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

Dan Griffin

DefCon 2013

What does the NSA think?

- The NSA has been public about:
  - The inevitability of mobile computing
  - The need to support cloud-based services
  - Even for use with secret data in the field
- General Alexander, head of the NSA, recently spoke of using smartphones as ID cards on classified networks.
- What works for them can work for you

Introduction

- Mobile devices are everywhere and leak like a sieve
- But we know that there are more and more of them every day
- So now do we stop the impending implosion?

Current Technology Landscape

- Why are mobile devices less secure
  - Too hard to enter secure passwords by thumb
  - Current antimalware is not up to the task
  - Some are owned by user (ByoD to work)
- But Mobile devices are (nearly) all ARM
  - Which supports Trusted Platform Module 2.0
  - Some new ones are on Intel Atom with TPM 2.0
  - So what's holding them back from being secure

What is needed to be secure?

- Must measure the current state of the mobile device
  - TPM, measured boot, remote attestation
  - ARM TZ, SOC
  - Send bootlogs to the RAS
  - What measurements can we use?
  - Firmware hash, time, etc.
- Create a statement of health (claim) signed by RAS
  - Send to mobile device
  - So mobile devices can prove it is healthy

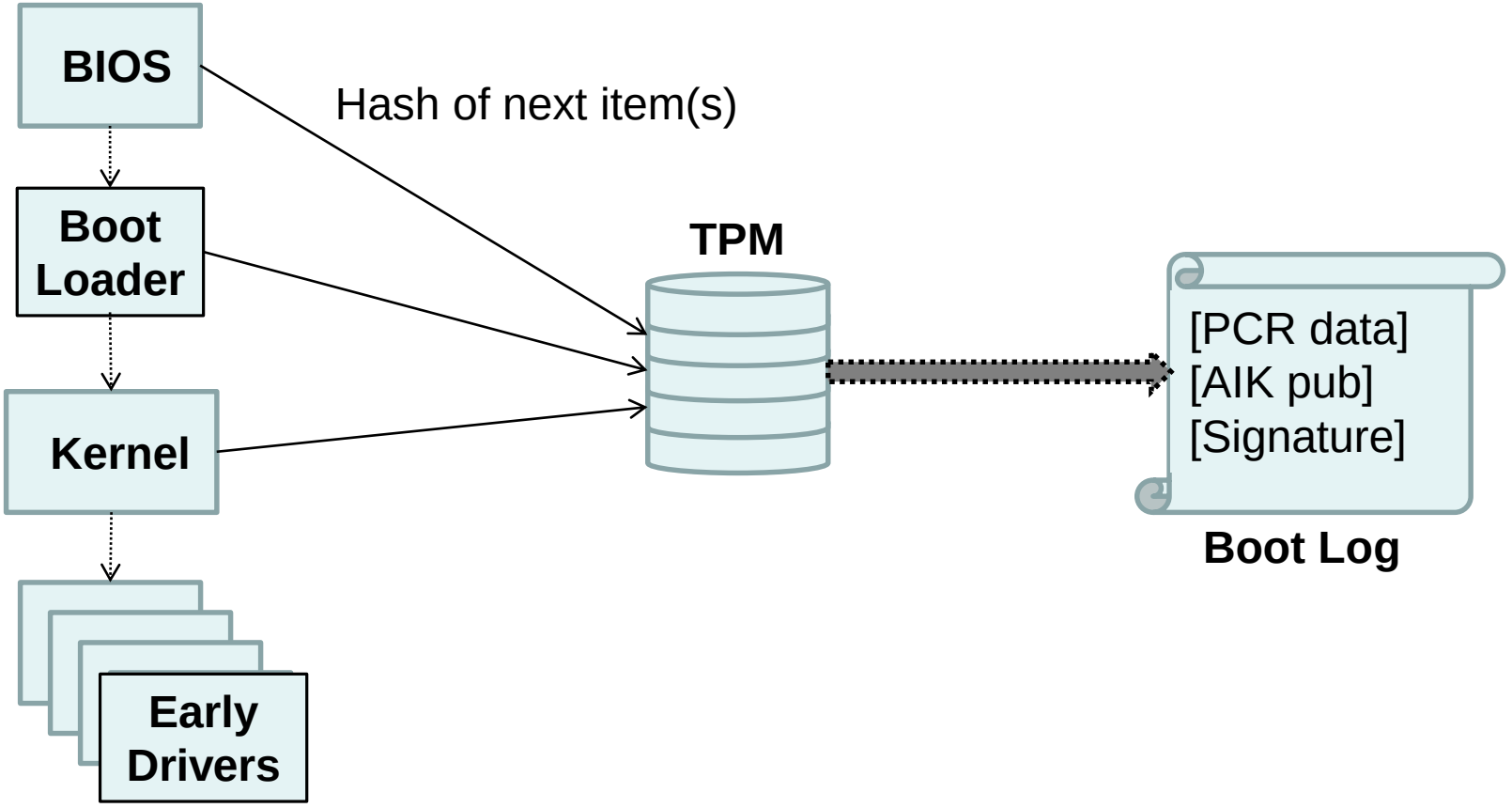
How to use the Health Claim

- The Device can use the health claim
  - To send to service to prove status
  - To unlock data protected on the device
- If the Device is measured to be insecure
  - Go to remediation
  - This is nothing new
    - works just like NAP today

Remote Attestation Service (RAS)

- Needs secure data from manufacturer
- Only ELAM is protected by TPM
  - State of ELAM in Windows *
- Still need traditional AM
  - Checks user mode code
  - Even that AM code is verified by the ELAM
- How does the content provider trust the RAS
  - Registration Authority

How does the RAS trust the Device?



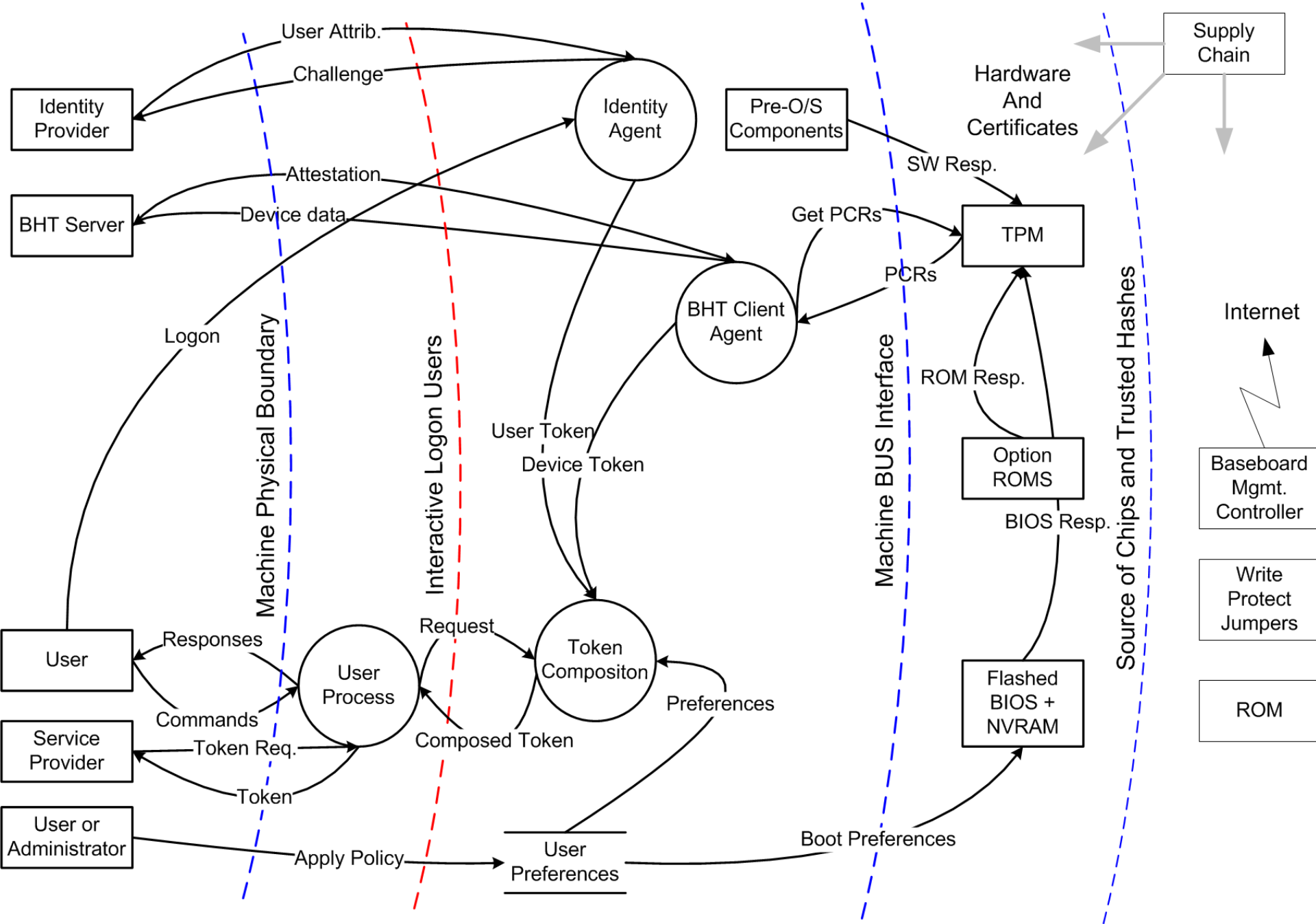
Is TPM/RAS really secure?

- Hardware root of trust secured within the TPM
  - Technical detail – firmware used by TPM 2.0
- PCRs are accumulated in secure location
- Send PCRs + boot log to RAS signed by TPM
- Secure time (actually just a boot counter)
  - How secure time works
  - What advantage does that give us?

DEMO of proof-of-concept code

- This has already be proven at RSA
- And several 3 letter agencies
- So, yes Virginia, there is a Santa Claus

Measured Boot – Threat Model



Policy-Enforced File Access

- BYOD
- Download sensitive files from document repository
- Leave laptop in back of taxi

What remains to be done

- Collecting signatures
  - from all BIOS and Early Launch code
- Heuristics to determine if new code should be provisionally trusted
- What the consumerization trend means for hackers
- Opportunities in this space

Supporting Files

- http://fedscoop.com/gen-alexander-cloud-key-to-network-security/
- **Endpoint Security and Trusted Boot** http://archive.constantcontact.com/fs007/1103180583929/archive/1110463148845.html
- Hacking Measured Boot and UEFI at DefCon 20

Speaker Bio

- Dan is the founder of JW Secure and is a Microsoft Enterprise Security MVP. He previously spent seven years working on smart cards and cryptography for Microsoft while on the Windows Security development team. He has published several articles on security software development, as well as on IT security, and is a frequent conference speaker.
- 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.