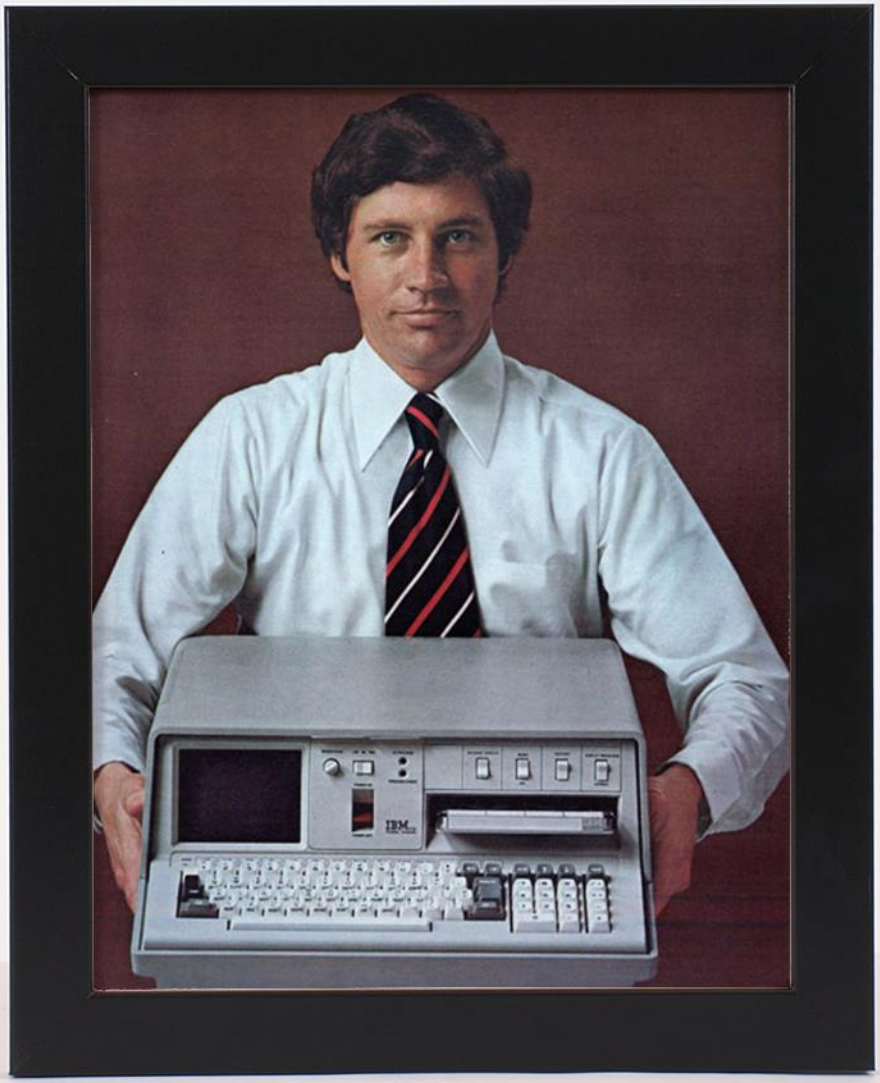
The Secret Life of Mobile Data

Cloud Developers Summit & Expo 2014
Dan Griffin
JW Secure, Inc.

WWNSAD?

- The NSA and NIST have 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



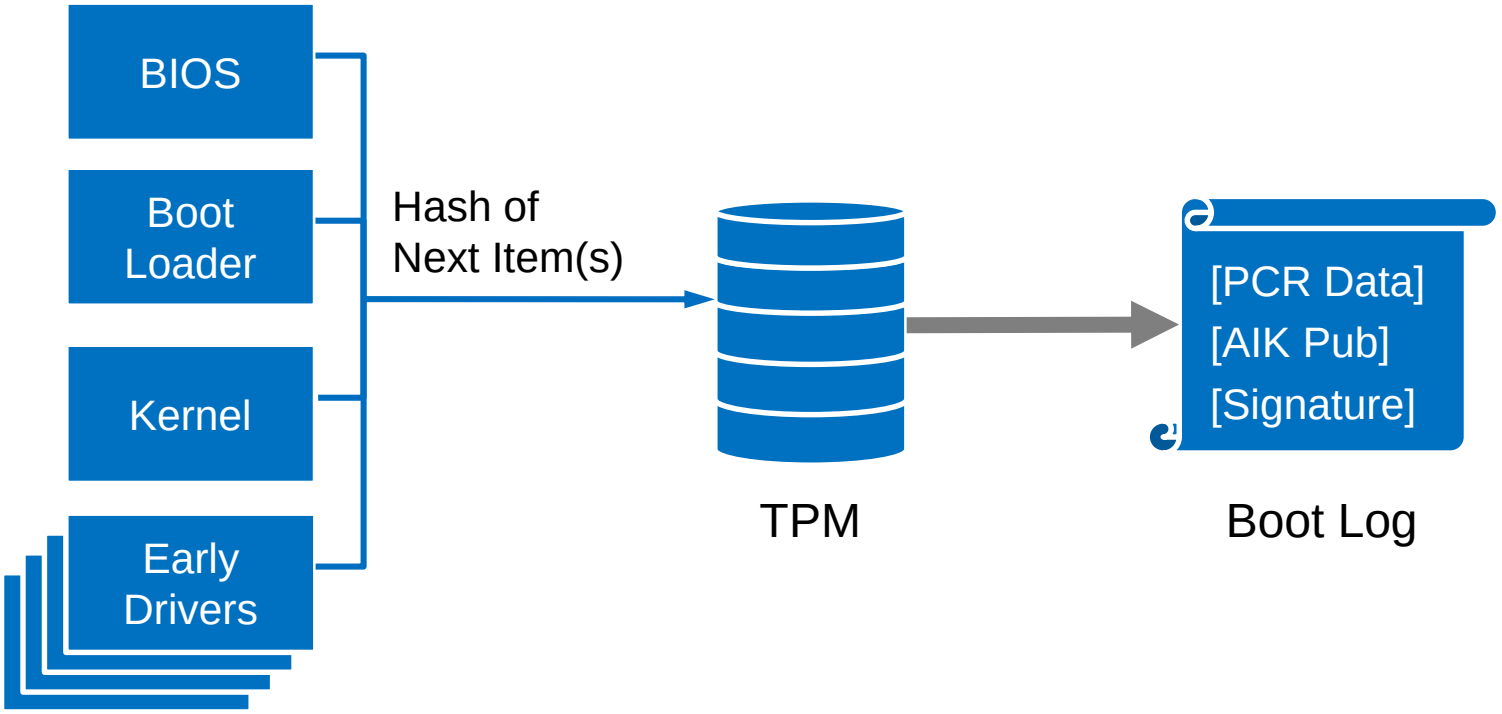
treo
Treo
12:38 pm
Card Info
CityTime
Carnival
Expense
Hot Snake
Memo Pad
McChords

Introduction

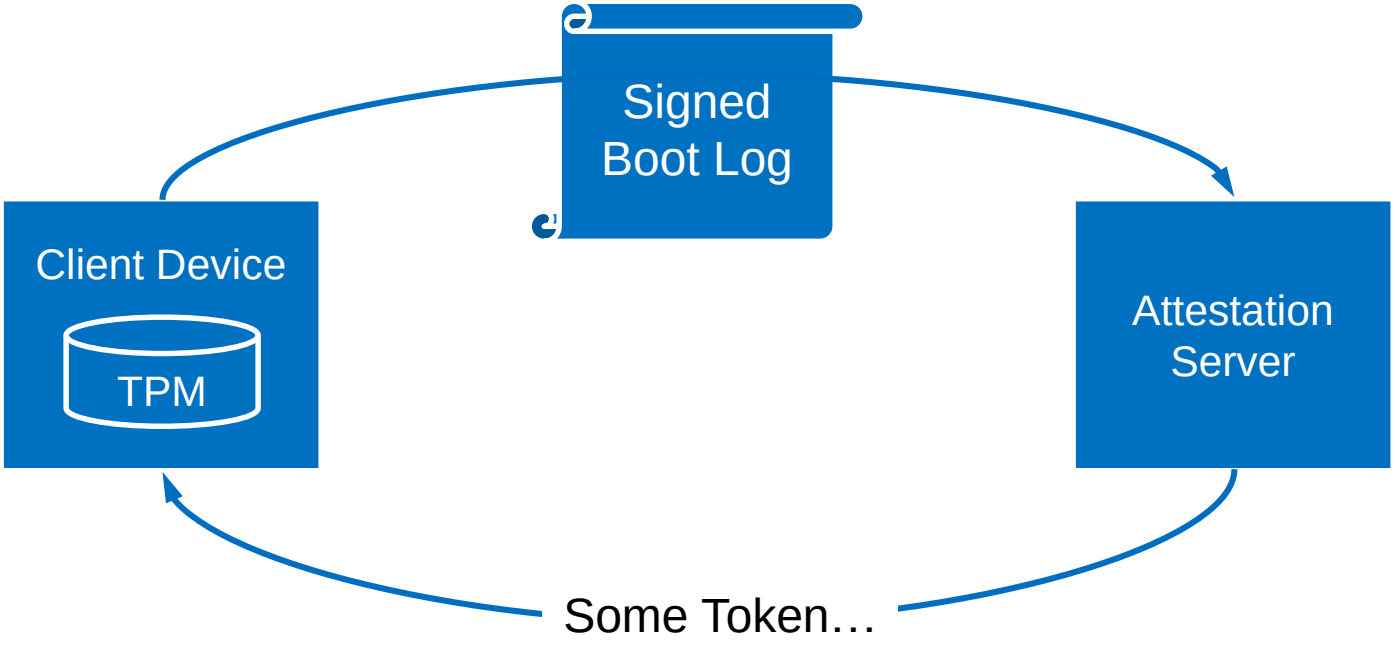
- What is a “TPM” (Trusted Platform Module)?
- What is “Measured Boot”?
- What is “remote attestation”?

Measured Boot and Remote Attestation

Measured Boot



Remote Attestation



Weaknesses

- Provisioning
  - Secure supply chain?
  - Manufacturer endorsement key database
  - Patching delay and whitelist maintenance
- Integrity of TPM hardware
  - Capping; electron microscopes
  - Trend of migration from hardware to firmware
- Hibernate file is unprotected (encrypt!)

Protecting Data with StrongNet™

- Data is encrypted
- Encryption key is bound to a specific, authenticated TPM
- Decryption is only possible when the device is policy-compliant
- Otherwise data cannot be viewed

Recent Developments

- Measurement-Bound Keys
  - “Trusted Tamperproof Time on Mobile Devices”
  - See jwsecure.com/dan
- Commercial availability
  - JW Secure StrongNet
  - Announced at RSA 2014

Questions?

dan@jwsecure.com

206-683-6551

@JWSdan

JW Secure provides custom security software development services.

"We know security, so you know who, when and why."

© 2014 JW Secure, Inc. All rights reserved.