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

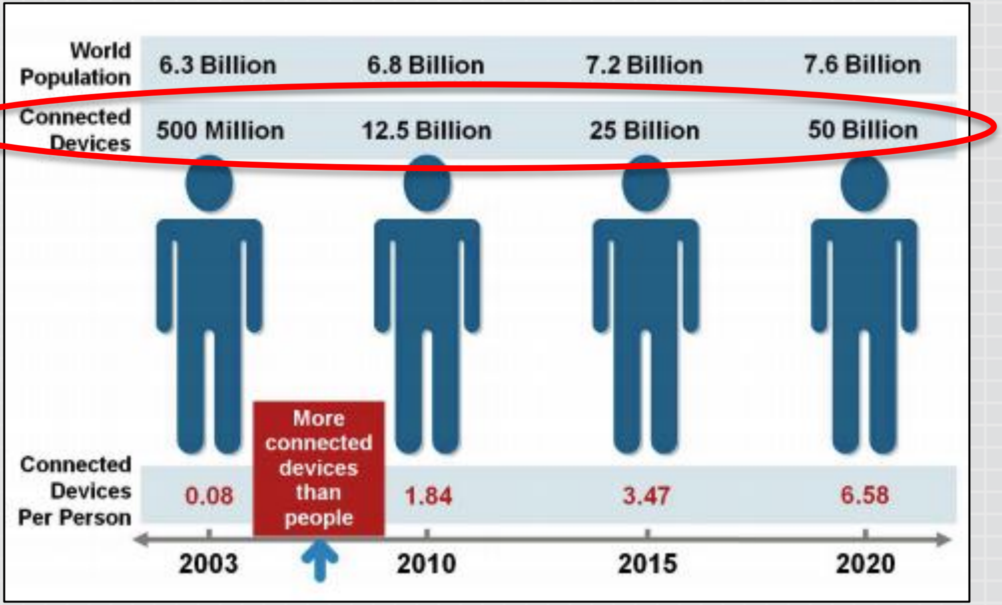
@BenjaminJun

CHOSE
NPLAI
NTEXT

#RSAC

v18

Lots of connected devices!



	2003	2010	2015	2020
World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Connected Devices Per Person	0.08	1.84	3.47	6.58

Source: Cisco

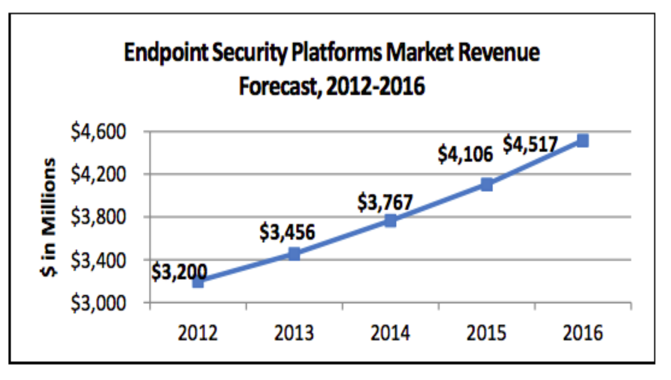
- PCs
- IP phones
- Mobile phones
- Consumer Electronics
- Machine-to-Machine

Endpoint security today

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

Recover
- System repair

Manage
- Centralized policy enforcement
- Deployment management

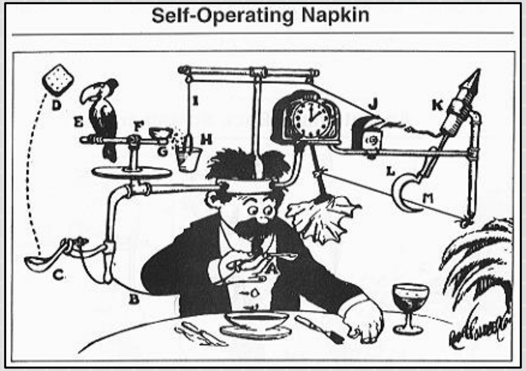


Endpoint Security Platforms Market
The Radicati Group, Inc. (2014)

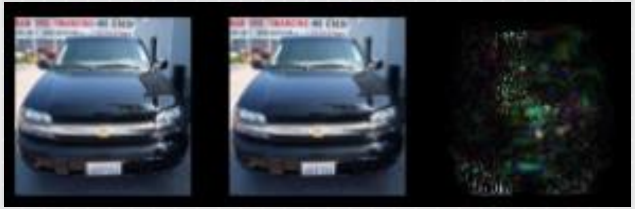
CHOSE
NPLAI
NTEXT

Endpoint security today

- Complexity hurts defense
  - Platform diversity – new ones have poor security
  - Lots of apps, smeared across cloud / device / IoT
- Machine learning has limits
  - 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

What lies ahead…

- **Internet of Things**
- Device Federation
- Application Portability
- Complex Trust Domains

The Internet of Things

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

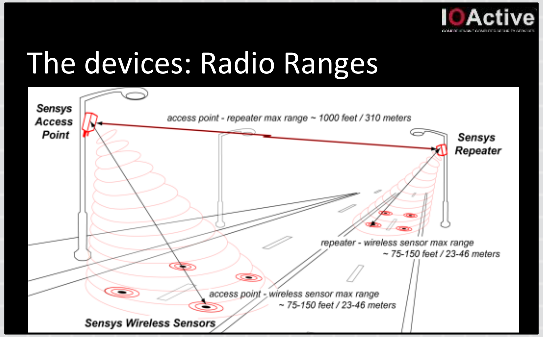
When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it.

– 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



IOActive

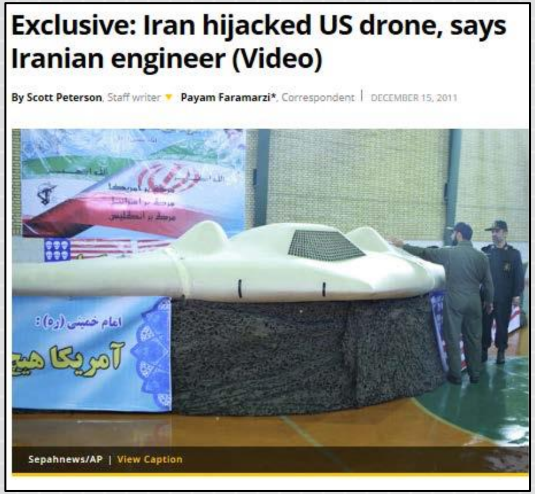
The devices: Radio Ranges

Sensys Access Point
access point - repeater max range ~ 1000 feet / 310 meters
Sensys Repeater
repeater - wireless sensor max range ~ 75-150 feet / 23-46 meters
access point - wireless sensor max range ~ 75-150 feet / 23-46 meters
Sensys Wireless Sensors

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 **not private**, **spoofable**
- Prediction: Chipset cores for environment attestation
  - Independent CPU maintains GPS + time history
  - Digitally sign data, traceable to module security certification



Exclusive: Iran hijacked US drone, says Iranian engineer (Video)

By Scott Peterson, Staff writer · Payam Faramarzi*, Correspondent | DECEMBER 15, 2011

Sepahnews/AP | View Caption

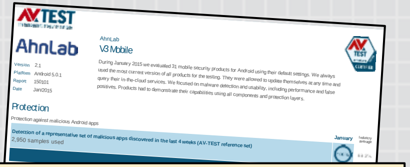
Captured RQ-170 Sentinel

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 builds device functionality
  - Product vendor makes customization

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



AhnLab
V3 Mobile

Version	2.1
Platform	Android 5.0.1
Report	150101
Date	Jan/2015

During January 2015 we evaluated 31 mobile security products for Android using their default settings. We always used the most current version of all products for the testing. They were allowed to update themselves at any time and query their in-the-cloud services. We focused on malware detection and usability, including performance and false positives. Products had to demonstrate their capabilities using all components and protection layers.

Protection

Protection against malicious Android apps

Detection of a representative set of malicious apps discovered in the last 4 weeks (AV-TEST reference set)
2,950 samples used

January
Industry average

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)

What lies ahead…

Internet of Things

Device Federation

Application Portability

Complex Trust Domains

Device federation

M2M peer cooperation

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

Google Cloud Print Ready

Wi-Fi PROTECTED SETUP

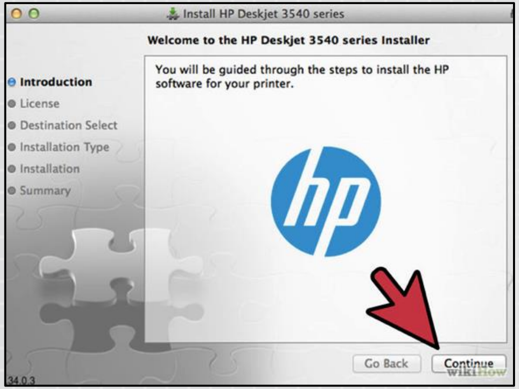
Need to discover, create, manage, and authenticate <u>endpoint</u> identities

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!



Install HP Deskjet 3540 series

Welcome to the HP Deskjet 3540 series Installer

- Introduction
- License
- Destination Select
- Installation Type
- Installation
- Summary

You will be guided through the steps to install the HP software for your printer.

www.wikihow.com

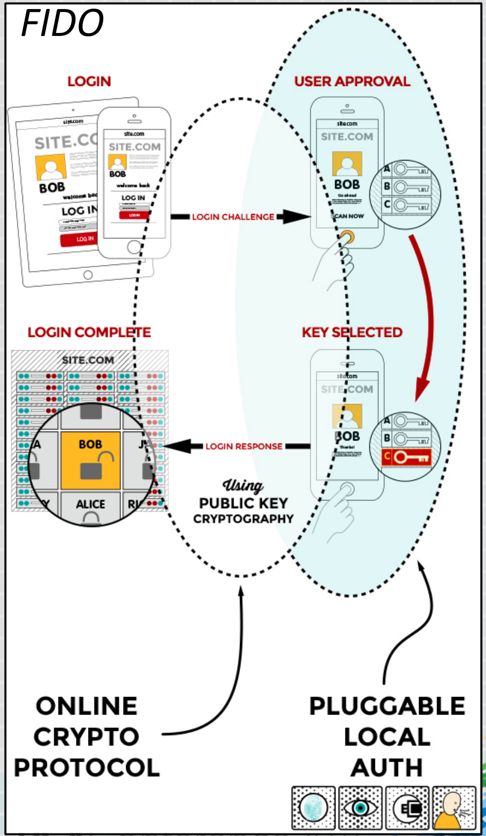
Genius or Scary?

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

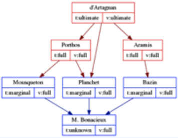
- **…not M2M / endpoint solutions!**
  - Need device discovery, P2P connection



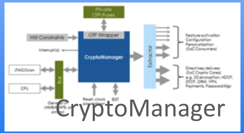
Decentralized device federation

Ease of 1st Connection

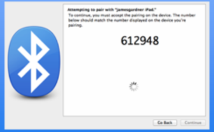
Proximity & web-of-trust



Embedded agent



Enroll to local hub



Attempting to pair with "jamesgardiner iPad."

To continue, you must accept the pairing on the device. The number below should match the number displayed on the device you're pairing.

612948

Wi-Fi PROTECTED SETUP™

Enroll to central service

box

Google Cloud Print Ready

Dropbox

Degree of Centralization

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

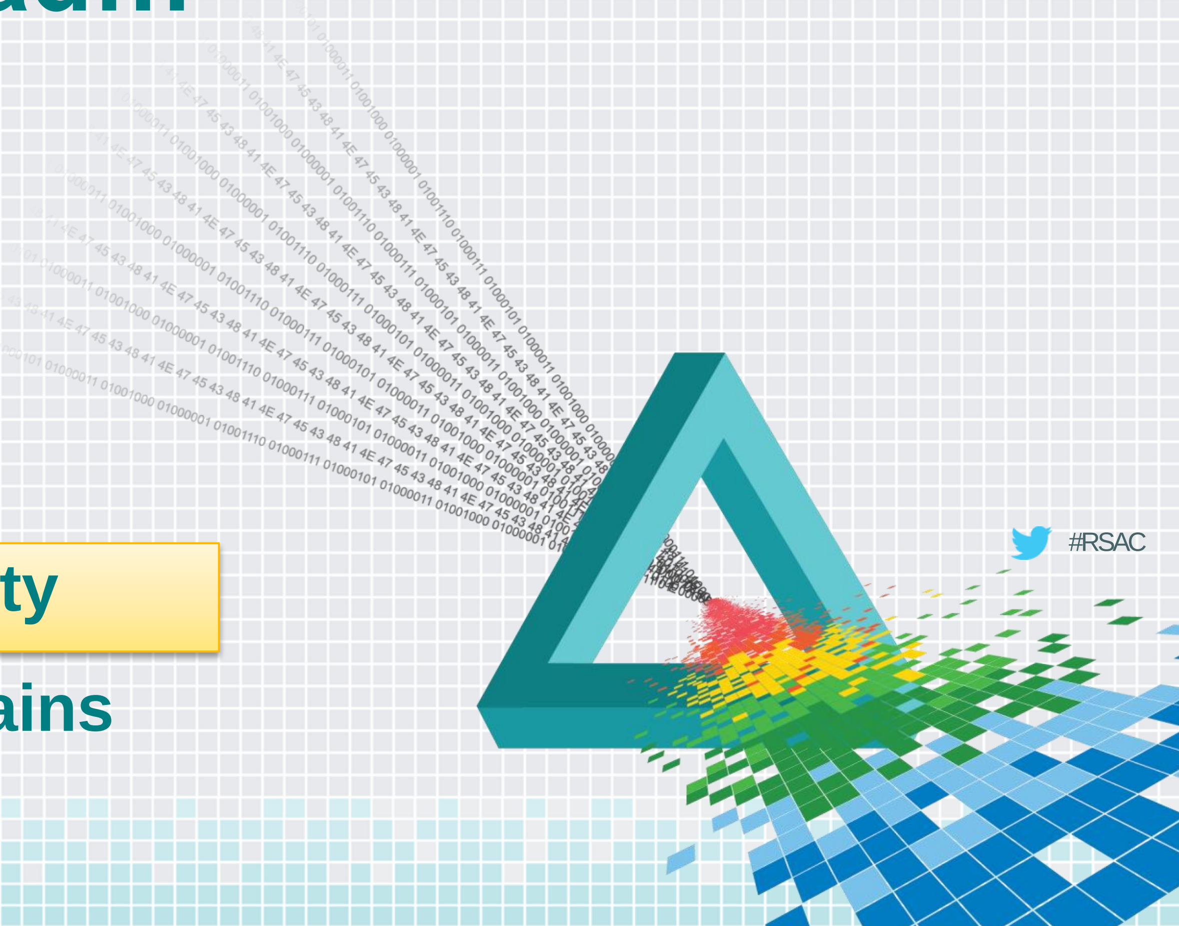
What lies ahead…

Internet of Things

Device Federation

Application Portability

Complex Trust Domains



Workspaces of the future

Instant global connectivity
Cross-domain collaboration
Hierarchical control

**“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 across independently managed devices.

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

- **When app and data <u>really matter</u>!**

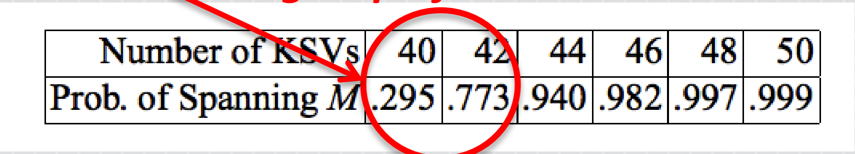
BBC Secret Fortune app

PadRacer (SMHK Funlab)

Attackers target interoperability controls

- Example: HDCP content pipe
  - “High Bandwidth Digital Copy Protection”
- 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

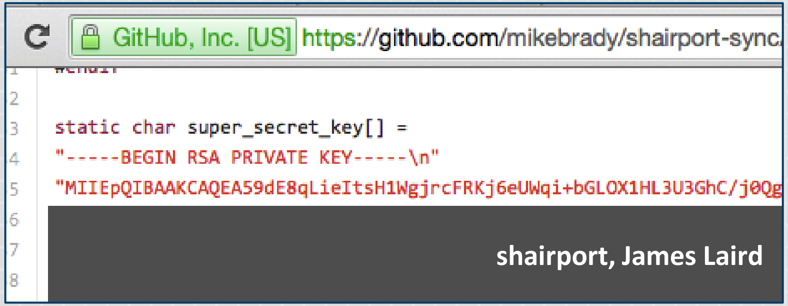
A Cryptanalysis of the High-bandwidth Digital Content Protection System
(Crosby, Goldberg, Johnson, Song, Wagner)

image from www.hdmi.org

App control is bound to keys... manage them well!

- 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**

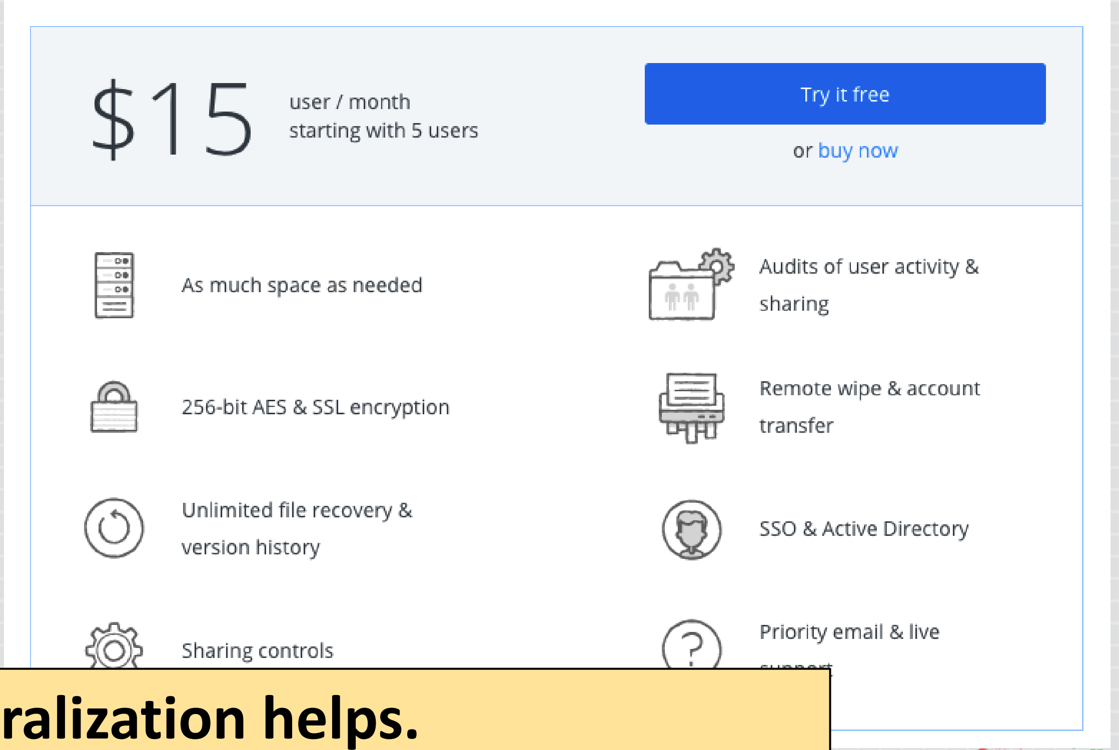


```
static char super_secret_key[] =
"-----BEGIN RSA PRIVATE KEY-----\n"
"MIIEpQIBAAKCAQEA59dE8qLieItsH1WgjrcFRKj6eUWqi+bGLOX1HL3U3GhC/j0Qg
```

shairport, James Laird

Portability requires centralized policies

- 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**



$15 user / month
starting with 5 users

As much space as needed

Audits of user activity & sharing

256-bit AES & SSL encryption

Remote wipe & account transfer

Unlimited file recovery & version history

SSO & Active Directory

Sharing controls

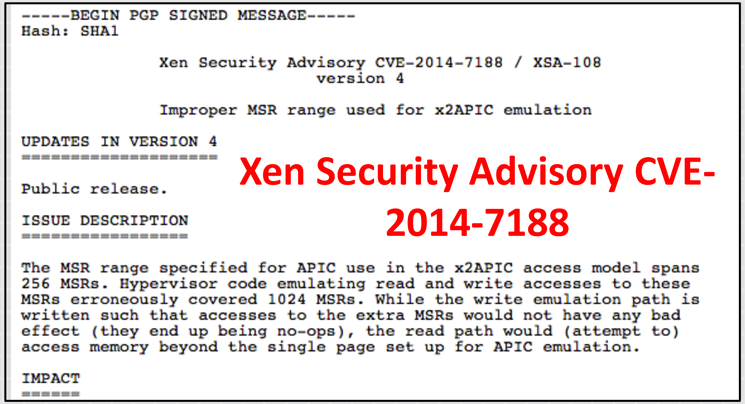
Priority email & live support

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

Centralization helps.
But device security is the limiting reagent!

Portability requires sandboxing
… but are software sandboxes robust?

The Great Cloud Reboot of 2014



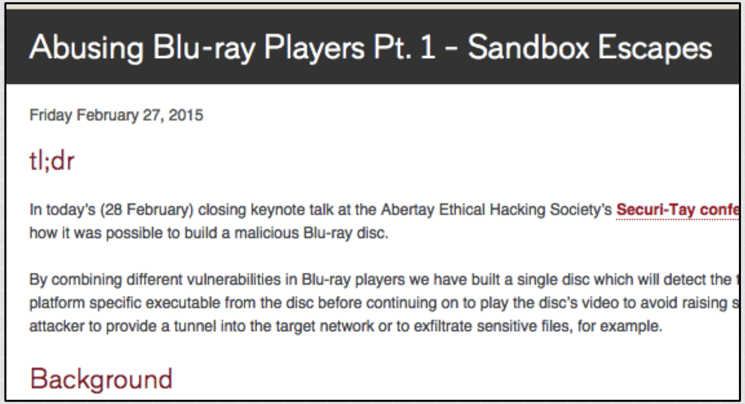
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

            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
======
```

Xen Security Advisory CVE-2014-7188

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 t
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/

Portability requires secure UI … but we can’t even do this locally!

- User interface == communication channel
  - Isolation, privacy, integrity
  - Many groups working on this
- Guiding lights?
  - SE Linux has right focus on interfaces
  - PIN pad standards (DUKPT)
- Um, 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/

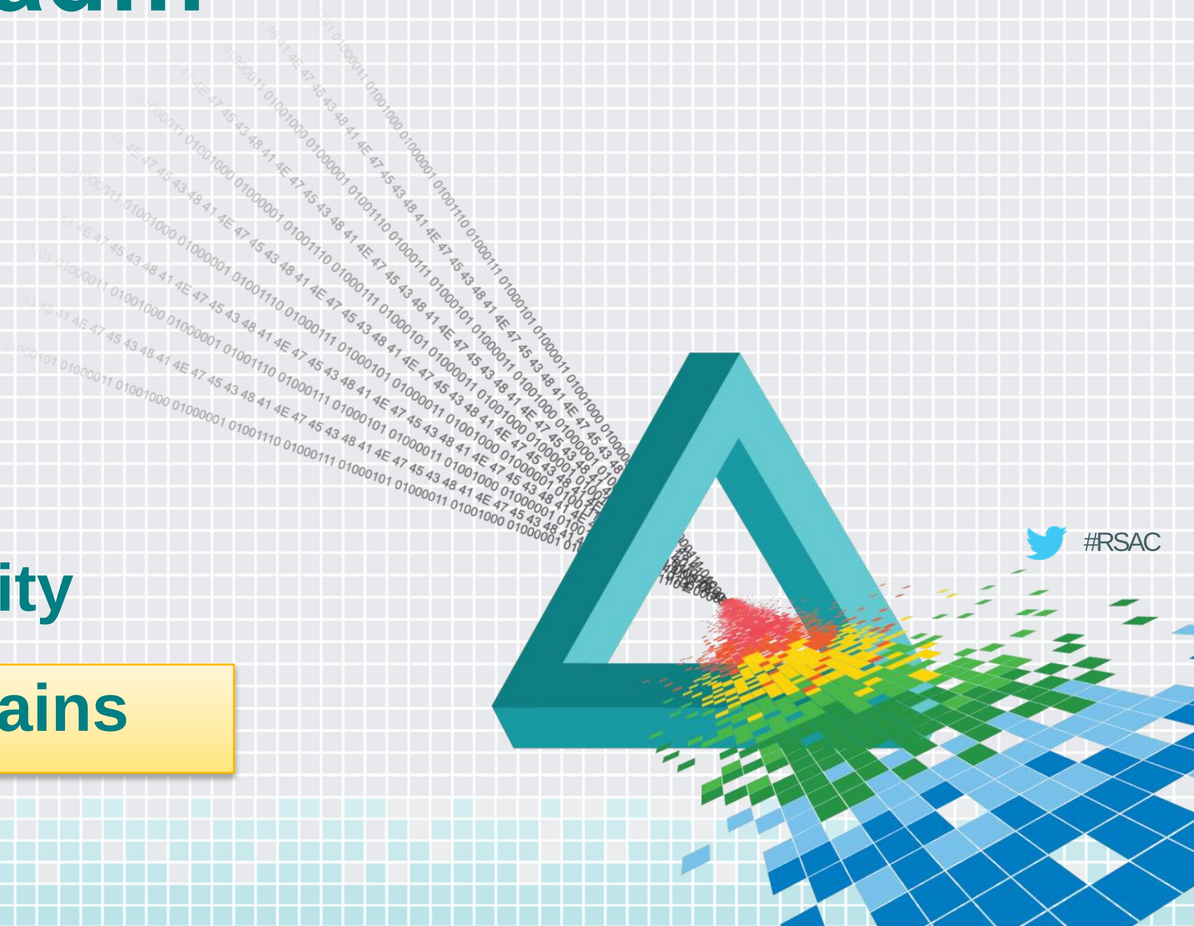
What lies ahead…

Internet of Things

Device Federation

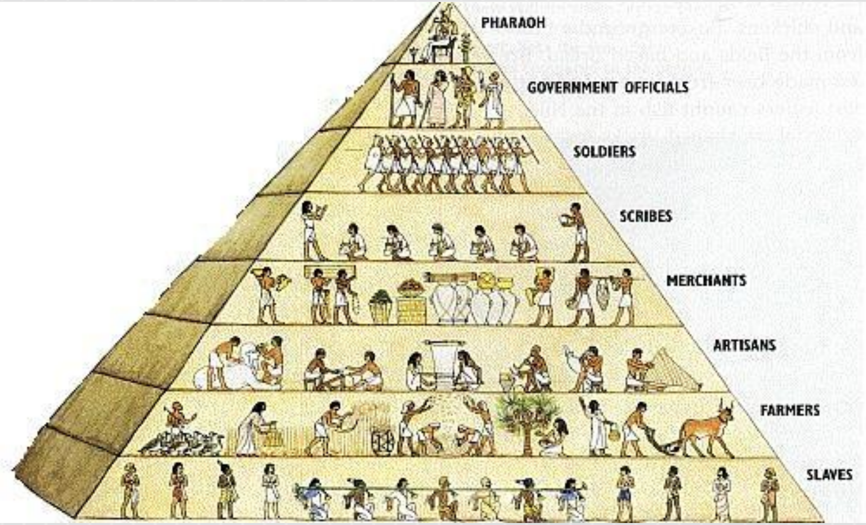
Application Portability

Complex Trust Domains



The good old days (pre-2010)

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



- Reality: “Possession is nine tenths of the law”

CHOSE
NPLAI
NTEXT

www.historyforkids.net

Many cooks in the kitchen!

Entities

Device owner

User(s)

Applications

Application developer

App store

BYOD administrator(s)

Mobile carrier / system operator

OS vendor

Device manufacturer

Chip manufacturer

Privileges

Run app

Unlock data

Read location info

Application keys

Access to crash logs

Platform attestation

Allow SW update

Debug unlock

Privileged developer hooks

Peripheral authentication

Encrypted key store

Pressure on trust boundaries

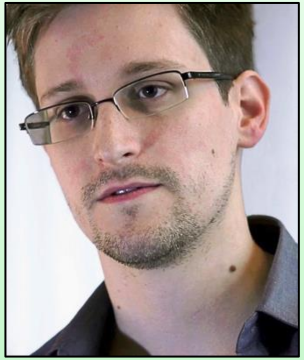
Pay

UV
ULTRA
VIOLET

VISA

NETFLIX

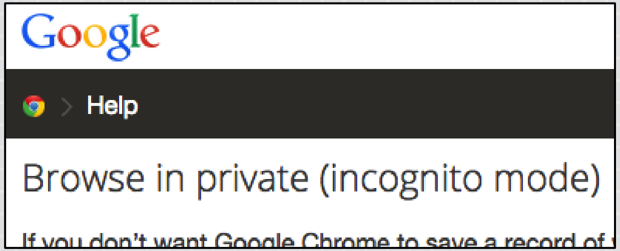
- App doesn’t trust user
- App doesn’t trust root
- User cannot touch app’s keys



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

CHOSE
NPLAI
NTEXT

Well intentioned but limited



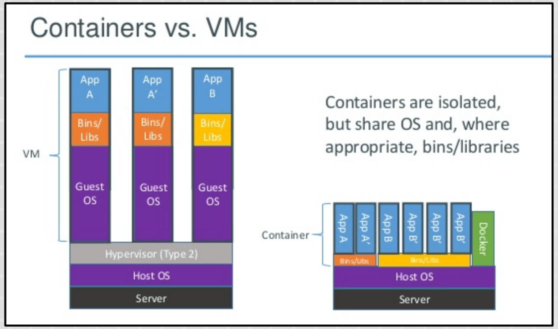
Google

Help

Browse in private (incognito mode)

If you don't want Google Chrome to save a record of y

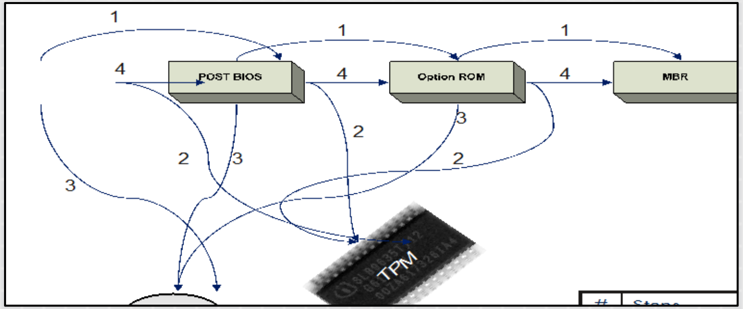
Red/black isolation too simplistic



Containers vs. VMs

Containers are isolated, but share OS and, where appropriate, bins/libraries

Sandboxes incomplete, make developers lazy



TPM attestation not for complex SW

Key rolling w/o device robustness?

CHOSE
NPLAI
NTEXT

eventwristbands.com
Infineon TPM overview, 2008
Docker

~~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 HW, not by OS**

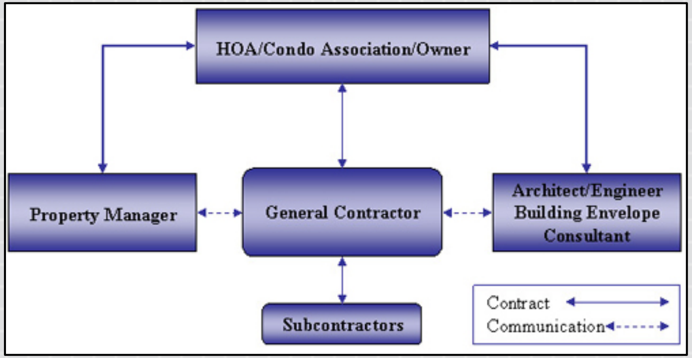
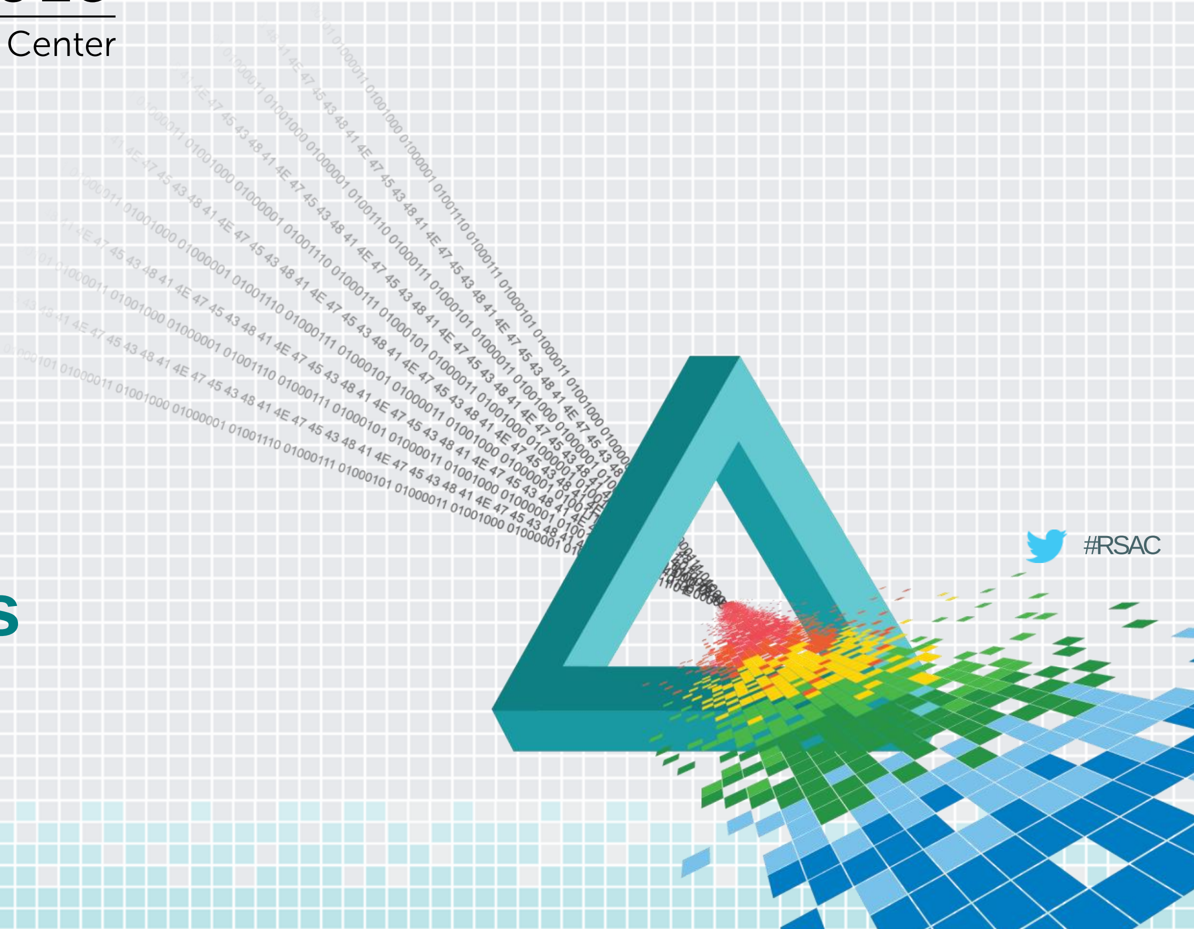

HOA/Condo Association/Owner
Property Manager
General Contractor
Architect/Engineer Building Envelope Consultant
Subcontractors
Contract
Communication

Chart: Credo Constructio

RSAConference2015

San Francisco | April 20-24 | Moscone Center

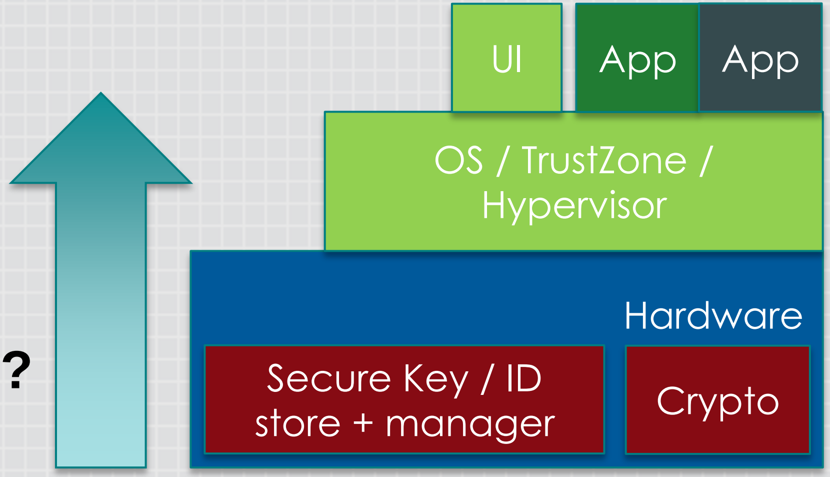
Healthy Endpoints



#RSAC

Endpoint foundation

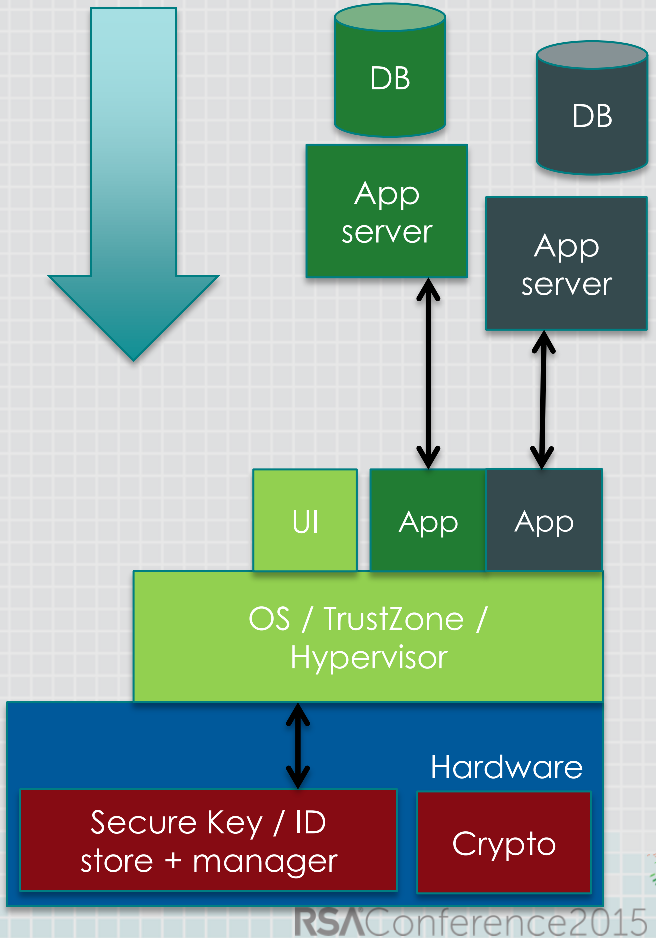
- **What gets to run on the platform?**
  - Boot / code authentication
  - Secure debug lock
- **Do my secrets remain opaque?**
  - Application partitioning
  - Hardware-based secure key storage
- **Am I in the real world or the matrix?**
  - Environment attestation
  - Peripheral authentication



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

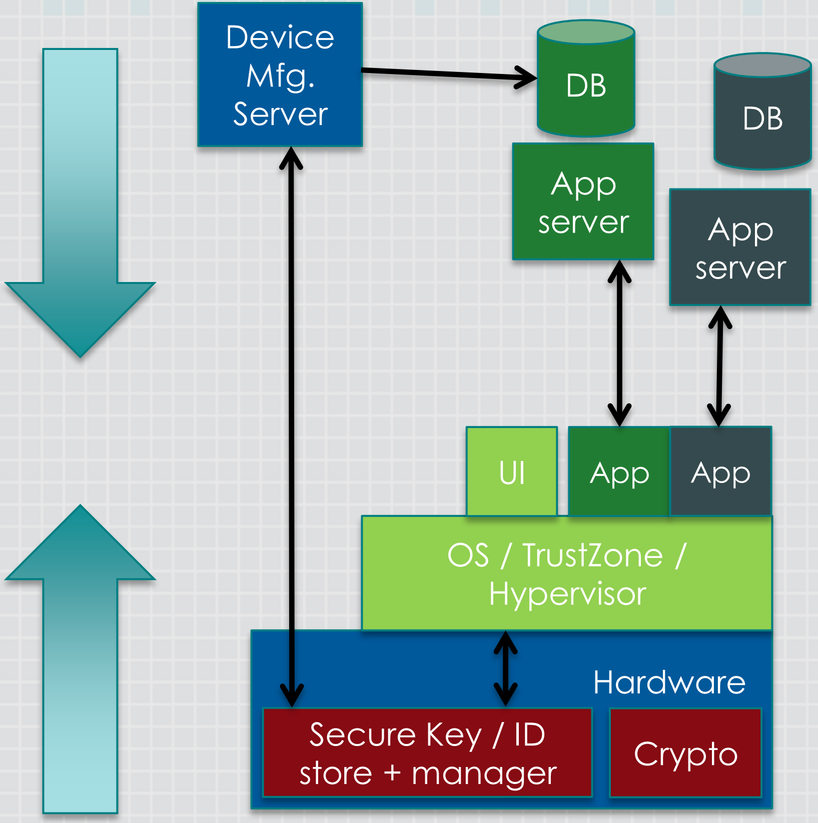
Security updates

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**
  - Appreciate where your roadmap deviates from your endpoint tools
  - Use available security building blocks!

- **Long term**
  - Advocate for platform improvements

Endpoints In the New Age

Questions?

@BenjaminJun

ben@ChosenPlaintext.com

Internet of Things

Device Federation

Application Portability

Complex Trust Domains