Safe Computing:
Lower Exposure and Risk

Presented by: Emyll Almonte
IT Systems Administrator

Disclaimer
Any instruction / proof-of-concept shown on this presentation has been done on systems owned by me, is for educational purposes only, and most of the information disclosed is readily available on the internet. I am not responsible for what you do with the information, even though as cybersecurity professionals, you need to understand the different forms of attack in order to come up with a protection plan.

What is “Safe Computing” ?

- In simple terms: Safe Computing combines the use of cybersecurity best practices, physical precautions with your equipment, and common sense.
- One of many online definitions: Safe Computing involves using available tools to aid the protection of computer systems from theft, infiltration, exfiltration, damage to the hardware, software, electronic data, as well as from the disruption or misdirection of the services they provide.
- Computers are up against hardware malfunctions, viruses, malware, adware, phishing, hijacking, spyware, identity theft, ransomware, and so on..

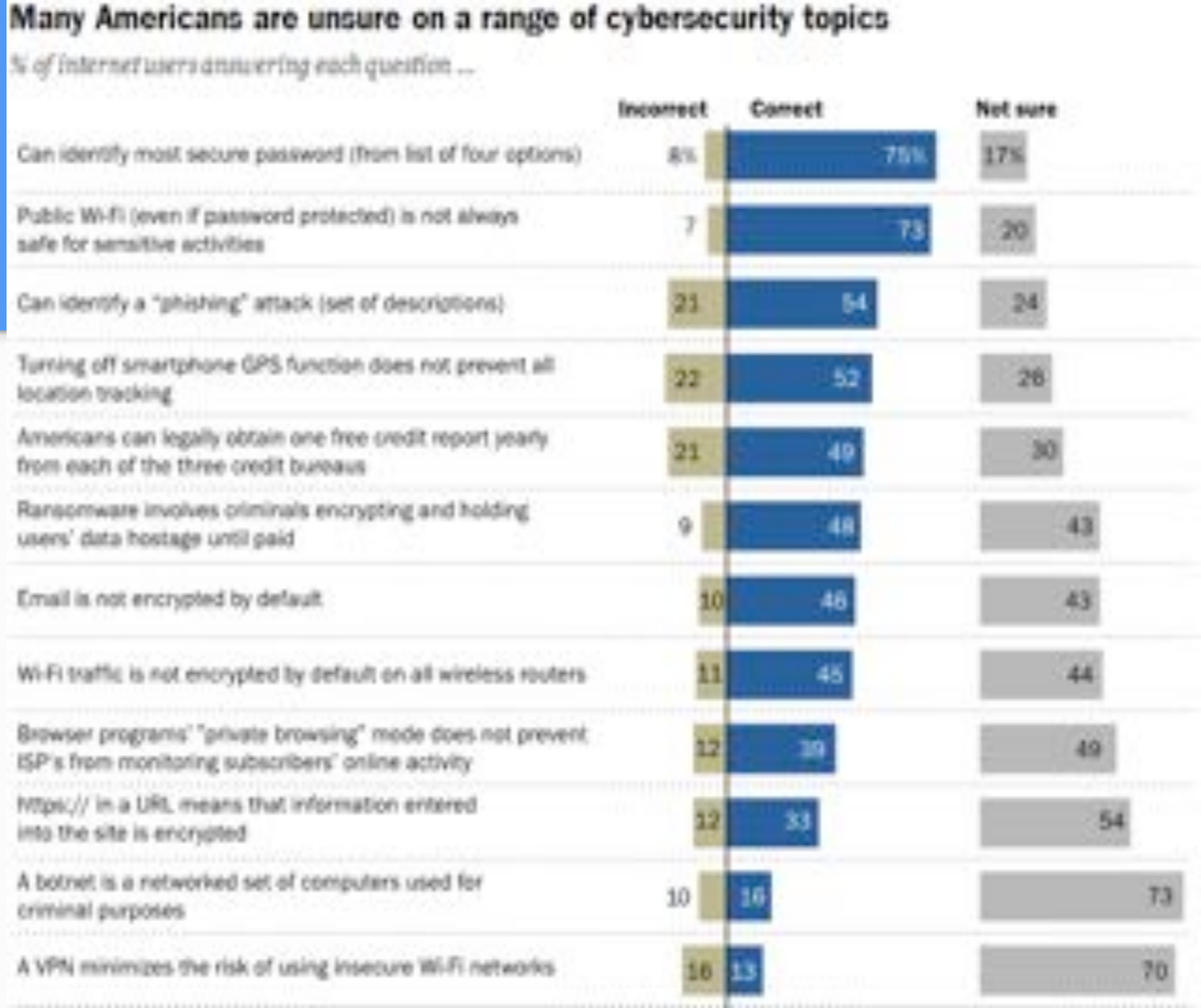
Exposure and Risks?

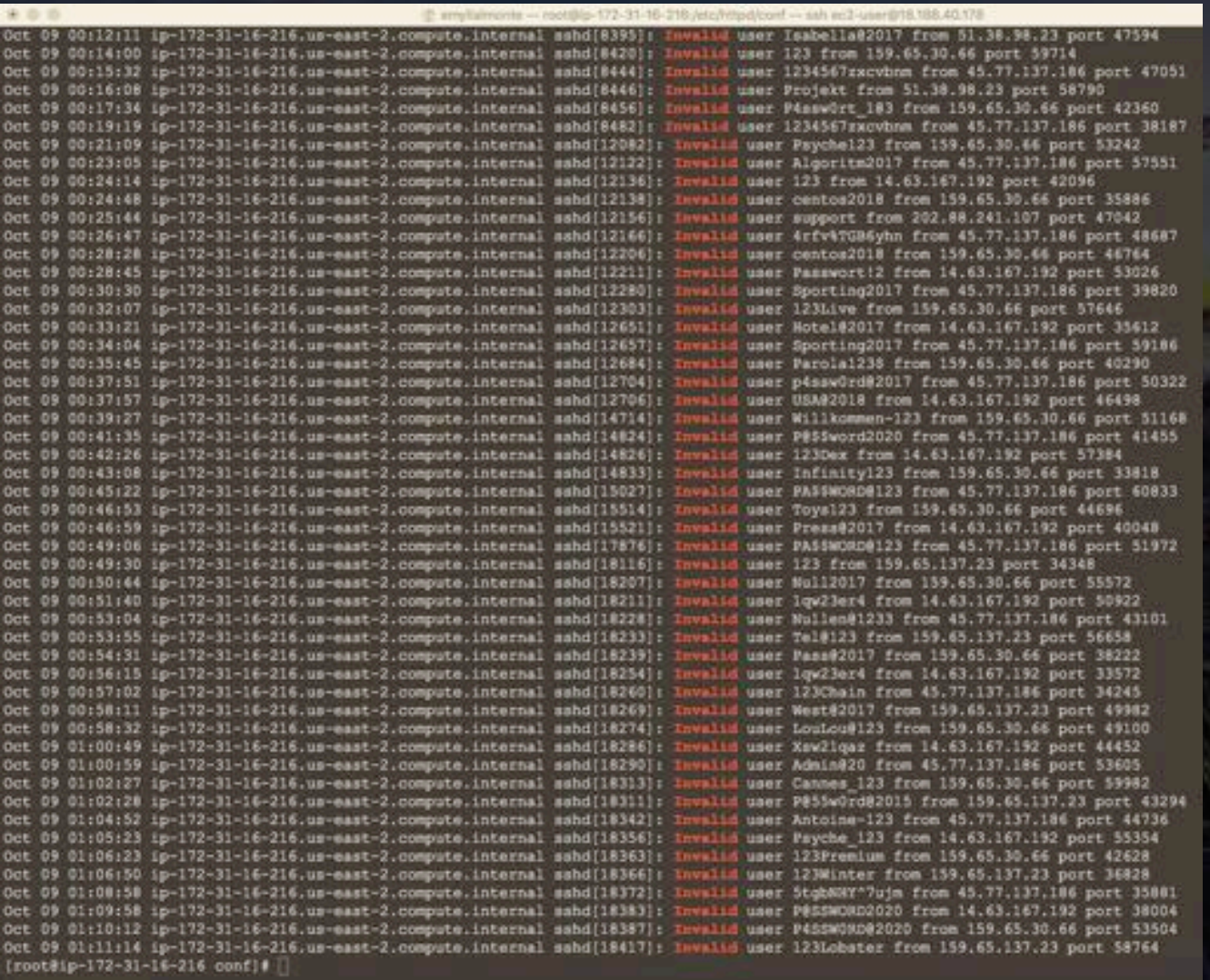
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Protecting the system from exposure doesn’t necessarily protect the user (email phishing, online scams, etc).
- These cyber/digital attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
- As IT Professionals, we must focus on figuring out ways to ***lower the risk*** of our systems and their users from such attacks because there is no tool or software that can protect with 100% guarantee.

“ Click here to protect your account! ”

The average computer user has very basic general knowledge and understanding of cybersecurity and how networks function overall..

It’s up to us to protect them as much as possible..





… Just minutes after turning on one of my Amazon EC2 instances.

… Imagine an out of the box computer being used by the average user with default settings.

“Keep all software up-to-date, he said”

- **Do not trust that your data or system is 100% safe just because you installed a firewall, antivirus or anti-malware software..**

MD5: message digest
SHA: secure hashing algorithm

www.theverge.com › ccleaner-hack-malware-security ▾

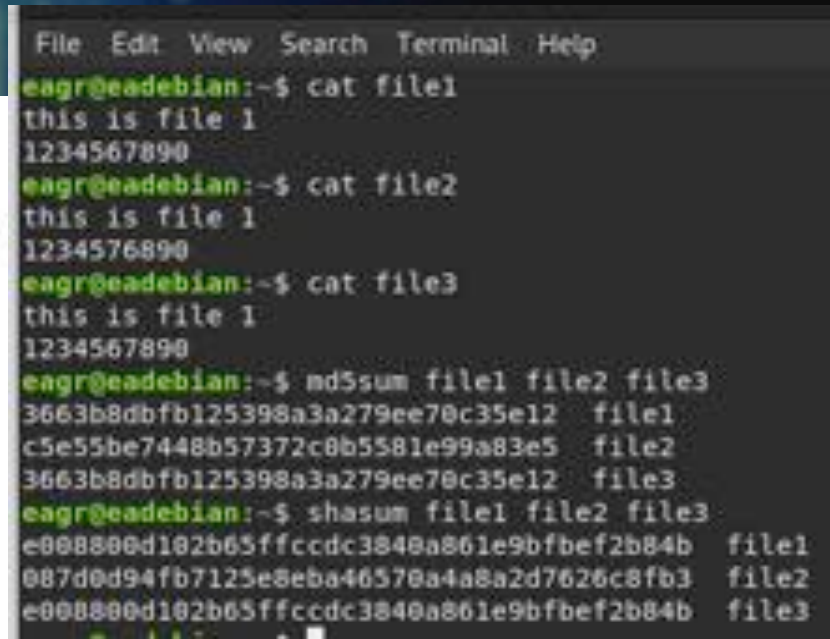
Hackers hid malware in CCleaner software - The Verge

Sep 18, 2017 - Hackers have successfully breached **CCleaner's** security to inject malware into the app ... An unusual attack on software **update** mechanisms.

www.vice.com › en_us › article › hackers-hijacked-asus-software-upd... ▾

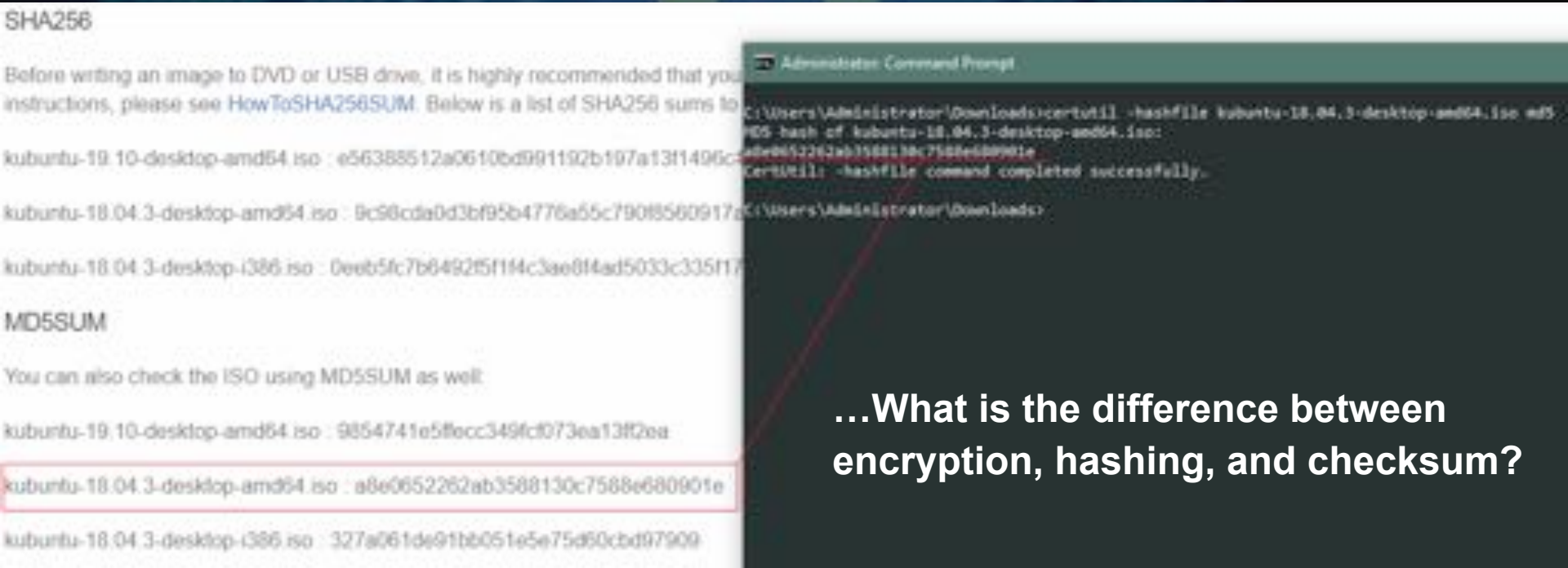
Hackers Hijacked ASUS Software Updates to Install ... - Vice

Mar 25, 2019 - Two different attacks discovered in 2017 also compromised trusted software **updates**. One involved the computer security cleanup tool known as **CCleaner** that was delivering malware to customers via a software **update**. More than 2 million customers received that malicious **update** before it was discovered.



“Keep all software up-to-date, he said”

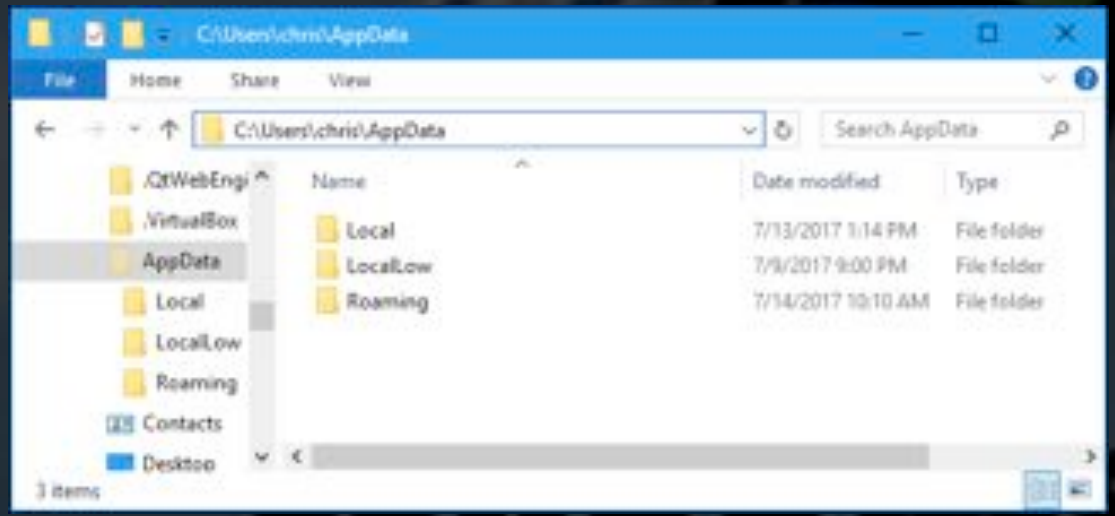
- **Do not trust that your data or system is 100% safe just because you installed a firewall, antivirus or anti-malware software..**

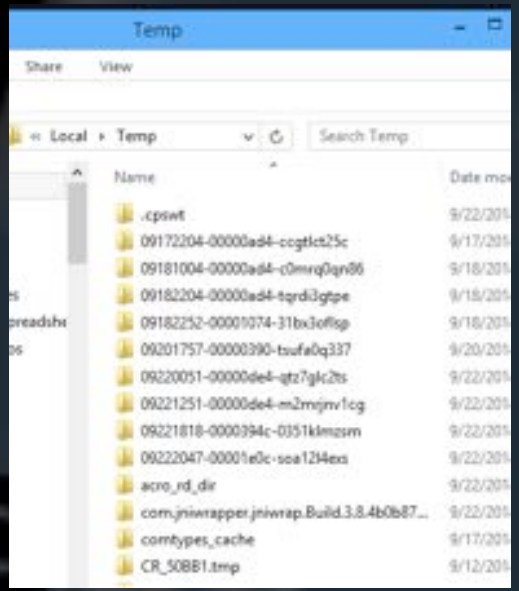


…What is the difference between encryption, hashing, and checksum?

Safe Computing: the OS + Network + Apps

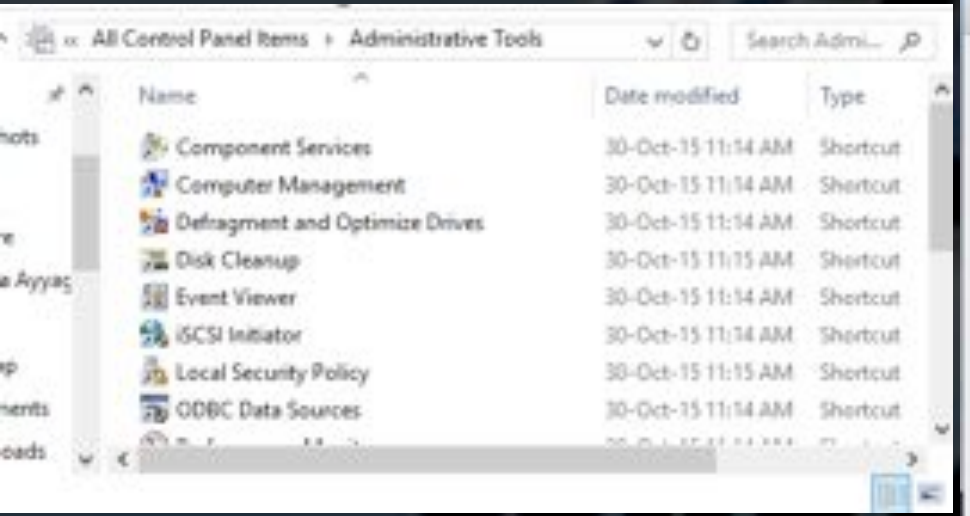
- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Setup user access to lower attack surface (thus lowering risk)
    - Intrusion comparison {admin vs standard vs guest}
    - Appdata folder vs System folder {adware/malware}





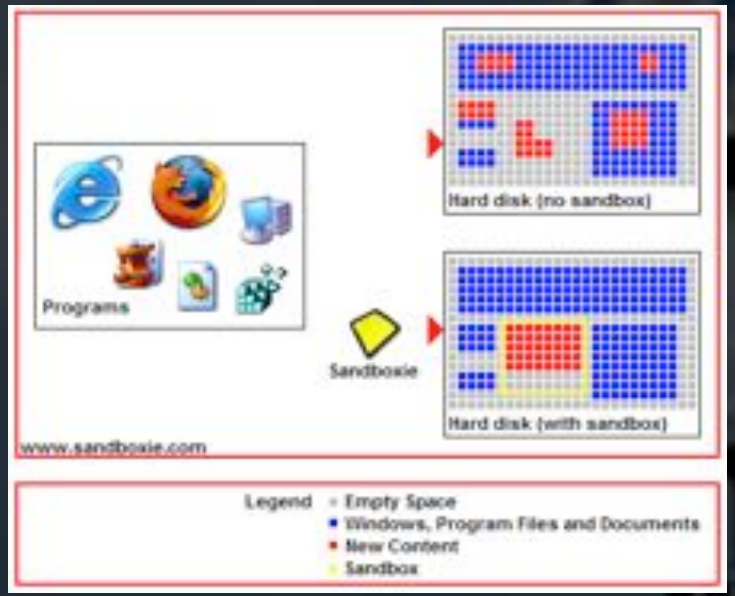
Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Setup user access to lower attack surface (thus lowering risk)
    - Intrusion comparison {admin vs standard vs guest}
    - Appdata folder vs System folder {adware/malware}



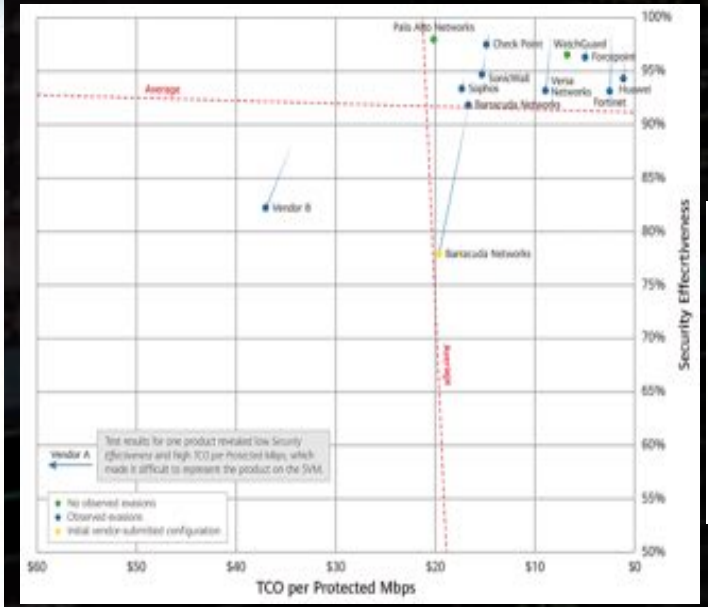
Safe Computing: the OS + Network + Apps

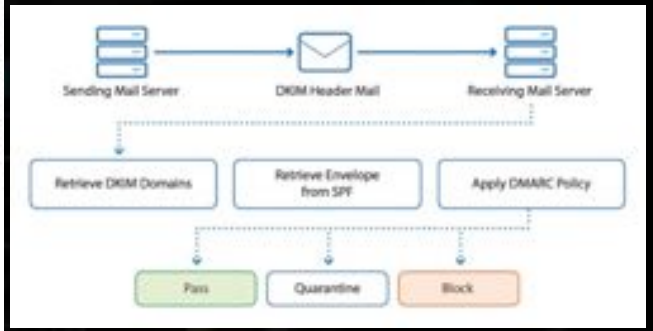
- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Setup user access to lower attack surface (thus lowering risk)
    - Intrusion comparison {admin vs standard vs guest}
    - Appdata folder vs System folder {adware/malware}
    - Sandboxing (apps) or DeepFreeze (system)



Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Install verified software (Firewall, AV, Antimalware, Anti-phishing, Encryption)
    - Compare products using NSS Labs, AV-Comparatives, or AV-Test
    - Sender Policy Framework and DomainKeys Identified Mail





Safe Computing: the OS + Network + Apps

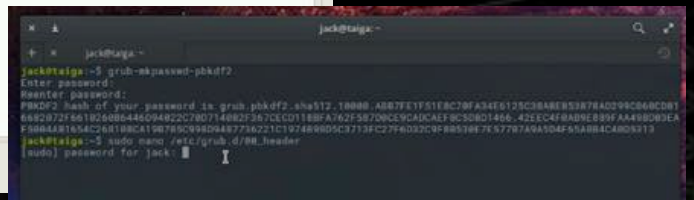
- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Install verified software (Firewall, AV, Antimalware, Anti-phishing, Encryption)
    - Compare products using NSS Labs and AV-Test results
    - Sender Policy Framework and DomainKeys Identified Mail
    - Bitdefender, Avast, Lulu, Snort, OpenDNS, Sandboxie, Firejail..

Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Install security extensions/add-ons on browser if necessary.. Balance between usability and protection..
    - uBlock, NoScript, Privacy Badger, VirusTotal, HTTPS Everywhere..

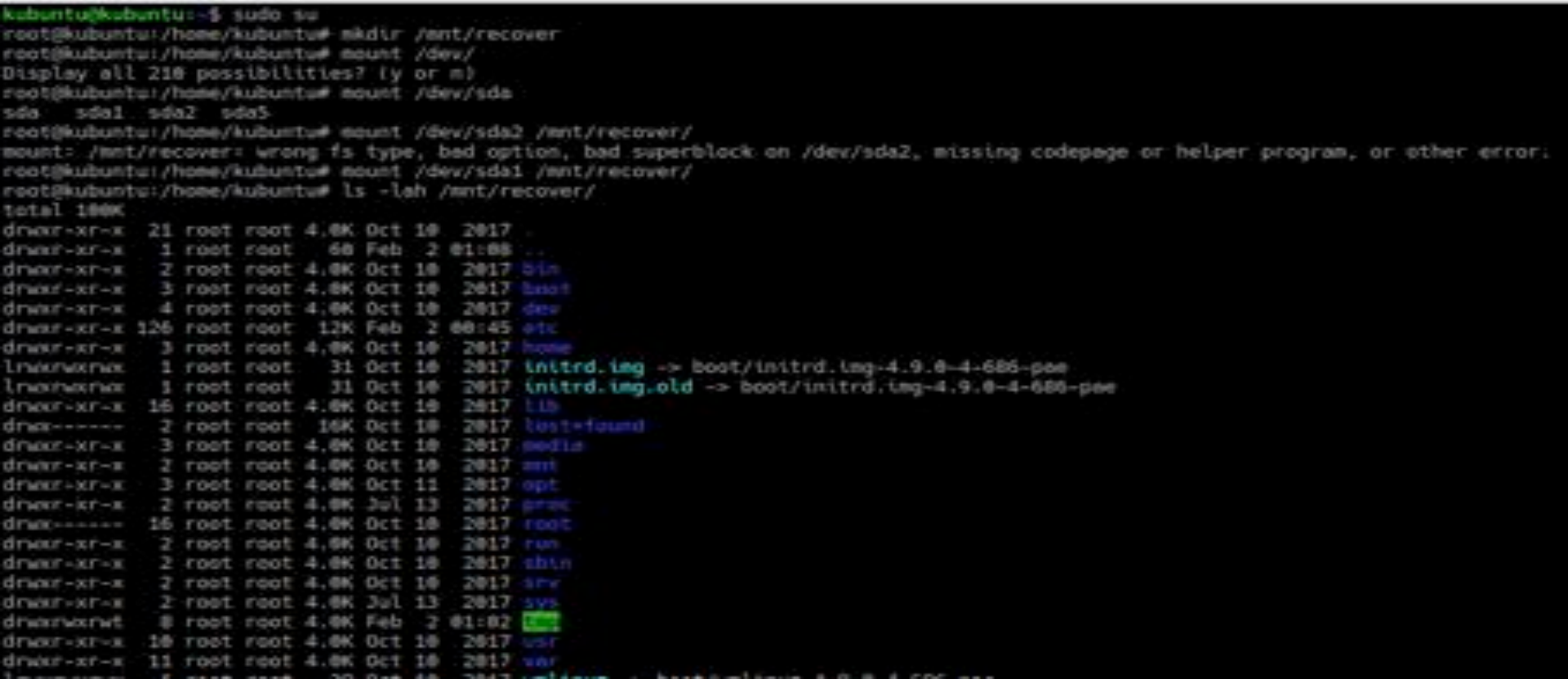
Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Install verified software (Firewall, AV, Antimalware, Anti-phishing, Encryption)
    - Compare products using NSS Labs and AV-Test results
    - Sender Policy Framework and DomainKeys Identified Mail
    - Bitdefender, Avast, Lulu, Snort, OpenDNS, Sandboxie, Firejail..
    - Entire Disk/Volume/System Encryption (VeraCrypt, LUKS, FileVault), TPM-chips..



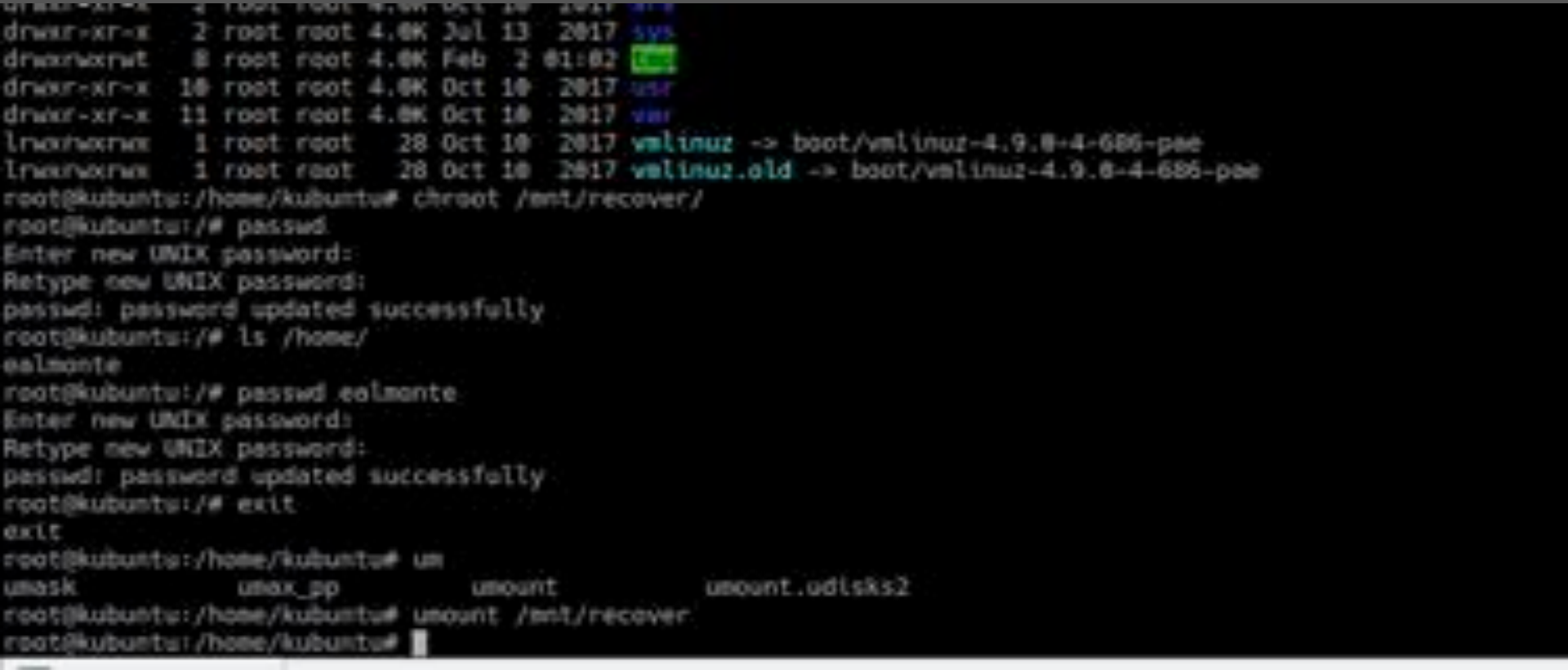
Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...



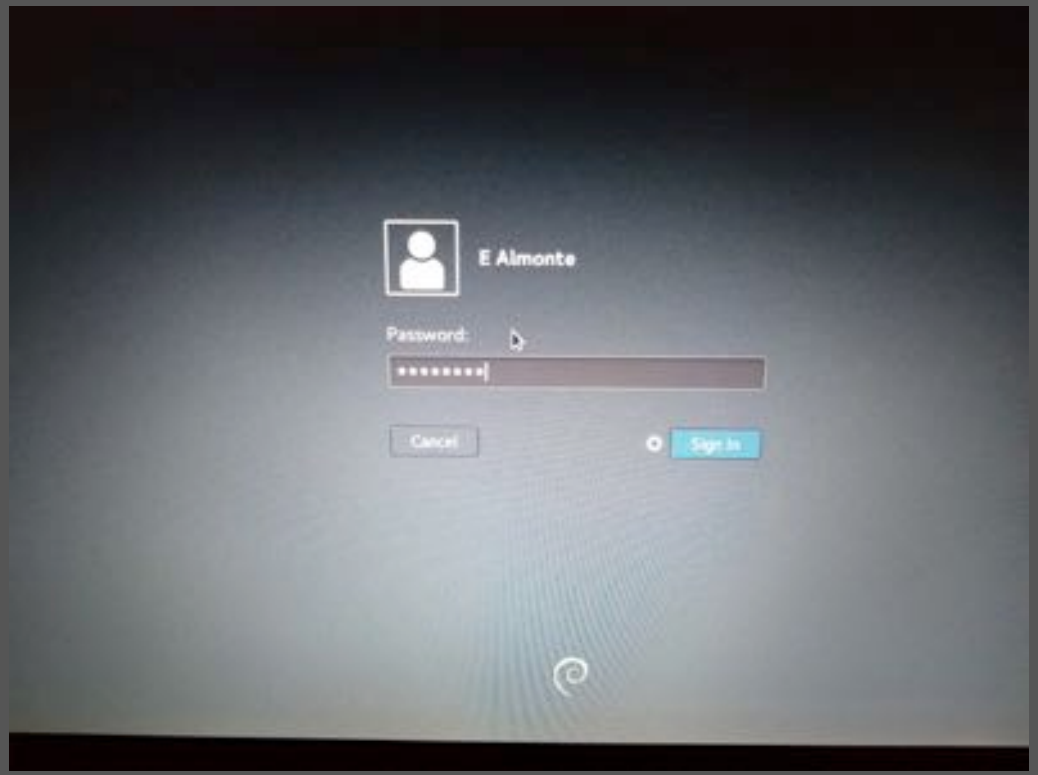
Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...



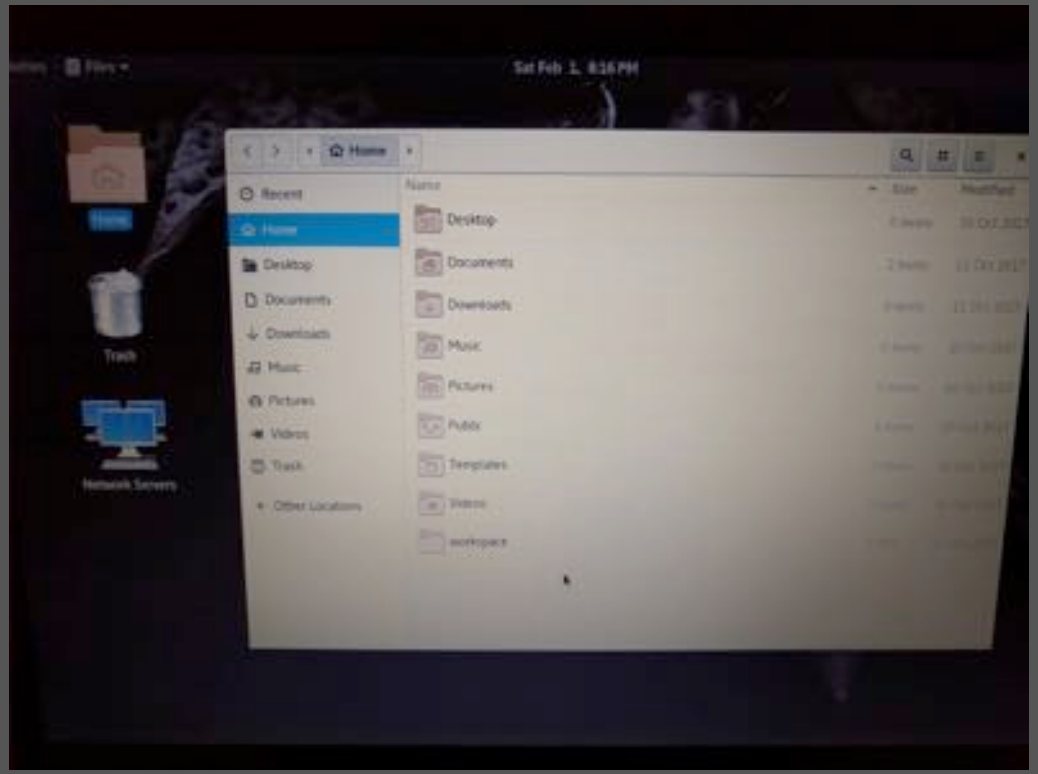
Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...



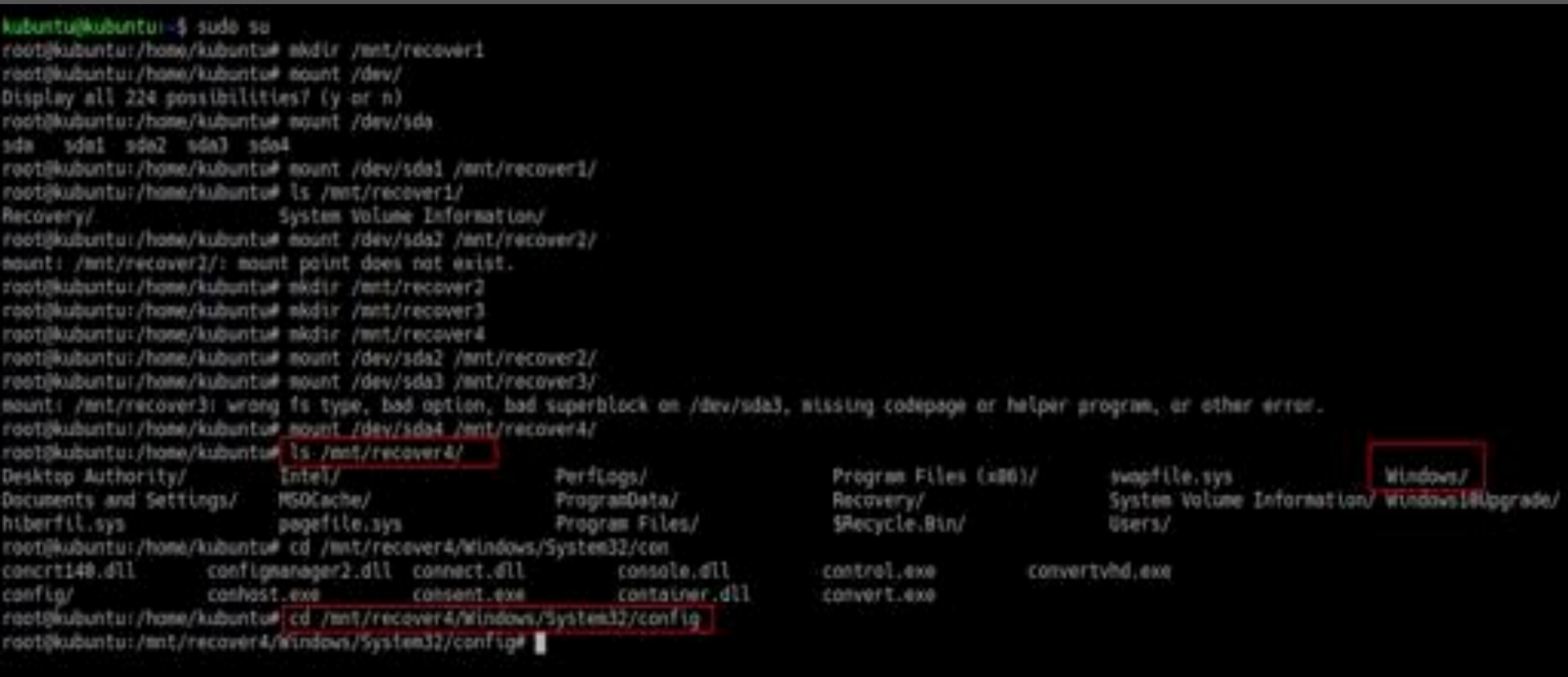
Safe Computing: the OS (linux)

- If you don't password-protect the bootloader and volume with encryption...



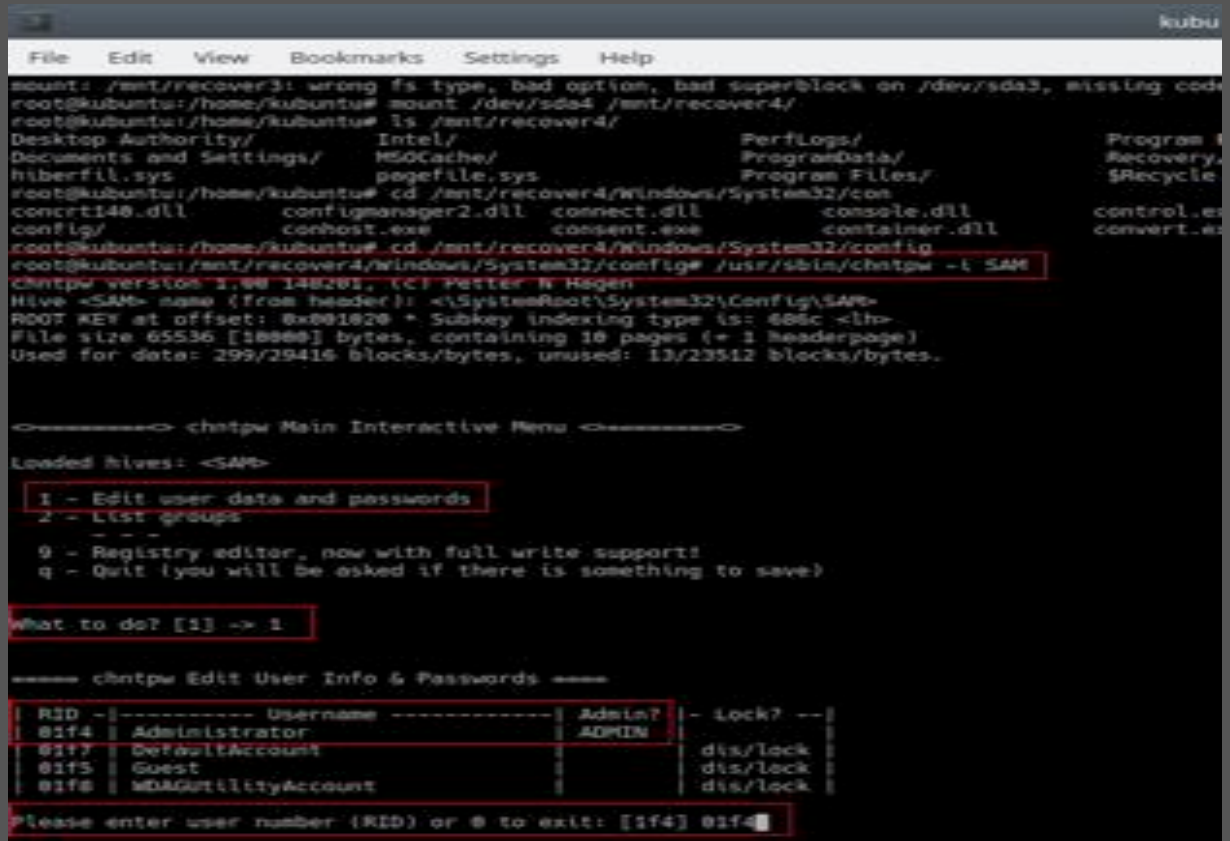
Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...



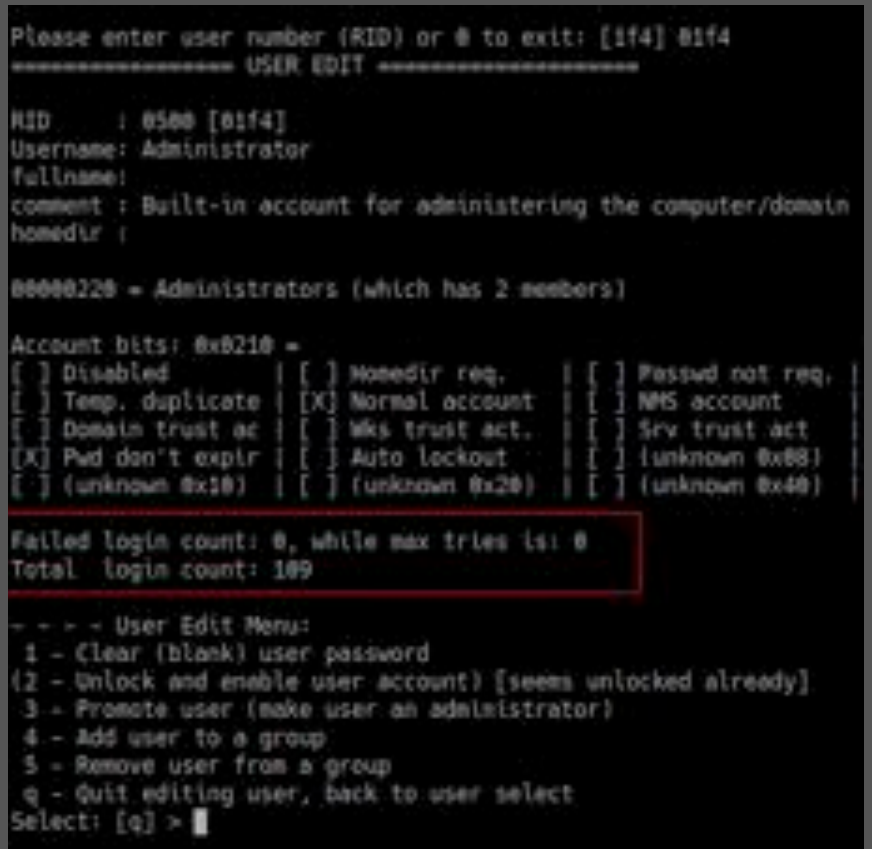
Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...



Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...



Safe Computing: the OS (windows)

- If you don't password-protect the bootloader and volume with encryption...

Safe Computing: the OS (windows)

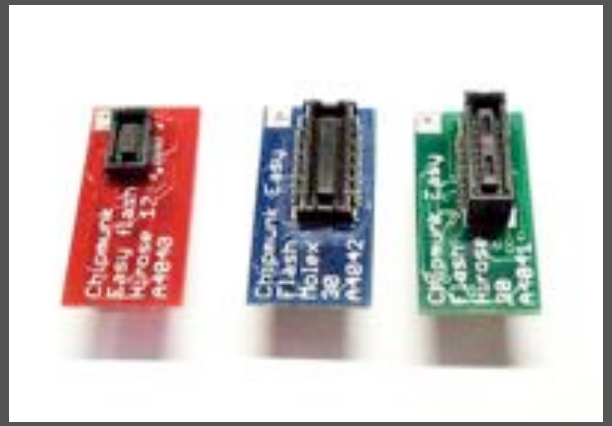
- If you don't password-protect the bootloader and volume with encryption...

> Exit & reboot, account password cleared.

Safe Computing: the OS (mac)

- If you do password-protect the bootloader but not the volume with encryption… Can you still haz protekshun?

CMIzapper



Safe Computing: the OS (mac)

- If you do password-protect the bootloader but not the volume with encryption… Can you still haz protekshun?

A4068 Keyboard for use with Medusa

The Medusa allows you to read the serial number from one Mac and write it to another Mac. When you replace the motherboard in a customer's Mac it is nice if the Mac keeps it's original serial number.

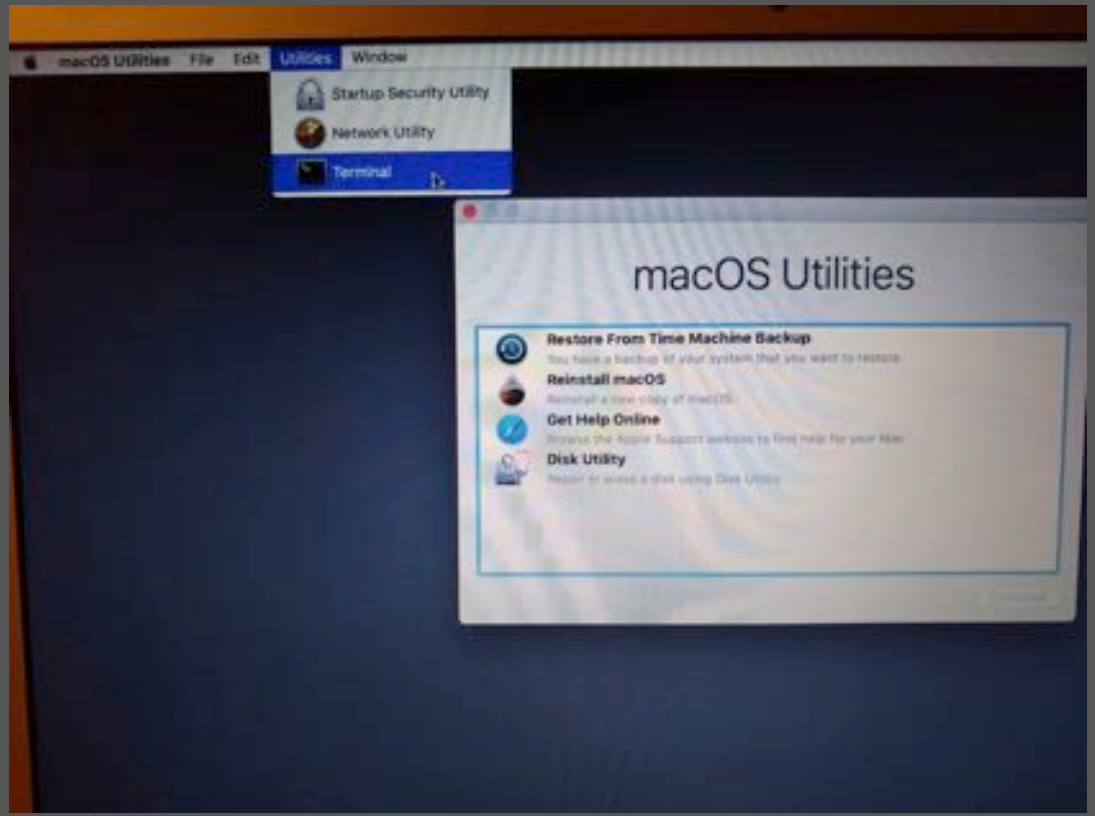
In case you can not read the original serial number from the old motherboard you can use this keyboard to edit the serial number to the one on the case of the Mac.

This keyboard allows you to edit the serial number stored in the Medusa so that you can write the modified number back to the Mac. Enter letters by holding the corresponding button down for a longer time.


```
eagr@eadebian:~$ nslookup www.icloud.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.icloud.com  canonical name = www-cdn.icloud.com.akadns.net.
www-cdn.icloud.com.akadns.net   canonical name = www.icloud.com.edgekey.net.
www.icloud.com.edgekey.net      canonical name = e4478.a.akamaiedge.net.
Name:   e4478.a.akamaiedge.net
Address: 23.54.185.223

eagr@eadebian:~$ nslookup www.apple.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.apple.com   canonical name = www.apple.com.edgekey.net.
www.apple.com.edgekey.net       canonical name = www.apple.com.edgekey.net.globalredir.akadns.net.
www.apple.com.edgekey.net.globalredir.akadns.net        canonical name = e6858.dsce9.akamaiedge.net.
Name:   e6858.dsce9.akamaiedge.net
Address: 184.25.177.104
Name:   e6858.dsce9.akamaiedge.net
Address: 2600:1408:20:193::1aca
Name:   e6858.dsce9.akamaiedge.net
Address: 2600:1408:20:194::1aca
Name:   e6858.dsce9.akamaiedge.net
Address: 2600:1408:20:183::1aca

eagr@eadebian:~$ nslookup apple.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   apple.com
Address: 17.178.96.59
Name:   apple.com
Address: 17.142.160.59
Name:   apple.com
Address: 17.172.224.47
```

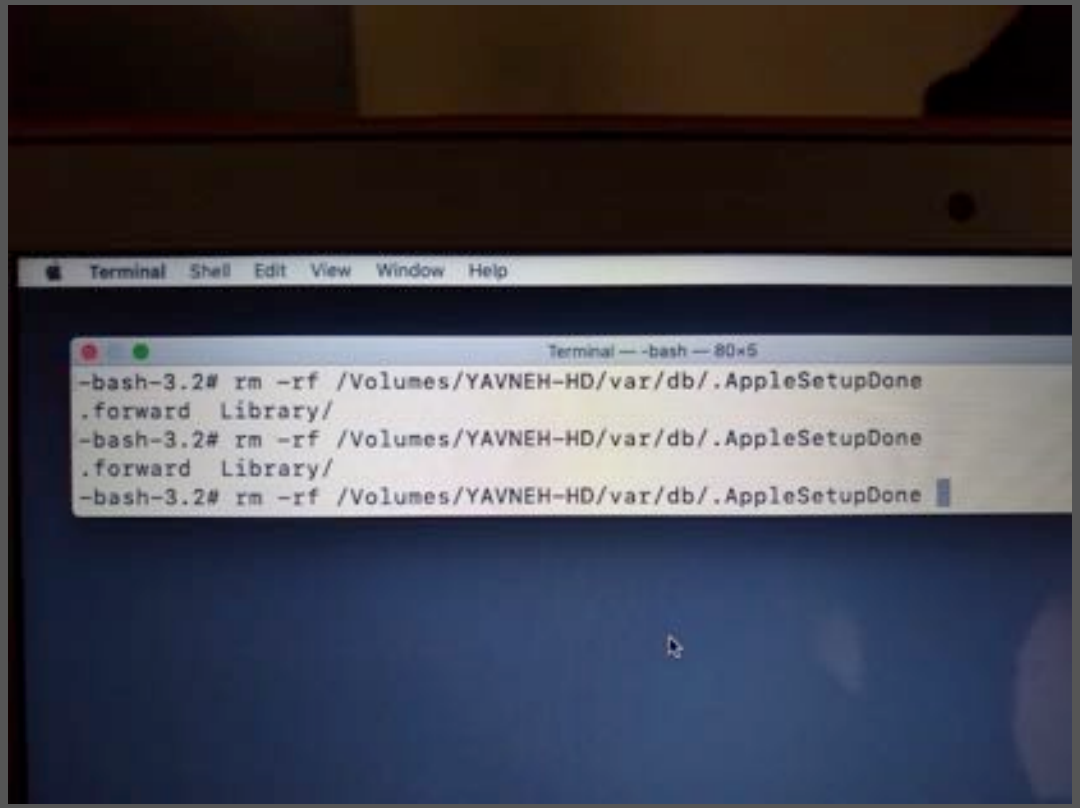
Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption…



Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption…



Safe Computing: the OS (mac)

- If you don't password-protect the bootloader and the volume with encryption…

Safe Computing: the OS (mac)

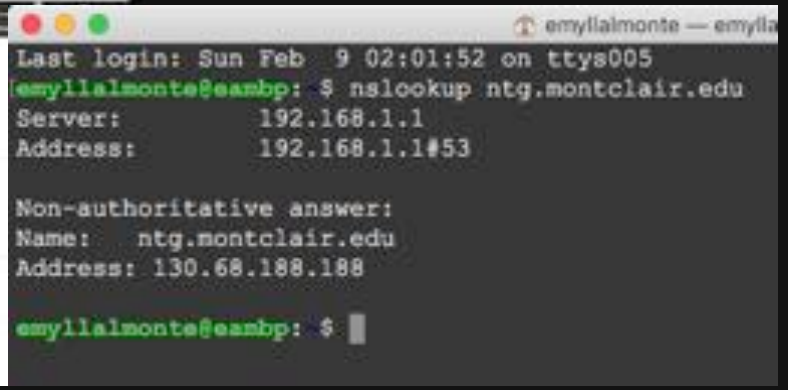
- If you don't password-protect the bootloader and the volume with encryption…

Safe Computing: the OS + Network + Apps

- Prepare the OS before letting anyone touch it, configure the system using best practices: (depends on the use case {government, banking, grandma})
  - Read Technical Implementation guides from NIST, CIS, etc
    - STIG (Security Technical Implementation Guides) Viewer
    - CIS (Center for Internet Security) Benchmarks

Safe Computing: the OS + Network + Apps

- Demo { shodan & montclair “authorization required” website }



Safe Computing: the OS + Network + Apps

```
if [ -f ~/docs.google.com/eapresentation == done ]
 then
  echo “The End”
  break
 else
   continue
fi
```

Q & A time..