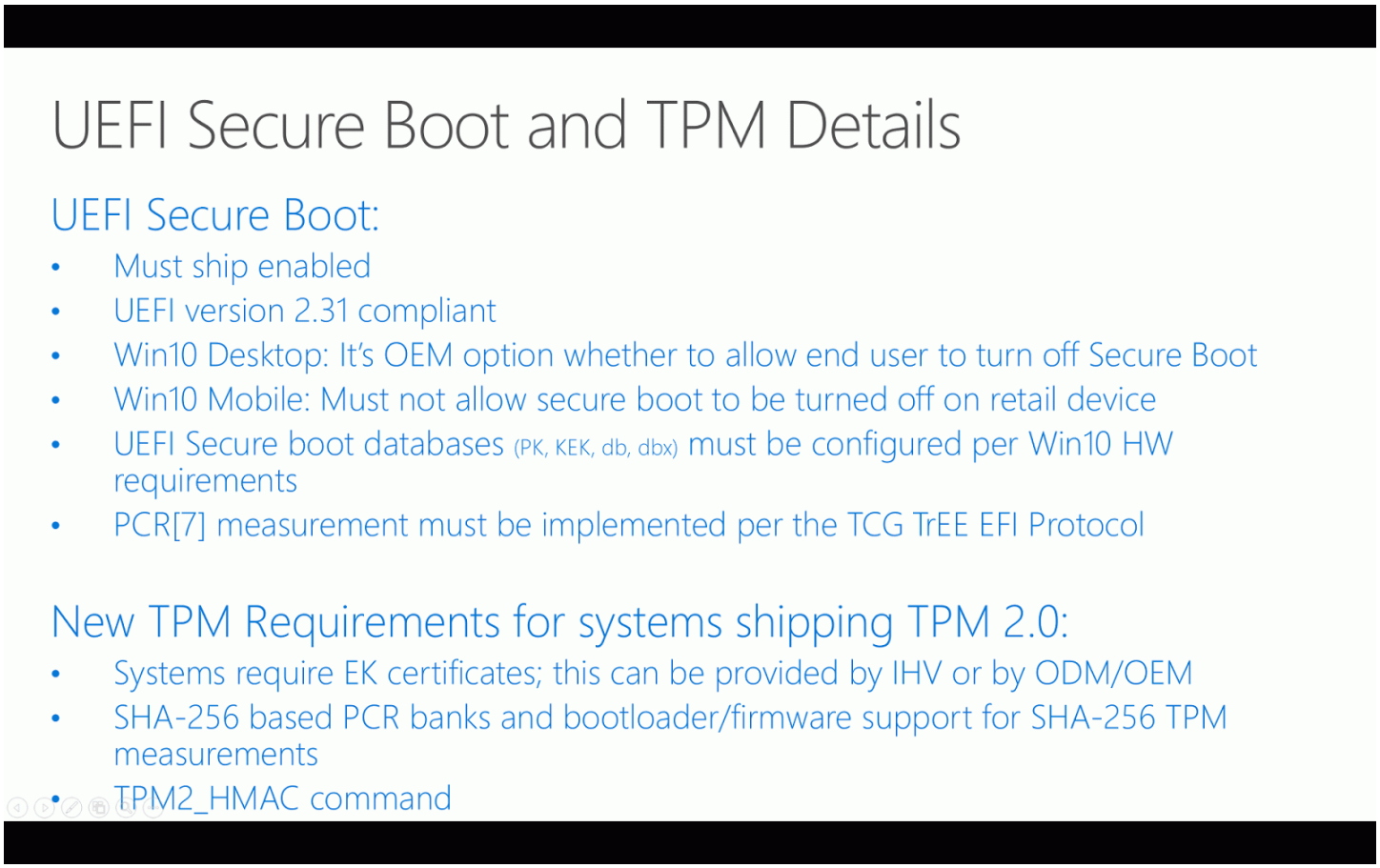
Security Now! #500 - 03-24-15

Windows Secure Boot

This week on Security Now!

- Security Now! Episode #500
- An apparently effective iPhone/iPad 4-digit PIN hack.
- Another really bad certificate found in the wild.
- Amazing Pwn2Own results.



http://cdn.arstechnica.net/wp-content/uploads/2015/03/windows-10-secure-boot.png

Security News

iPhone/iPad: How to crack 4-digit PIN codes

- http://www.techworm.net/2015/03/120-ip-box-can-be-used-to-hack-iphones-and-ipads-with-brute-force.html
- http://www.fonefunshop.co.uk/cable_picker/98483_IP-BOX_iPhone_Password_Unlock_Tool.html
- Bypasses the: "Erase data after 10 attempts" lockout.
- Performs a hard power interruption BEFORE the fact of the failed attempt can be written to non-volatile memory.
- Works up through v8.1... but was foreclosed by v8.1.1 last November.

Bad Certificates

- http://arstechnica.com/security/2015/03/google-warns-of-unauthorized-tls-certificates-trusted-by-almost-all-oses/
- http://googleonlinesecurity.blogspot.de/2015/03/maintaining-digital-certificate-security.html
- MCS Holdings, an Egyptian Intermediate Certificate Authority obtained an Intermediate CA certificate - having full certificate signing rights -- from China's CNNIC: the China Internet Network Information Center.
- CNNIC states that MCS Holdings obtained the certificate under the provision that they would only issue certificates for their own domains.
- But... rather than keeping this precious and powerful certificate locked down, they installed it into a Man-in-the-middle TLS proxy in order to intercept all network communications without requiring clients to install a local trust certificate.
- Google pushed out a CRLSet update to block this certificate.
- (Also... in addition to "live.fi", another cert was issued to "live.be."

Pwn2Own

- All 4 major web browsers hacked at Pwn2Own: Safari, Firefox, IE, Google Chrome
- https://threatpost.com/all-major-browsers-fall-at-pwn2own-day-2/111731
- Korean researcher Jung Hoon Lee pulled off three of the four:
    - Against Chrome, he won $110,000, the single highest payout in history:
    - Using more than 2000 lines of code, Lee took down both stable and beta versions of Chrome by exploiting a buffer overflow race condition in the browser. He then used an info leak and race condition in two Windows kernel drivers to secure SYSTEM access. The standalone Chrome bug fetched Lee $75,000 while the privilege escalation bug scored him another $25,000. To finish it off, Google's Project Zero, as it usually does when Chrome is hacked at the event, paid Lee an extra $10,000.

- Lee earned $65,000 for exploiting a 64-bit version of IE 11 with a time-of-check to time-of-use (TOCTOU) vulnerability. The vulnerability, exploited between the time a file

property is checked and the time the file is used, usually leads to privilege escalation. In this case the attack enabled him read/write privileges on the browser while another attack he used, a sandbox escape via JavaScript injection, helped him evade defensive mechanisms on the browser.

- He also leveraged a use-after-free vulnerability to take down Safari, exploiting an uninitialized stack pointer in the browser to bypass Safari's sandbox... and netted another $50,000.

    - ($225,000 total)

- Pwn2Own, hosted by HP's Zero Day Initiative and Google's Project Zero:
    - Microsoft Windows: 5 bugs
    - Microsoft IE 11: 4 bugs
    - Mozilla Firefox: 3 bugs
    - Adobe Reader: 3 bugs
    - Adobe Flash: 3 bugs
    - Apple Safari: 2 bugs
    - Google Chrome: 1 bug
    - $442,500 paid out to researchers

- A Firefox update was pushed out (v36.0.3). (now at .4)

Miscellany:

Sunday's TWiT

- Ed Bott... cares about protecting his privacy.
- VR headsets and pornography.

SpinRite:

Phil Horowitz
Location: Montreal, Quebec, Canada

Hello Steve and Leo,

My simple everyday SpinRite story: I was helping a friend who had a Windows 8 computer that hung at startup. He didn't know what to do. So he brought the computer over and I ran SpinRite. As I have seen before, there were no evident errors that were corrected. But nevertheless, after SpinRite completed, the PC started. Great!

Love Security Now - haven't missed a show!
Phil Horowitz

Episode #500 of Security Now!

Windows Secure Boot

WinHEC hardware conference on March 20th in Shenzhen, China.

- Not final, so might be subject to change... but...
- The requirements for Windows 10 Logo Desktop & Laptop machines allows manufacturers to ELIMINATE the option for system owners to disable Secure Boot. What does that mean?

The evolution of the BIOS

- System services
- Option ROMS
- DOS -> BIOS -> Hardware
- Video memory map.

UEFI - Unified Extensible Firmware Interface

- Vast array of services.
- SMBIOS manages all motherboard resources.
- ACPI power control
- Fans, Voltage, Current, Network Boot, Chassis Management...

UEFI Boot Services

- "PI" -Platform Initialization standard.
- Security added with UEFI v2.31 "Secure Boot"
- Uses the very familiar PKI public key infrastructure.
- PK - Platform Key.
    - Typically held my the system manufacturer.
- The firmware itself is signed and the verification public key is burned into ROM.
    - So ONLY signed and unmodified firmware can be used.
- KEK - Key Exchange Key database
    - contains trust anchors that are allowed to modify the Allowed Signatures database.
- Allowed Signatures database. (db)
    - contains trust anchors used for verifying UEFI firmware images.
- Forbidden database. (dbx)
    - Identifies signers that have been revoked and are no longer trusted.
- Drivers can either be SIGNED or have their signatures White or Black listed.
- Provisions for timestamping to prevent rollback and replay attacks.

Booting:

- UEFI Boot Manager's signature if checked using the RSA public key in ROM.
- UEFI Boot Manager loads EFI images for system components, checking them against the

Allowed and Forbidden databases. Only images whose signature matches an entry in the Allowed database (or whose signer is present in the Allowed database) and is not present in the Forbidden database (and whose signer is not present in the Forbidden database) are allows to the loaded and initialized.
- Notes about rejected images are kept for later remediation.

"Measured Boot" -- secure boot auditing
- Each component loaded is recorded ("measured") into the system's tamper-proof TPM.
- Later, the TPM's boot audit trail can be exported to a 3rd-party or verification.

"Secure Boot" + "Measured Boot" == TRUSTED BOOT.

Windows
- Secured Boot with Early Launch Antimalware (ELAM).
  - AM == Anti-Malware
- Measured Boot
  - Provides AM software with a trusted (resistant to spoofing and tampering) log of all boot components that started before AM software. AM software can use the log to determine whether components that ran before it are trustworthy.
- ELAM provides a mechanism for AM software to start before all other third-party components. AM drivers are initialized first, and allowed to control the initialization of boot drivers, potentially not initializing unknown boot drivers.
- EVERYTHING is logged in the TPM (to prevent tampering) and can be securely sent to another (uncompromised machine) for verification.

What does this mean?

Windows 8 "Logo" requirements:
- Microsoft mandated that UEFI Secure Boot must be *enabled* by default.
- BUT... Microsoft also required that every system must have a user-accessible "off" switch.
- Microsoft's rules also required that users be able to add their own signatures and cryptographic certificates to the firmware, so that they could still have the protection that Secure Boot provides, while still having the freedom to compile their own software.