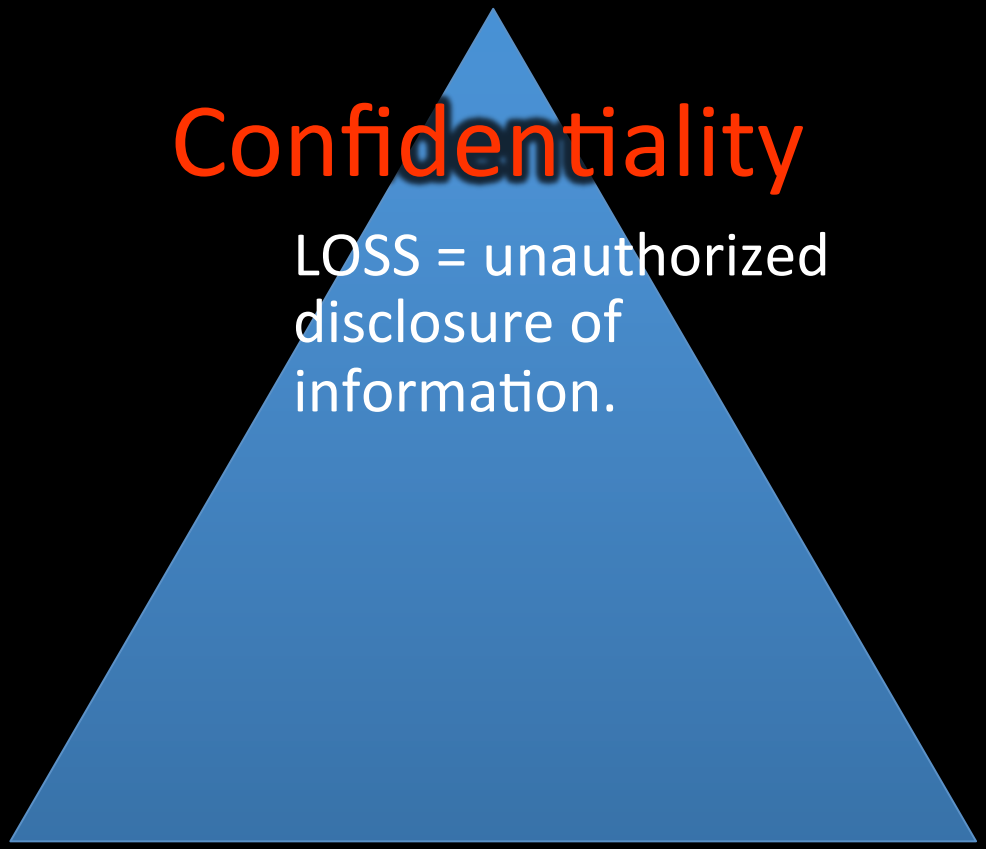
Protecting Mobile Apps and security in the context of Bring Your Own Device

Shane Williams

Alex Batlin

THE BASICS AND BACKGROUND

Basics – Security is the same

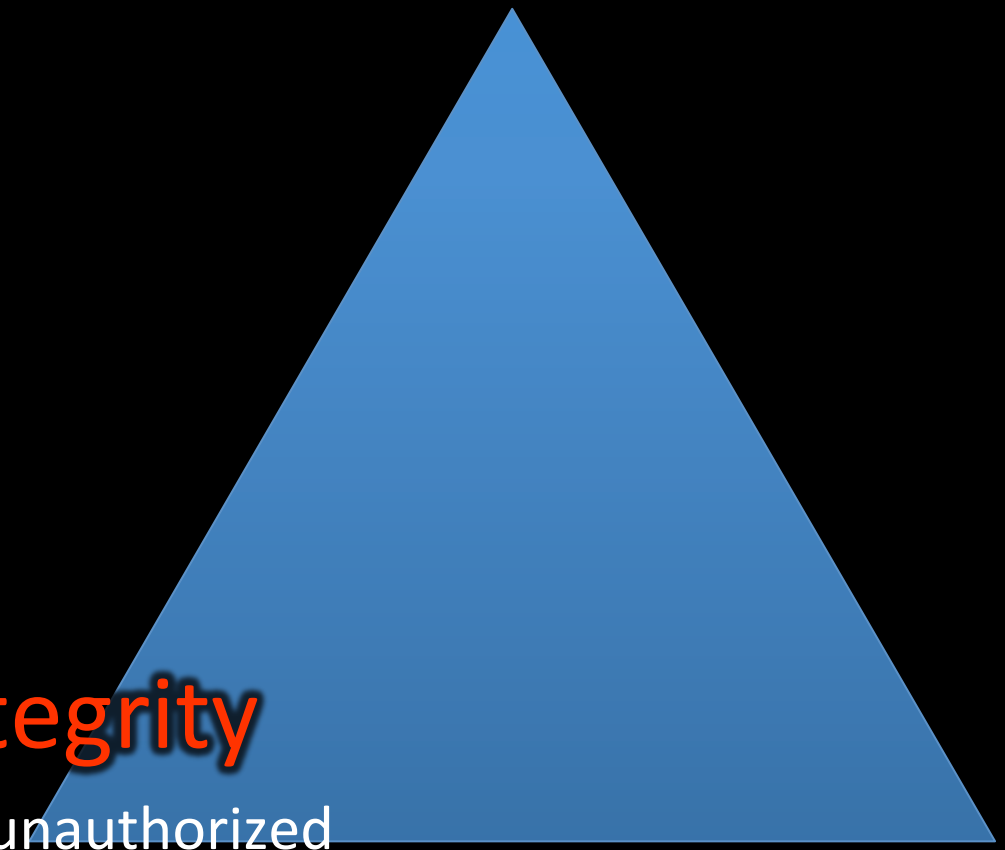


Basics – Security is the same

Availability

LOSS = disruption of access to or use of information or an information system.

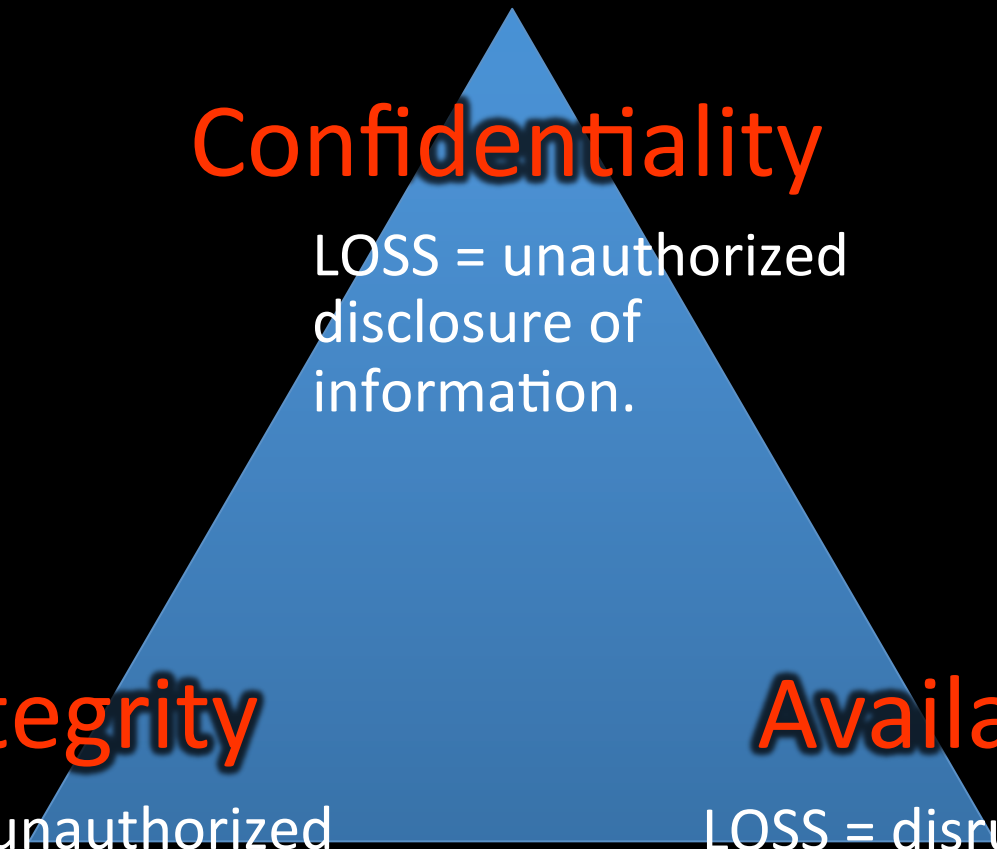
Basics – Security is the same



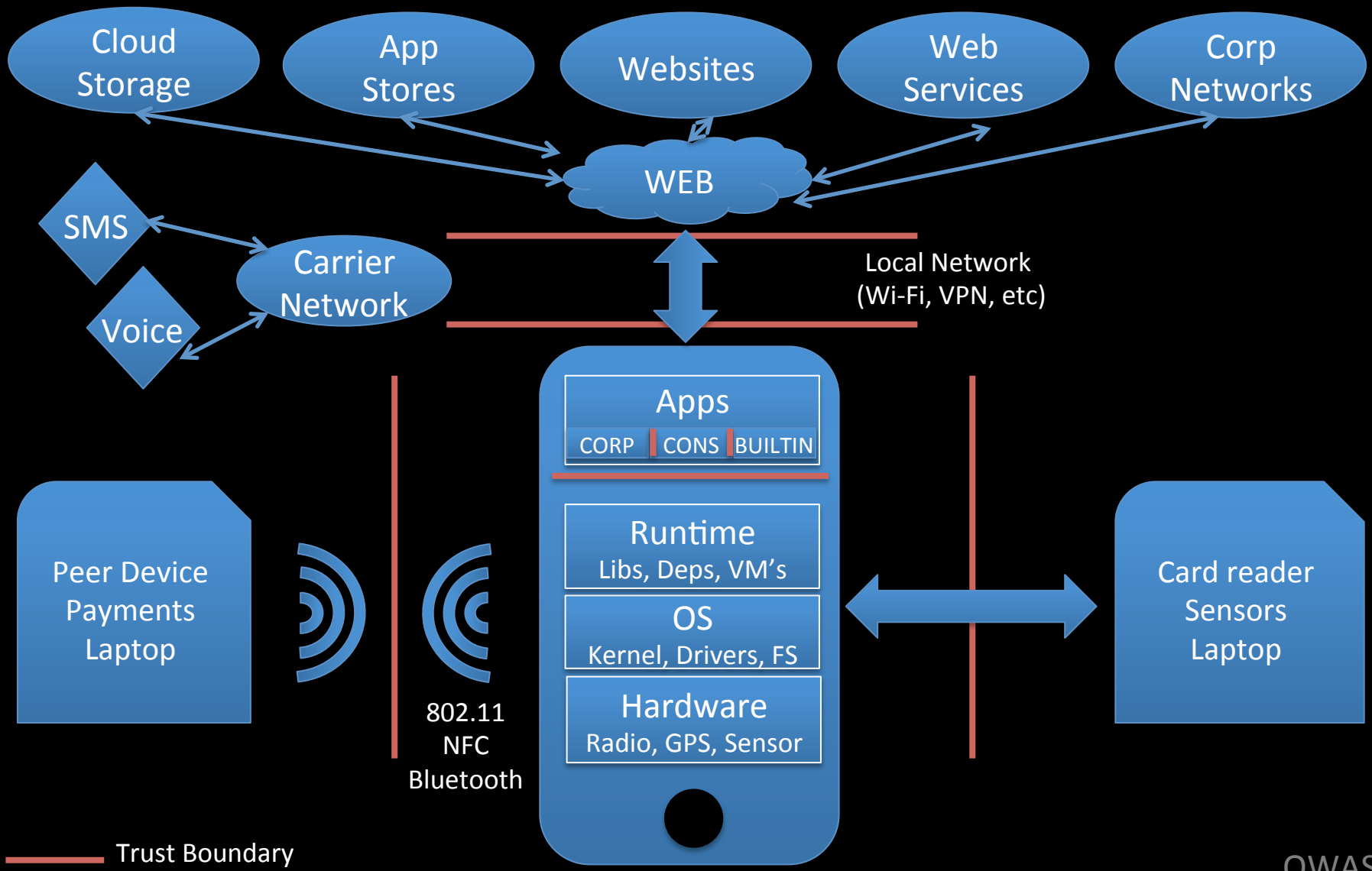
Integrity

LOSS = unauthorized modification or destruction of information

Basics – Security is the same



Mobile Threat Model



Threat paths

Threat Agents

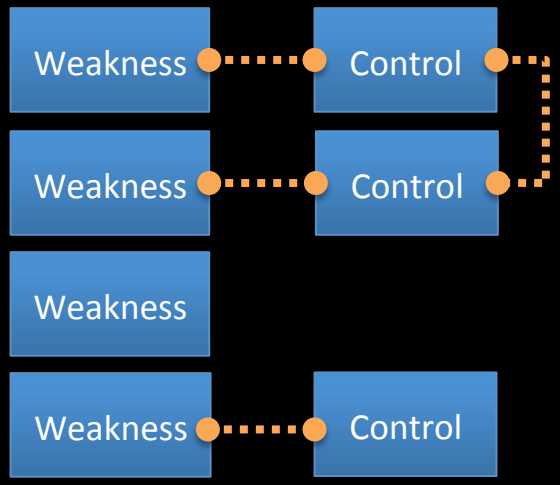
Attack Vectors

Security Weaknesses (Vulnerabilities)

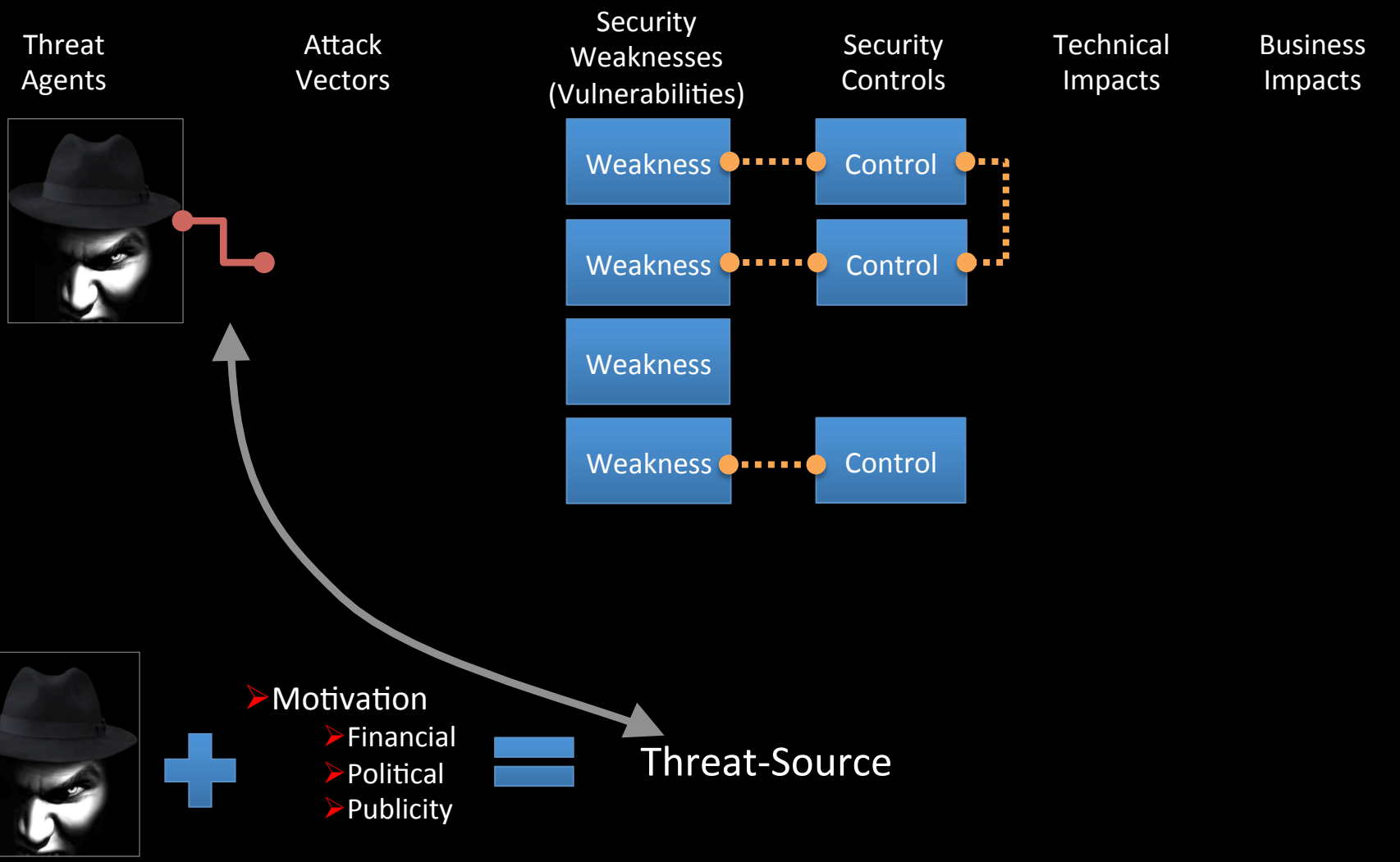
Security Controls

Technical Impacts

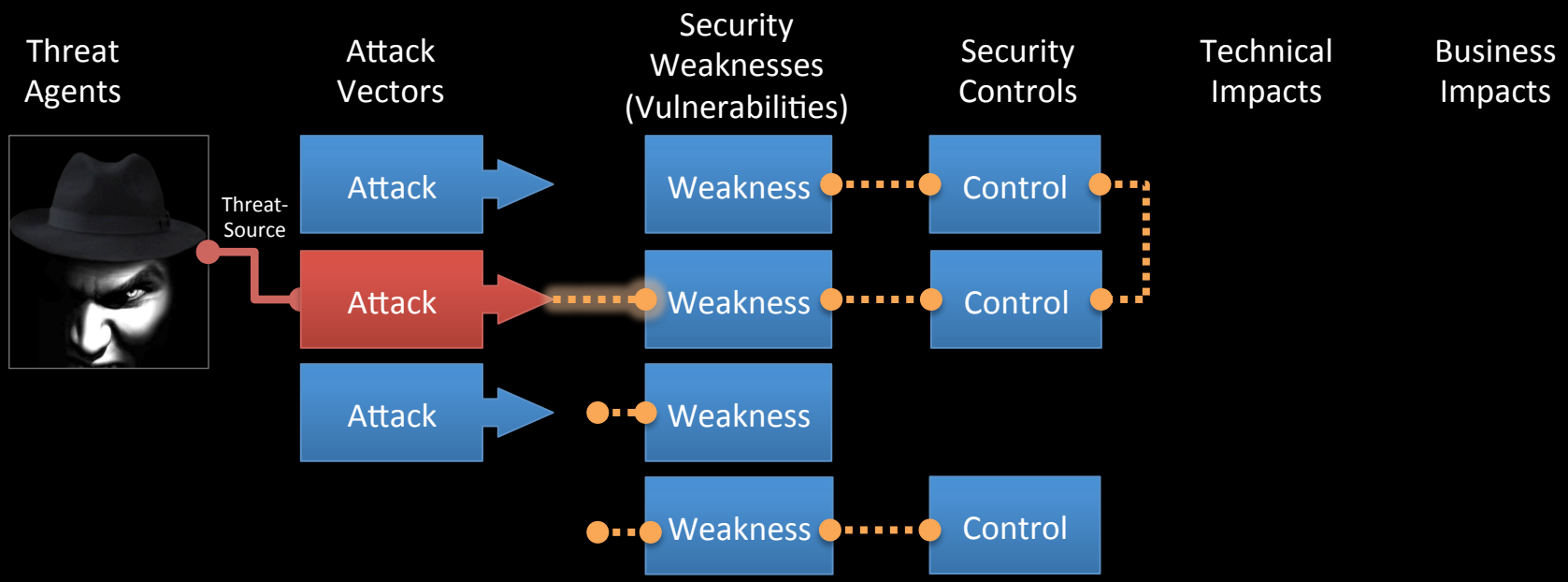
Business Impacts



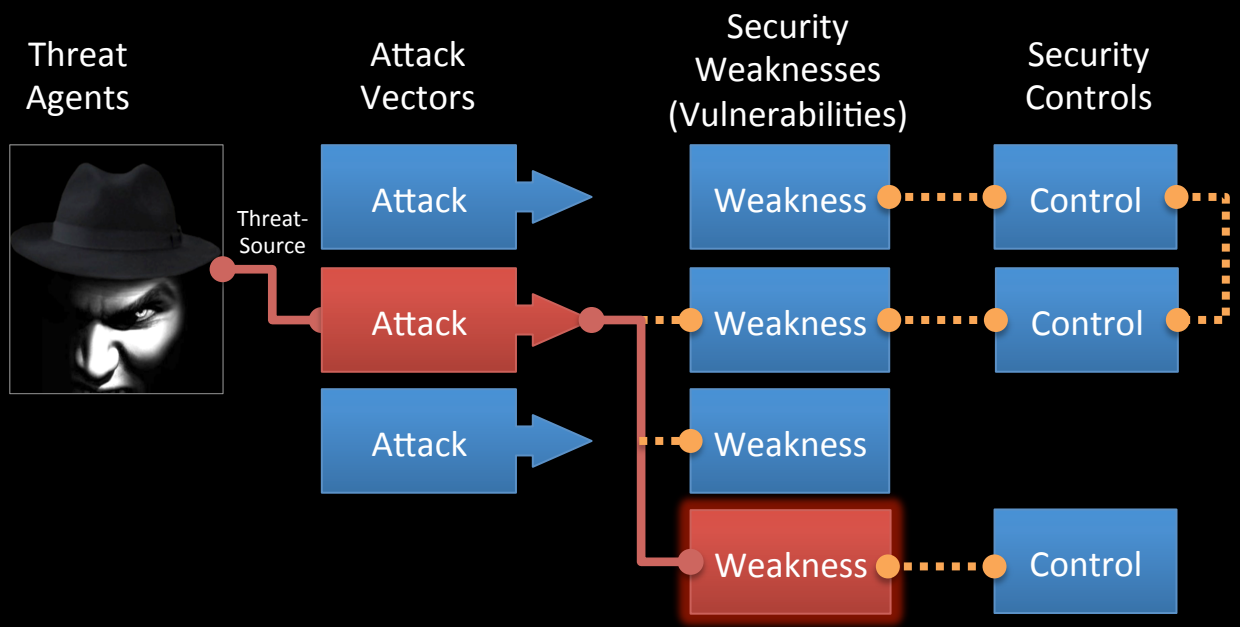
Threat paths



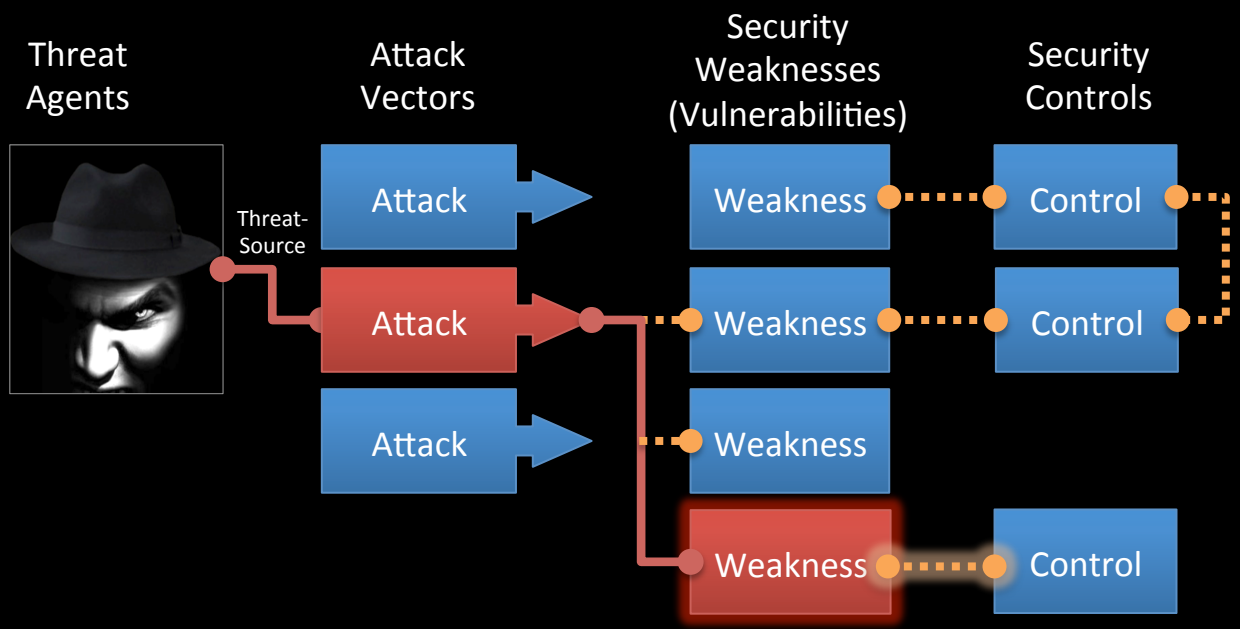
Threat paths



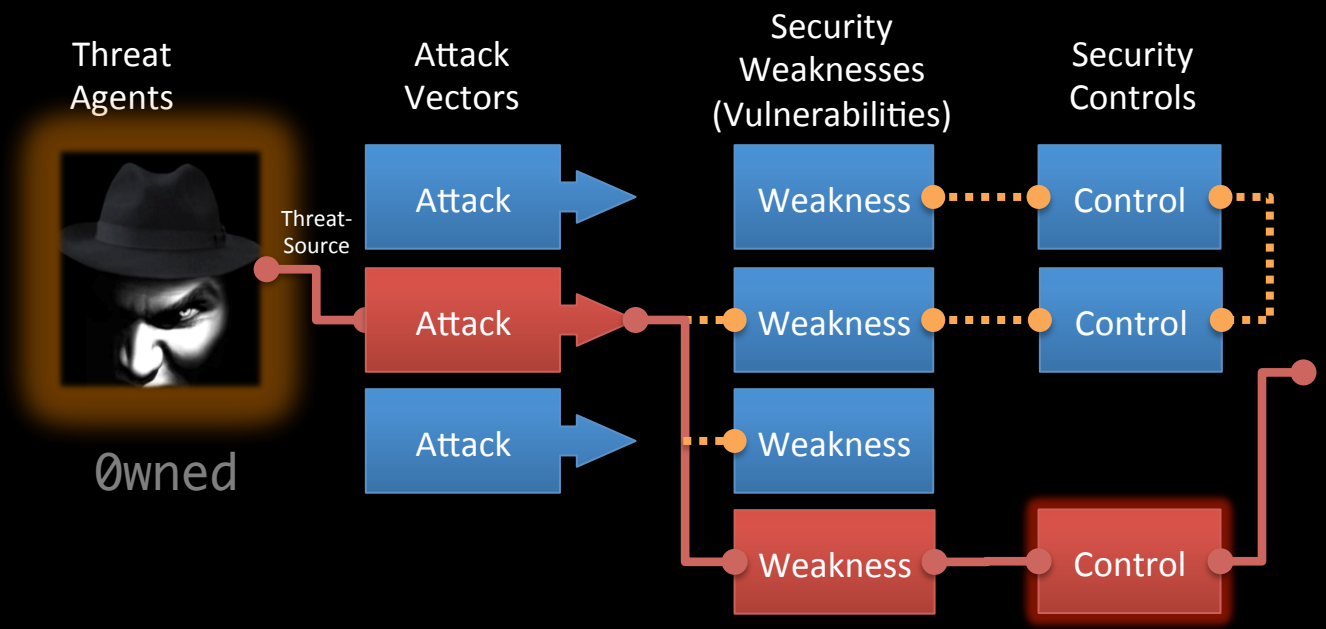
Threat paths



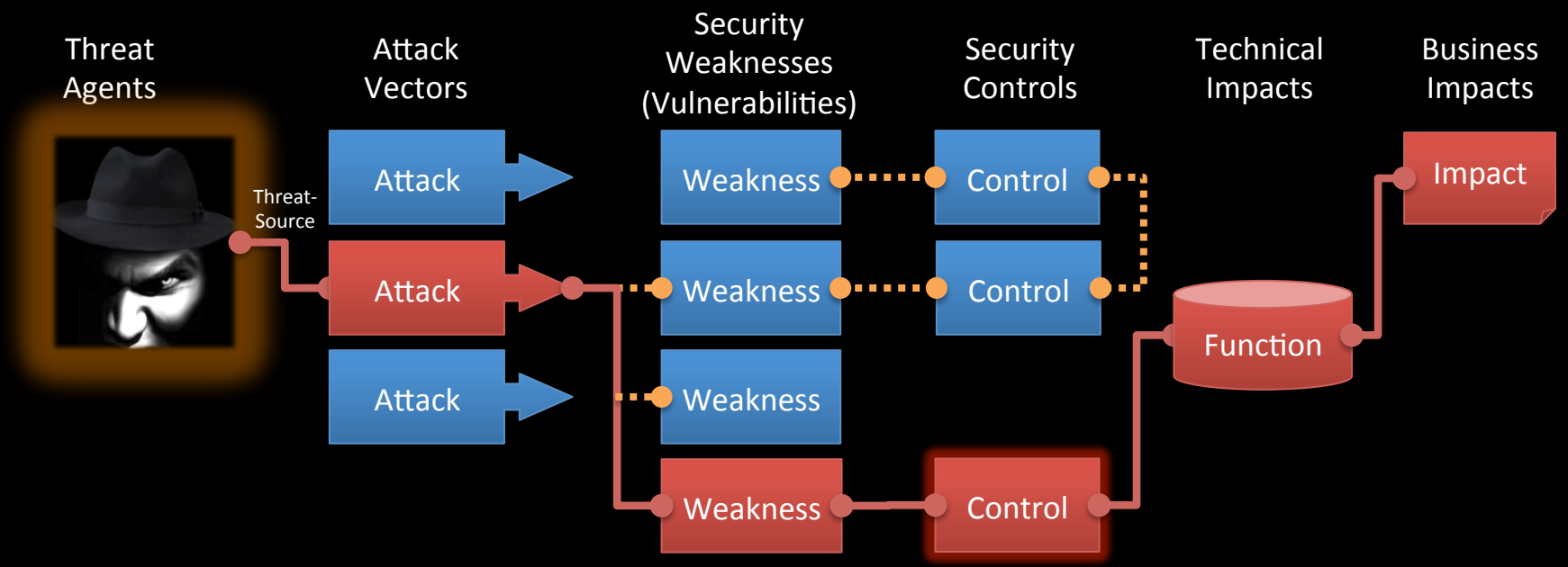
Threat paths



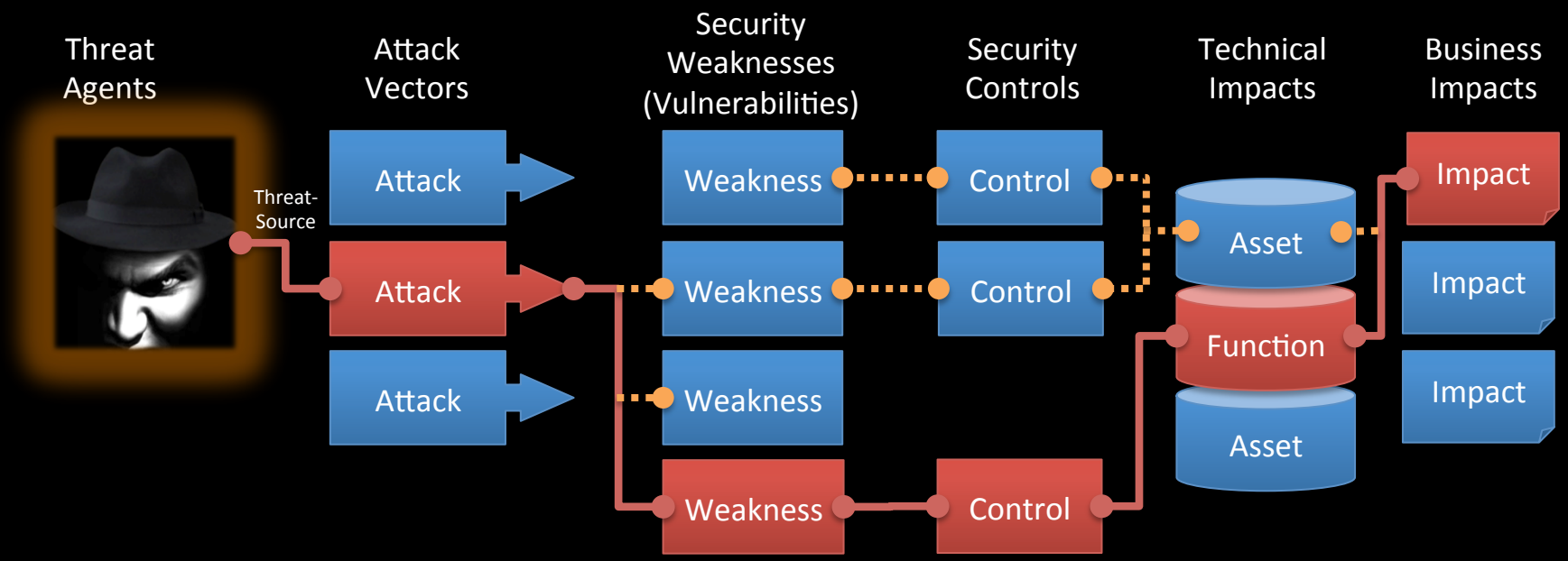
Threat paths



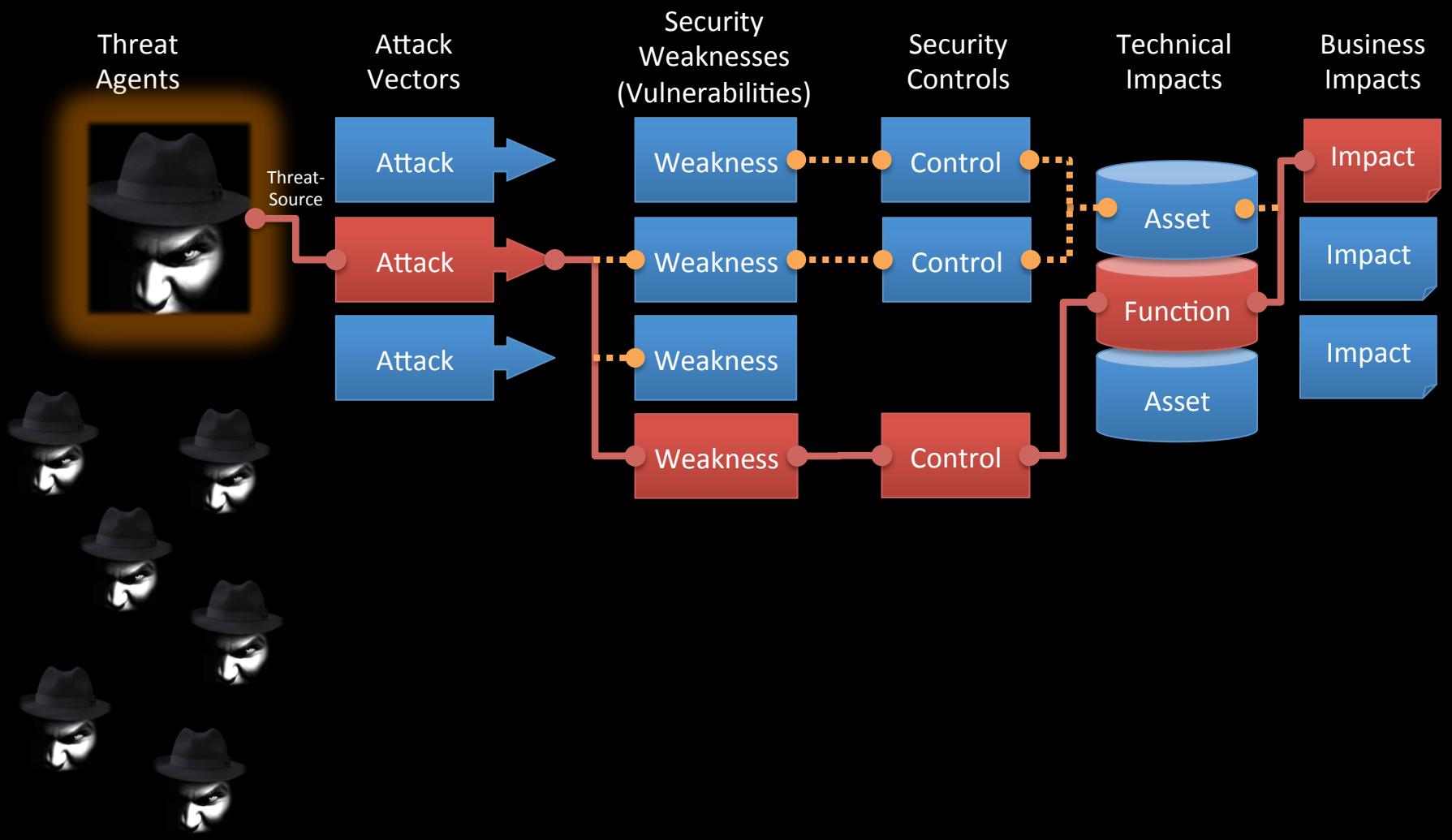
Threat paths



Threat paths



Threat paths



Top 10 Mobile Risks

?

The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

ISO 13335 – Information Technology Security Techniques

Top 10 Mobile Risks

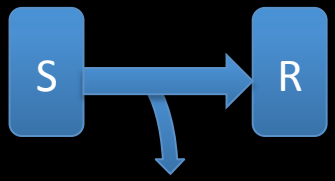
1.	Insecure Data Storage	Data at rest control
2.	Weak Server Side Controls	Bypass client to attack
3.	Insufficient Transport Layer Protection	Over-the-wire
4.	Client Side Injection	XSS, etc.
5.	Poor Authorization and Authentication	Low factors
6.	Improper Session Handling	Allow Hijacking
7.	Security Decisions Via Untrusted Inputs	Keyboards
8.	Side Channel Data Leakage	Listening, in-Sophisticated
9.	Broken Cryptography	Easily breakable, WEP
10.	Sensitive Information Disclosure	Data leakage, Social

Attacks

Attacks

Attacks

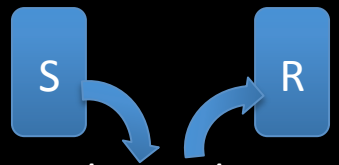
Attacks



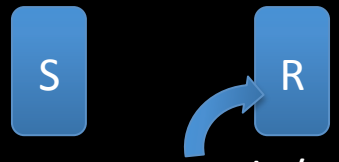
Attack Confidentiality

Eavesdrop/Copy

Attack Integrity

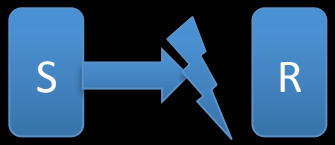


Stop/Delay/Modify



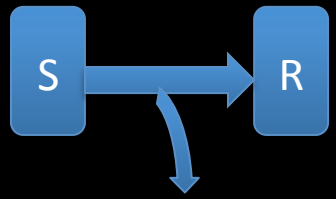
Masquerade/
Assume identity/
Authenticity

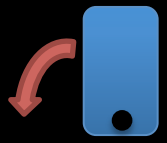
Attack Availability



Destroy channel,
corrupt, overwhelm

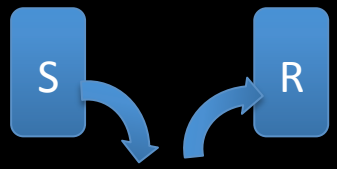
Attack Confidentiality

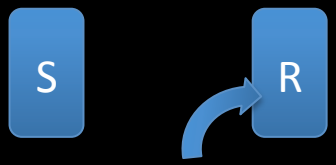




- Eavesdropping
- No Physical Boundaries
- Tracing/Tracking
- Device Capture

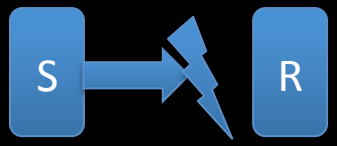
Attack Integrity





- SSL Stripping
- Reputation
- Fraud (Monetary/Identity)
- Browser icons common

Attack Availability



- Distributed Denial of Service
- Bandwidth Constraints
- Interference and Jamming

Recent Real World Examples

- Feb 2013 – Watering Hole attack

THE WALL STREET JOURNAL.

facebook

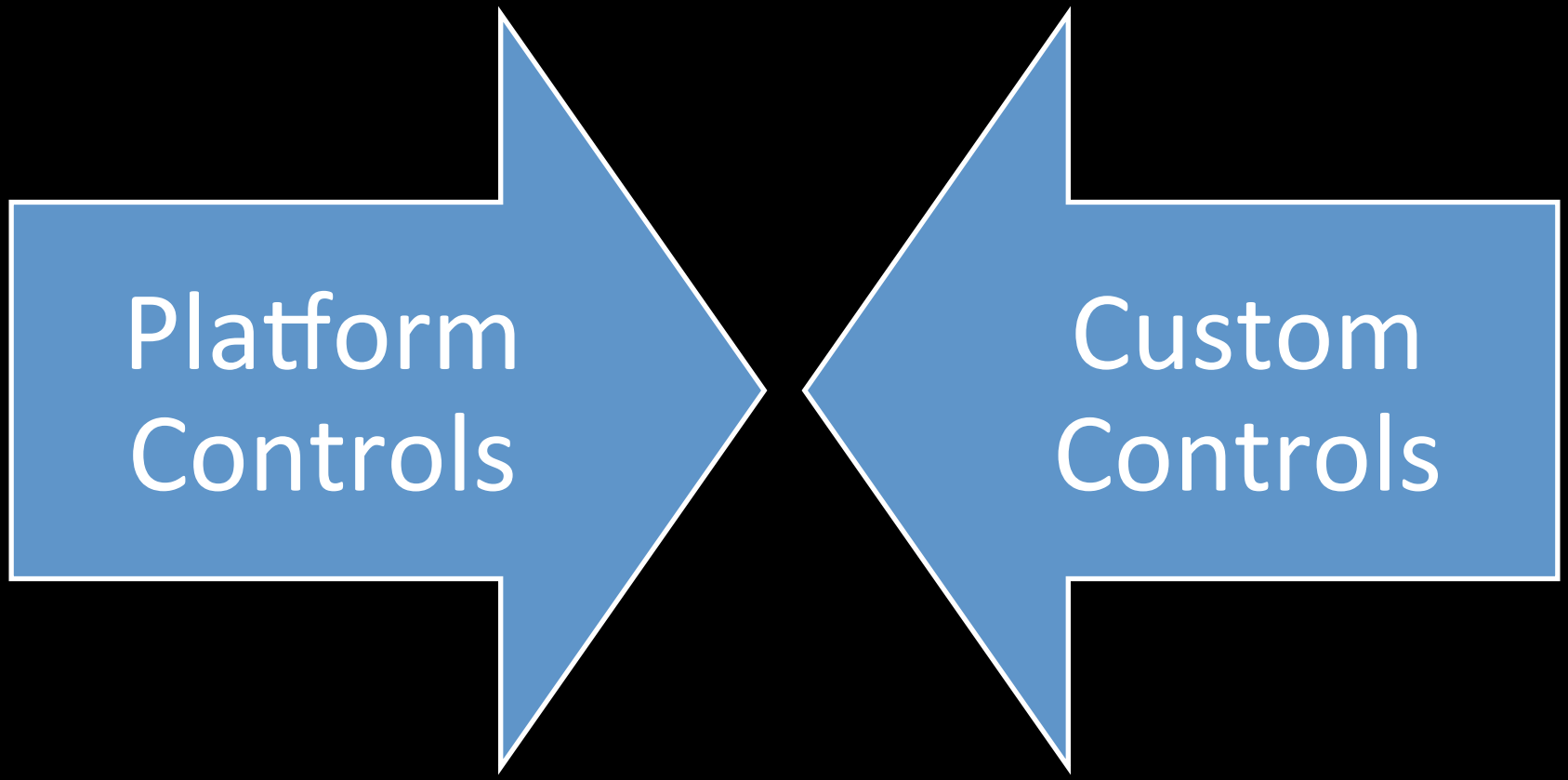
Microsoft

- Notable and news worthy

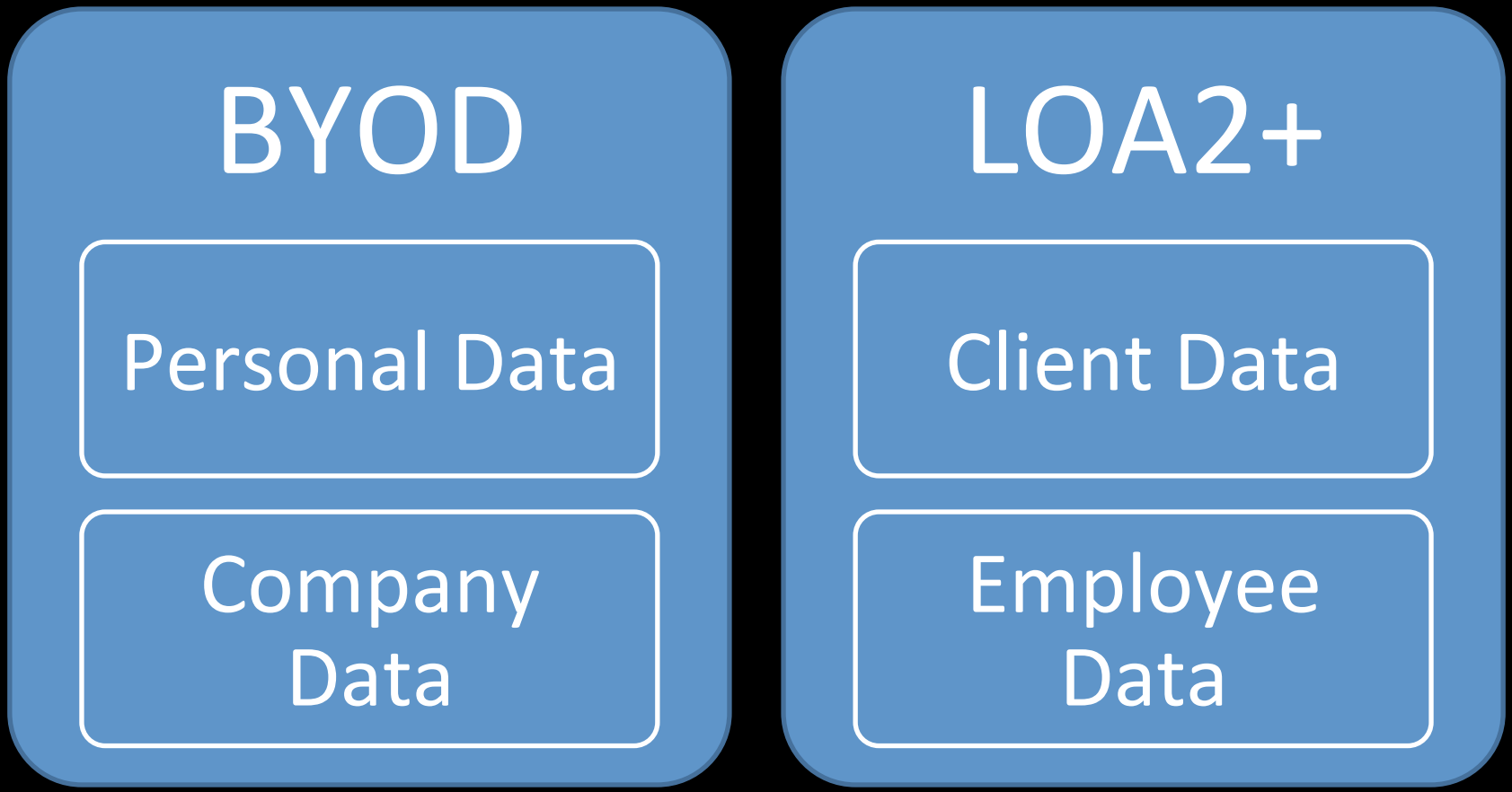
RSA

SECURITY CONTROLS

Security controls



Custom controls

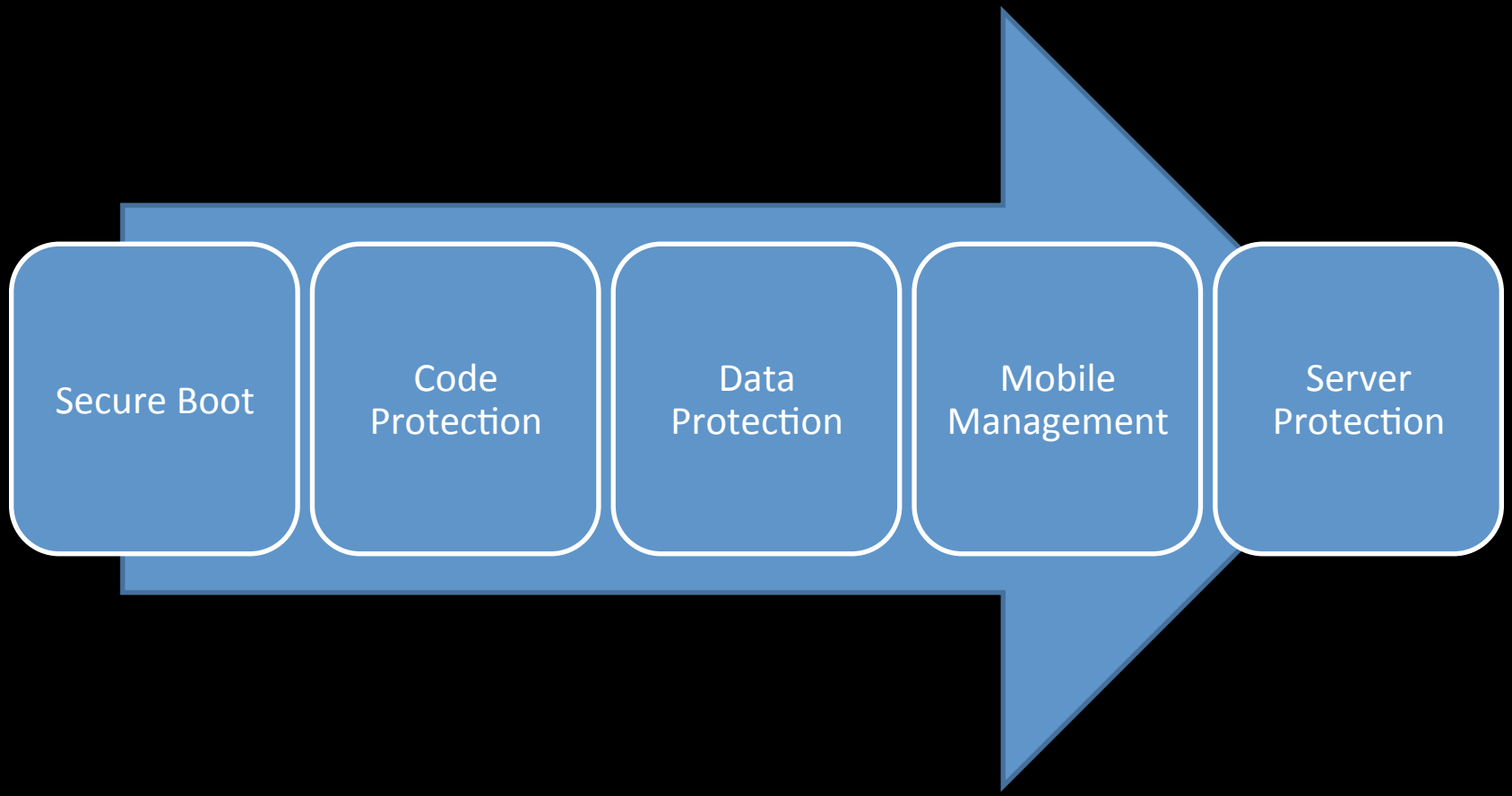


NIST Levels of assurance

Level of Assurance	Data Classification	Data Examples	Cumulative Authentication Requirements	Authentication Examples
L0 – No knowledge of identity.	Public Anonymous	Public Website	None	Public website
L1 - Little or no confidence in the asserted identity's validity.	Public	Public discussion forum	One of any factor	Username + password i.e. something you know
L2 - Some confidence in the asserted identity's validity.	Internal	Team process documents in SharePoint	One of any factor Verified identity	Username + password i.e. something you know, checked against company HR controlled LDAP directory.
L3 - High confidence in the asserted identity's validity.	Confidential	Company strategy presentation	Two or more of any factor	Password protected X509 soft certificate, is both something you have and something you know.
L4 -Very high confidence in the asserted identity's validity.	Strictly Confidential	Client or employee identifying documents	Two or more factors One hard FIPS 140-2 token Independent reader	Password protected smartcard over reader with button

Factors: something you know(username, password), you have (smartcard), you are (fingerprints)

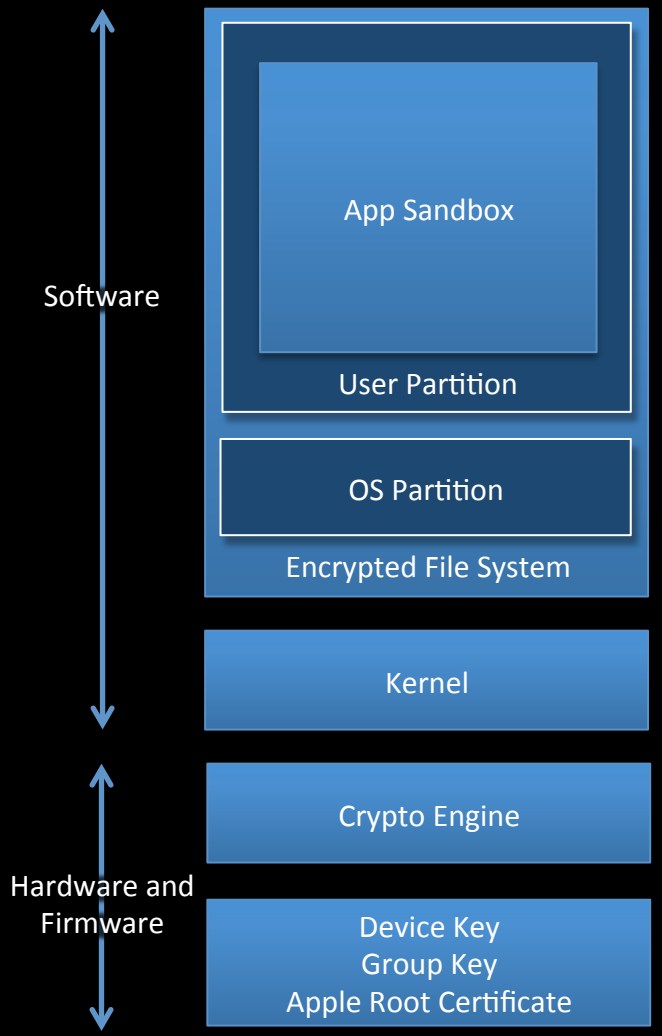
Control categories



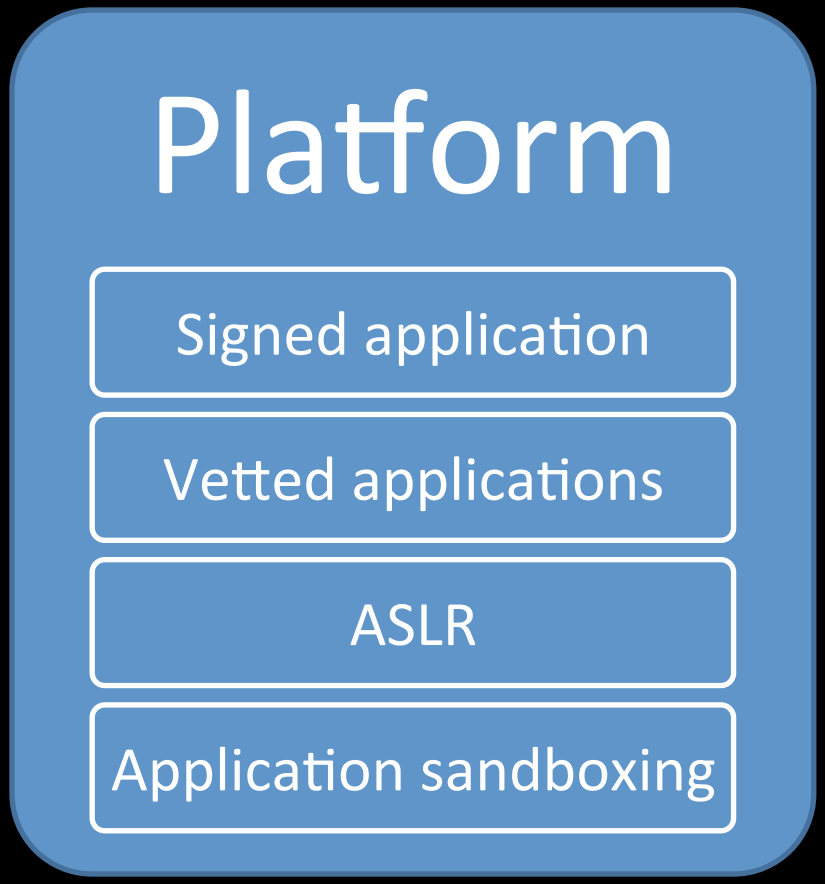
Secure Boot – Apple Example

- Protecting low level to create start of a chain of trust

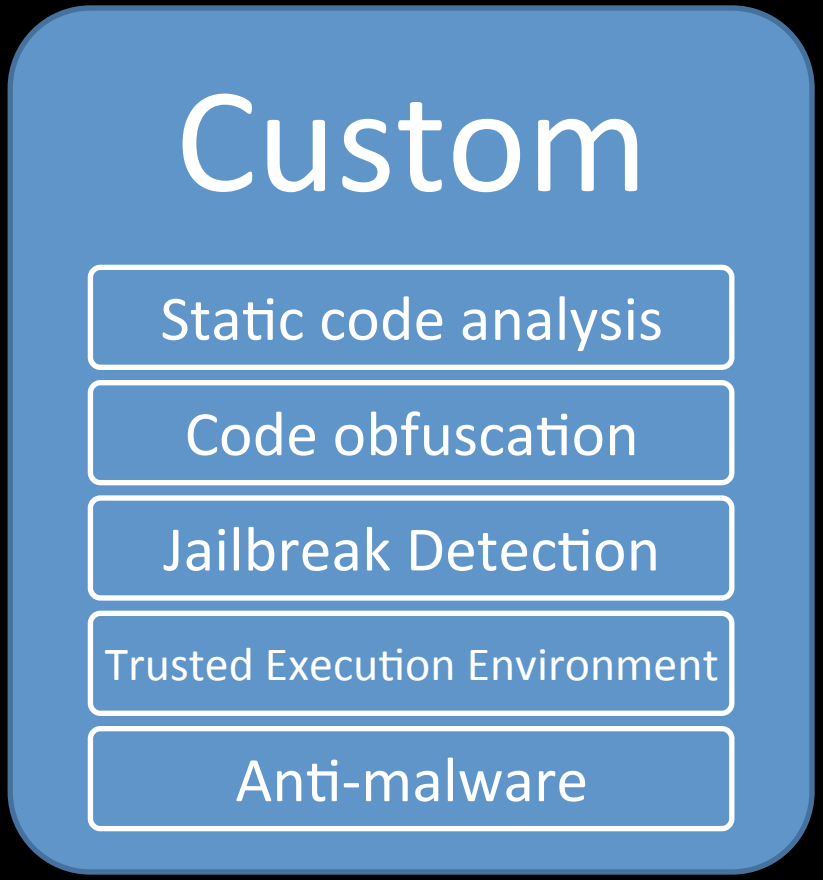
- Processor boots from read-only boot ROM – trusted – Protects Integrity
- Contains the Apple Root CA
  - Verifies Low-Level boot loader is signed by Apple
  - Secure boot chain ensures lowest levels of software are tamper free
  - Boot process ensures only Apple signed code can run on the device
- Jailbreaks have exploited boot loader vulnerabilities



Code Protection



Code Protection



Code Protection

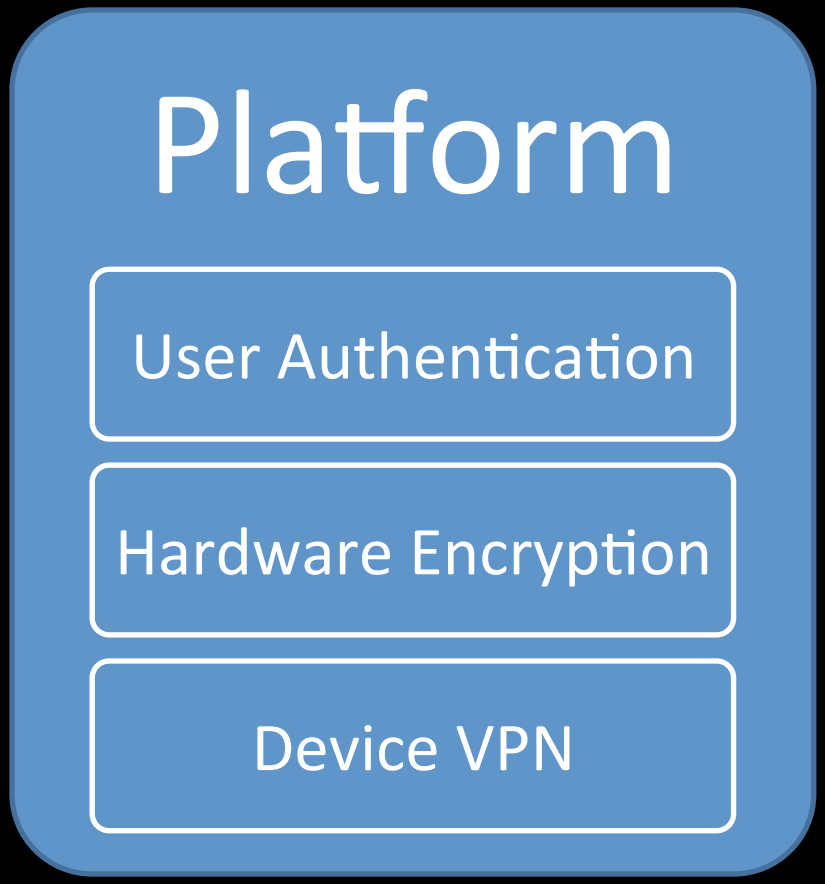
Platform

- Signed application
- Vetted applications
- ASLR
- Application sandboxing

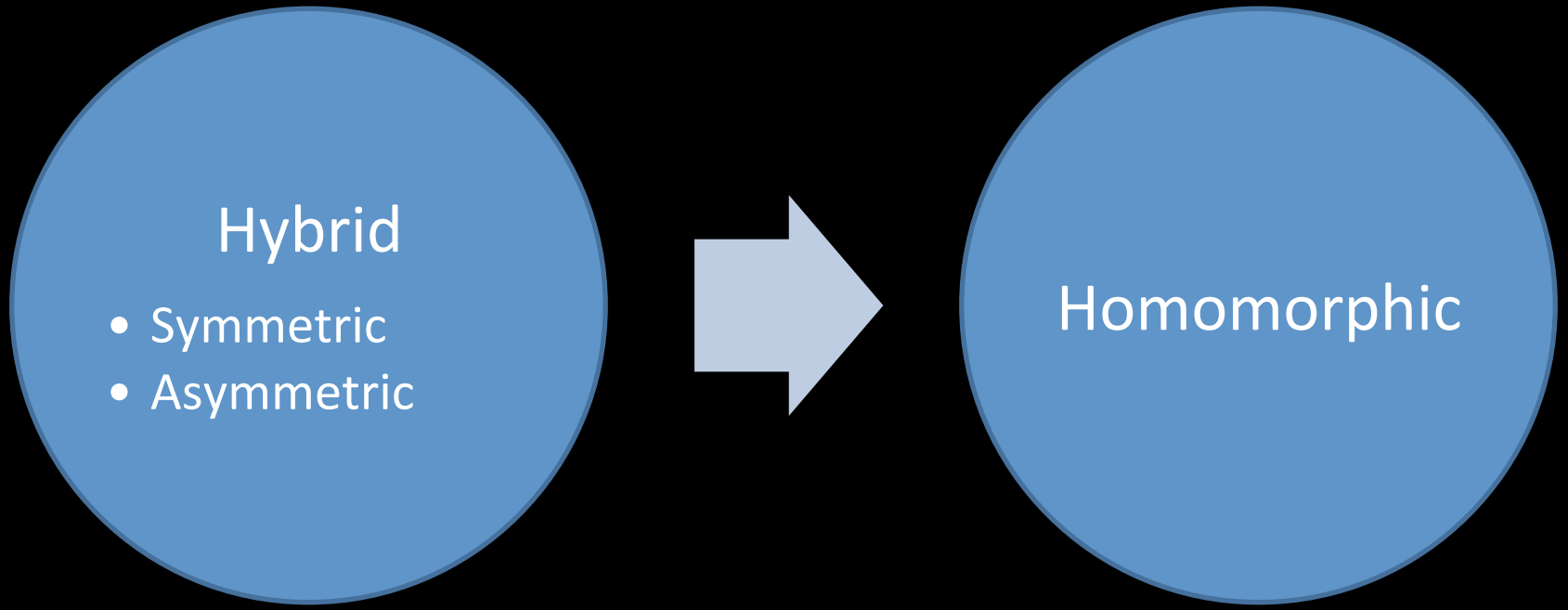
Custom

- Static code analysis
- Code obfuscation
- Jailbreak Detection
- Trusted Execution Environment
- Anti-malware

DATA Protection

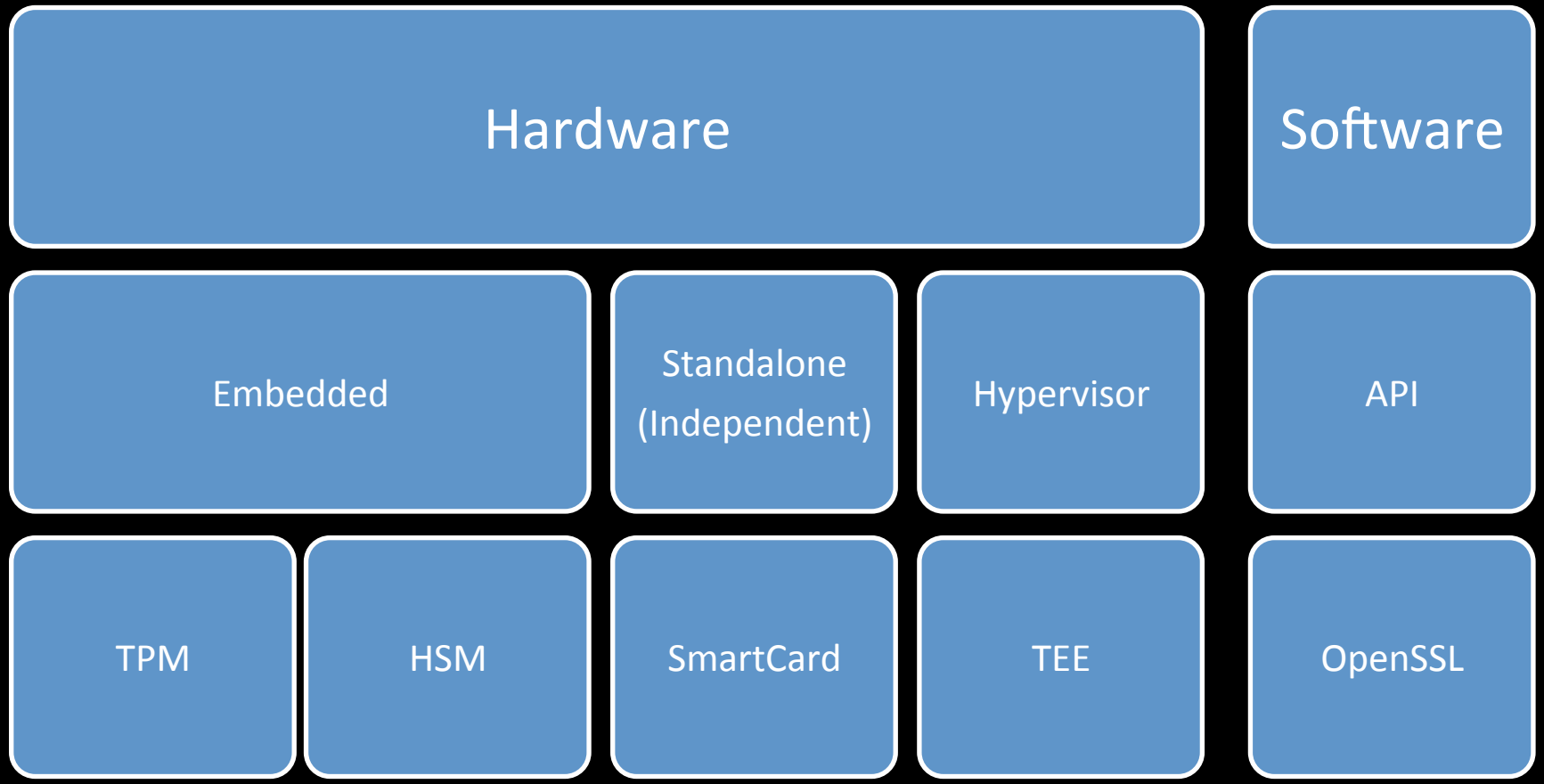


Data Protection - Encryption

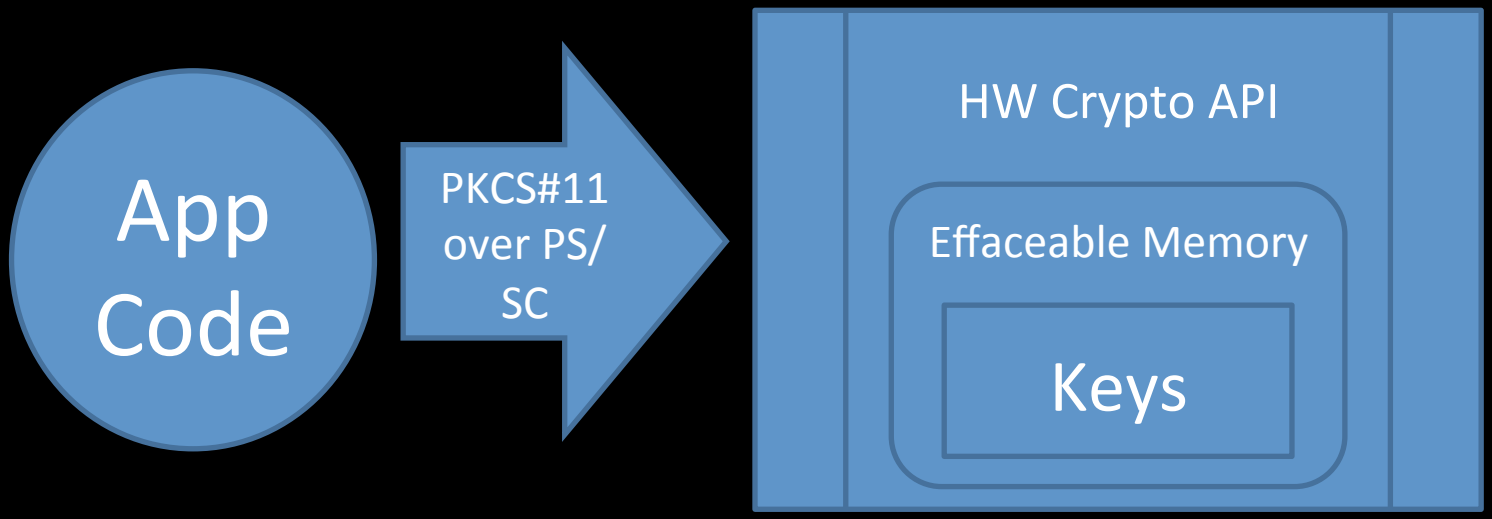


Data protection

Data Protection - Encryption



Data Protection - Encryption

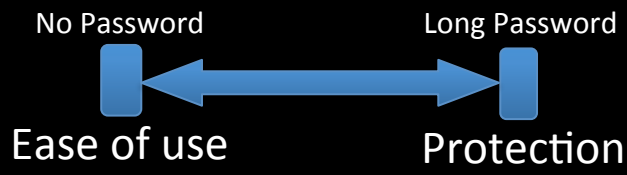


Data Protection - Authentication

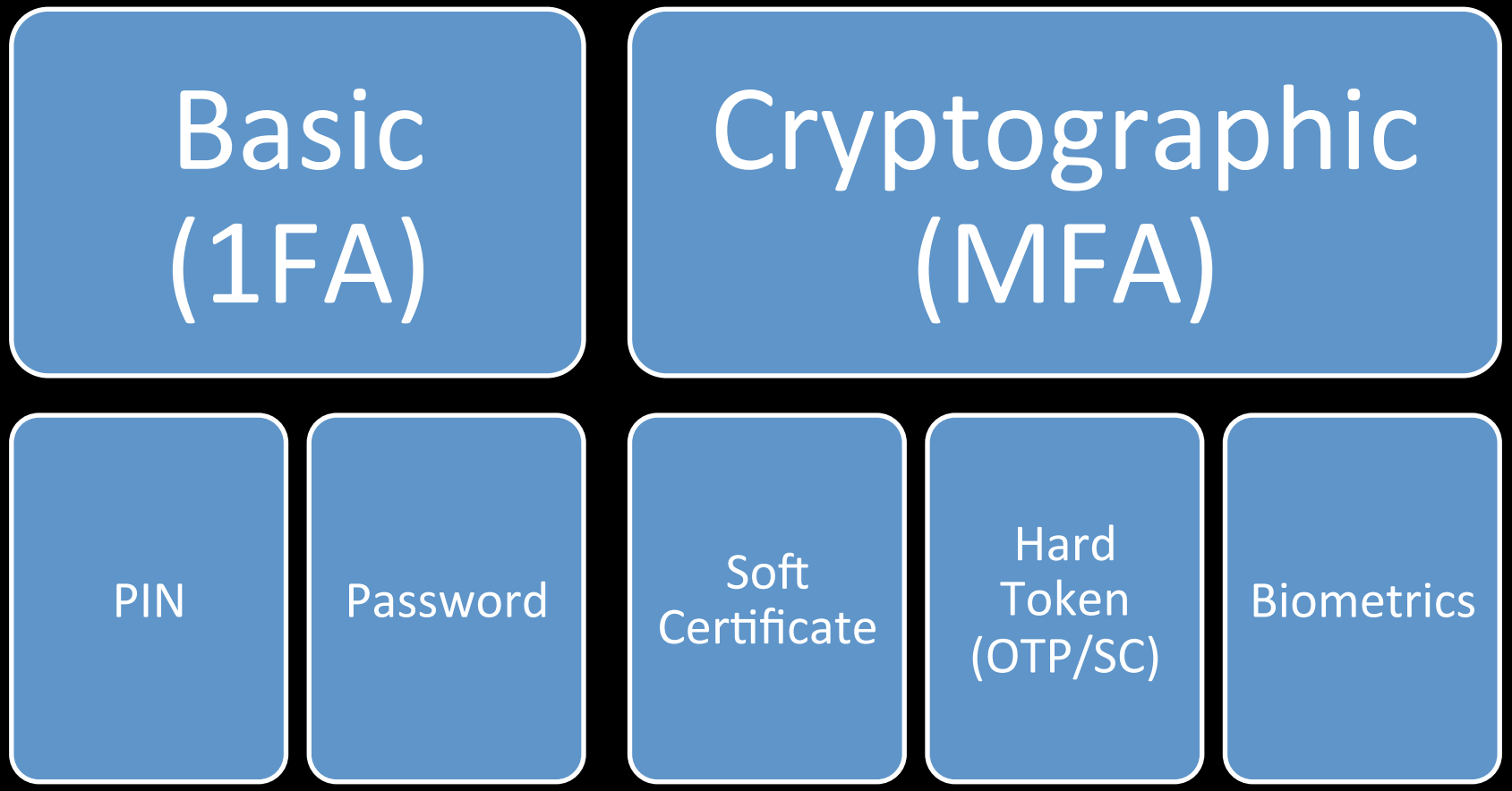
	PIN	Freq
#1	1234	10.71%
#2	1111	6.02%
#3	0000	1.88%
#4	1212	1.20%
#5	7777	0.75%
#6	1004	0.62%
#7	2000	0.61%
#8	4444	0.53%
#9	2222	0.52%
#10	6969	0.51%
#11	9999	0.45%
#12	3333	0.42%
#13	5555	0.40%
#14	6666	0.39%
#15	1122	0.37%
#16	1313	0.30%
#17	8888	0.30%
#18	4321	0.29%
#19	2001	0.29%
#20	1010	0.29%

Top 20 used pins…do you have one?

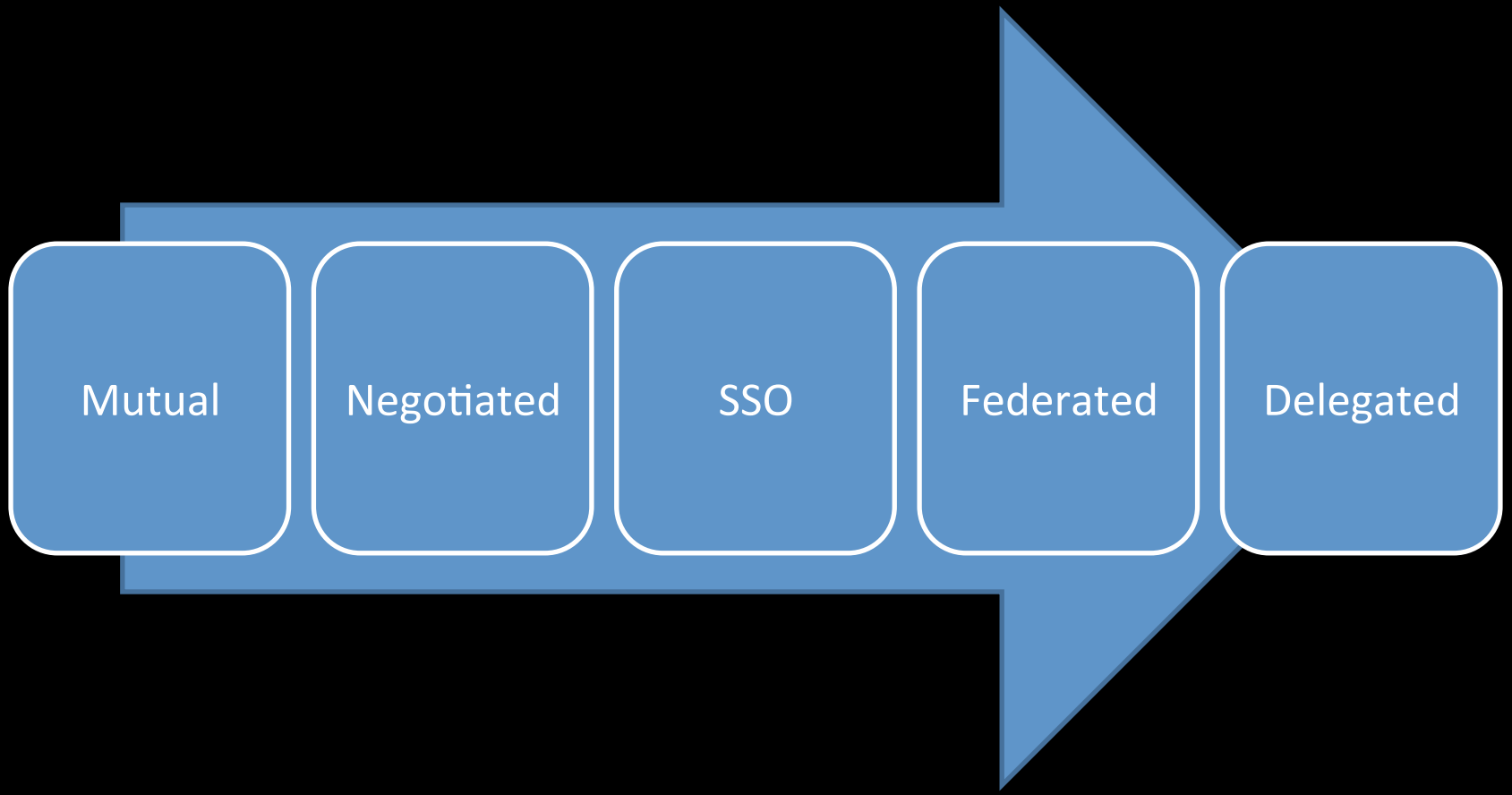
#22 = 2580 ?



Data Protection - Authentication



Data Protection - Authentication



Data protection

Platform

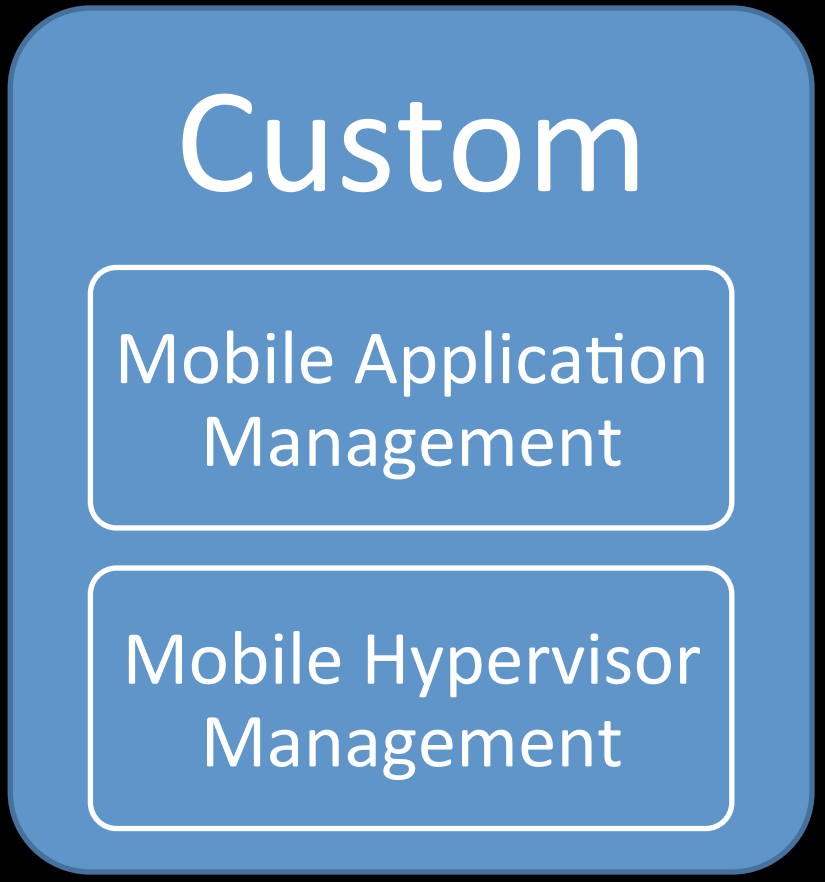
- User Authentication
- Hardware Encryption
- Device VPN

Custom

- Container FIPS 140-2 Encryption
- Container Tunnels
- Digital Rights Management
- Secure Tokens & OS

Mobile Management

Mobile Management



Mobile Management

Platform

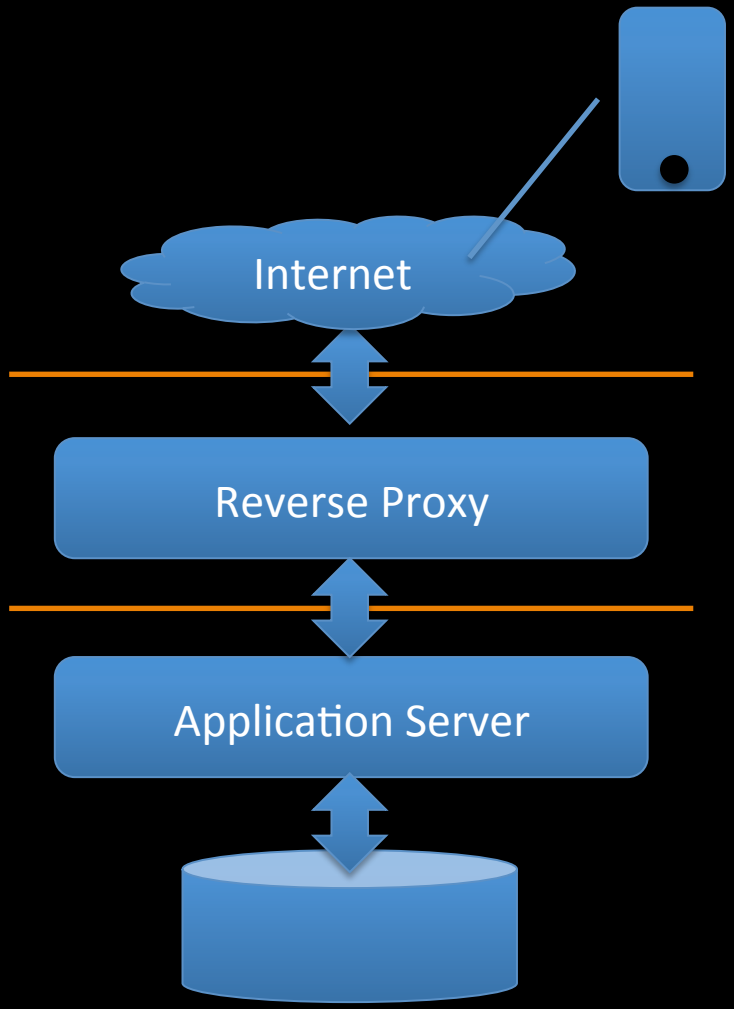
Mobile Device Management

Custom

Mobile Application Management

Mobile Hypervisor Management

Securing Access to Services



Securing Access to Services

- Risk Assessment

Securing Access to Services

- Black Hats and White Hats

Securing Access to Services

- Penetration Test

Closing Thoughts

- You get a lot without trying on mobile platform
- You have to spend the effort on the controls (Client / Server)
- Technology is improving to support security

Shane Williams
Alex Batlin

Thank You!

And Stay Safe