RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: AIR-W10

Coordinated Vulnerability Disclosure: Debate from the Trenches

Paul Kocher
Independent
(formerly Rambus/
Cryptography Research)

Alex Gantman
VP Product Security,
Qualcomm

Art Manion
Vul'n Analysis Tech Mgr
CERT Coordination Center

Alex Rice
Co-Founder & CTO
HackerOne

Paul Kocher (moderator)

Founded+ran Cryptography Research (1995-2017)

Technical projects include

- Protocols (incl. co-author of SSL v3)
- Many security chip/hardware projects
- Side channels (timing attacks, differential power analysis)
- Spectre

Member of National Academies' Forum on Cyber Resilience; IACR Fellow, Member of Nat'l Academy of Engineering, Advisor & investor to security start-ups

Alex Gantman

Establishment and evolution of a broad-scale product security practice at Qualcomm

- Billions of devices
- Thousands of products
- Tens of millions of lines of code
- Tens of thousands of engineers across the globe

20+ years of experience leading global organizations to deliver secure and reliable products at scale

Alex Rice

Founder & CTO @ HackerOne

Following a passion to open lines of communication between Hackers and Enterprises.

HackerOne has enabled 1,300 organizations to coordinate the disclosure and resolution of over 100,000 valid vulnerabilities discovered by the the hacker community.

Past Life: Led Product Security @ Facebook; Security Research @ Forcepoint; Security @ State of FL; Has authored an unforgiveable amount of vulnerable software

Art Manion

"The" CERT Coordination Center (at the SEI, an FFRDC at CMU)

Coordinated Vulnerability Disclosure since 1988 (2001 personally)

"Don't use IE" and "Replace CPU hardware"

CVD standards, policy, normalization in ISO, FIRST, CVE, OASIS, other places, also care about vulnerability data and information systems, prioritization and risk, supply chain transparency and relationships (SBOM!)

My team studies exploits, the vulnerability ecosystem, develops fuzzing (BFF) and other vulnerability discovery tools

Theory…

A good Samaritan finds a vulnerability

↓

Quietly notifies the vendor

↓

Vendor promptly creates fix and pushes to end users

↓

Spectre & Meltdown

Several discoverers (+ varying motives)

- Google Project Zero + me + academics…

Many vendors + vendor types

- CPU makers, chipmakers, O/S vendors, device makers, virtualization systems, cloud hosting, browsers, compilers, drivers, libraries…
- Other stakeholders: Gov't, major users, press…

Who coordinates… & decides who is 0-day'd?

- Discoverers, vendor(s), a 3rd party…

What if no clean, rapid fix?

- In-field mitigations may be partial or impossible
- Vendors may fear liability, PR, internal blame…
- Fixes can be slow to develop, percolate supply chain

Many bugs are uncomplicated, but Spectre messiness is not unique

- Differential Power Analysis
- WiFi/RC4 issues (KRACK…)
- Heartbleed
- Dual-EC DRBG
- Glibc vulnerabilities (getaddrinfo…)
- RowHammer
- DNS cache poisoning aka Kaminsky Bug
- Vendor-complicit privacy leaks
- …

Vulnerabilities in components, standards, or common practices

Conflicting incentives or expectations