Hacking Measured Boot and UEFI

Dan Griffin

JW Secure, Inc.

Introduction

- Who am I?
- What is UEFI?
- What is a TPM?

Hardware Landscape

- BYOD
- Capability standards
  - Phones
  - Tablets
  - PCs

Why Lock Down?

- OEM & ISV revenue streams
- Importance of app store based user experience
- Defense against rootkits & bad drivers

Demo #1

Measured Boot on Windows 8

Demo #2

Measured Boot Tool

Demo #3

LoB AuthN using Measured Boot

Weaknesses

- Provisioning
- Integrity of the TPM hardware
- Trend of migration from hardware to firmware

Conclusion

- Likelihood of mainstream adoption?
- What the consumerization trend means for hackers
- Opportunities in this space

Questions?

dan@jwsecure.com

206-683-6551

@JWSdan

JW Secure provides custom security software development services.