Digital Security
БЕЗОПАСНОСТЬ КАК ИСКУССТВО

На линии огня: UEFI BIOS

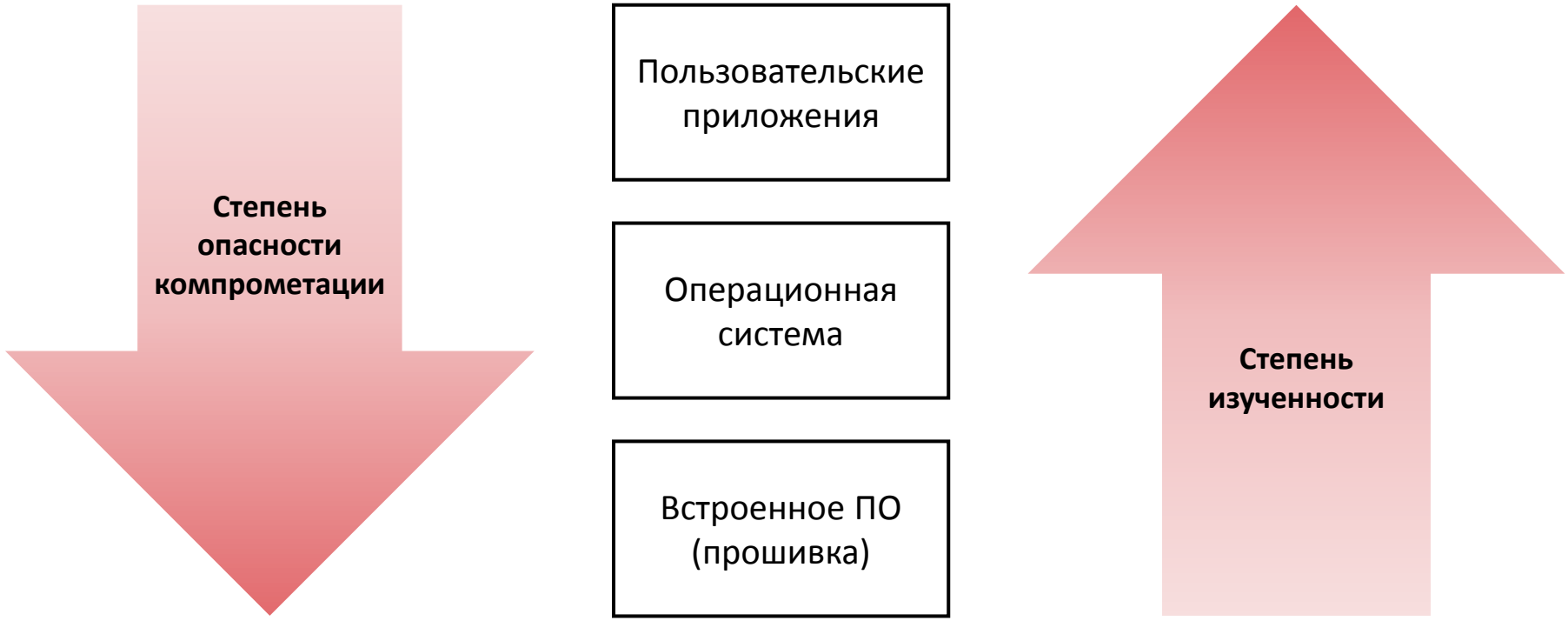
Насколько практично атаковать прошивки UEFI BIOS?

Руслан Закиров
Младший аналитик по информационной безопасности

План презентации

- Введение
- System Management Mode (SMM)
- Возможности атакующего
- Практическая сторона вопроса
- Известные инциденты
- Превентивные меры защиты
- Заключение

Текущее положение дел



Что такое BIOS

- BIOS (Basic Input/Output System) - «базовая система ввода-вывода»
- Расположен в SPI Flash-памяти
- Проверяет и конфигурирует аппаратные ресурсы
- Передает управление загрузчику ОС
- Старый тип прошивок принято называть «Legacy BIOS»

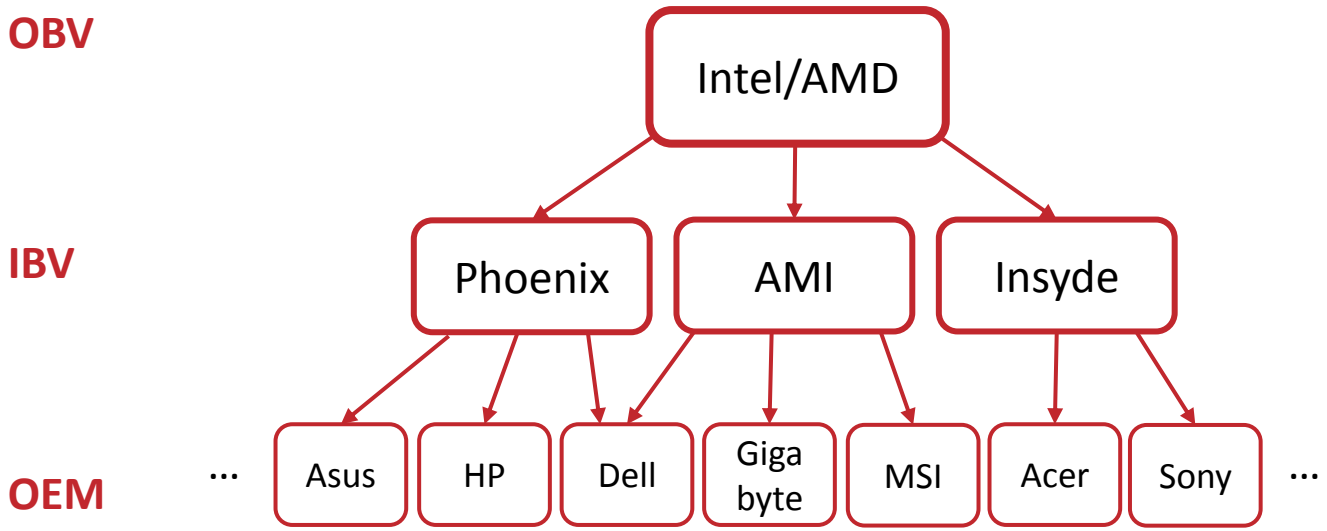
Что такое UEFI

UEFI (Unified Extensible Firmware Interface) – стандарт для унификации разработки BIOS (заменяет «legacy BIOS»)

- CPU-независимая архитектура
- Широкие возможности до запуска ОС (включая работу с сетью)
- Стандартизированная модульная структура прошивки
- Обратная совместимость
- Предоставляет runtime сервисы для ОС

Разработка кода прошивок

- Все прошивки содержат **заимствованный код** (reference code)
- Уязвимости в заимствованном коде представляют большую опасность
- Существует открытая реализация прошивки UEFI – Tianocore EDK2



Кольца привилегий

Ring 3: Пользовательские приложения

Ring 0: Ядро операционной системы

Ring -1: Гипервизор

Ring -2: SMM

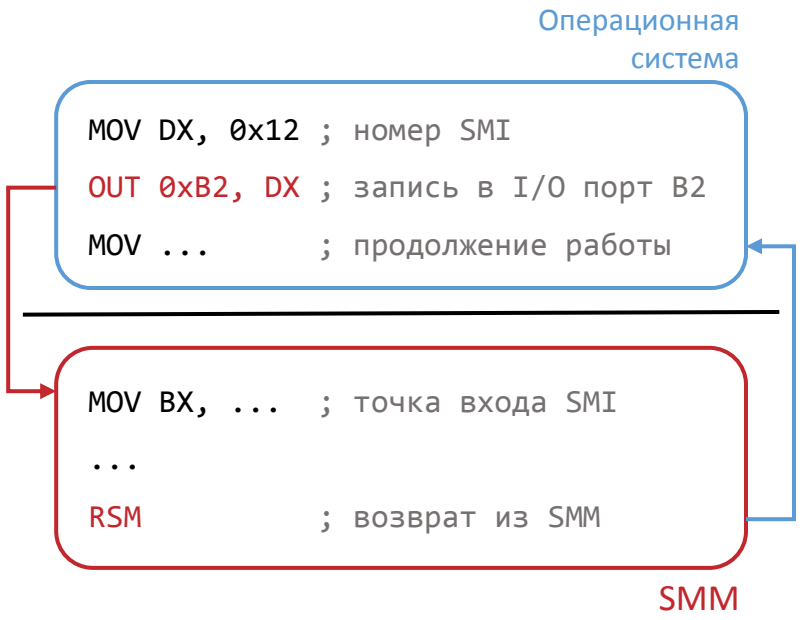
Центральный процессор

Ring -3: Intel® ME

Чипсет

System Management Mode (SMM)

- Наиболее привилегированный режим исполнения центрального процессора
- BIOS содержит код, предназначенный для исполнения в режиме SMM
- Во время загрузки помещается в недоступную для ОС память (SMRAM)
- Предназначен для управления аппаратными ресурсами
- Выполняется незаметно для ОС
- Переход в режим SMM происходит через вызов системного прерывания (System Management Interrupt)
- В момент работы SMM выполнение ОС полностью останавливается



Возможности SMM / Возможности атакующего

- Доступ ко всей физической памяти
- Доступ к любым устройствам
- Вмешательство в любое действие ОС
- Недосягаемость для ОС

→ Дамп приватных ключей из памяти

→ Перехват нажатий клавиш (все пароли и почта)

→ Запуск приложений, чтение файлов

→ Невозможность обнаружения антивирусными продуктами

- Свободный доступ к сетевому интерфейсу в обход любых фильтров ОС
- Запись в SPI Flash (место хранения BIOS)

→ Прослушивание трафика и скрытая коммуникация с командным центром вредоносного ПО

→ «Иммунитет» к переустановке ОС

Возможности атакующего (закрепление в системе)

- **Unified** Extensible Firmware Interface → возможность атаковать большее количество платформ
- Появляется много «доказательств концепции» (proof of concept) вредоносного ПО → готовая основа:
  - The Sea Watcher
  - dreamboot
  - UEFI-Bootkit
  - SMM backdoor

Возможности атакующего (закрепление в системе)

- **Unified** Extensible Firmware Interface → возможность атаковать большее количество платформ
- Появляется много «доказательств концепции» (proof of concept) вредоносного ПО → готовая основа:
  - The Sea Watcher
  - dreamboot
  - UEFI-Bootkit
  - SMM backdoor

  - Инфицирование модуля прошивки UEFI
  - Дамп памяти SMM (SMRAM)
  - Чтение/запись любой области памяти
  - Повышение привилегий любого приложения

Практическая сторона вопроса

USER → SMM ?

- Пользователь → Администратор
- Администратор → Ядро ОС
- Ядро ОС → SMM

- SMM → Закрепление в системе

Практическая сторона вопроса

USER → SMM ?

- ✓ Пользователь → Администратор
- ○ Администратор → Ядро ОС
- ○ Ядро ОС → SMM
- ○ SMM → Закрепление в системе

- • Обход User Access Control (6 актуальных методов): UACMe

Практическая сторона вопроса

USER → SMM ?

- ✓ Пользователь → Администратор
- ✓ Администратор → Ядро ОС
- ○ Ядро ОС → SMM
- ○ SMM → Закрепление в системе

- • Обход User Access Control (6 актуальных методов): UACMe
- • Уязвимые подписанные драйверы (популярные): Secret Net, Virtual Box

Практическая сторона вопроса

USER → SMM ?

- ✓ Пользователь → Администратор
- ✓ Администратор → Ядро ОС
- ✓ Ядро ОС → SMM

- • Обход User Access Control (6 актуальных методов): UACMe
- • Уязвимые подписанные драйверы (популярные): Secret Net, Virtual Box
- • Уязвимости в обработчиках SMI (за прошлый год): 1, 2, 3, 4

- ○ SMM → Закрепление в системе

Практическая сторона вопроса

USER → SMM ?

- ✓ Пользователь → Администратор
- ✓ Администратор → Ядро ОС
- ✓ Ядро ОС → SMM
- ○ SMM → Закрепление в системе

- Обход User Access Control (6 актуальных методов): UACMe
- Уязвимые подписанные драйверы (популярные): Secret Net, Virtual Box
- Уязвимости в обработчиках SMI (за прошлый год): 1, 2, 3, 4
  - Мало кто задумывается об обновлении прошивок
  - Не все разработчики оперативно выпускают патчи
  - Разработчики могут перестать выпускать патчи для относительно старых систем
  - Низкобюджетные системы зачастую не получают обновлений прошивки

Практическая сторона вопроса

USER → SMM ?

- ✓ Пользователь → Администратор
- ✓ Администратор → Ядро ОС
- ✓ Ядро ОС → SMM
- ✓ SMM → Закрепление в системе

- Обход User Access Control (6 актуальных методов): UACMe
- Уязвимые подписанные драйверы (популярные): Secret Net, Virtual Box
- Уязвимости в обработчиках SMI (за прошлый год): 1, 2, 3, 4
  - Мало кто задумывается об обновлении прошивок
  - Не все разработчики оперативно выпускают патчи
  - Разработчики могут перестать выпускать патчи для относительно старых систем
  - Низкобюджетные системы зачастую не получают обновлений прошивки
- Уязвимые/выключенные механизмы защиты flash-памяти

Закрепление в системе в контексте SMM

Механизмы защиты, предотвращающие внедрение вредоносного кода в прошивку UEFI:

- BIOS Write Protection (регистры чипсета)
- UEFI Secure Boot

- Intel® TXT
- Intel® Boot Guard
- Intel® Bios Guard

Закрепление в системе в контексте SMM

Механизмы защиты, предотвращающие внедрение вредоносного кода в прошивку UEFI:

- ✓ BIOS Write Protection (регистры чипсета)
- ○ UEFI Secure Boot

- ○ Intel® TXT
- ○ Intel® Boot Guard
- ○ Intel® Bios Guard

- VU#766164, CVE-2015-3692, неправильная настройка

Закрепление в системе в контексте SMM

Механизмы защиты, предотвращающие внедрение вредоносного кода в прошивку UEFI:

- ✓ BIOS Write Protection (регистры чипсета)
- ✓ UEFI Secure Boot
  - ○ Intel® TXT
  - ○ Intel® Boot Guard
  - ○ Intel® Bios Guard

- VU#766164, CVE-2015-3692, неправильная настройка
- “Golden Key”, CVE-2016-5247, All Your Boot Are Belong To Us (CanSecWest, 2014)

Закрепление в системе в контексте SMM

Механизмы защиты, предотвращающие внедрение вредоносного кода в прошивку UEFI:

- ✓ BIOS Write Protection (регистры чипсета)
- ✓ UEFI Secure Boot
- ✓ Intel® TXT
  - ○ Intel® Boot Guard
  - ○ Intel® Bios Guard

- VU#766164, CVE-2015-3692, неправильная настройка
- “Golden Key”, CVE-2016-5247, All Your Boot Are Belong To Us (CanSecWest, 2014)
- ITL 2009, ITL 2009, ITL 2011

Закрепление в системе в контексте SMM

Механизмы защиты, предотвращающие внедрение вредоносного кода в прошивку UEFI:

- ✓ BIOS Write Protection (регистры чипсета)
- ✓ UEFI Secure Boot
- ✓ Intel® TXT
- ✓ Intel® Boot Guard
- ○ Intel® Bios Guard

- VU#766164, CVE-2015-3692, неправильная настройка
- “Golden Key”, CVE-2016-5247, All Your Boot Are Belong To Us (CanSecWest, 2014)
- ITL 2009, ITL 2009, ITL 2011
- Safeguarding Rootkits: Intel BootGuard (ZeroNights, 2016)

Закрепление в системе в контексте SMM

Механизмы защиты, предотвращающие внедрение вредоносного кода в прошивку UEFI:

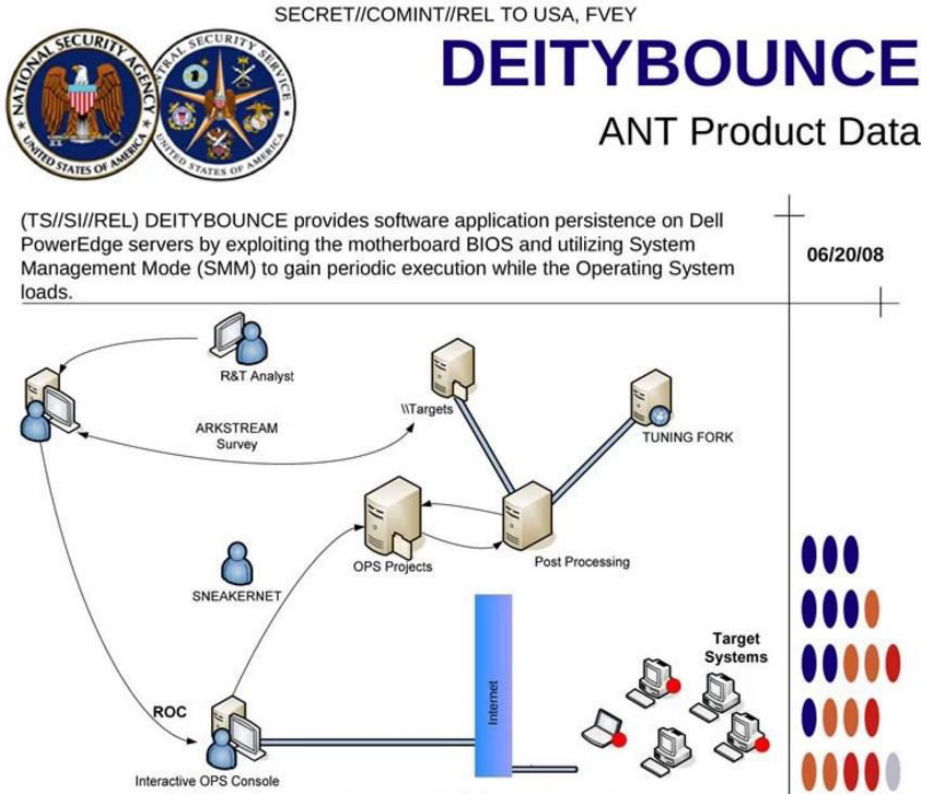
✓ BIOS Write Protection (регистры чипсета)	• VU#766164, CVE-2015-3692, неправильная настройка
✓ UEFI Secure Boot	• “Golden Key”, CVE-2016-5247, All Your Boot Are Belong To Us (CanSecWest, 2014)
✓ Intel® TXT	• ITL 2009, ITL 2009, ITL 2011
✓ Intel® Boot Guard	• Safeguarding Rootkits: Intel BootGuard (ZeroNights, 2016)
✓ Intel® Bios Guard	• Выключен по умолчанию

Большинство механизмов выключено по умолчанию!

Реальна ли эта угроза?

Известные миру инциденты:

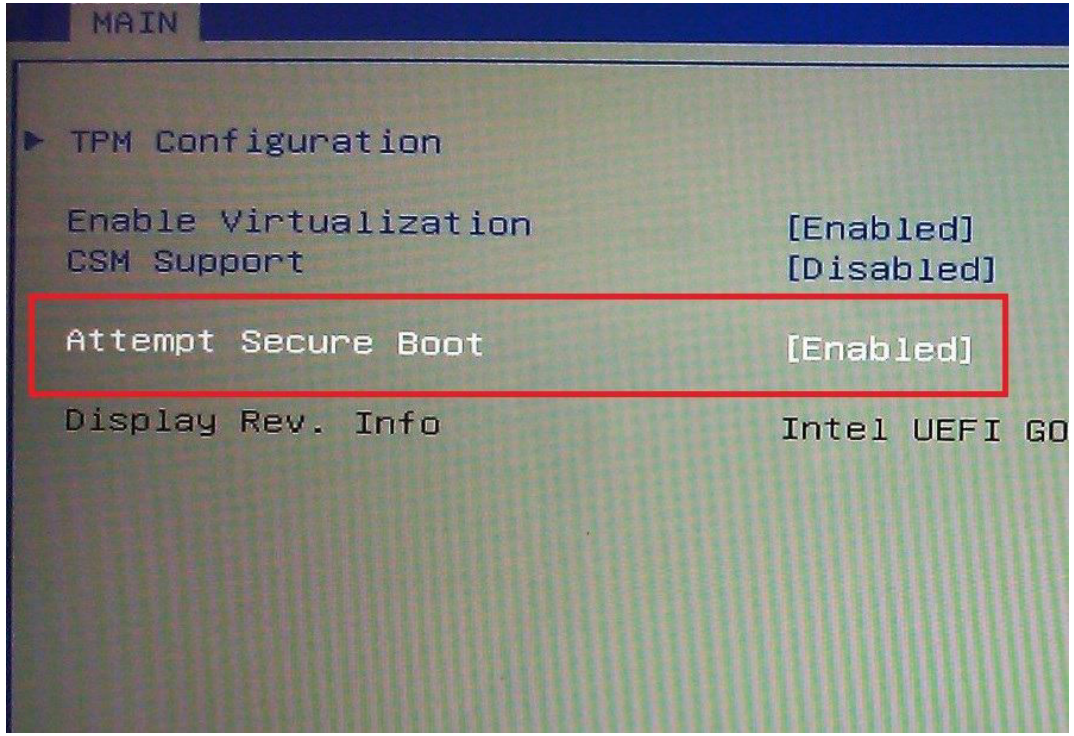
- Hacking Team UEFI Vector (bootkit)
- NSA DEITYBOUNCE (backdoor)
- Lenovo Computrace (spyware)



[The UEFI Firmware Rootkits: Myths and Reality (ZeroNights, 2016)]

Превентивные меры защиты

- Своевременные обновления BIOS
- Активация настроек безопасности в BIOS
- Windows SMM Security Mitigations Table (Windows 10, 1607)
- Системы автоматизированной проверки целостности встроенного ПО (Copernicus, virustotal)



Заключение

- Не стоит думать о безопасности прошивок, как о проблеме «завтрашнего дня»
- Чем ниже закрепляется атакующий, тем больше у него возможностей и тем труднее его обнаружить
- **А Вы уверены, что Ваша система не скомпрометирована?**

Вопросы?

Спасибо за внимание!
Вопросы?

Digital Security в Москве: (495) 223-07-86
Digital Security в Санкт-Петербурге: (812) 703-15-47

Руслан Закиров
r.zakirov@dsec.ru

BACKUP

Tails OS vs LightEater

EXTRA SLIDES

Tails OS:

- «Живая ОС»
- Все соединения идут через Tor
- Приватность и анонимность
- Не оставляет следов на машине
- Использовалась Эдвардом Сноуденом

LegbaCore LightEater:

- «Доказательство концепции» вредоносного ПО UEFI
- Работает из режима SMM
- Периодически сканирует память
- Дампит PGP ключи, пароли, расшифрованные почтовые сообщения

[How Many Million BIOSes Would you Like to Infect? (2015)]

Виртуализация

EXTRA SLIDES

- Высокая сложность полной виртуализации
- Компрометация SMM приводит к компрометации гипервизора
- Xen: Xen 0wning Trilogy (3 атаки)
- Attacking Hypervisors via Firmware and Hardware (BlackHat, 2015)

Изоляция на основе виртуализации