УДК 681.3

ПРОЕКТИРОВАНИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ИКИТ СФУ

Хохлов А.А.
Научный руководитель — профессор, к.ф.-м.н., ст. пр-ль Кучеров М.М
Сибирский федеральный университет

В настоящее время войти на территорию университета не составляет труда ни студентам, ни преподавателям, ни посторонним лицам. Так как редкий случай, когда охранник на пропускном пункте попросит предоставить документы. Но если и попросит, то не составляет труда вклеить в пропуск свою фотографию, заполнить данные и поставить поддельную печать.

Помимо данной уязвимости, студенческий билет (или преподавательский пропуск) имеет еще ряд недостатков. Во-первых, данные документы не позволяют контролировать учебный процесс. То есть в случае черезвычайной ситуации система безопасности не будет знать: кто вошел, кто вышел и кто где находится. Следовательно, будет сложнее установить причинно-следственную связь. Во-вторых, студенты всегда имеют сразу несколько документов при себе: студенческий билет, читательский билет, зачетная книжка, что является достаточно большим количеством для одного университета. А после утери одного из документов следует долгое восстановление: поднятие архивов, перебор стопок документов и т.д. В-третьих, данные документы уже давно отстали от текущих технологий и до сих пор заполняются от руки без наличия каких-либо автоматических процессов.

Из всего выше сказанного следует, что в настоящее время университету требуется универсальный идентификатор как для студентов, так для преподавателей и других сотрудников. Данный идентификатор должен быть уникальным и трудным для подделки, а также непосредственно учавствовать в автоматизации учебного процесса. Всем вышеперечисленным требованиям соответствует система контроля и управления доступом на базе бесконтактной смарт-карты и считывателей.

Система контроля доступа решает задачи ограничения и разграничения доступа на территории университета, контроля проезда через транспортные КПП, учета рабочего времени персонала, помогает организовать выдачу пропусков посетителям, формировать отчеты и анализировать состояние дисциплины, координировать действия охранников. При этом подобные меры контроля и ограничения доступа не должны доставлять серьезных неудобств или вызывать раздражение у персонала и посетителей.

ИКИТ СФУ является однофилиальным объектом, в подразделении которого находится около 150 преподавателей и свыше 5000 студентов. ИКИТ СФУ имеет две центральных проходных, переход из соседнего корпуса и 4 запасных выхода, насчитывает около 100 кабинетов, среди которых есть серверный отдел, компьютерные кабинеты и лаборантские.

Помимо контроля проходных помещений требуется контроль каждого кабинета, и при этом расходы желательно свести к минимуму. В данном случае следует спроектировать схему, совмещающую в себе IP-контроллеры и IP-считыватели. Данный вариант выбран по следующим причинам:

1. ИКИТ СФУ имеет свою локальную сеть, а значит для сокращения расходов следует использовать сетевые устройства.
2. Из-за большого потока студентов на проходных помещениях будет установлено по три или четыре преграждающих устройства на вход и выход. Для

управления ими производительнее использовать отдельные панели управления со встроеными базами данных, периодически обновляемых с сервера.

3. Доступ в каждый кабинет будет индивидуальный (только преподаватель может открыть или закрыть дверь, студент может отметиться только в кабинете, описанном в расписании), а следовательно с каждым считывателем следует оперировать отдельно, чего не позволяют последовательные соединения.
4. В случае тревоги необходимо как можно быстрее проинформировать считыватели для выполнения определенных операций (открытие/закрытие дверей и т.п.). Локальная сеть Ethernet работает значительно быстрее сети RS-485.
5. В ИКИТ СФУ установлена беспроводная сеть, что упростит установку оборудования.

Так как ИКИТ СФУ является однофилиальным объектом с большим потоком людей, то для снижения нагрузки сети и обеспечения отказоустойчивости следует спроектировать многомодульное программное обеспечение, каждый модуль которого работает независимо друг от друга, и в случае сбоя одного из модулей реализовать возможность замены его другим модулем. База данных для всех модулей едина.

Для реализации идентификации объекта следует использовать три типа смарт-карт:

1. Постоянная. Выдается преподавателям и студентам, для получения прав доступа. Действует на протяжении всего срока работы или учебы.
2. Временная. Выдается гостям при проведении мероприятий. Действует на протяжении проведения мероприятия.
3. Одноразовая. Выдается студентам, преподавателям при утере или блокировании постоянной карты. Также выдается абитуриентам при поступлении в институт. Действует один день.

Каждый серийный номер смарт-карты соответствует уникальным данным студента, преподавателя или гостя, каждый из которых имеет индивидуальные права доступа на территории ИКИТ СФУ.

Аутентификация в проходном помещении дает разрешение на вход в территорию ИКИТ СФУ или выход. Аутентификация в кабинеты корпусов преподавателям дает разрешение на открытие или закрытие двери кабинета, студентам или гостям на отметку о присутствии в кабинете. Отметка о присутствии действует на протяжении текущей ленты или мероприятия, а также до выхода из корпуса института. В базе данных ведется история о действиях каждого из субъектов: во сколько он пришел, какие кабинеты посетил и во сколько вышел.

Процесс аутентификации с помощью смарт-карты состоит в следующем: считыватель получает со смарт-карты серийный номер, отправляет его на сервер, сервер проверяет права доступа и посылает результат на считыватель. Считыватель, если требуется, считывает данные с памяти карты и отправляет на сервер для обработки.

Разработчики смарт-карт стараются защитить карты от дублирования, но случаи клонирования карт происходили неоднократно. Поэтому для защиты смарт-карт от копирования следует использовать переменные ключи. Для этого надо разделить ключ аутенфикации на три части. Первая постоянная часть ключа будет храниться на сервере, вторая постоянная часть ключа будет являться серийным номером карты, а третья переменная часть ключа будет храниться в памяти карты. Переменная часть ключа будет являться меткой времени последней аутентификации, зашифрованной ключем на сервере. Тогда процесс аутентификации будет происходить следующим образом: считыватель считывает серийный номер карты и отправляет его на сервер, сервер проверяет права доступа, если объекту доступ разрешен, то запрашивает переменную часть ключа, хранящегося в памяти карты. Получив данные, сервер расшифровывает своим

ключем и в базе данных проверяет, если метки времени совпадают, то доступ разрешен, иначе сервер заносит серийный номер карты в черный список. Далее сервер шифрует текущую метку времени и отправляет её считывателю, который перезаписывает переменную часть ключа.

Чтобы обосновать гарантию защищенности смарт-карты от копирования, надо перечислить варианты клонирования карты. Первый вариант — когда злоумышленник крадет смарт-карту у сотрудника предприятия, дублирует карту и незаметно возвращает её владельцу. Тогда у злоумышленника есть время использовать дубликат только до следущей аутенфикации хозяина оригинала. Если он успел использовать карту, то при аутентификации владельца оригинала обе карты заблокируются, и начнется выяснение обстоятельств. Так как студенты и преподаватели ходят в ИКИТ СФУ ежедневно и за день посещают несколько корпусов, то вероятность успеха злоумышленника очень мала. Второй вариант, когда злоумышленник является сотрудником предприятия. Если он копирует карту, чтобы отдать дубликат сообщнику, тогда после аутентификации одной из карт, аутентификация другой только заблокирует обе карты, а значит, в клонировании карты сотрудниками предприятия нет смысла.

Таким образом, внедрение систем контроля и управления доступом в ИКИТ СФУ автоматизирует немалую часть ежедневного учебного процесса, в котором человеку можно не участвовать до возникновения внеплановых ситуаций. Данная система будет контролировать работу как студентов, так преподавателей и других сотрудников ИКИТ СФУ, заменит весь объем документов одной универсальной бесконтактной смарт-картой, связанной с единой базой данных ИКИТ СФУ, которую очень сложно подделать. Что и требуется на данный момент с текущими технологиями.