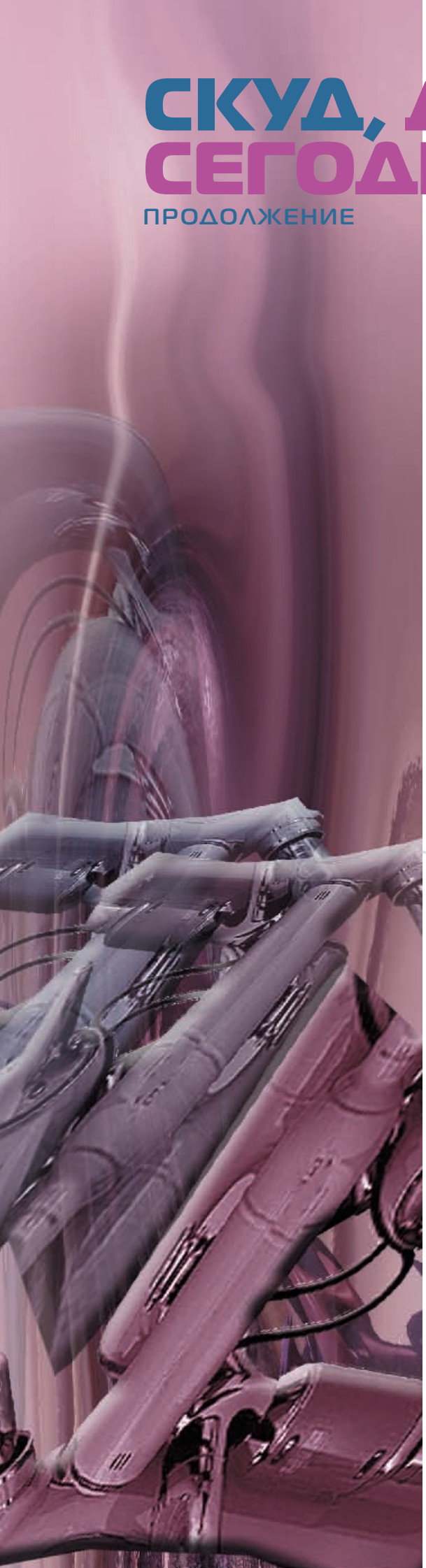
СКУД, ДЕНЬ СЕГОДНЯШНИЙ

ПРОДОЛЖЕНИЕ



Е. Кин
глава представительства Nedap N.V. Security Management в России

ЗАЩИТА ПЕРЕДАВАЕМОЙ ПО СЕТИ ИНФОРМАЦИИ

Основным доводом для скептиков при обсуждении вопросов интеграции существующих сетевых стандартов в оборудование СКУД является мнение о недостаточной защищенности соединений по протоколу TCP/IP, а также о возникающих проблемах при прохождении информационных пакетов через различные шлюзы и маршрутизаторы, разделяющие подсети. Одним из решений этого вопроса является организация VPN-соединения (Virtual Private Network) по SSL-протоколу (Secure Socket Layer) между сетевыми контроллерами и сервером системы. VPN в комбинации с SSL на данный момент считается самым безопасным методом для передачи данных в сетях.

Безусловно, это требует от производителя СКУД реализации VPN в ПО контроллера, для чего, опять же, более выигрышно смотрятся варианты на платформе Linux.

Помимо этого, для защиты доступа к информации на контроллере возможно использование существующих и уже зарекомендовавших себя решений на рынке IT. Например, в контроллерах Nedap AEOS, помимо реализованной технологии VPN/SSL для защиты доступа к контроллеру используется встроенный SAM-модуль. SAM-модуль (Security Account Manager) – это администратор учетных данных в системе защиты, т.е. подсистема, обеспечивающая ведение базы учетных записей пользователей, содержащих сведения об уровнях пользовательских привилегий, паролях и т.п. Наличие SAM-модуля предотвращает доступ неавторизованных пользователей к контроллеру. SAM-модуль может снабжаться ключами, с которыми пользователи могут работать по своему усмотрению.

РАБОТА В РЕЖИМЕ PoE

Безусловно, наличие режима PoE у IP-контроллеров СКУД, в отличие, скажем, от IP-камер, сейчас выглядит скорее маркетинговым ходом, чем серьезным техническим новшеством. В самом деле, устанавливая такие контроллеры на объекте, Вы не можете с чистой совестью сказать Заказчику, что к контролируемой двери нужно просто «пробросить» сеть. Дело в том, что контроллерам СКУД, в отличие от тех же IP-камер, необходимо управлять периферийными устройствами (считывателями и исполнительными механизмами), а в силу существующих стандартов PoE выходная мощ-

ность контроллеров СКУД, работающих в таком режиме, не позволяет им подавать питающее напряжение, например, на считыватели дальнего радиуса действия и, тем более, на электромеханические или электромоторные замки. С другой стороны, уже сейчас суммарная выходная мощность контроллеров Edge Solo компании HID равна 700 mA при 12 VDC, а аналогичная выходная мощность контроллера AEOS AP6003 компании Nedap делится как 200 mA для подключения внешнего считывателя и 500 mA для управления замком при тех же 12 VDC. Этих характеристик вполне достаточно для управления дверью с RFID-считывателем короткого радиуса действия и подачи управляющего напряжения на электрозамок или защелку. Но с точки зрения корректного монтажа системы доступа, в любом случае питание замка должно осуществляться независимо от питания контроллера и считывателя во избежание возможных скачков напряжения в сети, питающей чувствительную электронику. Дальнейшее же развитие стандартов PoE, на мой взгляд, расширит возможности применения этой технологии в СКУД и повлечет появление новых интересных разработок в этой области.

МУЛЬТИФОРМАТНЫЕ СЧИТЫВАТЕЛИ И КОНТРОЛЛЕРЫ

К настоящему моменту можно смело сказать, что в России уже достаточно давно сложился отдельный сегмент рынка систем безопасности, связанный с заменой и модернизацией ранее установленного оборудования на объектах заказчиков. И хотя рынок СКУД в России несколько моложе того же рынка видеонаблюдения и начинался он в середине 90-х годов прошлого века, причем сразу с RFID-технологии (чему сильно удивлялись попадавшие в то время в Россию представители западных стран). Поле для деятельности на этом «вторичном» рынке сейчас достаточно обширно. Требования по замене существующей СКУД могут выдвигаться заказчиком как исходя из существующих государственных предписаний (например, периодическая замена средств ТСБ в структурах Центробанка РФ), так и по объективным причинам морального и технического старения имеющейся системы. В большинстве случаев заказчик выдвигает, как минимум, одно, но очень жесткое требование: пропуска у сотрудников должны остаться прежними. И действительно, зачастую стоимость замены карт у многотысячного персонала крупного промышленного предприятия или компании с мультифилиальной структурой с лихвой перекрывает стоимость замены всего оборудования СКУД на объекте. К чисто техническому моменту по замене одних идентификаторов на другие добавляется настоящая организационная «головная боль» для сотрудников службы безопасности, связанная с физическим изъятием у сотрудников всех старых пропусков и плановой раздачей новых.

Естественно, для ведущих мировых производителей СКУД эта проблема возникла далеко не вчера, и в настоящий момент рынок предлагает два основных варианта решения вопроса сохранения (или плавного замещения) пропусков пользователей при замене существующей у заказчика системы.

Большинство современных СКУД имеет различные типы интерфейсных модулей или же универсальные устройства для подключения считывателей с различными распространенными типами интерфейсов. Чаще всего речь идет о Wiegand и Data&Clock интерфейсах с возможным добавлением специфичного внутреннего интерфейса конкретного производителя. При этом «хорошим тоном» является возможность одновременной работы в системе считывателей разных типов.

Другой вариант решения задачи сохранения пропусков – применение мультиформатных считывателей, обычно позволяющих читать, помимо карт «родного» формата производителя, еще 1-2 типа распространенных на рынке идентификаторов. Чаще всего это HID и/или Mifare.

В реализации этих решений есть и свои «передовики». Так, считыватели Transition Readers системы Cusi Rusco поддерживают работу сразу четырех форматов карт доступа: GE Proximity, HID, Mifare, VICINITY. Интерфейсные же модули Nedap AEOS для считывателей сторонних производителей серий AP1003/6003/4X03 после предварительной настройки способны поддерживать работу практически всех существующих на рынке считывателей. Помимо считывателей с интерфейсами Wiegand и Data&Clock, к ним можно подсоединять устройства с интерфейсами RS232, RS485, Omron и MagStripe. Библиотека «поведенческих» компонентов для этих модулей (встраиваемое ПО) содержит более восьмидесяти (!) типов различных форматов для считывателей с указанными интерфейсами.