ARMY CYBER INSTITUTE

Weekly Cyber Threat Report

Meltdown and Spectre Side-Channel Vulnerability Guidance.

Items of Interest: Defensive Cyberspace Operations / Critical Vulnerabilities

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre. These attacks are described in detail by CERT/CC's Vulnerability Note VU#584653, the United Kingdom National Cyber Security Centre's guidance on Meltdown and Spectre, Google Project Zero, and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz). The Linux kernel mitigations for this vulnerability are referred to as KAISER, and subsequently KPTI, which aim to improve separation of kernel and user memory pages.
>> U.S. CERT Guidance on "Meltdown" and "Spectre".

Chinese Hackers Target Think Tanks in Wave of Surgical Strikes.

Items of Interest: Cyber Strategy / Advanced Persistent Threats

Over the course of 2017, espionage-focused breaches by Chinese hackers have once again been on the rise, according to researchers at CrowdStrike. Those attempts were capped off by a series of attacks in October and November on organizations involved in research on Chinese economic policy, US-China relations, defense, and international finance. The attackers were likely companies contracted by the Chinese military, according to Adam Meyers, vice president of intelligence at CrowdStrike.
>> New Tactics and Targets From Chinese APTs.

Big Brother on Wheels: What Your Car Company Knows About You.

Items of Interest: Surveillance / Privacy Rights / Cyber Policy

By monitoring individual everyday movements, an automaker can vacuum up a massive amount of personal information about someone. Though drivers may not realize it, tens of millions of American cars are being monitored experts say, and the number increases with nearly every new vehicle that is leased or sold. The result is that carmakers have turned on a powerful spigot of precious personal data, often without owners' knowledge, transforming the automobile from a machine that helps us travel to a sophisticated computer on wheels that offers even more access to our personal habits and behaviors than smartphones. >> Who Watches the Watchmen?

How North Korea's Hacking Strategy is Related to Its Missile Tests.

Items of Interest: Cyber Strategy / Advanced Persistent Threats

North Korea has consistently used cyber-attacks as a distraction from its nuclear program. Since Pyongyang's second nuclear test in May 2009, its cyber-attacks have targeted South Korea's critical networks every time there is a nuclear test. After its third test in February 2013, South Korean TV stations and a bank suffered from the 3.20 cyber terror attack, known as DarkSeoul. In January last year, when North Korea had its fourth nuclear test, there was a massive spear phishing campaign targeting South Korean public officials, meant to distribute malware to their computers. After the fifth test in September last year, the South Korean military suffered a major breach that led to the loss of a cache of secret military files.
>> Links Between NK Nuke and Cyber Programs.

Okay, Say Someone Hacks into the US Power Grid. Then What?

Items of Interest: Critical Infrastructure / Crisis Response.

A joint research project between the Department of Energy and a geographic analytics company is mapping just how far the repercussions could spread. "On a scale of 1 to 10," the threat of a cyber-attack on U.S. critical infrastructure is "a 7 or an 8," DHS warns. So what happens if hackers launch a network attack that, say, causes a rolling blackout in the Midwest? Even without any bad actors targeting power grids or telecom networks, much of the U.S.'s aging infrastructure is vulnerable to disruptions large and small.
>> Modeling Cyber Attacks Against Infrastructure.

TECH TRENDS:

Stories/Links

- Creating Alternate Reality to Mislead Hackers.
  >> National Labs Constructs "HADES" to Confuse Hackers.
- Microsoft Says the Password Is Dead.
  >> Quest For More Secure Authentication Systems.
- Equifax Hack: What We Learned.
  >> Lessons Learned.
- Hacker Exploits Huawei Zero-Day to Build Botnet.
  >> Huawei 0 Day Contributes to Mirai Botnet.
- Britain's Spy Agency Can't Stop Bleeding Talent.
  >> UK Struggles to Stem Cyber Exodus.
- China Shuts Down 13K Websites For Breaking Internet Laws.
  >> Censorship By Another Name?
- UK Considers Taxes to Get Big Tech to Fight Extremism.
  >> UK Seeking to "Incentive" Big Tech in Cyber Battle.
- Six Cyber Threats to Really Worry About in 2018.
  >> Six Big Concerns in the Year Ahead.
- Iran's Cyber War on Dissidents Could Infiltrate Your Mailbox.
  >> Caught In the Online Crossfire.
- Iranians Resist Internet Censorship Amid Street Protests
  >> Iranians Turn to TOR to Avoid Regime.
- Intel Processor Design Flaw Forces Linux, Windows Redesign.
  >> Analysis of Scope and Impact of Meltdown and Spectre.
- "Of Course We Don't Spy on Our Users," Says WeChat.
  >> Overt Surveillance on Citizens in China.
- DLA Turns to Analytics to Protect Supply Chain.
  >> Combatting CAGE Jacking To Protect Supply Chain.
- Some Apps Were Listening to You Through Smart Phone Mic.
  >> Alphonso Has Been Listening to Us.
- Critical Flaw: phpMyAdmin Lets Attackers Damage Databases.
  >> Cross-Site request Forgery Attacks Vulnerable DBs.
- India's National ID DB Accessible for Less Than $10.
  >> A Warning For Us All.

Contact Us

Army Cyber Institute at West Point
2101 New South Post Road
West Point, NY 10996
Phone: 845-938-3436
Web: www.cyber.army.mil
Email: threat.cyber@usma.edu