АРХИТЕКТУРНЫЕ УЯЗВИМОСТИ МОДЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

М.В. Буйневич, доктор технических наук, профессор;
О.В. Щербаков, доктор технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России.
А.Г. Владыко, кандидат технических наук;
К.Е. Израилов.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Рассматриваются концептуальные модели современных цифровых телекоммуникационных сетей, включая SDN. Анализируются архитектурные уязвимости телекоммуникационных сетей применительно к рассмотренным моделям. Приводятся результаты их сравнительного анализа в табличной форме.

Ключевые слова: телекоммуникационные сети, концептуальные модели, архитектурные концепции, уязвимости, сравнительный анализ, SDN

ARCHITECTURAL VULNERABILITY MODELS OF NETWORKS

M.V. Buinevich; O.V. Shcherbakov.
Saint-Petersburg university of State fire service of EMECOM of Russia.
A.G. Vladyko; K.E. Izrailov.
Saint-Petersburg state university of telecommunication named after prof. M.A. Bonch-Bruevich

The conceptual models of the modern digital networks including SDN are considered. Architectural vulnerability of networks are analyzes in relation to the models. The results of their comparative analysis are presented in tabular form.

Keywords: network, conceptual model, architectural concepts, vulnerabilities, comparative analysis, SDN

Широкомасштабное использование цифровых телекоммуникационных сетей (ТКС) в современном мире сопровождается ростом количества инцидентов информационной безопасности, для предупреждения и нейтрализации которых требуется как комплексное применение защитных мер, так и опережающие научно-технические разработки [1]. Последние предполагают всестороннее исследование одной из основных причин появления указанных инцидентов – уязвимостей сетей [2]. Одним из наименее изученных и обделенных вниманием научной общественности являются так называемые архитектурные уязвимости, скрывающиеся и проявляющие себя в концептуальных особенностях построения ТКС [3].

И если для борьбы со средне- и низкоуровневыми уязвимостями специалистами накоплен достаточный арсенал методов и средств [4, 5], то для эффективной борьбы с высокоуровневыми уязвимостями в первую очередь необходимо исследовать концептуальные модели, лежащие в основе архитектуры известных ТКС. Эти модели достаточно подробно изложены в работе [6], но для выявления и локализации высокоуровневых уязвимостей достаточно определенной степени детализации описания с акцентом на особенности архитектуры.

Концептуальные модели ТКС

Концептуальная модель IMS (от англ. IP Multimedia Subsystem), изначально создаваемая как спецификация для передачи на базе протокола IP мультимедиа контента по ТКС, определяет сетевую архитектуру на основе пакетной транспортной сети, поддерживая доступ и реализацию большинства инфокоммуникационных услуг. Основной услугой считается двухсторонняя аудио и видео связь. Основополагающие функциональные возможности IMS определяются как поддержка QoS (от англ. Quality of Service) и взаимодействие с сетью Internet, инвариантность доступа к IMS в виде применения любых технологий доступа, эффективное внедрение и управление новыми услугами без существенных затрат ресурсов, широкие возможности роуминга, уровень безопасности не меньше канальных сетей коммутации, гибкое начисление тарифов провайдером связи. IMS обладает хорошей масштабируемостью своих решений по причине частичного построения на базе информационно-технологической облачной концепции [7]. Концепция широко используется операторами связи (ОС), в особенности мобильными; не исключением является и практика ее применения в ведомственном сегменте (ВС).

Архитектурная модель IMS делится на три плоскости: транспортный уровень, уровень управления и уровень приложений. Транспортный уровень содержит элементы, обеспечивающие подключение к сети и транспортировку данных пользователей, а именно: динамическое назначение IP-адресов, управление ресурсами, взаимообратные преобразования информации между сетями с коммутацией каналов и с IP-пакетами, поддержание сеансов мультимедиа и др. Уровень управления обеспечивает регистрацию пользователей и управление их сеансами связи, для чего содержит соответствующие функциональные объекты, поддерживающие базу данных профилей пользователей, управляющие медиашлюзами и взаимным преобразованием сигналов сетей ОКС-7 и IMS, осуществляющие выбор сети и маршрутизацию сеанса между абонентом канальной сети и IMS, а также взаимодействие с IP-сетями и др. Уровень приложений является верхним уровнем архитектуры и состоит из серверов, предоставляющих соответствующие услуги, такие как традиционная VoIP (от англ. Voice over IP), услуги интеллектуальных сетей, мультимедиа услуги на базе IP и др.

Ключевой особенностью рассмотренной архитектуры является то, что она строится на стандартной основе, обеспечивая функциональную совместимость IP и IMS.

Архитектурная концепция IN (от англ. Intelligent Network) обозначает архитектурную концепцию, применимую к сетям электросвязи и предусматривающую строго определенный набор гибко используемых средств; последние способствуют созданию и введению в сети связи новых услуг, включая управляемые пользователем. Концепция базируется на основополагающих свойствах, которыми должны обладать средства реализации и предоставления IN-услуг: независимость от вида услуг, структуры сети и производителя оборудования.

Перечни IN-услуг (и их составных элементов) получили название наборов возможностей – CSs (от англ. Capability Sets). В качестве общей для всех CSs модели описания архитектуры IN была предложена концептуальная модель INCM (от анг. IN Conceptual Model), отражающая эту архитектуру в разных плоскостях, дающих разную степень детализации. Модель содержит четыре расположенные друг над другом плоскости, каждая из которых является абстрактным представлением (со своей степенью детализации) тех возможностей, которыми обладает сеть концепции IN.

Верхняя плоскость модели – плоскость услуг представляет услуги так, как они «видны» конечному пользователю; такое представление не содержит информации, относящейся к способу и деталям реализации услуги в сети. На глобальной функциональной плоскости «появляется» сеть IN в виде единого функционального объекта. На этой плоскости представлены независимые от услуг конструктивные блоки и некие условные точки – обращения и возврата, представляющие собой функциональные интерфейсы.

«Цепочки» блоков, начинающиеся в одной и заканчивающиеся в другой точке, представляют различные IN-услуги. На распределенной функциональной плоскости IN-услуги реализуются соответствующими программными средствами распределенным образом; каждый функциональный объект, определенный на этой плоскости, может выполнять целый ряд определенных для него действий. Физическая плоскость представляет физические элементы; этими элементами могут быть коммутационные станции, специализированные компьютеры или базы данных.

Интегрированная архитектура TINA – это интегрированная архитектура, применимая к любым типам услуг и сетей, но нацеленная в основном на поддержку предоставления услуг мобильности, а также широкополосных и информационных услуг. TINA возникла как конвергенции двух основных телекоммуникационных направлений: IN и TMN (от англ. Telecommunications Management Network).

Архитектура базируется на следующих принципах: представление системы в виде набора объектов; распределение программных компонентов по разным частям сети в соответствии как с требованиями пользователя, так и с реальными сетевыми возможностями; независимость программных компонентов друг от друга, что гарантирует возможность замены любого компонента без модификации смежных компонентов; разделение приложений и среды, в которой эти приложения функционируют и пр. Принципы TINA нацелены на отделение вполне стабильных функций оперативного и эксплуатационного управления от требующих гибкости и динамичности функций разработки услуг и быстро меняющихся сетевых технологий.

В архитектуре TINA выделяют четыре основных уровня. Первый – уровень аппаратных ресурсов, к которому относят процессоры, память, коммуникационные и другие периферийные устройства. Второй – уровень среды выполнения, включающий в себя программные средства, обеспечивающие работу TINA-приложений: операционную систему, средства обмена данными и другие программные утилиты. Третий – уровень среды распределённой обработки DPE (от англ. Distributed Processing Environment), обеспечивающий технологически независимое представление аппаратных ресурсов, облегчая разработку и свободу перемещения TINA-компонентов. И четвертый – уровень собственно TINA-приложений.

Уязвимости архитектурных решений ТКС

Те или иные архитектурные решения, заложенные в моделях ТКС, являются источником различных уязвимостей. Эти уязвимости могут быть порождены как чисто архитектурными особенностями ТКС (например, топологическими или системотехническими), так и производными от них.

Проанализируем архитектурные уязвимости (АУ) применительно к рассмотренным моделям ТКС (для случая IMS – опираясь на практику использования в «связке» ОС+ВС).

АУ-1. Ошибки в протоколах и механизмах взаимодействия компонентов ТКС. Уязвимостью в данном случае является наличие логических ошибок (как случайных, так и преднамеренных) в протоколах и механизмах взаимодействия. Включает в себя также ошибки в программном обеспечении (ПО), реализующем указанные области. Известно, что ПО, реализующее функционирование ОКС-7, зачастую содержит ошибки [8]. Причинами этого является постепенное устаревание данной системы, ее низкоуровневость и «запутанность». Также, слабыми местами ОКС-7 является плохая устойчивость к перегрузкам (например, вследствие DDoS-атак) и «распространению отказов» (например, вследствие возникновения поврежденных пакетов или процедурных ошибок при замене версий ПО), что можно отнести к «логическим ошибкам переполнения и производительности».

Данная система сигнализации применяется как в ОС, так и в IN для поддержки INAP – из этого следует потенциальное наличие в них данной уязвимости. В TINA для

взаимодействия компонентов применяется перспективный и развивающийся механизм CORBA, который является более «объектным» и высокоуровневым, а значит удобным и надежным для проектирования, реализации и поддержки.

АУ-2. Ошибки в процедурах взаимодействия пользователей, операторов и администраторов с аппаратно-программным обеспечением ТКС. Уязвимостью является наличие ошибок (как случайных, так и преднамеренных) в процедурах взаимодействия пользователей, операторов и администраторов с аппаратно-программным обеспечением. Возникает, как правило, из-за применения специально разработанных, сложных и не отлаженных на других ТКС процедур.

Технические недостатки узлов сети ОКС-7, связанные с отсутствием средств контроля доступа, обнаружения перегрузок, проверки прав доступа, в некоторой мере сглаживаются административными процедурами в присоединенной сети. Однако их применение зачастую приводит к дорогостоящим процедурным ошибкам, связанным с критичностью правильности принимаемых человеком решений. К таким же ошибкам может приводить и разработка специализированных процедур по обслуживанию взаимодействия ТКС в нестандартных ситуациях.

Такие специализированные процедуры применяются в ОС и IN, например, для дополнительной поддержки авторизации, аутентификации и взаимодействия с другими сетями (в случае ОС+ВС). Архитектура TINA же разрабатывалась как главный инструмент конвергенции услуг IN и TINA, последняя из которых является концепцией, подразумевающей, в частности, ряд профилактических работ, направленных на поддержание сети в работоспособном состоянии. Эти работы выполняются с помощью системы эксплуатации и технического обслуживания сети. При этом сама TINA разрабатывалась еще и как унифицированный способ управления разнородными сетями. Также в архитектуре TINA изначально предполагается использование механизмов авторизации и аутентификации.

АУ-3. Ошибки согласования методов обеспечения информационной безопасности для разных компонентов сети. Уязвимостью здесь является наличие ошибок, возникающих в результате взаимодействия различных методов обеспечения безопасности. В случае наличия двух разнородных сетей, их безопасностью могут заниматься различные организации, при этом делая методы ее обеспечения закрытыми или не предоставляя полную информацию о них друг другу. Это может приводить к ошибкам согласования применяемых методов. При этом для одной из сетей возможно потребуется разработка и внедрение дополнительных методов защиты, плохо согласующихся с существующими, что также может привести к появлению ошибок в их работе.

Такая потенциальная ситуация несогласования имеет место в частном случае в ВС (при наличии ОС и наоборот) и в общем случае в IN (наличие любой другой сети со своими методами обеспечения безопасности, например Internet). Принципами TINA является ее применимость к любым типам сетей и услуг, что, в частности, означает возможность согласования их методов обеспечения безопасности уже на этапе проектирования.

АУ-4. Наличие встроенных мер обеспечения безопасности информации: отсутствие аутентификации, авторизации, шифрования, а также наличие ошибок в дополнительных средствах (межсессионные протоколы).

Уязвимостью является как отсутствие встроенных мер аутентификации, авторизации и шифрования, так и наличие ошибок в дополнительных средствах. Приведенные меры являются основными для обеспечения безопасности информации в ТКС. Их отсутствие при наличии доступа к сети извне, является серьезной уязвимостью.

Протокол INAP (прикладная часть интеллектуальной сети), являющийся частью IN и базирующийся на ОКС-7, не имеет таких встроенных мер обеспечения безопасности. В ОС, также использующем ОКС-7, данные меры были разработаны отдельно. В случае TINA меры уже встроены в архитектуру или могут быть в рамках нее реализованы, поскольку взаимодействие построено на базе механизма взаимодействия CORBA, протокол которого поддерживает данные меры. Также для их поддержки в архитектуру услуг TINA введена

концепция «сессия», объединяющая в себя процесс выполнения совместно определенных действий компонентами ТКС в определенный промежуток времени.

Таким образом, IN не имеет указанных встроенных мер обеспечения безопасности информации, в ОС+ВС данные меры реализовывались отдельно, а в TINA они заложены в архитектуру. Однако в последней это приводит к появлению сессионного механизма, что может являться источником дополнительных ошибок.

АУ-5. Открытость внутренних и пограничных компонентов ТКС для доступа извне с возможностью модификации аппаратно-программных средств ТКС нарушителем. Уязвимость возникает по причине наличия доступа нарушителя извне к внутренним компонентам ТКС (пусть и через внешние защищенные интерфейсы). Возможность получения доступа к внутренним компонентам ТКС извне возникает в случае ее взаимодействия с внешними сетями и недостаточной защиты от атак из них.

В случае ОС и IN такой доступ существует, поскольку ТКС взаимодействуют с другими сетями. Они базируются на ОКС-7, разработанным для закрытых сетей, а значит, их внутренние компоненты могут быть подвержены атакам. TINA изначально разрабатывалась для работоспособности в условиях разнородных сетей.

Таким образом, все модели позволяют получать доступ к внутренним компонентам ТКС и производить атаку. Однако в TINA такой доступ и средства защиты от соответствующих атак могут быть заложены в архитектуру, что сильно снижает степень уязвимости.

АУ-6. Ошибки в результате развертывания и модификации услуг, расширения возможностей ТКС. Уязвимость возникает по причине появления ошибок вследствие расширения ТКС, например, путем добавления или развития предоставляемых услуг. Вероятность появления данного типа ошибок напрямую связана с эффективностью создания новых услуг (сложностью самого процесса создания, необходимостью в модификации существующих отлаженных услуг, степенью трудоемкости и т.п.).

В ОС, как и в IN, поддержка расширяемости ограничена возможностями протоколов ОКС-7 и INAP. Таким образом, любое расширение данных ТКС, выходящее за рамки возможностей протоколов, связано с необходимостью их модификации и будет приводить к возникновению ошибок. Принципы TINA нацелены на отделение вполне стабильных функций оперативного и эксплуатационного управления от требующих гибкости и динамичности функций разработки услуг и быстро меняющихся сетевых технологий. TINA имеет хорошую расширяемость, благодаря среде распределенной обработки DPE, что упрощает реализацию новых услуг. При этом каждая новая услуга может быть создана на основе предыдущей, уже опробованной и отлаженной.

АУ-7. Ошибки взаимодействия ТКС с существующими системами. Уязвимость возникает в результате ошибок организации взаимодействия ТКС с существующими системами. Любое плохо согласованное взаимодействие разнотипных сетей может приводить к появлению ошибок на различных уровнях (архитектурных, логических, физических). Заложенные в архитектуре принципы поддержки разнородных сетей позволяют снизить вероятность появления таких ошибок и последующий ущерб. Например, отсутствие средств шифрования в архитектуре приводит к необходимости использования дополнительного уровня защиты информации, передаваемой между соединенными сетями; такое усложнение механизма обмена влечет к потенциальным ошибкам в их взаимодействии. Изначально только TINA разрабатывалась для работы с любым типом услуг и сетей. ОС и IN требуют разработки дополнительных согласующих устройств и протоколов взаимодействия как потенциальных источников ошибок.

АУ-8. Неэффективные механизмы обнаружения и устранения ошибок ТКС. Уязвимость возникает в результате отсутствия эффективных механизмов обнаружения и устранения ошибок ТКС и, по сути, отражает (не)способность архитектуры бороться с другими возникающими ошибками (уязвимостями). Эффективность обнаружения и устранения ошибок ТКС напрямую связана с выбранной парадигмой, используемой

архитектурой: чем на более «запутанных» уровнях, объектах и механизмах взаимодействия строится архитектура, тем более трудоемкими и сложными являются механизмы борьбы с ошибками в ней.

OC и IN по сравнению с TINA построены на более сложных для реализации и поддержки архитектурах. Например, в качестве принципов организации интерфейсов в первых используются сообщения. Вследствие этого процедурные ошибки (ошибки синхронизации) зачастую приводят к такому «странному» поведению системы, по которому определение причин крайне затруднено. В случае TINA упрощение разработки и поддержки обусловлено ее «заточенностью» на объектно-ориентированное программирование (в частности использование среды распределенной обработки DPE). Принципами организации интерфейсов являются объекты и методы, а для борьбы с процедурными ошибками синхронизации может применяться концепция сессии. Архитектура TINA определяет понятные модели отображений и средств описания, используемых для разработки телекоммуникационных сетей, что позволяет избавиться от потенциальных ошибок уже на этапе проектирования.

Проанализированные архитектурные уязвимости рассмотренных моделей ТКС сведены в таблицу, где: «+» – уязвимость присутствует; «+/–» – уязвимость присутствует частично, или степень риска невелика; «–» – уязвимость отсутствует.

Таблица

Архитектурная уязвимость			Модель ТКС		
Усл. №	Сущность		IMS	IN	TINA
АУ-1	Ошибки в протоколах и механизмах взаимодействия компонентов ТКС		+	+	–
АУ-2	Ошибки в процедурах взаимодействия пользователей, операторов и администраторов с аппаратно-программным обеспечением ТКС		+	+	–
АУ-3	Ошибки и несогласованные методы обеспечения информационной безопасности для разных компонентов сети		+	+	–
АУ-4	Встроенные меры обеспечения безопасности информации	отсутствие средств аутентификации, авторизации, шифрования	+/–	+	–
		наличие ошибок в дополнительных средствах (межсессионные протоколы)	–	–	+
АУ-5	Открытость внутренних и пограничных компонентов ТКС для доступа извне с возможностью модификации аппаратно-программных средств ТКС злоумышленником		+	+	+/–
АУ-6	Ошибки в результате развертывания и модификации услуг, расширения возможностей ТКС		+	+	–
АУ-7	Ошибки взаимодействия ТКС с существующими системами		+	+	–
АУ-8	Неэффективные механизмы обнаружения и устранения ошибок ТКС		+	+	+/–

Модель и архитектурные уязвимости SDN

За рамками анализа остались АУ принципиально нового класса ТКС – программно-конфигурируемых сетей, как по причине ограниченного объема статьи, так и вследствие дефицита существующих знаний по этому вопросу. Построенные по идеологии SDN (от англ. Software-defined Networking) эти ТКС отличаются от традиционных сетевых инфраструктур за счет существенного переосмысления отношений между уровнем данных и уровнем управления сетевого устройства. Наиболее распространенным протоколом для них сейчас является OF-протокол (от англ. OpenFlow). В OpenFlow правила потока определяют базовые инструкции, которые регулируют пересылку, изменение или удаление каждого пакета, который попадает в SDN-коммутатор. Уровень управления в коммутаторе

упрощен, коммутатор только передает статистику и обращается за новыми правилами потоков к внешнему SDN-контроллеру.

В архитектуре OpenFlow контроллер находится выше SDN-коммутаторов, обычно реализуемых на более дешевом оборудовании. Контроллер содержит логику определения, обновления и адаптации правил потоков. Контроллер может взаимодействовать с несколькими коммутаторами одновременно, он может распределить набор согласованных правил потоков через коммутаторы для прямой маршрутизации или оптимизировать туннелирование, что позволяет значительно повысить эффективность транспортных потоков. Контроллер также предоставляет программный интерфейс API (от англ. Application Programming Interface), позволяющий разрабатывать OF-приложения, которые реализуют логику, необходимую, чтобы сформулировать правила потоков [9].

С одной стороны, такой подход дает большую гибкость к управлении сетью и существенно упрощает администрирование единой точки управления маршрутизацией потоков данных для множества коммутаторов в сети. С другой стороны, появление новых технологий управления сетью всегда сопровождается появлением новых АУ. В результате потенциальные потребители таких технологий не всегда могут оценить безопасность заявленных разработчиками технологических возможностей [10].

Результаты сравнительного анализа архитектурных уязвимостей рассмотренных концептуальных моделей современных и перспективных ТКС позволяют сделать вывод, что в условиях возрастающего уровня кибератак на цифровые сети наименее уязвимой может считаться ТКС, построенная согласно концепции TINA.

Программно-конфигурируемые сети гипотетически предоставляют уникальную возможность для эффективного выявления и сдерживания АУ, позволяя интегрировать составные приложения по обеспечению информационной безопасности в крупных сетях. Однако данный вопрос, в силу своего объема и отсутствия достаточной Best Practice, требует отдельного исследования и будет более подробно рассмотрен в последующих работах авторов.

Литература

1. Буйневич М.В. Информационная безопасность и защита информации. СПб.: СПбГИЭУ, 2011. 174 с.

2. Организационно-техническое обеспечение устойчивости функционирования и безопасности сетей связи общего пользования / М.В. Буйневич [и др.]. СПб.: Изд-во: СПбГУТ, 2013. 144 с.

3. Израилов К.Е. Архитектурные уязвимости программного обеспечения. «ИНЖЭКОН-2013»: тез. докл. VI Науч. конгресса студентов и аспирантов. СПб.: СПбГИЭУ, 2013. С. 35.

4. Buinevich M., Izrailov K. Method and Utility for Recovering Code Algorithms of Telecommunication Devices for Vulnerability Search. 16th International conference on advanced communication technology. 2014. Pp. 172–176.

5. Buinevich M., Izrailov K., Vladyko A. Method for Partial Recovering Source Code of Telecommunication Devices for Vulnerability Search. 17th International conference on advanced communications technology. 2015. Pp. 76–80.

6. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2000. 502 с.

7. Буйневич М.В., Магон А.Е., Ширяев Д.М. Анализ возможности безопасного масштабирования телекоммуникационной структуры АСУ путем принудительной маршрутизации трафика стандартными средствами // Вопросы современной науки и практики. Университет им. В.И. Вернадского. 2008. Т. 2. № 3. С. 161–164.

8. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Обеспечение безопасности сетей ОКС-7 // Сети и системы связи. 2003. № 2.

9. Dotsenko S., Vladyko A., Letenko I. A fuzzy logic-based information security management for software-defined networks. 16th International conference on advanced communication technology. 2014. Pp. 167–171.

10. Комплексная методика тестирования фрагмента программно-конфигурируемой сети / А.Г. Владыко [и др.] // Информационные технологии и телекоммуникации. 2015. № 2 (10). С. 20–29.