Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле,
Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел

Защита от хакеров беспроводных сетей



Protect Your Wireless Network From Attack

Christian Barnes
Tony Bautts
Donald Lloyd
Eric Ouellet
Jeffrey Posluns
David M. Zendzian
Neal O'Farell

SYNGRESS®



ЗАЩИТА ОТ ХАКЕРОВ

беспроводных сетей

Серия «Информационная безопасность»

Перевод с английского
А. В. Семенова

Кристиан Барнс
Тони Боутс
Дональд Ллойд
Эрик Уле
Джеффри Посланс
Дэвид М. Зенджан
Нил О'Фаррел

Академия АйТи
ДМК издательство
Москва, 2005

УДК 004.056
ББК 32.973.202
Р24

Р24 **Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле, Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел**
Защита от хакеров беспроводных сетей: Пер. с англ. А. В. Семенова. – М.: Компания АйТи; ДМК-Пресс, 2005. – 480 с.: ил. (Серия «Информационная безопасность»).

ISBN 5-98453-012-0

Цель этой книги – предоставить максимально исчерпывающую информацию о беспроводных коммуникациях людям, работающим во всех сферах бизнеса и информационных технологий, подготавливают ли они реальный бизнес-план для беспроводного проекта, являются ли они IS/IT-специалистами, планирующими новое беспроводное внедрение, включают ли они беспроводные возможности в домашнюю сеть, реагируют ли на атаку на их сеть или просто любят заниматься проблематикой безопасности.

УДК 004.056
ББК 32.973.202

Original Eglish language edition publihed by Singress Publishing, Inc. Copyright © 2002 by Singress Publishing, Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 1-928994-59-8 (англ.)
ISBN 5-98453-012-0 (АйТи)

Copyright © 2002 by Singress Publishing, Inc.
© Перевод на русский язык. Компания АйТи, 2004
© Оформление, издание. ДМК-Пресс, 2005

Содержание

Предисловие 17

Глава 1. Беспроводной вызов 19

Введение 20

Обзор беспроводных технологий 21

Определение беспроводных решений на базе сотовых сетей 21

Определение беспроводных LAN 21

Конвергенция беспроводных технологий 22

Тенденции и статистика 22

Рост использования беспроводных приложений 22

Ближайшее беспроводное будущее 24

Понимание перспектив беспроводной технологии 26

Беспроводные сети 28

Преимущества беспроводных технологий 33

Удобство 34

Доступность 39

Скорость 39

Эстетика 41

Производительность 41

Беспроводная реальность сегодня 41

Конфликты стандартов 42

Коммерческие конфликты 44

Проблемы принятия рынком 44

Ограничения «радио» 44

Ограничения беспроводной безопасности 49

Проверка беспроводных стандартов 56

Сотовые беспроводные сети 56

Беспроводные LAN 63

Инфраструктура общедоступных ключей в беспроводных сетях 79

Заключение 85

Ответы на ваши беспроводные вопросы

Вопрос: Будет ли i-Mode распространяться в Европе или Северной Америке?
Ответ: Хотя владелец i-Mode, компания NTT DoCoMo имеет заметные доли в пакетах акций нескольких северо-американских и европейский сотовых операторов, нет планов быстрого вывода i-Mode в современном виде на эти рынки. Это обусловлено прежде всего ограниченной скоростью доступа 9,6 Кб/с.

Краткое изложение решений 86
Часто задаваемые вопросы 89

Глава 2. Основы безопасности 91

Введение 92
Основы систем безопасности и принципы защиты 92
Обеспечение конфиденциальности 93
Обеспечение целостности 94
Обеспечение наличия 96
Обеспечение неприкосновенности конфиденциальной информации 97
Обеспечение аутентификации 97
Обеспечение авторизации 102
Обеспечение невозможности отказа 103
Следы создания отчетов и аудита 106
Использование шифрования 108
Шифрование голоса 109
Системы шифрования данных 110
Обзор роли политики 110
Идентификация ресурсов 112
Критерии классификации 114
Внедрение политики 114
Определение стандартов безопасности и конфиденциальности 116
Обзор стандартов безопасности 118
Обзор стандартов конфиденциальности и их регулирование 122
Обзор общих угроз и рисков 128
Случай потери данных 129
Случай отказа от предоставления услуг или разрушения услуг 129
Прослушивание 131
Предупреждение последствий организационных потерь 133
Заключение 135

Средства и ловушки

Текстовая аутентификация

Пример генератора словаря паролей для атак грубой силы, который может создавать этот словарь на основе набора букв, можно отыскать в Интернете на сайте www.dmzs.com/tools/files. Есть и другие генераторы для атак грубой силы на POP: Telnet, FTP, Web и т. п., их можно найти на http://packetstormsecurity.com/crackers.

Краткое изложение решений 136
Часто задаваемые вопросы 139

Глава 3. Архитектура и проектирование беспроводных сетей 141

Введение 142
Фиксированные беспроводные технологии 143
Услуга многоканального распределения сигнала между многими точками (MMDS) 144
LMDS – локальные услуги распределения сигнала по многим точкам 145
WLL (Wireless Local Loop – беспроводная локальная петля) 147
Микроволновая связь «точка-точка» 147
Беспроводные локальные сети – WLAN 149
Зачем нужен беспроводной стандарт LAN? 149
Развитие WLAN через архитектуру 802.11 158
Основной набор услуг 158
Расширенный набор услуг 160
Механизм CSMA-CA 162
Модульная конфигурация 164
Использование вариантов управления мощностью 164
Роуминг между многими ячейками 165
Безопасность WLAN 166
Развитие персональных сетей WPAN посредством архитектуры 802.15 167
Bluetooth 168
HomeRF 170
Высокопроизводительная радио LAN 171
Мобильные беспроводные технологии 171
Технологии первого поколения 173
Технологии второго поколения 174
Технология 2,5G 174
Технологии третьего поколения 174
Протокол беспроводных приложений WAP 175

Фиксированные беспроводные технологии

В беспроводных фиксированных сетях и передатчик, и приемник постоянно находятся в определенном месте в отличие от мобильных сетей. Эти сети используют питание от переменного тока. Они могут быть организованы по схеме «точка-точка» или же «точка-многоточка» и могут использовать как лицензируемый, так и нелицензируемый спектр.

Глобальная система мобильных коммуникаций 176
Пакетная радиоуслуга GPRS 178
Услуга коротких сообщений 179
Беспроводные оптические технологии 179
Исследование процесса проектирования 180
Проведение предварительных исследований 180
Анализ существующего окружения 181
Предварительное проектирование 182
Окончательное проектирование 182
Реализация внедрения 183
Создание документации 184
Создание методологии проектирования 184
Создавая сетевой план 185
Разработка сетевой архитектуры 191
Формализация стадии детального проектирования 195
Понимание атрибутов беспроводной сети в аспекте проектирования 200
Поддержка приложений 201
Природный ландшафт 204
Топология сети 206
Заключение 208
Краткое изложение решений 210
Часто задаваемые вопросы 214

Глава 4. Распространенные атаки и уязвимости 215

Введение 216
Слабости WEP 216
Критика общего проектирования 217
Слабость алгоритма шифрования 219
Слабости управления ключами 222
Слабости в поведении пользователей 225
Проведение разведки 227
Нахождение сети 227

Заметки из подземелья

Шлюз компании Lucent Technologies сообщает SSID открытым текстом даже в сетях с шифрованием

Как было объявлено в Интернете на сайте www.securiteam. com/securitynews/5ZP0I154UG.html, шлюз компании Lucent открывает атакующему простой путь для соединения с закрытой сетью. Чтобы соединиться с беспроводной сетью, пользователь должен знать SSID сети. Даже если сеть защищена при помощи WEP, часть передаваемых посланий шлюз передает в незашифрованном виде, включая SSID. Все, что должен сделать атакующий, – это «вынюхивать» сеть для определения ее SSID, после этого он сможет соединиться с сетью.

Нахождение слабостей в мишени 228
Использование этих слабостей 229
Вынюхивание, перехват и прослушивание 230
Определение вынюхивания 231
Устройства для вынюхивания 231
Сценарий для вынюхивания 231
Защита от вынюхивания и подслушивания 233
Подмена устройства и неавторизованный доступ 235
Определение «подмены» 235
Набор средств для «подмены» 236
Сценарий «подмены» 236
Защита от подмены и неавторизованных атак 237
Модификация сети и ее ограбление 238
Определение ограбления 238
Набор средств для ограбления 239
Сценарий «ограбления» 240
Защита от модификации сети и ее ограбления 240
Отказ от предоставления услуги и атаки переполнения 241
Определение атак переполнения и отказа от предоставления услуг 241
Набор средств для DoS 242
Сценарий DoS и переполнения 242
Защита от атак DoS и переполнения 243
Введение в злонамеренное ПО 243
Кражи пользовательских устройств 245
Заключение 247
Краткое изложение решений 247
Часто задаваемые вопросы 251

Глава 5. Контрмеры для обеспечения беспроводной безопасности 253

Введение 254

Стратегии для анализа угроз

- определить активы компании;
- определить возможные доступы к ним в точки зрения авторизации;
- определить вероятность того, что неавторизованный пользователь сможет получить доступ к этим активам;
- определить потенциальные потери;
- определить стоимость восстановления после потерь и ремонтных работ или оценить потери;
- определить необходимые контрмеры безопасности;
- определить стоимость внедрения контрмер;
- сравнить стоимость обеспечения безопасности ресурсов с величиной потерь.

Политика повторных визитов 255
Обращение к проблемам при помощи политики 257
Анализ угрозы 259
Угроза = риск + уязвимость 260
Проектирование и развертывание безопасной сети 266
Внедряя WEP 271
Определение WEP 271
Обеспечение конфиденциальности при помощи WEP 272
Процесс аутентификации в WEP 273
Преимущества и выгоды WEP 273
Недостатки WEP 274
Смысл безопасности при использовании WEP 274
Внедрение WEP в продуктах Aironet 274
Внедрение WEP в Orinoco AP-1000 275
Обеспечение безопасности WLAN при помощи WEP: примерный сценарий 276
Фильтрация MAC-адресов 278
Определение фильтрации MAC 279
Выгоды и преимущества от использования MAC-адресов 280
Недостатки MAC 280
Обеспечение безопасности при помощи фильтрации MAC-адресов 281
Внедрение MAC-фильтров в AP-1000 281
Внедрение MAC-фильтров в Aironet 340 281
Фильтрация MAC-адресов: сценарий конкретного случая 285
Фильтрация протоколов 285
Определение фильтров протокола 285
Преимущества и выгоды от применения фильтрации протокола 286
Недостатки фильтрации протокола 287