Кибербезопасность, основные угрозы 2016 и новые технологии Intel

Дмитрий Ларюшин

24.02.2016

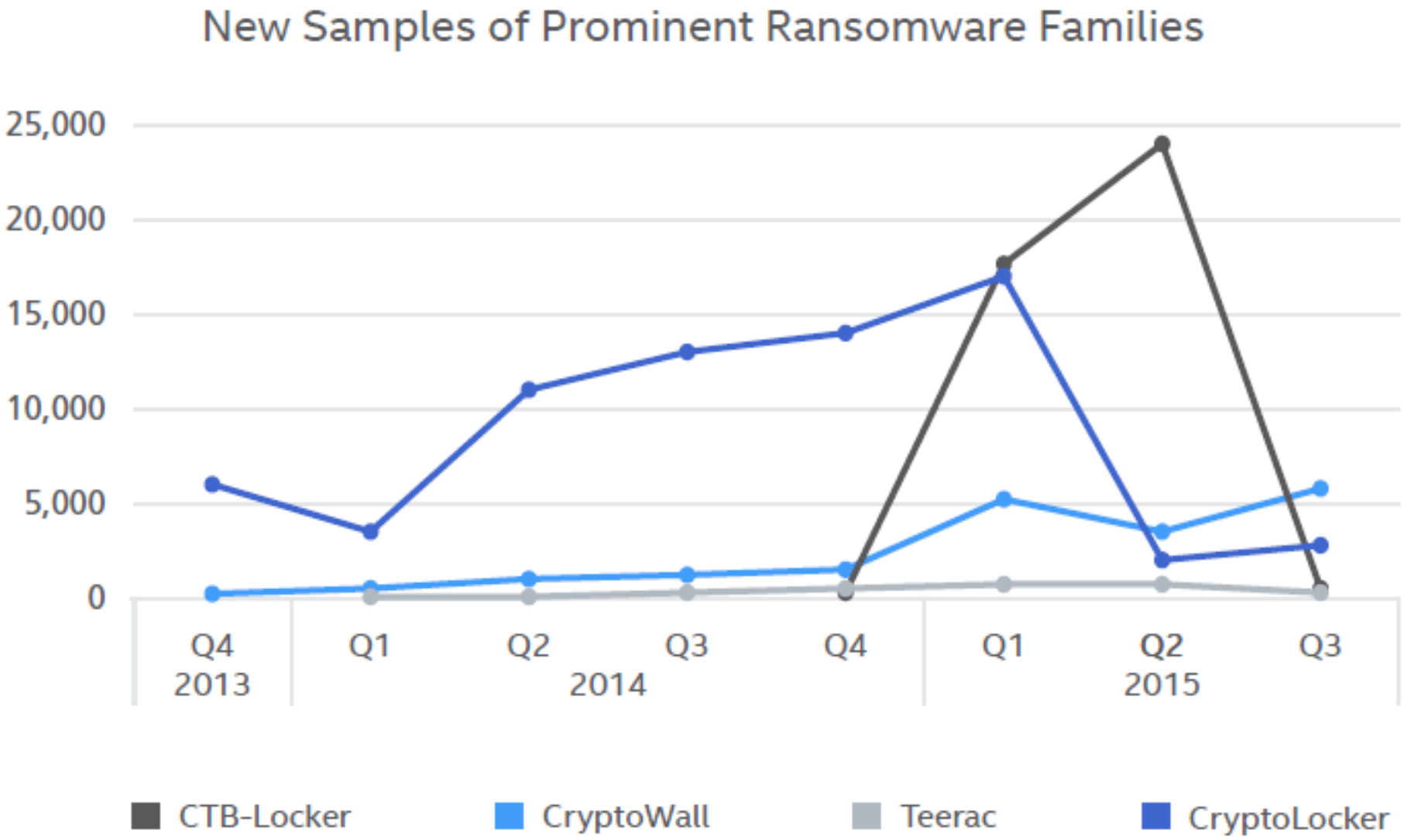
Основные угрозы ИБ на 2016+ (ISG)

- **Драйверы киберугроз (Предсказания 2011+):**
  - Расширение поверхности кибератак,
  - Индустриализация [отрасли] хакерства,
  - Растущая сложность и фрагментация рынка ИБ
- **Взгляды на 2016-2020:**
  - Продолжение расширегия поверхности кибератак,
  - Техническая изощренность атакующих,
  - Растущая стоимость потерь от разрывов в ИБ защите,
  - Недостаток интегрированных технологий ИБ безопасности,
  - Нехватка квалифицированных талантов для отражения кибератак

Основные Угрозы: Hardware

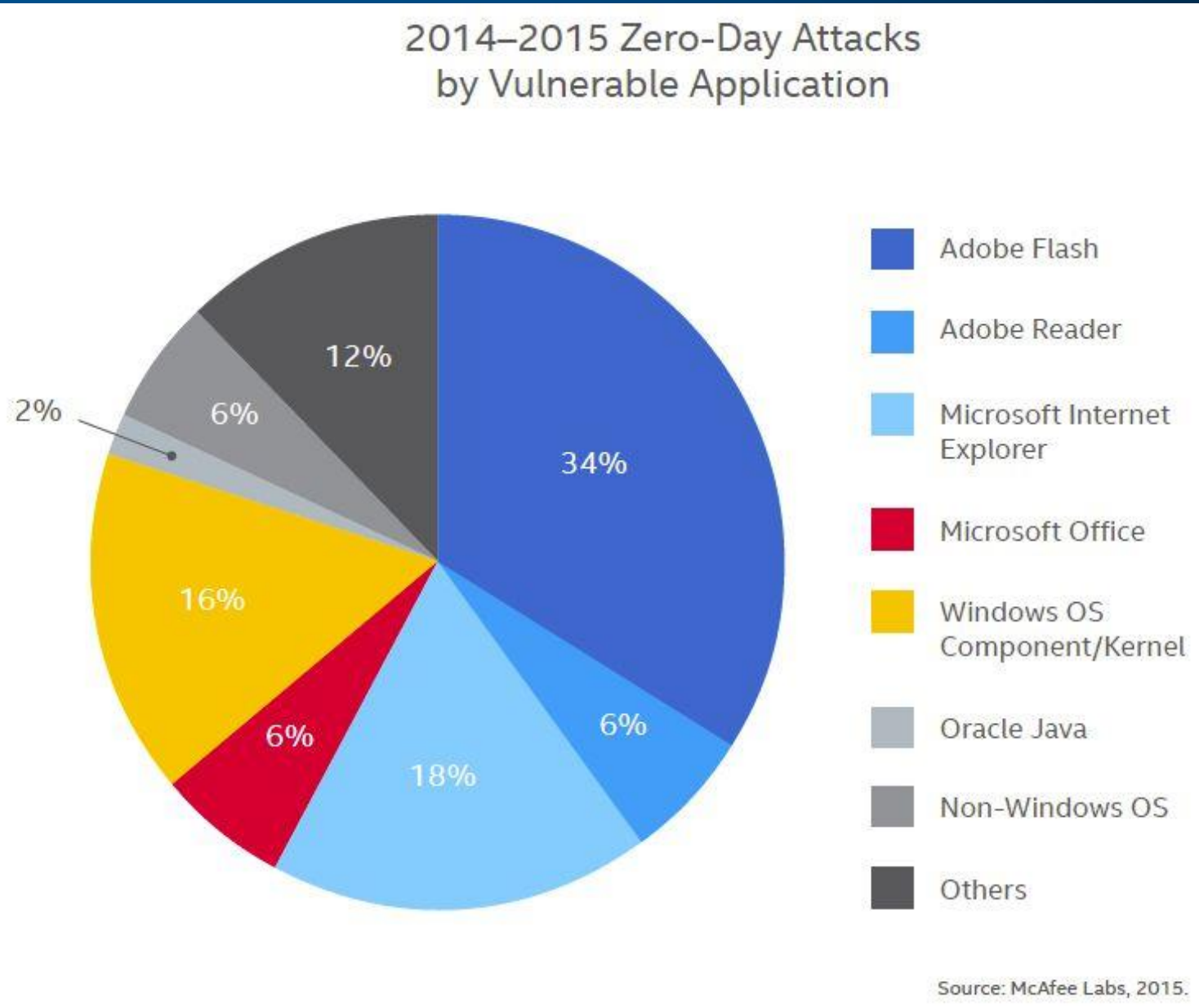
- Гонка вниз по стеку.
- К традиционным атакам на прошивки к жестким дискам и управлению графикой, мы наблюдаем увеличение атак направленных на уязвимости в BIOS (UEFI) и драйверах периферии.
- Последние атаки на аппаратную часть демонстрируют знание мельчайших подробностей встроенного кода различных производителей, при этом вирусы могут выживать даже после переустановки ОС и форматирования жесткого диска.
- Появление коммерческого инструметрия для атак UEFI Rootkit

Основные угрозы: Ransomware

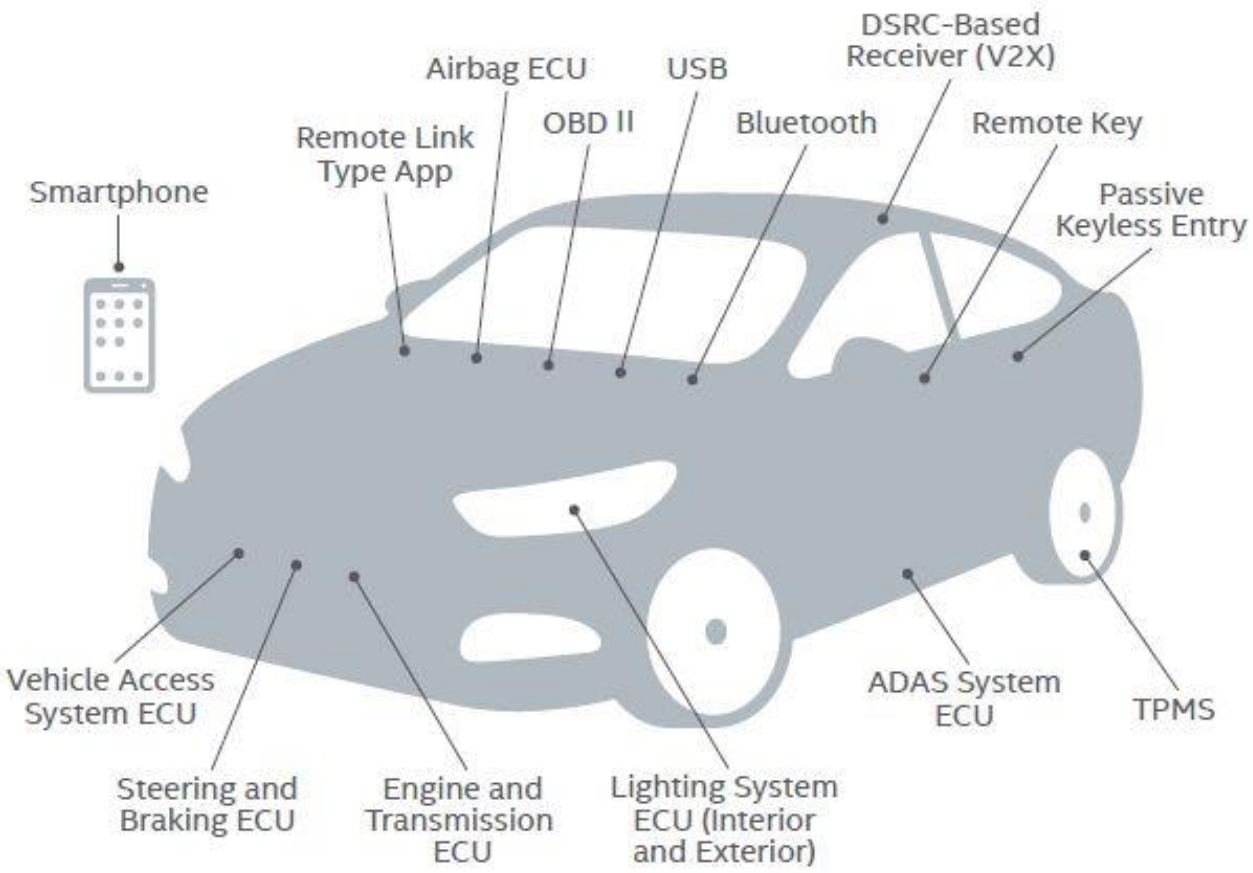


Source: McAfee Labs, 2015.

Основные угрозы: Уязвимости приложений



Основные угрозы: Автомобильные системы



Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

Основные угрозы

- Облака и облачные сервисы,
- Корпоративные системы,
- Виартуализация управления сетями (SDN, NFV),
- Объекты критической инфраструктуры:
  - Stuxnet (2009), иранские ядерные объекты,
  - Operation Dragonfly (2014), цифровые системы электроснабжения
- Кибер-шпионаж,
- Платежные системы,
- Персональные данные,
- Хактивизм

Индустрия ИБ наносит ответный удар

- Рост количества устройств (более 220 млрд к 2020) требует привлечения новых подготовленных специалистов. Исследовательские и образовательные усилия компаний.
- Обмен экспертизой угроз и отражения атак между предприятиями, поставщиками и спецслужбами.
- Поведенческая аналитика – новое оружие в инструментарии служб ИБ.
- Дальнейшее развитие иснтрументов защиты: защищенная загрузка, доверенная среда исполнения, ускорение криптографических алгоритмов, активная защита памяти, неизменная идентификация устройств и проч.

Технологии Intel, AES-NI

- Дополнительный набор микрокоманд центрального процессора x86, заточенный под ускорение операций шифрование протоколом AES,
- Модели использования:
  - Шифрование коммуникационного канала (SSL, TLS, HTTPS, FTP and SSH),
  - Полное шифрование диска (FDE),
  - Шифрование на уровне приложений (например, банковские транзакции).
- Технология особо востребована в серверах и облачных сервисах

Технологии Intel

- Intel ® Platform Protection Technology with BIOS Guard: программно-аппаратная аутентификация и защита против атак на BIOS,
- Intel ® Platform Protection Technology with Platform Trust: интегрированное решение для хранения учетных данных и управления ключами для MS Windows 8,
- Intel ® Platform Protection Technology with Boot Guard: аутентичный программный модуль (ASM), обеспечивающий защищенную загрузку и верификацию BIOS
- Intel ® Kernel Guard Technology: спецификация политик и фраймворк для обеспечения целостности ядра и компонентов платформы.

Технологии Intel, TXT

- Intel ® Trusted Execution Technology – аппаратная технология для повышения защищенности серверных платформ,
- TXT была специально спроектирована для укрепления защиты платформ от гипервизор атак, атак на BIOS и других программ нижнего уровня, установок вредоносного ПО.
- Технология усиливает защиту, обеспечивая более высокий уровень контроля за цепочкой запуска и давая возможность изоляции процесса загрузки.
- TXT расширяет VMX среду Intel ® Virtualization Technology, разрешая верифицированную безопасную установку, запуск и использование гипервизора или операционной системы.

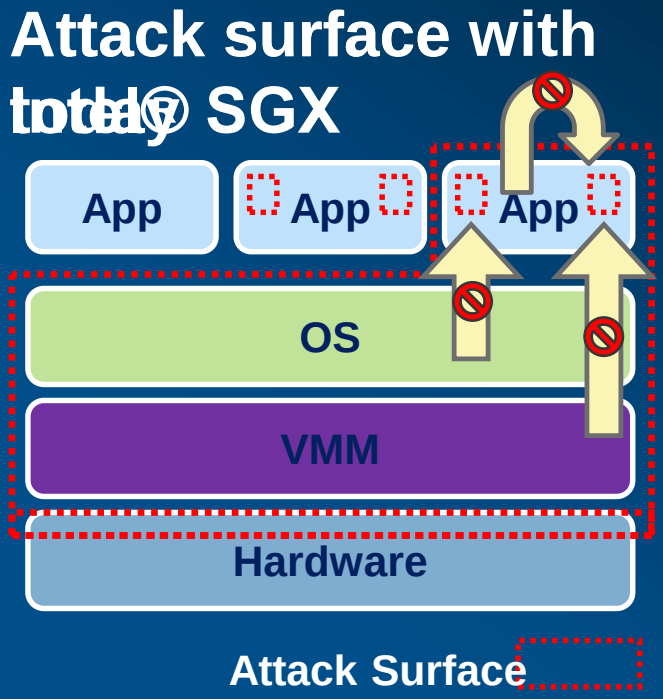
Intel® Software Guard Extensions (Intel® SGX)

- **Технология Intel® SGX:**
  - Набор новых инструкций центрального процессора, который позволяет приложениям создавать защищенные (приватные) зоны для сохранения критически важных секретов как во время исполнения, так и закрытом состоянии.

- **Intel® SGX возможности и преимущества:**
  - Существенно сжимает поверхность атаки, позволяя разработчикам приложений контролировать их безопасность.
  - Препятствует программным атакам даже в случае компрометации ОС/драйверов/BIOS/VM.
  - Препятствует слежке за шиной памяти и атак «холодного запуска» против образов памяти в RAM
  - Секреты защищены даже в случае, когда атакующий получает полный контроль за платформой.
  - Обеспечивает возможности аппаратной аттестации для измерения и верификации кода и сигнатур данных.
  - In-band исполнение программ, использующее все мощность Intel CPU

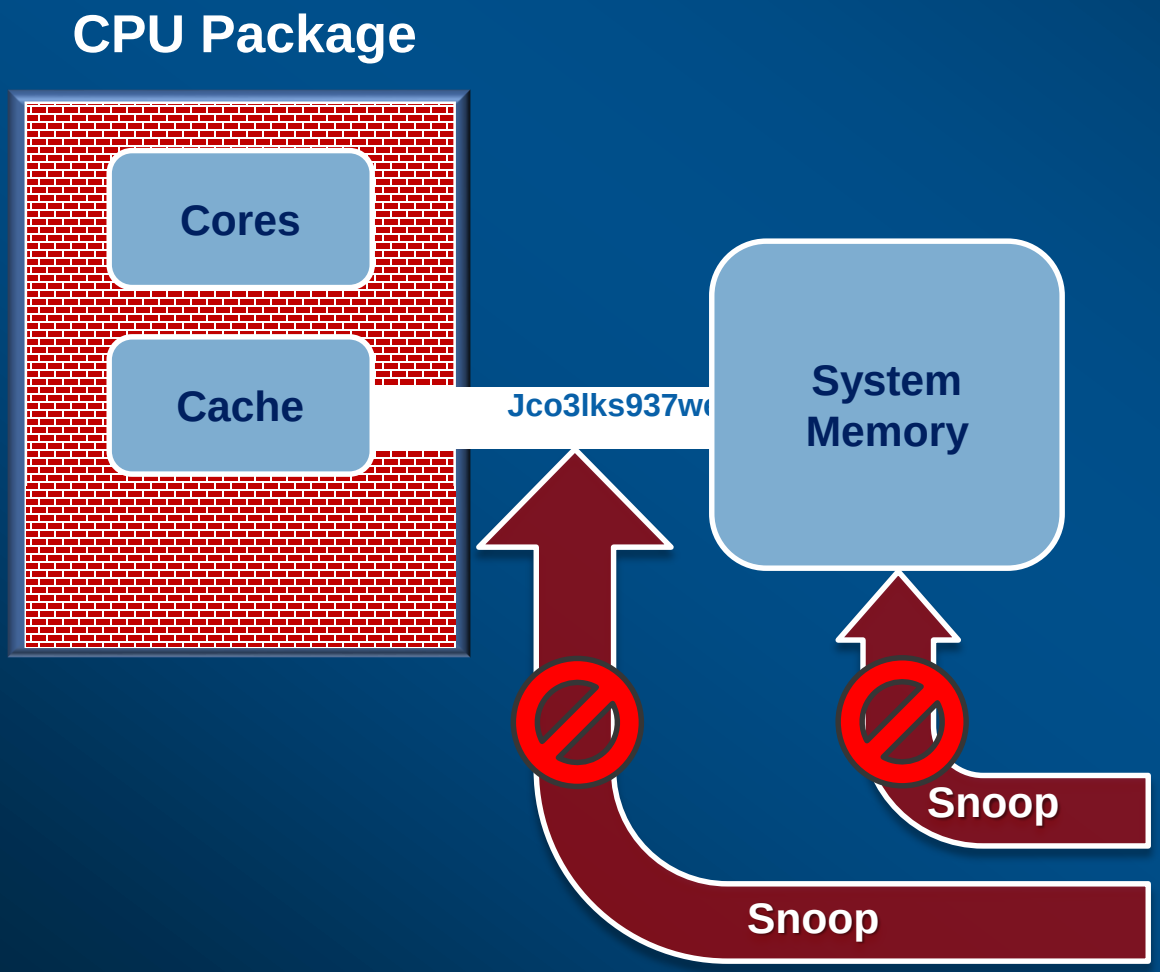
Сжатие поверхности атаки с Intel® SGX

- Приложение обретает способность защищать собственные секреты
  - Минимальная поверхность атаки (App private areas + HW)
  - Вредоносное ПО, которое разрушает любую программную компоненту выделенной зоны, не может украсть секрет из защищенной зоны.
- Знакомая IA архитектура для разработки и дебага
- Масштабирование
  - Производительность ЦП
  - Память анклава приложения может быть безопасно выгружена



Масштабируемая безопасность

Защита от прослушивания шины памяти



1. Защищенным периметром является граница процессора.
2. Данные и код вне процессора зашифрованы, а целостность проверяется.
3. Чтение оперативной памяти и прослушка шины сталкивается с зашифрованными данными.

Спасибо за внимание!

SGX video