

Безопасность хранения данных

Владимир Иванов

ivlad@amt.ru

СЕТИ И ТЕЛЕКОММУНИКАЦИИ



Краткое содержание

- Технологии хранения данных и новые угрозы
- Возможные направления атак
- Методы противодействия угрозам



Новые угрозы в сетях хранения данных

СЕТИ И ТЕЛЕКОММУНИКАЦИИ



- Сети хранения в основном используют протокол Fibre Channel
 - данные хранятся централизованно, в системах хранения, доступны в виде блоков
 - выделенная сеть создает иллюзию безопасности
 - администраторы безопасности не подозревают или не интересуются FC-сетями



- Сети хранения становятся все больше, количество подключений растет, снижается доверие к сети и устройствам
 - Подключение удаленных ЦОД через FCIP, CWDM/DWDM
- Традиционные проблемы безопасности, существовавшие в IP-сетях актуальны и в FC SAN
 - WWN spoofing, E-Port replication, MitM-attacks во многом сходны со своими «родственниками» в IP



Новые угрозы и проблемы безопасности

СЕТИ И ТЕЛЕКОММУНИКАЦИИ



- Архитектура сетей Fibre Channel обеспечивает доступ к служебной информации для любых устройств
- Администраторы систем и сетей хранения не имеют опыта в области информационной безопасности
- Управление устройствами в сети хранения осуществляется по тому же каналу, что и передача данных (in-band)
- Протоколы аутентификации устройств (стек FCSP) окончательно не разработаны



Атаки в сетях Fibre Channel

СЕТИ И ТЕЛЕКОММУНИКАЦИИ



Session Hijacking

- В сети FC взаимодействие между узлами осуществляется посредством *последовательностей (sequence)*
 - последовательности определяются Seq_ID, каждый пакет в рамках последовательности определяется Seq_CNT
 - Seq_ID остается постоянным, Seq_CNT увеличивается на единицу в каждом пакете
- Может быть применимо для подмены in-band сессии управления, например, дисковым массивом



MitM Attack

- В сети FC соответствие между 64-bit WWN и 24-bit FCID устанавливается средствами Fabric Name Server
 - FNS расположен по известному адресу 0xfffffc, запрос на регистрацию не аутентифицируется

WWN Spoofing

- WWN используется для аутентификации узлов как при организации *zoning*, так и для *LUN masking*
- ПО драйверов позволяет изменить WWN



E-Port Replication

- Взаимодействие коммутаторов в FC-сети осуществляется через E-port
- Аутентификация при подключении коммутаторов не производится
 - атакующий может объявить себя коммутатором FC
 - «коммутатор» может управлять маршрутизацией в фабрике
 - «коммутатор» может изменять политики zoning
 - «коммутатор» может объявлять о существовании новых узлов

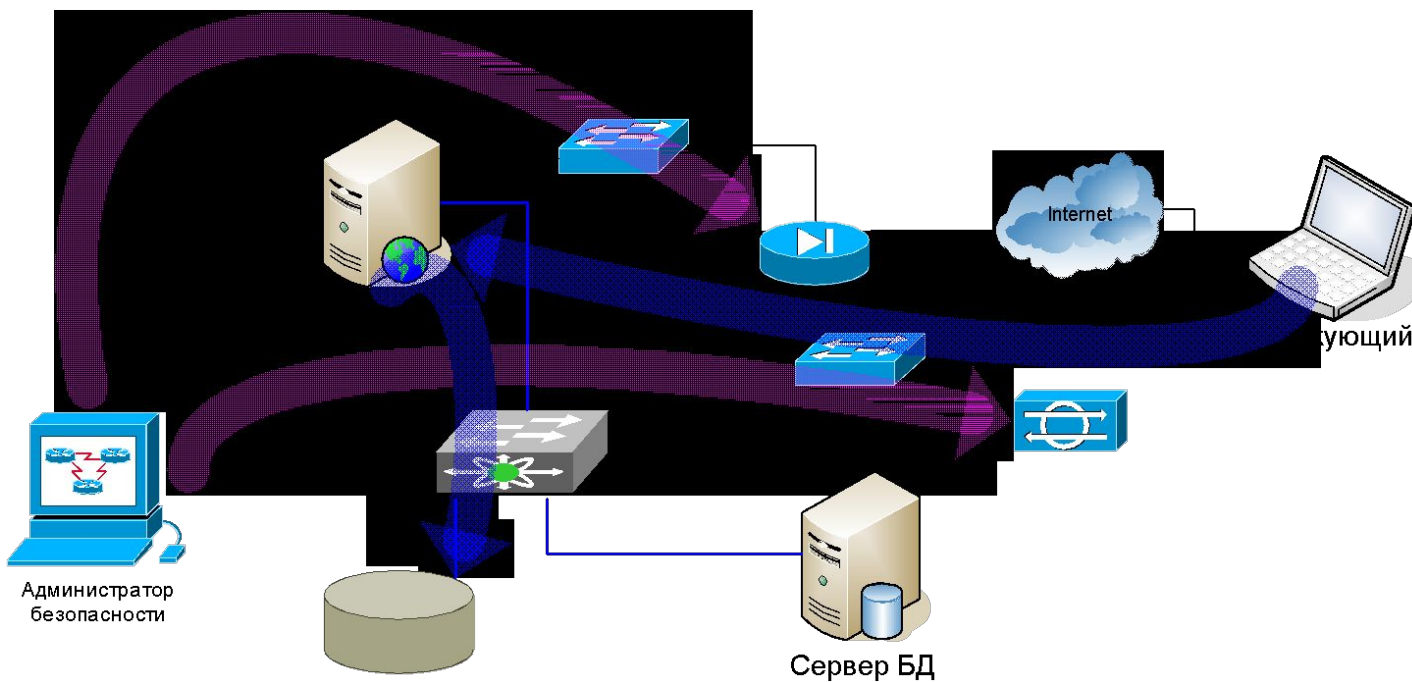


Сценарий атаки

СЕТИ И ТЕЛЕКОММУНИКАЦИИ



Атака через сеть хранения



Методы противодействия

СЕТИ И ТЕЛЕКОММУНИКАЦИИ



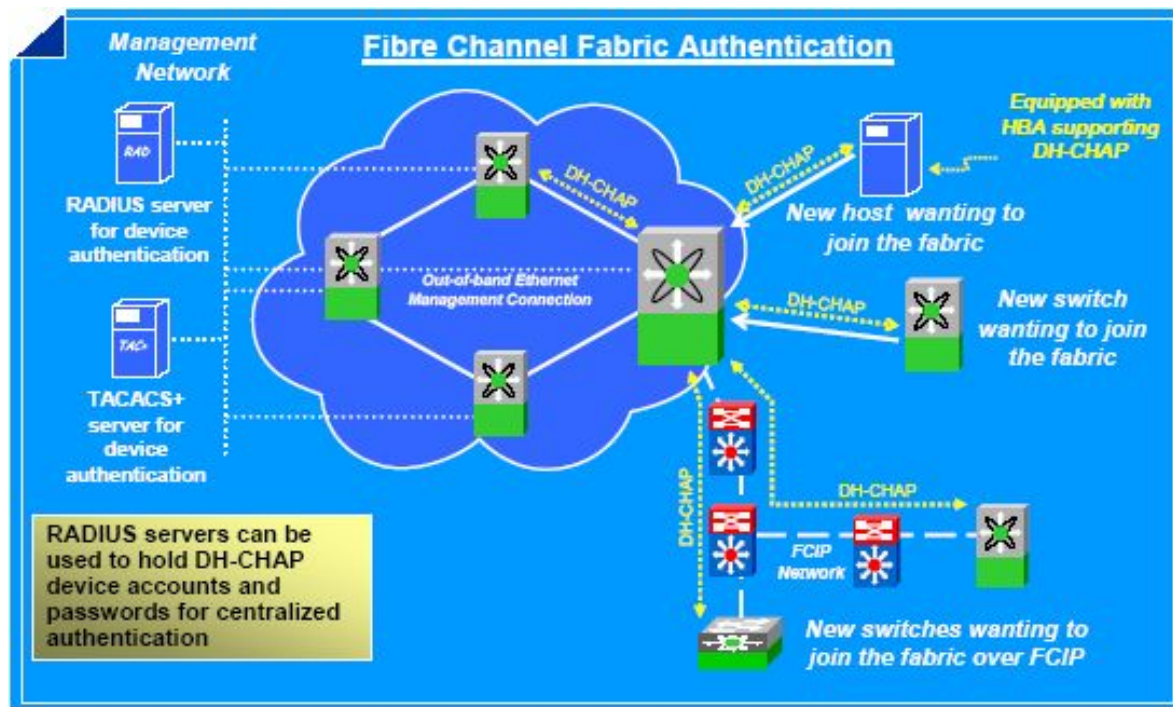
Аутентификация

- Аутентификация устройств в сети хранения: протокол FCSP
 - Обеспечивает аутентификацию устройств (host-to-switch и switch-to-switch, host-to-host) в сети хранения Fibre Channel
 - Реализация FCSP DN-CHAP поддерживается рядом производителей FC-коммутаторов и FC-НВА
 - Аутентификация устройств интегрируется в общую платформу аутентификации (RADIUS)



Авторизация

- Ближайший этап – использование PKI для аутентификации устройств (FCAP)



Авторизация

- Сейчас используются WWN
- Использовать:
 - port-based zone
 - hardware zoning
 - port locking
 - VSAN (Cisco-only)



Конфиденциальность

- Проблема конфиденциальности для сетей хранения стоит более остро, чем для сетей передачи данных в силу агрегации информации в одной точке
- В настоящий момент стек FC не предусматривает никаких средств криптозащиты
 - ведется, но не закончена, разработка стека протоколов FCSec
- Для FCIP и iSCSI применим IPSec
- Рекомендуется защищать не только среду передачи, но и сами данные в процессе хранения



Вопросы?

