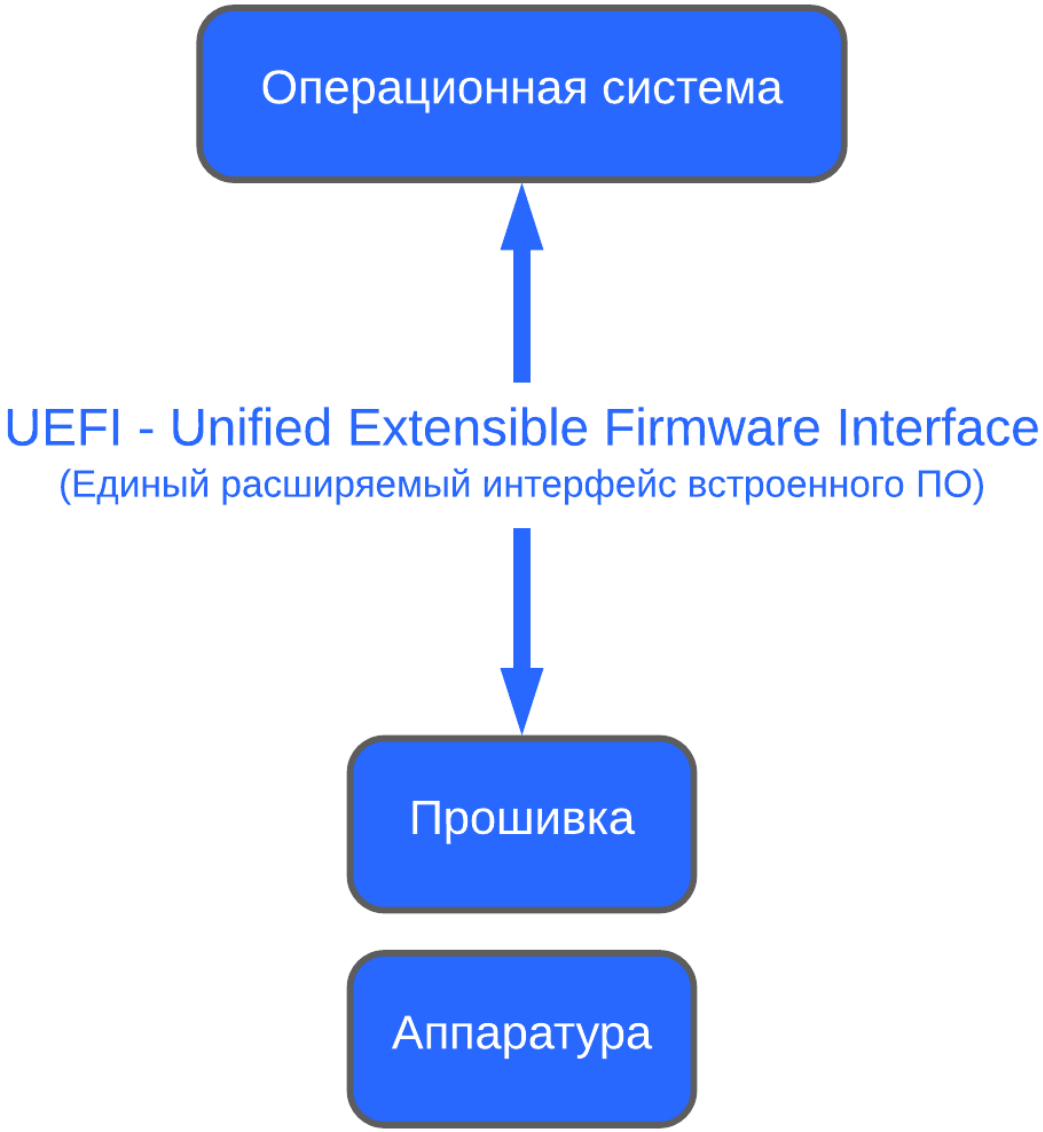
Защищённая UEFI прошивка для виртуальных машин

М. Ю. Кричанов <krichanov@ispras.ru>
В. Ю. Чепцов <cheptsov@ispras.ru>

15 октября 2021 г.

ИСП РАН

Назначение UEFI



Прошивка UEFI сегодня

- Мини-ОС, как средство взаимодействия с пользователем с максимально широким функционалом.

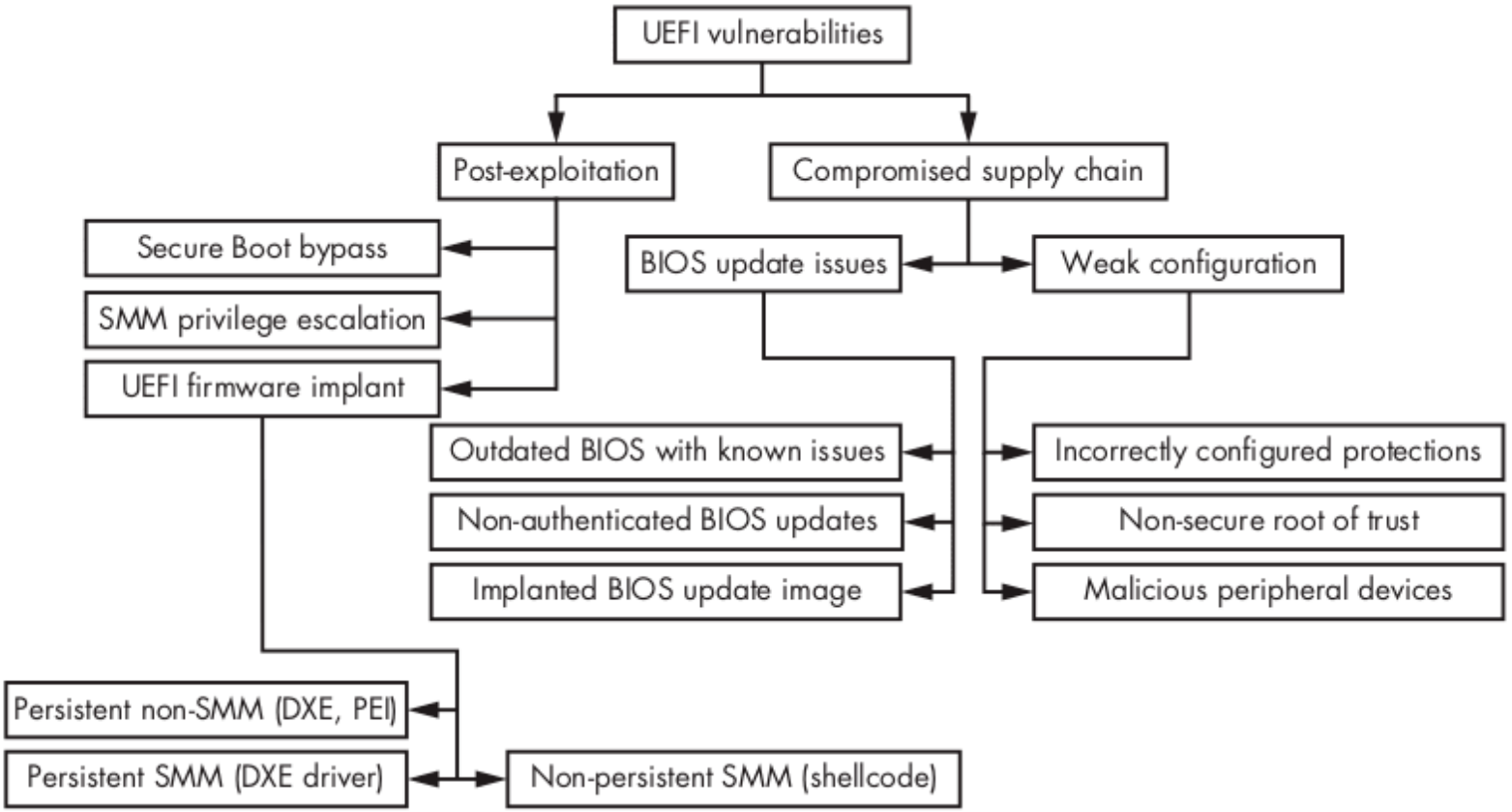
Прошивка UEFI сегодня

- Мини-ОС, как средство взаимодействия с пользователем с максимально широким функционалом.
- Если удалить из прошивки код, который не нужен для загрузки ОС, то можно получить выигрыш до 70%.

Модель материнской платы	Исходный размер прошивки (KiB)	Конечный размер прошивки (KiB)	Процент удалённого кода
SuperMicro A1SAi-2550F (V519)	3013	903	70.91%
Tyan 5533V101	4520	1916	39.82%
HP DL380 Gen10	46102	27809	39.68%

Jake Christensen, Ionut Mugurel Anghel, Rob Taglang, Mihai Chiroiu, Radu Sion: **DECAF: Automatic, Adaptive De-bloating and Hardening of COTS Firmware**. In: 29th USENIX Security Symposium, USENIX Security 2020.

Почему прошивка должна измениться (и уменьшиться)?



Alex Matrosov, Eugene Rodionov, Sergey Bratus: **Rootkits and Bootkits. Reversing Modern Malware and Next Generation Threats**. No Starch Press, Inc, San Francisco, 2019.

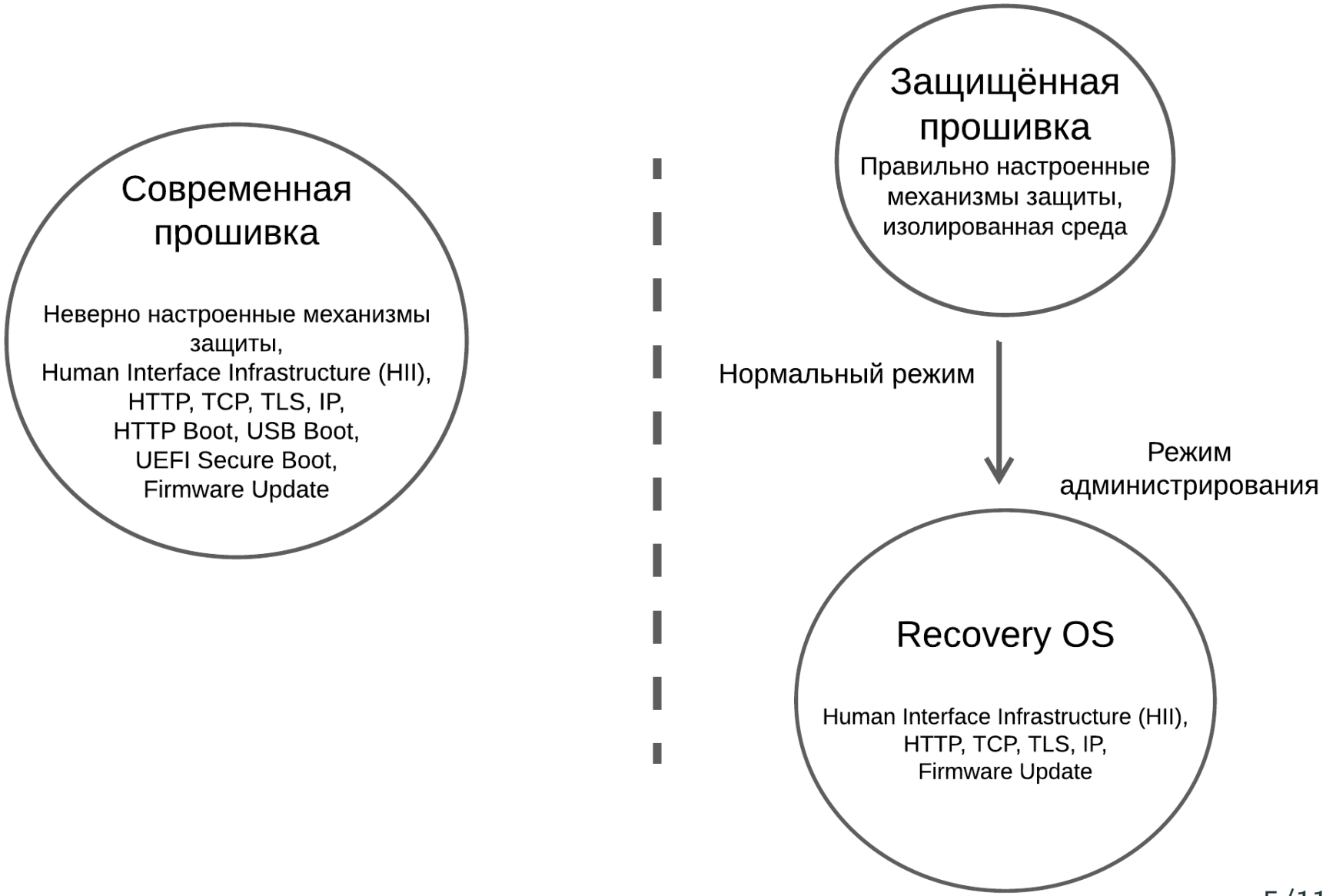
Типичные проблемы безопасности на UEFI платформе

- ☞ Software
  1. Широкая поверхность для атак в опциональном коде.
  2. Обновление BIOS без аутентификации.
  3. Устаревший BIOS с известными проблемами безопасности.
  4. Загрузчики ОС некорректно строят цепочку безопасности.
  5. UEFI Secure Boot содержит ошибки в архитектуре и реализации.
- ☞ Hardware
  1. Неверно настроенные механизмы защиты SPI флэш-памяти.
  2. Использование SMM как trust boundary.
  3. Вредоносные периферийные устройства с поддержкой DMA.
  4. Выход из S3 приводит к менее безопасному состоянию платформы.
  5. Сопроцессоры (например, Intel ME) имеют привилегированный доступ к платформе и содержат уязвимости.

Прошивка UEFI завтра

Прошивка UEFI завтра

Прошивка UEFI завтра



Виртуальные машины

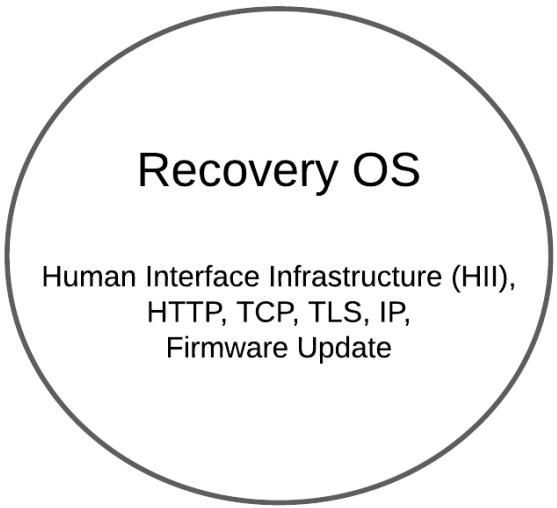
- Для запуска гостевой ОС также необходима прошивка.
- Все современные ОС поддерживают или требуют UEFI (например, Windows 11).
- Многие возможности современной аппаратуры (например, шифрование памяти AMD SEV, изолированная среда Intel SGX, TPM 2.0) реализованы только для UEFI окружения.
- Как следствие, проблемы прошивок для реального железа переносятся и на виртуальные машины.

Особенности прошивки для виртуальных машин

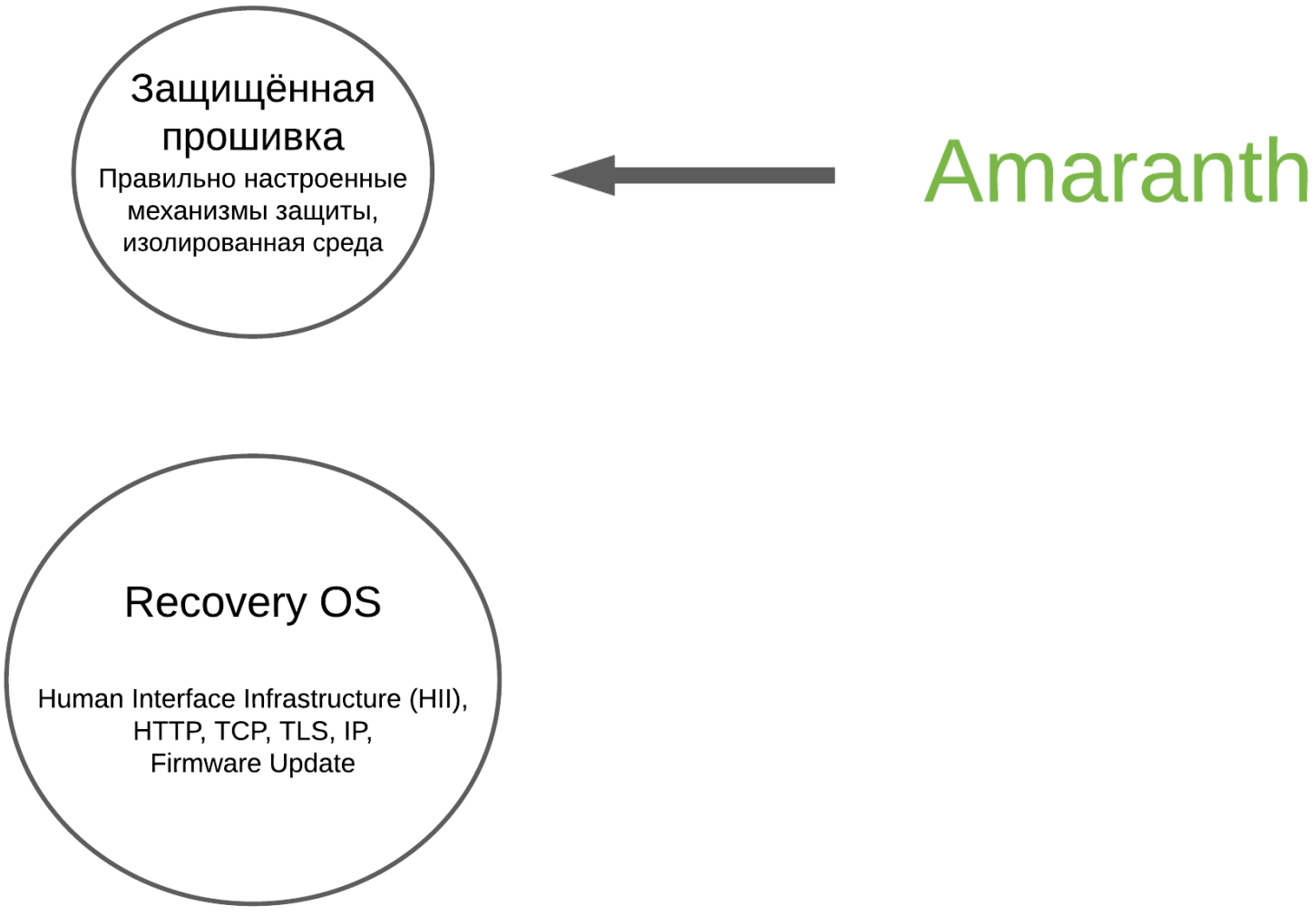
1. Отключена возможность записи во флэш-память.
2. SMM может быть отключён*.
3. Периферийные устройства ограничены.
4. Отсутствует S3 – система не спит.
5. Сопроцессоры наподобие Intel ME вне контура.

* Если в прошивке можно реализовать безопасную загрузку без SMM.

UEFI прошивка для виртуальных машин сегодня

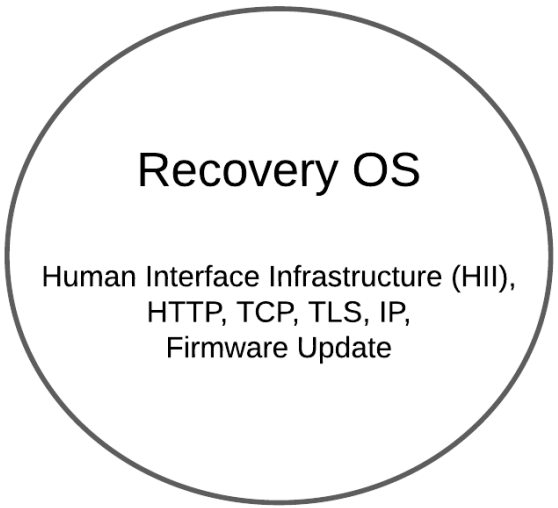


UEFI прошивка для виртуальных машин сегодня



UEFI прошивка для виртуальных машин сегодня

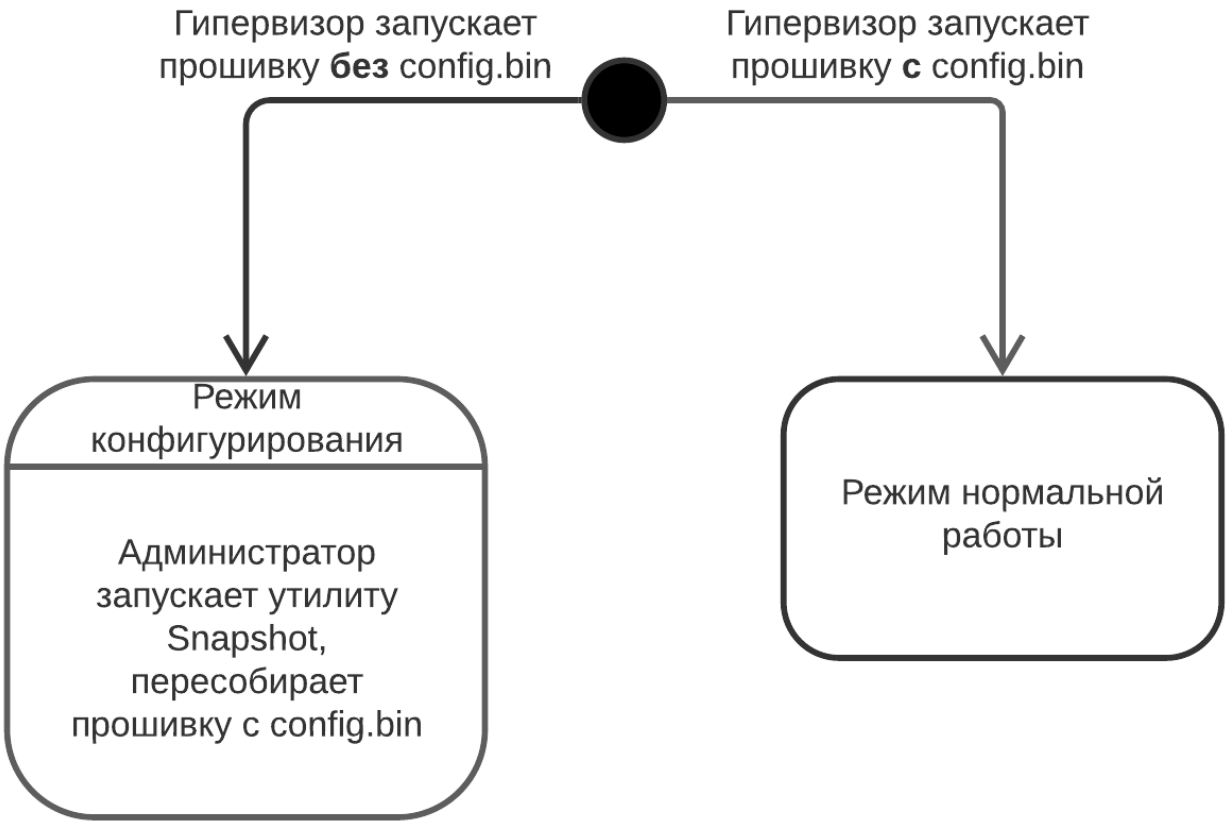
Amaranth



Интерфейс гипервизора

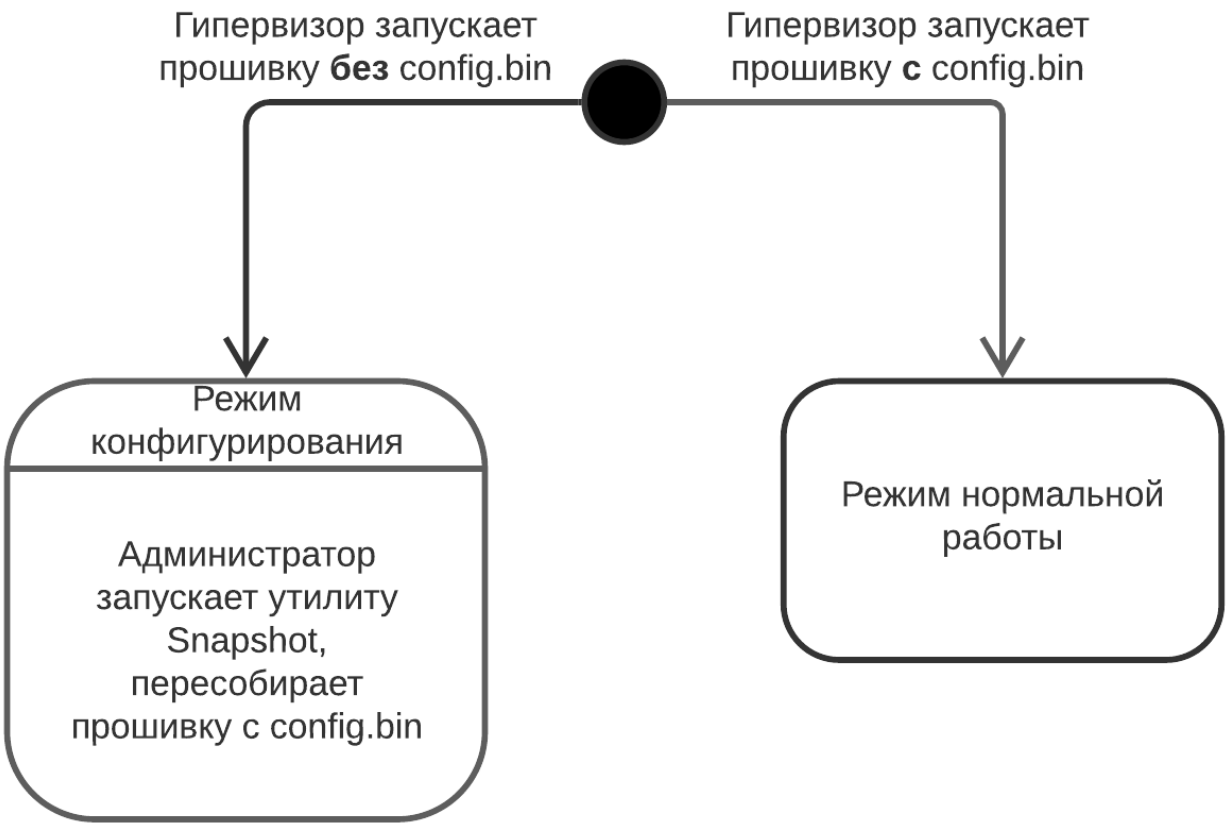
Защита гостевой ОС

- Для поддержания целостности ОС между перезагрузками, в том числе невидимыми для гипервизора, прошивка использует механизм Snapshot.



Защита гостевой ОС

- Для поддержания целостности ОС между перезагрузками, в том числе невидимыми для гипервизора, прошивка использует механизм Snapshot.
- Механизм Snapshot позволяет администратору настроить проверки достаточно гибко для любой ОС.



Защищённая среда Amaranth

- Используются современные средства разработки критически важного ПО, такие как фаззинг-тестирование, статический анализ и формальная верификация*.

*Marvin Häuser, Vitaly Cheptsov: *Securing the EDK II Image Loader*

Защищённая среда Amaranth

- Используются современные средства разработки критически важного ПО, такие как фаззинг-тестирование, статический анализ и формальная верификация*.
- Поддерживаются архитектуры x86 и x86_64.

*Marvin Häuser, Vitaly Cheptsov: *Securing the EDK II Image Loader*

Защищённая среда Amaranth

- Используются современные средства разработки критически важного ПО, такие как фаззинг-тестирование, статический анализ и формальная верификация*.
- Поддерживаются архитектуры x86 и x86_64.
- Поддерживается защита памяти, стековые канарейки и автоматическая инициализация переменных.

*Marvin Häuser, Vitaly Cheptsov: *Securing the EDK II Image Loader*

Защищённая среда Amaranth

- Используются современные средства разработки критически важного ПО, такие как фаззинг-тестирование, статический анализ и формальная верификация*.
- Поддерживаются архитектуры x86 и x86_64.
- Поддерживается защита памяти, стековые канарейки и автоматическая инициализация переменных.
- Функционал прошивки минимизирован до необходимого для запуска предела.

*Marvin Häuser, Vitaly Cheptsov: *Securing the EDK II Image Loader*

Защищённая среда Amaranth

- Используются современные средства разработки критически важного ПО, такие как фаззинг-тестирование, статический анализ и формальная верификация*.
- Поддерживаются архитектуры x86 и x86_64.
- Поддерживается защита памяти, стековые канарейки и автоматическая инициализация переменных.
- Функционал прошивки минимизирован до необходимого для запуска предела.
- В вычислительно ёмких операциях используется аппаратное ускорение вычислений.

*Marvin Häuser, Vitaly Cheptsov: *Securing the EDK II Image Loader*

Заключение

Amaranth позволяет существенно уменьшить угрозы:

- имплантов в UEFI прошивке, при программных перезагрузках ОС в обход гипервизора;
- подмены (изменения) загрузчика ОС и/или файлов, используемых им в процессе загрузки, в том же сценарии перезагрузки;
- повышения привилегий в результате эксплуатации уязвимостей служб времени исполнения прошивки.

Заключение

Amaranth позволяет существенно уменьшить угрозы:

- имплантов в UEFI прошивке, при программных перезагрузках ОС в обход гипервизора;
- подмены (изменения) загрузчика ОС и/или файлов, используемых им в процессе загрузки, в том же сценарии перезагрузки;
- повышения привилегий в результате эксплуатации уязвимостей служб времени исполнения прошивки.

Опыт применения Amaranth к виртуальным машинам планируется распространить на физическое оборудование для платформ Intel.

Спасибо за внимание