Как поссорились Иван Интелович с Иваном Опёнковичем

Вадим Жуков <zhuk@openbsd.org>
LVEE 2018, Раков, Беларусь

Широко известные факты

- **В августе 2017 года OpenBSD нарушил эмбарго на раскрытие сведений об уязвимости WPACRACK.**
- **После этого Intel не стал раскрывать OpenBSD подробности об уязвимостях в процессорах Meltdown и Spectre.**

Широко известные факты

«Всё было не так, Профессор»

— Ник Перумов

(кажется)

Краткая история CPU

Pentium FDIV	Pentium F0 0F	Intel HT
1994	1998	2008
замена	костыль	микрокод

Краткая история CPU

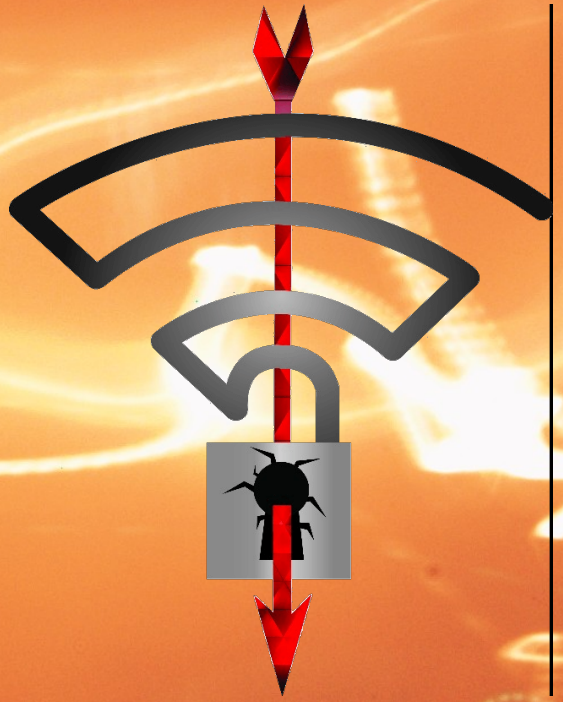
Pentium FDIV	**Pentium F0 0F**	**Intel HT**
1994	**1998**	**2008**
замена	**костыль**	**микрокод**
Motorola 6502	**AMD pop+ret**	**SPARC T4 L2**
1976	**2011**	**2014**
замена	**микрокод**	**прошивка**

Не только CPU

WPA KRACK

Key Reinstallation AttaCKs

Идея: повторное использование nonce



WPA KRACK

- **Летом 2017 года Mathy Vanhoef находит уязвимость в реализациях WPA2-PSK почти всех современных ОС.**
- **OpenBSD, с разрешения Mathy, вносит 30 августа (досрочно) исправления под видом минорной правки.**

WPA KRACK

- **OpenBSD, с разрешения Mathy, вносит 30 августа (досрочно) исправления под видом минорной правки.**
- **Ряд специалистов обратил внимание на данный патч, вследствие чего пришлось раскрыть информацию досрочно.**

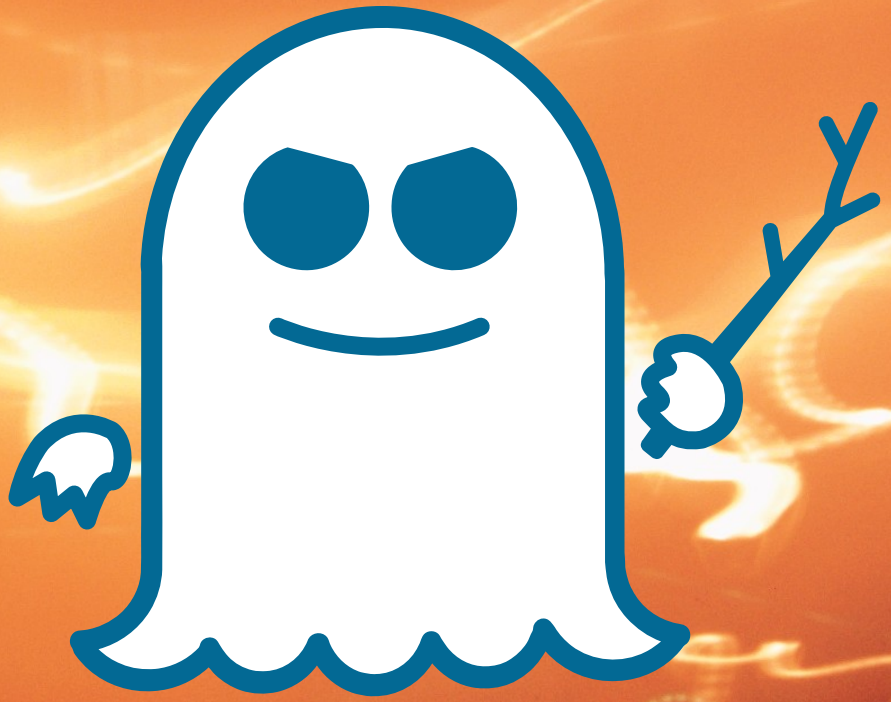
WPA KRACK

- **OpenBSD, с разрешения Mathy, вносит 30 августа (досрочно) исправления под видом минорной правки.**
- **Аналогичным образом поступили и другие разработчики ОС.**

WPA KRACK

- **OpenBSD, с разрешения Mathy, вносит 30 августа (досрочно) исправления под видом минорной правки.**
- **Тем не менее в рядах общественности сложилось мнение, что проект OpenBSD целенаправленно нарушил эмбарго.**

Meltdown & Spectre



Meltdown & Spectre

Список авторов:

- **Jann Horn (Google Project Zero)**
- **Werner Haas и Thomas Prescher (Cyberus Technology)**
- **Daniel Gruss, Moritz Lipp, Stefan Mangard и Michael Schwarz (Грацский технический университет)**

Meltdown & Spectre

- Позволяли из браузера получить доступ к памяти ядра ОС.
- Не могут быть полностью исправлены чисто программно, в т.ч. микрокодом.
- Уязвимы: x86, ARM, SPARC…
- Самые серьёзные проблемы у Intel.

Meltdown & Spectre

Уведомлены:

- **FreeBSD project**
- **Linux (разработчики ядра, Red Hat...)**
- **Microsoft**
- **Oracle и другие разработчики железа**

Meltdown & Spectre

Не уведомлены:

- **DragonFly BSD project**
- **NetBSD project**
- **OpenBSD project**
- **и вообще все остальные**

Meltdown & Spectre

Лечение (симптоматическое):

- **Доработки для компиляторов**
- **Обновление микрокода**
- **Снижение точности таймеров**
- **Отделение адресного пространства ядра**

Meltdown & Spectre: возвращение

- Spectre 3a (NG), 4...

Meltdown & Spectre: возвращение

- Spectre 3a (NG), 4...
- LazyFP

Meltdown & Spectre: возвращение

- Spectre 3a (NG), 4…
- LazyFP
- TLBleed

Meltdown & Spectre: возвращение

- Spectre 3a (NG), 4...
- LazyFP
- TLBleed
- L1TF/Foreshadow

Meltdown & Spectre: возвращение

- Spectre 3a (NG), 4...
- LazyFP
- TLBleed
- L1TF/Foreshadow
- и другие

Meltdown & Spectre: возвращение

- Spectre 3a (NG), 4...
- LazyFP
- TLBleed
- L1TF/Foreshadow
- и другие

Часть атак работает только вместе с HT!

Последствия для Intel

- Ускорился разворот в сторону ARM
- Много вопросов к менеджменту касаемо замалчивания проблем
- Пользователи высказывают претензии, поставщики оборудования внимают
- Цыплят будем считать в январе 2020 года


Спасибо!
Вопросы?

Что почитать

- Крис Касперски, «Remote Code Execution through Intel CPU Bugs»
- Paul Terner, «Retpoline: a software construct for preventing branch-target-injection»