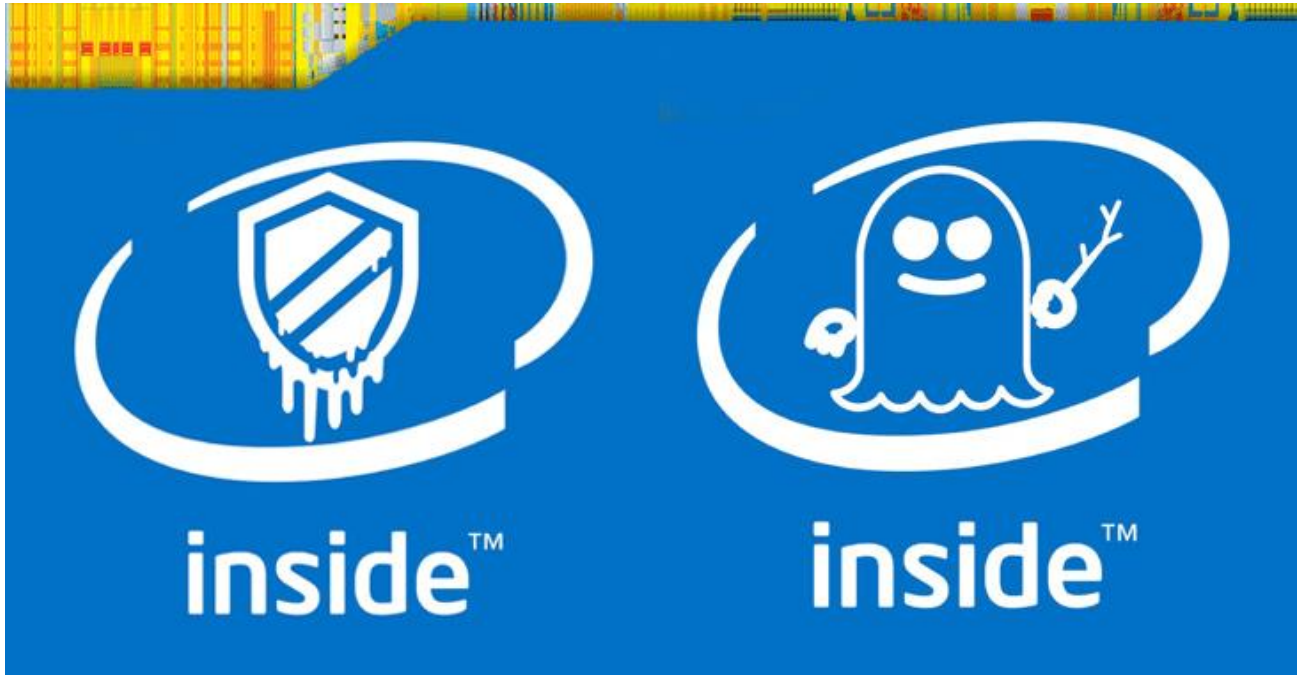
Attacks, Concepts, and Techniques

- **Security vulnerabilities** are any kind of software or hardware defect. After gaining knowledge of a vulnerability, malicious users attempt to exploit it.
- An **exploit** is the term used to describe a program written to take advantage of a known vulnerability.
- The act of using an exploit against a vulnerability is referred to as an **attack**. The goal of the attack is to gain access to a system, the data it hosts or to a specific resource.

- After a rollercoaster day of speculation on Jan. 3 2018, about a severe Intel chip flaw, Google's Project Zero research team revealed later that same day details about the CPU vulnerabilities.
- **Meltdown** breaks the mechanism that keeps applications from accessing arbitrary system memory, consequently, applications can access system memory. **Spectre** tricks other applications into accessing arbitrary locations in their memory.



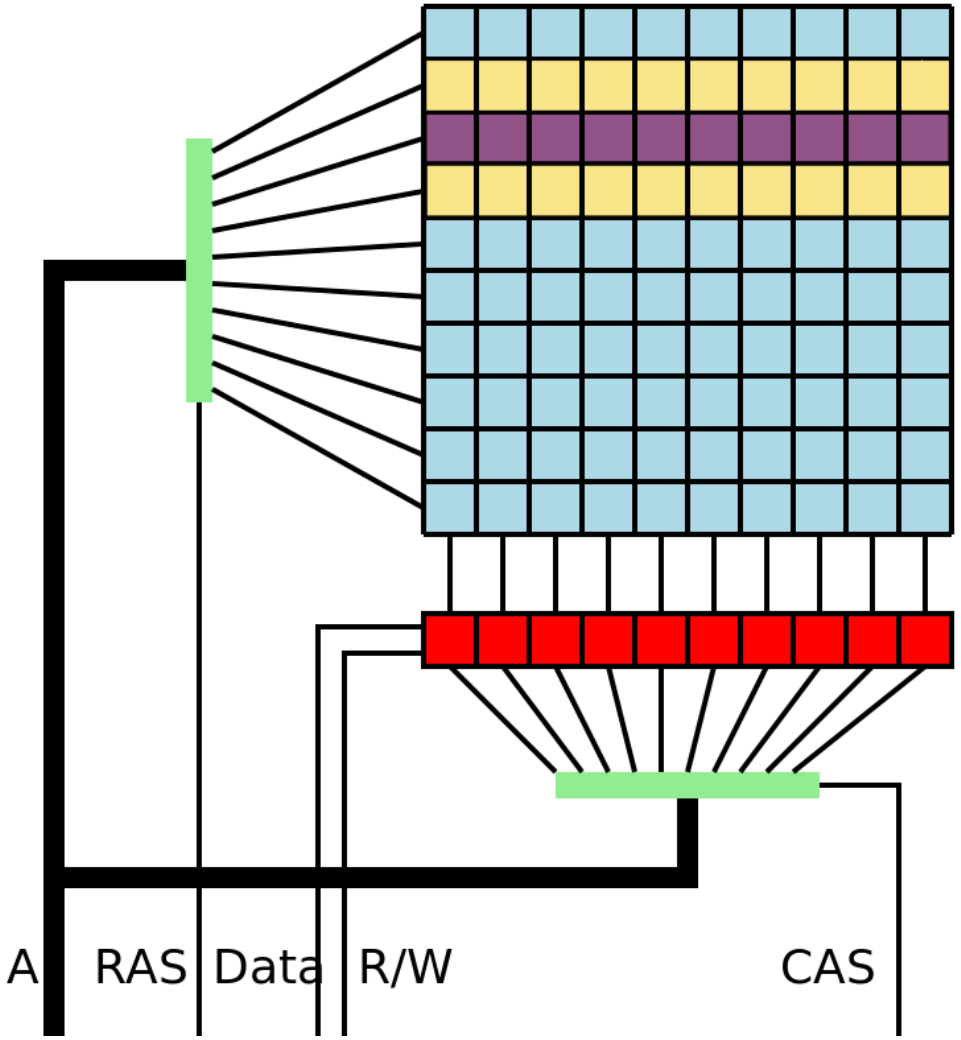
Meltdown and Spectre (2018) CPU Flaws Expose Modern Systems to Risk

Software Vulnerabilities

- Software vulnerabilities are usually introduced by **errors in the operating system or application code**. Despite all the effort companies put into finding and patching software vulnerabilities, it is common for new vulnerabilities to surface. Microsoft, Apple, and other operating system producers release **patches and updates** almost every day. Application updates are also common. Applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.
- The goal of software updates is to stay current and avoid exploitation of vulnerabilities. While some companies have **penetration testing teams** dedicated to search, find and patch software vulnerabilities before they can get exploited, third party **security researchers** also specialize in finding vulnerabilities in software.
- In **2015**, a **major vulnerability**, called **SYNful Knock**, was discovered **in Cisco IOS**. This vulnerability allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco 1841, 2811, and 3825 routers. The attackers could then monitor all network communication and had the ability to infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed in the routers. To avoid this, always verify the integrity of the downloaded IOS image and limit the physical access of the equipment to authorized personnel only.
- **Google's Project Zero** is a great example of such practice. After discovering a number of vulnerabilities in various software used by end-users, Google formed a **permanent team dedicated to finding software vulnerabilities**.

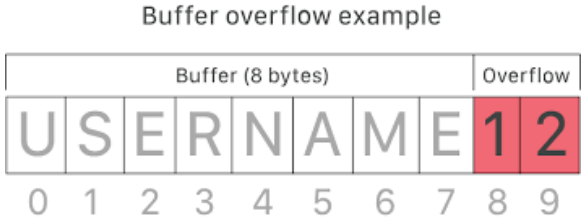
Hardware Vulnerabilities

- Hardware vulnerabilities are often introduced by **hardware design flaws**.
- RAM memory for example, is essentially capacitors installed very close to one another. It was discovered that, due to proximity, constant changes applied to one of these capacitors could influence neighbor capacitors. Based on that design flaw, an exploit called **Row Hammer** was created. By repeatedly rewriting memory in the same addresses, the Row Hammer exploit **allows data to be retrieved from nearby address memory cells**, even if the cells are protected.
- Hardware vulnerabilities are **specific to device models** and are not generally exploited through random compromising attempts. While hardware exploits are **more common in highly targeted attacks**, traditional malware protection and a physical security are sufficient protection for the everyday user.



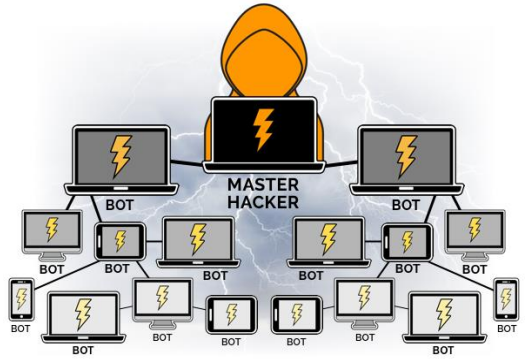
Row Hammer: Rapid row activations (yellow rows) may change the values of bits stored in victim row (purple row).

Categorizing Software Vulnerabilities



- **Buffer overflow** – Occurs when data is written beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.
- **Non-validated input** – Input data coming into a program could have malicious content, designed to force the program to behave in an unintended way. Consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.
- **Race conditions** – When the output of an event depends on ordered or timed outputs, it becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or proper timing.
- **Weaknesses in security practices** – Systems and sensitive data can be protected through techniques such as authentication, authorization, and encryption. It is strongly advised that developers use security libraries that have already created, tested, and verified.
- **Access-control problems** – Many security vulnerabilities are created by the improper use of access controls. Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file.
- Nearly all access controls and security practices can be overcome if the attacker has physical access to target equipment. For example, no matter what you set a file's permissions to, the operating system cannot prevent someone from bypassing the operating system and reading the data directly off the disk.

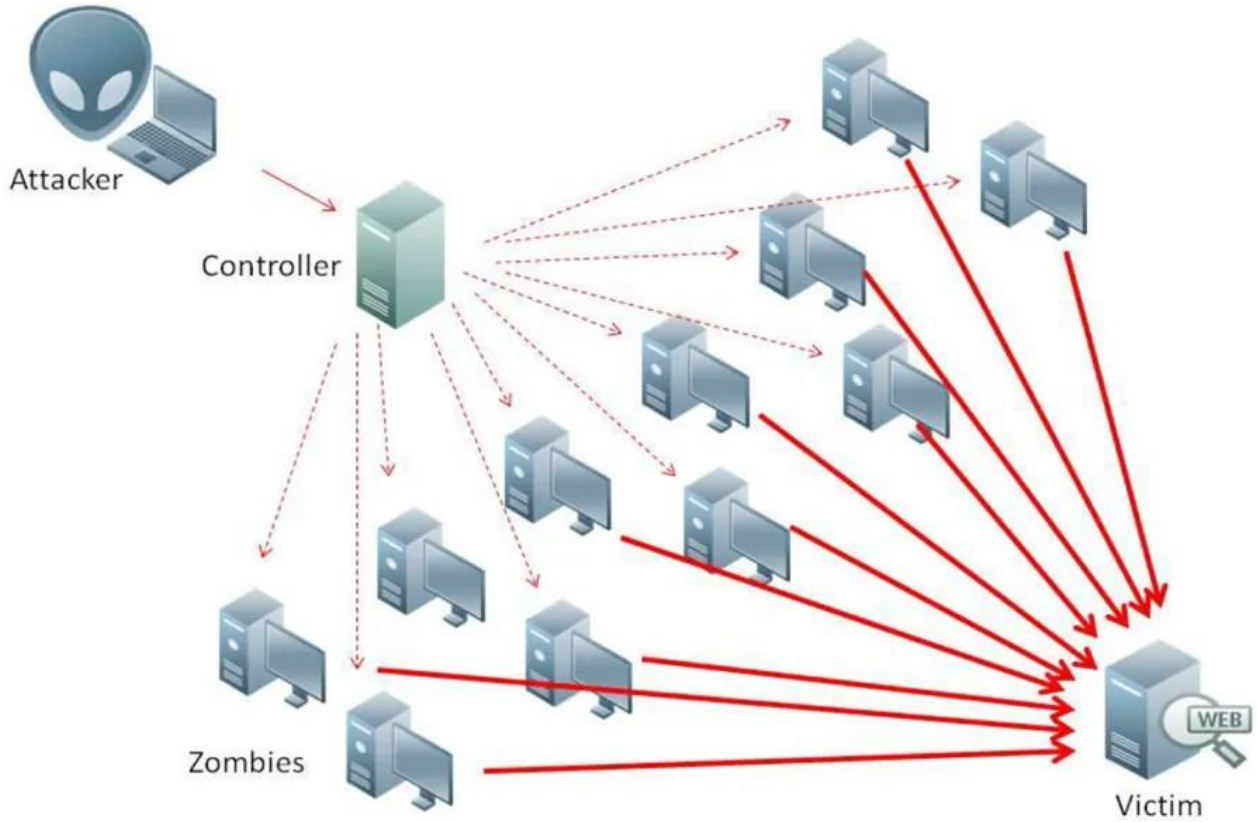
Types of Malware



- **Spyware** includes activity trackers, keystroke collection, and data capture. It often bundles itself with legitimate software or with Trojan horses.
- **Adware** is designed to automatically deliver advertisements.
- **Ransomware** is designed to hold a computer system or the data it contains captive until a payment is made.
- **Scareware** conveys forged messages stating the system is at risk or needs the execution of a specific program to return to normal operation.
- **Rootkit** is designed to modify the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely.
- **Bot** is designed to automatically perform an action, usually online. Several computers infected with bots, called **botnet**, are programmed to quietly wait for commands provided by the attacker.
- **Virus** attaches to other legitimate executable files, that can perform destructive actions.
- **Trojan horse** attaches to non-executable files (games, images, audio) in disguise to perform malicious acts.
- **Worms** run themselves and replicate by exploiting vulnerabilities in networks, usually slowing it down. Worms are responsible for some of the most devastating attacks on the Internet (Code Red, 2001).
- **Man-In-The-Middle (MitM)** attacker takes control over a device without the user's knowledge. Widely used to steal financial information.
- **Man-In-The-Mobile (MitMo)** is a variation of MitM, used to take control over a mobile device. ZeuS (2010) allowed attackers to quietly capture 2-step verification SMS messages sent to users.

Denial of Service (DoS)

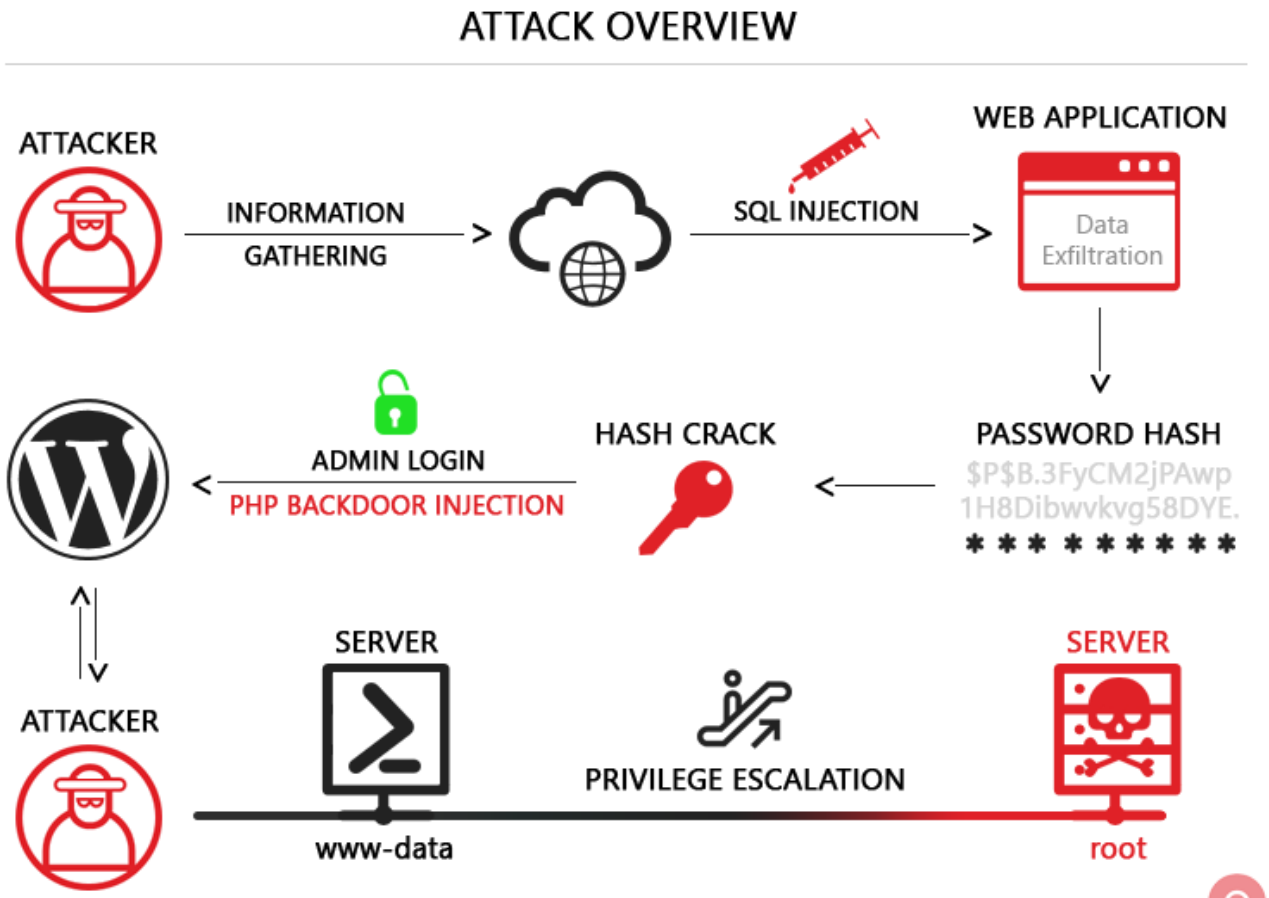
- A DoS attack results in some sort of interruption of network service to users, devices, or applications. This causes a slowdown in transmission or response, or a crash of a device or service.
- **Overwhelming Quantity of Traffic** - A host is sent data at a rate which it cannot handle.
- **Maliciously Formatted Packets** - A host is sent packets containing errors which causes it to crash or slowdown.
- **Distributed DoS Attack (DDoS)** - Similar to a DoS attack but originates from a network of infected hosts, called a botnet. The infected hosts are called zombies. The zombies are controlled by handler systems.
- DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money.



Vulnerability Exploitation

- Exploiting vulnerabilities is another common method of infiltration. Attackers will scan computers to gain information about them. Below is a common method for exploiting vulnerabilities:
- **1. Gather information** about the target system, its operating system, version, and list of services running.
- **2.** Look for any **known vulnerabilities** specific to that version of OS or other OS services.
- **3.** When a vulnerability is found, look for a previously written **exploit** to use. If no exploits have been written, consider writing an exploit.

- **Advanced persistent threats (APTs)** consist of a multi-phase, long term, stealthy and advanced operation against a specific target. Due to its complexity and skill level required, an APT is usually well funded.



More Attack Types

- **Social engineering** is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. An attacker could call an authorized employee with an urgent problem that requires immediate access. The attacker could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to employee's greed.
- **Pretexting** - Attacker calls an individual and lies to them in an attempt to gain access to privileged data.
- **Tailgating** - This is when an attacker quickly follows an authorized person into a secure location.
- **Something for Something (Quid pro quo)** - Attacker requests personal information from a party in exchange for something, like a free gift.
- **WiFi password cracking** - A few password brute-force tools include Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
- **Phishing** - Fraudulent email disguised as being from a legitimate, trusted source, to trick the recipient into installing malware on their device, or into sharing personal or financial information (Claim prize!).
- **Spear phishing** - A highly targeted phishing attack. The attacker researches the target's interests before sending the email.
- **SEO poisoning** - Goal is to increase traffic to malicious sites that may host malware or perform social engineering. To force a malicious site to rank higher in search results, attackers take advantage of popular search terms.
- **Blended attacks** - Attacks that use multiple techniques to compromise a target. Many of the most damaging computer worms like Nimbda, CodeRed, BugBear, Klez and Slammer are better categorized as blended attacks. The recent Conficker and ZeuS/LICAT worms were also blended attacks.