



Network Nightmare

Ruling the nightlife between
shutdown and boot with pxesloit

#whoami

- Matt Weeks
- Scriptjunkie if you hang out on irc
- I have a twitter but I don't use it
- <http://www.scriptjunkie.us/>
- scriptjunkie {shift+2} scriptjunkie.us

What's going on here

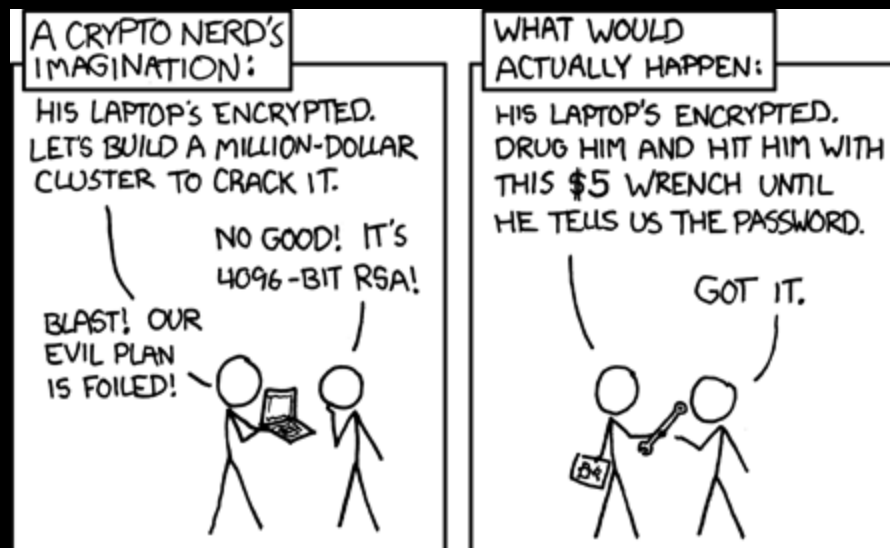
- To compromise another LAN system...
- Legit credentials
- Write an 0-day for [network service]
 - But that can take a lot of time
 - Fuzzing/static analysis -> Vulnerability ID -> exploit
 - > Bypass protections -> ... escalate privs

Easier way?

- How about we try an offline attack?

Offline attacks

- Evil maid attack
- Rubber hose cryptanalysis



Downsides

- Physical access
- Unstealthy
- Jail?
- Still common

PXE

[preboot execution environment]

PXE

- Intel-introduced firmware to boot from NIC
- BIOS-level access
 - Full system control
 - Bypass host hardening/OS/AV
 - OS-agnostic
 - Network!

How it works

- Step 1 – Your computer shuts down



How it works

- Step 2 – Wake up ... something's different



(The Godfather) © 1972 Paramount Pictures

PXE Proliferation

- Almost every system BIOS is PXE-capable
- How widely enabled?
- I have seen PXE ...
 - left on
 - occasionally enabled & used
 - turned off

Why would Intel do this to us?

- Top syadmin reasons:
 - Image deployment
 - System restoration
 - Just in case
 - What's that? I have that on?



How PXE works

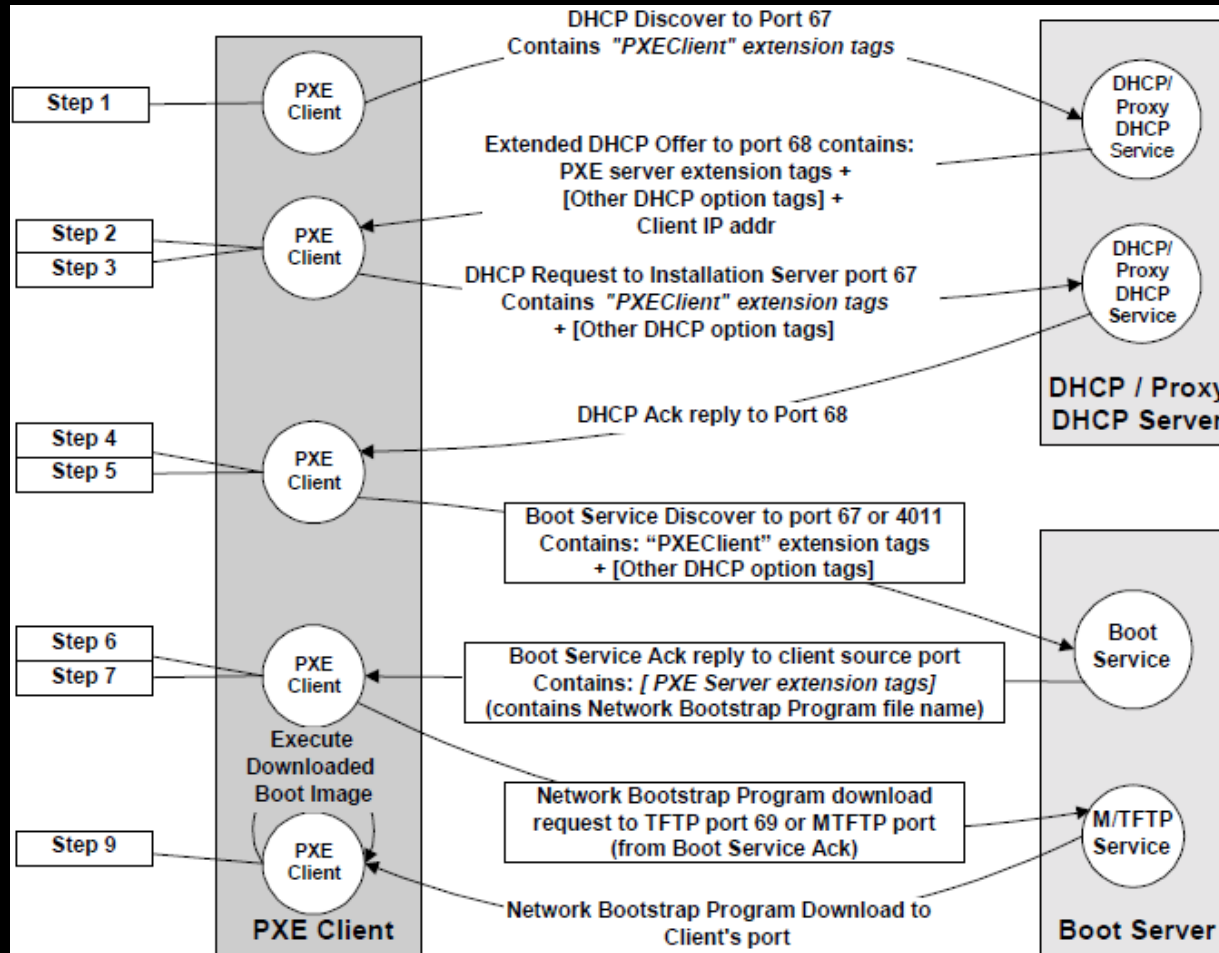


Figure 2-1 PXE Boot

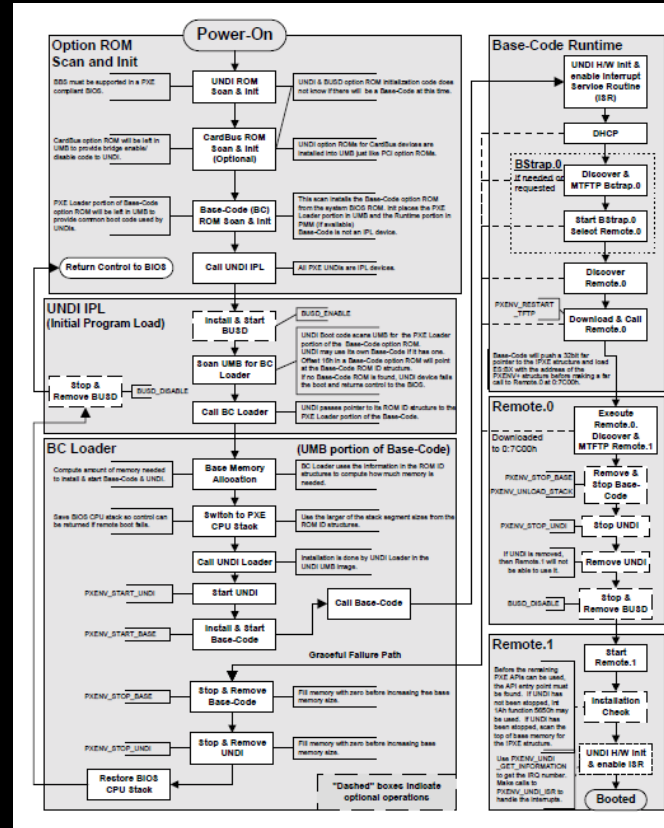
PXE Difficulties

- Passive
 - Wait
 - Wake-on-LAN
- DHCP extension
 - Race condition
- Forward to TFTP
- Execute code
 - Code running on bare metal

PXE Difficulties

Preboot Execution Environment (PXE) Specification

Version 2.1

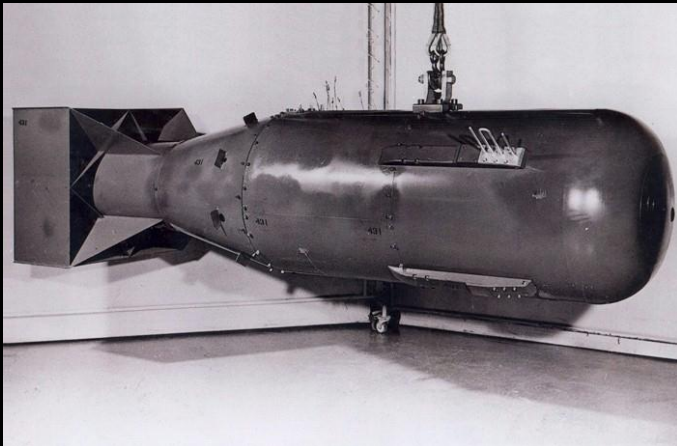


Current PXE “attacks”

- Not attack-oriented
- Admin tools
 - Imaging
 - PxeLinux

Current PXE “attacks” - Imaging

- Requires server software
- Time-consuming
- Imaging = wipe out data



Current PXE “attacks” - PXELinux

- Manual PXE server creation
- Manual DHCP configuration
- Difficult to deploy remotely
- Unreliable or lack targets
- Lack custom payloads



Online Control

Online Control

- PXE-bootable Linux live CDs
 - DSL
 - Tiny Core
 - Knoppix
- Strategy
 - Remaster live CD
 - Boot live CD via PXE
 - Auto-run scripts connect back
 - Shell!

Online Control Demo

Online Control Advantages

- Any OS
- Flexibility
- No need to code the whole attack beforehand

Online Control Problems

- MyNetworkCard™ drivers
 - Distro != initrd
- Time
 - Human in the loop
 - Visual indicators

Offline Code Injection

Offline Code Injection

- You'll do it anyway
- Root outside < admin inside

Offline Linux Code Injection

- Shellcode on boot
 - Write/edit file to RCE
 - /etc/init.d/...
 - ~/.bashrc etc
- User add
 - /etc/passwd
 - ~/.ssh/authorized_keys

Offline Windows Code Injection

- Bootkits
- Binary planting
- Binary swapping
- Binary embedding/modification
- DLL preloading
- Registry edits
- Binary swapping + service editing

Note!

- This presentation will not be addressing FDE
- See cold boot attack or evil maid attack details

Bootkits

- Sinowal
- Stoned
- Whistler
- TDL/Alureon
- eEye BootRoot (PiXiE)

Bootkits: Advantages

- Skillz points
- Stealth
- Full privileges



Copyright © 1985-2004
Microsoft Corporation

Microsoft

voxx - Belchfire

Bootkits: Disadvantages

- OS-specific
- Fail when MS patches OS protections
- Work factor

Binary Planting

- Startup folders
 - C:\Documents and Settings\All Users\Start Menu\Programs\Startup
 - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
 - Unprivileged
- WBEM .mof method
 - **Stuxnet!**
 - Not compatible with Vista+

Binary Swapping

- Example:
 - Swap services/svchost/wininit/...
 - Spawn old exe and payload
 - Swap back
- Advantages:
 - Guaranteed RCE
 - Portable



Binary Swapping Problems

- Bluescreens
 - Early processes bluescreen on exit
 - Cleanup requires exit
- Disabled services
 - Late process non-critical
 - Spoolsv.exe ...

```
A problem has been detected and windows has been shut down to prevent damage to your computer.
```

```
PANIC_STACK_SWITCH
```

```
If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:
```

```
Check to make sure that any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.
```

```
If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup options, and then select Safe Mode.
```

```
Technical information:
```

```
*** STOP: 0x0000002B (0x00000000,0x8A5F340D,0x00000008,0xC0000000)
```

```
***   rspndr.sys - Address 8A5F340D base at 8A5F1000, DateStamp 36B0052A
```

Binary Embedding/Modification

- Inject additional code into existing .exe files
 - svchost/wininit/winlogon/...
- Example:
`msfvenom -f exe -x svchost.exe -k -p - < pay > a.exe`

Binary Embedding Problems

- Architectures
 - x86 != x64
- Slack space
- Cleanup

DLL Preloading

- Swap system dll
- Add dll higher in search path
- Problems:
 - Architecture
 - Imports
- Still an option

Registry Edits

- Lots of options!
 - Run keys -
HK(LM|CU)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - Reliable
 - Unprivileged
 - Service addition
HKLM\SYSTEM\CurrentControlSet\Services
 - Privileged!
 - OS version differences

Registry Edits

- Service Editing

 - HKLM\SYSTEM\CurrentControlSet\Services

 - Privileged!
 - Change binpath string
 - Check type, start

- Known DLL's

 - Privileged!
 - Add string

- And others

Registry Edits

- Linux initrd
- Adding registry data
- Chntpw's ntreged library
- Warning ...
- HKLM corruption =
game over



Photo from Cleveland.com

Binary Swapping + Regedit

- Swap a non-essential service
- Edit DWORD start value
- Profit

Binary Swapping + Regedit

- Reliable
- No bluescreens
- Cross-arch
- No registry corruption warnings



Pivoting

Pivoting

- Attacking other systems on LAN
- Run in memory via meterpreter
 - Railgun
 - Network delay
 - Extension
 - Compiled program

Meterpreter Review

- TLV request
- Embedded DLL
- Reflective Loader
- Method Calls

Attack Recap

1. Dynamic payload generation
 1. [wake-on-LAN]
2. DHCP forwarder
3. TFTP serve
4. PXELinux kernel, initrd load
5. Binary swap
6. Registry edit
7. Reboot to OS
8. Swapped EXE spawns payload, cleanup

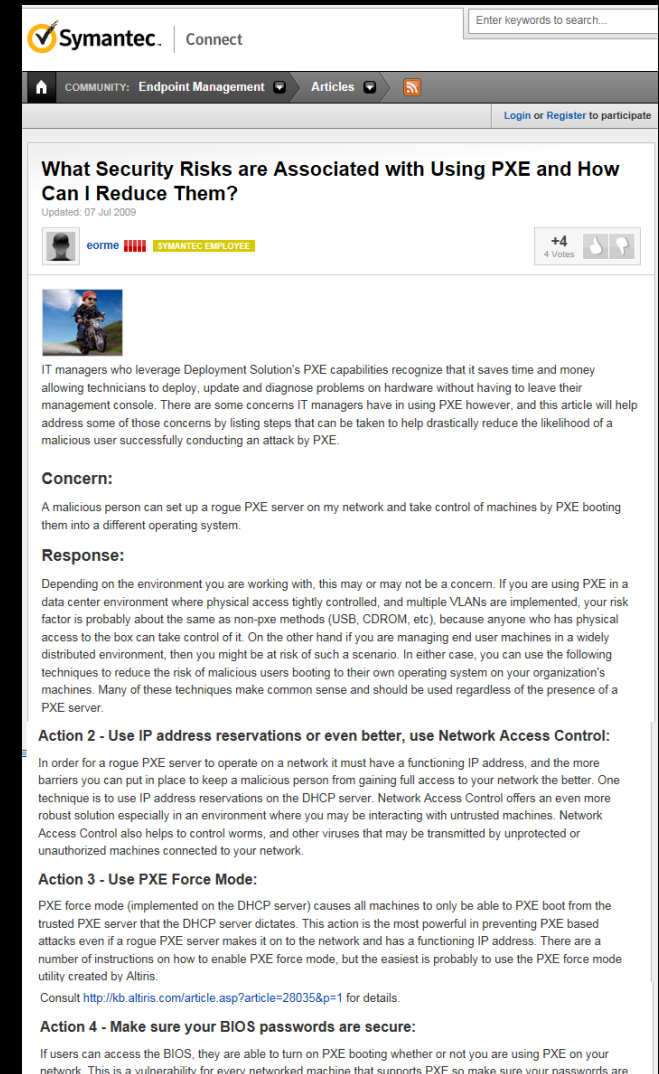
Metasploit Demo

The background is a dark blue, textured surface with a faint, abstract map of South America. The map is rendered in a lighter blue, almost white, color, showing the outline of the continent and its major landmasses. The texture of the background is grainy and slightly mottled, giving it a sense of depth and movement.

Defense

Defense: Fail

- Lots of bad advice
- How to fail at defense:
 - IP reservations
 - NAC
 - PXE Force Mode
 - BIOS passwords



The screenshot shows a Symantec community article page. At the top, there is a search bar and navigation links for 'COMMUNITY: Endpoint Management' and 'Articles'. The article title is 'What Security Risks are Associated with Using PXE and How Can I Reduce Them?' with an update date of '07 Jul 2009'. The author is 'eorme', a Symantec employee, with a rating of +4 votes. The article content includes an introduction, a 'Concern' section about rogue PXE servers, a 'Response' section discussing physical access and network security, and four numbered actions: 1. Use IP address reservations or even better, use Network Access Control; 2. Use IP address reservations or even better, use Network Access Control; 3. Use PXE Force Mode; 4. Make sure your BIOS passwords are secure.

What Security Risks are Associated with Using PXE and How Can I Reduce Them?
Updated: 07 Jul 2009
+4
4 Votes

Concern:
A malicious person can set up a rogue PXE server on my network and take control of machines by PXE booting them into a different operating system.

Response:
Depending on the environment you are working with, this may or may not be a concern. If you are using PXE in a data center environment where physical access tightly controlled, and multiple VLANs are implemented, your risk factor is probably about the same as non-pxe methods (USB, CDROM, etc), because anyone who has physical access to the box can take control of it. On the other hand if you are managing end user machines in a widely distributed environment, then you might be at risk of such a scenario. In either case, you can use the following techniques to reduce the risk of malicious users booting to their own operating system on your organization's machines. Many of these techniques make common sense and should be used regardless of the presence of a PXE server.

Action 2 - Use IP address reservations or even better, use Network Access Control:
In order for a rogue PXE server to operate on a network it must have a functioning IP address, and the more barriers you can put in place to keep a malicious person from gaining full access to your network the better. One technique is to use IP address reservations on the DHCP server. Network Access Control offers an even more robust solution especially in an environment where you may be interacting with untrusted machines. Network Access Control also helps to control worms, and other viruses that may be transmitted by unprotected or unauthorized machines connected to your network.

Action 3 - Use PXE Force Mode:
PXE force mode (implemented on the DHCP server) causes all machines to only be able to PXE boot from the trusted PXE server that the DHCP server dictates. This action is the most powerful in preventing PXE based attacks even if a rogue PXE server makes it on to the network and has a functioning IP address. There are a number of instructions on how to enable PXE force mode, but the easiest is probably to use the PXE force mode utility created by Altiris.
Consult <http://kb.altiris.com/article.asp?article=28035&p=1> for details.

Action 4 - Make sure your BIOS passwords are secure:
If users can access the BIOS, they are able to turn on PXE booting whether or not you are using PXE on your network. This is a vulnerability for every networked machine that supports PXE so make sure your passwords are

Defense: Less Fail

- Detection of rogue DHCP servers
 - Scan periodically
 - Check for duplicate replies
 - Check for ARP poisoning
 - Check for unregistered clients if possible

Defense: Good Idea

- Firewalls
 - Only allow DHCP traffic to/from server
 - Watch for ARP poisoning

Defense: Better Idea

- VLAN isolation
 - Separate systems via VLAN
 - Localize broadcast domains
 - Forward DHCP traffic
 - Configure via enterprise switch/routers

Defense: Great Idea

- Boot Integrity Services
 - + PXE extension
 - + Only runs signed code
 - Must install certificate in all PXE clients
 - Requires compatible firmware

Defense: Best Idea

- Turn it off

Questions

