Потенциальные угрозы для сетей специального назначения

Б.С. ГОЛЬДШТЕЙН, зав. кафедрой СПбГУТ, доктор технических наук, профессор,
Н.А. СОКОЛОВ, главный научный сотрудник ЛО ЦНИИС, доктор технических наук

Исторически сложившимся научным центром по проблематики безопасности сетей связи всегда был и остается С.-Петербург с его научными центрами — СПбГУТ им. проф. М.А. Бонч-Бруевича, ЛОНИИС, "Красная заря", НИИДС и др. Эта работа проводилась сначала для ОГСТфС (Общегосударственной сети телефонной связи), потом для ЕАСС (Единой автоматизированной сети связи), ВСС (Взаимоувязанной сети связи), ЕСЭ (Единой сети электросвязи). Сегодня, по известным причинам, проблематике безопасности ЕСЭ РФ и построенных на ее основе сетей специального назначения связисты уделяют особое внимание. Поэтому редакция посчитала интересным попросить высказаться на эту тему своих постоянных авторов, участвовавших в системных проектах всех вышеупомянутых поколений отечественных сетей связи и в исследовании сетевых аспектов построения перспективных сетей связи различного назначения.

Введение

Термины "угроза", "безопасность" и им подобные все чаще встречаются в публикациях отечественных и зарубежных специалистов. Возникающие риски проявляются практически во всех сферах жизни современного общества, но особо критичны они для безопасности государства [1], под которой обычно понимается уровень его защищенности от внешних и внутренних угроз. С этой точки зрения актуальными становятся задачи устойчивого и безопасного функционирования современных сетей специального назначения (ССН). Для сетей подобного рода потенциальные угрозы уместно классифицировать по виду основных источников преднамеренного воздействия:

пользователи сети, включая эксплуатационный персонал;

программное обеспечение (ПО);

аппаратные средства (АС).

Для большинства ССН хорошо разработаны механизмы практического исключения (теоретически — радикальной минимизации) влияния источников первого вида. По этой причине ниже рассматриваются потенциальные угрозы, обусловленные преднамеренными воздействиями через программные продукты и аппаратные средства.

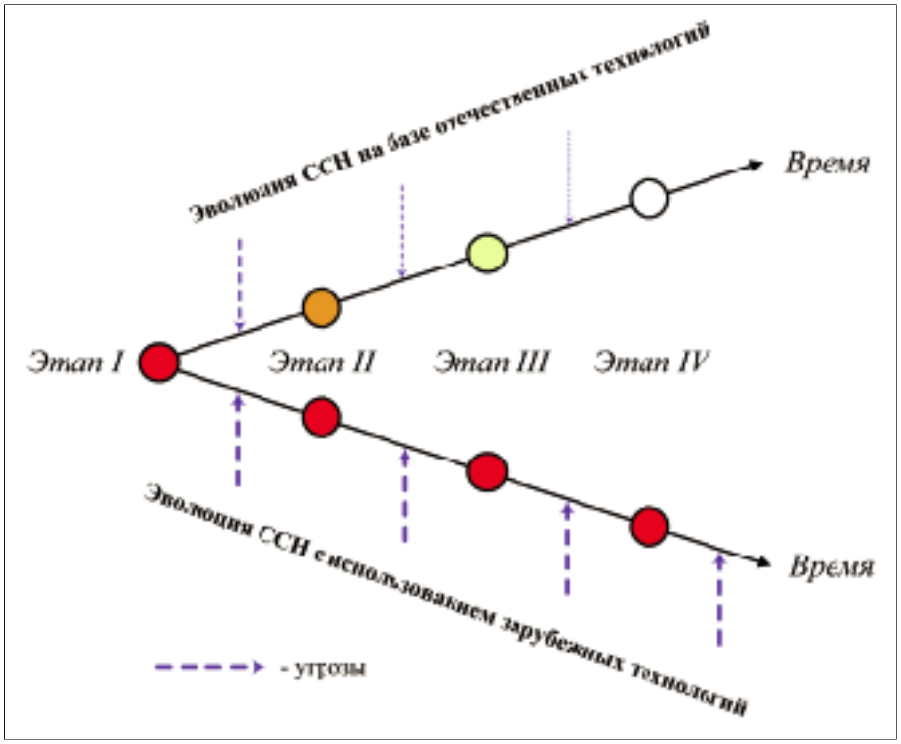


Рис. 1. Два основных сценария развития ССН

Сценарии создания и развития ССН

Создание и поэтапная эволюция ССН могут осуществляться по двум базовым сценариям. Эти сценарии иллюстрирует рис. 1 для четырех этапов эволюции ССН. Первый сценарий подразумевает эволюцию ССН с использованием зарубежных технологий и, как правило, технических средств. Второй сценарий основан на дальнейшем развитии ССН с поэтапным переходом на отечественные технологии, что подразумевает постепенное замещение импортного оборудования передачи, коммутации и обработки информации. Предложенную иллюстрацию следует рассматривать как формализованную схему развития ССН. Тем не менее, она позволяет изложить основные соображения, которым посвящена данная статья.

Динамика первого сценария в чем-то похожа на движение по дороге с заминированными участками. С ростом времени сложность мин замедленного действия (например, закладок в составе ПО) повышается. Их обнаружение носит вероятностный характер. В некоторых случаях принципы обнаружения мин определенного типа (как и ранее — закладок в составе ПО) могут быть разработаны после первого взрыва (проявление действия закладки). Поскольку технология минирования (скрытости закладок) постоянно совершенствуется, на всех этапах

уровень угроз предполагается идентичным (окраска этапа), и вероятность нанесения ущерба считается неизменной (толщина пунктирных линий).

Существенное отличие заключается в строительстве своего рода новой дороги, на которой — после наступления четвертого этапа — мин (проблем любого технического характера) не будет в принципе. По этой причине каждый этап отображается кружком более светлой окраски, а толщина линий, характеризующая потенциальный ущерб, снижается. Процесс функционирования ССН на четвертом этапе ее развития будет осуществляться с максимальным уровнем безопасности.

Нет необходимости доказывать целесообразность развития ССН на базе отечественных технологий. Важной задачей следует считать разработку таких принципов эволюции ССН, которые позволяют минимизировать известные и прогнозируемые риски, а также сократить время перехода к максимальному уровню безопасности. Для достижения этих целей следует провести анализ практических примеров потенциальных угроз, порождаемых применением импортных технических средств, и разработать рациональные принципы перехода к ССН, которой присущ максимальный уровень безопасности.

Практические примеры потенциальных угроз

В технической литературе и во всемирной паутине можно найти множество публикаций, посвященных потенциальным угрозам различного рода. Некоторые из этих публикаций столь несерьезно трактуют факты, что у читателей складывается ложное впечатление об уровне реальной опасности. Определенную лепту вносят рекламные материалы, чрезмерно преувеличивающие значимость конкретных продуктов, которые позволяют избежать угроз любого вида. По этим причинам представляется актуальным комплексный анализ угроз, который не ставит целью рекламировать какой-либо продукт и запугивать участников инфокоммуникационного рынка мифическими проблемами. Тем не менее, проводя такой анализ, следует помнить, что если рассматриваемая возможность найти брешь в системе безопасности действительно существует, то она рано или поздно будет использована.

Комплексный анализ угроз — предмет для объемной монографии. В этой статье кратко рассматривается ряд примеров, иллюстрирующих, по мнению авторов, те наиболее типичные ситуации, которые представляют потенциальные угрозы для ССН.

В статье [2] изложены результаты очень простого эксперимента, проведенного аудиторской компанией Secure Network Technologies. Сотрудники этой компании до начала рабочего дня разбросали в проверяемой организации 20 привлекательных флеш-накопителей, подключаемых к разъему USB. В течение рабочего дня было подобрано 15 флеш-накопителей; все они были подключены к компьютерам проверяемой организации. В каждый накопитель был предварительно записан набор файлов с изображениями. Одно из них содержало программу, запускаемую при открывании файла. Пока рассматривалась эта картинка, программа, запущенная “ложным” изображением, устанавливала связь с компьютером, через который создавался доступ к информационным ресурсам проверяемой организации.

Первоначальный вывод о сути проблемы заключается в стандартной ссылке на “человеческий фактор”. С другой стороны, следует помнить, что флеш-накопители могли попасть к сотрудникам проверяемой компании официально. Это значит, что одним из источников угроз, внедрение которого не требует серьезных усилий со стороны злоумышленника, остаются накопители, подключаемые к персональным компьютерам. Более того, этот способ нарушения безопасности постоянно совершенствуется. Типичный пример такой “эволюции” — размещение в корпусе флеш-накопителей миниатюрных передатчиков для извлечения необходимой информации. Интересные сведения о подобных разработках приводятся в публикациях Эдварда Сноудена.

В феврале 2005 г. у бизнесмена Джо Лопеса хакеры украли с банковского счета 90 тыс. долл. [3]. В результате расследования выяснилось, что в компьютер Джо Лопеса попал вирус, который фиксировал все нажатия на клавиатуре персонального компьютера. Эта возможность позволила хакерам узнать пароль и логин, необходимые для взаимодействия с банком через Интернет.

Подобные возможности реализуются при помощи так называемых “клавиатурных шпионов”, более известных как кейлоггеры. Данный термин образовался как “калька” от слова “keylogger” в английском языке — регистратор нажатий клавиш. Технология несанкционированного доступа к информации при помощи “клавиатурных шпионов” также постоянно совершенствуется. Информация о “новинках” регулярно появляется и в Интернете, и в технической литературе.

Методы борьбы с подобными угрозами известны. Они также постоянно совершенствуются. Аналогичная ситуация характерна и для других видов несанкционированного доступа — включения устройств в разрыв кабелей, размещения аппаратных закладок внутри системного блока персонального компьютера или сервера, съема информации за счет обработки сигналов в виде акустических и электромагнитных излучений, а также других противоправных приемов.

Подобные потенциальные угрозы обнаруживаются сравнительно простыми методами (конечно, данное утверждение следует воспринимать с некоторой осторожностью). Иная ситуация складывается с “высокотехнологичными” угрозами. В частности, в монографии [4] рассматриваются задачи, возникающие с проверкой подлинности интегральных схем для обнаружения аппаратных закладок. Очевидно, что методы ликвидации угроз, приемлемые для приведенных выше примеров, не будут эффективными.

Сложность обнаружения "высокотехнологичных" угроз возрастает не в разы, а на порядки. Ситуация усугубляется в тех случаях, когда приходится проверять не набор интегральных схем, а готовые аппаратно-программные средства — маршрутизаторы, контроллеры и другие элементы ССН. При использовании импортной элементной базы и, тем более, зарубежных аппаратно-программных средств достоверность обнаружения недокументированных возможностей (НДВ) никогда не будет приемлемой. Процесс повышения достоверности обнаружения НДВ можно исследовать методами, принятыми в теории игр [5]. В этой игре первый ход (а иногда — и выбор правил) всегда остается за злоумышленником.

Поучительный пример реализации НДВ приведен в [6]. Международная группа преступников сумела внедрить нетривиальную шпионскую закладку во множество современных устройств ввода PIN (персонального идентификационного номера), работающих с банковскими карточками класса "Chip & PIN". Карточки этого типа содержат чип (микропроцессор), на котором хранится часть данных. Считается, что скопировать их сложнее, чем при использовании банковских карточек с магнитной полосой.

Выявленная сеть шпионских закладок позволяла преступникам в течение не менее девяти месяцев красть деньги с банковских счетов. Общая сумма хищений исчисляется десятками миллионов долларов. Технология этого изощренного преступления любопытна и сама по себе. Не менее интересен тот факт, что год назад серьезнейшая слабость в защите современных устройств ввода PIN (они известны также по аббревиатуре PED — PIN entry device) уже была обнаружена. Специалисты из лаборатории компьютерной безопасности Кембриджского университета, обнаружившие "дыру", оповестили все заинтересованные инстанции, что в схемах терминалов есть участок, где конфиденциальные данные проходят в незашифрованном виде. Подсоединившись к такому тракту, злоумышленник может похитить все реквизиты карты, PIN-код доступа и изготовить полноценную копию — клон.

В ответ на свои предупреждения исследователи получили отписки, трактующие их работу как далекие от жизни "лабораторные эксперименты". Есть своеобразная ирония в картине, открывшейся вместе с выявлением закладок в PED. Она продемонстрировала, как выглядят реальные угрозы для защиты данных в сегодняшнем мире. В частности, до сих пор неизвестно, где и как встраивались закладки в PED-терминалы — непосредственно в процессе сборки в Китае или же на складах перед отправкой получателю. В любом случае, закладка внедрялась профессионально, никаких внешних следов на корпусе или упаковке устройств не оставалось, поэтому у получателей терминалов не было ни малейших сомнений в "чистоте" своих аппаратов.

Закладка была аккуратно прикреплена к днищу системной платы PED и подключена к тому ее участку, где данные со считываемых карт проходят в открытом виде перед попаданием в криптомодуль терминала. В функции закладки, кроме копирования реквизитов карты и PIN-кода доступа, входят шифрование, хранение в собственном буфере памяти и отправка злоумышленникам всех собранных данных при помощи модуля сотовой связи. Как было установлено, серверы, на которые утекала информация и откуда поступали команды, управляющие всей сетью закладок, находятся в пакистанском городе Лахор.

Похищенные данные использовались для изготовления карточек-клонов с магнитной полосой, пригодных для покупок или снятия наличных в банкоматах тех стран, где еще не перешли на технологию "Chip & PIN". Делалось все чрезвычайно аккуратно. Частота соединений с "центром" зависела от количества считанных карт и оплаченных с них сумм. Поэтому сессии связи могли осуществляться и раз в день, и реже одного раза в неделю. Кроме того, сервер мог регулировать работу каждой закладки после очередного опустошения буфера за счет, например, выдачи команд типа "копировать каждую десятую карту" или "только карты Visa Platinum". Наконец, краденые реквизиты не сразу пускались в дело, а "мариновались", по меньшей мере, пару месяцев, чтобы максимально затруднить выявление мест похищения.

Понятно, что в таких условиях выявить сам факт существования закладки было чрезвычайно сложно. Хотя подробности этой истории попрежнему хранятся в тайне, известно, что первыми неладное заподозрили специалисты Master Card. Один из пострадавших клиентов компании уверенно утверждал, что использовал свою карточку только в одном-единственном месте. Более того, он смог это убедительно доказать. Поскольку мошеннические изъятия по той же карте проходили из-за рубежа, следствию не оставалось ничего другого, как подробнее изучить PED-терминал в торговой точке. Стоит ли говорить, какой сюрприз их ждал?

Коль скоро внешним осмотром, без вскрытия терминалов, обнаружить модуль закладки невозможно, то самым простым способом выявления "шпиона" стало взвешивание считывателей карточек на весах. Отличие веса аппарата от стандартного на 80 — 100 г стало главным признаком для выявления скомпрометированных устройств. Поэтому все последние месяцы по Европе колесили группы инспекторов, занятых тщательным взвешиванием имеющихся в кассах магазинов PED-терминалов. На сегодняшний день, по меньшей мере, в пяти странах — Бельгии, Великобритании, Дании, Голландии и Ирландии — обнаружено больше сотни таких закладок, исправно отправлявших данные на серверы в Пакистан. Точка в этой истории, разумеется, еще не поставлена.

Решения, использованные злоумышленниками в финансовой сфере, следует учитывать при построении и развитии ССН. В частности, необходимо обратить внимание, по крайней мере, на три аспекта. Во-первых, должны контролироваться участки пространства, в которых можно скрытно разместить различные средства, реализующие функции

закладок. Во-вторых, надо устранить те участки в тракте обмена данными, где информация не защищена с требуемым уровнем. В-третьих, следует учесть применение злоумышленниками изощренных алгоритмов хищения информации, затрудняющих процесс поиска НДВ.

Принципы достижения максимального уровня безопасности

Достижение максимального уровня безопасности ССН обеспечивается за счет замещения импортных средств передачи, коммутации и обработки информации, начиная с тех аппаратно-программных средств, которым присущ максимальный уровень потенциального риска. Ранжирование элементов ССН по уровню потенциального риска выполняется группой экспертов, наделенной полномочиями принятия решений [7], или иным методом, который приемлем для решения данной задачи.

Принципы достижения максимального уровня безопасности могут быть представлены при помощи алгоритма, приведенного на рис. 2. Этот алгоритм основан на выполнении последовательности операций, суть которых определяется их названиями.

Предлагаемый алгоритм включает проверку ожидаемого уровня безопасности — ромб в нижней части модели. Выполнение необходимых операций зависит от характеристик ССН и предъявляемых к ней требований. В общем случае возникает нетривиальная задача, плохо поддающаяся формализации. Методика решения подобной задачи — предмет отдельного исследования. Левый нижний блок введен в состав алгоритма в качестве необходимой операции для решения этой задачи.

Название правого нижнего блока следует трактовать как приостановку работы алгоритма после успешного решения текущей задачи на период времени τ. Все операции в составе алгоритма следует повторять для контроля способности ССН противостоять новым видам угроз. Этот процесс должен осуществляться после завершения каждого этапа модернизации ССН и при возникновении

Рис. 2. Алгоритм достижения максимального уровня безопасности ССН

каких-либо сомнений в обеспечении заданного уровня безопасности. Желательно также периодически активировать алгоритм между этапами эволюции ССН.

Заключение

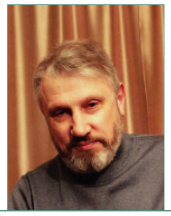
Читателям, которые не сталкивались с реальными проблемами безопасности, раздел статьи “Практические примеры потенциальных угроз” может показаться набором “страшилок”, но авторы ничего не придумывали. Просто такова реальность. Большинство людей, в силу своих психологических установок, не хочет задумываться о глобальных рисках [8].

Существование угроз комплексной (не только информационной) безопасности телекоммуникационных сетей подтверждается публикацией серьезных монографий отечественных и зарубежных специалистов [4, 9 — 11]. Для сложных и важных систем, к которым следует отнести ССН, предотвращение угроз комплексной безопасности — одна из самых актуальных задач. Нет никакого сомнения, что без перехода на полностью отечественные технические средства для построения, технической эксплуатации и долгосрочного развития ССН задачи комплексной (включая, в первую очередь, информационную) безопасности решить невозможно.

Литература

1. Макаренко Д.И., Хрусталев Е.Ю. Концептуальное моделирование военной безопасности государства. – М.: Наука, 2008.
2. Лемос Р. Флэш-накопители – новый источник опасности. – PCMagazine, 28 января, 2007.
3. Гребенников Н. Клавиатурные шпионы. Принципы работы и методы обнару-жения.Часть I.
4. Tehranipoor M., Salmani H., Zhang X. Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection. – Springer, 2014.
5. Оуэн Г. Теория игр. – М.: Вузовская книга, 2008.
6. http://old.computerra.ru/own/378826.
7. Ларичев О.И. Теория и методы принятия решений. – М.: Логос, 2002.
8. Воробьев Ю.Л., Малинецкий Г.Г., Махутов Н.А. Управление риском и устойчивое развитие. Человеческое измерение. – Общественные науки и современность, № 6, 2000.
9. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. Том 1: Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая Линия – Телеком, 2006.
10. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. Том 2: Средства защиты в сетях. М.: Горячая Линия – Телеком, 2008.
11. Kim D., Solomon M.G. Fundamentals of Information Systems Security. – Jones & Bartlett Publishers, 2013.

Борис Соломонович ГОЛЬДШТЕЙН
bgold@niits.ru



Николай Александрович СОКОЛОВ
sokolov@niits.ru