTRL + V і використовувати його для запуску команди, яка змінює вміст буфера обміну.

Pastejacking - це метод, який шкідливі веб-сайти використовують для того, щоб взяти під контроль буфер обміну вашого комп'ютера і змінити його вміст на щось "шкідливе" без вашого відома.

Більш того, таким чином ви можете вставити контент прямо в консоль, наприклад в PowerShell або вікно командного рядка, і тоді може виконатися шкідлива команда. Користувачі *Mac* мають деяку безпеку, якщо вони використовують iTerm. Це емуляція, яка дозволяє користувачам Mac замінити консоль за замовчуванням. При використанні iTerm він запитує користувачів, чи дійсно вони хочуть вставити щось, що містить символ «нового рядка». Потім користувачі можуть вибрати «Так» або «Ні» в залежності від того, що вони роблять.

Символ нового рядка це фактично половина клавіші Enter. Клавіша Enter зображена, як правило, стрілкою, яка здається починається від верхньої лінії до нижньої, а потім вліво. Клавіша Enter являє собою комбінацію символу нового рядка (перехід до наступного рядка) і повернення (читається як «повернення каретки в крайнє ліве положення x, 0», як в друкарських машинках). Коли ви натискаєте клавішу Enter, виконується будь-яка команда в цьому рядку консолі. Але це може залежати від консолі, щоб запросити підтвердження.

У більшості випадків, в командному рядку Windows не вимагається підтвердження на виконання команд. Рядок запитує підтвердження тільки в тому випадку, якщо ви