4. Основы технической диагностики. *П.П. Пархоменко, В.В. Карибекий, Е.С. Соломонян, В.Ф. Холчёв.* М.: Энергия, 1976

Поступила 12.01.2009р.

УДК 621.3

Ю.-Ю.М.Коростіль, С.О.Нікулін

МОЖЛИВОСТІ СУЧАСНИХ ТЕХНОЛОГІЙ ПРИ РОЗВ'ЯЗКУ ЗАДАЧ ЗАХИСТУ ДОСТУПУ

Захист система доступу в мережі Інтернет є однією з основних проблем забезпечення безпечного функціонування користувачів та окремих систем, що зв'язані з мережею. Це обумовлюється тим, що використання обчислювальних ресурсів, використання інформаційних ресурсів, управління об'єктами та інші задачі, розв'язок яких передбачає використання комп'ютерних мереж є неможливим без реалізації системи доступу. Особливо важливі проблеми захисту доступу у комп'ютерних мережах викликало у зв'язку з розвитком комерційних Інтернет систем. До таких систем відносяться наступні:

- інтернет-магазини,
- інтернет-системи, що орієнтовані на різні сфери бізнесової діяльності, до яких можна віднести такі системи як B2B, P2P, B2C та інші,
- діяльність в галузі Інтернет реклами,
- в галузі надання послуг громадянам держави між установами та ін.

Системи доступу в більшості випадків розглядаються як системи віддаленого доступу, коли об'єкт доступу і користувач, який відповідний доступ ініціює є територіально рознесені. Тому в подальшому будемо мати на увазі віддалений доступ. Системи доступу і відповідні методи захисту таких систем можна класифікувати на основі різних підходів, наприклад, на основі способів реалізації процесів віддаленого доступу, на основі типу послуг, або задач, які передбачається розв'язувати з використання віддаленого доступу, на основі систем, що мають певну функціональну орієнтацію в рамках такої системи, якщо можливості віддаленого доступу є територіально рознесені. Тому в подальшому будемо мати віддалений доступ. Системи доступу є відповідні методи захисту таких систем можна класифікувати на основі різних підходів, наприклад, на основі способів реалізації процесів віддаленого доступу на основі типу послуг або задач, які передбачається розв'язувати з використання віддаленого доступу на основі

систем, що мають певну функціональну орієнтацію і в рамках доступу є відповідною характеристикою цієї орієнтації можна класифікувати систему віддаленого доступу і т. д. Тому приведемо класифікацію відповідних систем, не тримаючи якоїсь, однієї ознаки. Прикладом такої класифікації можуть служити методи захисту, що використовується у відповідних системах:

- системи доступу користувачів до ресурсів чи послуг комп'ютерної системи на основі паролів та ключів,
- системи доступу до веб-серверів, що використовують віртуальні приватні канали зв'язку,
- системи, що використовують віртуальні приватні канали зв'язку, які прийнято називати VNP-системи,
- системи, що використовують криптографічні протоколи аут ідентифікації,
- системи доступу, що побудовані на основі використання засобів мобільного зв'язку,
- системи доступу, що використовують для захисту окремі технології.

Найбільш поширеними, і, відповідно, найбільш простими, з точки зору організації захисту, є системи доступу, що використовують паролі, ключі, додаткові етикетки та ідентифікатори, кожний з видів використовується для цього типу засобів захисту і характеризується стійкістю до окремих видів атак [1]. По відношенню до такої стійкості розглянемо різні способи аутентифікації. В даному випадку тип стійкості системи доступу будемо спів ставляти з типом атак, по відношенню до якої відповідний спосіб захисту є стійким. В даному випадку розглядаються атаки, що полягають у спробах несанкціонованого доступу до ресурсів. В переважній більшості, такі атаки реалізуються шляхом не уповноваженого захоплення пароля доступу. Спосіб захисту доступу перед атакою, що полягає у пасивному перехопленні пароля ґрунтується на використанні системою захисту хеш-функції для перетворення коду пароля у закодований вигляд і передачі по відкритому каналу в закодованому вигляді. В цьому випадку пароль, що передається по каналу зв'язку запишеться у вигляді g=h(p), де g — закритий код пароля з допомогою хеш-функції h. В системі захисту, що знаходиться на прийомній стороні використовується база даних, що вміщає значення паролів у перетвореному хеш-функцією вигляді. Ідентифікація користувача проводиться на основі порівняння, яке знаходиться в базі даних з g, що передано по каналу зв'язку. Схема такого з'єднання записується у вигляді: A→[id, g] →B(Id, g'). В цьому випадку несанкціонований користувач може сформулювати таблицю паролів і по такій таблиці може виконувати спроби відгадування паролів.

Спосіб, що утруднює такий тип атаки полягає у використанні, крім пароля, ідентифікатора для формування захищеного коду аутентифікації користувача. Формально це записується у вигляді:

$$A\ [id, g= h\ (pxid)] \rightarrow B(Id, g'), \qquad (1.1).$$

де p — відкритий код пароля, id — ідентифікатор користувача, g — закритий код пароля, що знаходиться в системі захисту. В цьому випадку несанкціонований користувач (NK) може заволодіти базою паролів, і це призведе до компрометації SZ, а відповідна атака називається компрометацією. Спосіб, що протидіє такій атаці, полягає в тому, що закриття пароля здійснюється на стороні SZ, по каналу p передається відкритим способом. Формально це записується у вигляді:

$$A[id, g] \rightarrow B[\ g=h(p_1 x\ id, g'), \qquad (1.2)$$

В цьому випадку база даних, в якій знаходяться g, може бути прочитана, що дозволить здійснити несанкціонований доступ до ресурсів системи. Для протидії цій атаці використовується наступна схема аут ідентифікації користувача, що формально описується наступною схемою:

$$A\ [id, h_1(pxid)] \rightarrow B\ [r'=h_2(gxid), (r=r^1)], \qquad (1.3)$$

В цій схемі, на відміну від схеми 1.2 на стороні SZ g перетворюється функцією h2, а в базі даних SZ зберігаються значення r. В рамках цієї схеми в SZ існує база фондованих паролей, доступ до якої може бути зламаний. Для протидії такій можливості використовується наступна схема організації доступу до ресурсів:

$$A[(g=h_1(p*id)] \rightarrow r=h_3(g*t),\ id, t] \rightarrow B[r'=h_2(g'*t),(r'=r)], \qquad (1.4)$$

Де t — представляє собою випадкове число, що генерується на стороні A кожний раз при ініціації зв'язку, або представляє собою одиницю часу. На стороні B в базі даних зберігається g, який відповідає g, що формується в A. Найбільш ефективними, з точки зору забезпечення високого рівня захисту являються одноразові паролі, які можна формувати різними способами:

- сформувати тільки для A і B списки випадкових паролів та забезпечити подвійний спосіб синхронізації вибору від подвійних паролів однією та другою стороною,
- на основі використання генераторів випадкових чисел з однаковими для двох сторін початковим станом відповідного псевдо випадкового генератора,
- на основі використання механізмів часових етикеток.
- з використанням системи єдиного часу.

Реалізація одного з таких способів формально може бути описана такою схемою:

$$A[((g'=h_1(k*p))\rightarrow(r=h_3(g*k*t))) id] \rightarrow B[id, g, k, r'=h_2(g*k*t)], \qquad (1.5)$$

де k — персональний ключ, який на стороні A використовується у вигляді апаратно реалізованого ключа. Інший спосіб реалізації ідей одноразових паролей можемо описати наступними співвідношеннями. Випадковим чином генеруємо число r для параметра n=const. Обраховуємо величину ω_0 по формулі:

$$\omega_0= h(h(\ldots h(\omega_n)\ldots)),$$

Де h(x) — функція хешування, яку повторюємо r разів при r<n. В цьому випадку ω_0, n і d передаємо стороні B. Система захисту ці параметри зберігає

в базі даних. Якщо необхідно здійснити новий сеанс зв'язку, то n=r зменшуємо необхідну і обраховуємо ω_1 по формулі:

$$\omega_1 = h(h(\ldots h(\omega_n)\ldots)),$$

і передаємо ω_1 і n-1 стороні В. Кожний раз сторона А буде використовувати новий пароль з послідовності $\omega_1,\ldots, \omega_k$, де k<n. Завдяки чому можна реалізувати k сеансів зв'язку. Приведені вище методи аутентифікації реалізуються однією передачею даних від А до В. Підвищити в рамках підходу рівень захищеності доступу можна шляхом збільшення операцій обміну між А і В. Прикладом такого методу може служити метод, що називається «зошит-відповідь». На першому етапі користувач пересилає в SD свій логін. У відповідь на ідентифікований поділ сторона В пересилає стороні А псевдо випадкове число С. Після цього сторона реалізує кінцеву форму запиту з використання числа С, яке вислала сторона В. Формульно така схема може бути описана у вигляді:

1. $A[id,] \rightarrow B[((id) \rightarrow C)] \rightarrow A$
2. $A[((g=h_1(p*id)) \rightarrow r=h_3(g*C))),\ id] \rightarrow B[r'=h_2(C*g'),(r'=r)]$

Розширення методу підвищення рівня захисту системи доступу за рахунок збільшення операцій обміну в процесі аут ідентифікації являється використанням криптографічних протоколів аут ідентифікації. Типовим представником такого типу протоколів являється протокол Діджі-Хеллмана, що використовує неспецифічні шифри [2]. По суті, процес аутентифікації забезпечується тим, що дві сторони одержують можливість обмінятися таємними ключами, які в майбутньому можна використати для реалізації процедури захищеного обміну інформацією. Тому алгоритм Діджі-Хеллмана називають алгоритмом безпечного обміну ключами шифрування. Алгоритм реалізації цього протоколу полягає в наступному.

1. Вибираються два відкриті числа g і α, де g — просте число, α — корінь g такий, що α^x mool g є простими числами в діапазоні від одного до
2. Користувач А вибирає випадкове число X^a< g, і обчислюється $Ya=\alpha^x$ mool g і зберігає Ха в таємниці. Користувач вибирає випадкове число Хв<g, і обчислює $Ув=\alpha^{хв}$ mool g і зберігає Хв в таємниці.
3. Число Уа сторона А передає стороні В, а сторона В передає число В стороні А.
4. Сторона А обчислює таємний ключ К по формулі: $K=(Ya)^{Хв}$ mool g, що в подальшому дозволяє стороні А і В обмінюватися інформацією, яку можна шифрувати таємним ключем К, що відомий тільки для А.

В цьому полягає аут ідентифікація двох сторін обміну. Веб-сервери досить широко використовуються в бізнесі як засоби відображення рекламних даних про продукцію, про надання послуг. Тому будь-які несанкціоновані втручання у веб-сервери можуть призвести до значних втрат. Один із способів несанкціонованого втручання у веб-сервер ґрунтується на використанні потоків даних, що адресуються відповідно до

серверу. Такі потоки даних можуть ініціюватися довільним користувачем веб-сервера, який виявив бажання ознайомитися з рекламною інформацією, що на ньому розміщається. Більш небезпечною є ситуація, коли веб-сервер використовують для реалізації інтернет-магазину, який приймає участь у трансакціях, пов'язаних з придбанням у інтернет-магазині товарів і т.д. В цьому випадку необхідно захищати відповідні трансакції, що адресуються до веб-серверів. Існує декілька підходів для захисту даних на цих серверах. До таких підходів можна віднести:

- захист трансакцій на мережному рівні,
- захист на транспортному рівні,
- захист на прикладному рівні.

Захист на мережному рівні реалізується На основі використання протоколу IPSec. Цей протокол є видимим для кінцевого користувача. Крім того, він забезпечує універсальність розв'язку задачі захисту. Захист на транспортному рівні полягає в тому, що засоби захисту розміщуються відразу ж над протоколом TCP. Для захисту веб-сервера на транспортному рівні розроблено протокол SSL або нова версія цього стандарту TLS. Архітектура протоколу SSL включає протоколи встановлення зв'язку, протокол зміни параметрів шифрування н а протокол повідомлення. Базовим елементом цього протоколу являється протокол запису SSL. Цей протокол забезпечує конфіденційність при визначенні спільного ключа шифрування для сервера і користувача та цілісність повідомлення, яка забезпечується використанням спільного ключа для обчислення значення MAK. Загальна схема роботи протоколу запису складається з наступних кроків її реалізації:

1. Протокол, отримавши повідомлення для відправки, фрагментує дані, розбиваючи їх на блоки необхідних розмірів. Розмір таких блоків не більший ніж 214 байт.
2. Кожен фрагмент може компресуватися. Така компресія не повинна приводити до втрат може приводити до збільшення розміру блоку не більше ніж1024 байт. В алгоритмі TLS компресія не використовується.
3. Обраховується код ідентичності повідомлення або значення MAC складається з наступних етапів, реалізація яких може мати різні варіанти.
    a. За допомогою хеш-функції перетворюють повідомлення в його скрут H(M).
    b. За допомогою ключа K шифрується H (M) у відповідності із співвідношенням MAC=F[K, H(M)].
4. Обрахований MAC додається до повідомлення M.
5. Повідомлення (M*MAC) шифрується симетричним шифром. При шифруванні довжина блока не повинна збільшитися більше ніж на 1024.
6. Завершується робота протоколу SSL створенням заголовка, який

складається з таких полів:

- тип протоколу, який повинен обробляти інший фрагмент,
- номер версії протоколу SSL, який використовується,
- додатковий номер версії протоколу SSL,
- довжина стиснутого фрагмента.

Крім протоколу SSL, широко використовується протокол SET для захисту трансакції за допомогою пластичних карток. Для захисту доступу на самі трансакції інформації до об'єкту доступу є надзвичайно важливим, оскільки для взаємодії між сторонами, в якості середовища, через яке відповідний обмін інформацією здійснюється, являється мережа Інтернет. Одним з перспективних засобів відповідної трансакції є створення віртуального приватного тунелю між двома сторонами, що зацікавлені у створенні зв'язку. Суть такого каналу, який прийнято називати каналом VPN полягає в тому, щоб інформацію, включаючи службові поля розмістити в середині нового пакету, який став аналогом зовнішнього конверта, в який поміщається конверт з інформацією, що укривається [4]. Щоб забезпечити конфіденційність даних, що передаються, відправник шифрує вихідний пакет, упаковує його в зовнішній пакет з новим IP-заголовком відправляє його по транзитній мережі.

Найбільш поширеним стандартним протоколом тунелю являється протокол PPTP. Пакети, що передаються в рамках сесії PPTP мають наступну структуру:

- заголовок канального рівня,
- заголовок IP,
- заголовок загального методу інкапсуляції для маршрутизації GRE,
- вихідний пакет PPP, що включає пакет IPX.

В рамках цього протоколу проводиться аут ідентифікація віддаленого користувача та шифрування інформації, що передається. Згідно з стандартами PPTP, аут ідентифікація віддаленого користувача проводиться на основі наступних протоколів:

- протоколу розпізнавання пароля PAP,
- протоколу розпізнавання при потискуванні руки CHAP.

Перший тип протоколу досить детально розглядався вище. Другий тип протоколу передбачає виконання двох кроків:

- виклик,
- відповідь.

Після другого кроку підтверджується з'єднання або відмовляється в повторному з'єднанні віддаленому користувачеві. Для реалізації VPN необхідно сформувати сторонам, що передбачають обмінюватися даними по VPN цілим рядом даних, які необхідні для коректного встановлення відповідного зв'язку. До таких даних відносяться:

- IP-адреса отримувача
- протокол безпеки

- таємні ключі
- метод форматування
- індекс захисту параметрів

Всі перераховані дані формують санкції безпеки, які є необхідними компонентами для довжелезного тунельного каналу. Розвиток системи мобільного зв'язку та розвиток засобів зв'язку привели до інтенсивного проникнення системи мобільного зв'язку в сферу комп'ютерних мереж. Ця обставина призвела до розширення проблем забезпечення безпеки в комп'ютерних мережах. В рамках мобільних мереж проблеми забезпечення безпеки розв'язуються. І тому коротко зупинимося на методах забезпечення безпеки в мобільних мережах. Основні цілі безпеки, проти яких використовуються засоби захисту, полягають у порушенні ідентифікації та конфіденційності. Для протидії відповідним цілям використовується протокол IS-41-[45]. В рамках цього протоколу виконуються п'ять операцій, що забезпечують протидію відповідним атакам. До цих операцій відносяться:

- процедури перевірки реєстрації рухомого пристрою
- процедури виклик/відповідь,
- перевірка місцеположення рухомого пристрою,
- оновлення секретних даних, що розподіляються (SSD).

Процедура реєстрації починається передачею мережею повідомлення про ідентифікацію, в якому вказується, що рухомий пристрій відправив в мережу обраховане значення, що визначене алгоритмом ідентифікації. Рухомий пристрій здійснює обрахунок AUTHR і відправляє в мережу частину випадкового числа RAND, яке визначається RANDC, електронний серійний номер ESI, ідентифікаційний номер рухомого пристрою MIN1 і результат COUNT-s-p, який може використовуватися центром аут ідентифікації АС системи GSM разом із RAND для аутентифікації рухомого пристрою. Наступна в часі подія полягає в тому що АС передається отримана від рухомого складу інформація. Після аут ідентифікації пристрою АС мережа відправляє у пристрій результат ідентифікації і тим самим визнає або не визнає рухомий пристрій легальним. Процедура виклик-відповідь також призначена для ідентифікації рухомого складу пристрою і відрізняється від процедури ідентифікації реєстрації тим, що мережа виконує обчислення та відправку виклику. По-друге, якщо ідентифікація реєстрації не вдалась, то може бути ініційована операція виклик/відповідь. По-третє, значення RAND, що використовуються для ідентифікації реєстрації рухомого пристрою, пересилається всім рухомим пристроям і періодично поновлюється мережею. Ідентифікація дзвінка від рухомого пристрою ініціалізується цим пристроєм шляхом генерації AUTHU, але замість значення MIN1, як у процедурі ідентифікації і реєстрації використовуються останні шість цифр номера, що набирається. Пристрій пересилає в мережу AUTHO разом з RANDC та COUNT-s-p.

Оновлення SSD — це операція по завершенню конфіденційності. Коли

мережа створює SSD, то відправляє з пристрою повідомлення за допомогою RANDSSD з вказівкою про оновлення SSD. Пристрій на основі ключа К, що зберігається в мережі і пристрої ESN і RANDSSD. Після цього пристрій пересилає мережі, використовуючи випадкове RANDBS. Після цього прилад генерує OUHTBS на основі RANDSSD і нового SSD-A. Цю процедуру виконує мережа. Генероване AUTHBS передає у пристрій. Пристрій порівнює AUTHBS отримана з мережі зі своїм, і у випадку їх рівності передає в мережу підтвердження про оновлення SSD.

Перевірка місцеположення рухомого прикладу переважно використовується як окрема послуга локалізації. І для її надання використовуються наступні методи:

- метод, що використовує вимірювання напрямів радіосигналів
- метод, що використовує вимірювання рівнів сигналу,
- метод, що використовує час розповсюдження сигналу,
- метод, що використовує вимірювання різниці часу розповсюдження сигналу,
- кореляційні методи, що використовують бази даних результатів різних вимірювань,
- методи, що ґрунтуються GPS.

При забезпеченні безпеки функціонування спеціалізованих комп'ютерних систем вимоги до необхідного рівня безпеки системи можуть вимагати більш складних методів забезпечення безпеки, ніж ті методи, що використовуються в комп'ютерних мережах та системах. У цьому випадку необхідно використовувати спеціальні технології забезпечення безпеки системи. Такі технології виникають на основі модифікації та розвитку відомих методів та відповідних засобів, використання яких на практиці дало можливість отримати експериментальні дані про їх ефективність та рівень захисту, який вони забезпечують. Технологія забезпечення безпеки спеціалізованої комп'ютерної системи відрізняється від методів захисту, що широко використовуються в комп'ютерних системах зв'язку цілим рядом факторів. Один з важливих факторів, який визначає таку різницю, полягає в наступному. Технологія забезпечення безпеки інформаційної системи використовує в комплексі цілий ряд методів і засобів захисту в залежності від ситуації, що складається на об'єкті захисту. Другим важливим фактором являється оцінка реального рівня безпеки системи, яким забезпечується текучий момент функціонування. Третім важливим фактором, що відрізняє технологію захисту від методу захисту, являється те, що в рамках технології захисту завжди передбачається активна протидія небезпекам, що ініціюють атаки по відношенню до об'єкту захисту. Прикладом такої технології може бути технологія RONEYPOT.

1. *Чмора А.Л.* Современная прикладная криптография. – М.: Гелиос АРВ, 2002.
2. *Смарт Н.* Криптография. – М.: Техносфера, 2005.
3. *Мас-Клар С., Шах Ш.* Хакинг в Web: атаки и защита. – М.: Издательский дом

«Вильямс», 2003.
4. *Ибе О.* Сети и удаленный доступ. Протоколы, проблемы, решения. – М.: ДМК Пресс, 2002.
5. *Ирвин Дж.*, *Харль Д.* Передача данных в сетях: инженерный подход. – СПб.: БХВ-Петербург, 2003.

Поступила 19.01.2009р.

УДК 681.785.45

А.С. Ляпандра, Я.Г. Притуляк, ТНЕУ, Тернопіль
Р.О. Корж, національний університет «Львівська політехніка», Львів

ОЦІНКА ПОХИБОК ПЕРЕТВОРЕННЯ ХЕМІЛЮМІНЕСЦЕНТНОГО СИГНАЛУ ТА ЇХ МІНІМІЗАЦІЯ

Annotation: in the article the analysis of informing is conducted to the chemiluminescent signal and the ways of its increase are set.

Вступ

Хемілюмінесцентний (ХЛ) сигнал несе відомості про антиоксидантні властивості біопроби [1] на основі процесів, котрі проходять на атомарному рівні. Наявність шумів та похибок знижує інформативну властивість ХЛ-сигналу, що приводить до зменшення його діагностичної здатності [2]. Похибки перетворення ХЛ-сигналу, які виникають в процесі первинного та вторинного опрацювання сигналу, вносять вагомий вклад у загальну його похибку. Тому їх аналіз з метою мінімізації впливу на точність вимірювання є актуальною науково-практичною задачею.

Аналіз похибок перетворення хемілюмінесцентного сигналу

З метою проведення аналізу похибок перетворення ХЛ-сигналу відобразимо компоненти похибок контролю. Запишемо сигнал на виході сенсора – фотоелектронного помножувача (ФЕП):

$$u_{вих} = \gamma \overline{A}(x,y) + u_m + u_{\frac{1}{f}} + u_{кв}, \qquad (1)$$

де γ – функція, яка визначає залежність корисного сигналу від його параметрів ; $\overline{A}(x,y)$ – параметр вимірювального ХЛ-сигналу; u_m – напруга внутрішніх термошумів ФЕП; $u_{\frac{1}{f}}$ – напруга низькочастотних шумів з розподілом $\frac{1}{f}$; $u_{кв}$ – шуми квантування.

