Problem Class 2

Jingjie Li

Question 1

“De-perimeterization is great. I don’t have to worry anymore about malicious or out-of-date devices on my network anymore.” To what extent is this statement true? Does the Mirai Botnet tell us anything about de-perimeterization?

Question 1

“De-perimeterization is great. I don’t have to worry anymore about malicious or out-of-date devices on my network anymore.” To what extent is this statement true? Does the Mirai Botnet tell us anything about de-perimeterization?

- It only really works if you have a good inventory of devices so you can check they’re all up to date
- You may also want to have a perimeter with DDoS defenses even if all authentication is per device

Question 2

How comfortable would you be logging into your bank account on a public airport WiFi? Would a VPN offer you additional protection in this scenario?

Question 2

How comfortable would you be logging into your bank account on a public airport WiFi? Would a VPN offer you additional protection in this scenario?

- Suppose the ‘free wifi’ hub is a malicious device operated by another person in the airport
- What’s the main threat – bad DNS to a phishing site and a MITM attack?
- What’s the appropriate defense against that?

Question 3

The default settings used in VPNs are probably intentionally weak. So, do VPNs have any value in any setting?

Question 3

The default settings used in VPNs are probably intentionally weak. So, do VPNs have any value in any setting?

- In an ideal world you might de-perimeterize
- In the real world you may have the most critical machines running on ancient software that cannot be patched, e.g., MRI scanners on Windows 7
- Your customers may have policies that require secure networks for certain functions
- And then there's the Operational Technology

Question 4

What's the point of locks, if they can be so easily bumped? Why even bother breaking a lock if you can just smash a window?

Question 4

What's the point of locks, if they can be so easily bumped? Why even bother breaking a lock if you can just smash a window?

- Some locks are not bad. Lever locks must be drilled or impressioned; multipoint locks broken
- Locks generally deter Derek and Charlie, nudging them to pick other targets
- They remove legal excuses
- They're a condition of insurance

Question 5

Might an IoT device need some forms of tamper resistance? What about a video games console?

Question 5

Might an IoT device need some forms of tamper resistance? What about a video games console?

- Many examples, most of them protecting a business model from circumvention by the user!
- Started with printer cartridges
- Rights-management chips are now everywhere from tractors to water filters and insulin pumps
- Video games consoles use them so they can subsidize the console from sales of games and accessories

Question 6

Differential Power and Fault analysis are really complicated. You are a CISO trying to explain to your CEO the possible attacks that may occur on your new IoT device, of which you have produced 3 million units. How far up the list of risks should these attacks be, and how would you explain their potential for damage and the circumstances under which this damage could occur?

Question 6

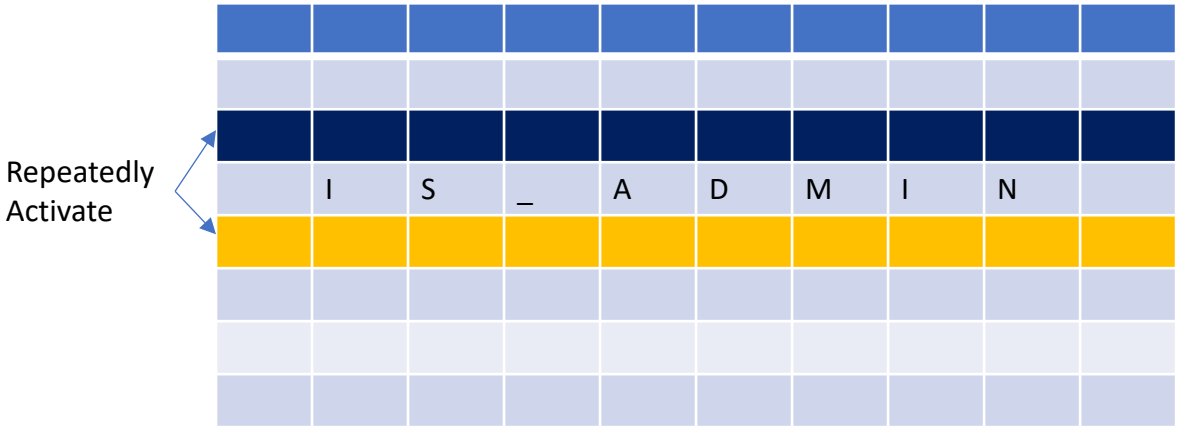
Differential Power and Fault analysis are really complicated. You are a CISO trying to explain to your CEO the possible attacks that may occur on your new IoT device, of which you have produced 3 million units. How far up the list of risks should these attacks be, and how would you explain their potential for damage and the circumstances under which this damage could occur?

- Could someone extract a key and then undermine your business model with compatible spare parts?

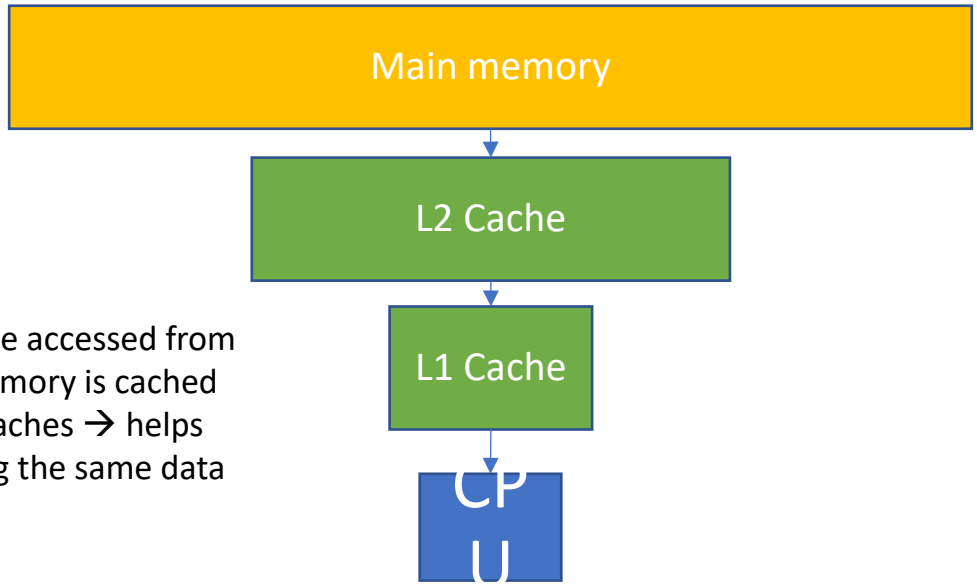
Question 7

A Rowhammer attack requires the rapid access of rows within the CPU's Random Access Memory. However, all modern systems have caches that act as a fast buffer for frequently accessed memory. Does such a cache make a Rowhammer attack impossible, given that it typically reduces the rate of access to main memory?

Rowhammer



Cache Hierarchy



Data once accessed from main memory is cached in CPU caches → helps accessing the same data faster

Question 7

A Rowhammer attack requires the rapid access of rows within the CPU's Random Access Memory. However, all modern systems have caches that act as a fast buffer for frequently accessed memory. Does such a cache make a Rowhammer attack impossible, given that it typically reduces the rate of access to main memory?

- You must work out some way to bypass the cache, whether directly with a cache flush or indirectly with a suitable access pattern

Question 8

To eliminate Spectre attacks, your boss suggests you buy a processor without a cache. How effective do you think this might be, how feasible, and would there be any disadvantage?

Question 8

To eliminate Spectre attacks, your boss suggests you buy a processor without a cache. How effective do you think this might be, how feasible, and would there be any disadvantage?

- Cacheless designs are way too slow
- In-order cores are Spectre proof even with a cache but still too slow
- Most buyers (other than majors like Google) have to take what they're given

Question 9

Does SGX eliminate Spectre attacks? If so, how? If not, what does SGX achieve? Is SGX only beneficial in a data centre, rather than on end-consumer hardware?

Question 9

Does SGX eliminate Spectre attacks? If so, how? If not, what does SGX achieve? Is SGX only beneficial in a data centre, rather than on end-consumer hardware?

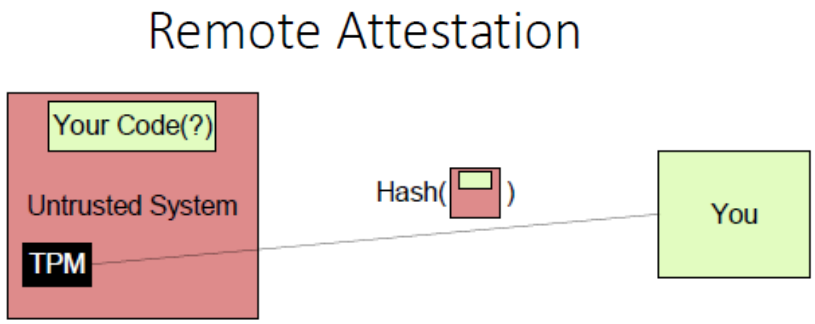
- No, and SGX hasn't really been successful and is now marked as obsolete
- SGX was brought in for Blu-Ray disks in 2016 but consumer devices now use different tech such as TrustZone and Blu-Ray has been replaced by streaming services

Question 10

Why do we need remote attestation? Can't we just trust that a good data centre will be running the right thing? Are there any parts of the system for which the guarantees on attestation provided by e.g. a TPM or SGX are insufficient?

Question 10

Why do we need remote attestation? Can't we just trust that a good data centre will be running the right thing? Are there any parts of the system for which the guarantees on attestation provided by e.g. a TPM or SGX are insufficient?



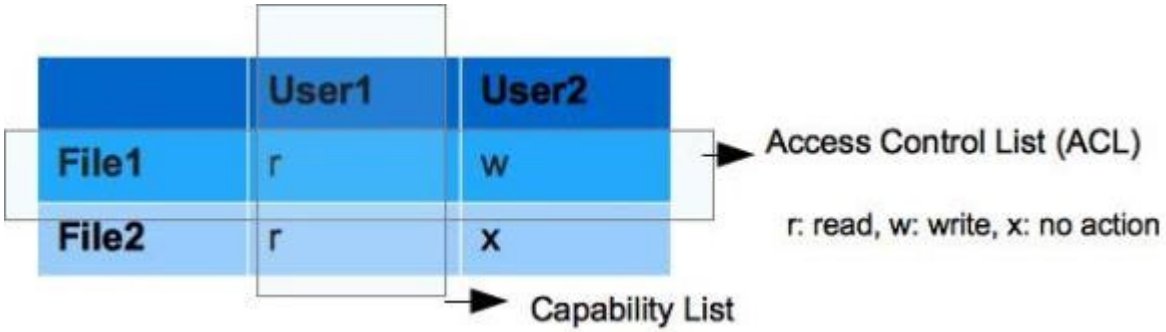
Question 10

Why do we need remote attestation? Can't we just trust that a good data centre will be running the right thing? Are there any parts of the system for which the guarantees on attestation provided by e.g. a TPM or SGX are insufficient?

- You may trust Amazon or Google, but the NSA?
- If you trust SGX you also assume Intel is trustworthy.
- Attestation doesn’t help much with side channels.
- SGX may provide good cover for data-centre providers to not provide bulk intercept to host governments – but that’s not really how it’s sold…

Question 11

“All access control is just a matrix matching users to files, so capabilities and access control lists are exactly equivalent.” How accurate is this statement?



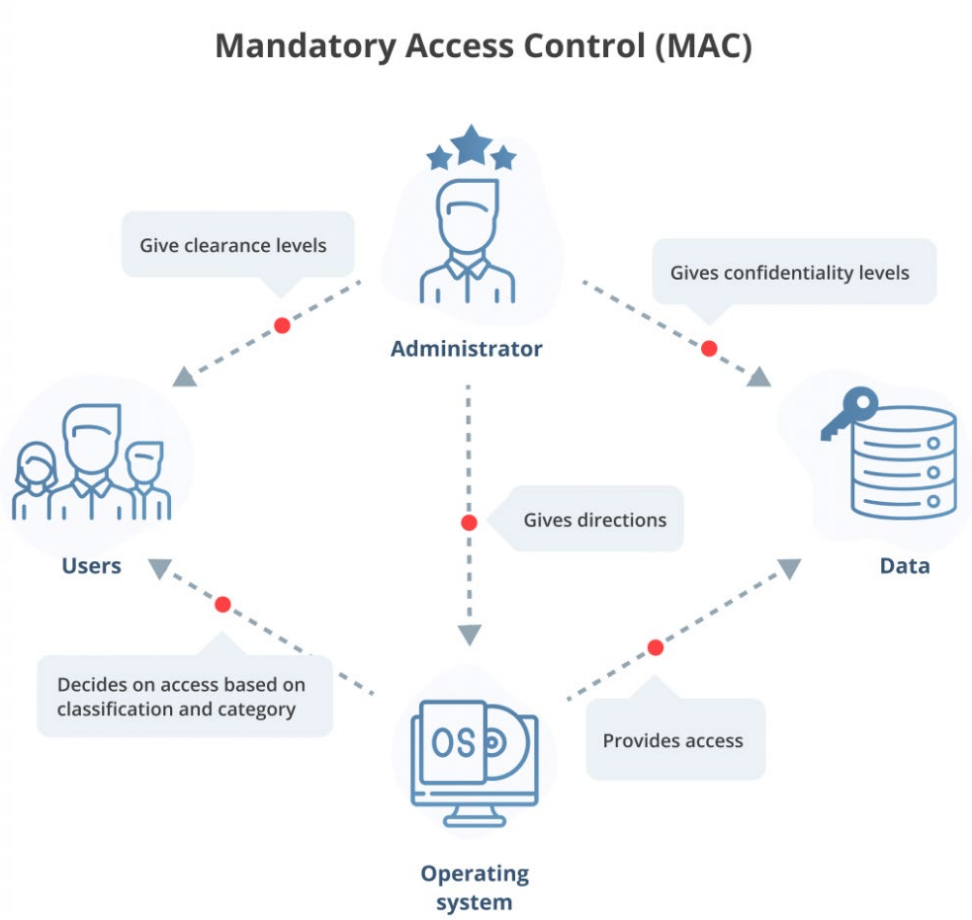
Question 11

"All access control is just a matrix matching users to files, so capabilities and access control lists are exactly equivalent." How accurate is this statement?

- There is a big performance difference
  - ACLs are convenient for storing and managing simple rules
  - Capabilities are better at runtime
- Then there are more complex rules
  - Sometimes you need (user, program, data) triples
  - Sometimes you need roles
  - Sometimes users and resources management different

Question 12

“The mandatory access control mechanisms in Android just serve to take control away from the user and place it in the platform holder’s hands. Any benefit to the consumer is just an illusion.” How accurate is this statement?


Mandatory Access Control (MAC)
Give clearance levels
Administrator
Gives confidentiality levels
Users
Gives directions
Data
Decides on access based on classification and category
OS
Provides access
Operating system

Question 12

“The mandatory access control mechanisms in Android just serve to take control away from the user and place it in the platform holder’s hands. Any benefit to the consumer is just an illusion.” How accurate is this statement?

- Android (and iOS) have a lot less malware than Windows thanks to MAC
- There’s also the environmental hygiene of the app store ecosystem

Question 13

Why would Apple only store biometrics in their own proprietary Secure Enclave, rather than using TrustZone and/or allowing access to the iOS kernel more generally? Does this really improve security?

Question 13

Why would Apple only store biometrics in their own proprietary Secure Enclave, rather than using TrustZone and/or allowing access to the iOS kernel more generally? Does this really improve security?

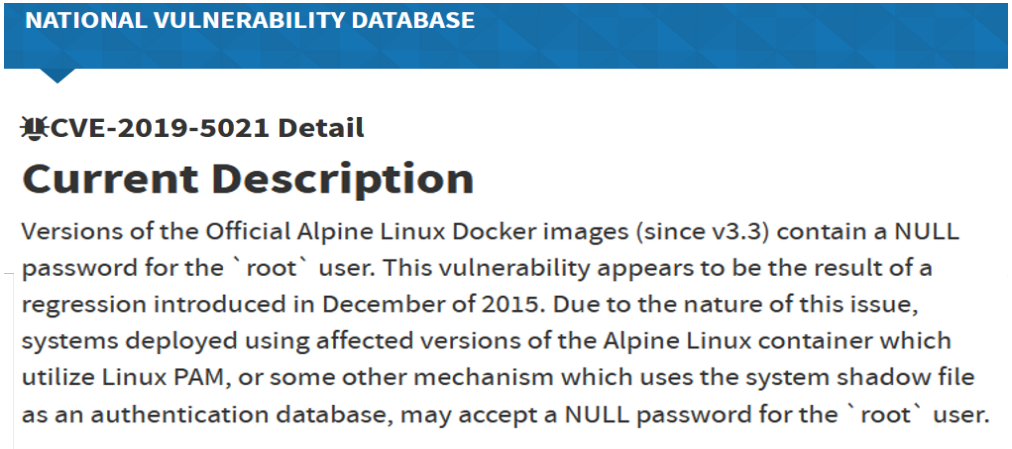
- The Secure Enclave is the equivalent of the TPM or Secure Element in an Android phone
- It's a minimal design that doesn't run any third-party software, unlike TrustZone

Question 14

“The comparison between containers and virtualization shows that all new, under-tested technology is bad for security.” Do you agree with this statement?

Question 14

“The comparison between containers and virtualization shows that all new, under-tested technology is bad for security.” Do you agree with this statement?


NATIONAL VULNERABILITY DATABASE

CVE-2019-5021 Detail

Current Description

Versions of the Official Alpine Linux Docker images (since v3.3) contain a NULL password for the `root` user. This vulnerability appears to be the result of a regression introduced in December of 2015. Due to the nature of this issue, systems deployed using affected versions of the Alpine Linux container which utilize Linux PAM, or some other mechanism which uses the system shadow file as an authentication database, may accept a NULL password for the `root` user.

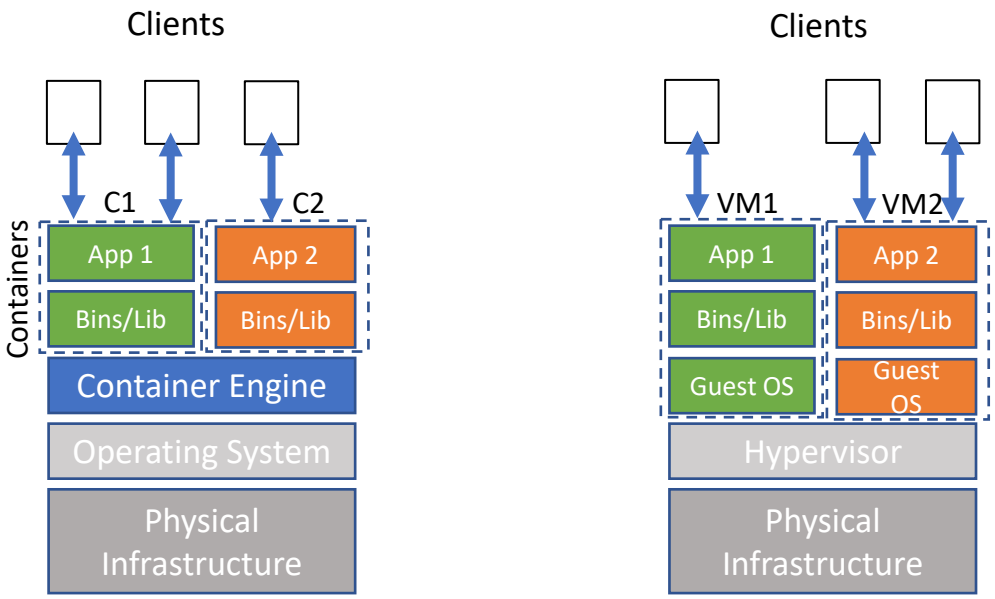
Question 14

"The comparison between containers and virtualization shows that all new, under-tested technology is bad for security." Do you agree with this statement?

- Inflated claims were made about the security offered by containers when they were new…
- The example on the previous screen wasn't a fundamental issue with containers but more to do with poor defaults, poor usability and lack of standards.
- But containers aren't just a cheap form of virtualization – they're also for ease of deployment.

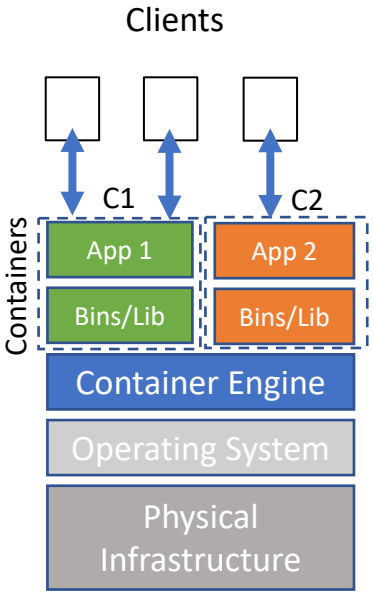
Question 15

“Isolation costs money, and so there will inevitably be a race-to-the-bottom on security technologies in the cloud.” What might this statement be referring to, and to what extent is it true?



Example use-cases of modern data centers

Question 15



Isolation in containers

- Cheaper than a VM but less secure
- Isolation guaranteed at application level; OS/Hardware is shared
- Creates namespaces for isolation
- Syscall filtering; can restrict syscalls using seccomp; change root to a local directory

Question 15

“Isolation costs money, and so there will inevitably be a race-to-the-bottom on security technologies in the cloud.” What might this statement be referring to, and to what extent is it true?

- For virtualisation framework on top of a hypervisor, the TCB is (in theory) just the hypervisor, which is small and easy to verify, right???
  - Nobody actually does verify a hypervisor formally
- VMs are still very widely used in cloud platforms, which suggests that the security is valued in practice over cheaper containers.