$\overline{T}пр$ характеризует среднее время, в течение которого программы по обслуживанию событий в системе ожидают освобождения центрального процессора. В это время программы фактически "простаивают". Желательно, чтобы $\overline{T}пр$ было достаточно мало.

Представленная модель ориентирована на обеспечение выполнения требований стандартов и анализ случайных процессов, физически свойственных интегральным системам безопасности независимо от их функционального приложения. Применение модели позволяет оперативно вычислять временные характеристики системы, а также аргументировано обосновывать количественные требования технического задания к характеристикам системы при ее проектировании. Модель позволяет оценить выполнение требований заказчика и выявлять «узкие места» и уязвимости системы.

1. *Белоус В. Ядерный терроризм в современном мире.- Ядерная безопасность. – 2000. - № 34-35.*
2. *Забулонов Ю.Л., Лисиченко Г.В. Нові засоби оперативного контролю за нерозповсюдженням ядерно - радіаційних матеріалів // Сб. науч. тр. СНИЯЭиП. – Севастополь, 2005. - Вып. 12. – С. 31-38.*
3. *Гихман И.И., Скороходов А.В. «Теория случайных процессов» М 1973 г.*
4. *Корн Г., Корн Т. «Справочник по математике для научных работников и инженеров» Издательство «Наука» М 1973 г.*
5. *Хинчин А.Я. Работы по математической теории массового обслуживания. М. 1963 г*

Поступила 29.01.2009р.

УДК 004.087.5

А.М. Давиденко, В.В. Душеба, Р.В. Яровий

АНАЛІЗ ВРАЗЛИВОСТЕЙ СМАРТ-КАРТ В АСПЕКТІ МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ НА ЇХ ОСНОВІ

The analysis of vulnerability of intellectual cards is conducted, as a constituent of the informatione system

Вступ. Смарт-ка́ртка (англ. *smart card*) — пластикова картка, що містить інтегральну схему, яка забезпечує певний рівень програмованості та невеликий обсяг пам'яті.

Смарт-карти використовуються для ідентифікації, одно- і двофакторної автентифікації користувачів, зберігання ключової інформації та проведення

 © А.М. Давиденко, В.В. Душеба, Р.В. Яровий

криптографічних операцій в довіреному середовищі. Смарт-картки знаходять все більш широке застосування в різних областях: від систем накопичувальних знижок до кредитових і дебетових карт, пропускних документів, телефонів стандарту GSM і проїзних квитків, а також для кодування таких індивідуальних відомостей, як наприклад, історія хвороби.

Смарт-карти - унікальне сполучення низької ціни, малих розмірів, портативності й універсальності, що постійно зростають. Швидкість обчислень і криптографічні можливості карт підвищуються з кожним роком. Якщо ця тенденція збережеться надалі, то смарт-карти знайдуть і займуть такі прикладні ніші, про які зараз ми навіть не можемо припустити.

Без сумніву однією з головних переваг смарт-карт є зручність, яка базується, насамперед, на широких функціональних можливостях при їх використанні. Багатофункціональні смарт-карти універсальні й зручні, але вони найбільш вразливі до різних атак. Основна проблема зараз - це неефективний захист смарт-карт перед достатньо дешевим способом фізичної атаки.

Області застосування смарт-карт різноманітні, у тому числі, зберігання даних (Stored Value Card), які можна використовувати в електронній комерції, тобто для оплати покупок через Інтернет. Завдяки особливостям своєї конструкції вони забезпечують високу ступінь захисту важливої інформації. Але все-таки рівень захисту інформації в смарт-картах часто переоцінюється. Розглянемо основні вразливості смарт-карт, та способи використання цих вразливостей зловмисниками.

1. Атаки при штатному використанні смарт-карти

При штатному використанні смарт-карти найбільш вразливим є канал передачі даних. Атаки на канал використовують пасивне прослуховування протоколу обміну смарт-карти і рідера з метою реєстрації змін деяких параметрів, наприклад: зміна й аналіз аналогових характеристик при роботі карт, тобто зміна споживання потужності; зміна рівня випромінювання якогось елемента при виконанні мікропроцесором карти будь-яких операцій і т.п. Запобігти неагресивним атакам, або атакам на канал, украй важко.

Зафіксовано такі різновиди атак на канал [1]:

- блокування доступу для рідера;
- часовий аналіз;
- простий аналіз споживаної потужності;
- атаки на відмову.

Розглянемо їх докладніше.

Найпростіша атака - це *блокування доступу для рідера* до відповідного контакту на карті. В цьому випадку для отримання несанкціонованих послуг (наприклад, доступу до платного ресурсу) блокується фізичний доступ до контакту, який керує процесом запису на смарт-карту. Найбільш часто приводяться приклади платного телебачення і телефонії. Подібна атака часто застосовувалася до карт доступу платного телебачення. Блокувався вхід,

через який телекомпанія подавала сигнал про припинення показу неоплаченого каналу. Якщо заблокувати цей контакт то знову можна буде дивитися всі канали. Аналогічно були модифіковані карти для телефонів-автоматів. Контакт, що зменшує суму на цій передплаченій карті, спеціально ізолювався, і карта ставала "вічною". Навіть сьогодні у використанні знаходиться дуже небагато смарт-карт, в яких така вразливість не ліквідована.

Часовий аналіз заснований на тому, що оцінюється час виконання смарт-картою якої-небудь операції. Якщо атакуючий має фізичний доступ до карти й може робити подібні виміри, то він зможе використовувати отримані дані для обчислення ключа карти. Простий і ефективний спосіб протидії такій атаці - вводити нелінійні затримки при використанні ключової інформації.

Простий аналіз споживаної потужності, диференціальний аналіз і диференціальний аналіз високого порядку стають можливими через те, що при роботі смарт-карти змінюються характеристики спожитої нею потужності і, на основі їхнього аналізу, можна отримати матеріал для обчислення секретного ключа й використаних у смарт-карті протоколів і алгоритмів. Через те що методика аналізу потужності смарт-карт опублікована порівняно недавно, поки не винайдено практичних рішень по запобіганню таких атак. Деякі методи, які запропоновані для цього захисту, повинні бути впроваджені в смарт-карті. Самий перспективний метод, при якому в коло електроживлення смарт-карти включається діодно-конденсаторна схема, був запропонований Ади Шаміром.

Атаки на відмову (збій) програмного протоколу (мається на увазі не тільки протокол передачі, але й порядок виконання програмного коду) спрямовані на недоробки або помилки чіпа. Подібні атаки вимагають детально проаналізувати схемотехніку чіпа і його програмне забезпечення або довго і ретельно вивчати чіп методом проб і помилок, щоб визначити, як він реагує на різні впливи: швидкі або повільні тактові частоти, коливання рівня електроживлення й інші імітації збоїв навколишнього середовища.

Дана технологія може бути використана, наприклад, для зміни стану контрольних пристроїв (датчиків на кристалі). Якщо використовувати сигнал від годинника або випадкове значення із багатопоточних операцій для зміни внутрішньої тактової частоти, то буде відвернене передбачення часу виконання команд. Крім того, багато смарт-карт випускаються зі встановленими в них контрольними датчиками, які відключать процесор, якщо змінюється зовнішня тактова частота, температура навколишнього середовища або рівень електроживлення. На жаль, ці датчики часто спрацьовують без поважних причин, тому що вони досить примхливі в роботі й самі стають джерелом відмови чіпа.

2. Реінженірінг смарт-карт

Фізична атака на чіп дуже проста й може забезпечити доступ до його

найбільш захищених частин. Атакуючий може дослідити й проаналізувати картковий чіп у стандартній системі налагодження, від'єднавши процесор від пластика. Розробка власного налагоджувального комплекту не є чимось надскладним. Патрик Гель у своїй книзі наводить принципові схеми й тексти програм подібних для дослідження смарт-карт [2]. Anderson і Kuhn опублікували кілька інших способів дешевих фізичних атак. Вони змогли прочитати зміст пам'яті й навіть змінити його, використовуючи в якості "редактора" спрямований потік іонів. За допомогою лазера своєї установки вони змогли змінювати стани навіть окремих осередків ПЗУ. Такі досягнення призводять до серйозної небезпеки: існує атака на DES, при якій зміна декількох біт приводить до дискредитації всієї ключової інформації. Аналогічно організуються атаки й на ППЗУ.

Але є спосіб запобігти такій атаці - встановити ємнісний датчик, що фіксує зміну обсягу або опору середовища. Другий спосіб - встановити оптичний датчик під непрозорою фольгою, що захищає мікросхему. Якщо захист спрацює, то незворотною буде зруйнована критична інформація. Однак ці датчики недостатньо надійні, і тому, поширені мало.

Фірма Philips пропонує свій спосіб захисту від фізичної атаки. Компанія рекламує техніку так званої логіки клею (glue logic). Ця техніка "перемішує" логіку чіпа випадковим чином. Схоже на технологію "візуального" шифрування, при якій блоки перемішані настільки, що з'ясувати логіку їхнього з'єднання практично неможливо. Інший спосіб - захист пам'яті, при якій адреса й фактичне розміщення даних ніяк не пов'язані. Однак такий підхід працює тільки для динамічних об'єктів, а отже, придатний тільки для ОЗУ.

Донедавна вважалося, що розшифрувати інформацію, записану на пластиковій карті можна тільки за допомогою спеціального устаткування й при наявності надскладного коду. Однак двоє дослідників з Кембриджського університету (один з них Сергій Скоробогатов - фахівець з програмного забезпечення ядерної зброї, що емігрував з Радянського Союзу) з'ясували, що зламати такий чіп можна всього лише за допомогою фотоспалаху й мікроскопа [3].

Якщо таку картку підставити під фотоспалах, то всі захисні покриття виявляться зруйнованими й мікропроцесор може вийти з ладу. А якщо за допомогою мікроскопа на чип направляти винятково тонкі промені світла, то з їхньою допомогою можна послідовно сканувати окремі елементи мікросхеми, що дозволить розшифрувати закодовану в них інформацію.

Повідомлення про зроблене відкриття було опубліковано в спеціалізованому журналі, а також стало предметом дискусії на спеціальному семінарі з питань безпеки й захисту конфіденційної інформації. Офіційної реакції з боку виробників подібних карт поки не спостерігається, хоча в приватних бесідах з авторами відкриття про впевненість у невразливості своєї продукції заявив усього лише один з них.

3. Правові та організаційні аспекти використання смарт-карт

Можливо, найскладніше питання в системах безпеки - проблема розподілу повноважень, суть якої в тому, що одна сторона контролює частину функціональних можливостей смарт-карти і впливає на контроль функціональних можливостей іншої сторони. Наприклад, функціональні можливості смарт-карти потенційно розподілені між такими сторонами:

- власник карти (Cardholder).
- власник даних (Data owner).
- POS-термінал, ATM і взагалі всі, із чим взаємодіє карта (Terminal).
- сторона, що випустила карту в обіг (Card issuer).
- виготовлювач карти (Card manufacturer).
- розроблювач програмного забезпечення (Card software developer).

Підроблений термінал, що списує з карти одну суму, а в чеку вказує іншу або зберігає в себе приватну інформацію (наприклад PIN) є негативним результатом такого розподілу. Такі атаки (імітатор банкомату) цілком реальні.

При цьому важливу роль грає правове і організаційне забезпечення. Дуже часто розробник і власник системи перекладають відповідальність на користувачів системи. Автори можуть привести приклад, коли при укладенні договору на зарплатну картку банк, що надає послуги в договорі з клієнтом включав пункт про відшкодування останнім будь-яких можливих збитків від використання картки, у тому числі і пов'язані з перевитратою коштів. У відповідь на питання про необхідність використання відповідних технічних алгоритмів і засобів захисту, було сказано, що «захищати – це є справа банка, а покривати збитки – це справа клієнта».

При одному із способів попередити атаки, з боку термінала на карту або, навпаки, з боку власника карти на термінал, процесинговий центр поетапно контролює процес угоди і, якщо виявляється підозріла діяльність, встановлює прапорець попередження. Більшість атак неможливі на окремому комп'ютері, тому що вони в такому випадку привертають увагу єдиної системи безпеки. Зовсім інша ситуація із системами на смарт-картах, функціональність яких (у тому числі захисту) розподілена між багатьма учасниками.

Багатофункціональні, а отже, універсальні карти потенційно уразливі до атак саме через поділ повноважень безпеки по системах, які вони підтримують. Безліч додатків, які підтримує смарт-карта, вимагає солідного різноманіття від засобів автентифікації та безпеки в різних системах, що використовуються. Рідер повинен підтвердити дійсність картки і власника картки, а картка, у свою чергу, валідність "зчитування" і автентичності програмного забезпечення. Крім того, при зчитуванні, картка повинна впевнитися в санкціонованості та наявності підключених до неї периферійних пристроїв.

Один з головних недоліків смарт-карти полягає в тому, що вона не може самостійно зв'язатися з "зовнішнім світом" і змушена робити це через

спеціальне устаткування (термінал). Шнайер і Шостак (Schneier and Shostack) рекомендують об'єднати власника карти й власника даних в одну особу [4]. Часто вони і є одною особою, але програми смарт-карт не завжди приймають цей факт і розділяють доступ - це найпростіший і найдешевший спосіб захиститися від певного виду атак, які є бідою для багатьох систем, заснованих на смарт-картах. Альтернативний та більш дорогий спосіб зменшити проблеми поділу повноважень - введення в карту пристрою введення даних і екрана.

Таким чином при використанні смарт-карт в системах моделювання необхідно проаналізувати три основних фактори розподілу повноважень і відповідальності за інформацію, що використовується, наявність засобів захисту від реінженірінгу і атак при безпосередньому використанні карток.

Висновок. Проведений аналіз дозволяє оцінювати ризики використання смарт-карти як компоненти інформаційної системи і є основою для розширення бази моделювання системи захисту комп'ютеризованих систем.

1. *Андрей Межутков* Атаки на смарт-карты. Спецвыпуск: Хакер, номер #061, стр. 90-95.
2. *Патрик Гель* ПК и чип-карты**:** Пер. с фр. - М.: ДМК Пресс, 2003. - 144 с.
3. *Сергій Скоробогатов, Росс Андерсон* Смарт-карты – взгляд на безопасность при свете фотовспышки. -. IV ежегодная конференция MasterCard International, Дублин, 15-16 мая 2002 г.
4. *Нильс Фергюсон, Брюс Шнайер.* Практическая криптография. Practical Cryptography, Издательство: Вильямс, 2005 г, 424 с.

Поступила 15.01.2009р.

УДК 683.03

Ю.М.Коростиль, Г.А.Максименко

ОСНОВНЫЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ, ОРИЕНТИРОВАННОЙ НА ИСПОЛЬЗОВАНИЕ В СИСТЕМАХ РАДИО МОНИТОРИНГА

Сбор данных по радиочастотной обстановке не ограничивается только физической регистрацией источников радиосигналов, анализом их технических характеристик и определением значений их параметров. Необходимость расширенного анализа данных, которые могут быть получены в результате сбора данных РЧО в том числе и за счет радиочастотного мониторинга, определяется широким распространением индивидуальных средств приема-передачи информации, проникновением

© Ю.М.Коростиль, Г.А.Максименко