Protecting Data with Short-Lived Encryption Keys and Hardware Root of Trust

Dan Griffin

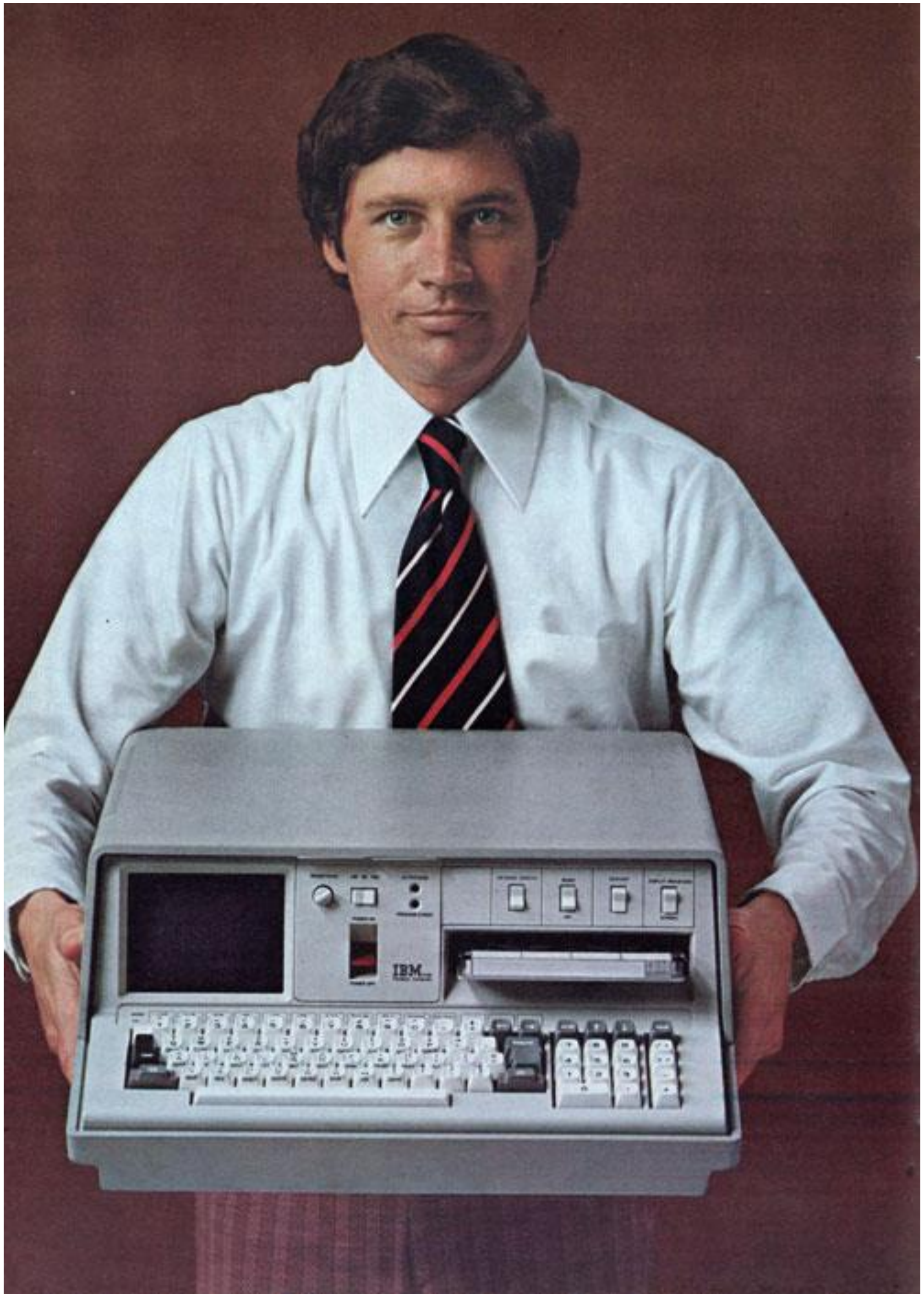
DefCon 2013

Time-Bound Keys Announcements

- New tool: TimedKey.exe
- New whitepaper: *Trusted Tamperproof Time on Mobile Devices*
- Check out http://www.jwsecure.com/dan

What does the NSA think?

- The NSA has been public about:
  - Inevitability of mobile computing
  - Need to support cloud-based services
  - Even for use with secret data in the field
- What works for them can work for you


IBM

trēo
12:38 pm
Treo
Card Info
CityTime
Carnival
Expense
Hot Snake
ate Book+
Memo Pad
McChords
tSync

wiseGEEK

How does the cloud know…

- Who you are?
- Where you are?
- Is your computer acting on your behalf?

Device Integrity

- A device is silicon
- It might be pretending to be me
- It might be pretending to be you
- Define device integrity to be “truth telling”
  - Is the device faithfully asserting delegation?
  - Is it faithfully representing the user’s intent?

Current Technology Landscape

- Why are mobile devices less secure?
  - Inconvenience of good passwords
  - Current antivirus is not up to the task
  - User-owned (BYOD/consumerization trends)
- But mobile devices do have security features
  - Screen lock
  - Secure storage
  - TrustZone & Trusted Execution Environment
  - Trusted Platform Module

Mobile Vulnerabilities

- Rootkits got harder, bad apps got much easier
- Mobile threat landscape:
  - Easy to steal the device
  - Easy to steal services
  - Easy to install apps that steal data
  - Even remote eavesdropping

What is needed to be secure?

- Encrypt user data
- Sandbox apps
- Secure, measured boot (TPM)
- Remote platform attestation

How to use a hardware root of trust

- Device receives TPM-bound token
  - Sends token to relying party to prove status
  - Token can carry decryption key as well
- If device is measured to be insecure
  - The good guys win!
  - Need to reset machine to clean it

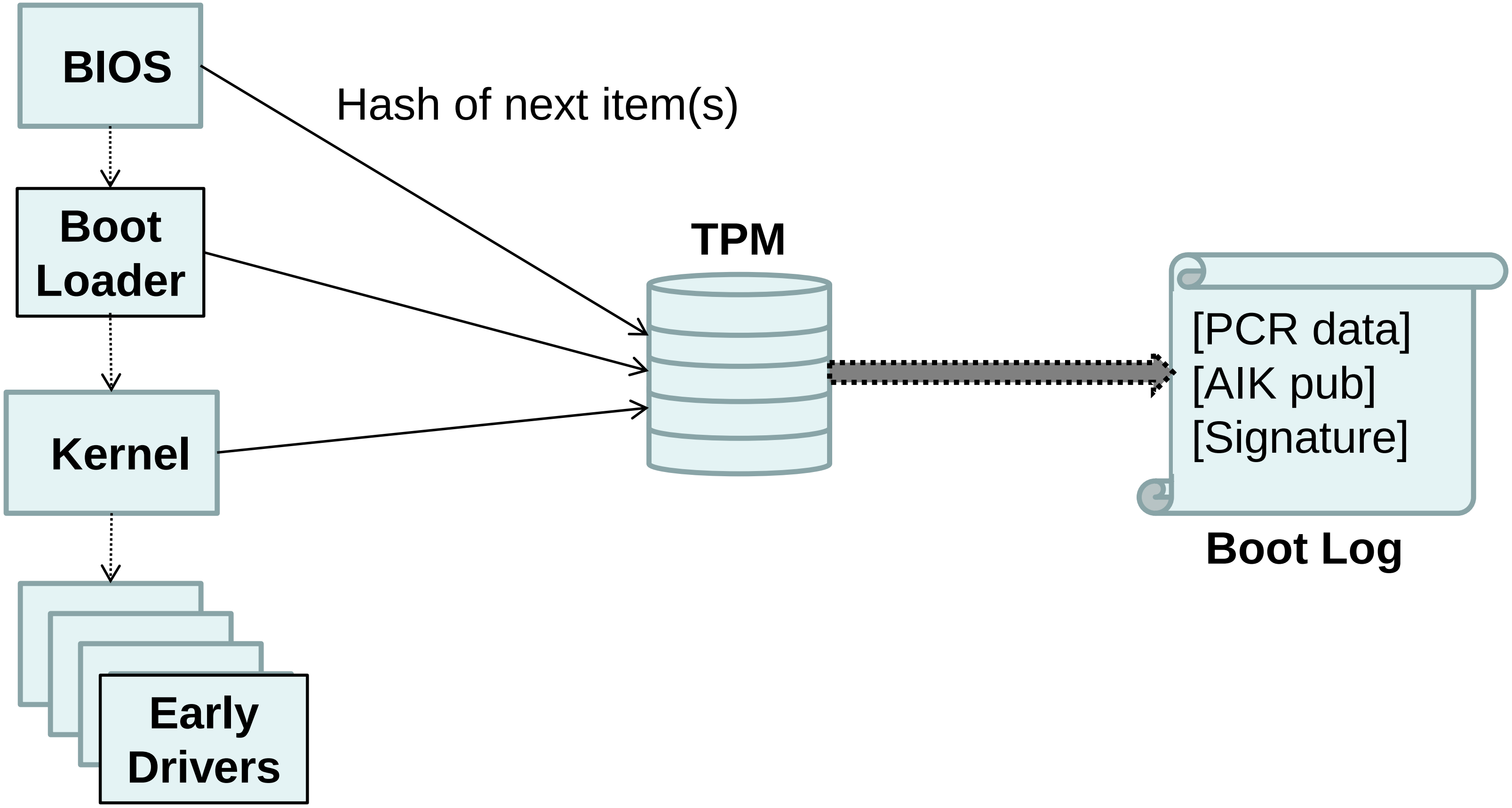
What is Remote Attestation?

- Remote attestation is enabled by the TPM
  - Can a server know the truth about the client?
  - Use root of trust to measure boot chain and configuration
- Remote attestation is a means to the truth
  - The TPM attests to device attributes
  - Rootkit-resistant, though not perfect

Remote Attestation Service (RAS)

- Needs secure data from manufacturer or telco
  - Hashes of known good code
- Only “early boot” code is hashed by the TPM
- Still rely on traditional antivirus for user mode protection
- The data/content provider must trust the RAS

How does the RAS trust the Device?



Is remote attestation really secure?

- Hardware root of trust within TPM (but might be firmware)
- PCRs are accumulated in secure location
- Send PCRs + boot log to RAS signed by TPM
- TPM 2.0 time counter
  - Can be expressed as policy
  - What advantage does that give us?

Time-based Authorization

- Secure local time reduces attack surface
- Devices now use authorization windows
  - Limit token lifetime
  - Otherwise, attacker can sleep the device, change the clock, continue to access data
- Great way to protect downloaded data

Mechanics of secure time

- See our whitepaper:
  - *Trusted Tamperproof Time on Mobile Devices*
  - http://www.jwsecure.com/dan
- Applicability to DLP and DRM

TimedKey.exe Tool

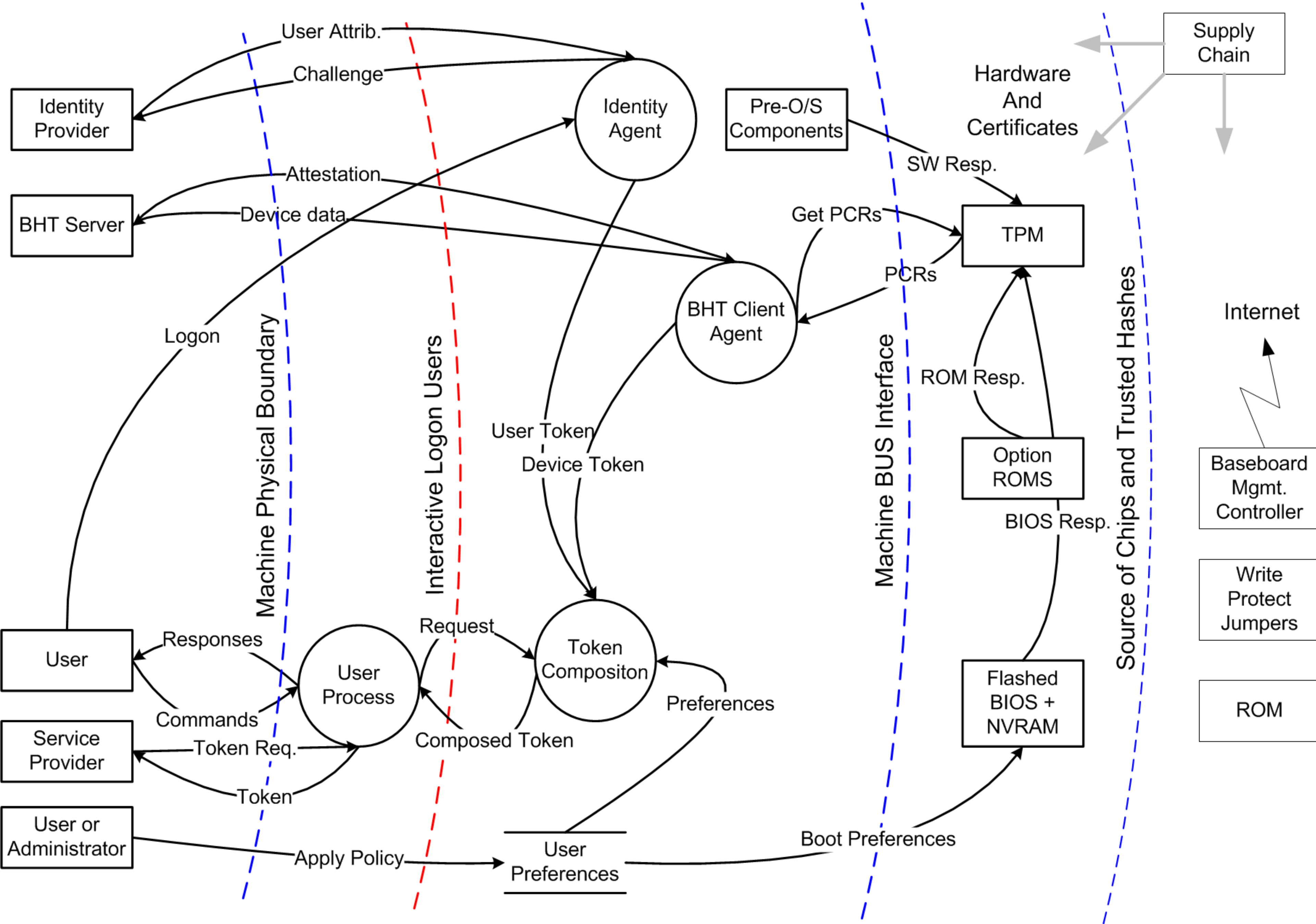
- Requires 32-bit Windows 8 with TPM 2.0
- See http://www.jwsecure.com/dan
- CLI:

```
C:\>TimedKey.exe
TimedKey.exe - JW Secure Demo: Policy bound hardware keys
CREATE   : -c:[1024, 2048] -k:KeyFile {-decrypt -sign -t:60 -p:PIN}
ENCRYPT  : -e:ClearText -k:KeyFile -o:CipherFile
DECRYPT  : -d:CipherFile -k:KeyFile {-p:PIN}
SIGN     : -s:Data -k:KeyFile -o:SignFile {-p:PIN}
VERIFY   : -v:Data -k:KeyFile -i:SignFile
```

Policy-Enforced File Access

- BYOD
- Download sensitive files
- Leave device in taxi

Measured Boot – Threat Model



Known Threats

- TPM setup on legacy devices = fail
- TPM reset attacks
- Hardware attacked, e.g., Black Hat
  - Given enough money it is always possible
- Attacking the supply chain

BitLocker Attacks

- Cold boot, Firewire, BIOS keyboard
- Keys in TPM can be used if PIN is weak
- Incorrectly configured local DLP
  - E.g., Bitlocker can be set to Standby
- Same considerations for similar apps

What remains to be done?

- Database of known-good hashes
- Heuristics to determine provisional trust of new code
- What measurements to enforce, and when?

Thank you!

- Dan Griffin is the founder of JW Secure and is a Microsoft Enterprise Security MVP. Dan is the author of the books Cloud Security and Control and The Four Pillars of Endpoint Security and is a frequent conference speaker and blogger.
- Dan holds a Master’s degree in Computer Science from the University of Washington and a Bachelor’s degree in Computer Science from Indiana University.

Supporting Files

- http://fedscoop.com/gen-alexander-cloud-key-to-network-security/
- **Endpoint Security and Trusted Boot**

http://www.jwsecure.com/jw-secure-informer-15/

- Hacking Measured Boot and UEFI at DefCon 20