YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

January 2018

Contents

First conviction for direct marketing email in Hong Kong

<web-link for this article>

Hong Kong supermarket PARKnSHOP was convicted of using personal data in direct marketing without consent and fined HK$3000 at Tuen Mun Magistrates' Court on 2nd January. The offence was under section 35E(1) of the Personal Data (Privacy) Ordinance which was an amendment that came into effect on 1st April 2013 and this was the first conviction for the offence.

Stephen Wong, the privacy commissioner for personal data, explained that the Ordinance does not prohibit direct marketing but, "Organizations must obtain a data subject's consent before using his personal data in direct marketing."

In this case, the complainant was a registered customer of PARKnSHOP's online store, but had not consented to receiving direct marketing materials. The complainant received a direct marketing email in January 2016. PARKnSHOP pleaded guilty, and clarified that the email was accidentally sent due to an isolated incident of human error during a system update.

Failure to comply with section 35E(1) is a criminal offence with a maximum penalty of a fine of up to HK$500,000 and imprisonment of up to 3 years. The Privacy Commissioner has published guidance: New Guidance on Direct Marketing to assist data users.

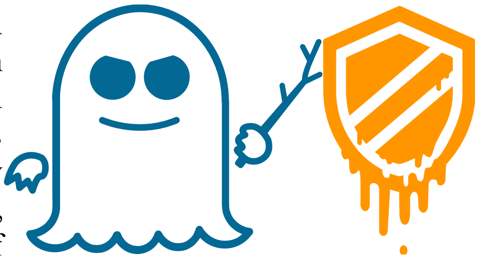
More Information

- Direct Marketing: Customers' Consent for Data
- PARKnSHOP fined for disrespecting personal data privacy
- New Guidance on Direct Marketing

Are Spectre and Meltdown a Big Deal?

<web-link for this article>

Allan Dyer



Spectre and Meltdown are the names give to design flaws in the processors that power most modern computers and they have hit the headlines worldwide in the last couple of days, but how important are they? This is not a detailed description of the flaws, there are many of those, from CERT/CC, on dedicated websites, Intel, the Register and others. Instead, I want to provide a brief guide to help ordinary users.

What is affected?

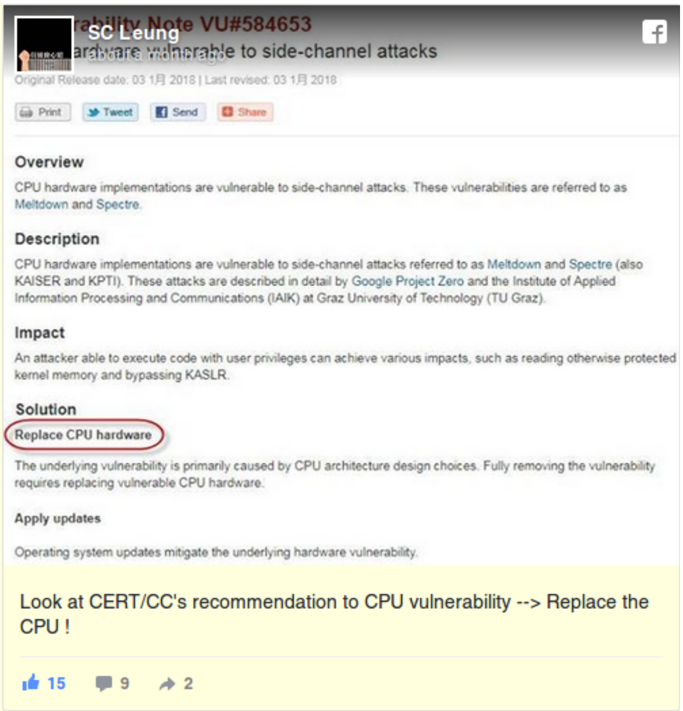
Just about every Intel processor currently in-use, and many ARM and AMD processors:

Meltdown

- Intel processors (except Itanium and pre-2013 Atoms) since 1995
- ARM Cortex-A75, Cortex-A15, Cortex-A57 and Cortex-A72

Spectre

- Intel processors (except Itanium and pre-2013 Atoms) since 1995
- ARM Cortex-R7, Cortex-R8, Cortex-A8, Cortex-A9, Cortex-A15, Cortex-A17, Cortex-A57, Cortex-A72, Cortex-A73, and Cortex-A75
- AMD's Ryzen family, FX and Pro



SC Leung

about a month ago

rability Note VU#584653

ardware vulnerable to side-channel attacks

Original Release date: 03 1月 2018 | Last revised: 03 1月 2018

Overview

CPU hardware implementations are vulnerable to side-channel attacks. These vulnerabilities are referred to as Meltdown and Spectre.

Description

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre (also KAISER and KPTI). These attacks are described in detail by Google Project Zero and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz).

Impact

An attacker able to execute code with user privileges can achieve various impacts, such as reading otherwise protected kernel memory and bypassing KASLR.

Solution

Replace CPU hardware

The underlying vulnerability is primarily caused by CPU architecture design choices. Fully removing the vulnerability requires replacing vulnerable CPU hardware.

Apply updates

Operating system updates mitigate the underlying hardware vulnerability.

Look at CERT/CC's recommendation to CPU vulnerability --> Replace the CPU !

What is not affected?

The Raspberry Pi (all models) does not use the affected ARM processors.

What Should I Do?

Install the updates as soon as possible.

The vulnerability note from CERT/CC initially advised replacing the processor, but the note now advises applying updates to the operating system and some applications.

The initial advice was accurate, but unhelpful. These are Design Flaws, so the only real fix is to replace the processor with a better-designed one.

However, even if the cost of replacing the processors in almost every computer and device was not astronomical, it is not possible in a reasonable timescale because the replacement processors are not available, and many devices have the processor permanently attached to the circuit board.

The revised advice is workable. If there is no update for your computer or device now, be prepared to install it as soon as it is released.

What are the Design Flaws?

Modern processors are extremely complicated, and processor designers are always looking for ways to make our computers run faster. They also need to enforce security, so when a user (well, a program run by the user) asks for some information, that request is given to the operating system (e.g. Windows, Linux or OS X) and the operating system checks whether the user is allowed to access that information. A design trick known as speculative execution allows a processor to execute some instructions out of order, in anticipation of a future decision, but to ignore the results if the decision went the other way. Speculative execution doesn't enforce the operating system restrictions of which program is allowed to see which data, the check happens later. The flaws are ways that a program can use speculative execution to ask for data it shouldn't be allowed to see, and then still observe an effect even though the decision went the other way and the results were 'ignored'.

So what does that mean?

One malicious program can access the data of any other program on your computer.

Is that important?

You only install genuine software and you run anti-virus, so all your software is trusted, therefore you might think you have nothing to worry about. However, there are a lot of programs that your computer runs that are not so trusted. For example, many webpages include programs, usually to make the page "cooler". It was assumed that because these programs were run inside a special environment in the web browser, they couldn't access sensitive information. By using these flaws, a webpage could try to **steal your passwords, your cryptographic keys or your bitcoin wallet**.

Will my Anti-Virus Save Me?

There have been no reports of this being exploited by malware yet. However, the flaws can be exploited in many ways so it seems unlikely that there could be a single malware definition that could recognise any exploit. So, if malware using these flaws appears, then anti-virus developers will quickly add specific detection but we won't have blanket protection.

You're saying this is a Very Big Deal, why are many reports less worrying?

The manufacturers, particularly Intel, have made a massive blunder in pursuing speed without realising the security implications. Their PR is carefully describing the problem in the least-damaging terms while still remaining technically accurate. Even so, share prices have been badly affected. For the purposes of this article, who to blame and the value of a company are irrelevant, the important thing is what should you do now? You should **install the updates as soon as possible**.

More Information

- Vulnerability Note VU#584653 CPU hardware vulnerable to side-channel attacks
- Mitigations landing for new class of timing attack
- Spectre (security vulnerability)

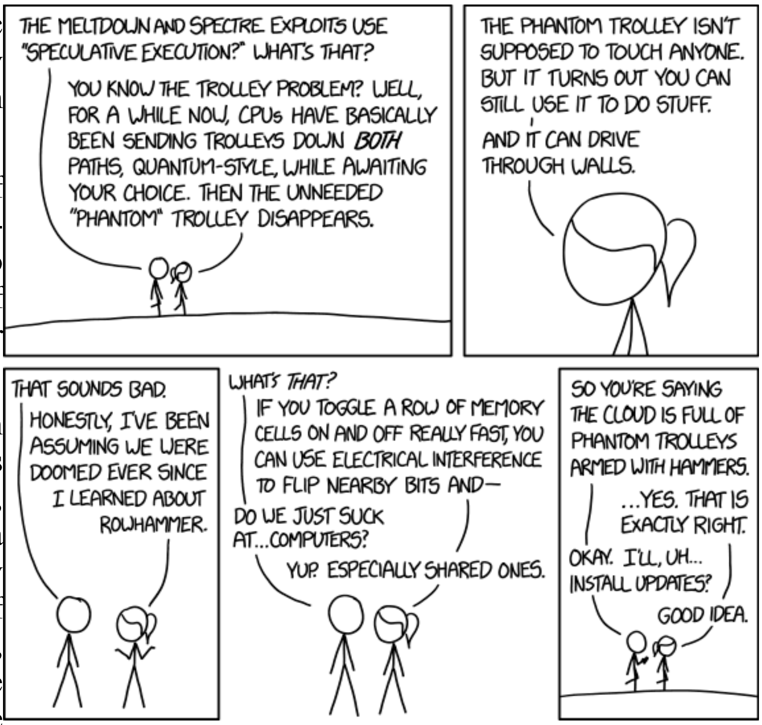
- Intel Responds to Security Research Findings
- Intel Issues Updates to Protect Systems from Security Exploits
- Raspberry Pi
- Linux Kernel Information for VU#584653
- CPU Multiple Vulnerabilities (aka Meltdown and Spectre)
- We translated Intel's crap attempt to spin its way out of CPU security bug PR nightmare
- Spectre
- Meltdown
- Meltdown, Spectre: The password theft bugs at the heart of Intel CPUs
- Amazon: Intel Meltdown patch will slow down your AWS EC2 server
- CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754 (Meltdown and Spectre) Windows antivirus patch compatibility
- Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign
- Microsoft patches Windows to cool off Intel's Meltdown – wait, antivirus? Slow your roll

A Minor Criticism of XKCD

<web-link for this article>

Allan Dyer

Randall Munroe's webcomic XKCD has an excellent summary (far better than mine) of Meltdown and Spectre:


THE MELTDOWN AND SPECTRE EXPLOITS USE "SPECULATIVE EXECUTION?" WHAT'S THAT?
YOU KNOW THE TROLLEY PROBLEM? WELL, FOR A WHILE NOW, CPUs HAVE BASICALLY BEEN SENDING TROLLEYS DOWN *BOTH* PATHS, QUANTUM-STYLE, WHILE AWAITING YOUR CHOICE. THEN THE UNNEEDED "PHANTOM" TROLLEY DISAPPEARS.
THE PHANTOM TROLLEY ISN'T SUPPOSED TO TOUCH ANYONE. BUT IT TURNS OUT YOU CAN STILL USE IT TO DO STUFF.
AND IT CAN DRIVE THROUGH WALLS.
THAT SOUNDS BAD.
HONESTLY, I'VE BEEN ASSUMING WE WERE DOOMED EVER SINCE I LEARNED ABOUT ROWHAMMER.
WHAT'S *THAT?*
IF YOU TOGGLE A ROW OF MEMORY CELLS ON AND OFF REALLY FAST, YOU CAN USE ELECTRICAL INTERFERENCE TO FLIP NEARBY BITS AND—
DO WE JUST SUCK AT...COMPUTERS?
YUP. ESPECIALLY SHARED ONES.
SO YOU'RE SAYING THE CLOUD IS FULL OF PHANTOM TROLLEYS ARMED WITH HAMMERS.
...YES. THAT IS EXACTLY RIGHT.
OKAY. I'LL, UH... INSTALL UPDATES?
GOOD IDEA.

But I do have a minor criticism of the mouse-over text: "New zero-day vulnerability: In addition to rowhammer, it turns out lots of servers are vulnerable to regular hammers, too."

Anyone who's studied information security standards, such as ISO/IEC 27000, will know that, while the specific threat of a regular hammer is not usually mentioned, the general class of physical attacks is. For example, Douglas Adams in his book "The Hitchhiker's Guide To The Galaxy" quotes Zaphod Beeblebrox as saying, "Computer... if you don't open that exit hatch this moment I shall zap straight off to your major data banks and reprogram you with a very large axe, got that?" Controls to mitigate this class of attacks vary according to the value of the systems and the perceived threat level, but include a wide variety of measures, such as locked doors, guards (possibly armed, *Quis custodiet ipsos custodes?*) and off-site backups.

More Information

- Meltdown and Spectre
- Are Spectre and Meltdown a Big Deal?

VTech data breach settlement ~HK$1.70 per child

<web-link for this article>

Hong Kong toymaker VTech that exposed personal data of about 3 million children in the US in 2015 has reached a settlement with the US Federal Trade Commission (FTC) where the toymaker pays US$650,000 and conducts biannual third-party security assessments.

In the deal, VTech does not admit to breaking the law but does agree to pay the FTC, conduct security assessments by a CISSP, CISA, GIAC or other approved individual or entity for 20 years, and keep records and make compliance reports for 10 years. The law that VTech is not admitting to have broken is the Children's Online Privacy Protection Act (COPPA), which came into effect on 21st April 2000 in the US. COPPA is intended to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children's personal information online by operators of Internet Web sites and online services.

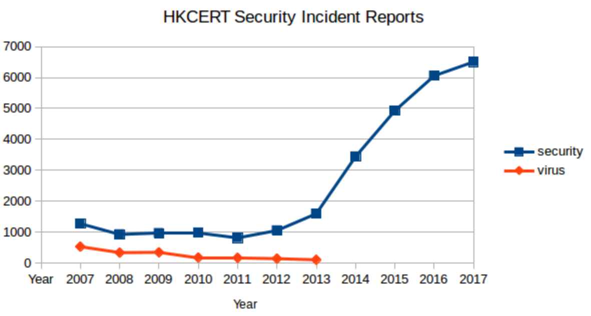
Yui Kee Chief Consultant Allan Dyer commented, "Although this settlement seems inadequate considering the scale of the negligence and too small to provide a credible economic incentive to companies to give personal data protection the attention it requires, it is still an improvement over the lack of action by the Hong Kong Privacy Commissioner in VTech's home jurisdiction. Will the Hong Kong Government give the Privacy Commissioner some real teeth?"

More Information

- VTech hack fallout: What is a kid's privacy worth? About 22 cents – FTC
- VTech Data Breach Exposes Personal Data of Hundreds of Thousands of Children
- PCPD Initiates Compliance Check on VTech's Data Leakage Incident
- VTech Quietly Passes Privacy Responsibility to Customers
- US Court Likely to Dismiss Damages Claim Against HK Toymaker VTech for Personal Data Breach
- USA vs. VTech Complaint, Case No : 1:18-cv-114
- FTC's Unopposed Motion for the Entry of the Stipulated Order, Case No : 1:18- cv-114

Hong Kong Cybercrime Continues to Rise

<web-link for this article>



Figures from the Hong Kong Police and HKCERT (Hong Kong Computer Emergency Response Team Coordination Centre) show that technology crime continued to rise in 2017, despite a general trend of other types of crime decreasing.

Speaking at a press conference on 23 January 2018, the Commissioner of Police, Mr Lo Wai-chung reported that the overall law and order situation in Hong Kong continued to improve in 2017, with the lowest overall crime rate since 1975. However, online business fraud was up by 394 cases to 1996 cases, with losses of HK$34.5 million. Most of the cases involved customer-to-customer online trading. The number of "romance scams", that usually involve online communication and overseas fraudsters, more than doubled to 235 cases, with a loss of HK$108 million.

However, cyber-blackmail was substantially reduced. "Naked chat" blackmail fell by 56.2% to 305 cases with a total loss of HK$900,000. Ransomware was down 32% to 43 cases, even though the WannaCry ransomware substantially affected other jurisdictions in May 2017. The Police have noted that some perpetrators took advantage of the anonymous nature of Bitcoin in blackmail and money laundering cases, so the Cyber Security and Technology Crime Bureau (CSTCB) has set up a dedicated unit to more effectively handle cases involving Bitcoin. Mr Lo did not indicate whether the unit would also handle cases involving other cryptocurrencies.

The Police's Anti-Deception Coordination Centre (ADCC), previously reported in this newsletter, has received over 12,000 calls since its establishment in July 2017.

HKCERT statistics also show a rise in security incident reports, they handled a total of 6506 incidents in 2017, compared to 6058 in 2016. Statistics from the Government InfoSec website were not available for 2017 at the time or writing.

More Information

- Crime hits new low
- Overall law and order situation saw continuous improvement in 2017
- HKCERT Statistics
- Computer Related Crime Statistics
- Hong Kong Cybercrime on the Rise (2013)
- Hong Kong Cybercrime Continues to Soar (2014)
- Hong Kong Cybercrime Increases Again; Privacy Under Attack (2015)
- New Hong Kong Police Commissioner to Focus on Fighting Cybercrime
- Hong Kong Police Open Anti-Scam Centre

Hong Kong Computer Society Announces Cyber Security Specialist Group

<web-link for this article>

The Hong Kong Computer Society (HKCS) has announced that it is consolidating its seven Special Interest Groups, including the Information Security Special Interest Group (ISSIG) into four Specialist Groups, with the Cyber Security Specialist Group (CSSG) replacing the ISSIG.

The Convenors of HKCS Specialist Groups: Mr. Ricky Woo (Cyber Security) at far left. © HKCS

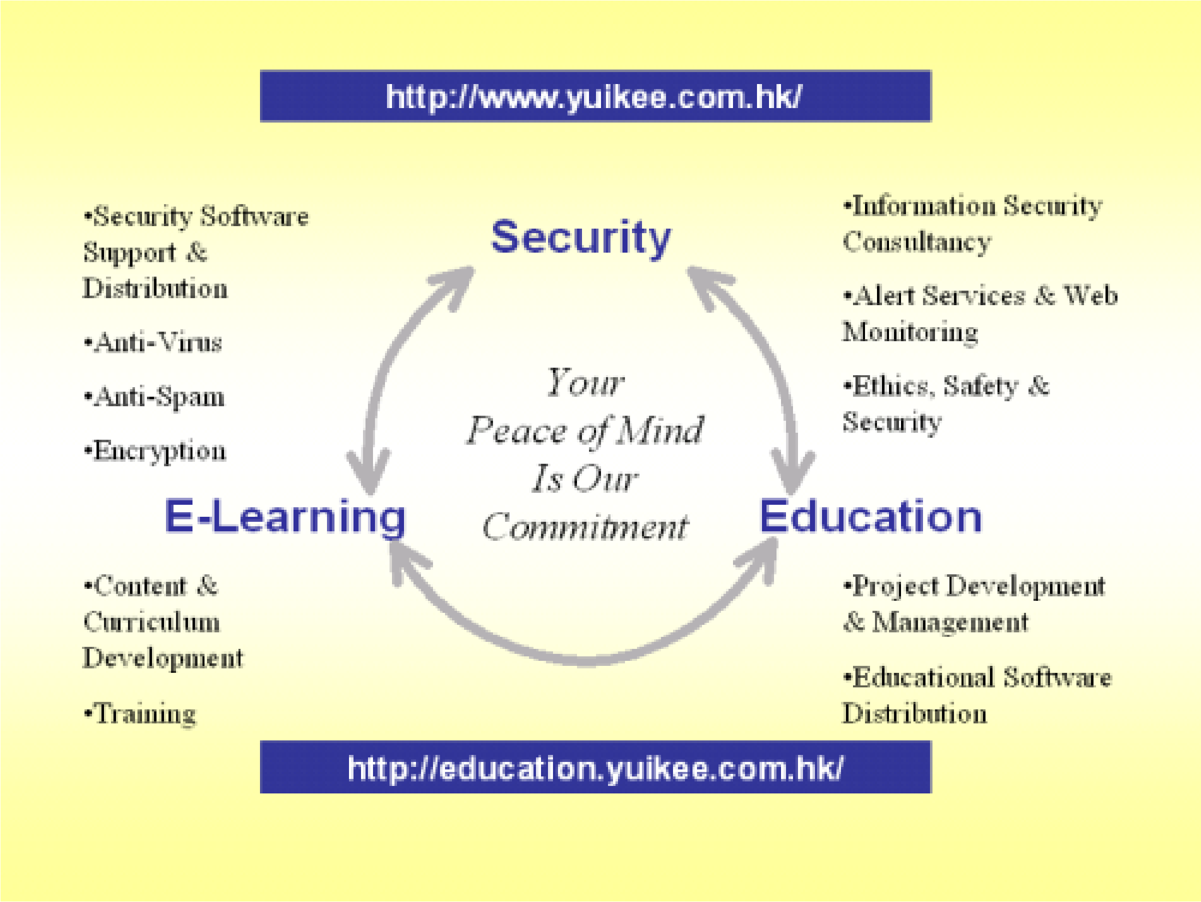
The group will be headed by Mr. Ricky Woo of the Bank of China (Hong Kong). It will be a platform for HKCS members to collaborate, discuss and share experiences on the topic of cyber security. It will keep abreast with and focus on enabling and evolving technologies of cyber security and it will be a catalyst for innovation through thought leadership. It will cultivate leadership and technical competencies for members within the cybersecurity field and act as a professional body in representing Cyber Security participants to the community, including media. It will assist member's career growth by providing professional development events, career path information, mentoring and coaching services, and networking opportunities.

More Information

- Hong Kong Computer Society Announces the Consolidation of Seven Special Interest Groups in to Four Specialist Groups

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/