CE876 - Information Security Mng. & Eng.

Lecture 3: Personal Device Protection

Department of Computer Engineering
Sharif University of Technology
Spring 1403

S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content. These slides were initially developed by Seyedeh Atefeh Musavi and Mehdi Kharrazi.

What is a personal device?

S4Lab

- A laptop? Your smart phone? Your …. ?
- Everything Is Becoming a Computer
  - Recall an old-style telephone, compare that to the telephone in your pocket right now.
    - It’s not really a telephone; it’s a computer running a telephone app.
  - Now they are computers with things attached to them(even a refrigerator or a car).

[Image: https://cs.goldiran.ir/]

[Schneier, Bruce. *Click here to kill everybody: Security and survival in a hyper-connected world*, 2018]

What is a personal device?

- Our conception of the Internet is also shifting. We no longer go to a specific place in our homes or offices and log on to what appears to be a separate space.
  - Those spatial metaphors don't make sense anymore, and saying "I'm going on the Internet" will make about as much sense as plugging in a toaster and saying "I'm going on the power grid."
  - It will become harder and harder for you to buy a new washing machine without Internet connectivity.
  - Today, it might seem dumb that your washing machine has an Internet connection, and impossible that your T-shirt someday will. But in a few years, it will just be the normal state of things.

[Schneier, Bruce. *Click here to kill everybody: Security and survival in a hyper-connected world*, 2018]

Smart Devices

- Why “The ‘Smart Everything’ Trend?
  - Why anyone would put their coffeepot or toothbrush on the Internet.
  - The answer is simple: market economics.
- It’s really the Internet + Things.
  - More accurately, the Internet + Things + us. Or, for short, the Internet+.
  - Humans are just another component in many of these systems.
    - We provide inputs to these computers and accept their outputs. We are the consumers of their automated functionality.

[Schneier, Bruce. *Click here to kill everybody: Security and survival in a hyper-connected world*, 2018]

Protecting a Personal Device

S4Lab

- Despite the wide range of personal devices today, much of the existing classic literature is for personal laptops/computers.
- In this session we discuss how to protect a personal computing device/personal computation.
  - With trusted initial state (device protection)?
    - TPM (discussed in previous session)
    - Anti-theft technologies
    - Malware resistance
    - Secure update
    - data encryption(full memory/full disk/filesystem).
    - Secure log
    - Secure data storage/deletion
  - Without trusted initial state (computation protection on an untrusted device)?
    - Stateless computing

Anti-theft technologies

More important for devices which are not physically secured

Anti-theft technologies

S4Lab

- Proximity-based solutions
- Remote command channels
- Behavior-based solutions
- Software-based

Proximity-based solutions

S4Lab

- Most are RFID-based to track Automobiles/goods.
- Bluetooth-based
- We will discuss further in the supply chain session.

[image: https://sanatino.com]

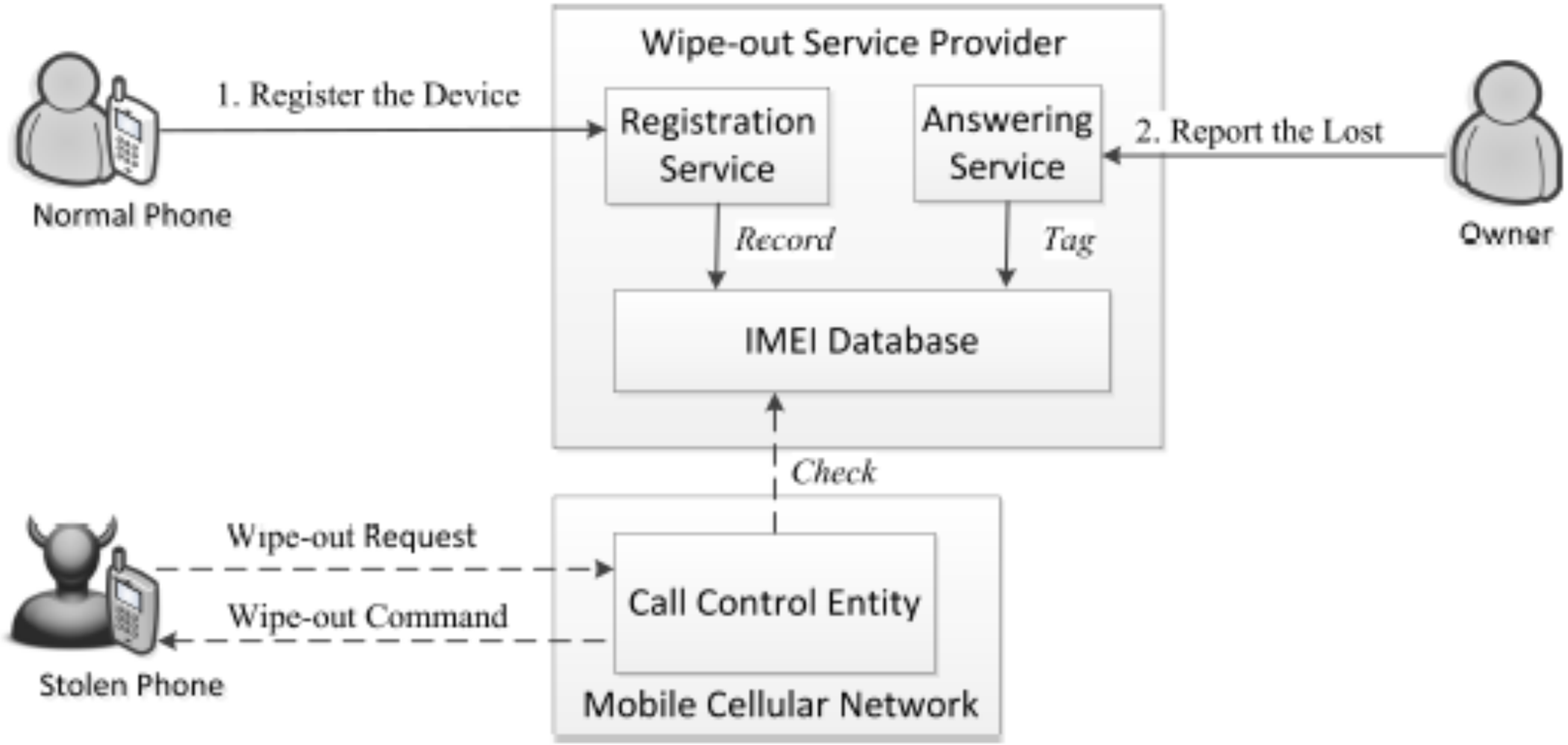
Remote command channels

S4Lab

- Required for tracking the device or wiping out data if the device is stolen.
- The adversary is able to turn of wifi/device, or remove the sim card.
- So How can we use other remote channels?

Emergency call channel

S4Lab



[Yu, X., et al., Remotely wiping sensitive data on stolen smartphones. *ACM symposium on Information, computer and communications security*, 2014]

Behavior-based solutions

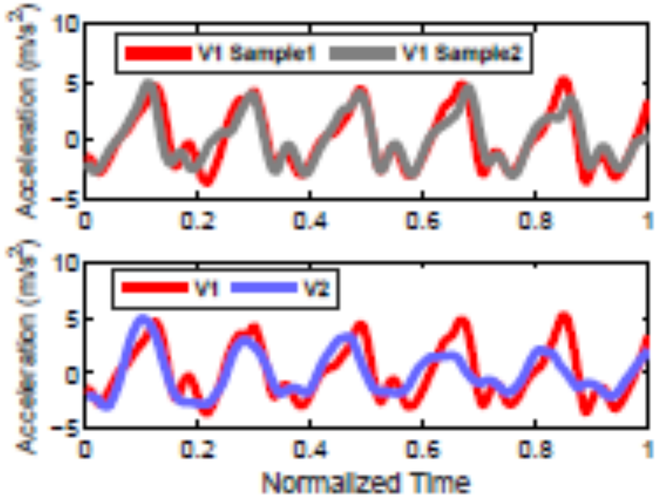
S4Lab

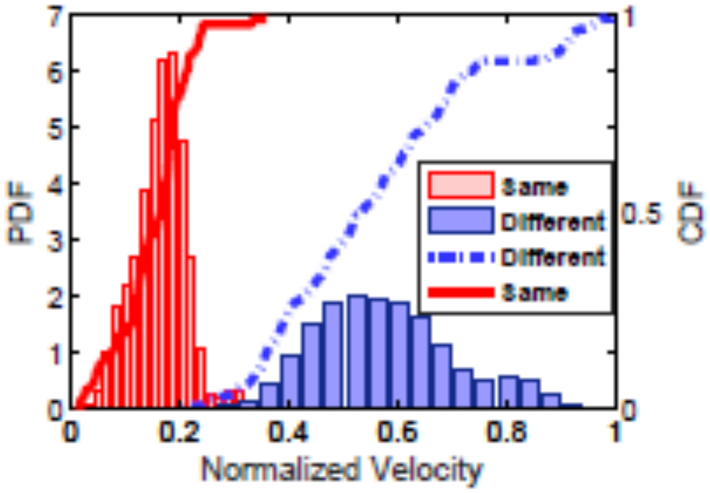
- Some behavioral features (often obtained from device sensors)
- Find the pattern of abnormal behavior

A behavior-based example: iGuard

S4Lab

- Provides a Markov Chain based model, which continuously track motions of the smartphone user, and instantly estimate the probability that the motions are performed by the user himself/herself.
  - Acceleration
  - DTW (Dynamic Time Warping)





[Jin, M., et al., iGuard: A real-time anti-theft system for smartphones. *IEEE Transactions on Mobile Computing*, *2018]*

Software-based

S4Lab

- Can you have a anti-theft SW platform?

Software-based example: Clean OS

S4Lab

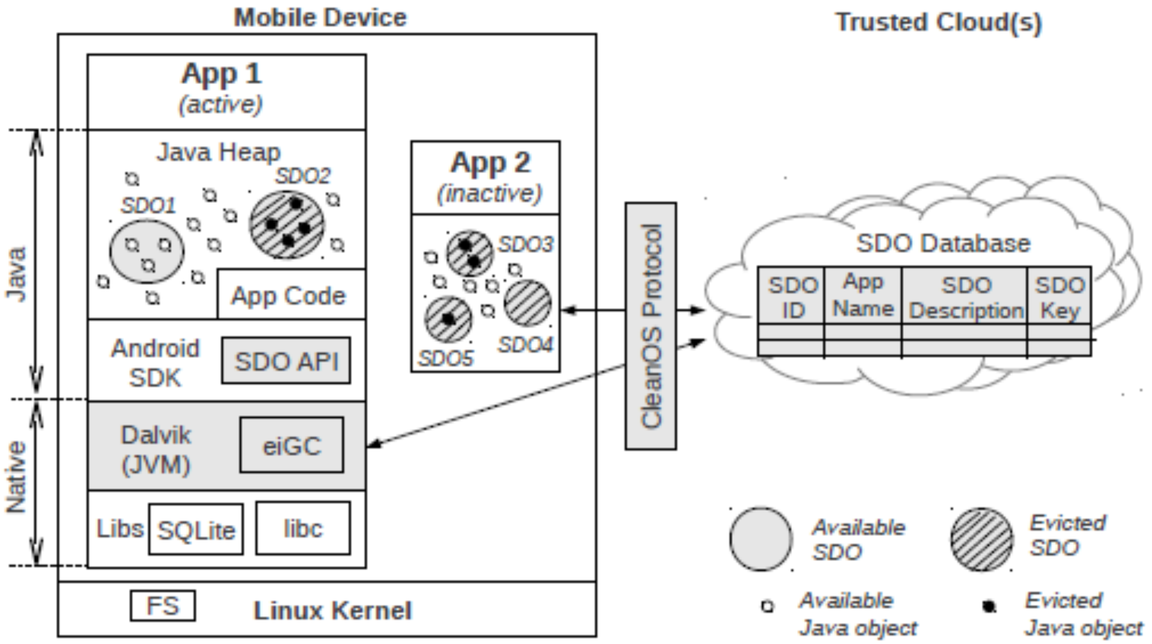
- Typical OSes were never designed with physical insecurity in mind.
- Mobile OSes should manage sensitive data rigorously, so as to maintain the device “clean” at any point in time in anticipation of device theft/loss.
- The goal: If device is stolen or lost:
  - The minimal amount of sensitive data is exposed.
  - User retains post-theft control over unexposed data.
- New Android-based OS that minimizes sensitive data exposure by evicting it to a trusted cloud whenever not under active use.

[Tang, Y., et al. CleanOS: Limiting mobile data exposure with idle eviction. *OSDI, 2012]*

CleanOS architecture

S4Lab

- The sensitive data object (SDO) abstraction.
- A modified, eviction-aware version of the Dalvik interpreter, along with an evict-idle garbage collector (eiGC).
- The SDO cloud store.



[Tang, Y., et al. CleanOS: Limiting mobile data exposure with idle eviction. *OSDI, 2012]*

Secure update of personal devices

Secure update

S4Lab

- What is a secure update?
- Different types of update process?

Secure update

S4Lab

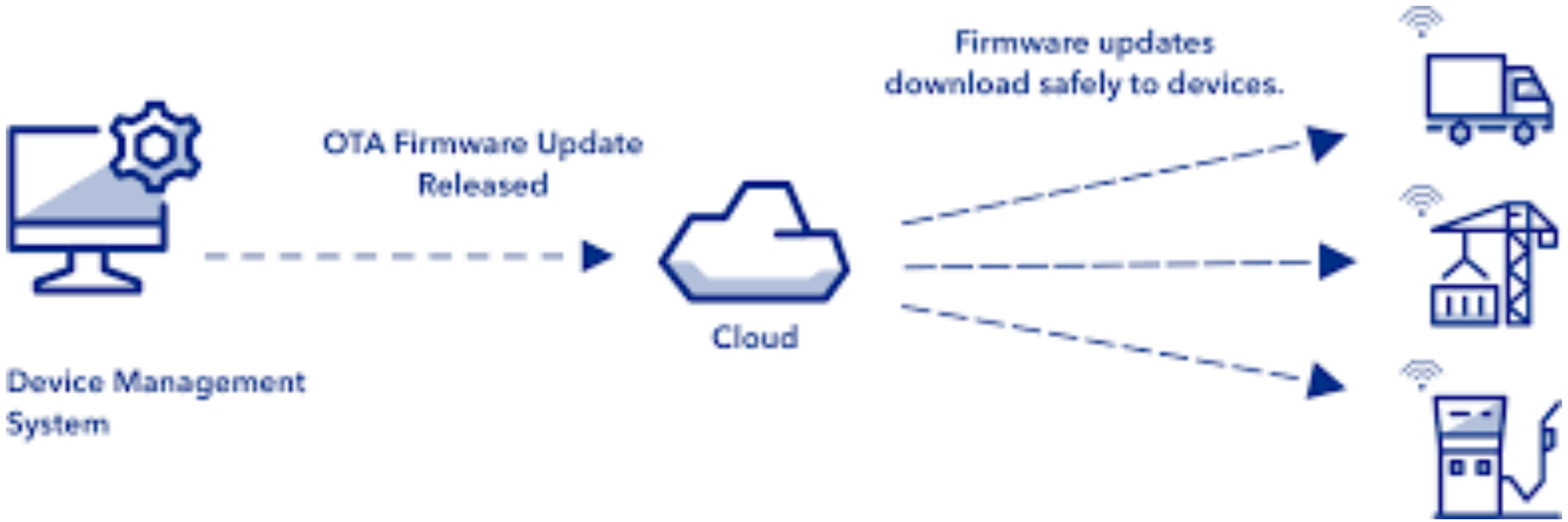
- What is a secure update?
  - Would an original none-malicious update, suffice?
  - Delivery at correct time (Freshness).
    - Roll back/downgrade attack
    - Delayed update (Fast-forward-attack/Indefinite freeze attacks)
  - No other file/functionality
  - No denial of service caused by process of updating
  - Fail-safe
- Different types of update process
  - Administered locally via a network
  - Over-the-Air (OTA)
  - Update isolated critical devices without internet access

[https://github.com/theupdateframework/tuf/security/policy]

OTA update

S4Lab

- Over-the-air programming (OTA) refers to various methods of distributing new software, configuration settings, and even updating encryption keys to devices.
  - One central location can send an update to all the users, who are unable to refuse, defeat, or alter that update.



[https://en.wikipedia.org/wiki/Over-the-air_programming]
[image :https://blog.particle.io/ota-firmware-updates/]

OTA update

S4Lab

- The good:
  - Update Automation.
    - How many ECU? LOCs in a car?
  - OTA updates provide OEMs with the ability to provide security patches.
  - Over-the-air (OTA) updates are great things, in theory. You get the latest monthly Android security patch delivered to your smartphone.
- The bad:
  - New silent attack surface.
  - The trust problem. OEM full control over our device?

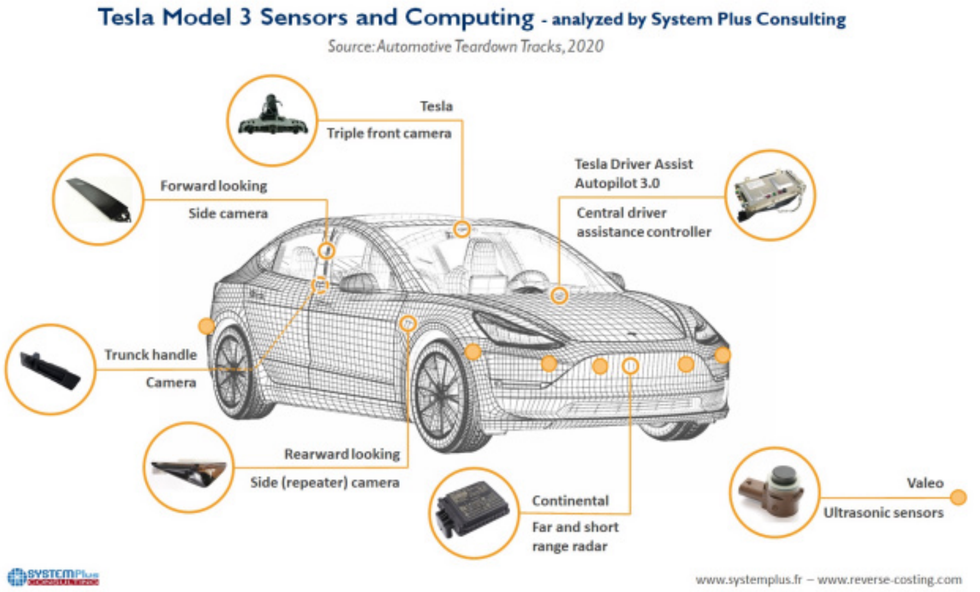
[https://www.forbes.com/]


TikTok
@sergeygusev190
Tesla cars software update
via satellite

The case of Tesla

S4Lab

- Braking distance on the Tesla Model 3 was worse than that of a Ford F-150, CEO Elon Musk took the criticism and found a solution.
- Days later, Tesla shipped an over-the-air update that, according to CR's testing, improved the braking distance by 19 feet.
- It creates the feeling that you could get out of your car one night, and by the time you get back in the next morning, the car could do some things — maybe everything — in a totally different way.
- You don't buy a car, or a phone, or soon enough a house or a medical implant or whatever: you buy an interface to, or an aspect of, a huge platform-company-ecosystem-whatever that changes by the minute.



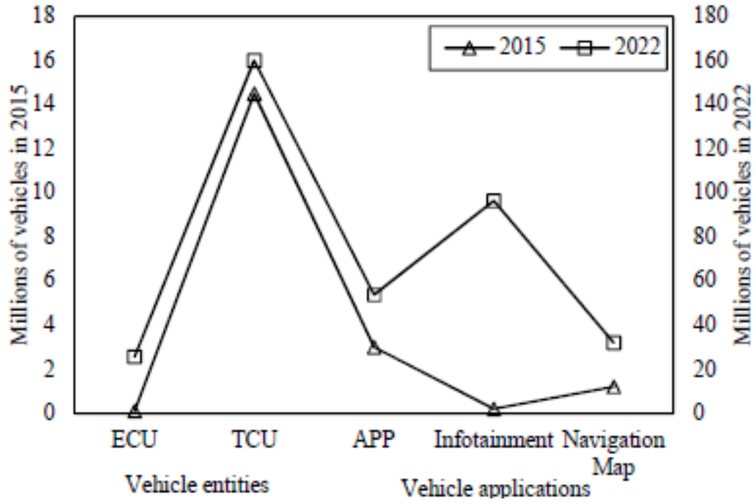
[https://www.theverge.com]

Car OTA

S4Lab

- Many parties are involved :Car, Cloud Server, Mobile Phone, OEM, Spare part OEM, Software Distributor (SD), Car Owner, Service Center, Insurance Company and Law and Enforcement Personnel
- TCU downloads the updated software package from the cloud server. After successful downloading, the TCU at firsts verifies the software package and subsequently distributes the software to the appropriate ECUs.

[mehrnews.com/xTdB5]



[Halder, S., Ghosal, A., & Conti, M., Secure ota software updates in connected vehicles: A survey, 2019, arXiv:1904.00685]

Over-the-air vs on-the-go software updates

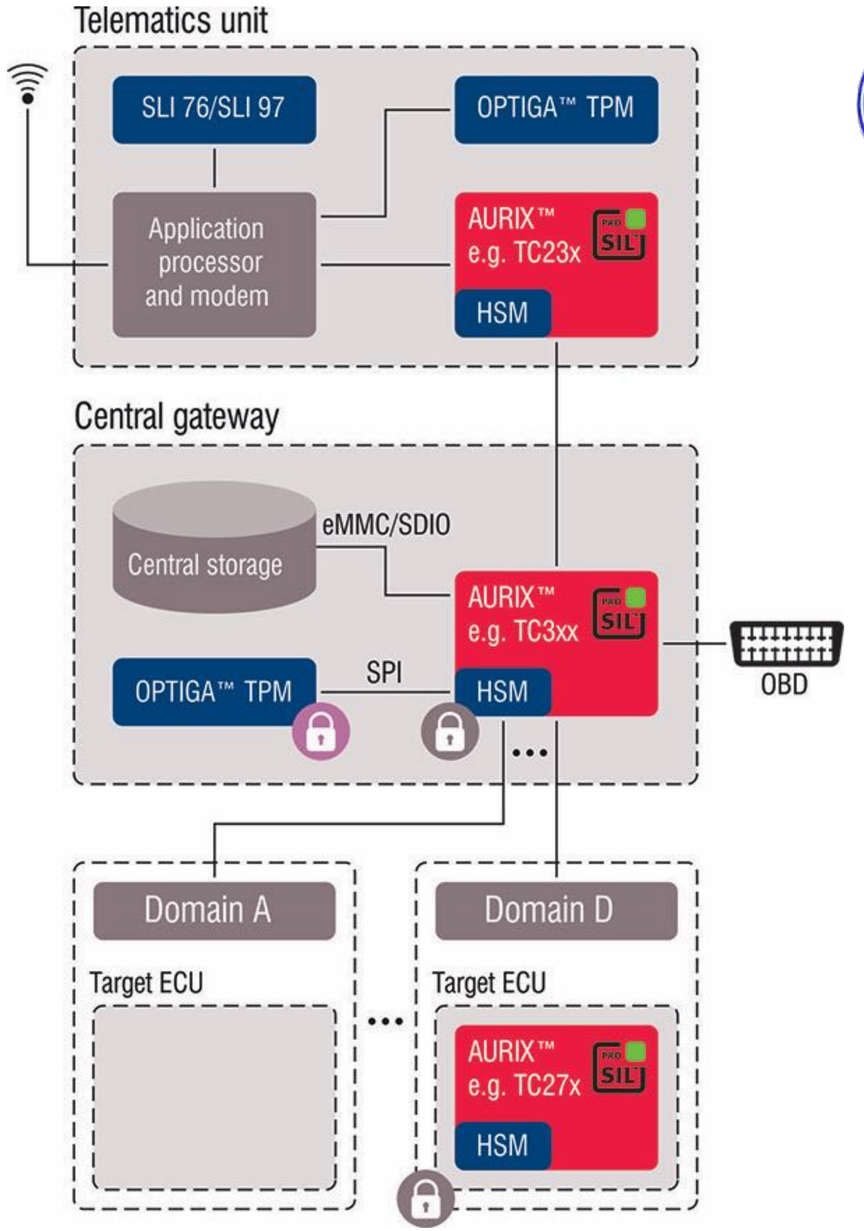
S4Lab

Car Companies	S/W Update Triggered by Whom	Update Notification	Driving Possibility during Update Process
Tesla [92]	Tesla	Sent through an embedded AT&T 3G data connection or a Wi-Fi router for Model S cars	No
BMW [93]	BMW	Customer receives notification through Connected Drive system present in the car	No
Mercedes Benz [94]	Costumer	Update notification sent through an embedded Verizon 3G data connection for C and S class cars	No
Audi [95]	Information N/A	Update notification sent through an embedded T-Mobile 3G data connection for its A3, A4, A5, Q2, Q5 and Q7 cars	No
General Motors [96]	Information N/A	Chevy Volt model uses the OnStar Verizon 3G data connection for receiving update notification	No

[Halder, S., Ghosal, A., & Conti, M., Secure ota software updates in connected vehicles: A survey, 2019, arXiv:1904.00685]

SOTA

- Securing the OTA
- The vehicle architecture for SOTA can basically be subdivided into three ECU blocks in which different security micro-controllers perform different security functions:
  - Telematics controller
  - Central gateway
  - Target control unit



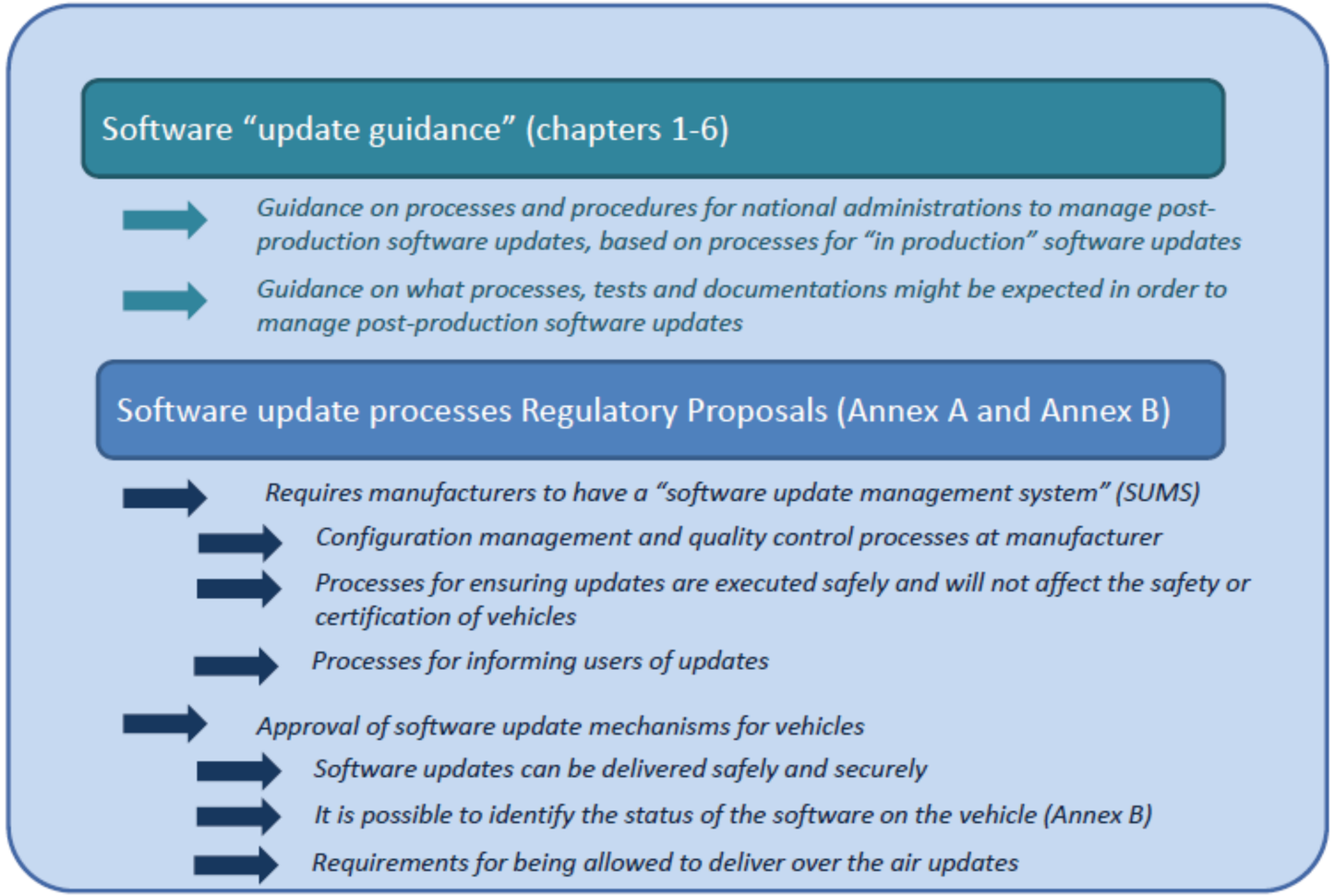
[https://electronicsmaker.com/]

UNECE software update recommendations

S4Lab

UNECE

- By United Nations Economic Commission for Europe.
- Regulation aim for connected vehicles. By Task Force on Cybersecurity and OTA.



[https://unece.org/]

Mobile OTA

S4Lab

- The fragmented nature of the Android smartphone ecosystem, with a myriad of different manufacturers, handset models, network providers and geographic combos out there:
  - Getting the monthly OTA security update promptly cannot be guaranteed.
- Google releases security updates only through OTA updates monthly.
  - However, a month is a sufficient time window that allows the attacks.
- Google's security OTA updates are only for their own Nexus (Pixel) devices, while the other manufacturers catch up according to their capabilities.

[Wu, J., & Yang, M., LaChouTi: kernel vulnerability responding framework for the fragmented Android devices. *Joint Meeting on Foundations of Software Engineering,* 2017]

Seem-less update

S4Lab

- A/B system updates
- OTA updates can occur while the system is running,
- use two sets of partitions referred to as slots (normally slot A and slot B).
- The system runs from the current slot while the partitions in the unused slot are not accessed by the running system during normal operation.
- This approach makes updates fault resistant by keeping the unused slot as a fallback.
- Decide when to take an update. Because A/B updates happen in the background, they are no longer user-initiated. To avoid disrupting users, it is recommended that updates are scheduled when the device is in idle maintenance mode, such as overnight, and on Wi-Fi. However, your client can use any heuristics you want.

https://source.android.com/devices/tech/ota/ab

Image: https://www.e-consystems.com/blog/system-on-module-SOM

Other secure update challenges

S4Lab

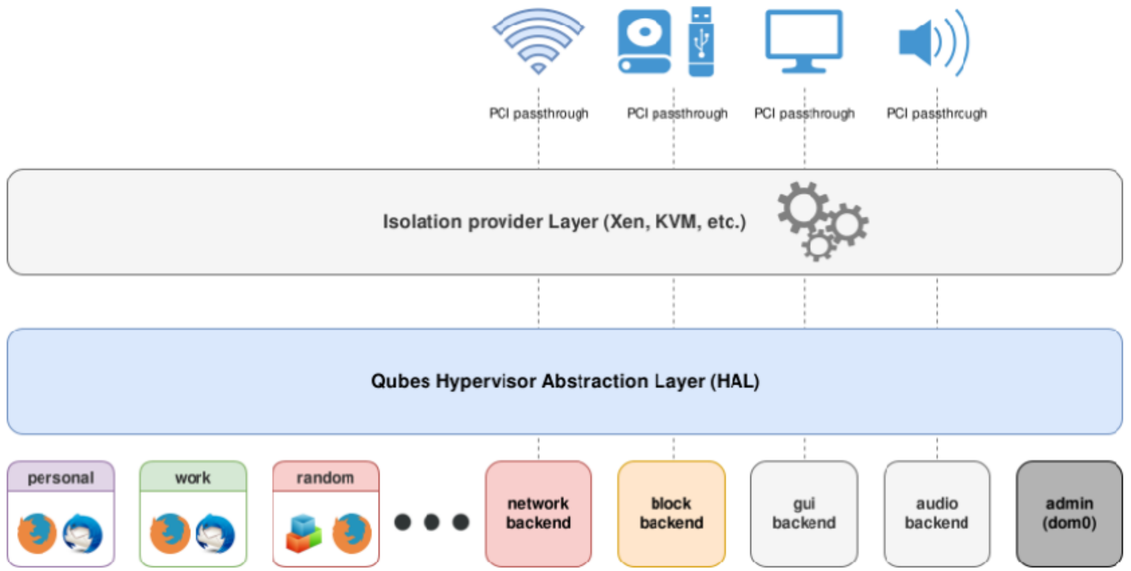
- Secure / verified boot story still problematic.
- Usually hardware specific.
- Trusted execution environment not widely used.
- Trusted execution of the OTA client (image update / swap).
- Runtime integrity check.
- Trusted storage / eMMC

[Salveti R., Bennett, A.m BoF: Secure OTA Collaboration, 2017]

Update isolated critical devices without internet access : An example

S4Lab

- Qubes OS has different domains.
- Dom0 is the most trusted domain on Qubes OS.
  - For this reason they decided to design Qubes in such a way that Dom0 is not connected to any network.
    - This makes it hard to update.
  - Updates (*.rpm files) are checked and downloaded by UpdateVM, or any other, network-connected VM.



https://www.qubes-os.org

Secure storage

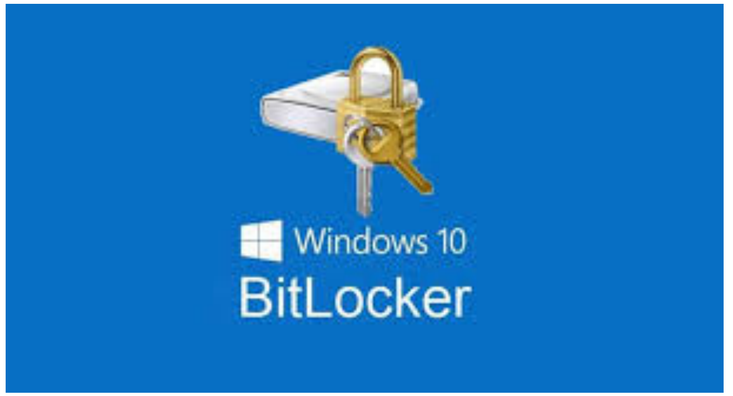
When data is at rest in our system

Disk-level vs file level protection policies

S4Lab

- Hard disk level
  - Full disk encryption
  - All or none! Decrypts all once you have entered the pass till you turn the system off.
    - Truecrypt/Bitlocker
- File-system level
  - Cryptographic file systems e.g. Encrypting File System (EFS) for NTFS

APPLE
FILEVAULT
ENCRYPTION



Pre-boot authentication

S4Lab

- Encryption isn’t sufficient, if all protections implemented as post-boot protections.
  - Bootkits
  - It isn’t secure to unlock or decrypt data before authenticating.
- So Pre-boot authentication is required
  - By Password/token/…
- FDE (i.e. full disk encryption) products have some built-in pre-boot authentication mechanisms.

Dangers of an OS on an unauthenticated system

S4Lab

- Our products often work inside the OS.
- What about:
  - Evil maid attacks
  - Cold boot attacks
- What are the choices?
- Authenticating a system by:
  - Pre-boot authentication?
  - Secure-boot/verified boot/TPM
  - Hardware-based disk encryption

Boot chain

S4Lab

- CPU Reset vector in ROM → legacy boot block
- Basic CPU, chipset initialization →
- Initialize Cache-as-RAM, load and run from cache →
- Initialize DIMMs, create address map.. →
- Enumerate PCIe devices.. →
- Execute Option ROMs on expansion cards
- Load and execute MBR →
- 2nd Stage Boot Loader / OS Loader → OS
- or a Full-Disk Encryption Application
- or a Bootkit

[Bulygin, Y., Evil maid just got angrier: Why full-disk encryption with TPM is insecure on many systems. *CanSecWest, 2013]*

Evil maid just got angrier: Why full-disk encryption with TPM is insecure

S4Lab

Attack Outline Against Encrypted OS Drive

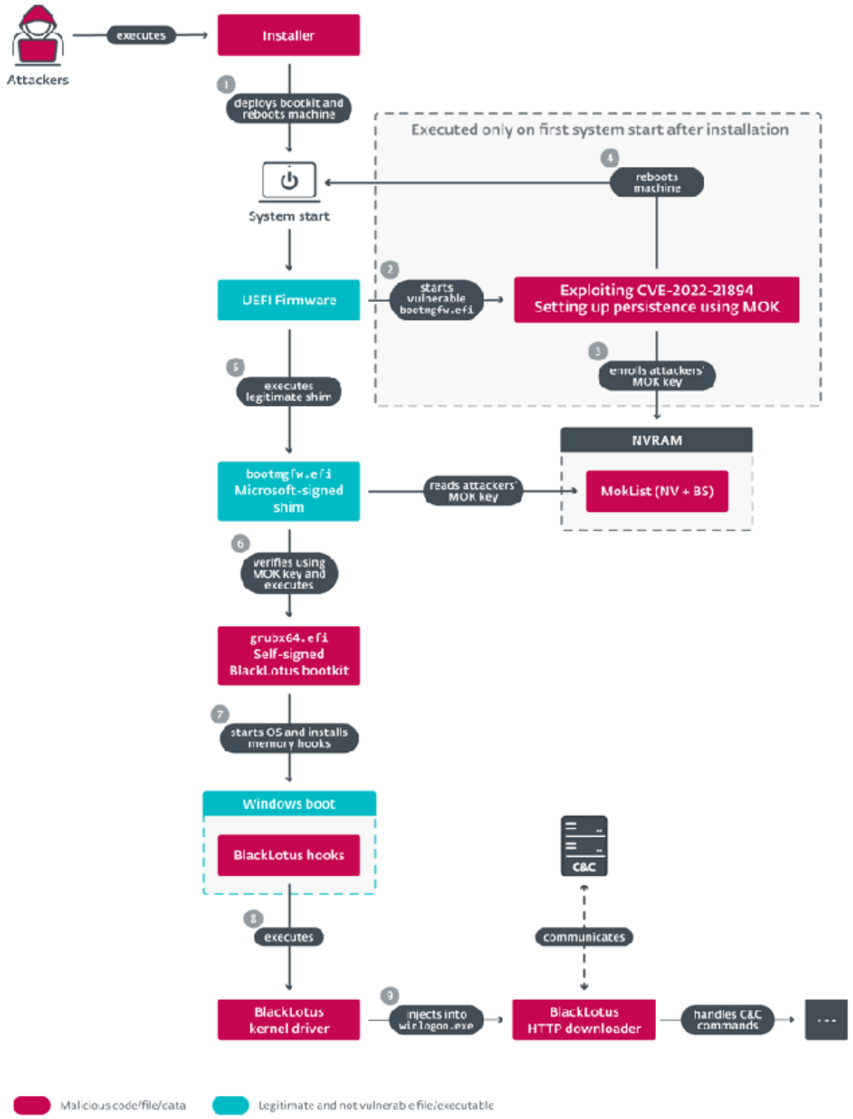
1. While the owner is not watching and system is shut down..
2. adversary plugs in and boots into a USB thumb drive
3. which auto launches exploit directly modifying UEFI BIOS in unprotected SPI Flash
4. Gets out until owner notices someone is messing with the system
5. Upon next boot, patched UEFI BIOS sends expected 'good' measurements of all pre-boot components to TPM PCRs
6. TPM unseals the encryption key as the measurements are correct

[Bulygin, Y., Evil maid just got angrier: Why full-disk encryption with TPM is insecure on many systems. *CanSecWest, 2013]*

BlackLotus UEFI bootkit

S4Lab

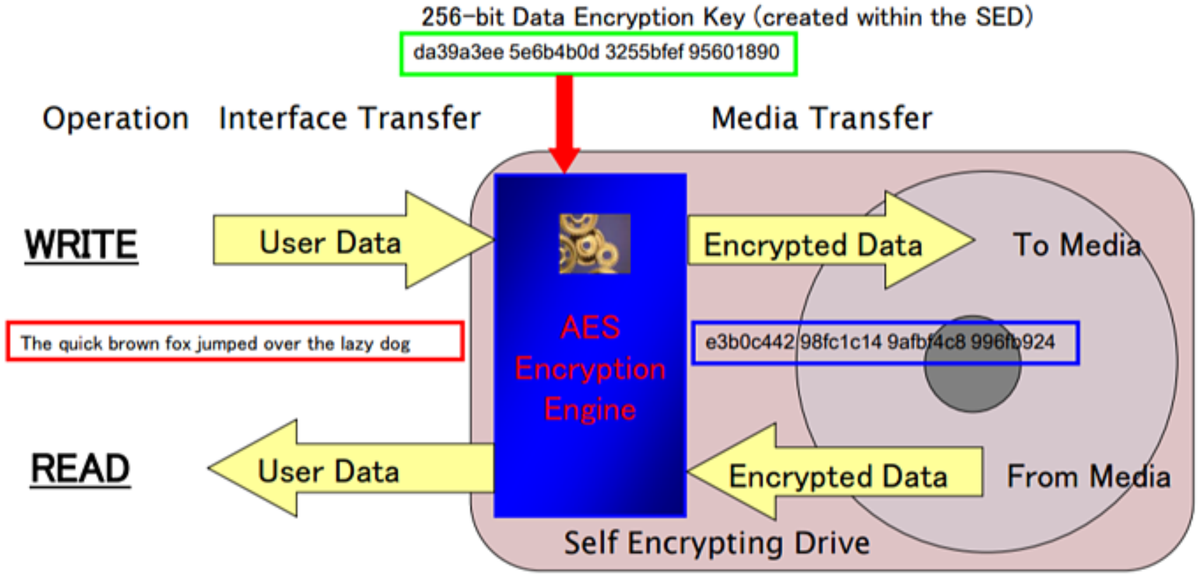
- Report from March1st, 2023
- Runs on the latest, fully patched Windows 11 systems with UEFI Secure Boot enabled.
- Exploits (CVE-2022-21894) to bypass UEFI Secure Boot and set up persistence for the bootkit.
- Capable of disabling OS security mechanisms such as BitLocker, HVCI, and Windows Defender.



Self-encrypting drive (SED)

S4Lab

- Hardware-based disk encryption.
- No need for user input or disk encryption software.
- Major technology and data storage companies
  - i.e. Samsung, Seagate, and Toshiba.
- Drawbacks?



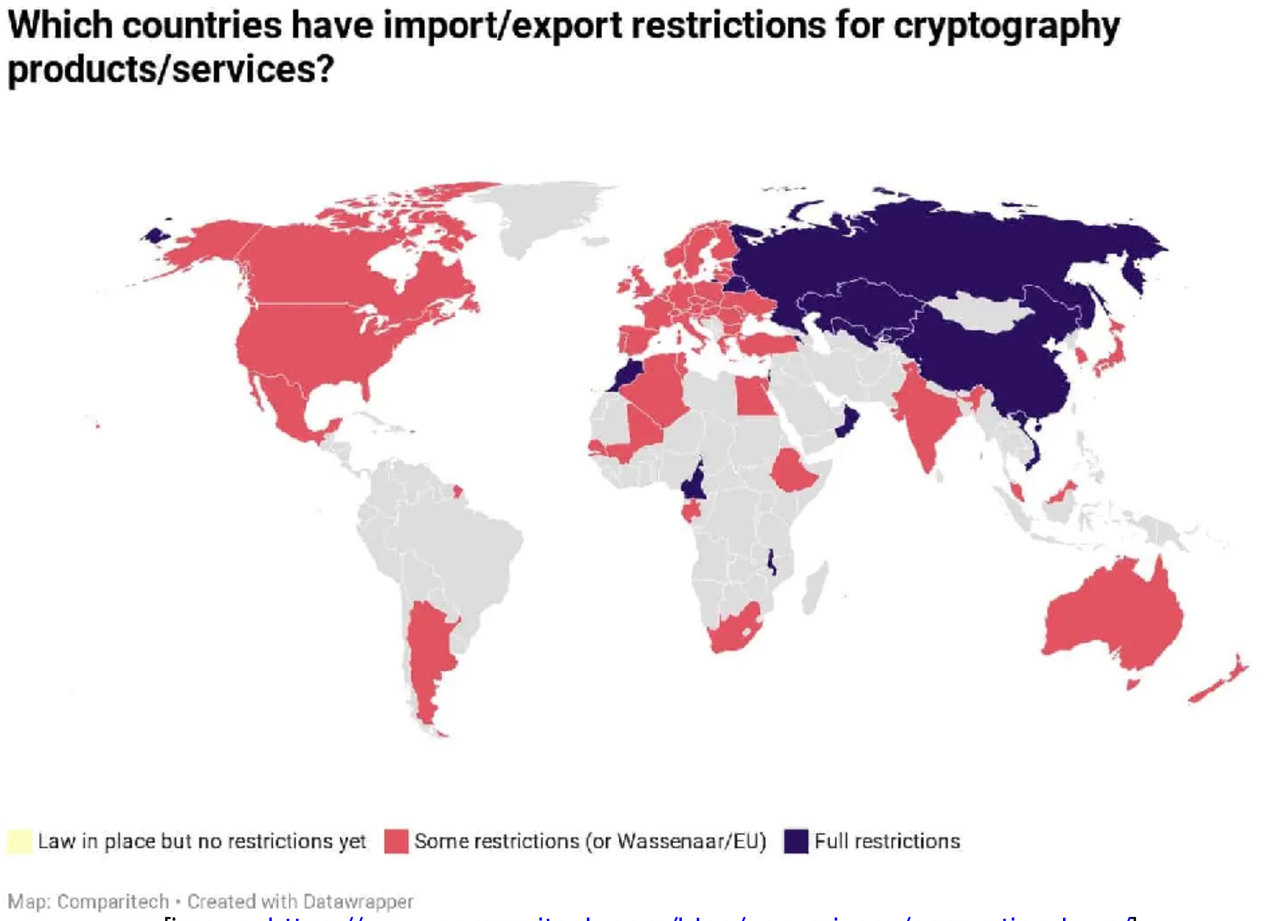
[Image: https://www.trentonsystems.com/]

[https://www.trentonsystems.com/]

The passion of encryption

S4Lab

- How legal to use encryption?
- There are many countries ban/regulate the import, export and use of products with encryption power.



[image: https://www.comparitech.com/blog/vpn-privacy/encryption-laws/]

Wassenaar Arrangement

S4Lab

- COCOM (Coordinating Committee for Multilateral Export Controls) was an international organization for the mutual control of the export of strategic products and technical data from country members to proscribed destinations
- In 1995, 28 countries decided to establish a follow-up to COCOM, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

[Image: https://www.wassenaar.org/participating-states/]

[http://www.cryptolaw.org/cls2.htm]

Wassenaar Arrangement

S4Lab

- The main goal of the COCOM regulations was to prevent cryptography from being exported to "dangerous" countries.
- Exporting to other countries is usually allowed, although states often require a license to be granted.
- 1998: up to 64-bit encryption HW/SW
- 2015: addressed a new type of cyber weapons known as intrusion software,
- Can you name a great actor who is not a member?

[http://www.cryptolaw.org/cls2.htm]

[Ruohonen J., Kimppa K., Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity, Journal of Information Technology & Politics, 2019]

Personal use exemption

S4Lab

- Allows a traveler to freely enter a participating country with an encrypted device under a "personal use exemption" as long as the traveler does not create, enhance, share, sell or otherwise distribute the encryption technology while visiting.
- Many nations do not recognize a "personal use exemption." Before traveling to these countries with an encrypted laptop, you will need to apply to their specified governmental agency for an import license.
- A loaner laptop?

[https://informationsecurity.princeton.edu/encryption/encryption-and-internatio]

Secure Log management

S4Lab

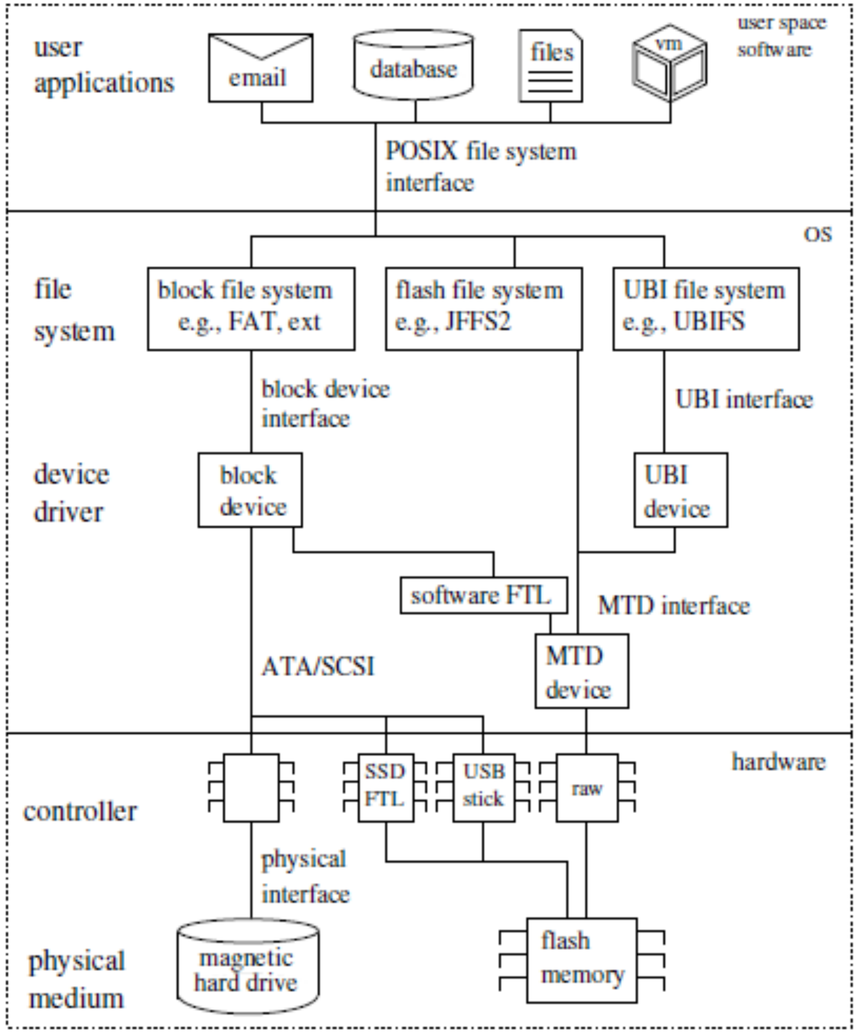
- Logs are one of the most important data at rest on your system.
- The attacker has several motivations to modify the logs.
  - Hiding evidence by altering event logs.
- An IT security professional who knows the defense mechanisms can prevent an intruder’s entry to computing machines.
  - Activate logging
  - Setting proper permissions
  - Using a separate logging server
  - Encrypting log files
  - Making log files append only
  - Protecting log files using write-once media

[https://eforensicsmag.com/course/log-files-attacks-defenses-w39/]

A broader look

S4Lab

- Secure data at rest policies should involve different layers.
- User-app, file system, device driver, controller, physical medium



[Reardon, J., Basin, D., & Capkun, S.,Sok: Secure data deletion, IEEE symposium on security and privacy, 2013]

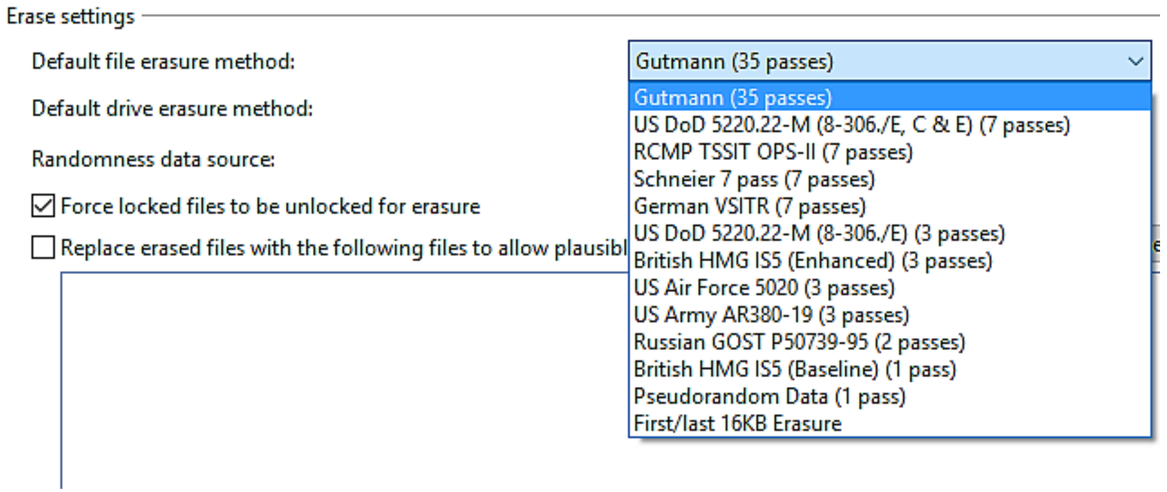
What is a secure deletion process?

A story against “the more, the better ” misconception

More is better?

S4Lab

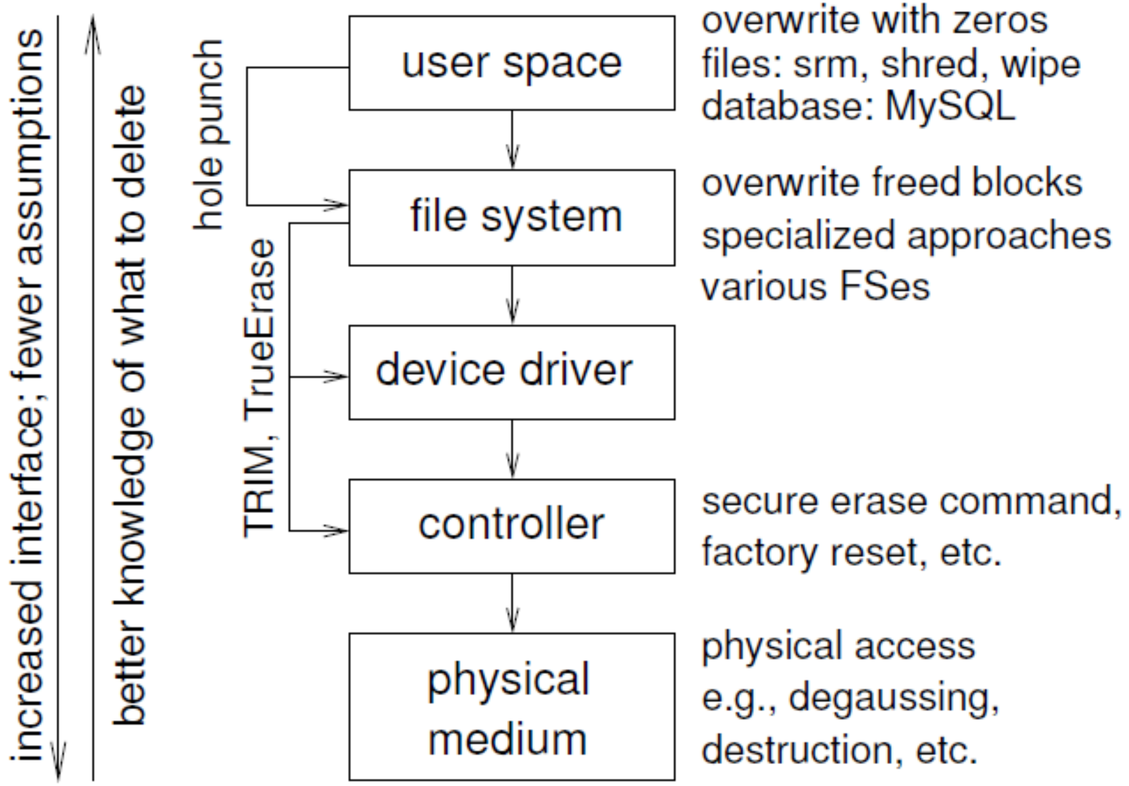
- A common realization is “more is better“.
  - Multiple times of over-writing is necessarily better.
  - Number of overwriting passes in 5220.22-M is 3.
- So a 3-time deletion is more secure than 1? And 7 is more secure than 3?
- Where do these numbers come from?
  - Head positioning in hard drives.



Secure deletion

S4Lab

- “Delete” a file often means unlinking files.
- Only changes file system metadata to indicate that the file is now “deleted”.
- Users typically assume, falsely, that when they delete the data is from that moment on irrecoverable.



[Reardon, J., Basin, D., & Capkun, S.,Sok: Secure data deletion, IEEE symposium on security and privacy, 2013]

Other considerations

S4Lab

- Imagine an ideal deletion policy and technique is present.
- What are other considerations which highly affect the secure deletion process?

Other considerations

S4Lab

- Imagine an ideal deletion policy and technique is present.
- What are other considerations which highly affect the secure deletion process?
  - The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address.
  - Any configuration options limiting the ability to access the entire addressable area of the storage media.

[Kissel, R., et al., Guidelines for media sanitization. US DoC, National Institute of Standards and Technology, 2014]

Is there any standard process?

S4Lab

	DoD 5220.22-M	NIST 800-88 Rev. 1
Number of overwriting passes	3	1
Standard current date	Revised 2006	Revised 2012
Considers new technology (e.g.: SSD)	No	Yes
Sector created for	Government	All organizations
Outlines specific data erasure methods	No	Yes
Verifiable secure method of erasure	Yes (HDD only)	Yes
Maximum ecological conservation	No	Yes

[https://www.sipicorp.com/wp-content/uploads/2019/09/NIST_vs_DoD_V3.pdf]

State considered harmful…

What does stateless mean?

S4Lab

- A spectrum of different approaches:
  - From use of a live OS.
  - To a completely stateless computer ideas.
- The idea is to be as stateless as possible.
  - Do not rely on any untrusted persistent data which may be compromised by the attacker.
- Here, stateless is a related but not the same concept as in the web context.

[Rutkowska, Joanna, State considered harmful, 2015]

The idea of Stateless computers

S4Lab

- A new trend to have stateless computers, i.e. lacking any persistent storage.
- This includes it having no firmware-carrying flash memory chips.
- All the state is to be kept on an external, trusted device.
  - A small USB stick or SD card form factor.
- This clean separation of state-carrying vs. stateless silicon is, however, only one of the requirements.
- Additional stateless requirements:
  - Endpoint (laptop) hardware.
  - Trusted “stick”.
  - The host OS.

[Rutkowska, Joanna, State considered harmful, 2015]

States in Laptop

S4Lab

- State-carrying (persistence-carrying) elements on a modern x86 laptop.
  - The SPI flash chip carrying the BIOS, ME, and other firmware.
  - The Embedded Controller (EC),
  - Additional discrete devices:
    - e.g. the WiFi or BT modules.
      - Typically they would contain their own flash memories to hold their own firmware.
  - Finally, there is the hard disk.

[Rutkowska, Joanna, State considered harmful, 2015]

Discrete devices

S4Lab

- Occasionally there might be additional discrete devices on the laptop, such as a discrete GPU.
  - Such devices will likely come with their own internal flash memory, thus breaking the stateless principle.
- In most cases these discrete devices would also be bus-mastering devices (capable of issuing DMA to host memory).
  - They could not only be used as a secret storage, but also interfere with the platform boot process if it is not properly secured against DMA from devices.
- It’s thus best to ensure no discrete devices are present on the laptop, especially no discrete GPUs.

[Rutkowska, Joanna, State considered harmful, 2015]

Stop sending the state!

S4Lab

- The wireless devices Can send the state on the network.
  - The easiest way to address all the above mentioned problems is to fit a physical kill switch for each (or all) of the wireless devices.
    - An actual switch, not just an ask window :)
    - Physical kill switches are not an elegant solution, as in most cases the user would like to have some form of wireless connectivity.
  - It would be beneficial to either:
    - Not have any internal WiFi or BT card, or
    - A simple networking proxy implemented on an external (trusted) uC, not directly connected to the host processor.

[Rutkowska, Joanna, State considered harmful, 2015]

Live OS choice

S4Lab

- Loads from a removable storage device
  - A CD/DVD, an external data drive, or even a USB stick.
- In this context stateless == Live == no persistence
- An example is Tails
  - Aims to be a stateless OS that leaves no trace on the computer of its presence
- LiveUSB OSes like Ubuntu Linux apply all filesystem writes to a casper filesystem overlay (casper-rw).
  - Once full or out of flash drive space, becomes unusable and the OS ceases to boot.

Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA

When NSA whistle-blower Edward Snowden first emailed Glenn Greenwald, he insisted on using email encryption software called PGP for all communications. But this month, we learned that Snowden used another technology to keep his communications out of the NSA's prying eyes. It's called Tails. And naturally, nobody knows exactly who created it.

[https://www.wired.com/2014/04/tails/]

Acknowledgments

S4Lab

- [welivesecurity] BlackLotus UEFI bootkit: Myth confirmed, https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/, Visited Feb 2024.

Questions?