“Построение системы управления сетевыми соединениями на базе протокола RADIUS”

Омский филиал НИУ Институт математики им. С.Л. Соболева СО РАН

Хрущев Сергей Анатольевич, Черенкова Светлана Юрьевна

Существующие RADIUS-серверы

- Ориентация на Unix
- Хранение настроек в текстовых файлах
- Необходимость установки “патчей” для интеграции с внешними системами
- Необходимость перекомпиляции при смене ОС

Преимущества языка Java

- Многоплатформенность системы
- Поддержка сетевых возможностей
- Поддержка доступа к базам данных

Защищенность коммуникаций по протоколу RADIUS

- Установка на NAS и сервере RADIUS закрытого ключа достаточной длины
- Генерация на NAS удостоверений пакетов с использованием “хорошего” ГСЧ, отсутствие повторений значений
- Стойкость алгоритма хеширования MD5

Необходимые условия для атаки на систему, использующую RADIUS

- Возможность перехвата UDP пакетов, идущих от NAS к RADIUS-серверу и обратно
- Возможность подмена пакетов идущих от RADIUS-сервера к NAS
- Знание секретного ключа, либо эффективный алгоритм его восстановления

Развитие RADIUS-сервера

- Интеграция с биллинговой системой
- Обеспечение поддержки IPv6