RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CCT-R05

ARM: A Security Opportunity against Advanced Persistent Threats

Siddharth Anbalahan

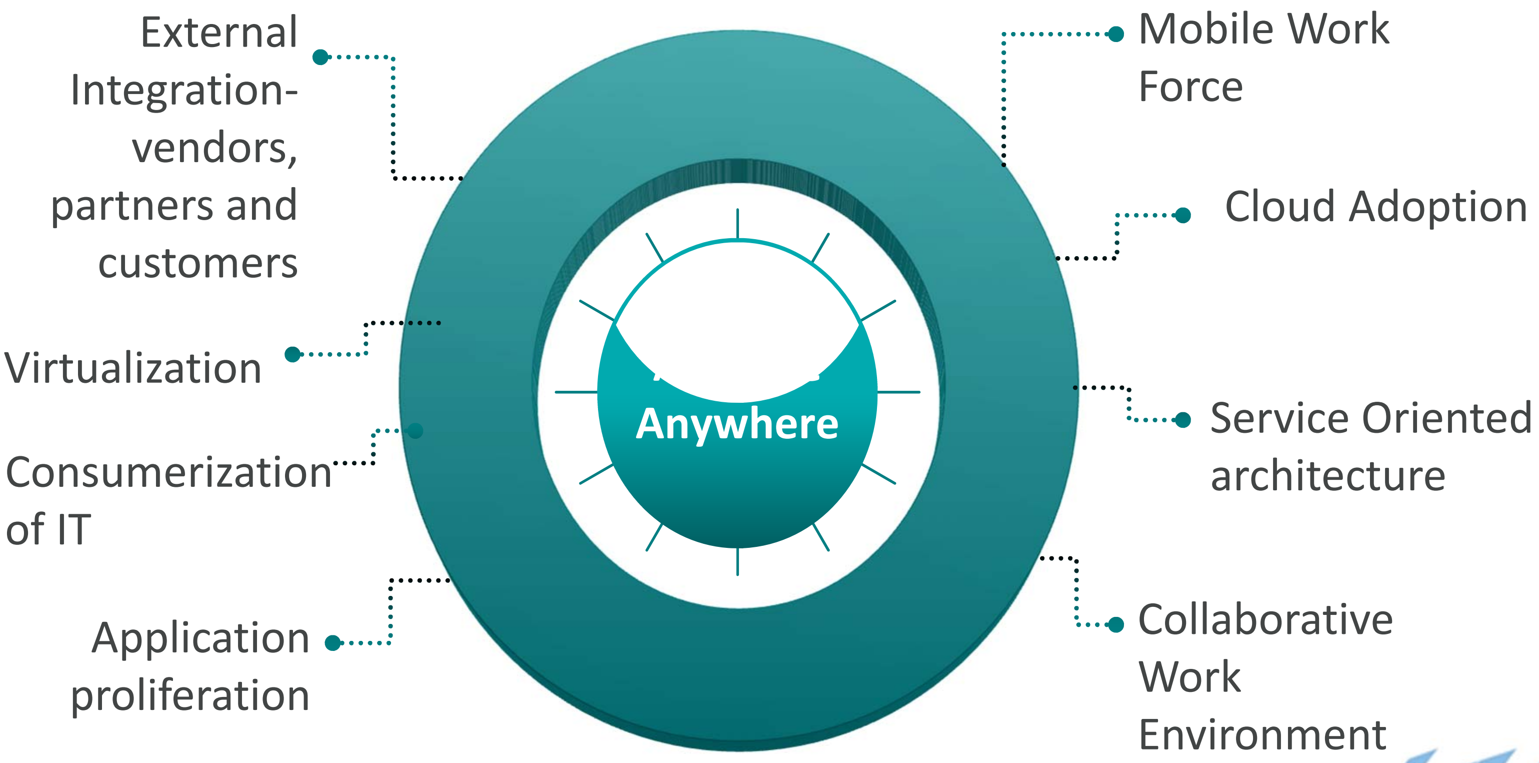
Practice Head-Security Testing
Paladaion Networks Pvt Ltd.
Siddharth.anbalahan@paladion.net

#RSAC

Agenda

- Evolving IT Landscape
- Evolving IOT Landscape
- Anatomy of APT Attacks
- IT Security Ecosystem
- ARM Revolution
- ARM TrustZone and opportunity
- Summary
- Future: APTs in the IoT World

Evolving IT Landscape



External Integration- vendors, partners and customers

Virtualization

Consumerization of IT

Application proliferation

Anywhere

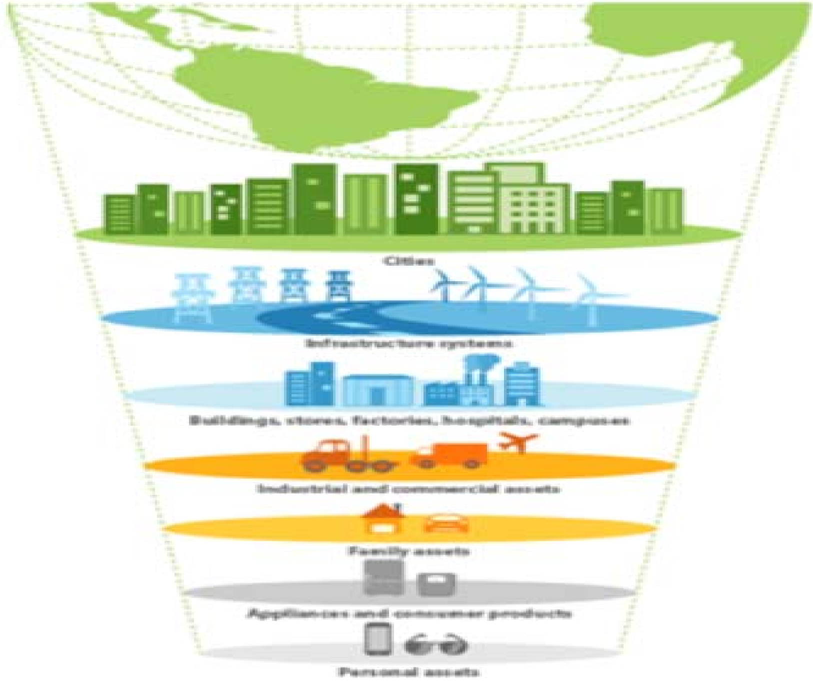
Mobile Work Force

Cloud Adoption

Service Oriented architecture

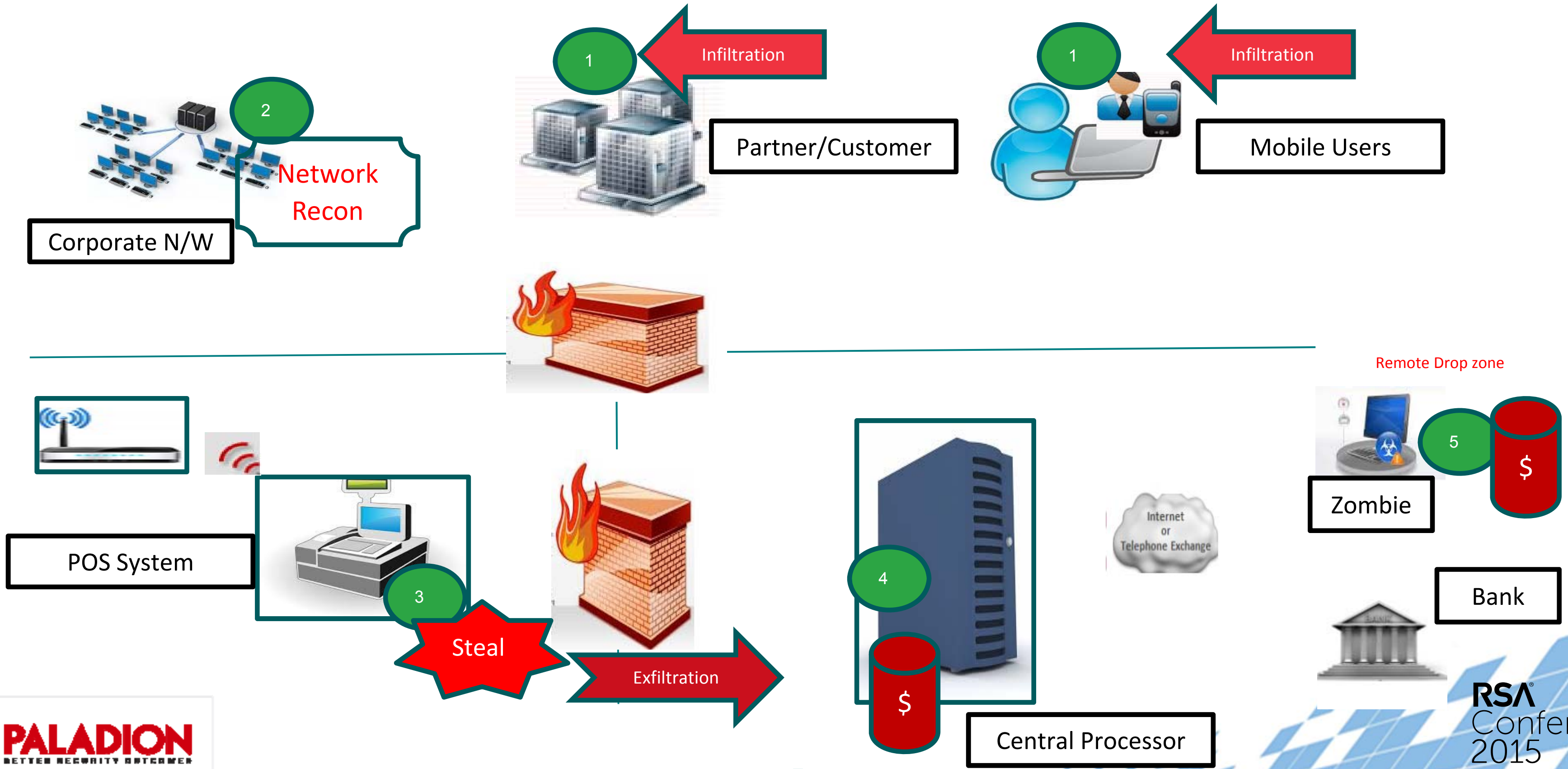
Collaborative Work Environment

Evolving IOT Landscape


Cities
Infrastructure systems
Buildings, stores, factories, hospitals, campuses
Industrial and commercial assets
Family assets
Appliances and consumer products
Personal assets

According to Cisco
"Currently 10 billion things are connected out 1.5 trillion things that are yet to be connected"

Anatomy of APT Attacks



1

Infiltration

1

Infiltration

2

Network Recon

Corporate N/W

Partner/Customer

Mobile Users

Remote Drop zone

5

$

Zombie

POS System

3

Steal

Exfiltration

4

$

Central Processor

Bank

PALADION

BETTER SECURITY OUTCOMES

RSA Conference 2015

Abu Dhabi

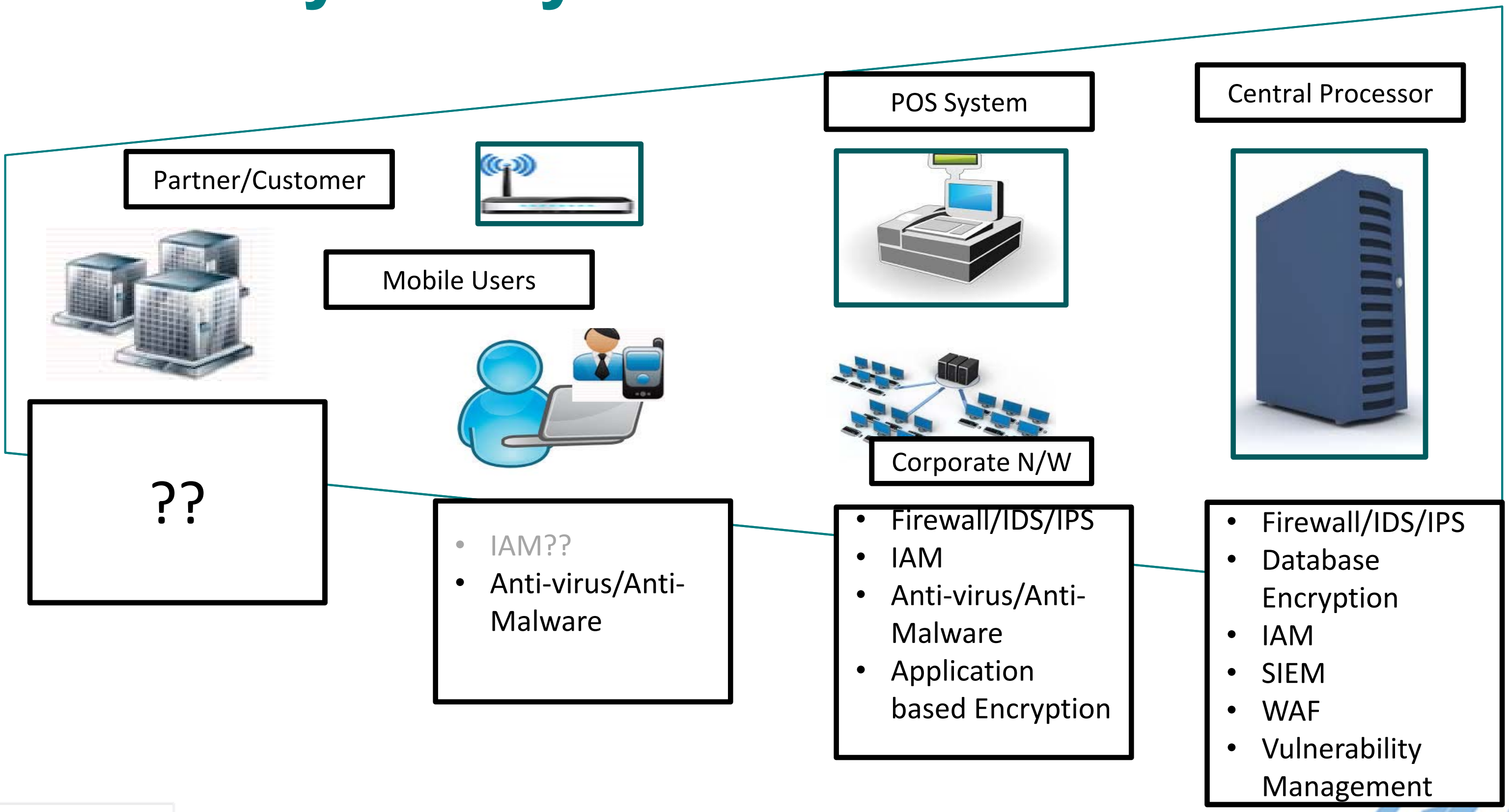
Anatomy of APT Attacks

- Infiltration happens at the weakest link
  - Example: Target - External Vendor Network had access to billing management system
- Once inside the network they usually get into user PCs or peripheral Servers and perform a network recon
- Traversing the network they get into POS systems either via software vulnerabilities or poor user management
- Using memory stealing techniques they can gather and dump data to a Server that connects to the internet

Anatomy of APT Attacks – Key Systems

- Infiltration happens at the weakest link
  - Example: Target - External Vendor Network had access to billing management system
- Once inside the network they usually get into user PCs or mobile devices and perform a network recon
- Traversing they network they get into POS systems either via software vulnerabilities or poor user management
- Using memory stealing techniques they can gather and dump data to a Server that connects to the internet (insecure configurations)

IT Security Ecosystem



Partner/Customer

Mobile Users

POS System

Central Processor

Corporate N/W

??

- IAM??
- Anti-virus/Anti-Malware

- Firewall/IDS/IPS
- IAM
- Anti-virus/Anti-Malware
- Application based Encryption

- Firewall/IDS/IPS
- Database Encryption
- IAM
- SIEM
- WAF
- Vulnerability Management

IT Security Ecosystem

- Recent statistics and reports have shown that organizations still rely on Anti-Malware/virus protection systems for protection against APT attacks
  - Many ways to evade detection - Styx-Crypt
  - Can evade most Malware detection mechanisms in at least the first 12 – 24 hours
- Weakest link: Most B2B contracts still do not discuss security controls to curtail APTs

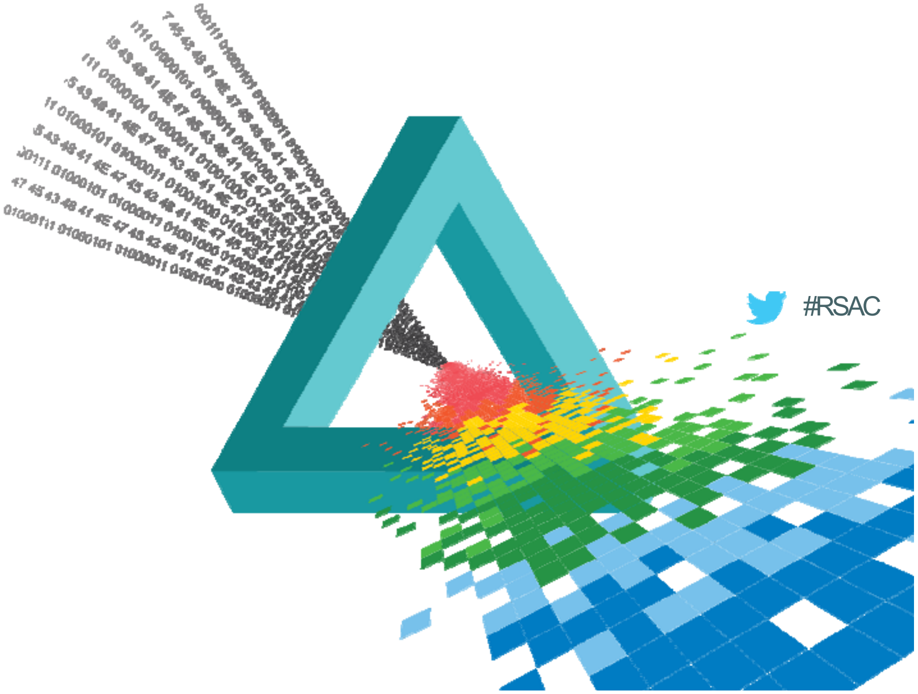
Data Breaches are expensive

- Ponemon Institute and IBM released a study where on an average data breaches costed - $3.8 million
- It is not enough to only classify data and monitor usage
- There is a need to classify IT environments fundamentally between secure and normal operations
  - Data and information can flow through all points of an IT infrastructure

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

The ARM Revolution



#RSAC

ARM Revolution

- Today's biggest SoC manufactures use ARM based CPUs
  - Focus on low power consumption
  - IP based business partner model – MediaTek, Snapdragon, Tegra, Samsung
  - IPv6 is here
- IoT will fundamentally change enterprise infrastructure ecosystem.
  - More players a.k.a devices will be added
  - Taking classification based and layered approach to security will prove detrimental

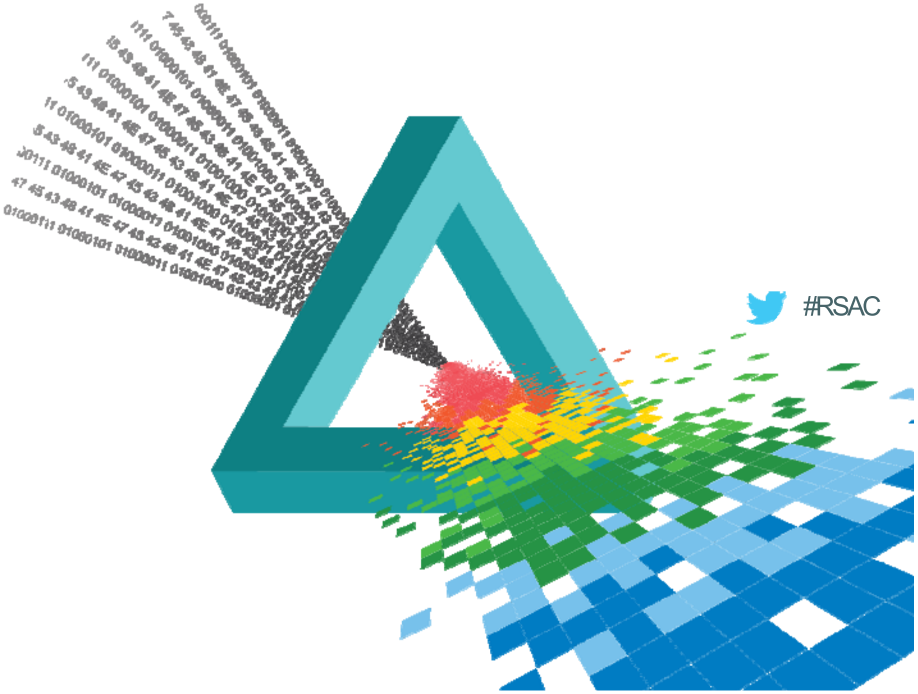
ARM Revolution – Moving up the value chain

- Can they operate on high end servers or processing?
- Can they compete?
  - MIPS I-Class I64500 Warrior CPU (Imagination)
  - 64-bit architecture, and virtualization
  - Support for Hardware Multi-threading – 4 per core
  - Approaches 1.5 GHz at lower power consumption

RSAConference2015

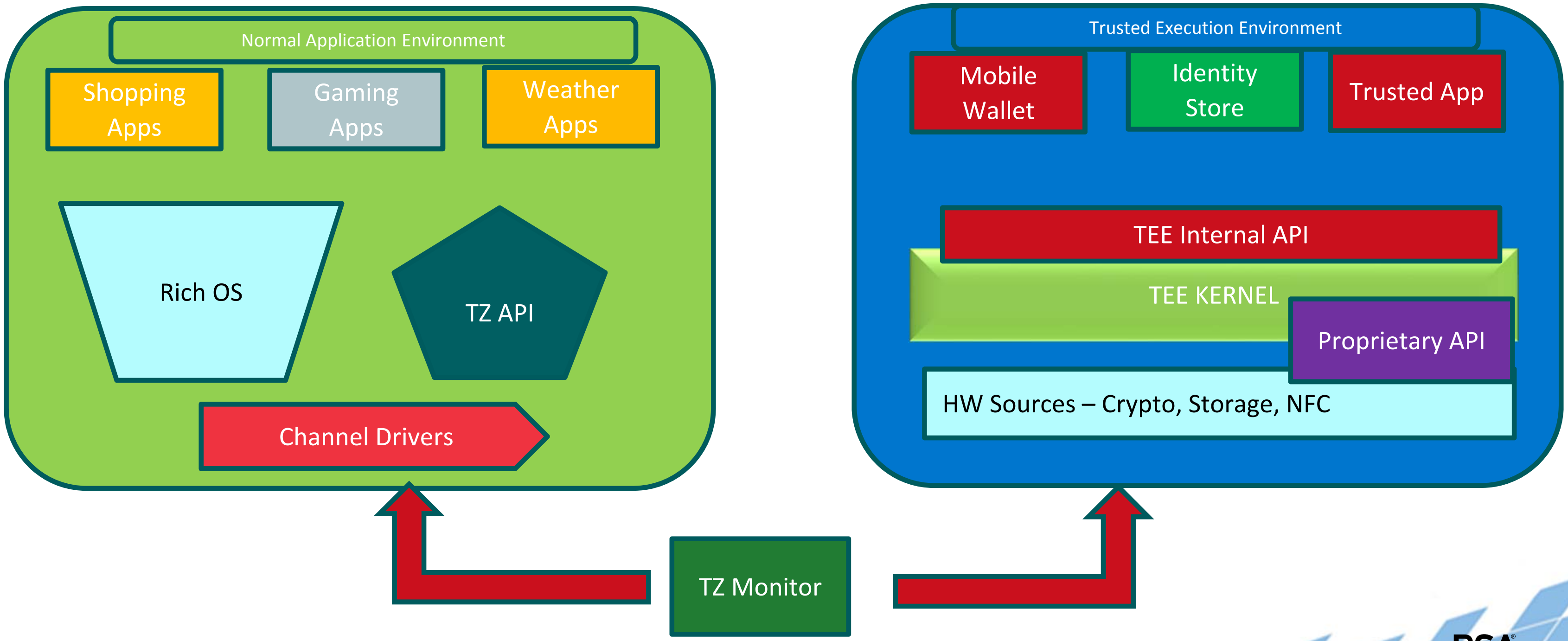
Abu Dhabi | 4–5 November | Emirates Palace

ARM TrustZone



#RSAC

ARM TrustZone



ARM TrustZone

- Hardware root of trust
  - A basis for system integrity
- Integrity through Trusted Boot
- Secure peripheral access
  - Screen, keypad , fingerprint sensor etc.
- Secure application execution
- Trust established outwards

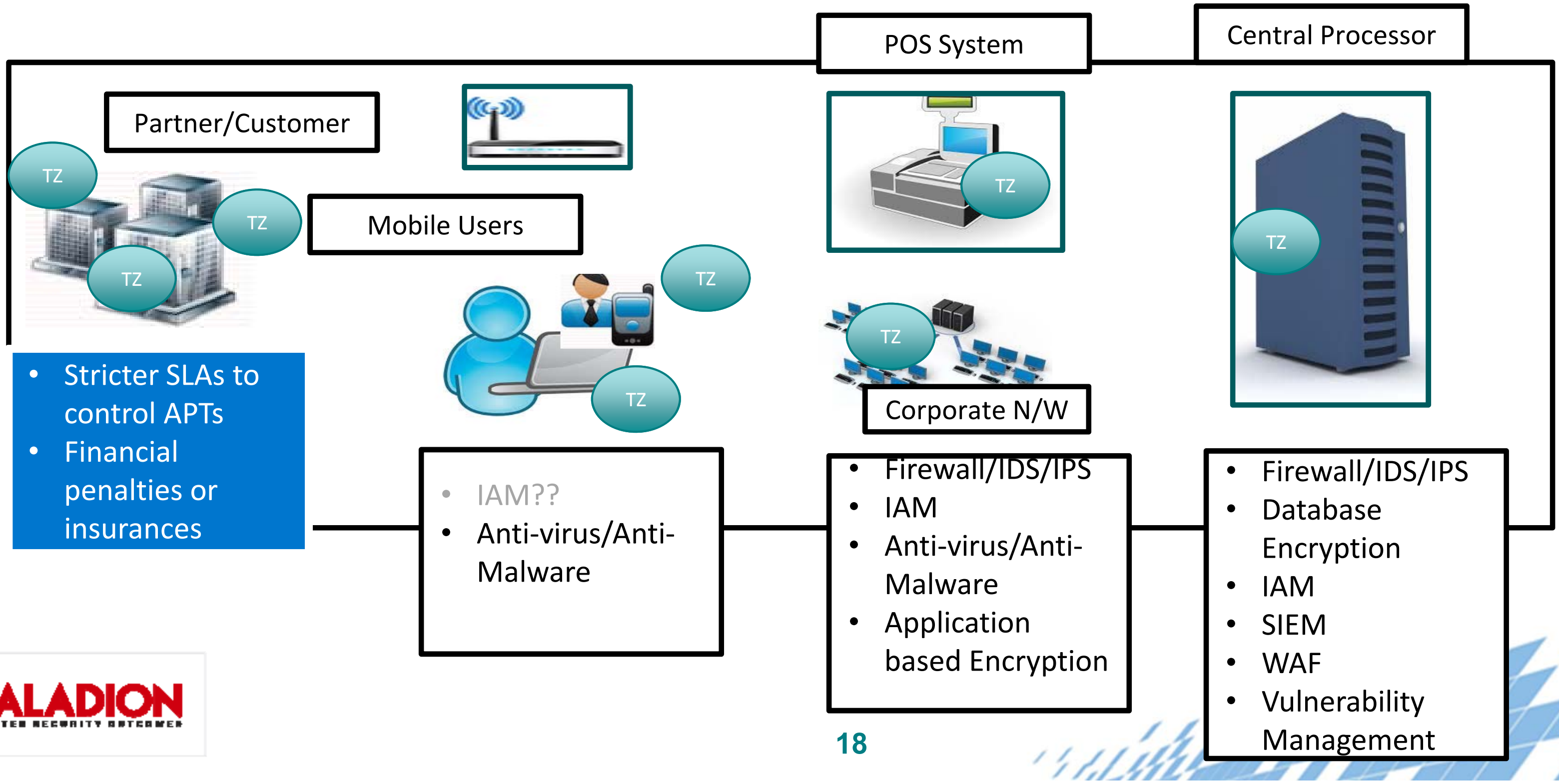
- Trusted Apps run in TEE
  - Isolation from software attacks
- App developers create hardened apps
- Trust established by signing each app.

How does it augment existing APT solutions?

- Secure Boot
  - Cryptographic boot loaders
  - Boot Process monitored for tampering
    - HW/SW Rootkit protection
- Anti-Malware App can check Normal OS in runtime
  - Least privilege principle ensures App cannot be evaded
  - Anti-Malware with trusted privilege will make it difficult for malware to go undetected for long
- Ability to Wipe out software from the TrustZone
- Diagnostic tests can be run to monitor events from the TrustZone

ARM: IT Security Ecosystem

Data and Execution Environment Segregation Across the Ecosystem



Partner/Customer

- Stricter SLAs to control APTs
- Financial penalties or insurances

Mobile Users

- IAM??
- Anti-virus/Anti-Malware

POS System

Corporate N/W

- Firewall/IDS/IPS
- IAM
- Anti-virus/Anti-Malware
- Application based Encryption

Central Processor

- Firewall/IDS/IPS
- Database Encryption
- IAM
- SIEM
- WAF
- Vulnerability Management

Summary

- The Future will see a proliferation of IoT devices and apps running on them
- Current APT defense and response systems would prove inadequate
- ARM CPU processors are the defacto standard in at least the first wave of many of these devices
- Leveraging existing Trusted Computing principles of ARM will augment existing APT defense systems

Future:APTs in IoT world

- Current ecosystem has seen many “Software Attacks”
  - Malware & Viruses hiding in the OS layer
- IoT Ecosystem will see Non-Invasive H/W Attacks
  - Side Channel Attacks
  - Delivering Rootkits via Firmware updates
  - Requires effort and research with few PoCs available
- Need to raise the bar against “Software Attacks” to be prepared the Non-Invasive H/W Attacks

Future:APTs in IoT world

- ARM:TrustZone has the potential to raise the bar against "Software Attacks" and Non-Invasive H/W Attacks
- SoC Manufactures need to ensure that firmware updates happen via secure medium
  - Encryption and Integrity
- In an increasing inter-connected world – SLAs and financial assurance measures for combating APT may become a reality.

Apply what you have learned today

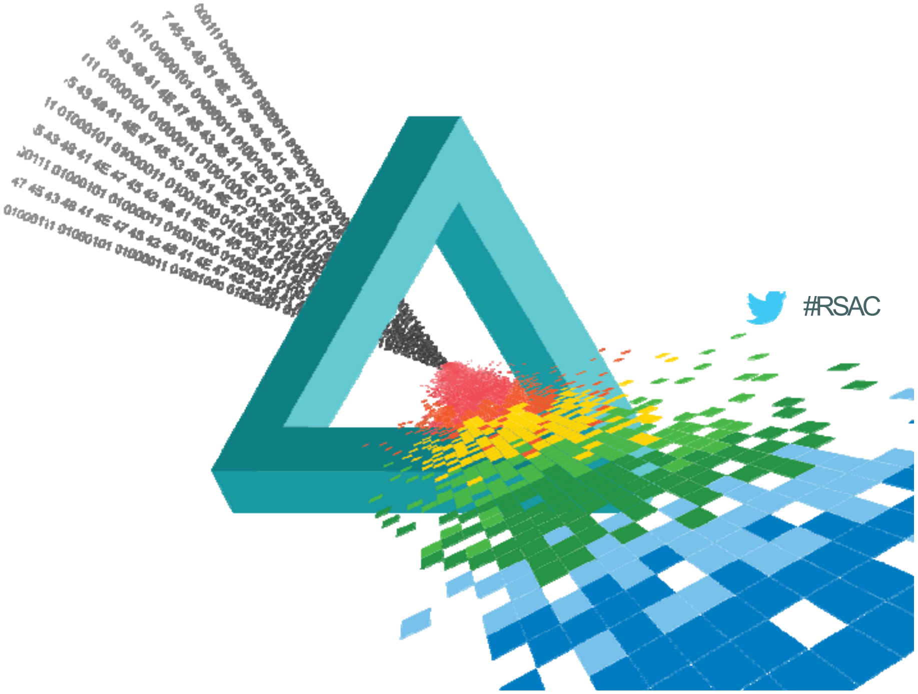
- In the first three months following this presentation you should:
  - Gather Trusted computing details for all types devices deployed in organization
  - Gather information on third party organizations
    - Access levels
    - Types of data and applications
- Next 1 year
  - Learn to embed critical functions via apps into “TrustZone”/TPM
  - Perform third party access audits to enforce tighter SLAs.

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank You

siddharth.anbalahan@paladion.net



#RSAC