– здійснює аудит операційної системи.

– Загальні способи обходу IDS

– Нестандартна фрагментація пакетів на рівнях IP, TCP або, наприклад, DCERPC, з якої IDS часом не здатна впоратися.

– Пакети з прикордонними або некоректними значеннями TTL або MTU також можуть оброблятися IDS некоректно.

– Неоднозначність сприйняття накладаються TCP-фрагментів (номерів TCP SYN) може трактуватися IDS інакше, ніж на сервері або клієнта, якому цей TCP-трафік призначався.

– Підставний пакет TCP FIN, наприклад з невірною контрольною сумою (т. Н. TCP un-sync), може бути сприйнятий як кінець сесії замість ігнорування.[5]

Вирішити ці проблеми можливо за рахунок повної бази сигнатур, що порівнюють пакети даних з сигнатурами відомих атак, а також обладнання, яке може аналізувати потік вхідних даних.

Проте, головна задача IDS полягає у виявленні та реєстрації атак, а також сповіщення при спрацьовуванні певного правила і покладатися лише на неї не можна.

Підводячи підсумок, можна зазначити що системи виявлення вторгнень це ефективний інструмент захисту користувача від різного роду несанкціонованих атак, проте не варто забувати, що якщо ми говоримо про повноцінну безпеки, IDS - всього лише елемент даної системи. Повноцінна безпека це: політика безпеки інтрамережі; система захисту хостів; мережевий аудит; захист на базі маршрутизаторів; міжмережевий екран; система виявлення вторгнень;політика реагування на виявлені атаки. І тільки правильно поєднуючи всі перераховані вище типи захисту, користувач може бути спокійний за безпеку зберігання і передачі важливих даних.

Список використаних джерел

1. IDS [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/IDS.
2. Что такое IDS? [Електронний ресурс] – Режим доступу до ресурсу: https://elhow.ru/kompjutery/kompjuternye-terminologii/chto-takoe-ids.
3. Системы обнаружения атак [Електронний ресурс] – Режим доступу до ресурсу: https://www.bytemag.ru/articles/detail.php?ID=6608.
4. Рубан І. В. Класифікація методів виявлення аномалій в інформаційних системах [Електронний ресурс] / І. В. Рубан, В. О. Мартовицький, С. О. Партика. – 2016. – Режим доступу до ресурсу: www.hups.mil.gov.ua/periodic-app/.../soivt_2016_3_24.pdf.
5. IDS - что это такое? Система обнаружения вторжений (IDS) как работает? [Електронний ресурс] – Режим доступу до ресурсу: http://fb.ru/article/186268/ids---chto-eto-takoe-sistema-obnarujeniya-vtorjeniy-ids-kak-rabotaet.

УДК 004.056.55

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ АНАЛІЗУ КЛАВІАТУРНОГО ПОЧЕРКУ

Мальцева М.В., студ.гр. КБ-161

Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання

Чернігівський національний технологічний університет

У сучасному світі загальної інформатизації особливого значення набувають завдання захисту інформації. Основні проблеми захисту інформації при роботі з нею, можна умовно розділити на три типи: перехоплення інформації (порушення конфіденційності інформації), модифікація інформації (спотворення вихідного повідомлення або заміна іншою інформацією), підміна авторства (крадіжка інформації та порушення авторського права). Основною задачею безпеки інформаційних комп'ютерних систем є обмеження кола осіб, що мають доступ до конкретної інформації, і захисту її від несанкціонованого доступу.

Існує багато методів захисту інформаційних систем, такі як: фізичні, програмні та апаратні. Ці методи захисту інформації передбачають використання певного набору засобів.

Одними з найбільш перспективних і активно розвиваючих фізичних методів є метод біометричної аутентифікації. Біометричні системи аутентифікації - системи, що використовують для посвідчення особи людей їх біометричні дані. Біометрична аутентифікація - процес докази і перевірки автентичності заявленого користувачем імені, через пред'явлення користувачем свого біометричного способу і шляхом перетворення цього образу відповідно до заздалегідь певним протоколом аутентифікації. Біометричні системи розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, способу особи, малюнка ліній долоні, райдужної оболонки, голоси) або поведінкових рис (підписи, ходи) [1]. Оскільки ці риси фізично пов'язані з користувачем, біометричний розпізнавання надійно в ролі механізму, що стежить, щоб тільки ті, у кого є необхідні повноваження, могли потрапити в будівлю, отримати доступ до комп'ютерної системи або перетнути кордон держави. Біометричні системи також мають унікальні перевагами - вони не дозволяють відректися від досконалої транзакції і дають можливість визначити, коли індивідуум користується декількома посвідченнями

(наприклад, паспортами) на різні імена. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності.

Біометрична аутенфікація поділяється на: статичні методи (аутефікація по відбитку пальця, радужній оболонці ока, сітківці ока, геометрії руки, геометрії обличчя та термограмі обличчя) та динамічні (аутенфікація по голосу та клавіатурному почерку). В даній роботі я роздивляюся метод клавіатурного почерку[2].

Клавіатурний почерк - поведінкова біометрична характеристика, яку описують такі параметри: швидкість введення, кількість введених символів, розділене на час друкування; динаміка введення, яка характеризується часом між натисканнями клавіш і часом їх утримання; частота виникнення помилок при введенні; використання клавіш, як приклад, які функціональні клавіші натискаються для введення великих літер; сила натискання на клавіші та ін. [3]. Аутентифікація користувача по клавіатурного почерку дешевий і досить простий для реалізації варіант, так як для такої системи не потрібно додаткового обладнання. Потрібно стандартний набір периферійних пристроїв, які має в своєму розпорядженні будь-який персональний комп'ютер - клавіатура і монітор. А в якості системи безпеки буде виступати програмний продукт, розробка якого і представляє основну складність.

Існує два способи аутентифікації користувача по клавіатурного почерку: по введенню відомої фрази (пароля); по введенню невідомої фрази, що генерується випадково [4].

Обидва способи мають включати в себе два режими: режим навчання і режим аутентифікації. У режимі навчання шляхом багаторазового повторення вводами повинні розрахувати еталонні характеристики набору тексту. У режимі аутентифікації за допомогою введення відомої і невідомої фрази можна порівнювати різницю між інтервалами часу при введенні знайомої і незнайомої фрази. Це дозволяє правильно ідентифікувати користувача, не дивлячись на втому або інші психофізичні чинники.

Система аутентифікації користувача по клавіатурного почерку повинна працювати в трьох режимах : навчання, аналіз, блокування. Режим навчання (в ньому визначаються і зберігаються еталонні характеристики клавіатурного почерку користувача), режим аналізу (в ньому система порівнює еталонні характеристики з знову введеними, після чого може залишатися в режимі аналізу, або перейти в режим блокування), режим блокування - в цьому режимі система просить ввести пароль, який буде перевірений на справжність і знову пройде аналіз клавіатурного почерку. Якщо все пройде успішно, то програма перейде в режим аналізу[3].

Спосіб аутентифікації має певні уращливості: додаток необхідно постійно навчати, сильна залежність від клавіатури (в разі заміни клавіатури доведеться навчати програму заново), сильна залежність від психофізичного стану оператора. Якщо людина захворіла, то він цілком ймовірно не зможе аутентифікуватися (з іншого боку, може і не варто цього робити в хворому стані). Щоб система могла працювати найбільш точно, на навчання для запам'ятовування їй буде потрібно близько тижня. Після цього вона вже може перевірити людину: він чи ввів ключову фразу або не він.

Основними перевагами аутентифікації користувачів по клавіатурного почерку можна віднести: простота реалізації і впровадження. Реалізація виключно програмна, введення здійснюється зі стандартного пристрою вводу (клавіатури), а значить - використання не потрібне придбання ніякого додаткового обладнання. Це найдешевший спосіб аутентифікації по біометричних характеристик суб'єкта доступу. Не вимагає від користувача ніяких додаткових дій і навичок. Користувач, так чи інакше, напевно використовує пароль, який можна призначити пральний фразою, по якій буде проводитися аутентифікація. Можливо, шахраєві вдасться отримати логін і пароль для входу в систему, але ось скопіювати клавіатурний почерк не є можливим. Можливість прихованої аутентифікації - користувач може не знати, що включена додаткова перевірка, а значить не зможе повідомити про це зловмисникові[5].

Як висновок можна сказати, що аутентифікація лише з використанням аналізу клавіатурного почерку є неприйнятною в системах, що вимагають високого рівня захисту. Але в поєднанні з іншими системами аутентифікації може виявитися досить ефективною. Однак, незважаючи на свої переваги, дана сфера мало вивчена, і має величезний потенціал.

Список використаних джерел

1. Комплексна біометрична аутентифікація особистості [Електронний ресурс] – Режим доступу до ресурсу: http://www.hups.mil.gov.ua/periodic-app/article/16564/ukr.
2. Задорожний В. Огляд біометричних технологій // Захист інформації. Конфидент. -2003. - № 5.
3. Клавиатурный почерк [Електронний ресурс] – Режим доступу до ресурсу: http://infoprotect.net/varia/klaviaturnyiy_pocherk.
4. Клавиатурный почерк как средство аутентификации [Електронний ресурс] – Режим доступу до ресурсу: https://www.securitylab.ru/blog/personal/aguryanov/29985.php.
5. Аутентификация по клавиатурному почерку: выгоды и проблемы использования [Електронний ресурс] – Режим доступу до ресурсу: https://research-journal.org/technical/autentifikaciya-po-klaviaturnomu-pocherku-vygody-i-problemy-ispolzovaniya/.