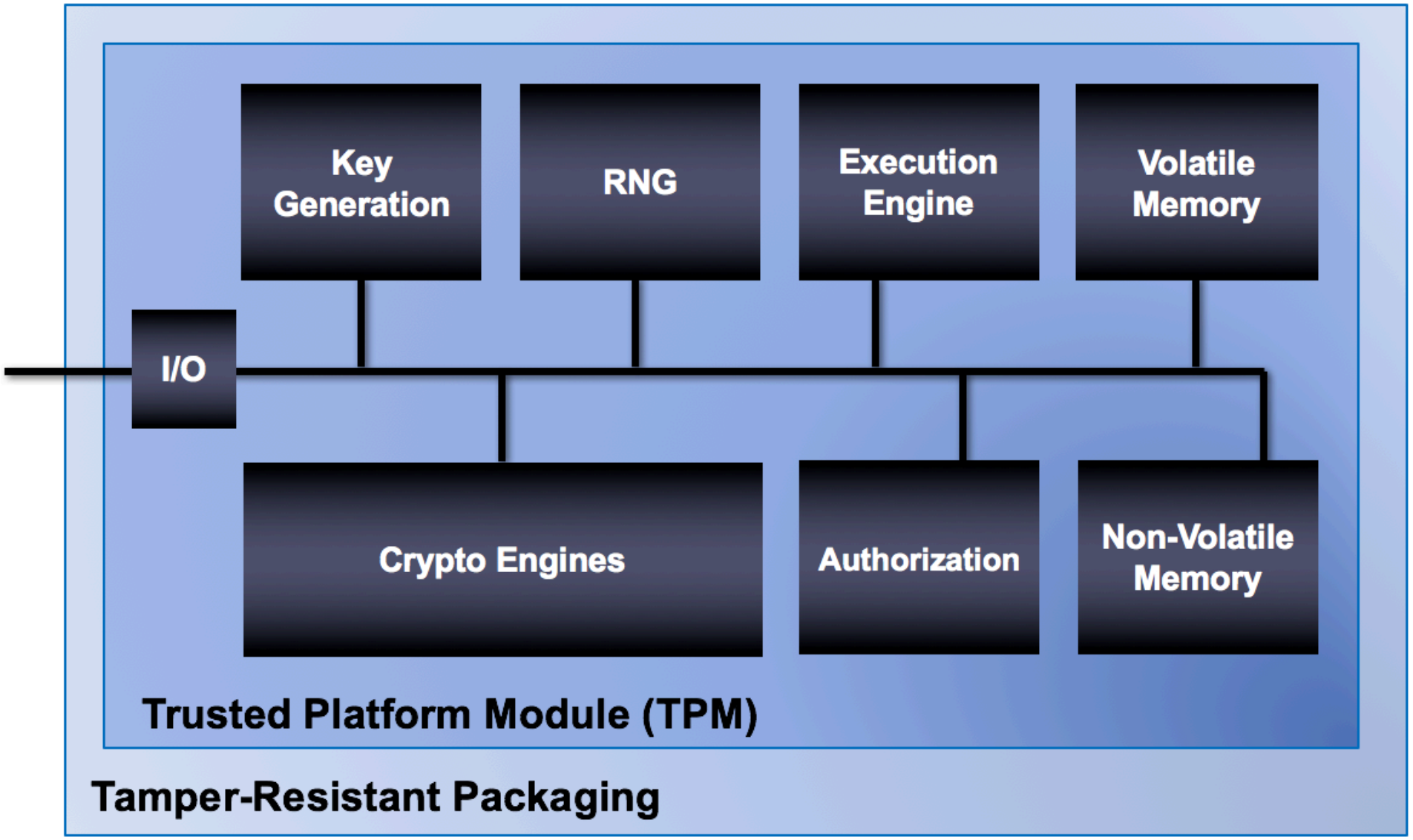
Lecture 28: Trusted Hardware

CS 5430

5/9/2018

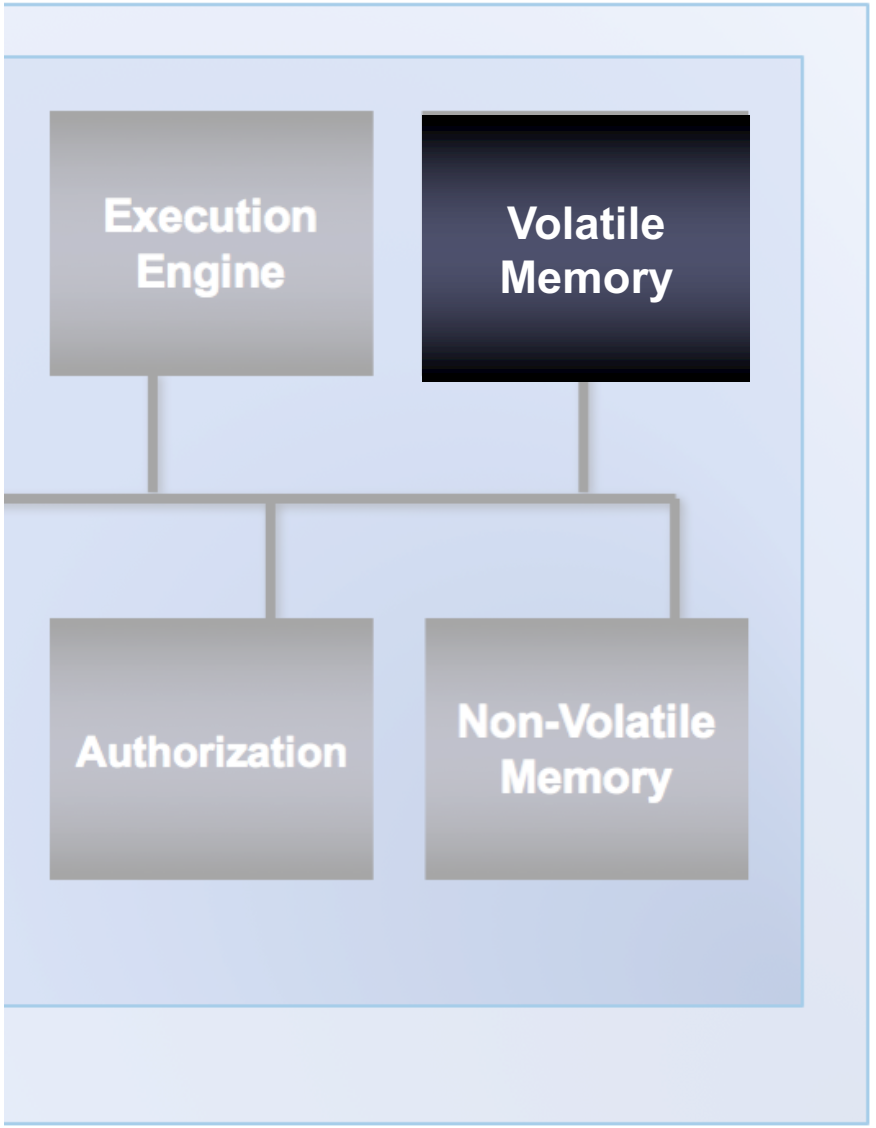
Trusted Platform Module (TPM)

What's in a TPM?



Volatile Memory

- PCR Banks
- In-use keys
- Sessions
- Etc.



Platform Configuration Register (PCR)

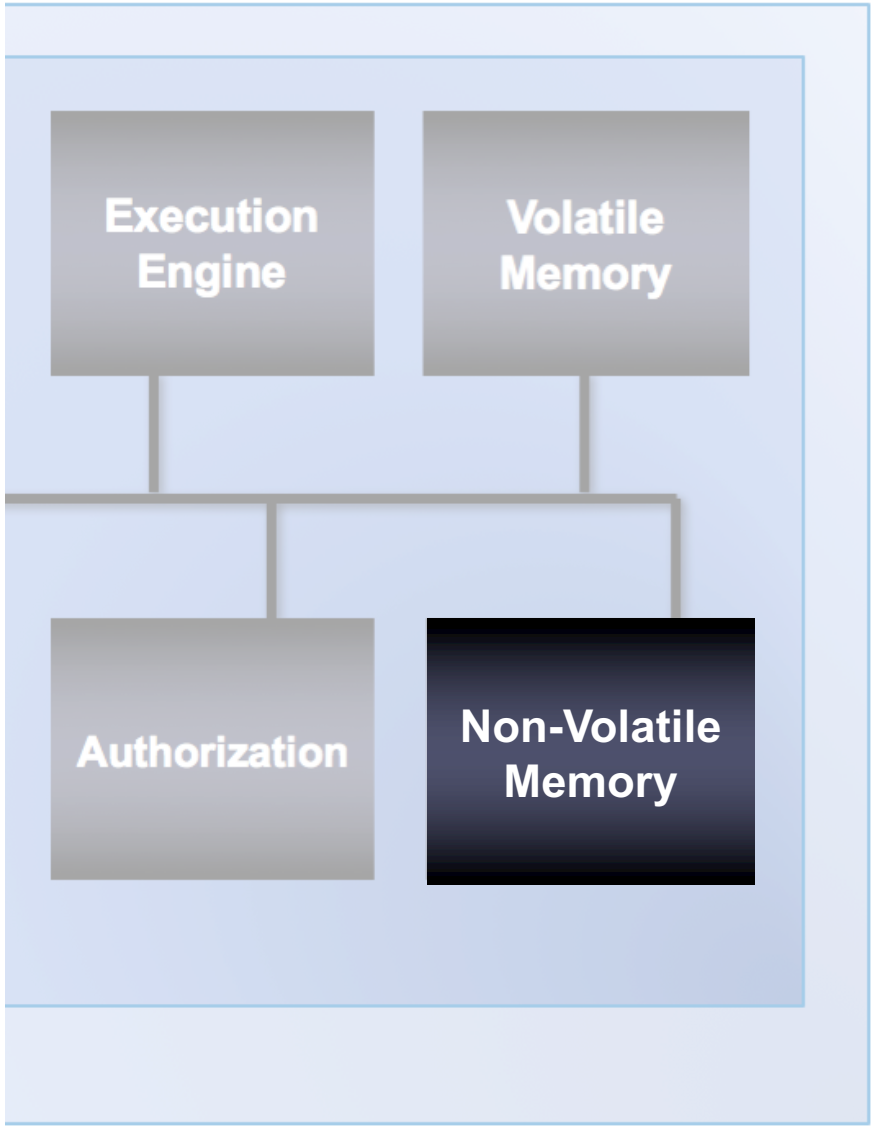
- Contain hashes of programs
- Modification: TPM2_Extend()

$$PCR_{new} = H(PCR_{old} || data_{new})$$

- Attestation: TPM2_Quote()

Non-Volatile Memory

- Platform Seed
- Endorsement Seed
- Storage Seed
- Monotonic Counters
- Etc.



Seeds used for attestation, etc

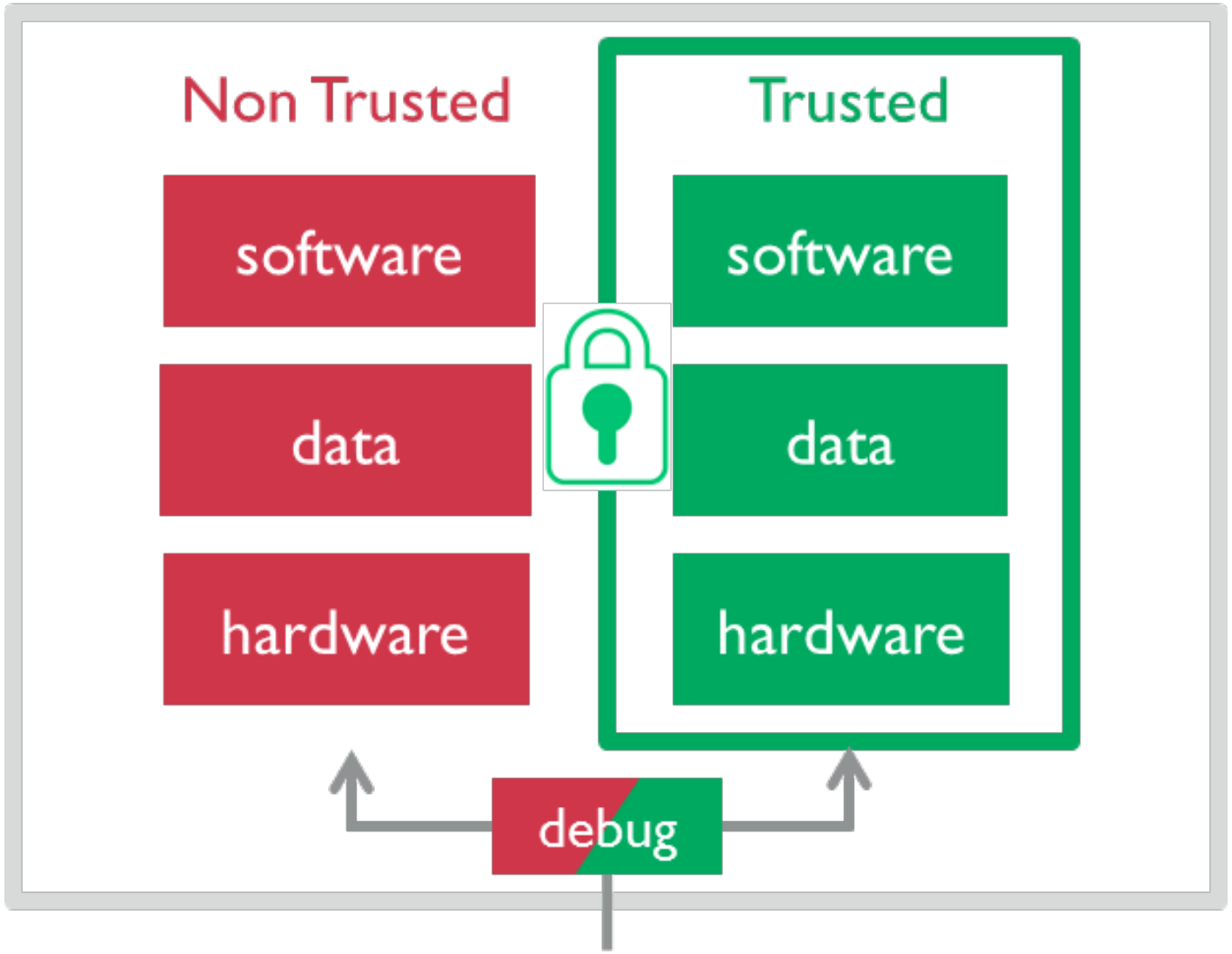
- Endorsement seed used to derive endorsement keys (EKs)
- Manufacturer attests validity of EKs
- EKs used to attest other TPM-derived values including
  - other keys: TPM2_Certify()
  - audit logs: TPM2_GetSessionAuditDigest()

Binding and Sealing

Bitlocker

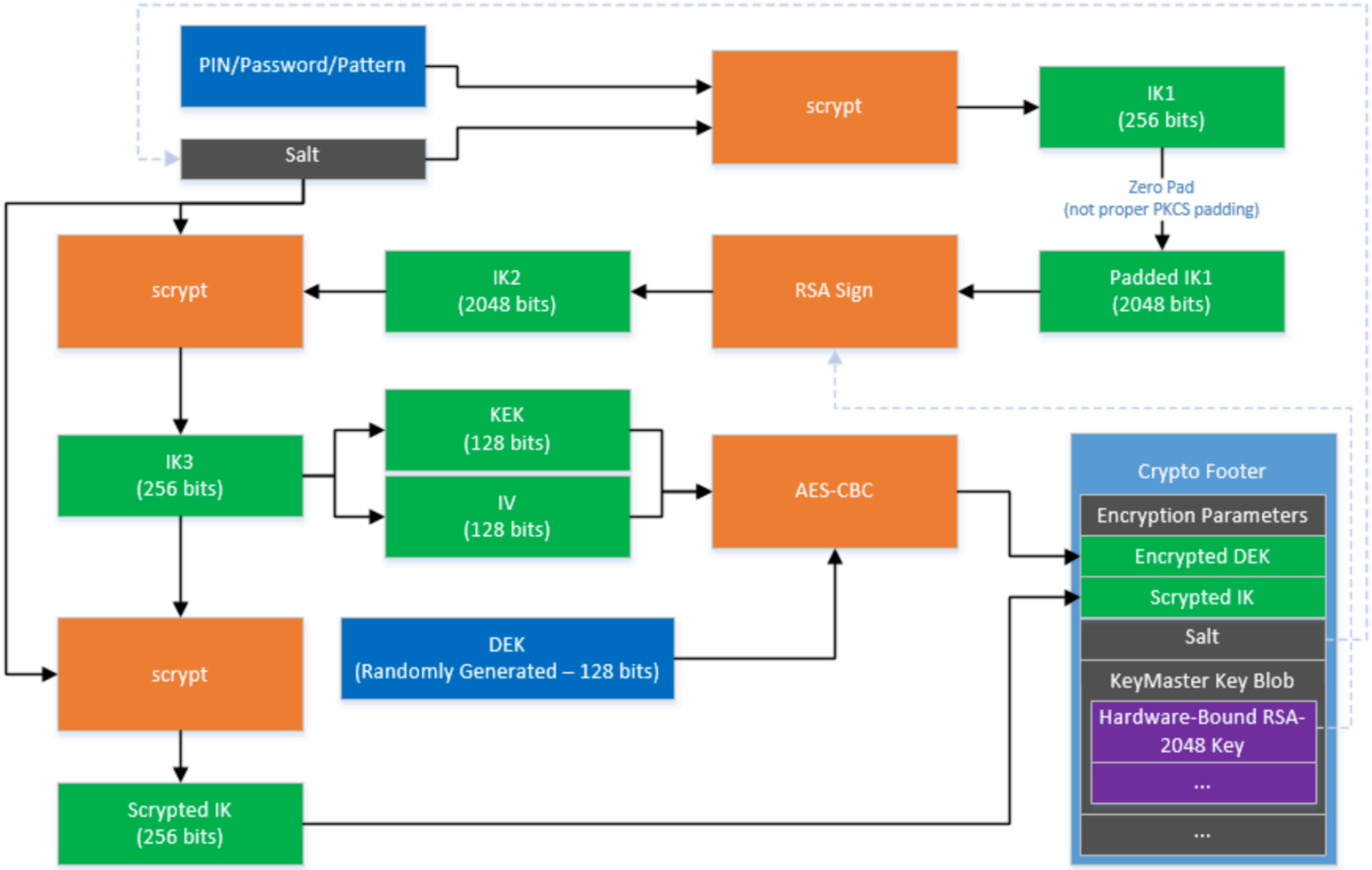

BitLocker
Enter the password to unlock this drive
Press the Insert key to see the password as you type.

ARM TrustZone



Android Full Disk Encryption

Android Full Disk Encryption

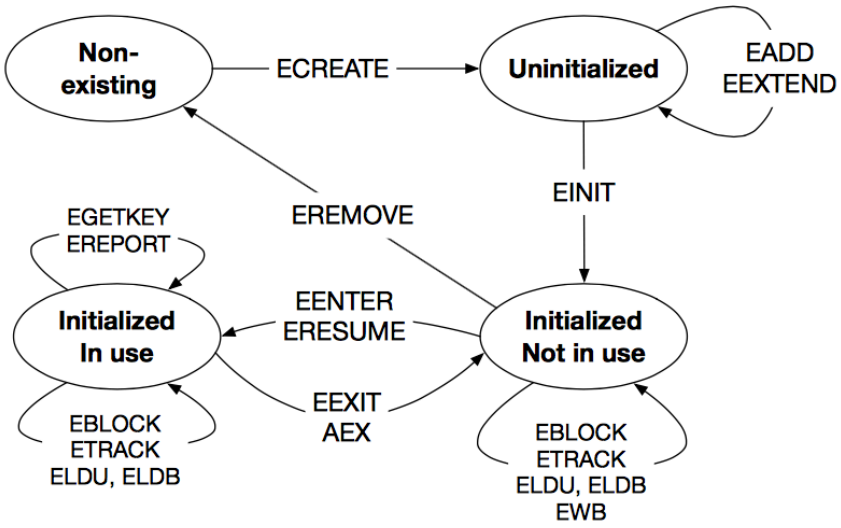


Android FDE's KDF

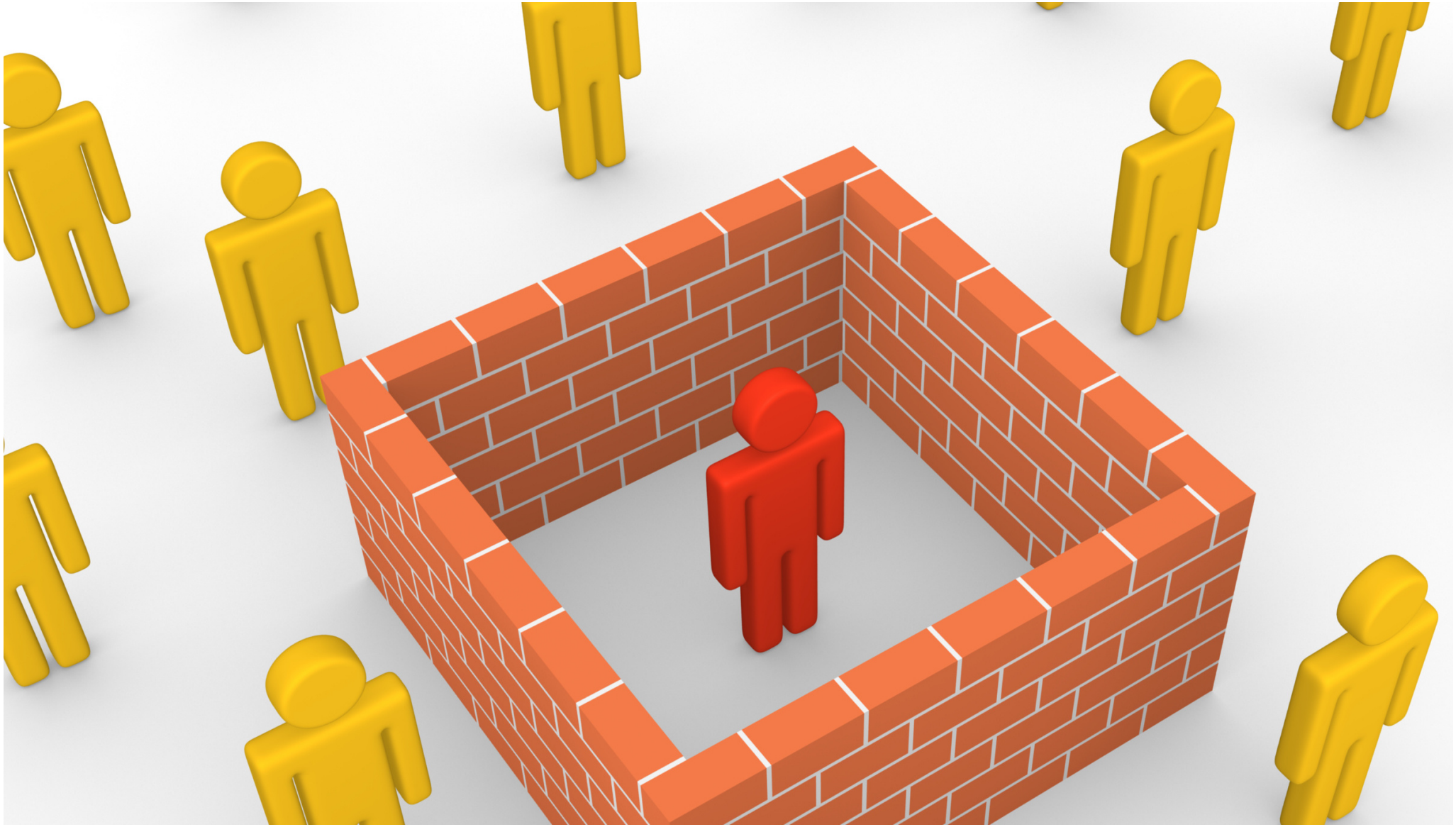
SGX

Enclaves

- Isolated computing environments
- Access hardware-derived keys
- Provide
- Provide local and remote attestation

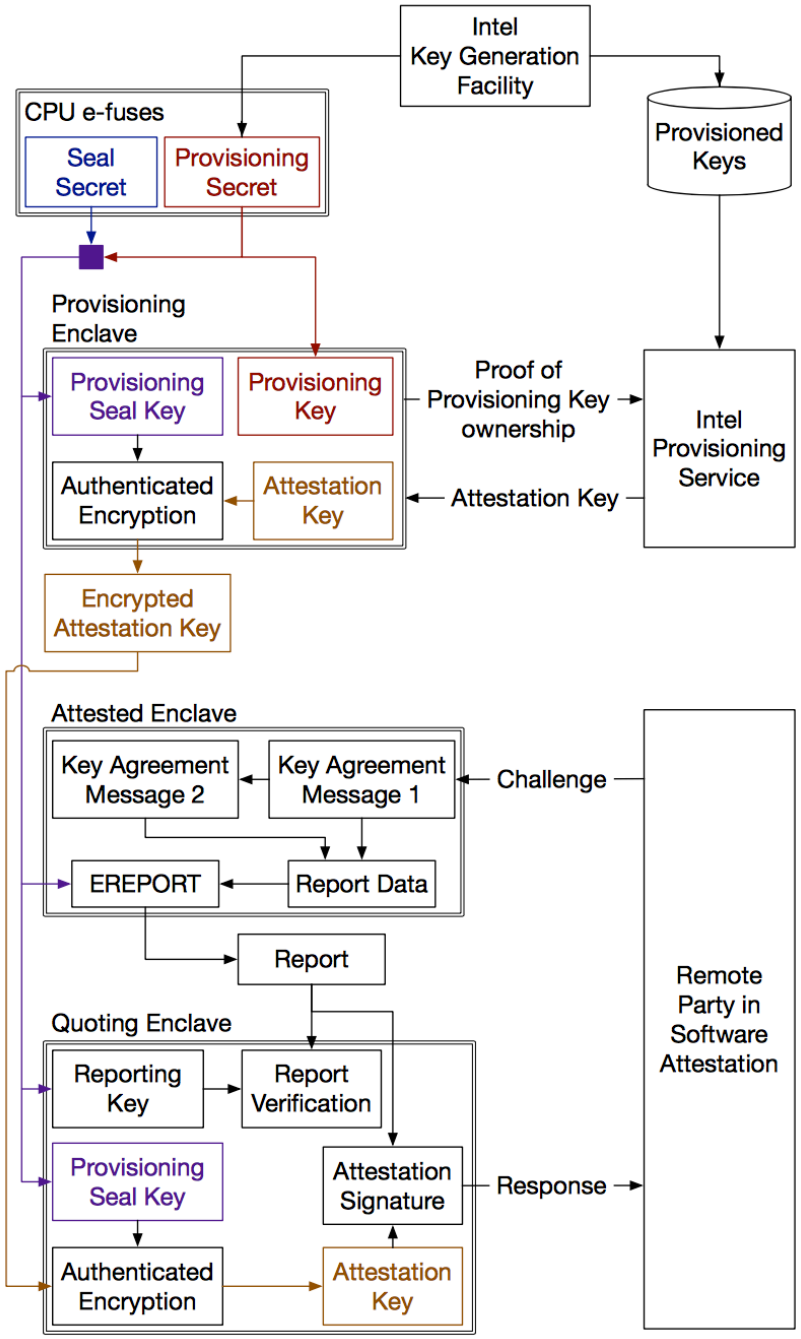


Isolation

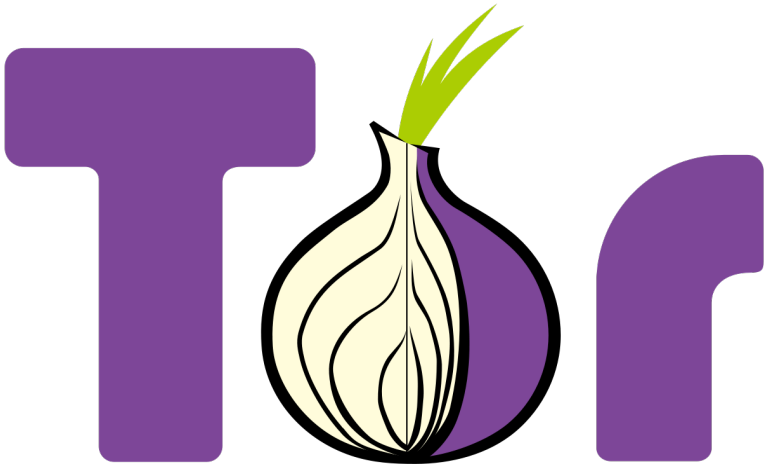


Sealing

Attestation



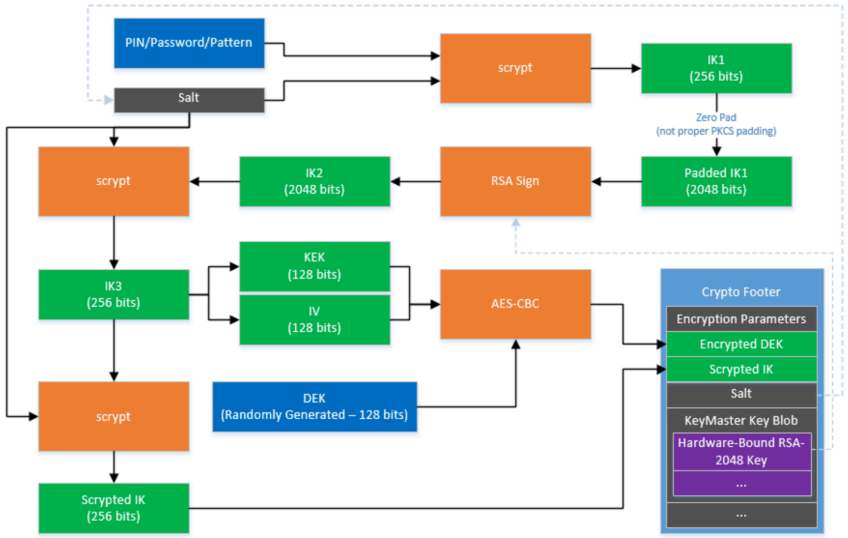
SGX in use



Microsoft®
Windows®

Vulnerabilities

Trustworthiness of Trusted Code



Android FDE's KDF

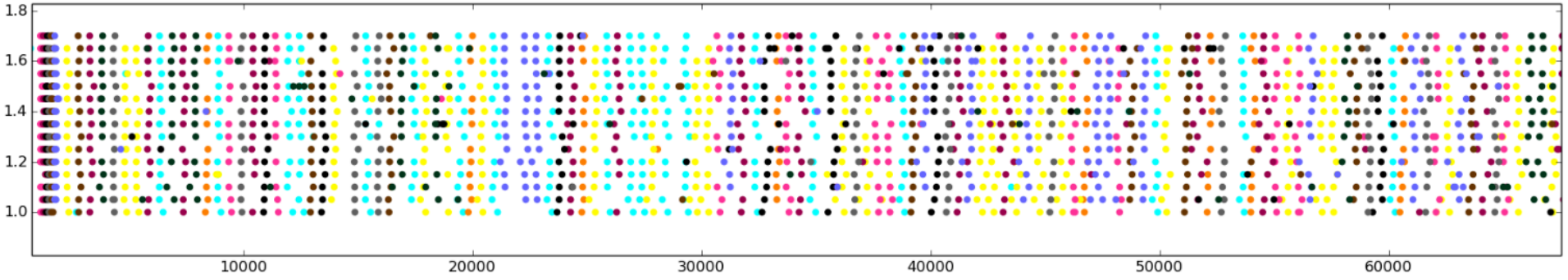
Side Channels

Algorithm 1 Fixed-window exponentiation

Input: $a, e, N \in \mathbb{N}$

Output: $x \leftarrow a^e \mod N$

1: Precompute $g[i] \leftarrow a^i$ for $1 \leq i \leq 2^k$
2: Let $e = (e_j, e_{j-1}, \ldots, e_1, e_0)$ be the base 2^k representation of the exponent e with $e_j \neq 0$
3: Initialize $x \leftarrow e_j$
4: **for** $i \leftarrow j-1$ **down to** 0 **do**
5: $\quad x \leftarrow x^{2^k} \mod N$
6: $\quad$ **if** $e_i \neq 0$ **then**
7: $\quad\quad x \leftarrow g[e_i] \cdot x \mod N$
8: $\quad$ **end if**
9: **end for**



Comparison of Hardware Solutions

Adversary	Attack	TPM	TrustZone	SGX
OS	direct probing	n/a (OS measured)	access checks on TLB misses	Access checks on TLB misses
OS	page faults	n/a (OS measured)	secure page tables	X
OS	cache timing	n/a (OS measured)	X	X
Another container	direct probing	n/a	n/a (secure world trusted)	access checks on TLB misses
Another container	cache timing	n/a	n/a (secure world trusted)	X
Peripheral	DMA	X	bus bounces accesses	IOMMU bounces DMA
Physical attacker	Physical DRAM	X	n/a (on-chip SRAM only)	memory encryption

So where are we?

The Bigger Picture

Attacks
are perpetrated by
threats
that inflict
harm
by exploiting
vulnerabilities
which are controlled by
countermeasures.

Threats

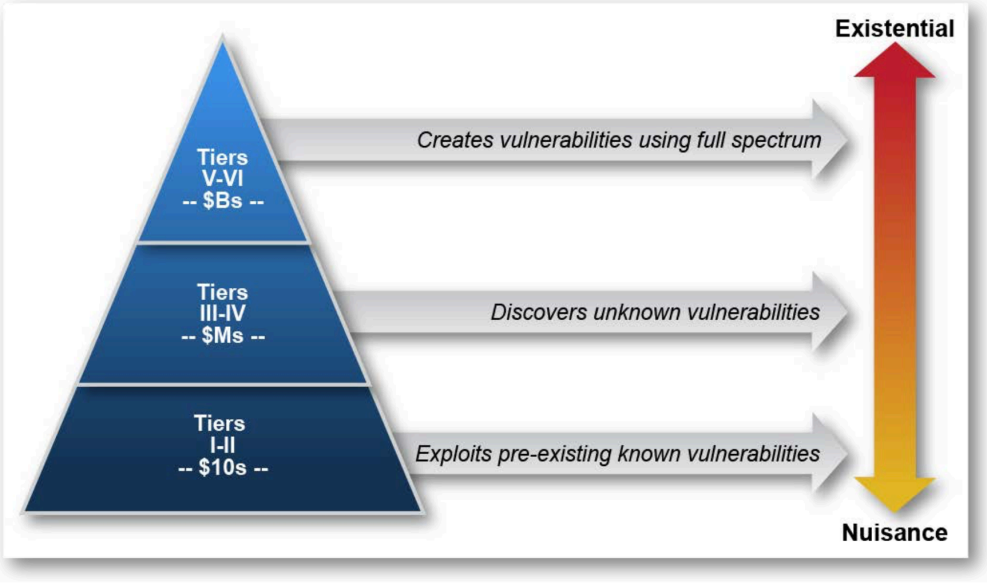
A principal that has potential to cause harm to assets

- Adversary or attacker: a human threat, motivated and capable
- Sometimes humans aren't malicious: accidents happen
- Sometimes non-humans cause harm: floods, earthquakes, power outage, hardware failure

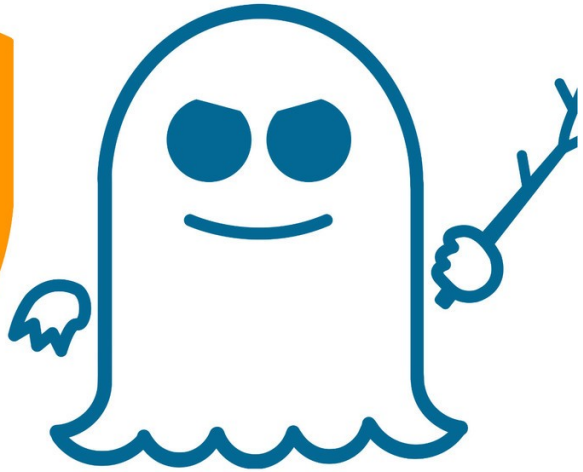
Threats

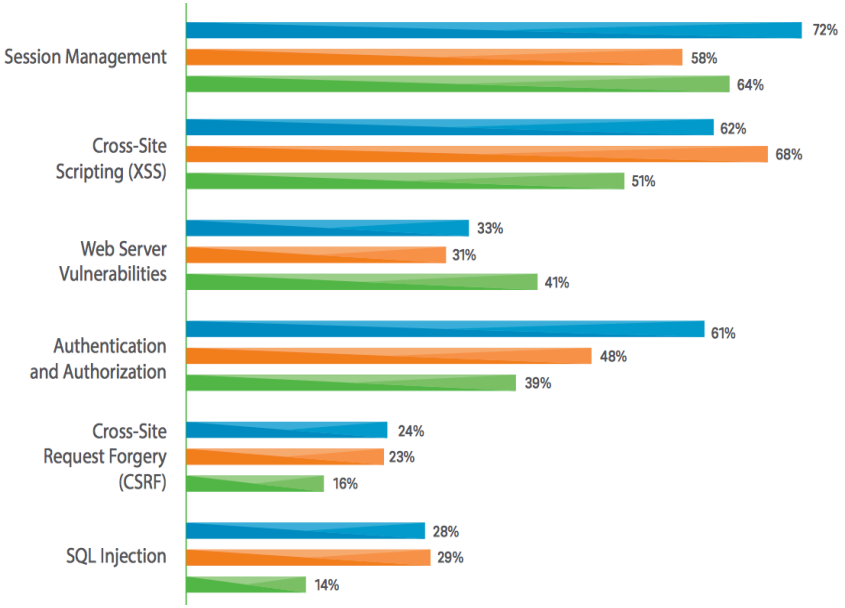

I KILLED A BLACK SNAKE
WHY U NOT HAPPY


未来日記
みらいにっき
えすのサカエ
1
Kadokawa Comics A

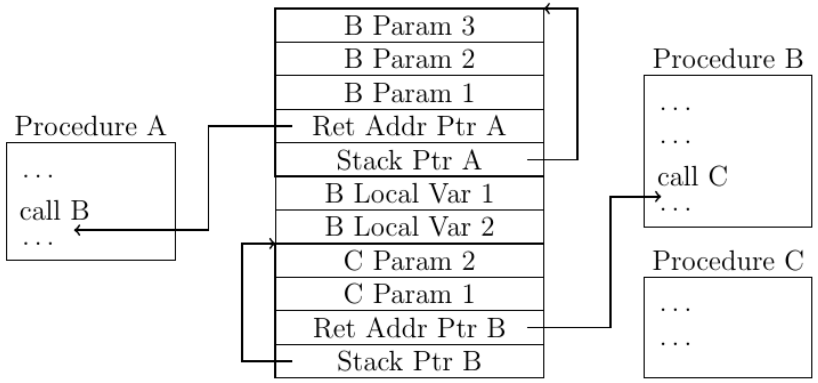

Existential
Tiers V-VI -- $Bs --
Creates vulnerabilities using full spectrum
Tiers III-IV -- $Ms --
Discovers unknown vulnerabilities
Tiers I-II -- $10s --
Exploits pre-existing known vulnerabilities
Nuisance

Vulnerabilities

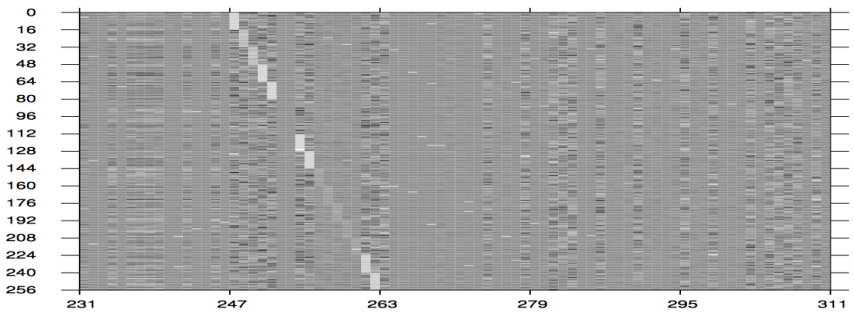


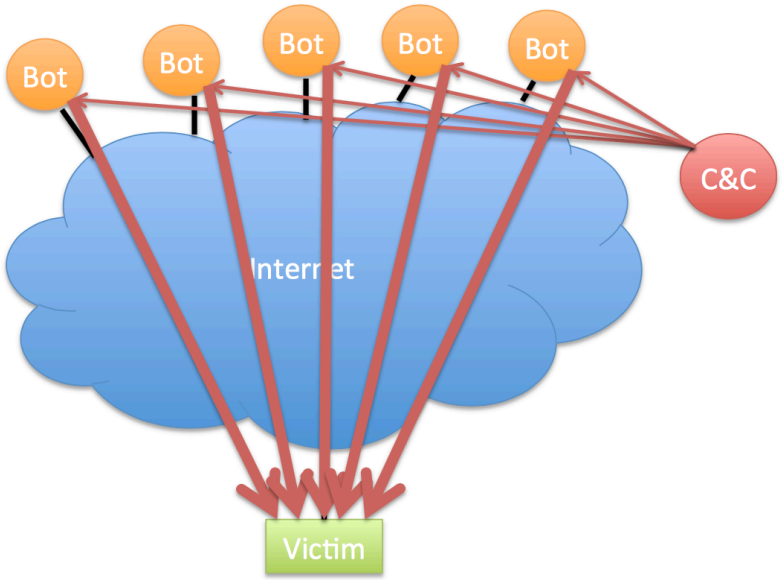


Attacks


Procedure A
...
call B
...
B Param 3
B Param 2
B Param 1
Ret Addr Ptr A
Stack Ptr A
B Local Var 1
B Local Var 2
C Param 2
C Param 1
Ret Addr Ptr B
Stack Ptr B
Procedure B
...
...
call C
...
Procedure C
...
...


Return-Oriented Programming
is A lot like a ransom note, but instead of cutting cut Letters from Magazines, you are cutting out instructions from .text segments

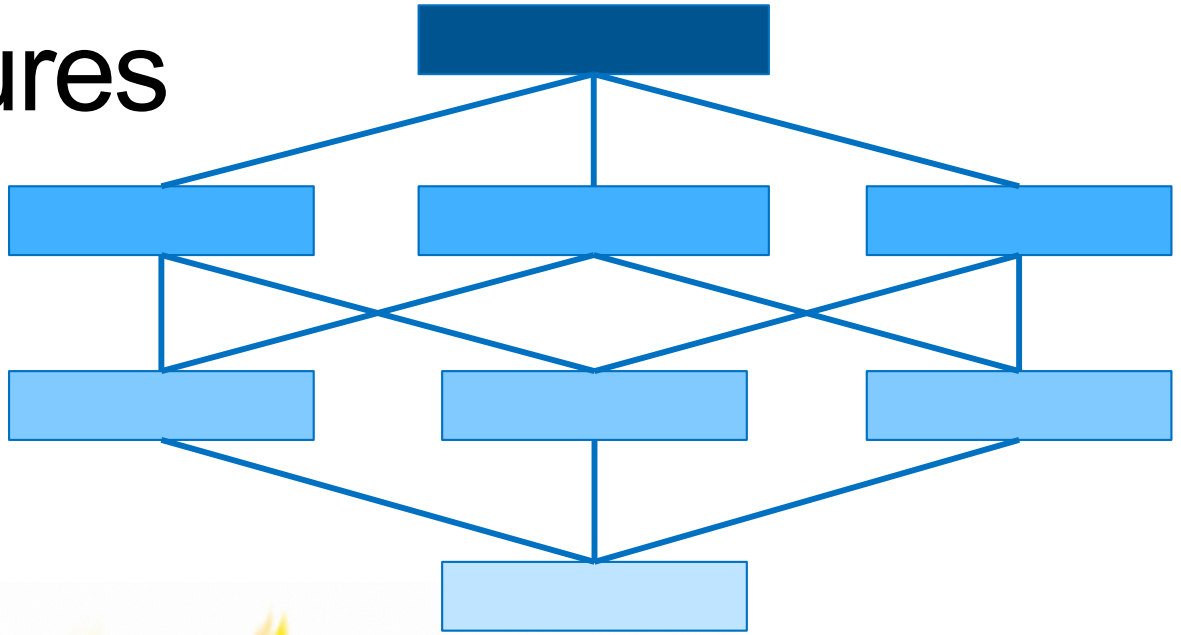

0
16
32
48
64
80
96
112
128
144
160
176
192
208
224
240
256
231
247
263
279
295
311

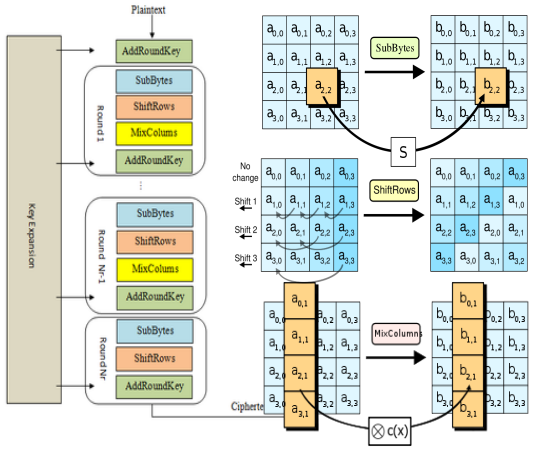

Bot
Bot
Bot
Bot
Bot
C&C
Internet
Victim

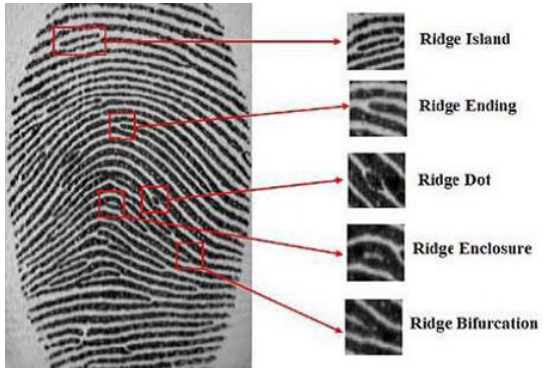
Functional Goals -> Harms -> Security Goals

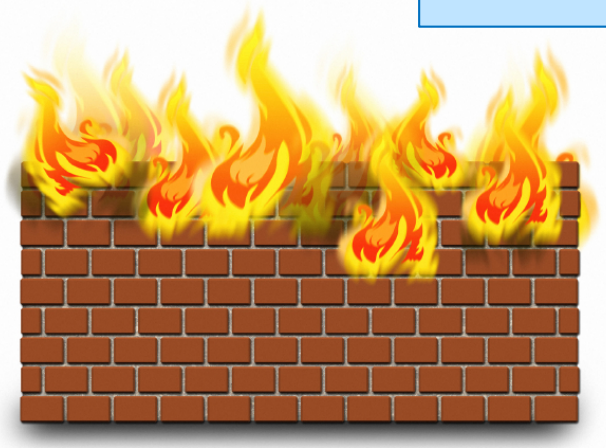
Confidentiality
Integrity
Availability

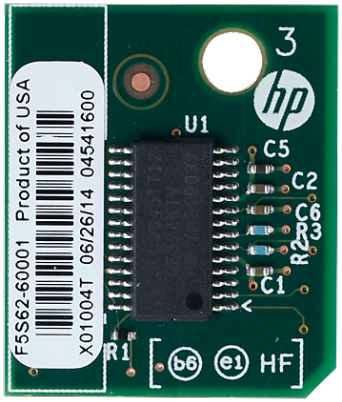
Countermeasures



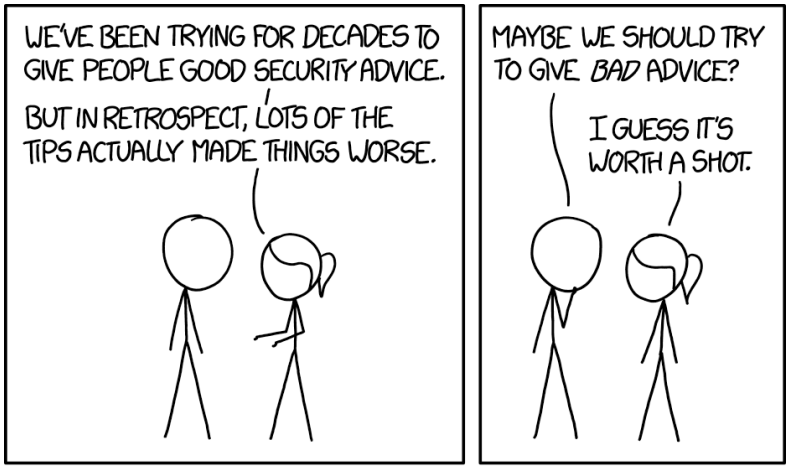








And now…



SECURITY TIPS

(PRINT OUT THIS LIST AND KEEP IT IN YOUR BANK SAFE DEPOSIT BOX.)

- DON'T CLICK LINKS TO WEBSITES
- USE PRIME NUMBERS IN YOUR PASSWORD
- CHANGE YOUR PASSWORD MANAGER MONTHLY
- HOLD YOUR BREATH WHILE CROSSING THE BORDER
- INSTALL A SECURE FONT
- USE A 2-FACTOR SMOKE DETECTOR
- CHANGE YOUR MAIDEN NAME REGULARLY
- PUT STRANGE USB DRIVES IN A BAG OF RICE OVERNIGHT
- USE SPECIAL CHARACTERS LIKE & AND %
- ONLY READ CONTENT PUBLISHED THROUGH TOR.COM
- USE A BURNER'S PHONE
- GET AN SSL CERTIFICATE AND STORE IT IN A SAFE PLACE
- IF A BORDER GUARD ASKS TO EXAMINE YOUR LAPTOP, YOU HAVE A LEGAL RIGHT TO CHALLENGE THEM TO A CHESS GAME FOR YOUR SOUL.