*presented by*

Microsoft

# Deploying Secure Boot: Key Creation and Management

UEFI Summer Summit – July 16-20, 2012

Presented by Arie van der Hoeven (Microsoft Corporation)

# Agenda

- Introduction
- Secure Boot Basics
- Secure Boot Keys
- Key Deployment
- Key Creation and Management
- Checklist

# Introduction

- Today partners are testing Secure Boot using WHCK tools and Microsoft provided certificates
  - But passing Windows requirements is just a start
- OEMs and ODMs need to have a plan for securely creating and managing their own keys
  - Customers will increasingly ask about this
  - What is your story?
- Reputations are on the line

# In the news...

Los Angeles Times

Microsoft warns of phone-call security scam targeting PC users

By Nathan Olivarez-Giles, June 17, 2011

Microsoft is warning its customers of a new scam that employs "criminals posing as computer security engineers and people at home to tell them" computer security

eWEEK.COM

Researchers Discover Link Between TDSS Rootkit and DNSchanger Trojan

By NICK BILTON, May 2, 2011

TDSS rootkit, the hard-to-remo malware behind numerous sophisticated attacks, appears have helped spread the DNSchanger Trojan.

eWEEK.COM

Microsoft Recommends Reinstalling Windows to Remove Nasty Rootkit Trojan

By Fahmida Y. Rashid, June 28, 2011

A new variant of the Trojan Popureb burrows deep enough into the Windows operating

COMPUTERWORLD

Expect targeted attacks after massive Epsilon email breach, say experts. Database of stolen addresse is a gold mine for hackers and scammers

By Gregg Keizer, April 4, 2011

The high-profile data breach Epsil Interactive reported April 1 caused company noted on its w lients' c

COMPUTERWORLD

RSA warns SecurID customers after company is hacked

By Robert McMillan, March 17, 2011

EMC's RSA Security division says the security of the company's two-factor SecurID tokens could be at risk following a sophisticated cyber

PCWorld

Microsoft Exposes Scope of Botnet Threat

By Tony Bradley, October 15, 2010

Microsoft's latest Security Intelligence Report focuses on the expanding threat posed by bots and botnets.

Microsoft this week unveiled the ninth volume of its Security Intelligence Report (SIR). The semi-annual

THE WALL STREET JOURNAL.

Mebroot: The Stealthiest Rootkit in the Wild?

BY Nick Wingfield

March 18, 2011

eds launched the raids against named operators of the Rustock otnet," a vast network of mputers around the globe cted with malicious software allows its masterminds to

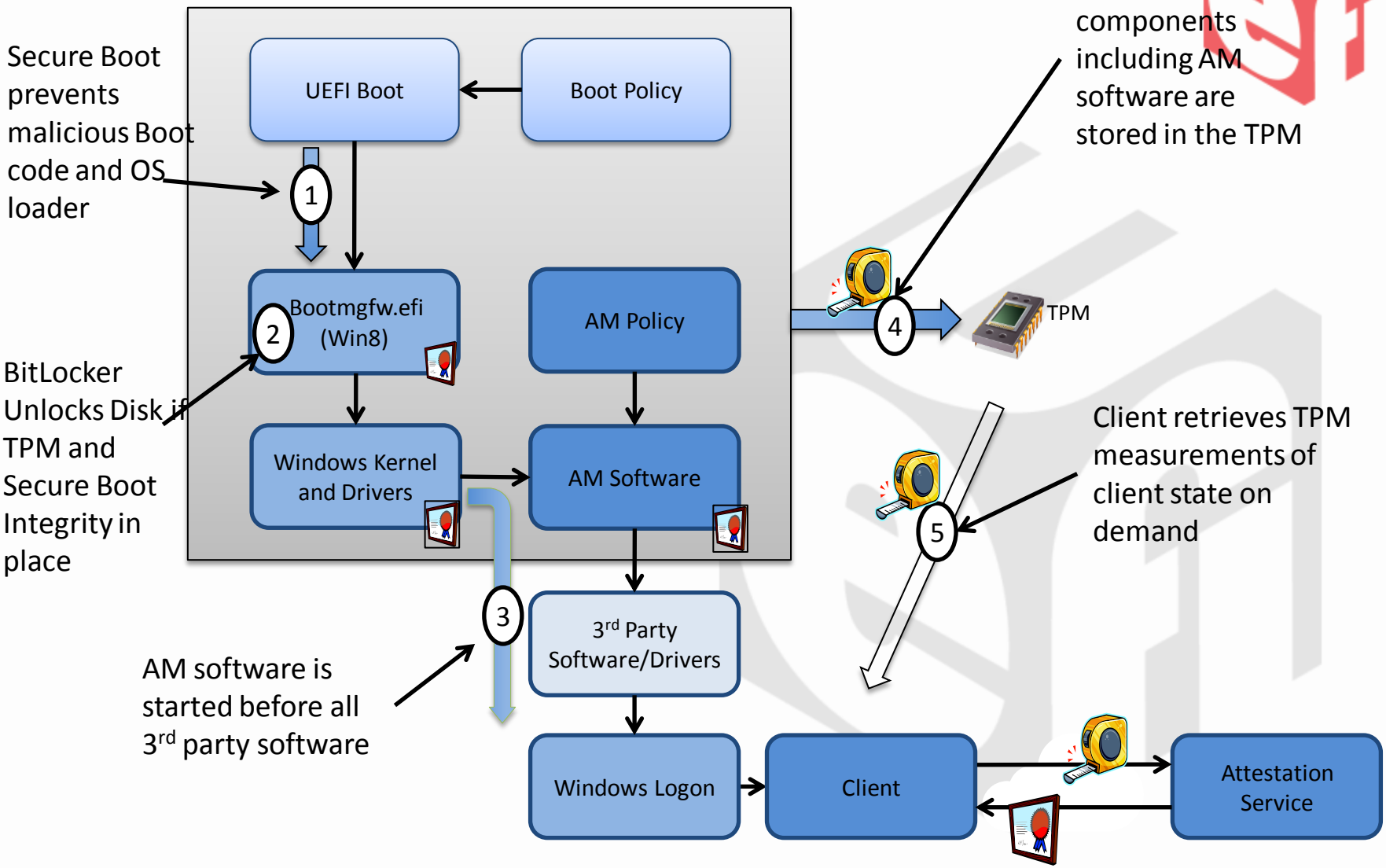
The Register

Hack attack spills web security firm's confidential data

By Dan Goodin in San Francisco Posted in Security, 11th April 2011

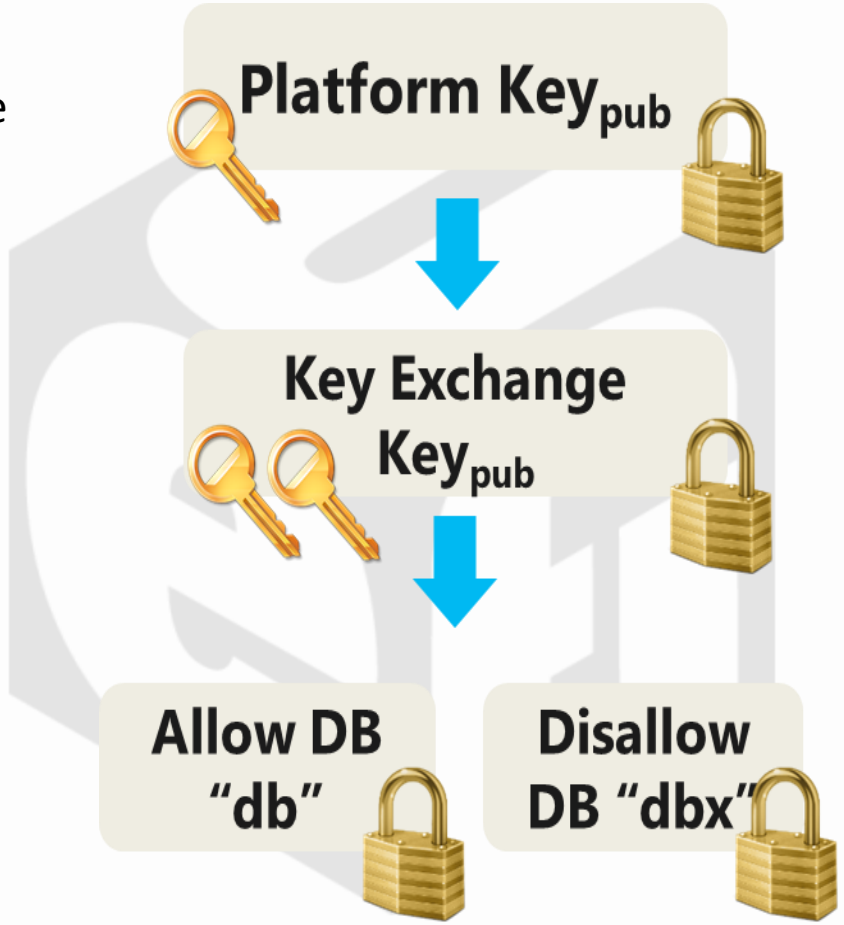
Try this for irony: The website of web application security provider Barracuda Networks has sustained an attack that

# Trusted Boot Architecture



# UEFI Secure Boot Keys

- Platform Key (PK)
  - One only
  - Allows modification of KEK database
- Key Exchange Key (KEK)
  - Can be multiple
  - Allows modification of db and dbx
- Authorized Database (db)
  - CA, Key, or image hash to allow
- Forbidden Database (dbx)
  - CA, Key, or image hash to block



# Keys Required for Secure Boot

| Key/db Name | Variable | Owner | Details |
|---|---|---|---|
| PKpub | PK | OEM | PK – 1 only. Must be RSA 2048 or stronger |
| Microsoft KEK CA | KEK | Microsoft | Allows updates to db and dbx: |
| Microsoft Windows Production CA | db | Microsoft | This CA in the Signature Database (db) allows Windows 8 to boot |
| Forbidden Signature Database | dbx | Microsoft | List of known bad Keys, CAs or images from Microsoft |

## + Required for Secure Firmware Updates

| Key/db Name | Owner | Details |
|---|---|---|
| Secure firmware update key | OEM | Recommendation is to have this key be different from PK. Must be RSA 2048 or stronger |

# Optional Keys for Secure Boot
## (non WinRT only)

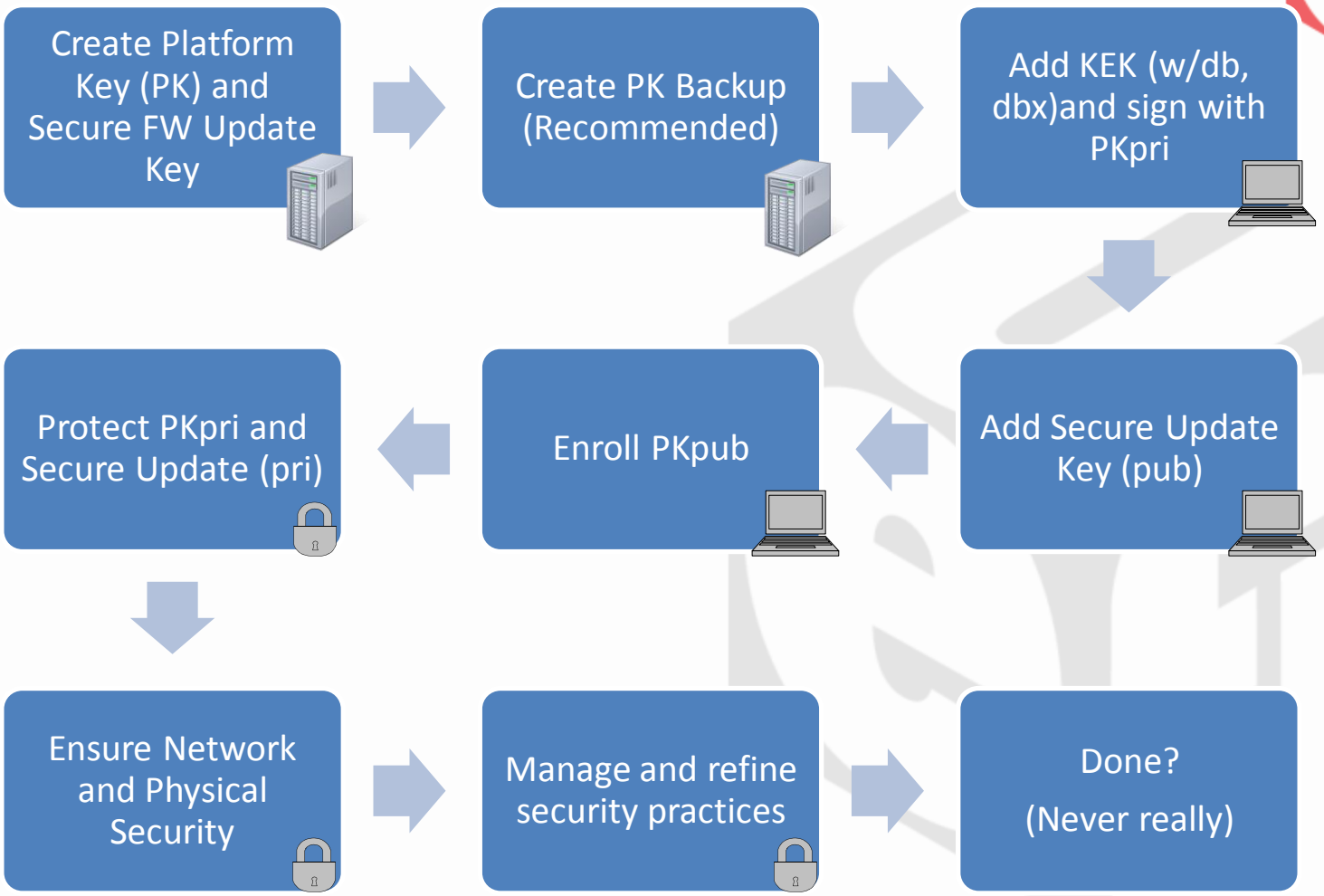
## Recommended for non WinRT Systems

| Key/db Name | Variable | Owner | Notes |
|---|---|---|---|
| Microsoft UEFI driver signing CA | db | Microsoft | Microsoft signer for 3'rd party UEFI binaries via DevCenter program |

## Optional for Customization

| Key/db Name | Variable | Owner | Notes |
|---|---|---|---|
| OEM or 3'rd party KEKpub | KEK | OEM/3rd party | Allows db/dbx updates e.g. for an alternate OS or Trusted 3'rd party |
| OEM or 3'rd party CA | db | OEM/3rd party | Allows 3'rd party OS or drivers singed by a trusted 3'rd party |
| Image Hashes | db | OEM | Hashes of images on PC that are allowed to execute even if not signed |
| Forbidden Signature Database (dbx) | dbx | OEM/3rd party | List of known bad Keys, CAs or images from OEM or partner |

# Key Deployment Process



# Hardware Security Modules

- Microsoft strongly recommends using a Hardware Security Module (HSM) for key creation
- Most HSMs have Federal Information Processing Standard (FIPS) Publication 140-2 level 3 compliance
  - Requires that keys are not exported or imported from the HSM.
- HSMs support multiple key storage options
  - Local on the HSM itself
  - On the server attached to the HSM - for solutions which requires lots of keys
- The cryptographic module security policy shall specify a physical security policy, including:
  - Tamper-evident seals, locks, tamper response and zeroization switches, and alarms
  - Policy includes actions required by the operator(s) to ensure that physical security is maintained such as periodic inspections

# Other Key Creation Options

- Trusted Platform Modules (TPM) or Smart Cards
  - Crypto processors slow for  manufacturing environment
  - Not suitable for storing large number of keys
  - May not be compliant to FIPS 140-2 level 3
- Software / Crypto API generated keys
  - Can use encrypted drives, VMs and other security options
  - Not as secure as using an HSM
- Makecert
  - Intended for testing purposes only
  - Discouraged by Microsoft

# Checklist

- ❑ Define your security strategy
  - ❑ Identify roles
  - ❑ Procure server and hardware for key management
    - Recommended solution – network or standalone HSM
    - Consider whether you will need one or several HSM's for high availability and also your key back up strategy
  - ❑ Set policy for how frequently will you be rekeying keys
  - ❑ Have a contingency plan for Secure Boot Key compromise
  - ❑ Identify how many PK and other keys will you be generating
- ❑ Use HSM to pre-generate secure boot related keys and certificates
- ❑ Get the Microsoft KEK and other Secure Boot related keys and certificates
- ❑ Sign UEFI drivers
- ❑ Update firmware with Secure Boot keys based on the system type
- ❑ Run tests including WHCK Secure Boot tests
- ❑ Deploy > Refine > Deploy > Refine…

# Resources

- Microsoft Connect http://connect.microsoft.com/
- MSDN: http://msdn.microsoft.com/
  - Search on keyword “Secure Boot”
- http://www.microsoft.com/security
- UEFI 2.3.1. Specification errata C: http://www.uefi.org/
- Trusted Computing Group: http://www.trustedcomputinggroup.org/
- Tianocore: http://www.tianocore.sourceforge.net
- UEFI and Windows: http://msdn.microsoft.com/en-us/windows/hardware/gg463149
- Beyond BIOS: http://www.intel.com/intelpress/sum_efi.htm

Thanks for attending the
UEFI Summer Summit 2012

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

*presented by*

Microsoft