Cross Platform Management and Provisioning with the Intel Platform Innovation Framework for EFI

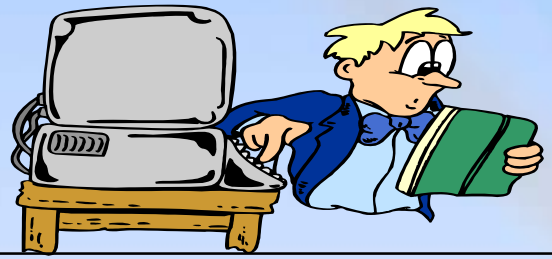
Vincent Zimmer
Staff Engineer
Intel SSG

Martin Wilde
Senior TME
Intel SSG

Agenda

- Current State of Affairs
- EFI solves problems
- Framework provides EFI
- Employing the Framework

Where are we today?



Integrator/OEM

Target machines

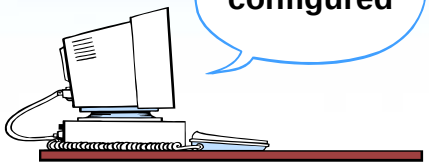
I am NOT configured

Client Model #4

I am NOT configured

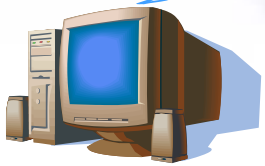
Client Model #1

I am NOT configured



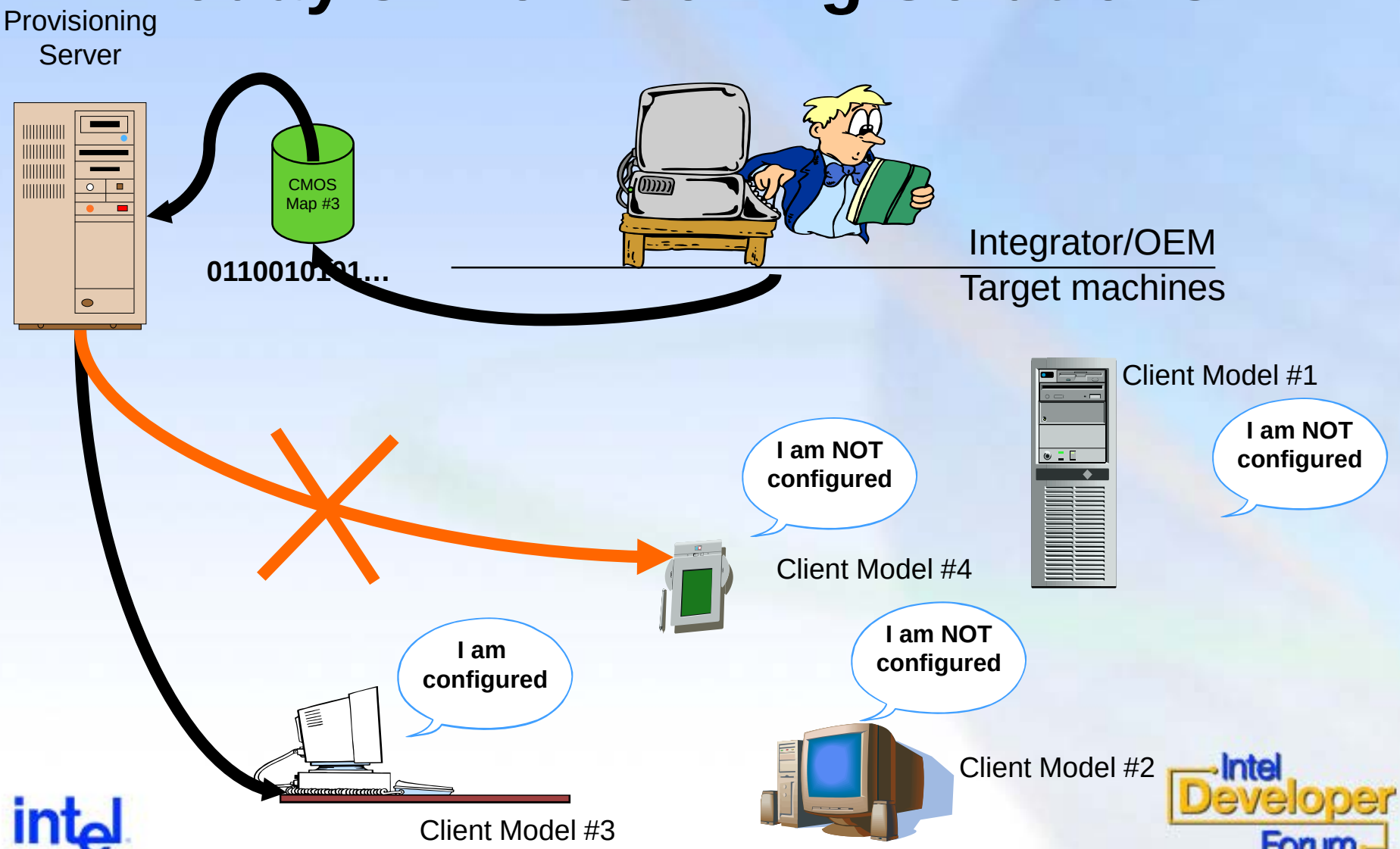
Client Model #3

I am NOT configured



Client Model #2

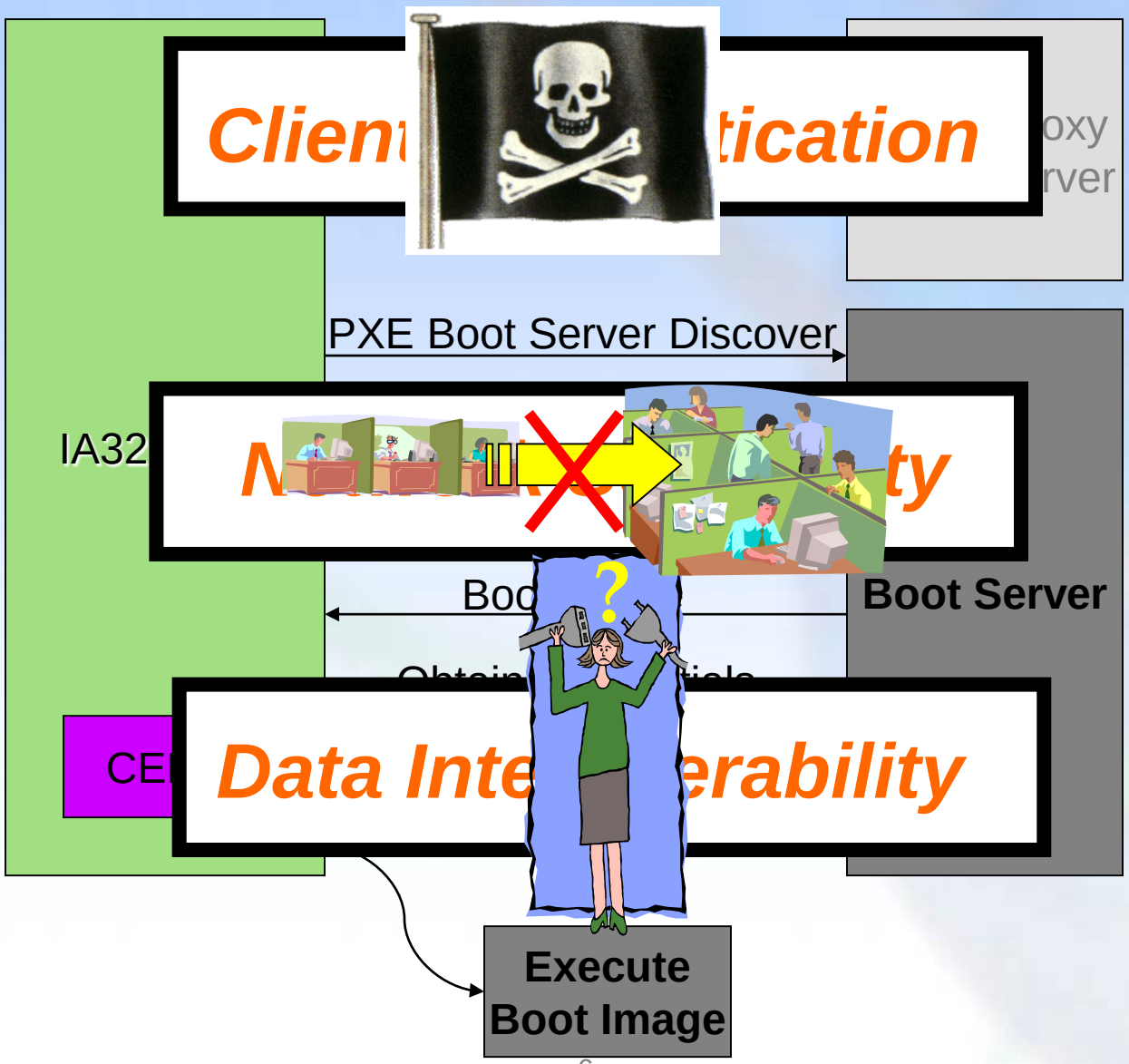
Today's Provisioning Solutions



What is Today's Technology

- PXE and BIS
  - Network boot standard introduced by WfM
- Homogeneous systems
  - PC/AT BIOS only
- Provisioning Agents and Servers
  - Each is different

Limitations Today



Head-aches for IT

- Lack of standards across platforms
  - PXE formerly limited to IA32 PC/AT BIOS
  - Setup does not automate well
- Insufficient security
  - No authentication of booting system
- Scalability concerns
  - Easy to saturate network w/ many clients
- Limited interoperability
  - Each infrastructure vendor has different solution

Current technology limited

The Future and EFI

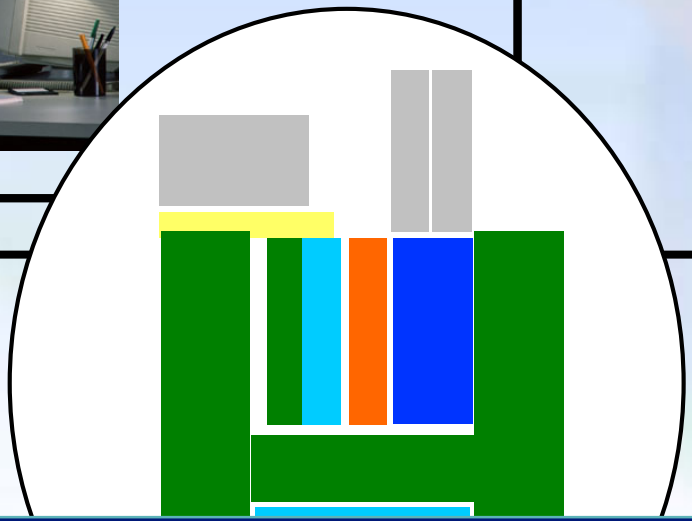
- Make computers more easily managed by other computers
- Enable secure automated management
- Scale technology across all platforms
- Solve the out-of-box configuration issues
- Standardize the technology aspects in the Framework to help reach this end
  - Sit tight & details to follow….

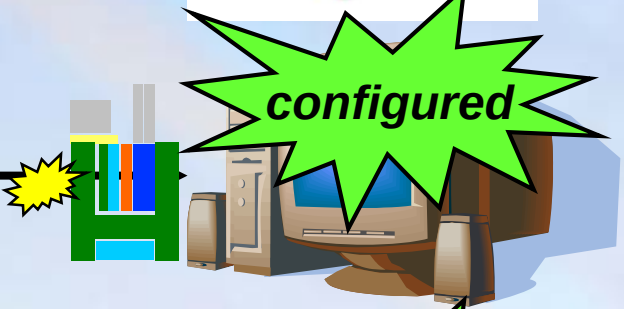
EFI Solves Problems

In an EFI-based world

IT Administrator

IT Policy: Schema-based description Of each machine





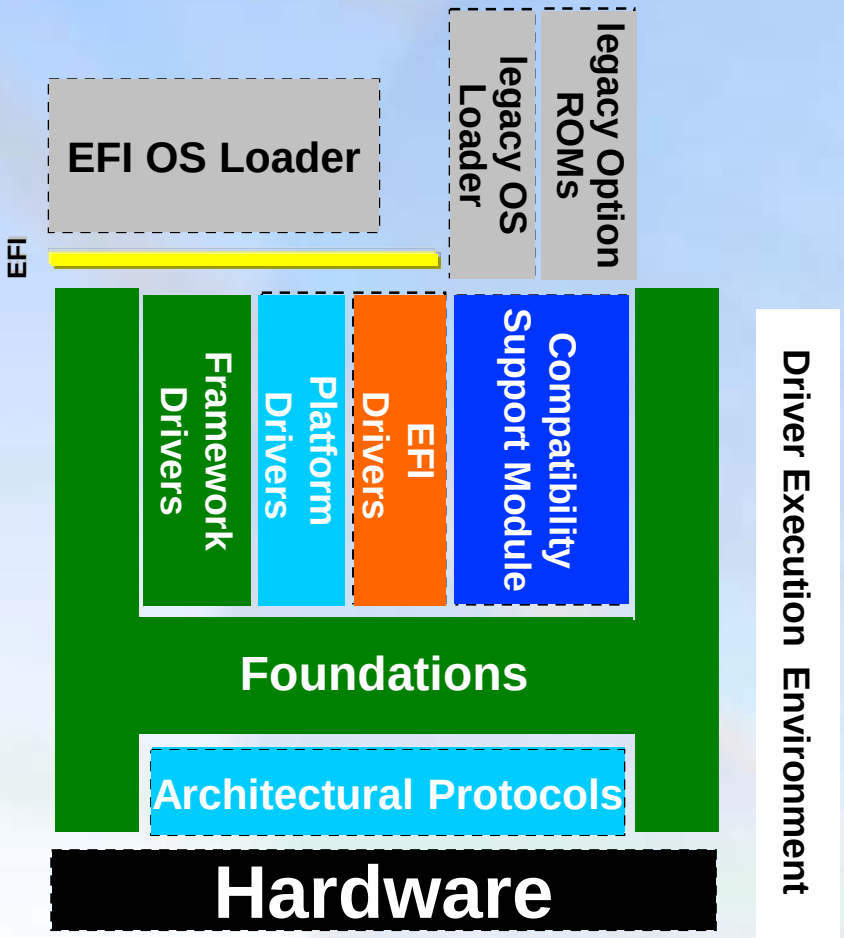
The Future Begins with EFI Everywhere

intel

Developer Forum

What is the Framework?

- Pre-EFI Foundation (PEI)
- Hardware-specific pre-EFI modules
- DXE Foundation
- Framework Drivers
- Hardware specific drivers and implementations of Architectural Protocols
- Platform Drivers
- EFI Drivers for adding value to the platform
- Compatibility Support Module (CSM)



Demo 1 “Basic Blocks” to solve problem

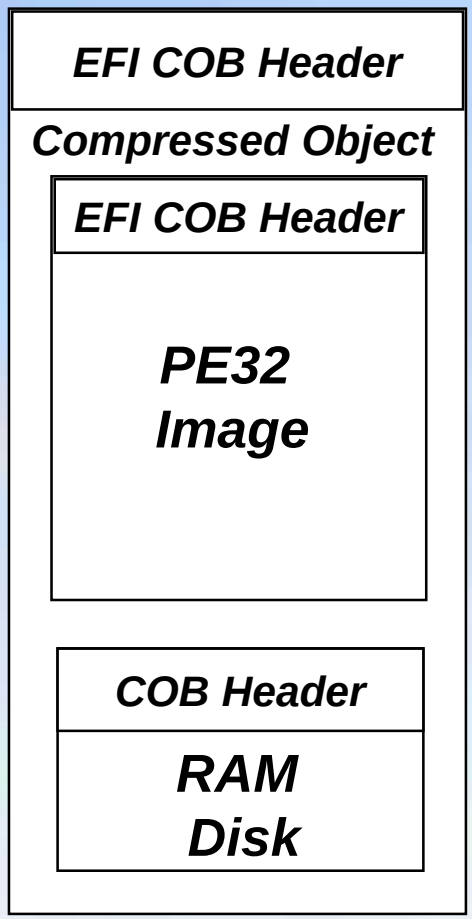
Move to EFI with the Framework

Configuration Building Block

- EFI Configuration Object (COB)
  - GUID'ed description of data
- Means by which for the OEM to add value
- Maintain the back-end IT infrastructure
- Allow for managing the integrity of the boot image and data

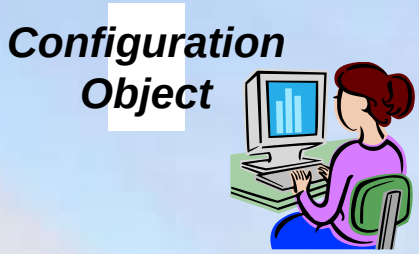
Configuration Building block and Provisioning

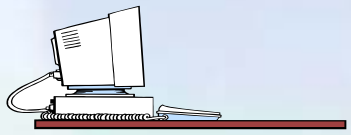
- EFI extends network boot program to be a collection of Configuration Objects
  - OEM provides standard objects
  - OSV provides modules that can be wrapped as standard objects
  - 3rd parties can provide value added objects
- Provisioning software appends EFI Objects together



Standardize platform information

- Configuration objects INTO the client
  - BIS Certificates
  - ASF Keys
  - iSCSI boot target
- Configuration objects FROM the client
  - SMBIOS tables
  - PCI configuration settings
- Both In and Out
  - Setup information





Network Scalability

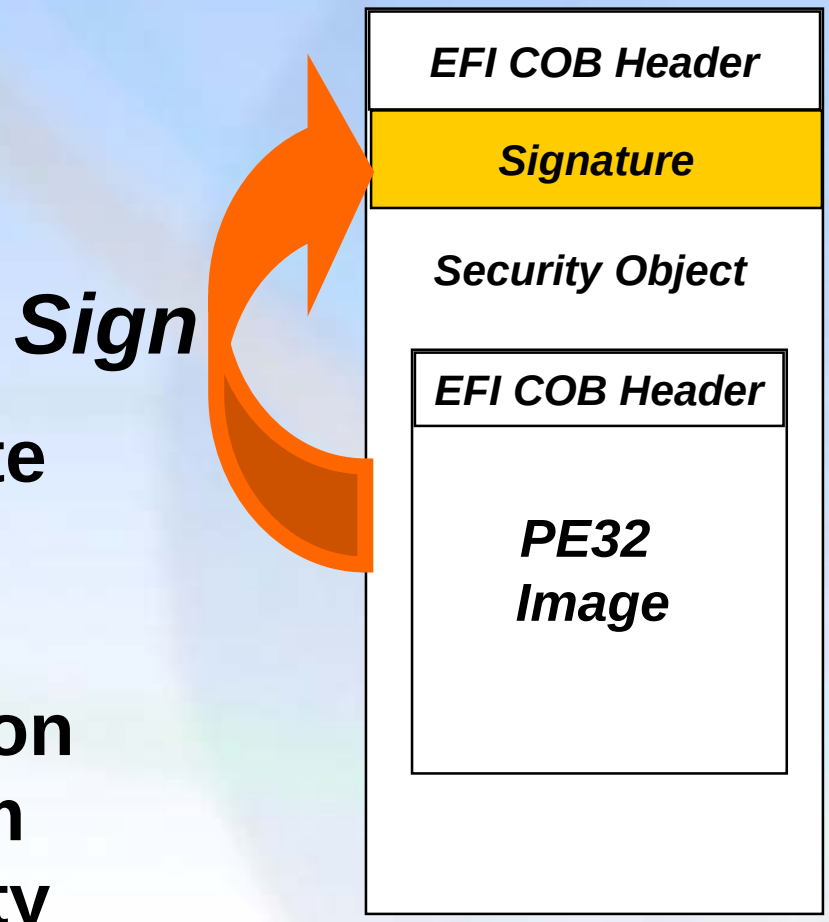
- Proposing RFCs to the IETF to multicast TFTP to improve scalability.
  - TFTP/MTFTP Block Count
    - Old 22 MB, New 2^{52} MB
  - Streaming Data
    - Removing acknowledgements for an approximate 50% performance improvement
  - Multi-Cast
    - Managed network saturation
- This entails software updates to BOTH the client and server software providers

Networking API Enhancements

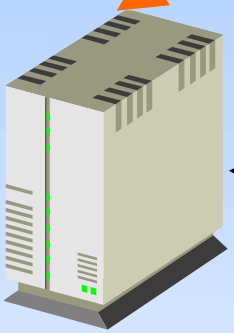
- Several new pre-boot API's
- Ability to now write several services on client
  - HTTP Server
  - Telnet Server
  - ….
- Published by client, usable by network boot agents and embedded code
  - Small, simple, in the flash part

Security problems to be Solved

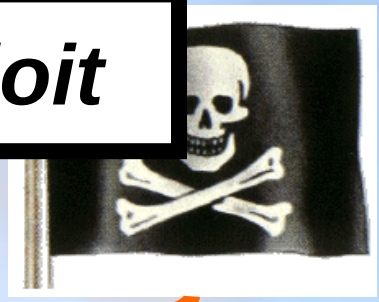
- Confirm identity of the client to be configured
- Associate appropriate PXE server with the client machine
- Send the configuration objects to the system with stronger integrity



Attack Vector - Server



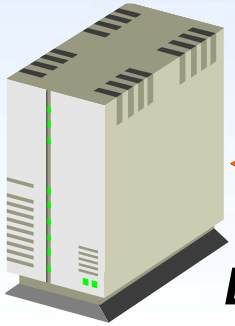
Successful Exploit



Rogue Server

Vintage Client

EFI Security Violation

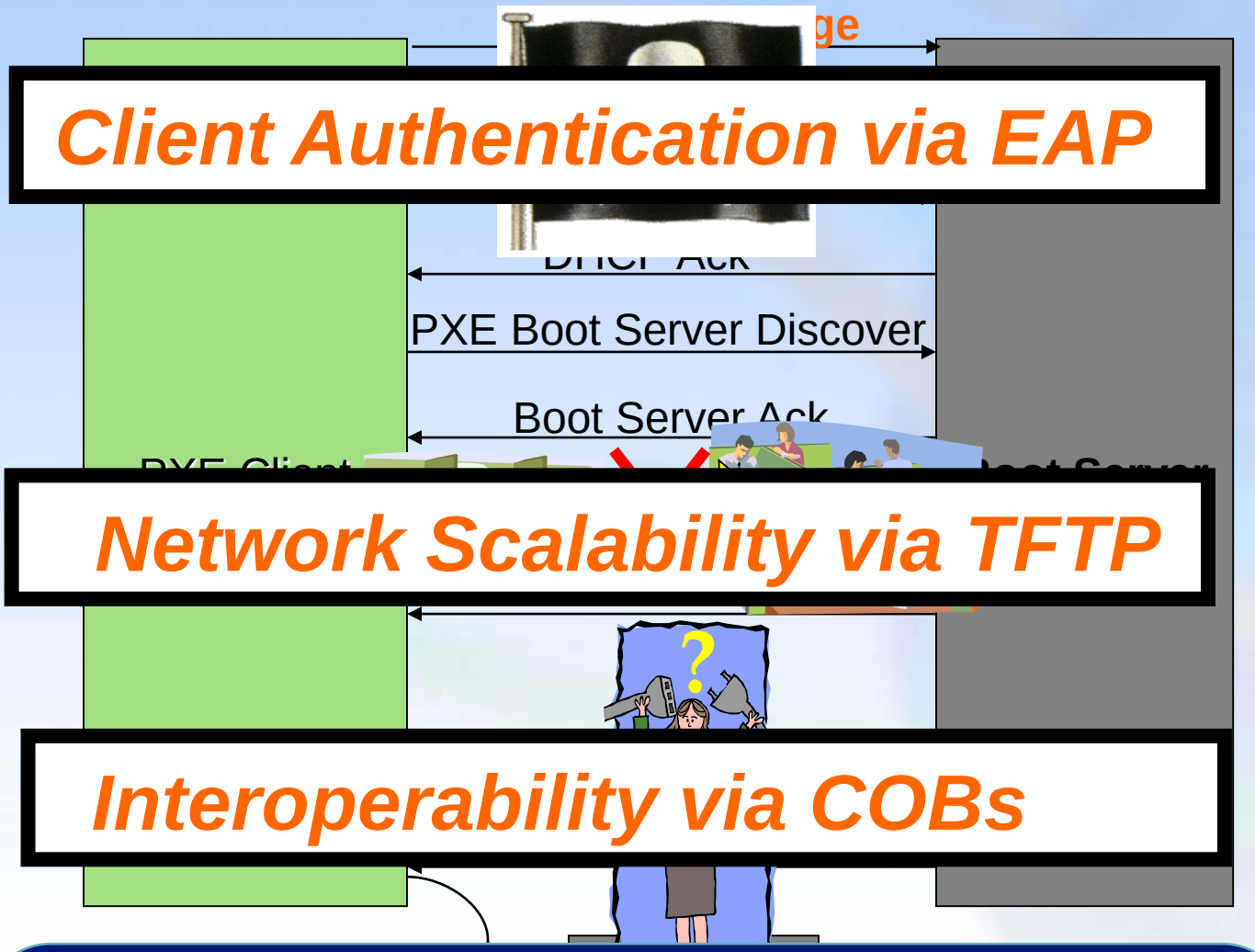


Enhanced Framework Client

PXE Server

Demo 2 Rogue attack

Tomorrow's Solutions



The Framework Removes Limitations

Summary

- Current Technology Limited
- The Future Begins with EFI everywhere
- Move to EFI with the Framework
- The Framework Removes Limitations

Call to action

- Platform builders move to Framework for enabling silicon
- Use the feedback
  - http://www.intel.com/technology/efi
  - http://www.intel.com/technology/framework
- Provisioning and OSVs investigate this technology
- IT investigate this technology

More Information

Session	#	Day	Time	Room
Intel® Platform Innovation Framework for EFI: *Overview, Roadmap and Getting Ready for Next Year*	S002	Tues	3:00-3:50 PM	2010
EFI IA32 and Microsoft	S003	Tues	5:00-5:50 PM	2010
Employing the Intel® Platform Innovation Framework for EFI for Mobile Platform Support	S004	Wed	10:00-10:50 AM	2010
OEM Firmware Development Using the Intel Platform Innovation Framework for EFI	S005	Wed	11:00-11:50 AM	2010

Birds-of-a-Feather Lunch Discussion

When: Wednesday 12PM – 1:30PM

Where: Level 3 Foyer ***(Not in the main lunch area)***

Arrive early – seating is limited

Q & A

Cross-Platform Management and Provisioning on the Intel® Platform Innovation Framework for EFI

http://www.intel.com/technology/framework

Please remember to turn in your session survey form.

Acronyms

- **ASF – Alert Standard Format**
  http://www.dmtf.org/standards/standard_alert.php
- **BIS – Boot Integrity Service**
  http://www.intel.com/design/security/bis/biswks.htm
- **CERT – Certificate like X.509**
  http://www.ietf.org/html.charters/pkix-charter.html
- **DHCP – Domain Host Controller Protocol**
- **RADIUS – Remote Authentication Dial-In User Service**
  http://www.faqs.org/rfcs/rfc2138.html
- **EAP – Extensible Authentication Protocol**
  http://www.faqs.org/rfcs/rfc2284.html
- **EFI – Extensible Firmware Interface**
  http://www.intel.com/technology/efi/main_specification.htm
- **802.1x – Port Based Network Access Control**
  http://www.ieee802.org/1/pages/802.1x.html
- **PXE – Preboot eXecution Environment**
  http://www.intel.com/technology/efi/

Acronyms

- **RCMP – Remote Management and Control Protocol**
  http://www.dmtf.org/standards/standard_alert.php
- **RFC – Request for Comment http://www.ietf.org**
- **TCO – Total Cost of Ownership**
- **TCP/IP – Transmission Control/Internet Protocol**
  www.faqs.org/rfcs/rfc793.html
- **TFTP – Trivial File Transfer Protocol**
- **TPM – Trusted Computing Group**
  http://www.trustedcomputinggroup.org
- **WBEM – Web-Based Enterprise Management**
  http://www.dmtf.org/standards/standard_wbem.php
- **WfM – Wired for Management**
  http://www.intel.com/labs/manage/wfm/index.htm