Tutorial 6

Yuvraj Patel

Announcements

Change in schedule

- 13th March – Guest Lecture (share details on Piazza); attend online
- Last tutorial moved from 20th March to 27th March

Coursework 2 will be released on 8th March

- Topic – OS Security
- Deadline – 22nd March (2 weeks)
- Start early

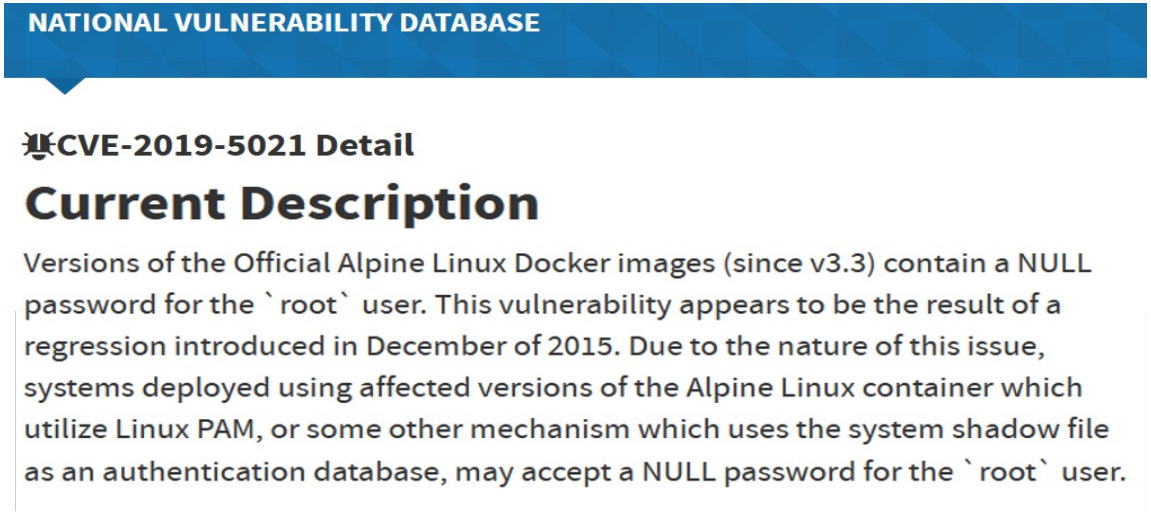
Please complete NSS Survey

Question 1

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

Question 1

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



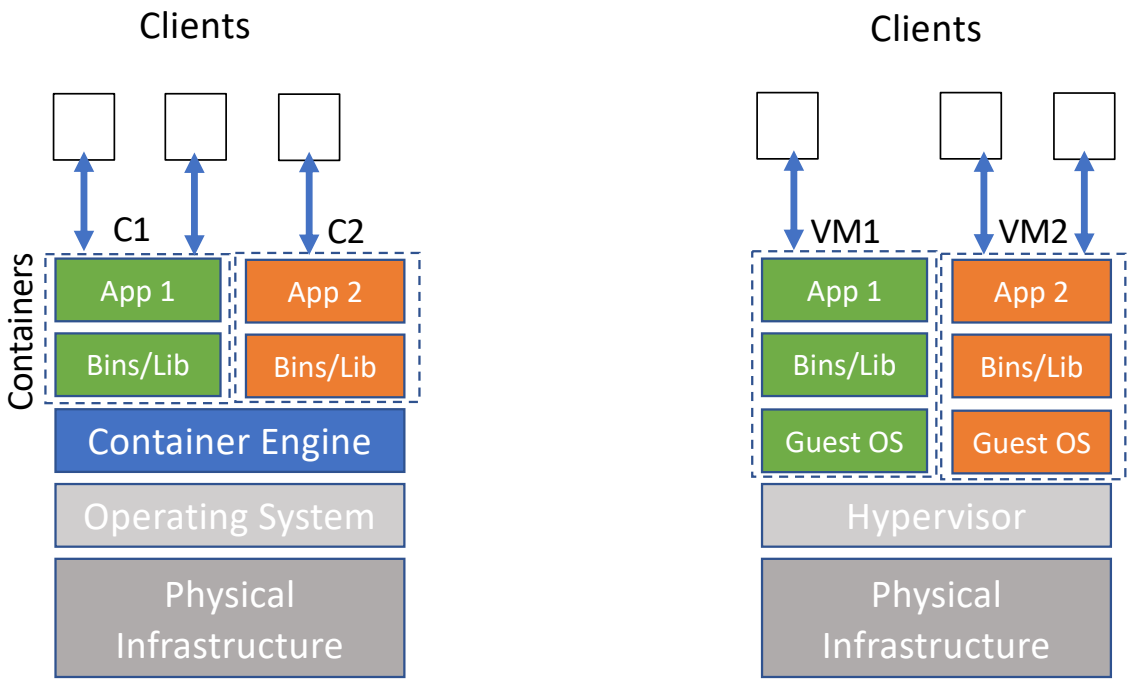
Question 1

"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.

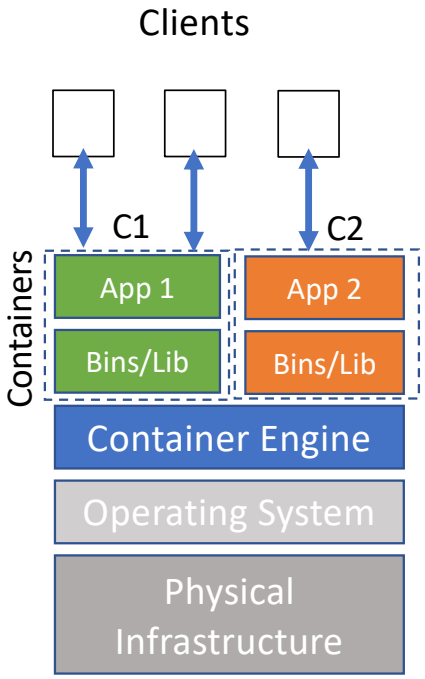
Question 2

“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 2



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 2

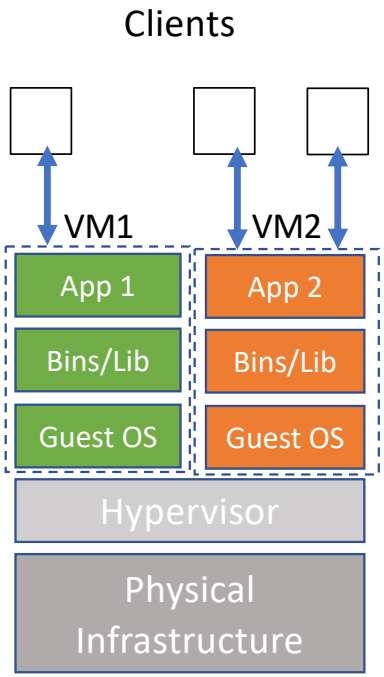
"Isolation costs money, and so there will inevitably be a race-to-the-bottom on security technologies in the cloud." What might this statement be referring to, and to what extent is it true?

- 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.

Question 3

Compare the isolation features between processes in Android to the isolation features provided by a virtualization environment such as VirtualBox.

Question 3



- Entire OS replaced with guest OS on top of hypervisor
- Mostly used in data centers
- HW support available for virtualization features (Intel VT-x); clean and faster
- Hypervisor much smaller compared to OS – better code review, testing, thin attack surface

Question 3

Compare the isolation features between processes in Android to the isolation features provided by a virtualization environment such as VirtualBox.

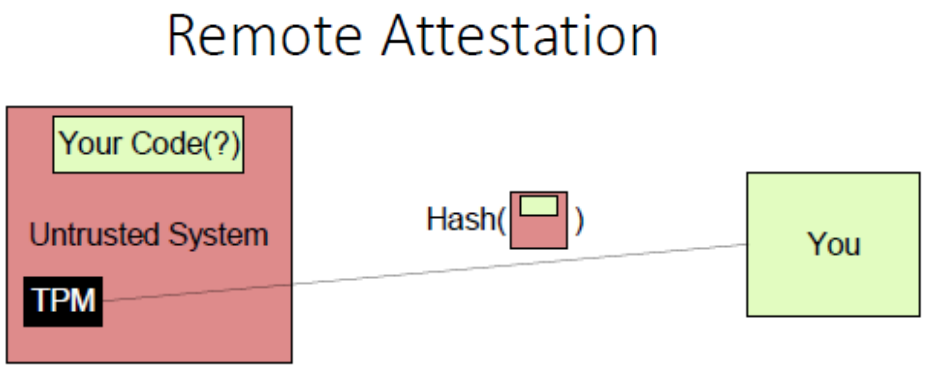
- Android shares the same Kernel but uses UID tricks and SELinux to isolate different apps from each other.
- Virtualization uses a hypervisor with nested page tables.

Question 4

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 4

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 4

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 5

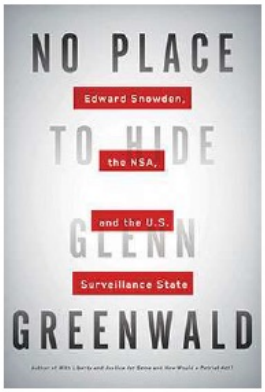
Why would you bother attacking the supply chain, when most systems use large amounts of software that are buggy and/or out-of-date, and spearphishing attacks are so easy to pull off?

Question 5

Why would you bother attacking the supply chain, when most systems use large amounts of software that are buggy and/or out-of-date, and spearphishing attacks are so easy to pull off?

Supply Chain Attacks: Operation Gunman

Supply Chain Attacks (2): Cisco Routers



Question 5

Why would you bother attacking the supply chain, when most systems use large amounts of software that are buggy and/or out-of-date, and spearphishing attacks are so easy to pull off?

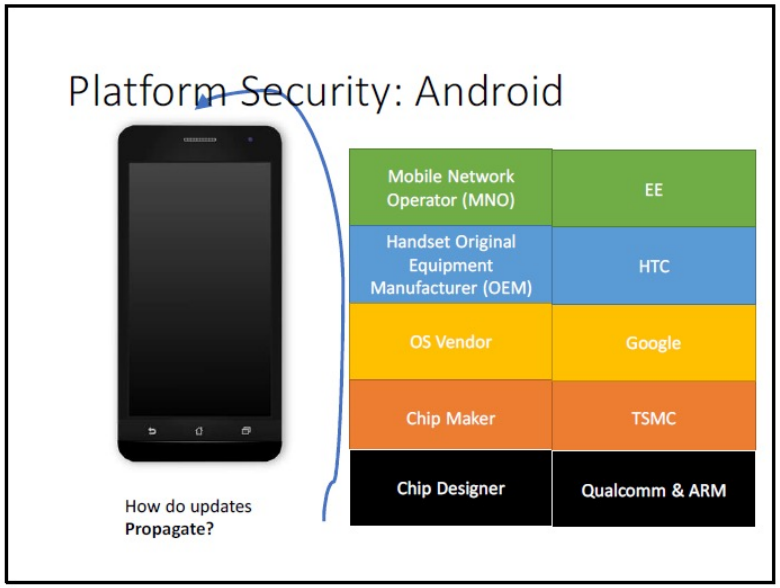
- Example: Solar Winds
- Can be more covert, and give real scale
- Great diversity of targets
- Some parts of the supply chain are opaque, overseas, or otherwise hard to defend
- US government initiative – Support Bill of Materials (SBOM)

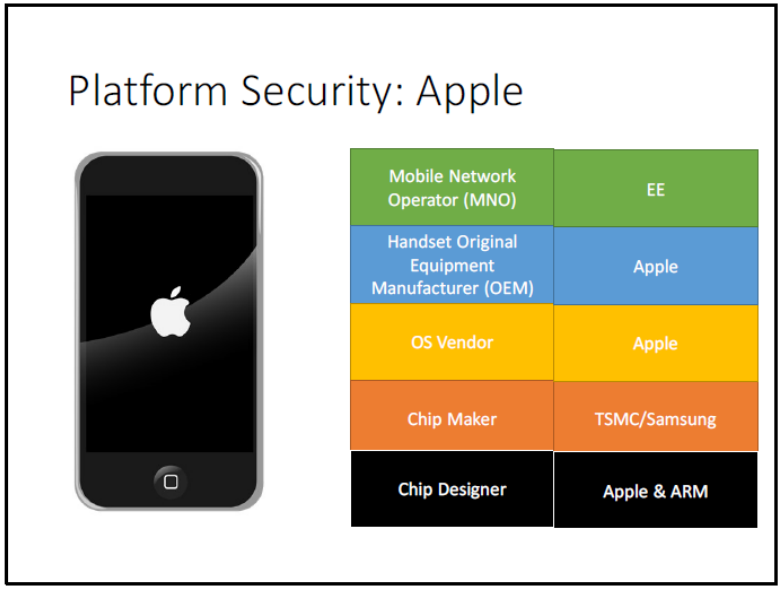
Question 6

Why is a Mobile Network Operator less incentivised to patch your phone than Google or Apple? Why does Apple update for longer than Google?

Question 6

Why is a Mobile Network Operator less incentivised to patch your phone than Google or Apple? Why does Apple update for longer than Google?





Question 6

Why is a Mobile Network Operator have less incentive to patch your phone than Google or Apple? Why does Apple update for longer than Google?

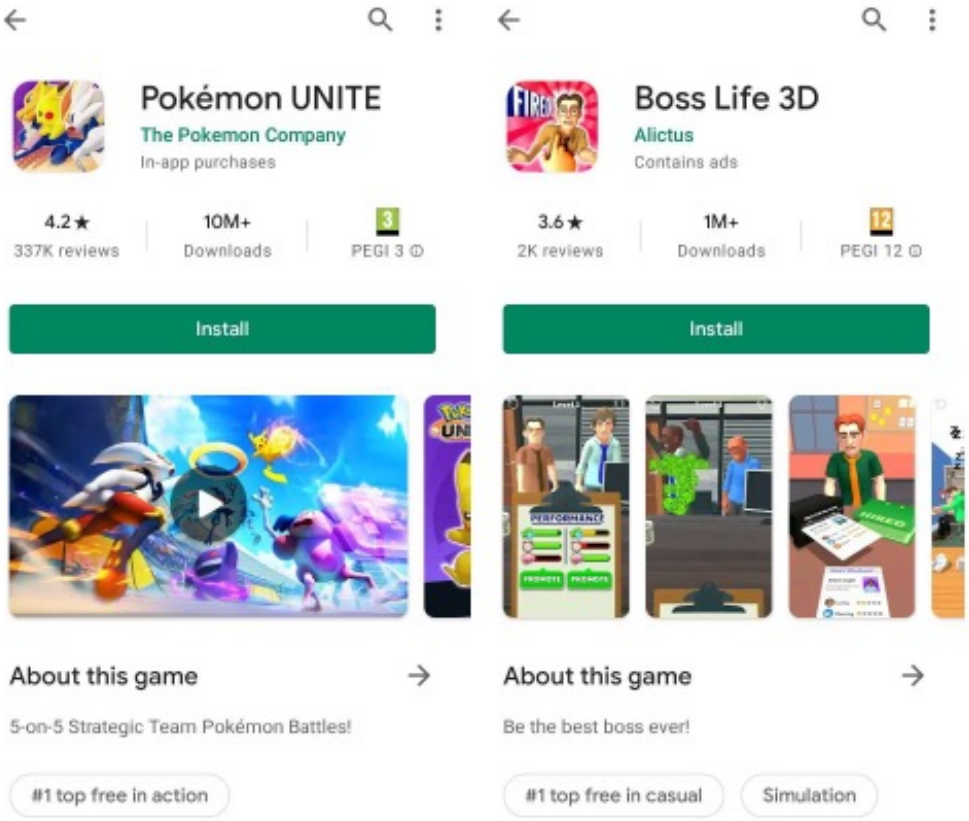
- The MNO makes money selling a new phone!
- They also don't have the technical expertise/scale to support lots and lots and lots of phones (and neither do the OEMs for that matter)
- Apple stack vertically integrated, so fewer misaligned incentives (the negative externalities become internalised)

Question 7

How does the existence of App stores alter ecosystem-wide security on mobile phones?

Question 7

How does the existence of App stores alter ecosystem-wide security on mobile phones?



Question 7

How does the existence of App stores alter ecosystem-wide security on mobile phones?

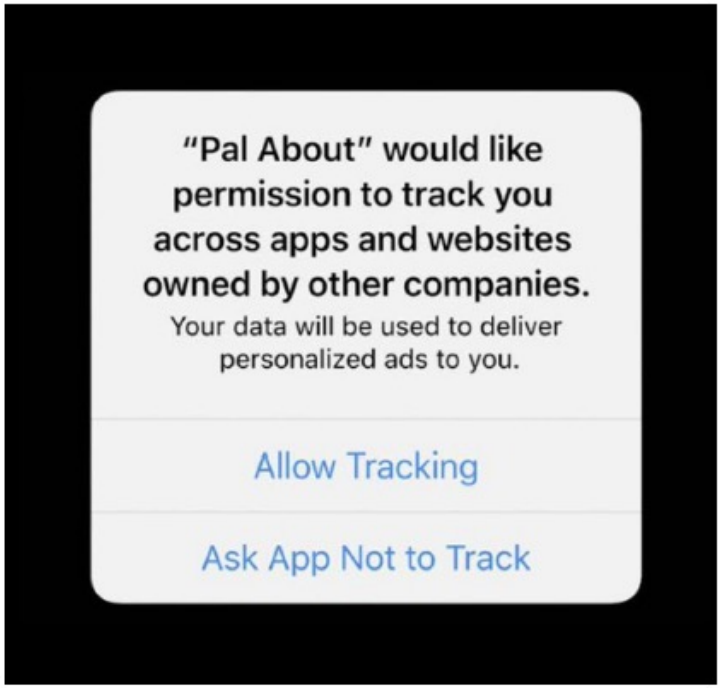
- Even the most popular apps may be somewhat predatory (IAPs, behavioural advertising)
- Since the business model depends on collecting data, and you're running these apps on your banking device, need strong isolation mechanisms.
- The app store gives Google more control over app updates than OS updates!

Question 8

Is Apple's IDFA (ID for Advertisers) good or bad?

Question 8

Is Apple's IDFA (ID for Advertisers) good or bad?



Question 8

Is Apple's IDFA (ID for Advertisers) good or bad?

- Changes behavioural advertising from opt-out to opt-in
- Most people don’t opt – so this pretty well killed off cross-app advertising in Apple’s ecosystem
- Look what happened to Facebook’s stock price!
- How does it just give Apple an advantage?
- Apple advertising, plus Apple’s 30% cut of app store revenue and (most) in-app payments

Question 9

“Open-source code should be used wherever possible. It has more eyes on it than closed-source applications, so is less likely to be buggy or malicious.” To what extent do you agree?

Question 9

"Open-source code should be used wherever possible. It has more eyes on it than closed-source applications, so is less likely to be buggy or malicious." To what extent do you agree?

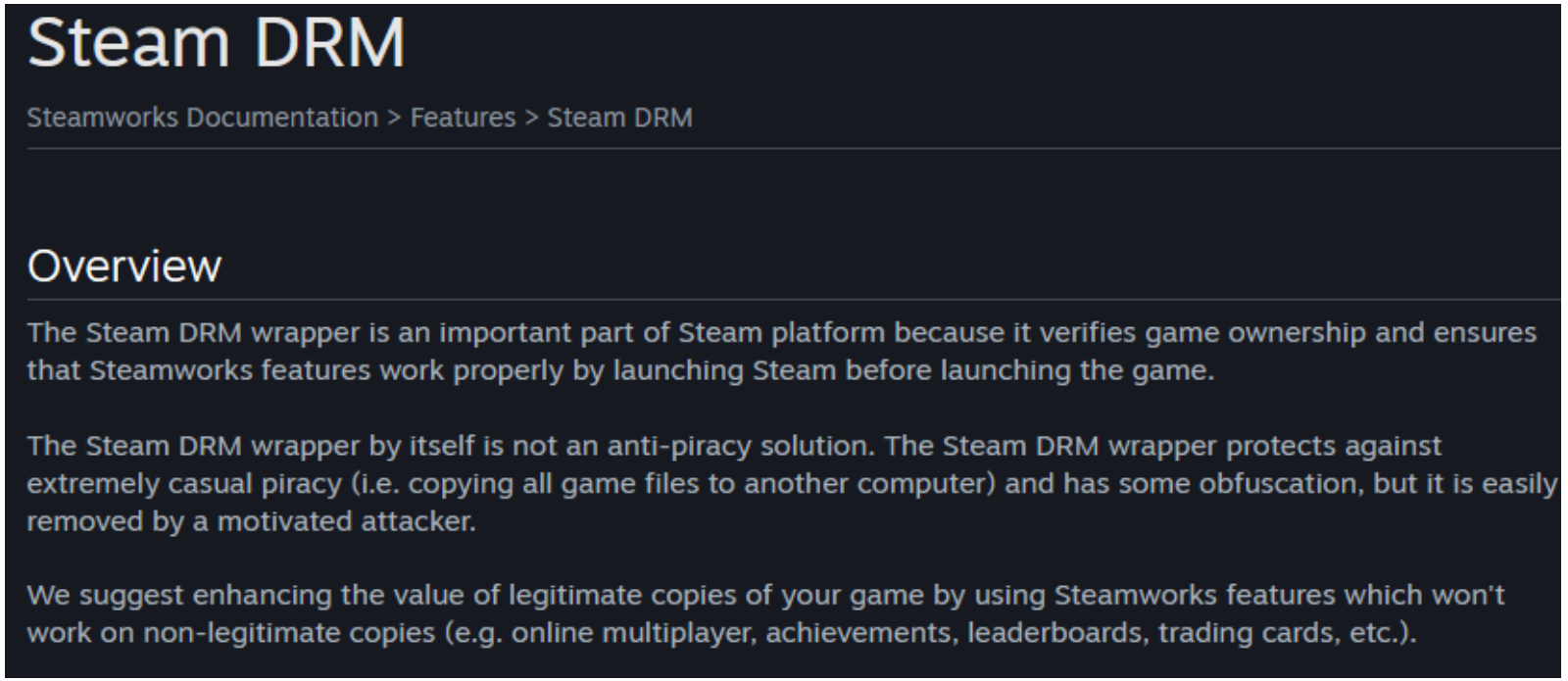
Question 9

“Open-source code should be used wherever possible. It has more eyes on it than closed-source applications, so is less likely to be buggy or malicious.” To what extent do you agree?

- In theory, open and closed are equivalent, but...
- If you‘re expecting “the community” to find your bugs, are you expecting that work for free? E.g. does someone richer than you maintain that library?
- It’s a complicated, empirical question...

Question 10

On the Steam website, Valve has this to say about its DRM mechanisms for its video game store. How might Valve improve the level of assurance given by their anti-piracy solutions, and why might they choose not to do so?



Steam DRM

Steamworks Documentation > Features > Steam DRM

Overview

The Steam DRM wrapper is an important part of Steam platform because it verifies game ownership and ensures that Steamworks features work properly by launching Steam before launching the game.

The Steam DRM wrapper by itself is not an anti-piracy solution. The Steam DRM wrapper protects against extremely casual piracy (i.e. copying all game files to another computer) and has some obfuscation, but it is easily removed by a motivated attacker.

We suggest enhancing the value of legitimate copies of your game by using Steamworks features which won't work on non-legitimate copies (e.g. online multiplayer, achievements, leaderboards, trading cards, etc.).

Question 10

On the Steam website, Valve has this to say about its DRM mechanisms for its video game store. How might Valve improve the level of assurance given by their anti-piracy solutions, and why might they choose not to do so?

- Practical example of code obfuscation
  - Given enough time, removing copy protection possible
- Surely Valve could go with SGX if they wanted real remote attestation
  - Implications → Performance hit/memory limitation, Need for specific Intel cores – what about those who do not have these cores?
- Most likely better to take the piracy hit than some other company's (Intel's) lock-in