Why TPM 2.0?

Reasons for Upgrade;
Use Cases for the Latest Release of the TPM Specification

06/17/15

Dave Challener

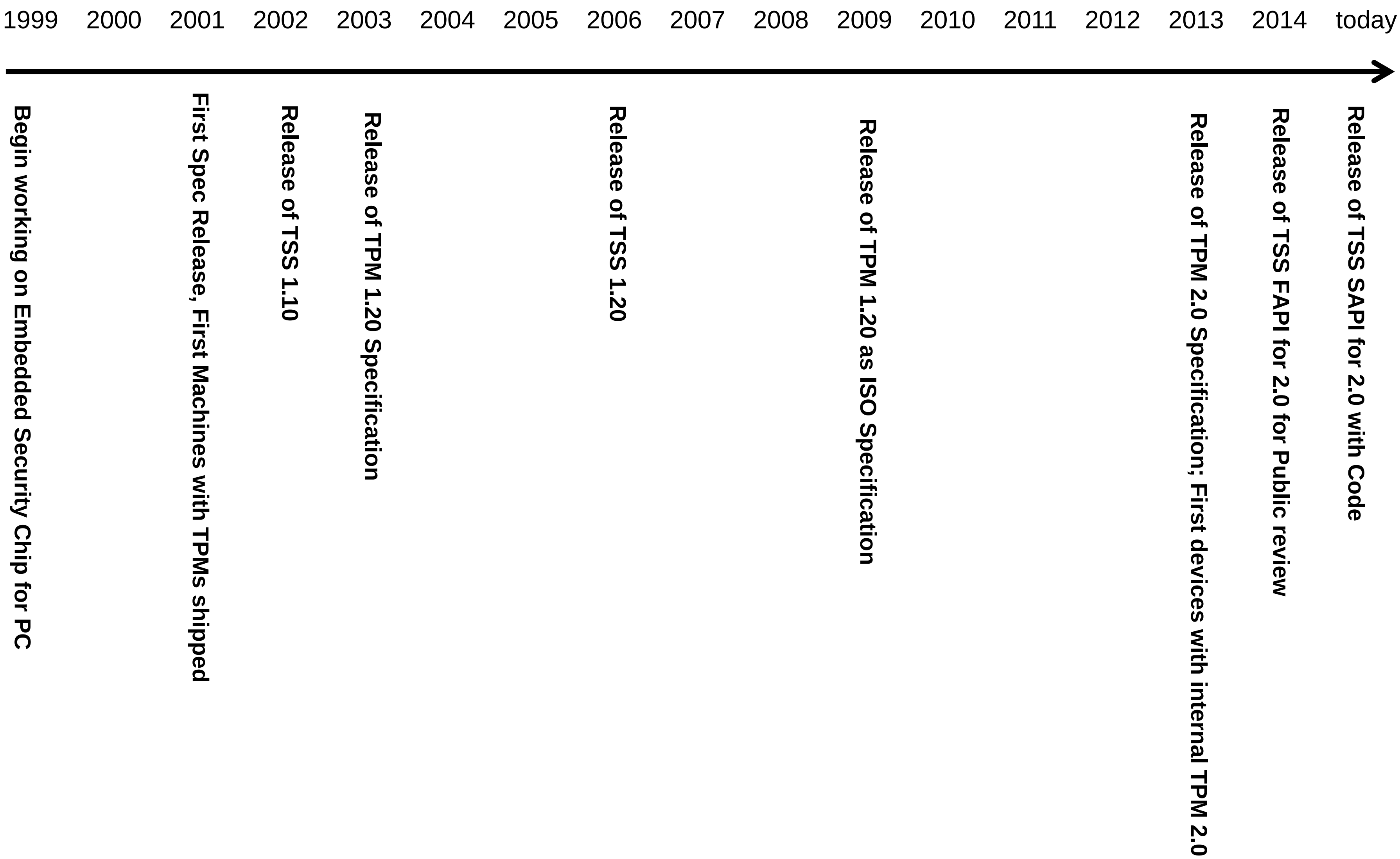
APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Level Setting: What is a TPM?

- A Security Co-Processor
  - Public Private Key Operations
    - Key Creation
    - Key signing
    - Key exchange
  - Non-Volatile Storage
    - Access protected
  - Symmetric encryption
    - HMAC operations
    - Limited symmetric encryption

- Purely Passive
  - It does NOT monitor your system

Level Setting: What is a TPM?



1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 today

Begin working on Embedded Security Chip for PC

First Spec Release, First Machines with TPMs shipped

Release of TSS 1.10

Release of TPM 1.20 Specification

Release of TSS 1.20

Release of TPM 1.20 as ISO Specification

Release of TPM 2.0 Specification; First devices with internal TPM 2.0

Release of TSS FAPI for 2.0 for Public review

Release of TSS SAPI for 2.0 with Code

Two Questions

- **Why was the Specification upgraded from 1.2?**
  - **Over 1 Billion served**

- **Why do I care?**
  - **How can I make use of TPMs to solve my current problems?**

Why the Change from 1.2?

- Security
  - TPM 1.2 was built around SHA-1
    - The algorithm was embedded in all structures
    - There wasn’t room enough to simply change to SHA256

- Complexity
  - TPM 1.2 had grown “organically” after 1.1b
  - It was unnecessarily complicated

- Ease of use
  - TPM 1.2 was hard to use
  - Complexity of authorization

- New Functionality
  - Algorithm flexibility
  - Unified Authorization
  - Fast Key loading

- Fred Brooks: “The management question, therefore, is not *whether* to build a pilot system and throw it away. You *will* do that. […] Hence *plan to throw one away; you will, anyhow.”*

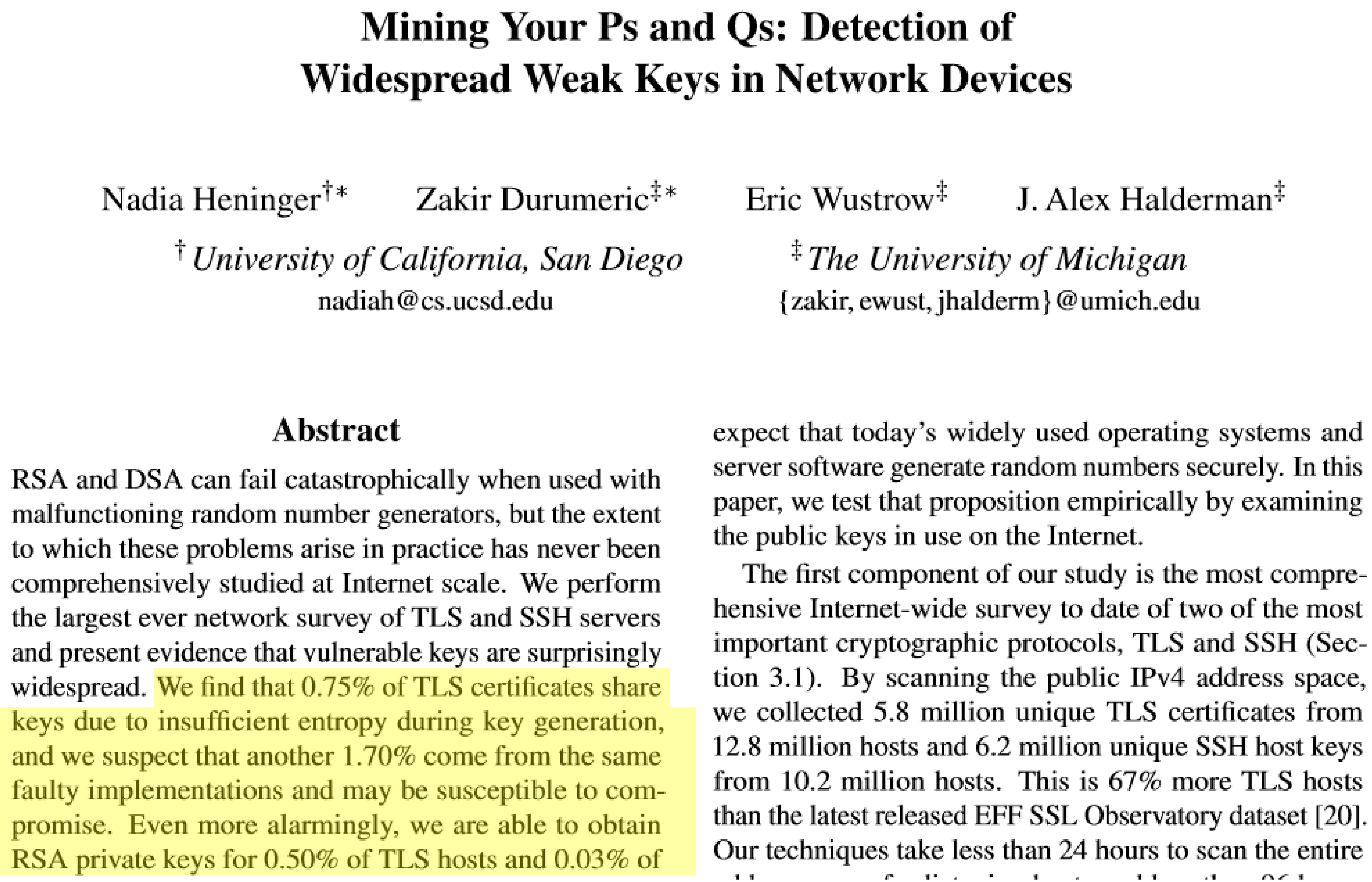
Why Use a TPM 2.0?

- Problems that can be solved/ameliorated with TPMs
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - **Poor entropy leading to weak keys**
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

Poor Entropy Sources Lead to Weak Keys



Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

Nadia Heninger[†*] Zakir Durumeric[‡*] Eric Wustrow[‡] J. Alex Halderman[‡]

[†] *University of California, San Diego*
nadiah@cs.ucsd.edu

[‡] *The University of Michigan*
{zakir, ewust, jhalderm}@umich.edu

Abstract

RSA and DSA can fail catastrophically when used with malfunctioning random number generators, but the extent to which these problems arise in practice has never been comprehensively studied at Internet scale. We perform the largest ever network survey of TLS and SSH servers and present evidence that vulnerable keys are surprisingly widespread. We find that 0.75% of TLS certificates share keys due to insufficient entropy during key generation, and we suspect that another 1.70% come from the same faulty implementations and may be susceptible to compromise. Even more alarmingly, we are able to obtain RSA private keys for 0.50% of TLS hosts and 0.03% of

expect that today's widely used operating systems and server software generate random numbers securely. In this paper, we test that proposition empirically by examining the public keys in use on the Internet.

The first component of our study is the most comprehensive Internet-wide survey to date of two of the most important cryptographic protocols, TLS and SSH (Section 3.1). By scanning the public IPv4 address space, we collected 5.8 million unique TLS certificates from 12.8 million hosts and 6.2 million unique SSH host keys from 10.2 million hosts. This is 67% more TLS hosts than the latest released EFF SSL Observatory dataset [20]. Our techniques take less than 24 hours to scan the entire

From http://web.stanford.edu/class/ee380/Abstracts/150513-slides.pdf
"How Not to Generate Random Numbers"

- Vast majority of weak keys generated by network devices
  - Network security devices / Routers
  - Server management cards
  - Industrial-grade firewalls
  - > 50 manufacturers
- Taiwanese smartcards produce weak keys
  - Most common factor appears 46 times!
- Debian weak keys

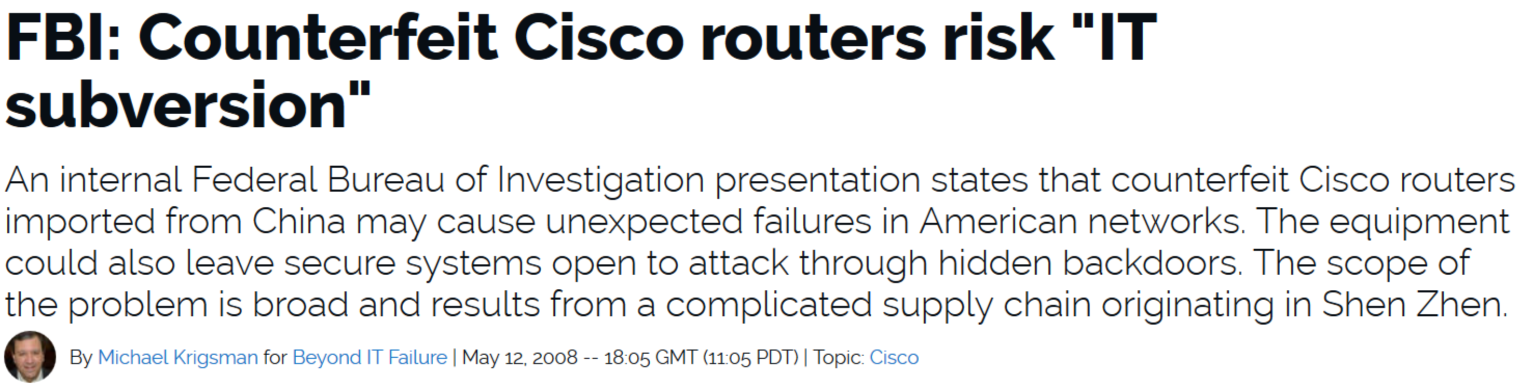
Hardware Random Number Generator

- Better seeding for the OS RNG
  - Also available in 1.2
  - Good for servers when first booted
  - Good for embedded devices

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - **Supply chain risks / Counterfeit hardware**
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

Supply Chain Risk Management



FBI: Counterfeit Cisco routers risk "IT subversion"

An internal Federal Bureau of Investigation presentation states that counterfeit Cisco routers imported from China may cause unexpected failures in American networks. The equipment could also leave secure systems open to attack through hidden backdoors. The scope of the problem is broad and results from a complicated supply chain originating in Shen Zhen.

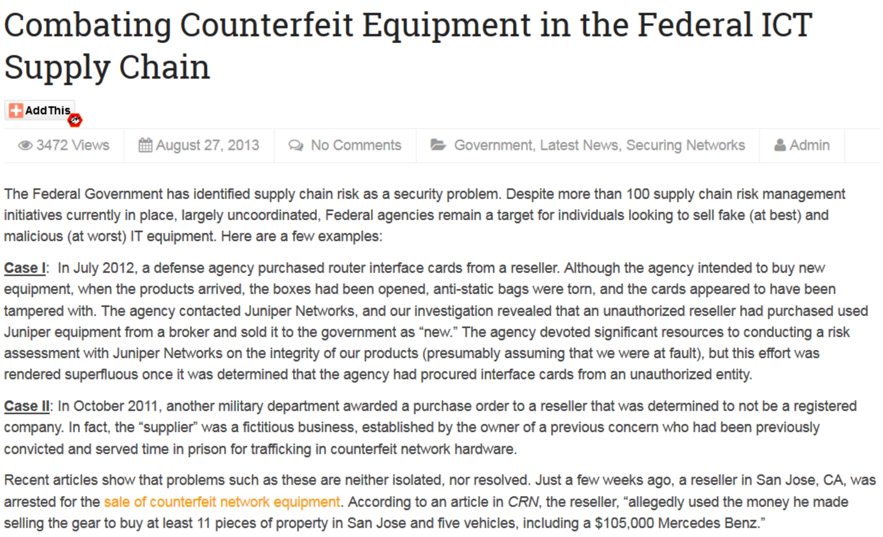
By Michael Krigsman for Beyond IT Failure | May 12, 2008 -- 18:05 GMT (11:05 PDT) | Topic: Cisco

Fake Apple Store In China

This is not a real Apple store

Just a really good fake that American blogger Jessica Angelson found in Kunming, an obscure southwestern Chinese city.

http://www.forbes.com/pictures/fi45eddmgk/this-is-not-a-real-apple-store/



Combating Counterfeit Equipment in the Federal ICT Supply Chain

3472 Views | August 27, 2013 | No Comments | Government, Latest News, Securing Networks | Admin

The Federal Government has identified supply chain risk as a security problem. Despite more than 100 supply chain risk management initiatives currently in place, largely uncoordinated, Federal agencies remain a target for individuals looking to sell fake (at best) and malicious (at worst) IT equipment. Here are a few examples:

Case I: In July 2012, a defense agency purchased router interface cards from a reseller. Although the agency intended to buy new equipment, when the products arrived, the boxes had been opened, anti-static bags were torn, and the cards appeared to have been tampered with. The agency contacted Juniper Networks, and our investigation revealed that an unauthorized reseller had purchased used Juniper equipment from a broker and sold it to the government as "new." The agency devoted significant resources to conducting a risk assessment with Juniper Networks on the integrity of our products (presumably assuming that we were at fault), but this effort was rendered superfluous once it was determined that the agency had procured interface cards from an unauthorized entity.

Case II: In October 2011, another military department awarded a purchase order to a reseller that was determined to not be a registered company. In fact, the "supplier" was a fictitious business, established by the owner of a previous concern who had been previously convicted and served time in prison for trafficking in counterfeit network hardware.

Recent articles show that problems such as these are neither isolated, nor resolved. Just a few weeks ago, a reseller in San Jose, CA, was arrested for the sale of counterfeit network equipment. According to an article in *CRN*, the reseller, "allegedly used the money he made selling the gear to buy at least 11 pieces of property in San Jose and five vehicles, including a $105,000 Mercedes Benz."

Endorsement Key+Certificate

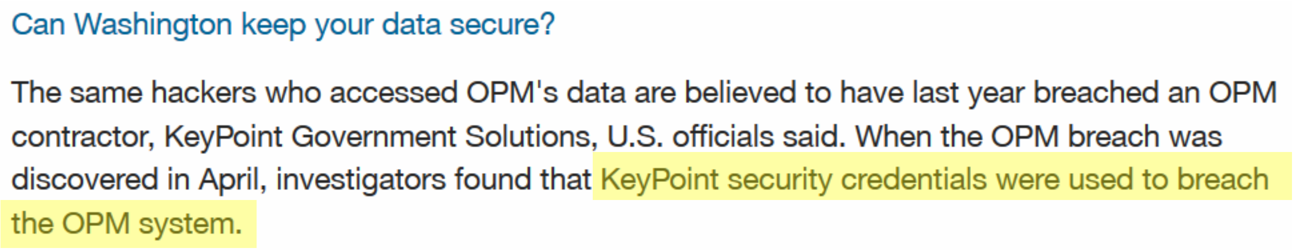
- **TPM 2.0 comes with a Certificate, which matches a key that can be regenerated inside the TPM!**
  - **Certificate signed by manufacturer**
  - **Proof it is a genuine TPM**

- **IDevID can also be provided by an equipment manufacturer**
  - **With OEM certificate**
  - **Can prove chip was on motherboard when it left the OEM facility**
  - **Can be used for warrantee**
  - **Can be used for creation of LDevIDs**

Why Use a TPM 2.0?

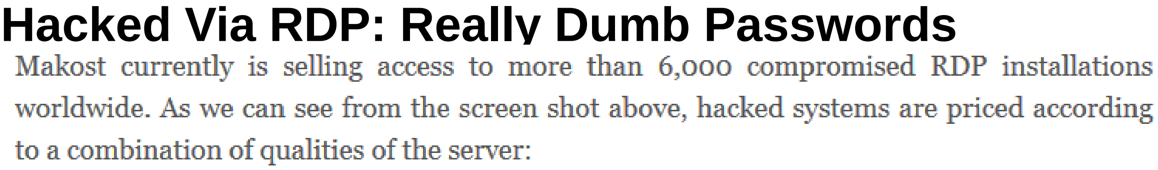
- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - **Keeping bad guys off of your internal network**
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

VPN password compromise



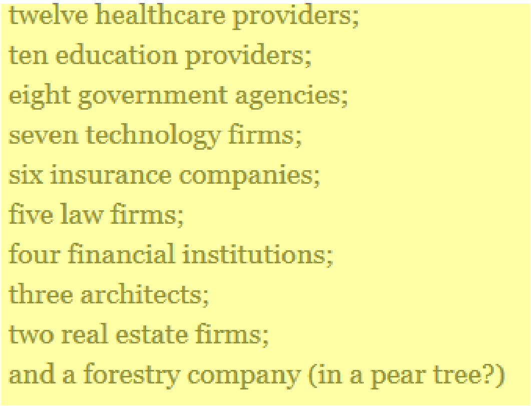
Can Washington keep your data secure?

The same hackers who accessed OPM's data are believed to have last year breached an OPM contractor, KeyPoint Government Solutions, U.S. officials said. When the OPM breach was discovered in April, investigators found that KeyPoint security credentials were used to breach the OPM system.

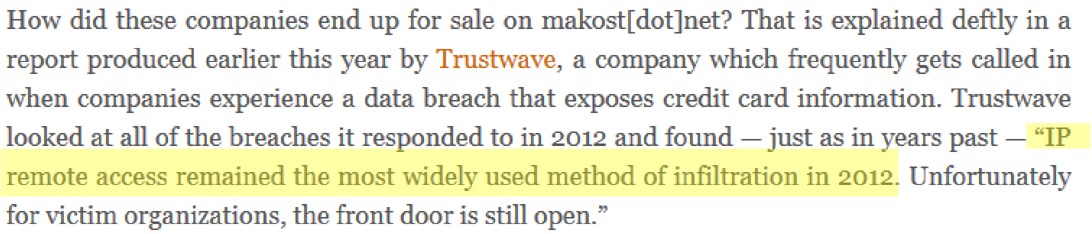


Hacked Via RDP: Really Dumb Passwords

Makost currently is selling access to more than 6,000 compromised RDP installations worldwide. As we can see from the screen shot above, hacked systems are priced according to a combination of qualities of the server:



twelve healthcare providers;
ten education providers;
eight government agencies;
seven technology firms;
six insurance companies;
five law firms;
four financial institutions;
three architects;
two real estate firms;
and a forestry company (in a pear tree?)



How did these companies end up for sale on makost[dot]net? That is explained deftly in a report produced earlier this year by Trustwave, a company which frequently gets called in when companies experience a data breach that exposes credit card information. Trustwave looked at all of the breaches it responded to in 2012 and found — just as in years past — "IP remote access remained the most widely used method of infiltration in 2012. Unfortunately for victim organizations, the front door is still open."

Use Public/private key for authentication!

- TPM can generate keys, which don’t leave the machine
- LDevID : IEEE8021-DEVID-MIB - LMSC, LAN/MAN Standards
- Make the Company Owned asset the “Thing you have”
  - Two factor authentication

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - **Keeping malware infected hardware off of your internal network**
  - Massive password database releases
  - Multi-factor authentication
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

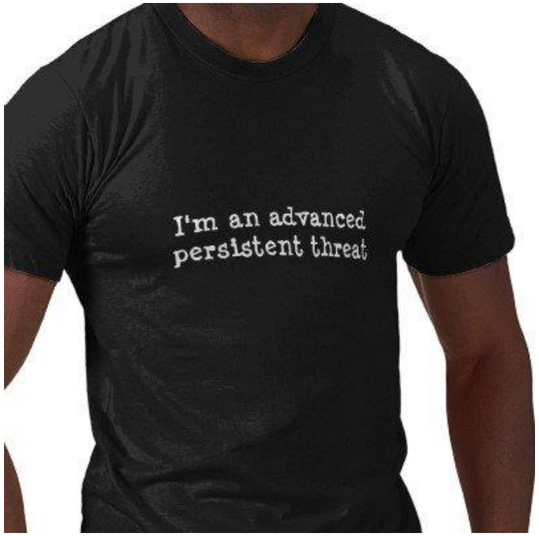
Advanced Persistent Threats

- **MBR based malware is hard to find**
  - **It gets in before the anti-virus and can hide**

- **UEFI firmware is even harder to find**

- **SMM based malware is even harder to find**

- **All have been compromised**



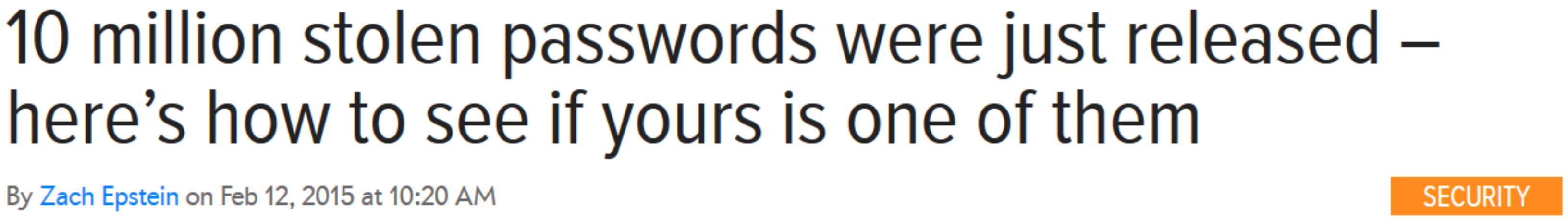
TPM 1.2 & 2.0 + New attestation models

- Intel hardware based measurement of boot block of firmware
- Firmware measures rest of firmware (including, SMM, UEFI, MBR)
- Measurements are stored in TPM PCRs via one way function
- TPM can use an internal private key to attest to boot sequence
  - 1.2: AIK (Attestation Identity Keys)
  - 2.0: Restricted Signing Keys
- Exists in current software for TPM 1.2!
  - StrongSwan VPN (Linux) using TNC
  - IMA (Linux)
  - Wave (Windows) Endpoint Monitor
  - JW Secure

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - **Massive password database releases**
  - Multi-factor authentication
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

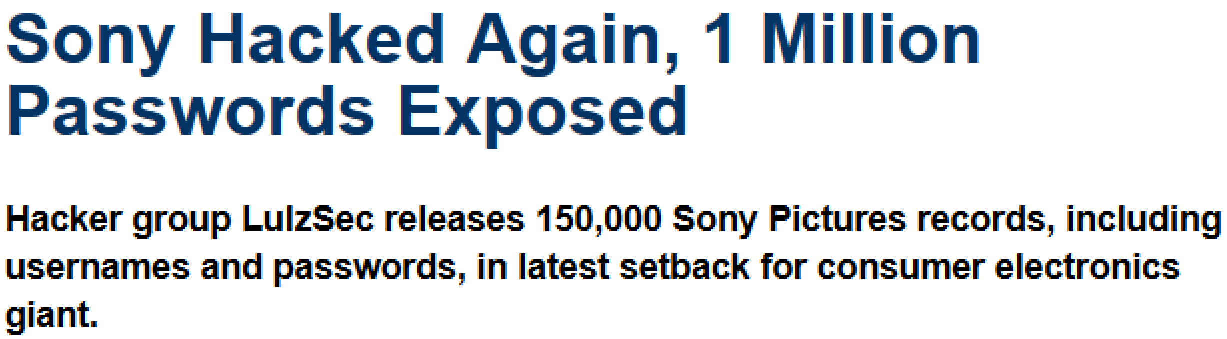
Compromised Password Databases



10 million stolen passwords were just released – here's how to see if yours is one of them

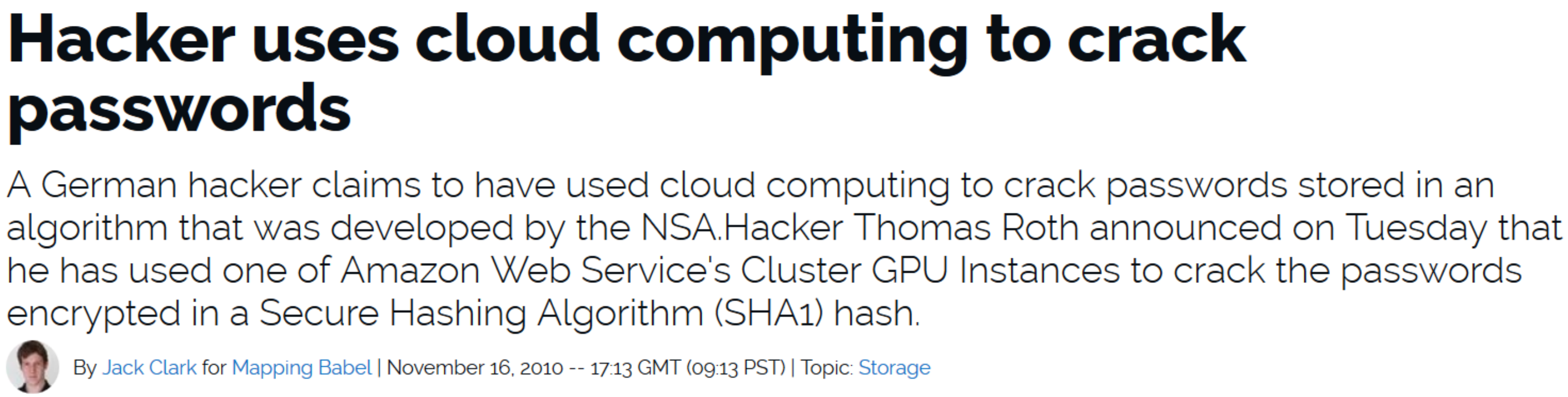
By Zach Epstein on Feb 12, 2015 at 10:20 AM

SECURITY



Sony Hacked Again, 1 Million Passwords Exposed

Hacker group LulzSec releases 150,000 Sony Pictures records, including usernames and passwords, in latest setback for consumer electronics giant.



Hacker uses cloud computing to crack passwords

A German hacker claims to have used cloud computing to crack passwords stored in an algorithm that was developed by the NSA.Hacker Thomas Roth announced on Tuesday that he has used one of Amazon Web Service's Cluster GPU Instances to crack the passwords encrypted in a Secure Hashing Algorithm (SHA1) hash.

By Jack Clark for Mapping Babel | November 16, 2010 -- 17:13 GMT (09:13 PST) | Topic: Storage

HMAC keys

- Servers today typically use PBKDF2 for protecting passwords store in shadow tables
  - Susceptible to dictionary and offline cloud based attacks

- TPM 2.0 can create, securely store, and use HMAC keys
  - HMAC “Userid || Password” and store that in the shadow table
  - Backup HMAC key as necessary

- NOT susceptible to *any* offline attacks.

- Probably faster than PBKDF2 as only one iteration is necessary
  - Per: NIST SP800-132, for PBKDF2:

  A minimum iteration count of 1,000 is recommended. For especially critical keys, or for very powerful systems or systems where user-perceived performance is not critical, an iteration count of 10,000,000 may be appropriate.

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - **Multi-factor authentication**
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

1
2
3
4
5
6
7
8
9
*

Multi-factor authentication

- **Means of Authentication**
  - Passwords are weak (especially by themselves)
    - If you can remember it, a computer can crack it
  - Biometrics are weak (especially by themselves)
    - Biometric Spoofing is an arms race
  - A “Thing you have” can be lost
    - Good for preventing remote (especially very long distance) attacks
  - Time of day / GPS Location / Revocation / n-use authorization
    - All good for some use cases, all have potential problems
- **Solution:**
  - Use more than one!

TPM 2.0 Enhanced Authorization

- All services in a TPM can be set up with Designer Authorization
  - 1-factor to n-factor (simple or complex)
  - Any type of authentication you can think of

- Services can be fine grained!
  - Not just on per object
  - Can be per operation on each object

- Examples:
  - Keys that can be duplicated ONLY to specified servers
  - Keys that can be duplicated ONLY by specified administrators
  - Keys that can only be used after separate authorization by two different authorities
  - Keys linked to specific external devices (biometrics, clocks, GPS)

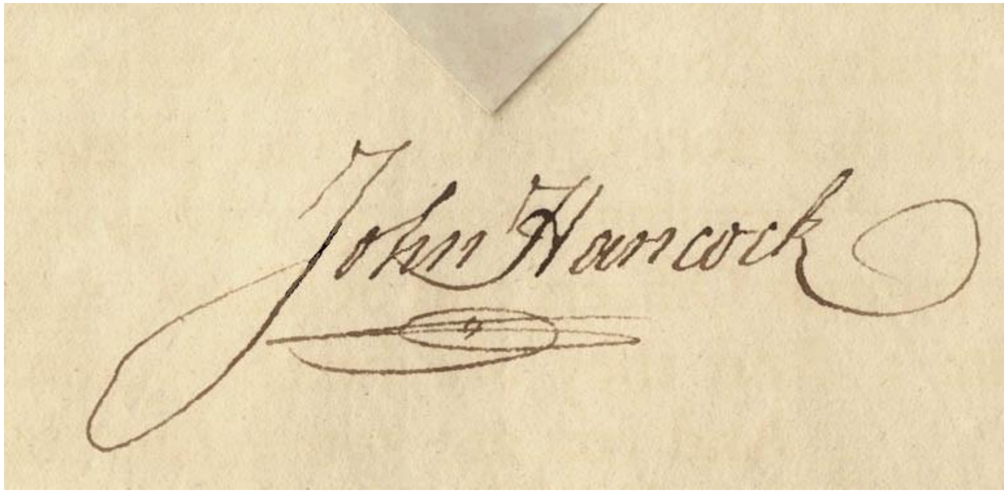
Multiple factor authentication

- New authentications in TPM allow for restricting use of TPM services in virtually any way you can think of
- Examples
  - A single user can be required to satisfy several things to authenticate
    - Biometrics
    - Smartcards
    - Passwords / HMACs
    - Machine State
    - GPS location
    - Etc.
  - Multiple users can authenticate separately to use the same key
  - Administrative tasks with keys (such as duplication) can be authorized separately from normal user tasks

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - **Email Security**
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - Merging physical and logical controls

Email Security – Email Signing



- Most Email clients have CSP interfaces
  - PKCS#11 or MSCAPI interfaces

- TPM 1.2 has PKCS#11 and MSCAPI CSP
  - TPM Keys can be used for signing

- TPM 2.0 can be used with Outlook

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - Email Security
  - **FIPS certified / Common criteria certified encryption engines**
  - Securing your root certificates
  - Merging physical and logical controls

Need a certified encryption engine

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

- Many TPMs are Common Criteria Certified
- Some TPMs are FIPS certified

- TPM can be used to do encryption, called from an APP
  - As a Crypto Service Provider

- Most TPMs don’t do bulk symmetric encryption
  - The spec allows for it
  - Blame import / export laws

Need a secure place to store a key in an embedded device

- No hard disk
- Don’t want to wait to load a key into the device anyway
- No full OS (preboot verification)
  - Locking encryption of hard disk to machine
    - For secure disposal if drive dies (How are you going to erase it?)

TPM 2.0 has NV with the same protections as any other service

Can restrict access to pre-boot!

Can store keys internally (not many, but some)

Can be used in VPN or HTTPS protocol to exchange keys

Can store just a public key for signature verification

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - **Securing your root certificates**
  - Merging physical and logical controls

Secure Storage

Need a place for secrets (e.g. password) or static information

- **NV can be used to store arbitrary information**
  - **Can be made only available to defined pre-boot OS**

- **NV can be used to store certificates / keys that represent the machine or for Root Certificates**

- **NV can hold “golden measurements” for the system**

- **NV can be used to store provisioning identifiers**
  - **Software that should be installed on system during provisioning**
  - **Security requirements of the system**

- **Read / Write permissions are “services” which can be given the same constraints as any other TPM services**

Why Use a TPM 2.0?

- **Problems that can be solved/ameliorated with TPMs**
  - Poor entropy leading to weak keys
  - Supply chain risks / Counterfeit hardware
  - Keeping bad guys off of your internal network
  - Keeping malware infected hardware off of your internal network
  - Massive password database releases
  - Multi-factor authentication
  - Email Security
  - FIPS certified / Common criteria certified encryption engines
  - Securing your root certificates
  - **Merging physical and logical controls**

Controlling the Physical World

GPIOs

- Behave just like NV memory
- Turn things on / off based on state, authentication
  - Open doors
  - Open/Close network connections
  - Trusted Path / Display

Problems caused by the upgrade to 2.0

- TPM 2.0 is *NOT* compatible with 1.2
  - It is feature compatible
  - It is not API compatible
- High level TSS API for 2.0 not yet available
  - Low level API is open source
- Abstraction can help
  - Microsoft APIs are TPM agnostic
    - Except for new 2.0 features
  - PKCS#11 APIs are TPM agnostic
    - Exist for TPM 1.2
    - Don’t (yet) exist for TPM 2.0
    - Don’t allow use of all TPM features

Software for TPM 1.2

- VPNs
  - StrongSwan
  - Cisco with Wave Systems MS CAPI CSP
  - Cisco with Charismathics software
  - Microsoft VPN or DirectAccess
  - Checkpoint Firewall VPN
  - TypeSafe 9 (TPM-backed TLS)
  - NCP’s Secure VPN GovNet Box

- Attestation
  - Wave Systems
  - StrongSwan
  - NCP’s Secure VPN
  - AnyConnect
  - JW Secure (Kerberos-like)
  - Integrity Measurement Architecture (Linux only)
  - TPM Quote Tools
  - Trusted Grub
  - TVE
  - Tboot
  - Flicker
  - VMware

Software for TPM 1.2 (Continued)

- **Full Disk Encryption**
  - **Bitlocker (MS)**
  - **dm-crypt (PKCS#11)**
  - **SecureDoc**

- **File and Folder Encryption**
  - **PGP (via PKCS#11)**
  - **OpenPGP(via PKCS#11)**

- **E-mail**
  - **Thunderbird (via PKCS#11)**
  - **Outlook (MS)**

- **Web Browsers**
  - **Internet Explorer (MS)**
  - **Firefox (via PKCS#11)**
  - **Chrome (via PKCS#11)**

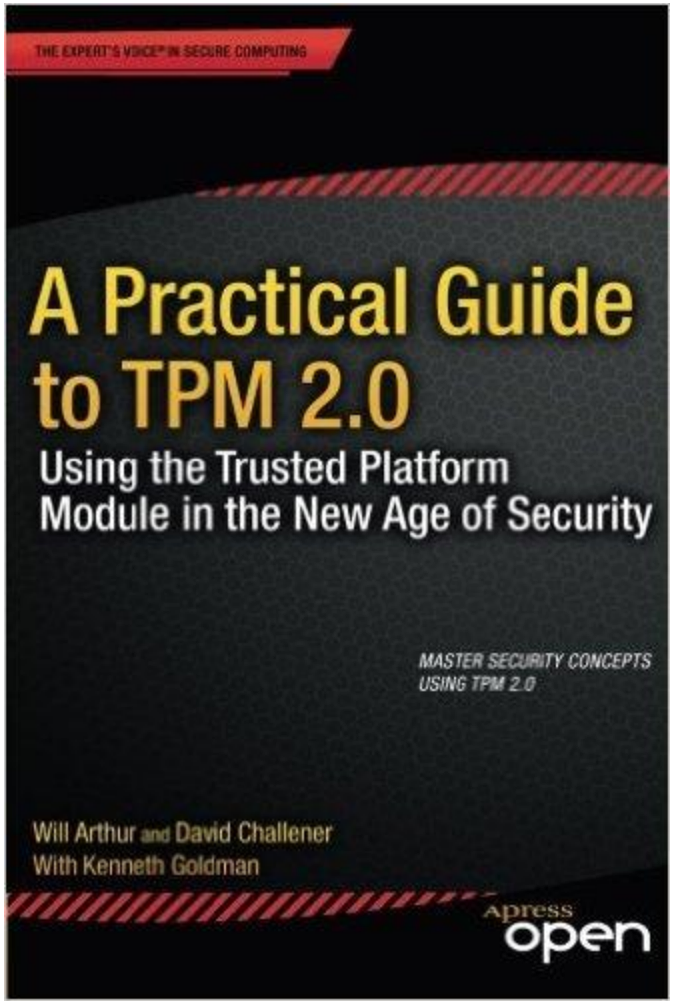
Software that doesn’t exist (AFAIK) for TPMs

- Remote/Cloud
  - Remote control software
  - Remote presentation software
  - Cloud storage (backup)
  - Browser tab sharing

- Server based
  - HMAC-based password protection
  - Full Kerberos implementations

- Client based
  - VOIP
  - Links to SEDs (How else do you erase it if it is dead?)

For more information



THE EXPERT'S VOICE® IN SECURE COMPUTING

A Practical Guide to TPM 2.0

Using the Trusted Platform Module in the New Age of Security

MASTER SECURITY CONCEPTS USING TPM 2.0

Will Arthur and David Challener
With Kenneth Goldman

Apress open

Available FREE as an e-Book

Also there is a software stack available for free here:

https://github.com/01org/TPM2.0-TSS