Network Boot in a Zero-Trust Environment with UEFI
Using SUSE & UEFI to Configure HTTPS Boot
Agenda

• Current State of Network Boot
• Limitations with the Legacy Model
• Modernizing Network Boot
• Use Cases for HTTP(S) Boot
• Call to Action
Current State of Network Boot

- Network client is Booted to a server on a local network.
- Boot based on Pre-Boot Execution Environment or PXE (defined by Wired for Management or WfM in the 1990’s).
- Architecture is based on the 16-bit Basic Input/Output System (BIOS).
- Requires a network controller to provide a low-level driver based on the Universal Network Device Interface (UNDI) format.
Limitations with the Legacy Model

- It doesn’t scale to large networks (limited to IPv4 & UDP).
- Must modify DHCP server to respond to PXE client queries.
- “Intranet”, not “Internet” - PXE server must be on same subnet or forward requests via proxy
- Router/Switch “fast learning spanning tree” may drop UDP packets.
- No security/authentication in PXE design.
- The first PXE server that responds will service the client (cannot specify server).
Limitations with the Legacy Model

- Legacy PXE is not designed for a “zero trust” network environment...
  “Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.”
  – CSO Online, Jan 2018
- Router/Switch using spanning tree may drop UDP packets.
- No security/authentication in PXE design.
- The first PXE server that responds will service the client (cannot specify server).
Modernizing Network Boot

The Unified Extensible Firmware Interface (UEFI) Specification introduces a number of improvements over the Legacy BIOS PXE.

- UEFI Networking Model.
- UEFI Network Boot via PXE.
- UEFI Secure Boot.
- UEFI Network Boot via HTTP/HTTPS.
UEFI 2.3.1+ Networking Model: IPv4 and IPv6

PXE BC / iSCSI (OS-boot-loader visible API’s)

Network App

- MTFTP4
- DHCP4
- TCP4
- UDP4
- IPv4
- ICMP
- IGMP

IP4CONFIG

Network App

- MTFTP6
- DHCP6
- TCP6
- UDP6
- IPv6
- ND
- MLD
- ICMPv6

IP6CONFIG

MNP

UNDI Driver (NIC UEFI Option ROM)

NIC
UEFI 2.3.1+ Network Stack (PXE and iSCSI)
UEFI Network Boot via PXE

- UEFI Network Boot was initially based on the PXE model.
- Added IPV6 & iSCSI/TCP features to existing IPv4 services.
- UEFI Secure Boot can provide a layer of authentication for PXE (signed bootloader, verified by certificates on client firmware).
- However… *none of the PXE limitations listed earlier are resolved by UEFI because they’re part of PXE architecture (unencrypted traffic via UDP).*
UEFI 2.5 HTTP(S)
Boot from URL/filename

<table>
<thead>
<tr>
<th>Driver</th>
<th>Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Boot Driver</td>
<td>HTTP Library</td>
</tr>
<tr>
<td>HTTP Driver</td>
<td>TlsLib Library</td>
</tr>
<tr>
<td>HTTP Utilities Driver</td>
<td>OpensITlsLib Library</td>
</tr>
<tr>
<td>TLS Driver</td>
<td></td>
</tr>
</tbody>
</table>

• Flexible Network Deployment
• Home Environment Support
• Corporate Environment Support
HTTP(S) Boot via UEFI Firmware

- Boot file URL, using IP address or DNS (i.e. www.xyz.com/bootme.efi).
- Works on any network topology supporting TCP & HTTP(S).
- Supports IPv4/IPv6, not limited to a single subnet.
- Supports UEFI Secure Boot for additional verification.
- HTTPS only allows URLs that can be verified via client certificates.
- Combine with RAMDisk to download package to local file system.
Putting the ‘S’ in HTTPS: Enrolling Certificates

Currently, UEFI HTTPS Boot only supports server authentication with an unauthenticated client. This requires enrolling a Server CA certificate (rootcert.pem) on the Client prior to boot.

Reference: Getting Started with UEFI HTTPS Boot on EDK II
Use Cases for HTTP(S) Boot

- Install/deployment of OS (with default ISO, if using RAMDisk).
- Firmware update without an OS (via UEFI Capsule Update).
- System recovery from LAN or cloud storage.
- Diskless systems boot to OS via HTTPS (blade, thin client, …).

*Use cases are extended beyond traditional “trust boundaries”*
Distributions that support install via UEFI HTTP(S)

Can install SUSE or openSUSE from a host server via UEFI HTTPS

- openSUSE 42.3 - HTTPS
- SUSE SLES 15 - HTTPS
- SUSE SLES 12 SP3 - HTTP (no HTTPS at this time)
Call to Action

Upgrade from legacy PXE boot to address “zero trust” model

Investigate UEFI Secure Boot & HTTP(S) boot implementations

Review openSUSE documentation for HTTP(S) configuration
Resources and References

https://github.com/tianocore/tianocore.github.io/wiki/HTTPS-Boot
https://www.tianocore.org/
https://www.uefi.org

Thanks to Harry Hsiung (Intel) for setting up the demo system.

Thanks to Gary Lin and Joey Lee (SUSE) for their work on UEFI support in SUSE/openSUSE and the related HTTP/HTTPS documentation.
UEFI HTTP(S) Installation Instructions

Setup UEFI HTTPS boot in OVMF (virtual environment)
https://en.opensuse.org/UEFI_HTTPPBoot_with_OVMF

Setup UEFI HTTPS for Physical Host Server
https://en.opensuse.org/UEFI_HTTPPBoot_Server_Setup

HTTP/HTTPS Boot Getting Started Guide for EDK II
Information on UEFI Systems with HTTP(S)

Information on HTTP(S) Boot in EDK II
https://github.com/tianocore/tianocore.github.io/wiki/HTTP-Boot
https://github.com/tianocore/tianocore.github.io/wiki/HTTPS-Boot

EDK II Open Virtual Machine Firmware (OVMF)
https://github.com/tianocore/tianocore.github.io/wiki/OVMF

MinnowBoard Max Turbot (support included in firmware images)
https://firmware.intel.com/projects/minnowboard-max

Hewlett Packard Enterprise* Proliant Gen10 servers
https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00016376en_us
Join Us at www.opensuse.org
License
This slide deck is licensed under the Creative Commons Attribution-ShareAlike 4.0 International license. It can be shared and adapted for any purpose (even commercially) as long as Attribution is given and any derivative work is distributed under the same license.

Details can be found at https://creativecommons.org/licenses/by-sa/4.0/

General Disclaimer
This document is not to be construed as a promise by any participating organisation to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. openSUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for openSUSE products remains at the sole discretion of openSUSE. Further, openSUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All openSUSE marks referenced in this presentation are trademarks or registered trademarks of SUSE LLC, in the United States and other countries. All third-party trademarks are the property of their respective owners.

*Other names and brands may be claimed as the property of others
© 2019 Intel Corporation

Credits
Template
Richard Brown
rbrown@opensuse.org

Design & Inspiration
openSUSE Design Team
http://opensuse.github.io/branding-guidelines/

*Other names and brands may be claimed as the property of others
Glossary

- IPv4 - Internet Protocol version 4
- UDP - User Datagram Protocol
- HTTP - Hypertext Transfer Protocol
- HTTPS - Hypertext Transfer Protocol Secure
- ISCSI – Internet Small Computer Systems Interface
- MTFTP – Multicast Trivial File Transfer Protocol
- DHCP – Dynamic Host Configuration Protocol
- TCP – Transmission Control Protocol
- ARP – Address Resolution Protocol
- MNP – Microcom Networking Protocol
- NIC – Network Interface Controller
- SNP – Scalable Networking Pack
- TCP/IP – Transmission Control Protocol/Internet Protocol
- TFTP – Trivial File Transfer Protocol
- TLS – Transport Layer Security
- BDS – Boot Device Selection
- URL – Uniform Resource Locator
- NII – Network Independent Interface
- ISO - International Organization for Standardization
Backup - Legacy PXE Stack Overview

UNDI provided by Platform BIOS or network controller Option ROM
Member Event: Spring 2019 UEFI Plugfest

April 8-12, 2019

Embassy Suites by Hilton Seattle Bellevue Bellevue, WA

All UEFI members are welcome to attend testing sessions, technical sessions, and networking events.

For more information go to the events page

To Join UEFI Forum go to the membership page

https://uefi.org/events/