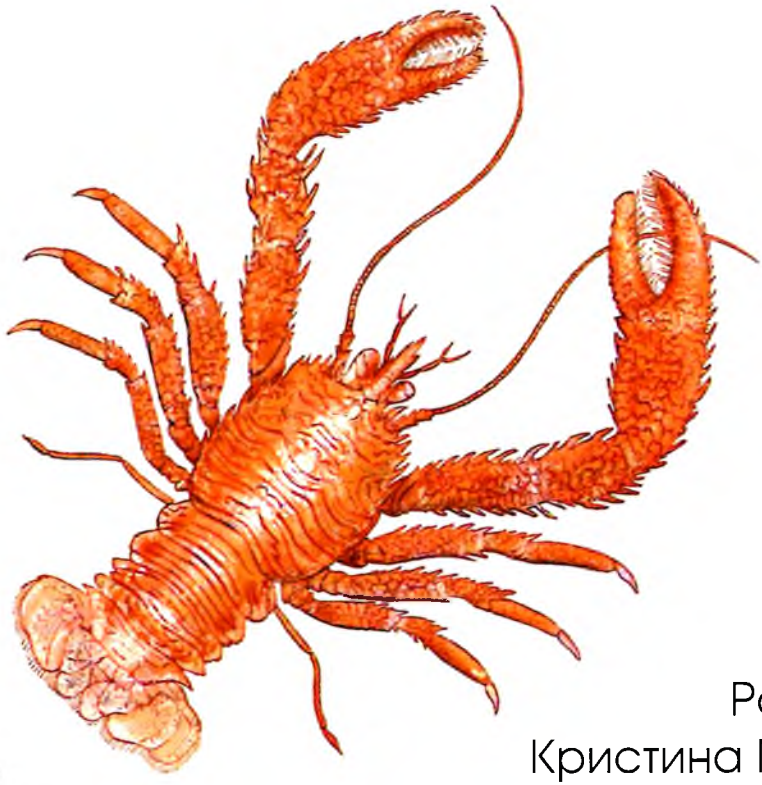
O'REILLY®

2-е издание

Сети с нулевым доверием

Построение безопасных систем в ненадежных сетях



Рази Райс,
Кристина Морильо,
Эван Гилман, Дуг Барт

alist

Содержание

Отзывы о книге "Сети с нулевым доверием" (2-е издание) **13**

Введение **15**

Кому предназначена эта книга 16
Зачем мы написали эту книгу 16
Как организована эта книга 17
Условные обозначения и соглашения 18
Платформа онлайн-обучения O'Reilly 19
Как с нами связаться? 19
Благодарности за первое издание 19
Благодарности за второе издание 20

ГЛАВА 1. Основы концепции нулевого доверия **21**

Что такое сеть с нулевым доверием? 22
Введение в уровень управления с нулевым доверием 24
Эволюция модели защиты периметра 24
Управление пространством глобальных IP-адресов 24
Появление пространства частных IP-адресов 26
Подключение частных сетей к публичным 26
Появление NAT 27
Современная модель защиты периметра 28
Эволюция ландшафта угроз 28
Недостатки защиты периметра 32
В чем заключается доверие 35
Автоматизация как стимул 35
Безопасность периметра или нулевое доверие 36
Применение в облачных сервисах 38
Роль концепции нулевого доверия в национальной кибербезопасности 39
Резюме 40

ГЛАВА 2. Управление доверием **42**

Модели угроз 43
Модели распространенных угроз 44
Модель угроз концепции с нулевым доверием 45
Строгая аутентификация 47

Подтверждение подлинности доверия 49
Что такое центр сертификации? 50
Роль инфраструктуры открытых ключей в модели с нулевым доверием 50
Приватная или публичная PKI 51
Публичная инфраструктура открытых ключей лучше, чем ничего 52
Минимум привилегий 52
Динамическое доверие 54
Коэффициент доверия 56
Недостатки коэффициента доверия 58
Уровень управления или уровень данных 59
Резюме 60

ГЛАВА 3. Контекстуальные агенты 62

Что такое агент? 63
Изменчивость агента 63
Что содержится внутри агента? 64
Как используется агент? 65
Агенты не для аутентификации 66
В какой форме должен быть представлен агент? 67
Сочетание твердости и гибкости 68
Рекомендуемая стандартизация 69
А пока? 70
Резюме 72

ГЛАВА 4. Принятие решений об авторизации 73

Архитектура авторизации 73
Исполнение 75
Движок политики 76
Хранилище политик 76
В чем залог хорошей политики? 77
Кто определяет политики? 80
Оценка политик 80
Механизм доверия 81
Какие сущности оцениваются? 83
Риски открытого доступа к коэффициенту доверия 84
Хранилища данных 85
Пример с пошаговым руководством 87
Резюме 91

ГЛАВА 5. Доверие к устройствам 93

Начальное формирование доверия 93
Создание и защита идентификационных данных 94
Защита идентификационных данных в статичных и динамичных системах 95

Аутентификация устройства на уровне управления ... 98
X.509 ... 98
Доверенный платформенный модуль ... 102
Аутентификация устройств с помощью TPM ... 106
Векторы атак на HSM и TPM ... 106
Управление оборудованием ... 108
Предсказуемые ожидания ... 109
Безопасное внедрение ... 111
Обновление и измерение доверия устройства ... 112
Локальное измерение ... 113
Дистанционное измерение ... 114
Унифицированное управление конечными точками ... 115
Управление конфигурацией ПО ... 117
Реестр на основе управления конфигурацией ... 117
Реестр оборудования с возможностью поиска ... 118
Надежный источник истины ... 118
Использование данных устройства для авторизации пользователя ... 118
Сигналы доверия ... 119
Длительное существование образа на устройстве ... 119
История доступа ... 120
Местоположение ... 120
Паттерны коммуникации в сети ... 121
Машинное обучение ... 121
Пример с пошаговым руководством ... 121
Пример: Боб хочет отправить документ на печать ... 125
Анализ запроса ... 125
Пример: Боб хочет удалить электронное сообщение ... 126
Анализ запроса ... 127
Резюме ... 128

ГЛАВА 6. Доверие к пользователям ... 129

Сетевая идентичность ... 129
Формирование сетевой идентичности в закрытой системе ... 131
Удостоверение личности государственного образца ... 132
Ничего не сравнится с физическим миром ... 132
Ожидания и оценки ... 133
Хранение сетевой идентичности ... 133
Использование каталогов ... 133
Поддержка каталогов ... 134
Когда нужна аутентификация через идентичность ... 135
Доверие через аутентификацию ... 135
Влияние уровня доверия на аутентификацию ... 136
Использование нескольких каналов ... 136
Кеширование идентичности и доверия ... 137

Как происходит аутентификация через идентичность ... 137
То, что вы знаете: пароли ... 138
То, чем вы обладаете: TOTP ... 139
То, чем вы обладаете: сертификаты ... 140
То, чем вы обладаете: аппаратный токен безопасности ... 141
То, кем вы являетесь: биометрические данные ... 141
Поведенческие паттерны ... 142
Внеполосная аутентификация ... 143
Единый вход в систему ... 143
Идентичности рабочей нагрузки ... 145
Смещение в сторону решений для локальной аутентификации ... 146
Аутентификация и авторизация групп ... 147
Схема разделения секрета Шамира ... 147
Проект Red October ... 148
Что-то увидели — сообщите ... 149
Сигналы доверия ... 149
Пример с пошаговым руководством ... 150
Случай: Боб хочет просмотреть отчет с чувствительными финансовыми данными ... 152
Анализ запроса ... 153
Резюме ... 154

ГЛАВА 7. Доверие к приложениям ... 156

Понимание конвейера приложения ... 157
Доверие к исходному коду ... 159
Безопасность репозитория ... 160
Аутентичный код и аудиторский след ... 160
Проверка кода ... 162
Доверие к сборке экземпляров ... 162
Список материалов программного обеспечения (SBOM): риски ... 163
Надежные входные и выходные данные ... 164
Воспроизводимые сборки ... 165
Разделение версий релизов артефактов ... 165
Доверие к дистрибуции ... 166
Продвижение артефакта ... 166
Безопасность дистрибуции ... 167
Целостность и аутентичность ... 168
Доверие к сети дистрибуции ... 169
Роль человека ... 170
Доверие к экземпляру ПО ... 172
Правило использования только свежих версий ... 172
Авторизованные экземпляры ПО ... 172

Безопасность среды выполнения ... 174
Методы безопасного кодирования ... 175
Изоляция ... 176
Активный мониторинг ... 177
Жизненный цикл безопасной разработки ПО (SDLC) ... 179
Требование и модель ... 179
Кодирование и внедрение ... 179
Статический и динамический анализ кода ... 179
Рецензирование и аудит кода ... 180
Проверка качества и тестирование ... 180
Развертывание и поддержка ... 180
Непрерывное развитие ... 180
Защита приложения и конфиденциальность данных ... 181
Как мы можем доверять приложениям, которые размещаем на хосте в публичном облаке? ... 181
Конфиденциальные вычисления ... 182
Понимание идеи аппаратного корня доверия ... 182
Роль аттестации ... 183
Пример с пошаговым руководством ... 183
Случай: Боб отправляет крайне деликатные данные для обработки в финансовое приложение ... 183
Анализ запроса ... 185
Резюме ... 186

ГЛАВА 8. Доверие к сетевому трафику ... 188

Шифрование или аутентификация ... 188
Аутентичность без шифрования? ... 189
Начальное формирование доверия: первый пакет ... 191
Сервис fwknop ... 192
Краткосрочные исключения ... 192
Рабочая нагрузка SPA ... 192
Шифрование рабочей нагрузки ... 193
Хешированный код аутентификации сообщения (HMAC) ... 193
Место концепции нулевого доверия в сетевой модели ... 194
Разделение клиента и сервера ... 195
Проблемы с поддержкой сетей ... 195
Проблемы с поддержкой устройств ... 196
Проблемы с поддержкой приложений ... 196
Прагматичный подход ... 197
Изоляция сервера на базе Windows ... 198
Протоколы ... 198
IKE и IPsec ... 198
Взаимная аутентификация через TLS (mTLS) ... 199

Доверие к облачному трафику: сложности и размышления 204
Брокеры безопасного доступа в облако (CASB) и федеративная идентификация 206
Фильтрация 207
Фильтрация на стороне хоста 207
Пограничная фильтрация 210
Промежуточная фильтрация 212
Пример с пошаговым руководством 214
Случай: Боб запрашивает доступ к сервису электронной почты через анонимную сеть анонимных прокси 214
Анализ запроса 216
Резюме 217

ГЛАВА 9. Создание сети с нулевым доверием 219

Первый шаг к созданию сети с нулевым доверием: понимание текущего устройства сети 219
Выбор области 219
Оценка и планирование 220
Требования: что в действительности нужно? 221
Все сетевые потоки следует подвергать аутентификации перед обработкой 222
Создание системной диаграммы 226
Понимание потоков 227
Микросегментация 230
Программно-определяемый периметр 231
Бесконтроллерная архитектура 231
"Жульничество" с управлением конфигурациями 231
Фаза реализации: аутентификация и авторизация приложения 232
Аутентификация балансировщиков нагрузки и прокси-серверов 233
Политика, ориентированная на взаимоотношения 234
Распределение политик 235
Определение и внедрение политик безопасности 235
Прокси-серверы с нулевым доверием 237
Переход на стороне клиента и сервера 238
Безопасность конечных точек 240
Тематические исследования 240
Тематическое исследование: Google BeyondCorp 241
Основные компоненты BeyondCorp 242
Внедрение и расширение GFE 246
Сложности с многоплатформенной аутентификацией 248
Переход на платформу BeyondCorp 248
Усвоенные уроки 251
Выводы 253

Тематическое исследование: независимая от облачных сервисов сеть компании PagerDuty 253
Управление конфигурациями в качестве платформы автоматизации 254
Динамически создаваемые локальные брандмауэры 255
Шифрование распределенного трафика 256
Децентрализованное управление пользователями 257
Внедрение 258
Ценность независимой от облачных сервисов системы 259
Резюме 259

ГЛАВА 10. Состязательный подход 261

Потенциальные сложности и угрозы 261
Векторы атак 262
Идентичность, права доступа 265
Кража учетных данных 265
Повышение привилегий и горизонтальное перемещение 266
Инфраструктура и сети 267
Безопасность уровня управления 267
Перечисление конечных точек 270
Ненадежная цифровая платформа 271
Распределенные атаки типа "отказ в обслуживании" (DDoS-атаки) 271
Атака типа "человек посередине" 272
Инвалидация 273
Фишинг 274
Физическое принуждение 274
Роль киберстрахования 276
Резюме 276

ГЛАВА 11. Стандарты, фреймворки и руководства по архитектуре с нулевым доверием 278

Правительства 279
Соединенные Штаты Америки 280
Великобритания 305
Европейский союз 305
Частные и публичные организации 306
Cloud Security Alliance (CSA) 306
The Open Group 307
Gartner 308
Forrester 309
Международная организация по стандартизации (ИСО) 310
Коммерческие поставщики 310
Резюме 312

ГЛАВА 12. Вызовы на пути внедрения архитектуры нулевого доверия 313

Вызовы 313
Изменение образа мышления 313
Теневые ИТ-решения 314
Разрозненные организации 315
Отсутствие связанных продуктов с нулевым доверием 316
Масштабируемость и производительность 316
Ключевые выводы 317
Технологические достижения 317
Квантовые вычисления 317
Искусственный интеллект 319
Технологии повышения конфиденциальности 321
Резюме 323

ПРИЛОЖЕНИЕ. Краткое введение в сетевые модели 324

Сетевые уровни, визуализация 324
Сетевая модель OSI 325
Уровень 1 — физический уровень 325
Уровень 2 — канальный уровень 325
Уровень 3 — сетевой уровень 326
Уровень 4 — транспортный уровень 326
Уровень 5 — сеансовый уровень 326
Уровень 6 — уровень представления 326
Уровень 7 — прикладной уровень 327
Сетевая модель TCP/IP 327

Предметный указатель 328

Об авторах 333

Об изображении на обложке 335