УДК 621.398: 004.056.5

Е.И. Подскальный, А.А. Галькевич, А.В. Желтухин

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ КОНТРОЛЯ ФИЗИЧЕСКОГО ДОСТУПА С АУТЕНТИФИКАЦИЕЙ НА ОСНОВЕ СМАРТ-КАРТ

Рассматриваются вопросы организации безопасного информационного обмена в СКФД. Оценивается современное состояние исследований в данной сфере. Обсуждаются основные компоненты таких систем и их возможные уязвимости, предлагаются рекомендации по организации стойких к атакам систем. Рассматривается возможность применения современных метрик и методик ИБ к существующим и проектируемым СКФД. Особенно отмечается необходимость формирования и применения целостных подходов по обеспечению ИБ в распределённых автоматизированных системах безопасности.

Ключевые слова: *информационная безопасность, СКФД (СКД, СКУД), системная безопасность, идентификация и аутентификация, протоколы обмена информацией, смарт-карты.*

Введение

В наше время классические методы обеспечения контроля физического доступа уступают место распределённым автоматизированным системам – так называемым СКУФД (далее СКУД) – системам контроля управления физическим доступом. Подобные системы могут значительно увеличить пропускную способность точек доступа, уменьшить расходы на вопросы безопасности, упростить учёт [1] и т.д. Однако такие системы представляют собой сложные комплексы обработки критической по своей сути информации, характеризующиеся особенностями [2]:

1. иерархичностью и многоуровневостью;
2. распределённостью компонентов;
3. большим числом внешних интерфейсов у компонентов;
4. потенциальным наличием открытых каналов как со стороны внешних, так и внутренних интерфейсов;
5. необходимостью работать в режиме жёсткого (или мягкого) реального времени;
6. обилием пространственно-временной логики;
7. транзакционным характером большинства операций;
8. ориентированностью на работу с персоналом

При этом на самом нижнем уровне архитектуры они состоят из сети подсистем - низкоуровневых контроллеров, для которых зачастую применяются проприетарные не стандартизированные протоколы и схемы. К сожалению, отношение к информационной безопасности (ИБ) к подобным встроенным, прикладным подсистемам недостаточно серьёзное [3-5]. К примеру, вспомним результаты [6], посвящённой встроенным подсистемам внутренней сети CAN в автомобилях крупных мировых марок, в которой было показано, что злоумышленник мог без особых усилий получить контроль над большинством систем автомобиля.

К тому же СКУД не являются отдельными независимыми системами, так как даже полностью автономные СКУД [1], будут являться частью общей системы безопасности (см. рис. 1). СКУД обеспечивают функции задержки и обнаружения [7] - функции системы физической защиты, при этом занимаясь хранением, передачей и учётом секретной информации, то есть функциями ИБ.

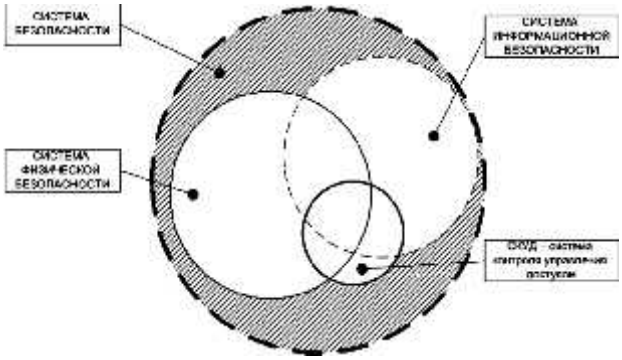

Рис. 1. Система безопасности - Диаграмма Эйлера

Учитывая то, что организация действительно качественной системы физической безопасности [7], работающей совместно со СКУД является дорогостоящей для большинства предприятий, и всё большего роста популярности автоматизированных СКУД, они будут становиться более предпочтительной целью для недоброжелателей на пути совершения воровства, саботажа или другого акта вредительства [7].

В наше время огромное внимание уделяется вопросам ИБ высокоуровневых сетей, хранилищ данных и ПО, противодействию социальной инженерии, но никакие брандмауэры, антивирусы и корпоративные политики безопасности не помогут, если злоумышленник может получить физический доступ внутрь защищённого периметра [8, 9]. Если

непосредственная физическая атака на систему физической безопасности может быть обнаружена и предотвращена охраной [7], то злоумышленник, использующий подобранный пароль, скопированную карточку доступа или сумевший найти уязвимость в СКУД для добавления своих идентификационных данных, будет вполне в состоянии проникнуть на предприятие через автоматизированную точку доступа, не привлекая лишнего внимания.

На настоящий момент вопросы безопасности информации в СКУД остаются в тени организации других аспектов СФЗ (таких как заградители, средства наблюдения, охрана в [1,7], идентификаторы [10, 11]), описываются с обобщённых точек зрения [1, 12]. Или, несмотря на практичность конкретных предложений, не предлагается системный, интегрируемый в процесс разработки и сопровождения подход [13, 14].

Исходя из всех указанных фактов, нами было выбрано данное направление ввиду его перспективности и малой исследованности.

В разделе "Архитектуры и компоненты СКУД " будут проведён обзор возможных архитектур и компонентов СКУД. В разделе "Факторы аутентификации" мы останавливаемся на факторах аутентификации и о том, как выбор идентификатора влияет на результирующую ИБ системы. Раздел "Метрики и методики" содержит краткий обзор потенциальных метрик и методик оценки ИБ для СКУД. Раздел "Уязвимости и атаки" является основным, описывая наиболее серьёзные уязвимости СКУД наряду с возможными методами их преодоления или смягчения. В последнем разделе подводятся итоги.

1. Архитектуры и компоненты СКУД

Структура и организация любой системы являются первичным фактором, определяющим её безопасность [15]. А так как системы контроля управления доступом могут сильно отличаться как по принципу организации взаимоотношений между основными актёрами [1], так и по конкретным реализациям компонентов, то в данном разделе нами будут рассмотрены основные актёры (компоненты) и возможные архитектуры сетевых СКУД в контексте вопросов информационной безопасности.

Актёры СКУД

На рис. 2 показаны самые базовые актёры [1] распределённой СКУД без привязки к реальным архитектурам СКУД или реализациям компонентов.

Рис. 2. Основные актёры СКУД

Показанные актёры СКД:

1. пользователь - основной актёр, который должен быть аутентифицирован СКД за счёт своего идентификатора и авторизирован для пропуска через УПУ;

2. идентификатор - нечто, позволяющее подтверждать право пользователя на проход через заградитель;

3. УС (Устройство считывания) - подсистема считывающая сигнатуру с идентификатора для её передачи в контроллер;

4. периферийный контроллер-модуль (ПМ) - устройство с различной возможной функциональностью, начиная от простейших посредников-ретрансляторов между считывателями, заградителями и высокоуровневыми контроллерами до многофункциональных систем;

5. УПУ (устройство преграждающее управляемое) - любое заграждающее устройство, которое можно контролировать (двери с электрозамками, турникеты, шлюзы и т.п.);

6. сервер безопасности - ПО и АО предоставляющее возможности мониторинга и контроля за СКУД, участвующее в обмене между контроллерами, администраторами и базой данных;

7. хранилище данных - предпочитаемая система хранения долгосрочной информации. Она может быть интегрирована с существующими БД предприятия или, наоборот, быть полностью автономной ввиду повышенных требований по безопасности;

8. утилиты администрирования - программное обеспечение, служащее для добавления, изменения и отслеживания данных СКД.

9. администратор - лицо, уполномоченное на доступ к средствам администрирования СКУД.

СКУД обычно интегрируется с различными системами слежения и тревоги [7], однако подобные подсистемы мы оставим за рамками работы.

Мы не указали на рис. 1 среды обмена (идентификатор-считыватель, периферийный модуль-сервер безопасности, административные утилиты - сервер безопасности и т.д.), представляюшие собой одно из самых слабых мест любой системы обработки информации. Эти каналы связи будут более подробно рассмотрены в разделе, посвящённом уязвимостям СКУД.

Архитектуры СКУД

В связи с ограничениями данного документа, мы рассмотрим архитектуры СКУД исходя из распределения ролей между контроллерами (периферийными модулями) и центральной системой безопасности.

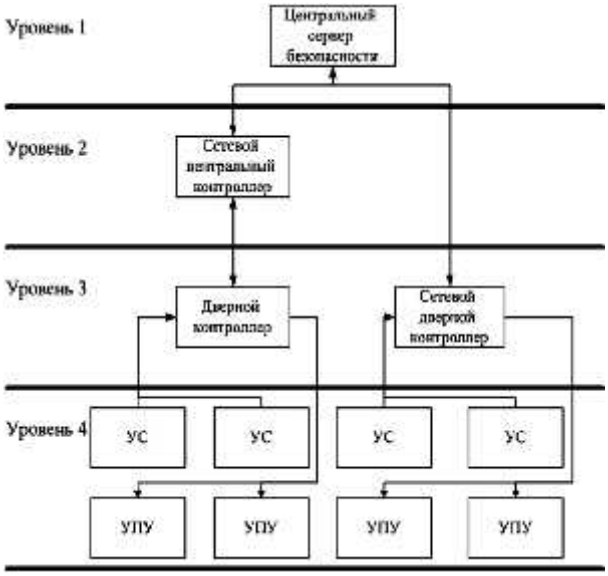

Рис. 3. Архитектура СКУД смешанного типа:
УС - устройство считывания;
УПУ - устройство преграждающее управляемое

СКУД смешанного типа включают в себя элементы всех остальных архитектур, поэтому она и выбрана для отражения возможных[1, 7] вариантов:

1. централизованная архитектура (левая ветвь дерева на рис. 3) - центральный сервер подсоединён к сетевым центральным контроллерам, которые связаны с группами простых дверных контроллеров, выполняющих роль посредников межу центральными контроллерами и периферийной аппаратурой;

2. распределённая архитектура (правая ветвь дерева на рис. 3) - центральные контроллеры отсутствуют, а их функции выполняются сетевыми дверными контроллерами. Обычно сетевой дверной контроллер работает прямо с парой заградитель-считыватель;

3. смешанная архитектура (весь рис. 3) - в этом случае часть точек доступа обслуживается центральными контроллерами через промежуточные дверные контроллеры, а другая контролируется прямо сетевыми дверными модулями;

4. многоуровневая архитектура - на рис. 3 показаны только два слоя архитектуры СКУД контроллеров, однако может возникнуть потребность для разграничения системы на большее число уровней для обеспечения лучшей степени абстрагирования и сосредоточения логики системы на нужных стратах;

5. облачная архитектура - использование контроллеров СКУД в качестве высокоуровневой сети для обеспечения необходимой избыточности СФЗ уже можно наблюдать в некоторых СКУД промышленного уровня [1], однако говорить о действительно распространённом новом типе архитектуры всё ещё несколько рано.

2. Идентификаторы и факторы аутентификации

Идентификатор или идентификаторы, использующиеся в СКУД, наиболее часто становятся фактором, ограничивающим максимально возможный уровень безопасности. Ведь если идентификаторы могут быть легко скопированы, изменены, украдены или скомпрометированы каким-либо другим способом, то никакой из показанных на рис. 1 актёров не будет способен предотвратить прорыв периметра. В этом случае вся надежда на предотвращение вреда будет возложена на компоненты системы безопасности, которые находятся вне нашего рассмотрения (служба безопасности, системы наблюдения и т.п.), которые более подробно описаны в [1][7].

Идентификаторы наиболее часто классифицируются по принадлежности к определённому фактору аутентификации – то есть по тому, за счёт чего осуществляется аутентификация его обладателя.

Фактор знания

Пароли, коды доступа и последовательности запрос-ответ широко распространены в системах безопасности. Это простое решение, позволяющее избежать необходимости иметь при себе вещи-идентификаторы и встречаться с особенностями биометрики. Но сами по себе они очень уязвимы [16] к подслушиванию (атака человек-в-центре) в открытых средах обмена информацией, в статической реализации имеют низкую энтропию ключа (позволяя злоумышленникам использовать словари или генераторы паролей) и считаются привлекательными целями для социальной инженерии. Поэтому обычно они используются в связке с другими идентификаторами при многофакторной аутентификации или в нетребовательной к безопасности среде.

Фактор обладания

Ключи, пропуски, карты и прочие подобные объекты в их явной реализации, как и статические пароли, имеют один очень большой недостаток - они на самом деле идентифицируют себя, а не персону обладателя. Если недоброжелатель достанет ключ однофакторной аутентификации, то он сможет легко пройти через автоматизированную точку входа. Поэтому такую однофакторную аутентификации неблагоразумно применять для зон с повышенной безопасностью. Хотя применение переменной аутентификации - к примеру, биометрии и смарт-карты [17] для входа на предприятие и доступа к критическим зонам, и только карты для доступа к менее важным

ресурсам, может быть оправданным решением для конкретной системы.

Наряду с переменной аутентификации и многофакторными методами граничат идеи интеграции ключей с дополнительными устройствами аутентификации (карты с датчиками отпечатка пальца [18], устройством ввода графического пароля [19] и т.п.). Подобные токены будут начинать обмен со считывателями только после успешного завершения аутентификации пользователя, позволяя повысить защищённость не изменяя аппаратуры ПМ.

Фактор неотделимости

Биометрическая аутентификация пришла в мир систем безопасности не очень давно, но уже занимает достойное место в этом секторе технологий. Отпечатки пальцев, сетчатка, радужка, капиллярный паттерн, ДНК, голос, подчерк или ещё более экзотические идентификаторы являются факторами аутентификации с высоким несходством между индивидуумами, большей или меньшей сложностью при копировании, и они обычно всегда с каждым пользователем [16]. Но считыватели биометрии сложны и относительно дороги, идентификаторы требуют больших объёмов пространства данных, идентификация может занимать много времени и требовать специальных действий, при сверке паттернов со снимками, ввиду недетерминированности, возможны случаи ложного доступа и ложного отказа в доступе. Но, несмотря на все свои недостатки, биометрия является самой активно развивающейся сферой в безопасности наряду с криптографией.

Многофакторная и сильная аутентификация

Как уже упоминалось, применение аутентификации основанной на использовании нескольких факторах является предпочтительным вариантом для предприятий с повышенными требованиями по безопасности [8, 11, 16]. Зачастую, понятие многофакторной аутентификации используют как синоним сильной аутентификации, однако сильная аутентификация не имеет чётко стандартизированного определения, и в большинстве контекстов позволяет использование нескольких идентификаторах из одной категории, в отличие от многофакторной аутентификации [16].

Выбор идентификатора

Выбор конкретного идентификатора в системе определяется множеством различных факторов, при этом требования безопасности практически всегда вступают в противоречие с бюджетными ограничениями [7, 15]. Зачастую, система уже существует и использует установившуюся инфраструктуру идентификаторов и считывателей, замена которой потребует значительных затрат.

Тем не менее, как уже упоминалось, СКУД не может быть более безопасной, чем это позволяет используемый в ней идентификатор. К тому же к современным идентификаторам [10] всё чаще предъявляются такие требования, как:

1. возможность применения, как при физическом, так и при логическом доступе;
2. возможность применения в нескольких приложениях
3. простота интеграции с другими идентификаторами (факторами);
4. возможность внедрения дополнительной информации.

Все эти требования приводят нас к необходимости использования в качестве базовых идентификаторов действительно многофункциональных «умных» устройств - смарт-карт.

Смарт-карты стали активно применяться в сфере контроля логического и физического доступа в последние 15-20 лет [10]. На данный момент они применяются в самых различных государственных и частных системах физического или совмещённого доступа: Sun Microsystems JavaBadge, Department of Homeland Security and Credentialling Card, NASA Smart Card Project, Microsoft ACS и др. [11].

Для демонстрации преимуществ смарт-карт ниже в табл. 1 приведена сравнительная характеристика свойств аутентификации на основе различных факторов и аутентификации на основе смарт-карт. Более подробное сравнение факторов аутентификации и идентификаторов можно найти в [16, 20].

Таблица 1

Сравнение различных средств аутентификации

Параметр	Пароли и т.п.	Другие физ-кие токены	Биометрия	Смарт - карты
Простота для пользователя	Средняя	Высокая	Средняя	Высокая
Скорость аутентификации	Средняя	Высокая	Низкая	Высокая
Распространённость	Высокая	Средняя	Низкая	Высок.
Простота для разработчика	Высокая	Средняя	Низкая	Средняя
Стоимость организации системы	Низкая	Средняя	Высокая	Средняя
Стоимость идентификатора	Нулевая	Средняя	Нулевая	Средняя
КЛД и КЛОД	Нулевая	Нулевая	Высокая	Нулев.
Простота интеграции с другими факторами	Средняя	Средняя	Низкая	Высокая
Возможность интегрирования дополнительной информации и функциональности	Очень низкая	Низкая	Нулевая	Высокая
Сложность подготовки копирования	Низкая	Средняя	Высокая	Высокая
Сложность копирования	Низкая	Средняя	Высокая	Высокая

С учётом всех указанных факторов, смарт-карты являются практически неоспоримым кандидатом для применения в качестве базового идентификатора [16] для любой системы контроля доступа, что и стало причиной их распространённости [11]. Исходя из этого, нами и было принято решение рассматривать СКУД именно с аутентификацией на основе смарт-карт, как самой

большой и при этом чётко определённой группы СКУД.

3. Метрики и методики

В этом разделе мы сначала, учитывая положение СКУД на границе СИБ и СФЗ, проведём обзор метрик эксплуатации и методик проектирования систем физической и информационной защиты, не привязанных к СКУД, после чего рассмотрим вопрос их применимости к СКУД.

Метрики и методики для физической безопасности

Существует множество методик [7] оценки эффективности систем физической защиты, которые хотя и слабоприменимы к СКУД сами по себе, однако в значительной степени зависят от защищённости и эффективности СКУД:

1. EASI (Estimate of Adversary Sequence Interruption).
2. ASSESS (Analytic System and Software for Evaluating Safeguards and Security).
3. SAFE (Safeguards Automated Facility Evaluation).
4. SNAP (Safeguards Network Analysis Procedure). и др.

Все эти методики оценивают вероятность успешного проникновения или задержания злоумышленника на охраняемом объекте вдоль определённого пути или совокупности путей. Они применяются при разработке или модификации системы.

Что же касается более привычных метрик времени эксплуатации, то, несмотря на меньшую степень рассмотрённости по сравнению с метриками ИБ, всё же существуют достаточно проработанные источники [21] посвящённые им.

Метрики и методики для ИБ

Метрики, применяемые для оценки информационной безопасности, являются очень хорошо рассмотренной темой, однако многие такие практики и методики взаимно противоречивы, о чём говорится в [15, 22-25]. В [26] предлагается следующая классификация метрик информационной безопасности:

1. метрики инцидентов (стоимость, средняя стоимость, число …);
2. метрики уязвимостей (покрытие поиска уязвимостей, процент систем без известных уязвимостей …);
3. метрики патчей (среднее время для пропатчивания, средняя цена пропатчивания);
4. метрики конфигурирования (процент соответствия конфигурации, соответствие защиты от вредоносного ПО …);
5. метрики изменений;
6. метрики приложений ПО;
7. финансовые метрики;
8. потенциальные и возможные метрики.

Применение к СКУД

Главной проблемой современных метрик является то, что многие из них, чётко определяя процедуры сбора и обработки информации, неспособны при этом обозначить цели - для чего мы их измеряем, что мы должны менять в системе, и к какому результату мы стремимся [23, 24]. Учитывая данный факт и то, что СКУД тесно связаны как с информационной, так и физической безопасностью, то вопрос о создании новых специализированных для СКУД метрик в данный момент не является актуальным. Тем не менее, применение существующих метрик и методик и добавление СКУД в существующие инфраструктуры сбора и анализа информации должно быть учтено при создании и сопровождении системы.

На этапе разработки системы одним из лучших вариантов для рассмотрения возможных уязвимостей, исходя из специфики СКУД, является применение диаграмм потоков данных с их последующим анализом путём составления деревьев угроз. Такая методика в течение многих лет успешно применяется при проектировании ПО [15, 27], позволяя эффективно отразить возможные пути воздействия на защищаемую информацию и оценить риски, применяя предпочитаемую схему риск-анализа (функцию от критичности и вероятности возникновения, DREAD или другую).

Касательно метрик времени эксплуатации мы рекомендуем дублировать для СКУД уже проверенные в общей системе ИБ или ФБ метрики, при этом интегрируя данные происходящие из СКУД в процесс вычисления общесистемных метрик. Такой подход позволяет одновременно учесть влияние СКУД во всей систему безопасности и отслеживать процессы в самой СКУД, применяя при этом установившуюся инфраструктуру [22, 24]. При корректно организованной системе учёта и обработки информации связанной с ИБ (ФБ), дублирование метрик будет достаточно простой задачей [26].

4. Уязвимости и атаки

В этом разделе описываются в обобщённой форме возможные уязвимости СКУД с аутентификацией на основе смарт-карт, атаки, эксплуатирующие эти уязвимости, а так же общие рекомендации по преодолению или уменьшению этих уязвимостей.

Ввиду обзорного характера данной работы мы не будем приводить анализ ИБ СКУД с применением диаграмм потоков данных, деревьев угроз [15] или других формальных техник [28, 29], а сразу перейдём к рассмотрению наиболее ключевых моментов. При этом стоит учесть, что наши рекомендации по смягчению угроз представляют собой лишь самые базовые, принципиально очевидные, но часто игнорируемые вопросы, которые стоит рассмотреть при проектировании и применении СКУД.

Для более подробной информации по реализации и анализу ИБ в СКУД предлагаются [11, 14]. Более общие сведения, касающиеся ИБ, могут быть найдены в [12, 15, 28] и в других источниках посвящённых общесистемной безопасности.

Идентификатор - смарт-карта

Как и любой физический токен, смарт-карта может быть украдена или утеряна. В этом случае злоумышленник может провести внутреннюю или внешнюю атаку для извлечения секретной информации [30-32].

Внутренние атаки на смарт-карты

Внутренние атаки - это группа инвазивных физических атак, которые требуют извлечения чипа из карты:

1. Микроскопический анализ - при этой атаке световые и электронные микроскопы используются для инспекции физической структуры чипа и реверс инженерии устройства или его области.
2. Механическое прощупывание - аналитик использует очень острые щупы для осуществления гальванического контакта с металлическими проводниками на чипе. Данные проходящие через шины могут быть перехвачены, хотя существует риск повреждения чипа.
3. Использование тестовых режимов - во время производства смарт-карт тестовые режимы и тестовые контакты используются для проверки чипа. Такие особенности могут быть найдены и восстановлены до работоспособного состояния, что позволит злоумышленнику получить доступ к внутренностям чипа.

Внешние атаки на смарт-карты

Внешние атаки (частичноинвазивные или неинвазивные атаки) задействуют карту или большое число карт. Они могут быть разработаны, используя старую или негодную карту, после чего перенесены на используемую карту. Такие атаки обычно требуют небольших вложений для разработки атаки под определенный вид устройств, что делает их особенно привлекательными, несмотря на низкие шансы на успех [31]:

1. Анализ проводников - это неинвазивная атака, при которой применяется низкочастотная манипуляция входов и наблюдение за выходами.
2. Измерение рабочих параметров - это вид частично инвазивных атак: в тех местах, где чип открыт, злоумышленник может попытаться считать данные прямо из памяти смарт-карт. Это достигается измерением рабочих характеристик, после чего применяется математический анализ и дедукция для определения секретных данных
3. Внедрение ошибок - при таких атаках секретные данные (в особенности секретный ключ) извлекаются путем создания ошибок в процессе вычисления и последующим анализом.

Атаки на карты и ИБ

Многие из вышеперечисленных атак использует различные недостатки программного и аппаратного обеспечения карты. Но даже карта, которая предусматривает противодействие всем указанным атакам, всё равно может быть взломана, пусть и за счёт больших усилий [32]. Не стоит забывать и об элементарной возможности прямого использования украденной карты. Несмотря на это смарт-карты нельзя назвать слабозащищёнными [30], так как все описанные атаки требуют физического обладания картой - носителем секретной информации, что для других идентификаторов намного более опасно ввиду простоты хранения секретной информации и отсутствия встроенной логики доступа [20].

Поэтому, с целью минимизации ущерба при возможной компрометации, смарт-карта:

1. не должна хранить секретную и конфиденциальную информацию (кроме прямо необходимых ключей) в открытом виде или использовать слабые функции хеширования.
2. должна находиться на постоянном учете, и ликвидироваться в соответствии с установленными процедурами;
3. при потере (или подозрении на утерю) должна быть немедленно деактивирована и лишена валидности;
4. не должна использоваться как единственный идентификатор для особо важных задач.

Периферийный модуль

Не теряя общности, мы будем считать, что наш гипотетический периферийный модуль работает в полуавтономном режиме и не имеет контроллера высшего уровня над собой, что предполагает одновременно и работу внутреннего хранилища данных контроллера, и обмен данными с компонентами на более высоких уровнях системы.

Идентификатор-считыватель (периферийный модуль)

При использовании в качестве идентификатора контактных карт компрометация системы во время обмена идентификатор-считыватель требует сложной атаки по стороннему каналу, поскольку данные передаются по контактному интерфейсу. В то же время бесконтактные карты стандартов ISO 14443 и ISO 15693 обмениваются данными в условиях открытого канала.

Для нас более интересны стандартные бесконтактные карты (ISO 14443[1]). Они имеют эффективную дальность работы от 10 до 20 см. в

[1] Карты ISO 15693, работающие на дистанциях порядка 50 см. не позволяют реализовывать сложные алгоритмы, ввиду слабой мощности и низкой производительности, что пока ограничивает их применение в СКУД с повышенными требованиями по безопасности.

зависимости от считывателя, карты и других факторов. Современные варианты, используемые для контроля доступа, применяют тот или иной протокол стартовой аутентификации (в несложных системах им обеспечивается аутентификация пользователя) с обязательным шифрованием данных симметричным или потоковым алгоритмом (DES в старых картах, 3DES или более сложными алгоритмами в современных).

Такая система представляется достаточно безопасной в условиях открытого канала, но исследования показывают, что относительно дешёвый RF-перехватчик может быть создан (или куплен) [33]. Такие устройства будут обладать дальностью перехвата более 10 метров. С использованием данных перехватчиков вполне реализуема атака криптоанализом, если карта не обладает достаточно сильным криптопроцессором, а используемый алгоритм аутентификации обладает недостатками. Подробно особенности взлома СКУД на уровне данного канала связи описываются в [33].

При проектировании протокола обмена между идентификатором и считывателем следует учитывать следующие рекомендации:

1. обмен должен инициироваться только после осуществления аутентификации и участники должны быть уверены, что во время обмена не произошла подмена;
2. любые обмены данными в любом направлении должны быть зашифрованы - несмотря на очевидность данного пункта, во многих системах атаки на подобные каналы напрасно считаются непривлекательным для атакующего[8, 9, 15];
3. пакеты данных должны быть скомпилированы так, что никакой пакет или их последовательность не могут быть использованы во время обмена посторонним лицом для отправки команд или данных;
4. при организации обмена, информация, относящаяся к аутентификации (ключи, шаблоны биометрии и т.п.) не должна покидать пределы карты и ПМ;
5. операции обмена должны осуществляться только при возможности гарантирования близости идентификатора (отсутствии посредников) или с жёсткими временными ограничениями.

Специфика периферийных модулей

Кража периферийных модулей может выглядеть нереалистичным событием, так как это потребует от злоумышленника применения физической силы и оборудования для извлечения. Но действительность (см. [7-9]) показывает, что не существует ничего невозможного для целенаправленного и обладающего ресурсами атакующего, так что мы не можем не учитывать такую угрозу. К тому же, как и любое подобное устройство, они могут быть подвергнуты неинвазивной атаки по побочному каналу во время нормального функционирования [34, 35].

В идеале периферийные модули должны быть не менее защищены от несанкционированного доступа, чем современные идентификаторы, что определённой степени так для продвинутых ПМ ведущих фирм, но более дешёвые контроллеры не обладают такими качествами. Поэтому если такие атаки действительно вероятны, то применяемые или проектируемые ПМ в своей программной и аппаратной реализации должен быть устойчивы к разбору.

В любом случае, мы рекомендуем обратить внимание на следующие пункты:

1. Внутреннее хранилище данных не должно содержать в прямой форме криптографических ключей, снимков биометрической информации и паролей - все они должны быть максимально представлены через хэш-функции и другие формы непрямого хранения.
2. Контроллер, если только он не привязан к контролируемой точке доступа с визуализацией, не должен содержать личной информации пользователей.

Компоненты уровня сети предприятия

Как уже упоминалось, за исключением, вероятно, предприятий с самыми жёсткими требованиями безопасности, СКУД в той или иной степени оказываются интегрированными в корпоративную сеть. Поэтому следующие компоненты и каналы можно считать подсистемами, оперирующими в сети высокого уровня:

1. канал контроллер - сервер безопасности;
2. сервер безопасности;
3. канал хранилище данных - сервер безопасности;
4. хранилище данных;
5. административные утилиты;

Учитывая то, что по вопросам организации ИБ в высокоуровневых сетях и сервисах имеется огромное количество работ [15], мы не будем останавливаться на сети предприятия и организации взаимодействия сетевых контроллеров, сервера безопасности и административных утилит. Обратим внимание лишь на некоторые самые важные или особенно специфические для СКУД вопросы:

1. возможность применения физических или виртуальных подсетей для разграничения контроллеров и корпоративной сети должна быть рассмотрена;
2. применение стандартных протоколов сетевой безопасности (TSL, IPsec) [15] для организации канала ПМ-сервер следует считать более предпочтительным, чем применение проприетарных протоколов.
3. преимущества интеграции логического и физического доступа должны быть взвешены по отношению к потенциальным недостаткам.

4. никакая информация, прямо использующаяся при криптографических или идентификационных операциях (ключи, снимки биометрии и т.п.) не должна быть считываемой для утилит администрирования;

5. доступ (в особенности модификация) к данным извне корпоративной сети должна быть максимально ограничен или вообще запрещён;

6. модификации данных должны заноситься в лог, удаление записей не должно быть финальным (удалённые записи должны быть отмечены как удалённые);

Социальная инженерия

Человек является самым слабым компонентом любой системы безопасности. Человека можно подкупить, принудить, обмануть и т.д. В связи с этим наиболее актуален вопрос социальной инженерии - обмана или мошенничество с целью сбора информации, введения в заблуждение или компьютерного доступа.

Различные методы социальной инженерии могут быть более или менее эффективны при попытке скомпрометировать те или иные компоненты СКУД. Чаще всего они применяются для получения доступа к компонентам высокого уровня, позволяя потенциально нанести огромный ущерб [8, 9]. Вопросы противодействия социальной инженерии достаточно хорошо освещены [8, 9, 36], и, ввиду отсутствия специфичных исключительно для СКУД моментов, мы не будем на них здесь останавливаться.

Комплексные уязвимости и атаки

Одной из самых больших ошибок при проектировании систем с повышенными требованиями по безопасности является то, что уязвимости и недостатки зачастую остаются не исправленными ввиду того, что сами по себе они были признаны неспособными нанести какой-либо вред безопасности информации [15]. Такой принцип некорректен исходя из следующих наблюдений:

1. Если для уязвимости не известно способов её эксплуатации, то это не значит, что их нет.

2. Если уязвимость сама по себе действительно не может быть использована для компрометации системы, то она может стать элементом составной атаки.

3. Даже если компоненты системы гипотетически не имеют уязвимостей, то результирующая система с высокой долей вероятности может содержать уязвимости и дефекты на границе интерфейсов используемых подсистем [15, 37].

В качестве примеров композитных атак на СКУД можно привести множество возможных комбинаций из атак на индивидуальные компоненты:

1. использование валидных карт и проприетарной информации по используемым форматам, средствам и процедурам, полученных методами социальной инженерии с целью упрощения атак ДАЭ;

2. внедрение вредоносного ПО в корпоративную сеть для отслеживания слабо защищённых обменов данными между контроллерами и сервером безопасности; анализ полученных данных, и последующее использование полученной информации для внедрения собственных данных в контроллеры и т.д.

Такие атаки могут быть более эффективными, чем обычные атаки, поскольку, в отличие от обычных узконаправленных атак, анализ и разработка противомер, являются затруднёнными ввиду эффекта комбинаторного взрыва [8, 9, 15].

Обычно при композитных атаках будут использоваться вышеупомянутые "некритические" уязвимости отдельных компонентов или наличие постоянных элементов или процедур в различных компонентах. Так же, вероятно, будет использоваться социальная инженерия (как наиболее затратоэффективный метод).

Поэтому, исходя из всех перечисленных фактов, следует обратить особое внимание на выполнение следующих общесистемных рекомендаций:

1. компонент ни в коем случае не должен знать больше информации, чем необходимо для его нормальной работы.

2. компонент должен считать весь внешний обмен потенциально скомпрометированным.

3. компонент СКУД должен придерживаться базовых рекомендаций для него.

4. обучение взаимодействию со СКУД должно быть частью программы осведомлённости по безопасности на предприятии.

Заключение

Современные системы безопасности с точки зрения разработки и эксплуатации страдают от следующих базовых проблем и недостатков:

1. Отсутствие эшелонированной и сбалансированной защиты [7-9] - системы опираются на один мощный слой защиты, при этом защищают возможные эквивалентные пути в различной степени.

2. Отсутствие понимания взаимодействия всей системы в целом [37] - фундаментальное противоречие между невозможностью и необходимостью одновременно осознавать систему на уровнях от строк программы до взаимодействия подсистем и аппаратуры.

3. Принцип "не самой слабой защиты" [8]- зачастую система проектируется не так, чтобы соответствовать требованиям, а так, чтобы быть не хуже, чем аналогичная система от конкурентов.

4. Принцип "никто не пойдёт на это" [8, 9] - некорректное применение или неприменение рискостоимостного анализа, когда определённая уязвимость не учитывается ввиду очень малой вероятности её эксплуатации злоумышленником.

5. Безопасность через скрытность (стеганография) [7-9, 15]- ослабленная защита на компоненте ввиду относительной сложности его нахождения извне.

6. Критерии наличия вместо критериев эффективности [7] - система проектируется исходя из принципа наличия (использования) определённых устройств, схем, подсистем, а не конкретных показателей, которых необходимо достичь.

7. Самоуверенность [8, 9] - отрицание того факта, что любая система имеет потенциальные недостатки и может быть скомпрометирована при наличии достаточных ресурсов.

8. Низкий уровень осведомлённости по безопасности [8, 9]- многих конечных пользователей не готовят к возможным атакам (в основном к атакам с применением социальной инженерии).

Всем этим проблемам так же подвержены и СКУД. Являясь лишь частью общей системы безопасности, они могут содержать огромное количество потенциальных уязвимостей, требуя комплексного целостного подхода при проектировании и эксплуатации. Но самой фундаментальной проблемой прямо относящейся к СКУД является то, что современные усилия по совершенствованию и стандартизации безопасности систем обходят стороной встраиваемые подсистемы многоуровневых систем, концентрируясь на более высокоуровневых компонентах, забывая, что безопасность является функцией от всей системы в целом, а не только от её отдельных частей.

Список литературы

1. Ворона В.А.,Тихонов В.А. "Системы контроля и управления доступом".-М.: Гор. линия-Телеком, 2010. - 272с.

2. S. Hasan Mirjalili, Arjen K. Lenstra Security Observance throughout the Life-Cycle of Embedded Systems, 2003 - 7 p.

3. Sri Parameswaran, Tilman Wolf "Embedded systems security—an overview", 2008 - 11 p.

4. Paul Kocher, Ruby Lee, Gary McGraw and oth. Security as a New Dimension in Embedded System Design, 2004 - 8 p.

5. Schneier B. "The Internet of Things Is Wildly Insecure — And Often Unpatchable" 2014 - 8 p.

6. Karl Koscher, Stephen Checkoway and oth. "Experimental Security Analysis of a Modern Automobile", 2010 - 16 p.

7. Garcia M.L. "The design and evaluation of physical protection systems" - USA: Elsevier Science, 2001. - 318 p.

8. Kevin D. Mitnick "The Art of Deception: Controlling the Human Element of Security ", 2003 - 352 p.

9. Kevin D. Mitnick, William L. Simon "The art of intrusion". Indianapolis: Wiley Publishing, 2005 - 291 p.

10. Smart card alliance "Physical access report", 2003.

11. Smart Card Alliance "Using Smart Cards for Secure Physical Access"2003 - 49 p.

12. Dacfey Dzung Martin Naedele "Security for Industrial Communication Systems" - 25 p

13. HID Global Best Practices in Access Control, 2008 - 7 p.

14. William MacGregor, Ketan Mehta, David Cooper Karen Scarfone "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)" - 71 p.

15. Michael Howard, David LeBlanc "Writing Secure Code, Second Edition" – Microsoft Press, 2002 – 732 p.

16. Смит, Ричард Э Аутентификация: от паролей до открытых ключей : Пер. с англ - М. : Вильямс, 2002 - 432 с.

17. Smart Card Alliance "Smart Cards and Biometrics" 2011 - 26 p.

18. R Sanchez-Reillo, L Mengibar-Pozo "Microprocessor Smart Cards with Fingerprint user Authentication" : Madrid, 2000 - 3 p.

19. Markus Ullmann, Ralph Breithaupt, Frank Gehring ""On-Card" User Authentication for Contactless Smart Cards based on Gesture Recognition" - 18 p.

20. Lawrence O' Gorman "Comparing Passwords, Tokens, and Biometrics for User Authentication" Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040

21. Department of Homeland Security Interagency Security Committee "Use of Physical Security Performance Measures", 2009 - 40 p.

22. Wayne Jansen "Directions in Security Metrics Research", Gaithersburg, 2009 - 35 p.

23. Steven M. Bellovin "On the Brittleness of Software and the Infeasibility of Security Metrics" ,IEEE security & privacy, 2009 - 3 p.

24. Gary Hinson "Seven myths about security metrics". - ISSA Journal, 2006 - 10 p.

25. Marianne S., Nadya Bartol, John Sabato "Security Metrics Guide for Information Technology Systems", 2006 - 99 p.

26. CIS "The CIS Security Metrics", 2010 - 175 p.

27. Marwan Abi-Antoun, Daniel Wang, Peter Torr "Checking Threat Modeling Data Flow Diagrams for Implementation Conformance and Security", 2006 - 21 p.

28. ISO/IEC 13335 "Information technology - Security techniques -Management of information and communications technology security", 2004-2007 - 198 p.

29. Information technology - Security techniques - Code of practice for information security management : ISO/IEC 27002:2005 - Действителен от 01.01.2005 - ISO/IEC - 90 с.

30. Eugene Lockett and other "Security aspects of smart cards" - San Diego state university, 2003 - 23 p.

31. Thomas S. Messerges, Ezzat A. Dabbish "Examining Smart-Card Security under the threat of Power Analysis Attacks", IEEE Transactions on computers 2002

32. Sergei P. Skorobogatov, Ross J. Anderson "Optical Fault Induction Attacks", 2005 - 12 p.

33. G.P. Hancke "Eavesdropping Attacks on High-Frequency RFID Tokens", IEEE Trans. on comp. 2009 - 28 p.

34. YongBin Zhou, DengGuo Feng "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing", 2000 - 34 p.

35. D. Genkin, A. Shamir, E. Tromer "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis", 2013 - 57 p.

36. Ayesha Khan "How to deal with social engineering": SANS, 2002 - 15 p.

37. Steve McConnell "Code Complete: A Practical Handbook of Software Construction, Second Edition", 2004 - 919 p.

Поступила в редколлегию 2.10.2013

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

АНАЛІЗ ИНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ КОНТРОЛЮ ФІЗИЧНОГО ДОСТУПУ З АУТЕНТИФИКАЦІЄЮ НА ОСНОВІ СМАРТ-КАРТ

Є.І. Подскальний, О.О. Галькевич, О.В. Желтухин

Розглядаються питання організації безпечного інформаційного обміну в СКФД . Оцінюється сучасний стан досліджень у даній сфері. Обговорюються основні компоненти таких систем та їх можливі уразливості , пропонуються рекомендації з організації стійких до атак систем . Розглядається можливість застосування сучасних метрик і методик ІБ до існуючих і проектованим СКФД . Особливо наголошується на необхідності формування та застосування цілісних підходів щодо забезпечення ІБ в розподілених автоматизованих системах безпеки .

***Ключові слова**: інформаційна безпека, СКФД (СКД, СКУД), системна безпека, ідентифікація та аутентифікація, протоколи обміну інформацією, смарт-карти.*

ANALYSIS OF INFORMATIONAL SECURITY OF PHYSICAL ACCESS CONTROL SYSTEMS WITH SMART-CARD BASED AUTHENTICATION

Ye.I. Podskalnyi, O.O. Halkevych, O.V. Zheltukhyn

The problems of secure informational exchange in PACS are considered. The modern state of researches in the sphere is assessed. The main components of such systems and their vulnerabilities are discussed; recommendations for attack resistant systems' implementations are given. Possibility of the application of modern metrics and methods of IS to existing systems or systems under development is considered. The need for creation and application of integral approaches to ensure IS in distributed automated security systems is especially noted.

***Key words:** informational security, PACS (ACS, ACAS), system security, identification and authentication, information exchange protocols, smart-cards.*