RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: ECO-T07R

Endpoints in the New Age: Apps, Mobility, and the Internet of Things

Benjamin Jun

CTO
Chosen Plaintext Partners
@BenjaminJun

CHOSE
NPLAI
NTEXT

#RSAC

v17

A look back…

Windows/Mac

Thin Client

Smartphone

BYOD

Internet of Things

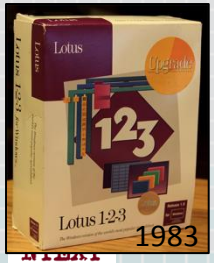
1980

1990

2000

2010

Lotus 1-2-3
WordPerfect



Browser
JavaScript

WiFi

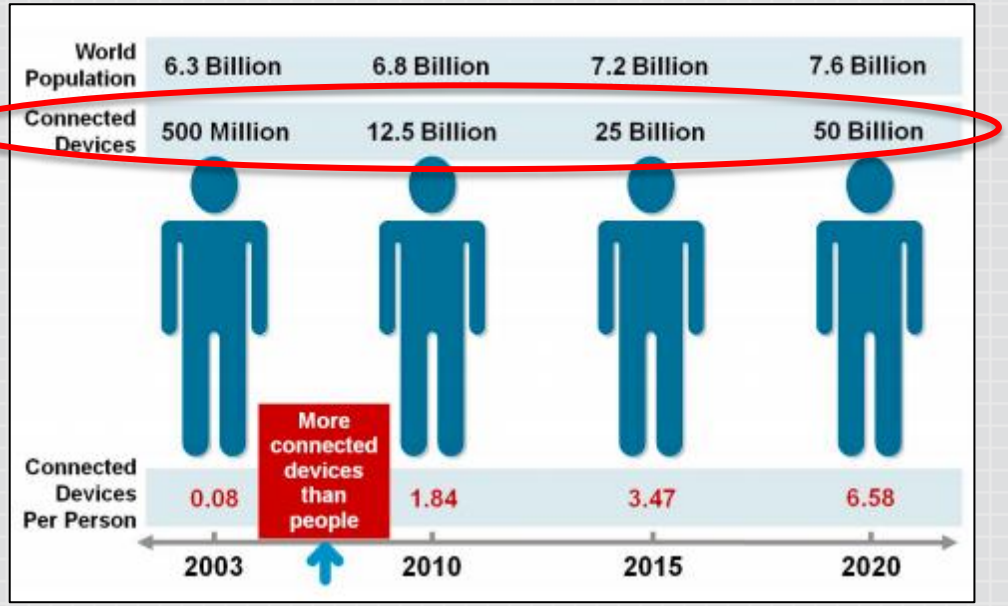
Cloud

App Store

HTML5

possible, dates specify when a platform reached critical mass
droid-life.com
Microsoft Windows 1.01, used with permission from Microsoft

Lots of connected devices!



Source: Cisco

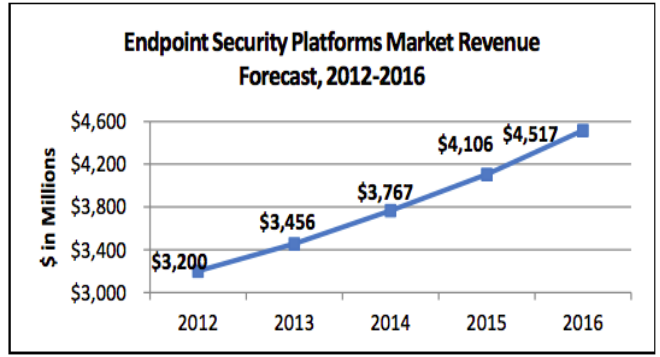
- PCs
- IP phones
- Mobile phones
- Consumer Electronics
- Machine-to-Machine

Endpoint security today

Monitor
- React to anomalous data/behavior
- Respond quickly to 0 day

Recover
- System repair

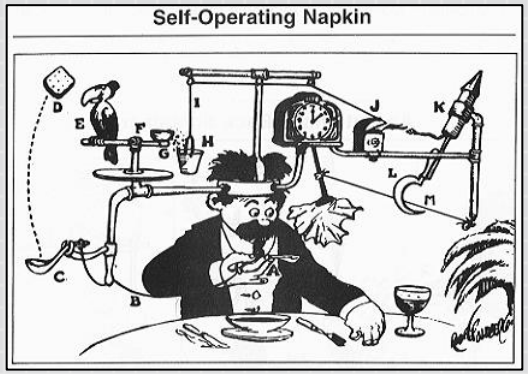
Manage
- Centralized policy enforcement
- Deployment management



Endpoint Security Platforms Market
The Radicati Group, Inc. (2014)

Endpoint security today

- Complexity hurts defense
  - Platform diversity
  - New platforms have terrible security
  - Lots of new apps
  - App logic smeared across cloud – device – IoT
- This is a classic machine learning situation
  - Machine recognition cuts through complexity
  - …but lousy against skilled adversaries
  - Result: race-to-update!
- Attackers are more subtle + deep (APT)
  - HARD to tune false positive vs. false negative



Rube Goldberg Archives

"car" "NOT car" delta

Intriguing properties of neural networks, Szegedy et al

CHOSE
NPLAI
NTEXT

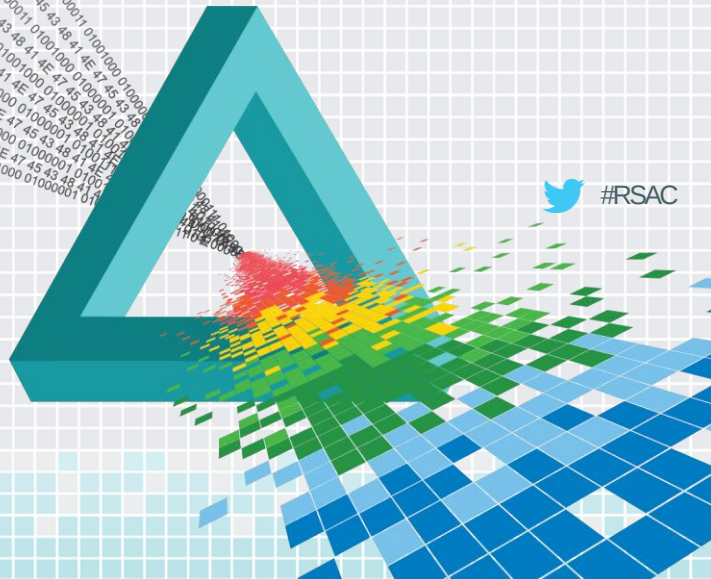
What lies ahead…

Application Portability

Device Federation

Complex Trust Domains

Internet of Things



Workspaces of the future

Global connectivity & collaboration
Instant access to different domains
Hierarchical control, security

**“Mobile [as a distinction] is dead
…I expect to use any screen”**

– Matias Duarte
VP of Design, Google

CHOSE
NPLAI
NTEXT

Application portability

Seamless sessions/data across independently managed endpoint devices.

- Securely “throw” an app to different device
  - Application bound to user, not device
  - Immediate, seamless response
  - Minimal admin (BYOD, friends house, hotel)

- **… when app and data really matter!**

CHOSE
NPLAI
NTEXT

Attackers target interoperability controls

- Example: HDCP secure content pipe
  - “High Bandwidth Digital Copy Protection”
  - Roles: Source [→ Repeater] → Sink
- Protects digital content, interoperability
  - Ease of use: Fast, offline, any-to-any
  - No one device contains global secret
- **Commercial exploit!**

but a group of 40 devices reveals it!

Number of KSVs	40	42	44	46	48	50
Prob. of Spanning M	.295	.773	.940	.982	.997	.999

A Cryptanalysis of the High-bandwidth Digital Content Protection System
(Crosby, Goldberg, Johnson, Song, Wagner)

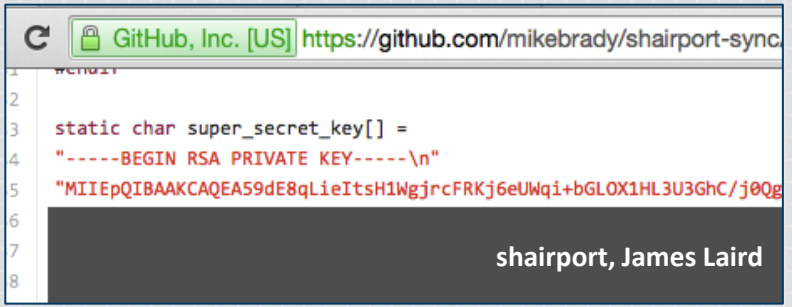
CHOSE
NPLAI
NTEXT

image from www.hdmi.org

Key management is hard

- Example: Apple Airplay

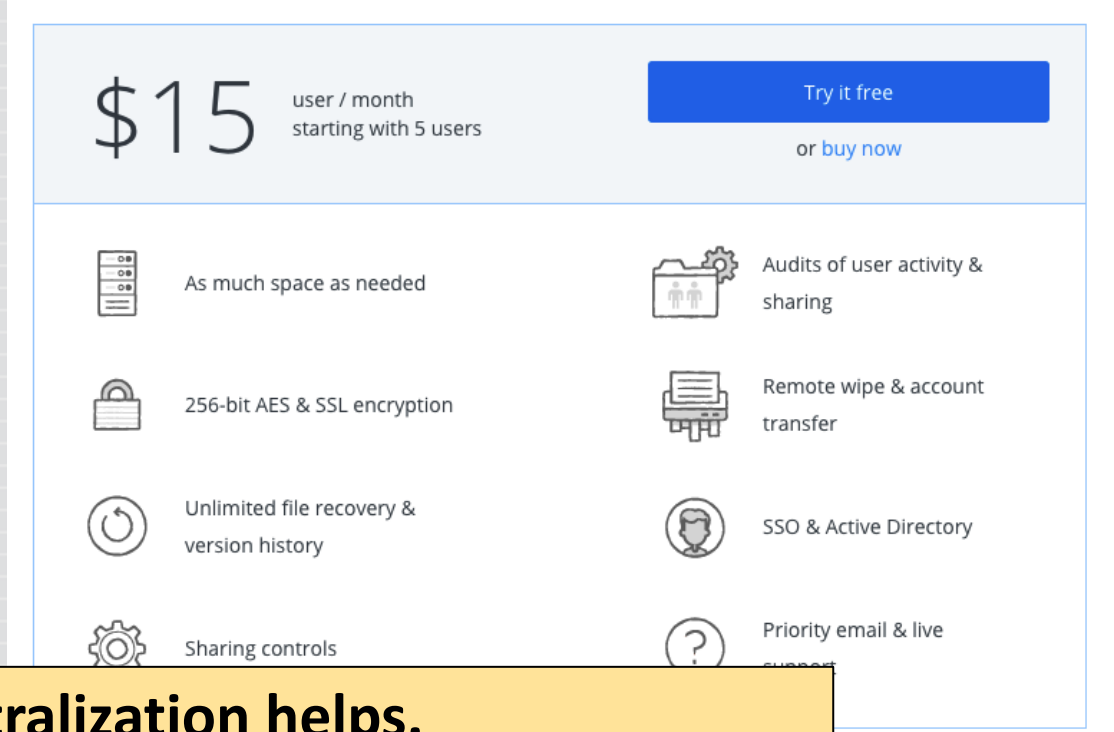
- Protects digital content, interoperability, **and** user binding
  - Fast, offline, any-to-any
  - Pipe + direct connection to Internet sources



- Security design
  - RSA keypairs for different roles
  - **Global keys extracted**

Policy centralization improves portability

- Cloud sync helps data portability
- **Sync + console greatly improve management tools**
- **But security of distributed data only as strong as weakest link**
- **Controls are coarse**



Centralization helps.
But device security is the limiting reagent.

www.dropbox.com (accessed 2/13/2015)

Software sandboxes not good enough

The Great Cloud Reboot of 2014

Xen Security Advisory CVE-2014-7188

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

                Xen Security Advisory CVE-2014-7188 / XSA-108
                              version 4

                Improper MSR range used for x2APIC emulation

UPDATES IN VERSION 4
====================

Public release.

ISSUE DESCRIPTION
=================

The MSR range specified for APIC use in the x2APIC access model spans
256 MSRs. Hypervisor code emulating read and write accesses to these
MSRs erroneously covered 1024 MSRs. While the write emulation path is
written such that accesses to the extra MSRs would not have any bad
effect (they end up being no-ops), the read path would (attempt to)
access memory beyond the single page set up for APIC emulation.

IMPACT
======
```

amazon web services™

rackspace

Content as threat vector

Abusing Blu-ray Players Pt. 1 - Sandbox Escapes

Friday February 27, 2015

tl;dr

In today's (28 February) closing keynote talk at the Abertay Ethical Hacking Society's Securi-Tay confe
how it was possible to build a malicious Blu-ray disc.

By combining different vulnerabilities in Blu-ray players we have built a single disc which will detect the
platform specific executable from the disc before continuing on to play the disc's video to avoid raising s
attacker to provide a tunnel into the target network or to exfiltrate sensitive files, for example.

Background

Blu-ray Disc™

https://www.nccgroup.com/en/blog/2015/02/abusing-blu-ray-players-pt-1-sandbox-escapes/

CHOSE
NPLAI
NTEXT

Secure user interface… elusive!

- Required for portability
  - UI isolation, privacy, integrity
  - But we don't have **local** secure UI!
- Guiding lights?
  - SE Linux has right focus on interfaces
  - PIN pad standards (DUKPT)
- But separated UI is good for security!
  - …did iMessage just kill SMS 2-factor?

CHOSE
NPLAI
NTEXT

http://blog.billguard.com/2014/07/look-easily-can-thwart-even-sophisticated-atm-skimmer/

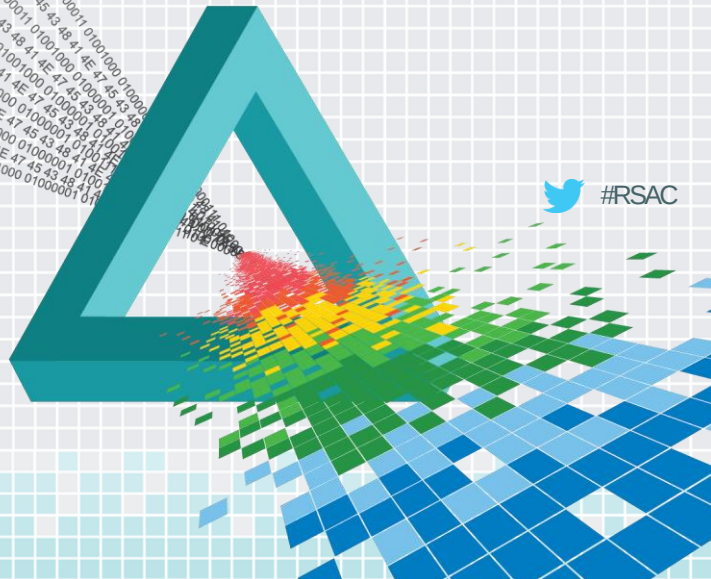
What lies ahead…

Application Portability

Device Federation

Complex Trust Domains

Internet of Things



Device federation

M2M peer cooperation

- To assess device environment
- For control + data flows
- When one device proxies a human

Need to discover, create, manage, and authenticate endpoint identities

Fridge: Marjan Lazarevski
S-beam: wonderhowto.com

…best practice for device federation?

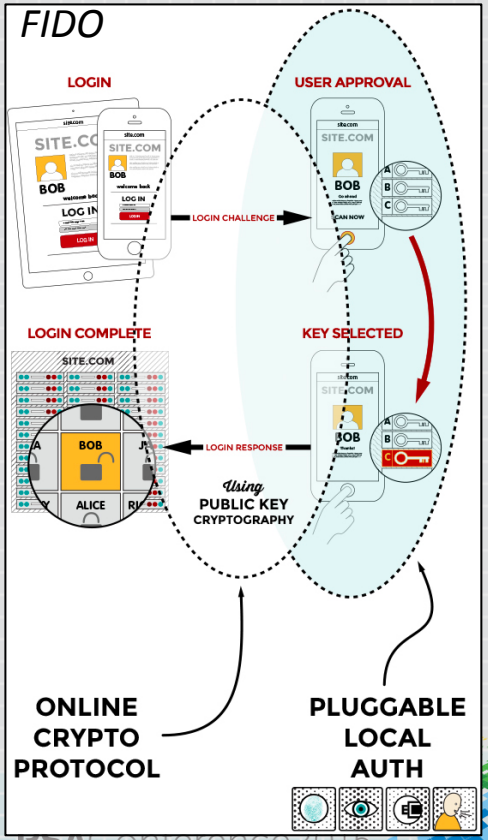
Problem: wifi-enroll a new printer

1. New printer defaults as open wifi AP
2. "HP Auto Wireless Connect"
   - Runs on your PC
   - Scrapes wifi access code from OS
   - Connects to printer AP and gives access code to printer
3. Printer joins your wireless network!

Genius or Scary?

Authentication standards filling out…

- Fast IDentity Online (FIDO) Alliance
  - **People** authentication
  - Leverages security features on user device
  - Agnostic to device authentication technology
- OAuth, OpenID
  - API access (**robot**) authentication
  - Client enrolled and given a key
- **…not M2M / endpoint solutions!**
  - Need device discovery, P2P connection



Decentralized device federation

Ease of 1st Connection

Degree of Centralization

Proximity & web-of-trust

Embedded agent

Enroll to local hub

Enroll to central service

CHOSE
NPLAI
NTEXT

Web of trust: www.linux.com
Bluetooth: cloudlink.soasta.com
CryptoManager: rambus.com
S-beam: wonderhowto.com

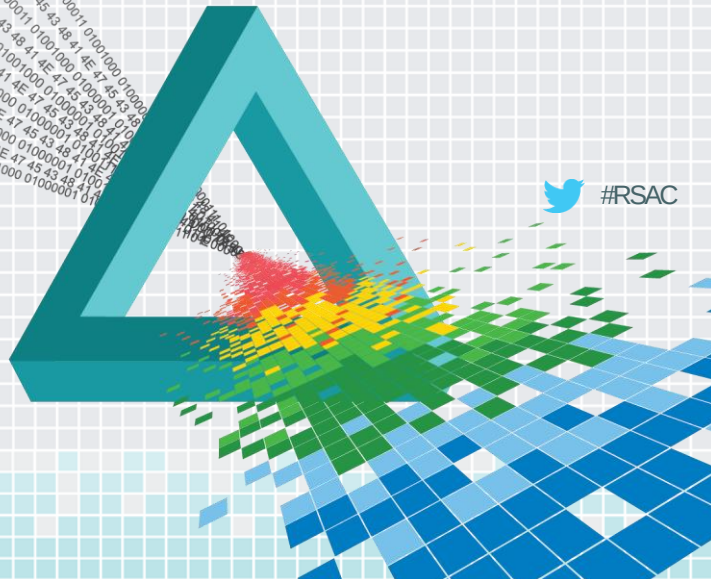
What lies ahead…

Application Portability

Device Federation

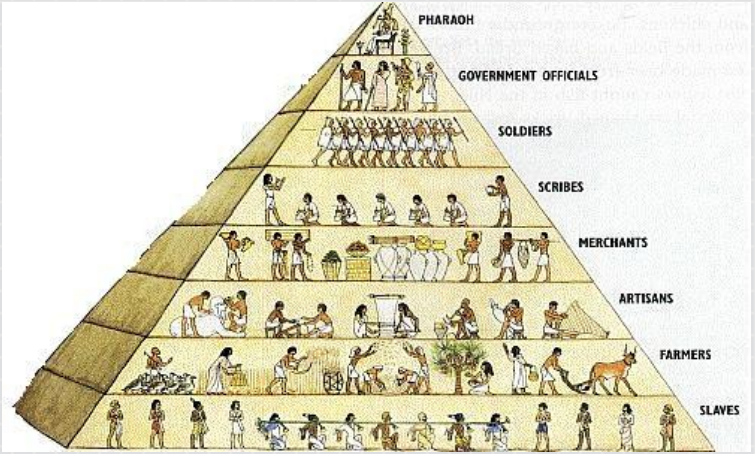
Complex Trust Domains

Internet of Things



The good old days (pre-2010)

- Hierarchical structure
  - Device Admin = Owner = Root
  - OS/BIOS in charge
  - Policies enforced via endpoint security product



- **Reality**
  - “Possession is nine tenths of the law”
  - Dangerous to do high-threat stuff on general IT platforms

Many cooks in the kitchen!

Entities	Privileges
Device owner	Run app
User(s)	Unlock data
Applications	Read location info
Application developer	Application keys
App store	Access to crash logs
BYOD administrator(s)	Platform attestation
Mobile carrier / system operator	Allow SW update
OS vendor	Debug unlock
Device manufacturer	Privileged developer hooks
Chip manufacturer	Peripheral authentication
	Encrypted key store

Pressure on trust boundaries

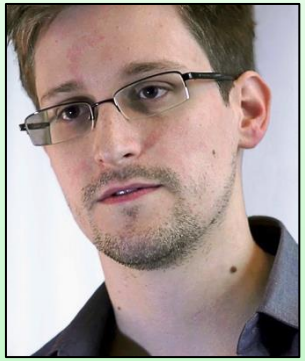
Apple Pay

UltraViolet

VISA

NETFLIX

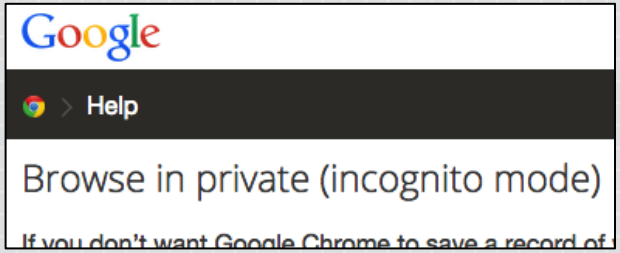
- App doesn't trust user
- App doesn't trust root
- User cannot touch app's keys



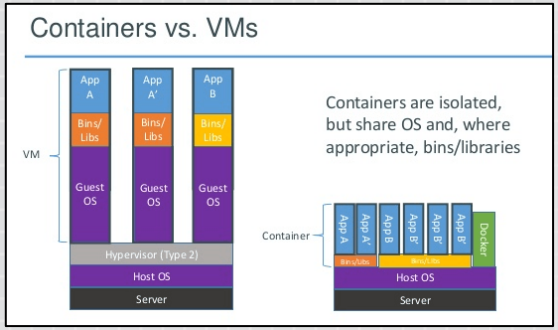
- Nobody trusts the software
- Auditable privilege limits
- No single administrator: multiple, limited authorities

CHOSE
NPLAI
NTEXT

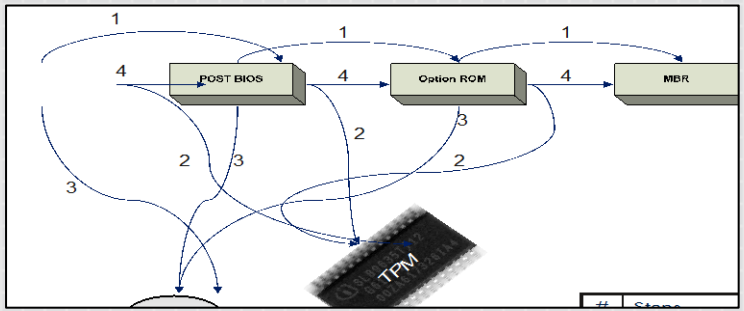
Well intentioned but limited



Red/black isolation too simplistic



Sandboxes incomplete, make developers lazy

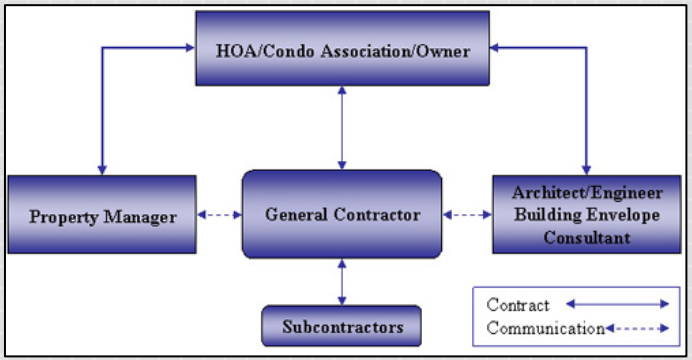


TPM attestation not for complex SW

Key rolling w/o device robustness?

~~One ring to rule them all?~~ Condominium HOA model

- **Multiple "owners", transparent limits, privilege transfers, situational override, auditable logs and limits**
  - Not trusted: Root / OS / vendor / govt
- Platform enforces data/program domains
- Privilege handoffs over device lifecycle
- Can remotely audit system attributes
- **Enforced in <u>HW</u>, not by OS**



CHOSE NPLAI NTEXT

Chart: Credo Construction

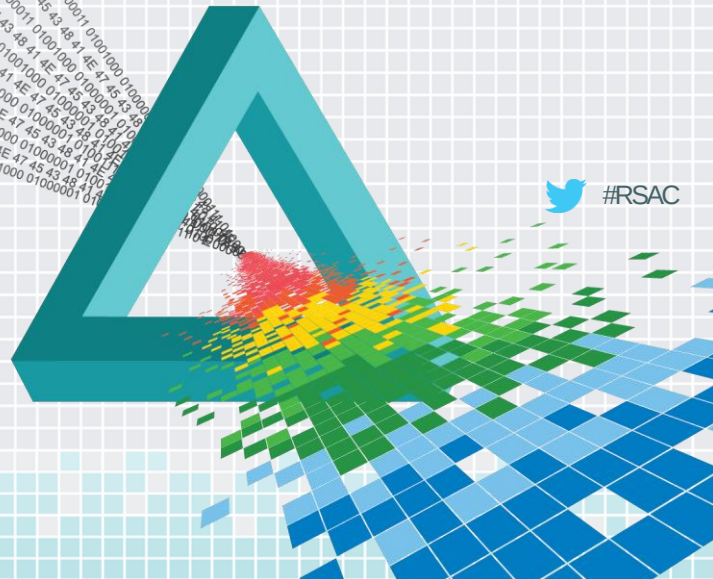
What lies ahead…

Application Portability

Device Federation

Complex Trust Domains

Internet of Things



The Internet of Things

The physical world is becoming a type of information system [with] sensors and actuators embedded in physical objects...

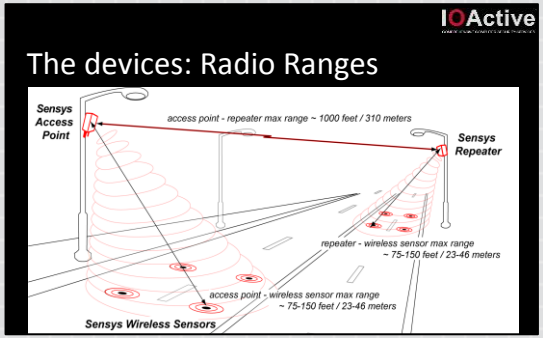
When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it.

– *McKinsey & Company*

Challenge: Break physical stuff, at scale

- Enron fakes grid transactions to manipulate market (2001)
- Stuxnet targets programmable logic controller (2010)
- IOActive demo'd vulnerabilities in Washington DC traffic management system, (2014)

Siemens Simatic S7-315



Hacking US Traffic Control Systems
Cesar Cerrudo, IOActive

Challenge: Time and Place

- IoT policies sensitive to **time/location**
  - App logic, pricing, proximity assessment, identity, pairing, DRM, …
- Today's approaches **spoofable**, **not private**

Captured RQ-170 Sentinel

- Prediction: Chipset cores for environment attestation
  - Independent CPU maintains GPS + time history
  - Digitally sign data, traceable to module security certification

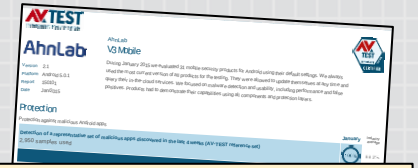
CHOSE NPLAI NTEXT

Christian Science Monitor 12/15/2011

Challenge: IoT device maintainabiliy

- Unmanaged IoT **hard to update**, **no clear owner**, **no mgmt $**
  - But today's endpoint security relies on updates!
- IoT infrastructure has **5x longer field life** than mobile device
- System components have **short lived support**
  - Chipset SW team builds Board Support Package (BSP)
  - ODM copies BSP, doesn't know innards
  - Product vendor makes minimal customization

…will the last one in the building patch the vulnerability?



Malware detection test: "We use only recent malware, which is **not older than 4 weeks**."

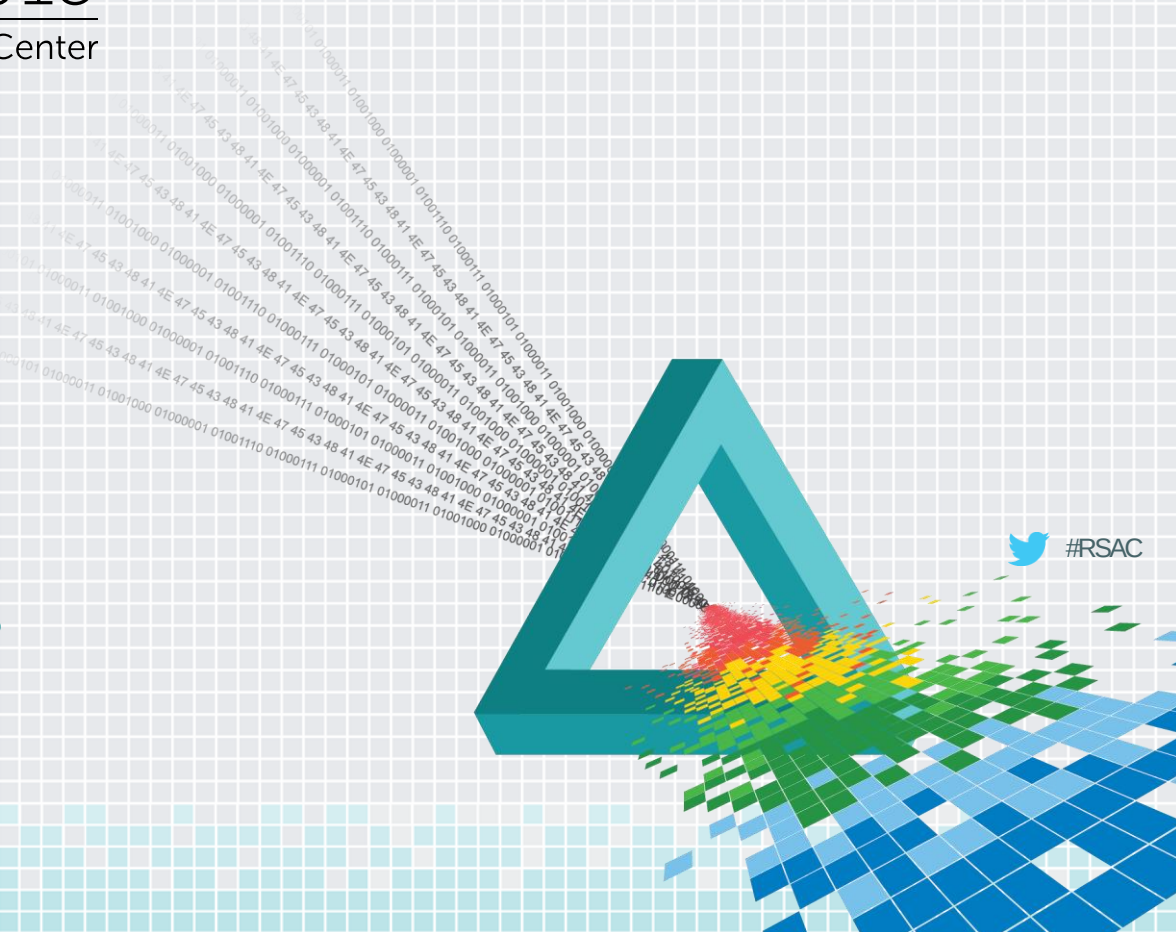
AV-TEST Independent IT-Security Institute
Android Testing Methodology (2013)

CHOSE
NPLAI
NTEXT

RSAConference2015

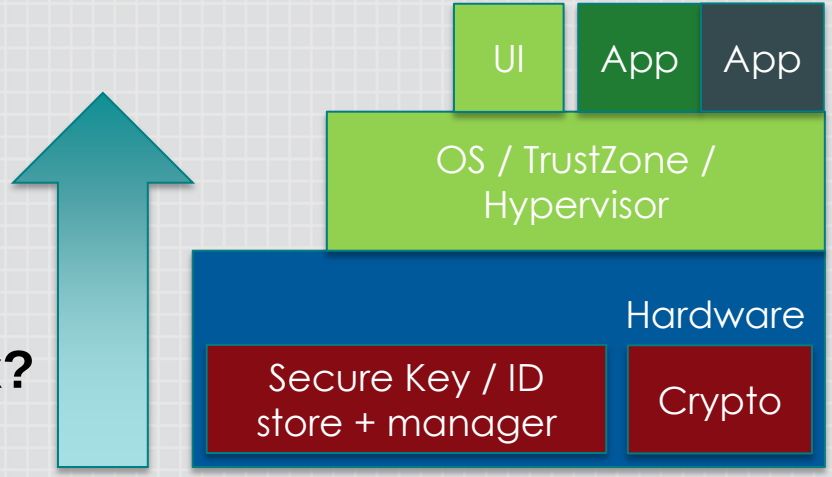
San Francisco | April 20-24 | Moscone Center

Healthy Endpoints



Endpoint foundation

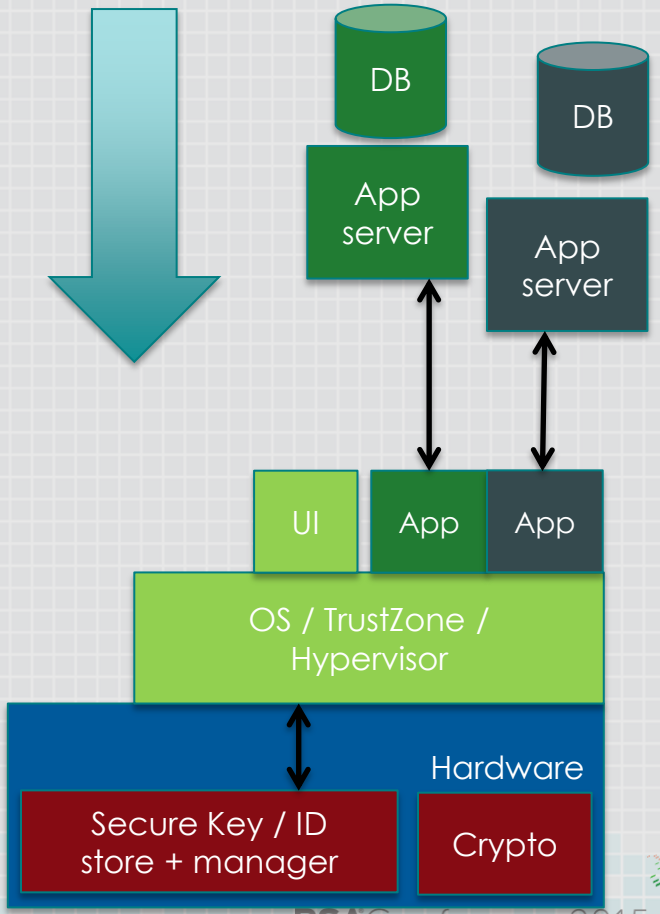
- **What gets to run on the platform?**
  - Boot / code authentication
  - Secure debug lock
- **Do my secrets remain opaque?**
  - Application partitioning
  - Hardware-based secure key storage
- **Am I in the real world or the matrix?**
  - Environment attestation
  - Peripheral authentication



CHOSE NPLAI NTEXT

Trust from the top down

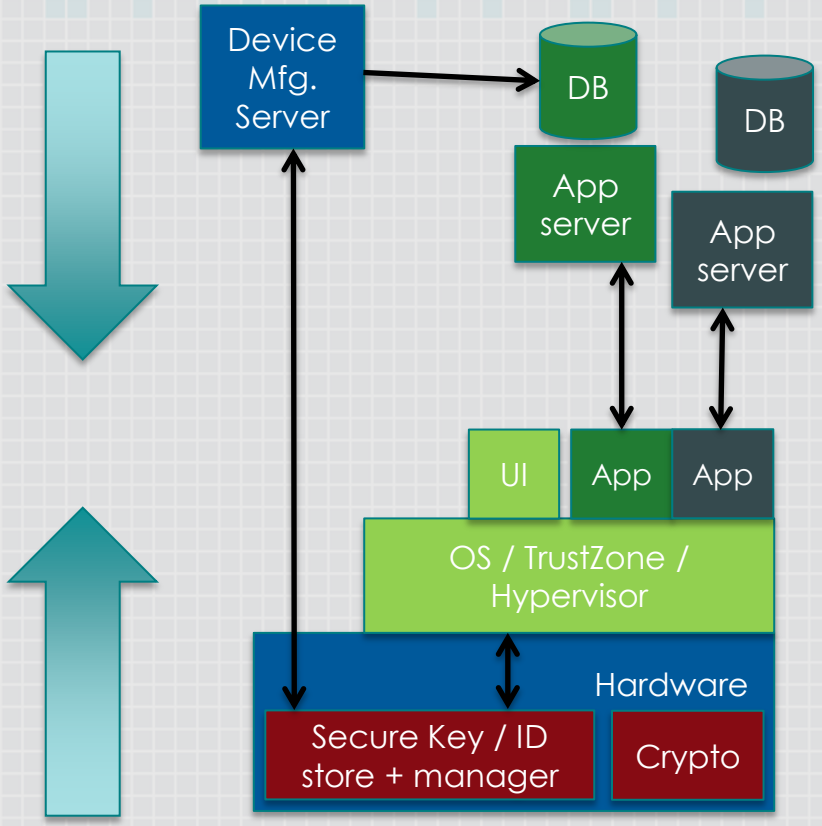
- Device enrollment
- App deployment & updates
- System audit & risk management
- Online revocation
- Policy management



Trust meets in the middle

Identity + key provisioning
Authentication service
Policy management
Security updates

Identity + key management
Sandboxed secrets
Partitioning of critical state
Reliability & integrity



Apply what you have learned

- **Near term**
  - Understand endpoint security systems (walk show floor!)
- **Mid term**
  - Understand the limits of your endpoint tools
  - Appreciate where your roadmap deviates from your security tools
  - Employ platform security building blocks
- **Long term**
  - Advocate for platform improvements

Endpoints In the New Age

Application Portability

Device Federation

Complex Trust Domains

Internet of Things

Questions?

@BenjaminJun

ben@ChosenPlaintext.com