



Weapons of Mass Pwnage: Attacking Deployment Solutions

DeepSec 2009

Luke Jennings

20th November 2009



Outline

- Introduction
- Threat Vectors
- Environment Concerns
- Case Study: Altiris Deployment Solution
- Defence
- Q&A



Introduction



What are they?

- Systems for centrally managing large networks
- Provision new machines
- Support thin client networks



Why use them?

- Centralised management = easier management
- Easier Management = better consistency
- Combination = lower operational costs and better quality



So why me?

- Why pwn just one system....?
- Used in enterprise environments
- Seem to have (security) issues...
- Often used to improve security...



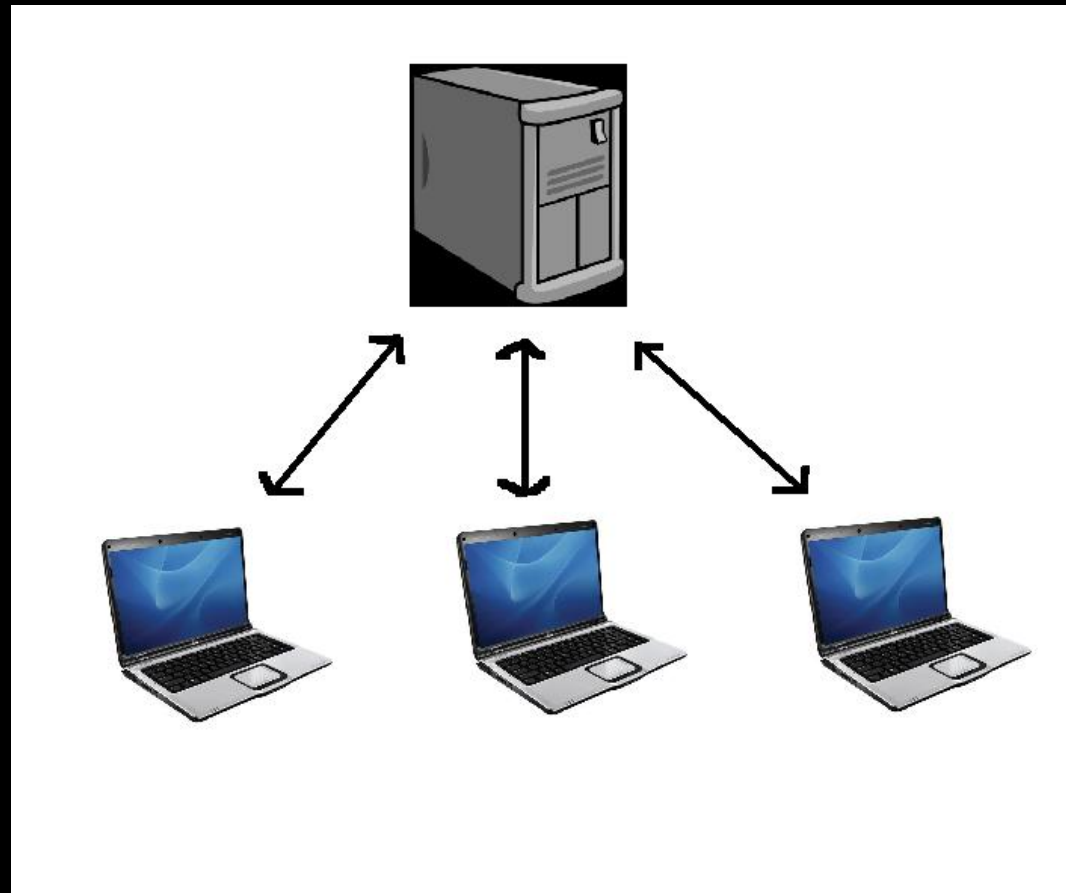
Outline

- Introduction
- Threat Vectors
- Environment Concerns
- Case Study: Altiris Deployment Solution
- Defence
- Q&A

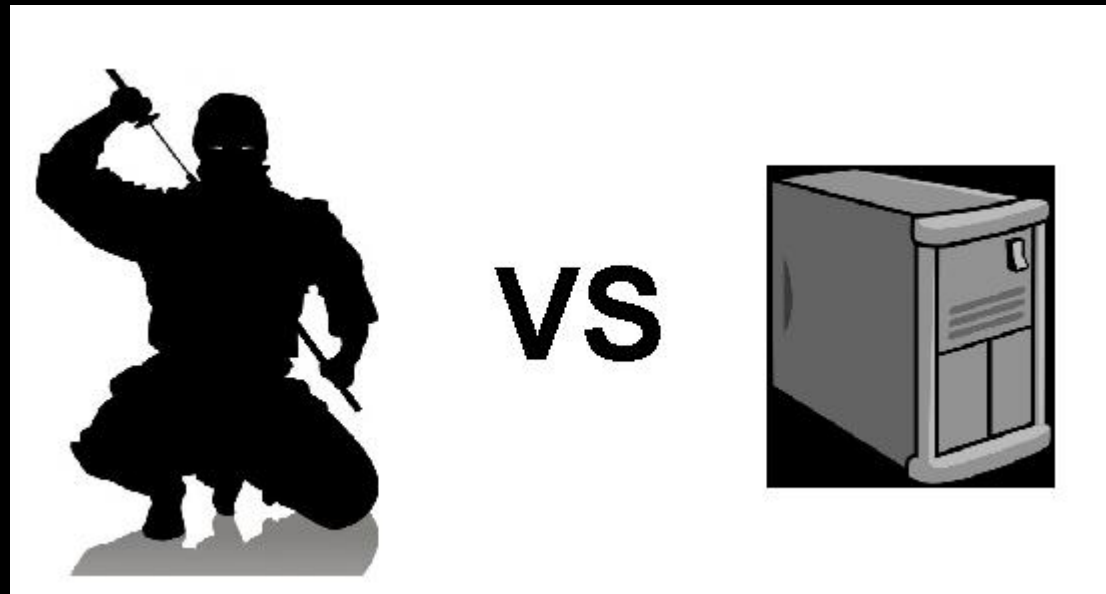


Threat Vectors

Basic Architecture Assumption



Deployment Server Attacks





Client Attacks





Methods of Conducting These...

- The usual suspects...
- Direct Attacks
- Server Impersonation
- Client/Server Traffic Interception
- The malicious client



Outline

- Introduction
- Threat Vectors
- Environment Concerns
- Case Study: Altiris Deployment Solution
- Defence
- Q&A



Environmental Concerns



When standard builds fail

- **Sysadmin** – “Automated Re-Imaging/PXE booting is going to save us so much time”
- **Hacker** – “I just stole your standard build and admin password muhahaha!”

Did someone say something about eggs?

- Deployment Server =
Holy Grail





Outline

- Introduction
- Threat Vectors
- Environment Concerns
- **Case Study: Altiris Deployment Solution**
- Defence
- Q&A



Altiris Deployment Solution



Overview

- Now owned by Symantec
- Rebadged by various different vendors
- Dell OpenManage
- HP Rapid Deployment
- Also partnered with Oracle, IBM, Cisco, Intel and VMWare



Basic Architecture

- Client/Server model
- Agent installed on every client
- Agents connect to server and receive commands
- SQL Server DB backend
- Server managed via thick client or web interface



Previous Vulnerabilities

- Plenty
- Client privilege escalation
- SQL Injection and Directory Traversal
- Server Impersonation due to lack of authentication

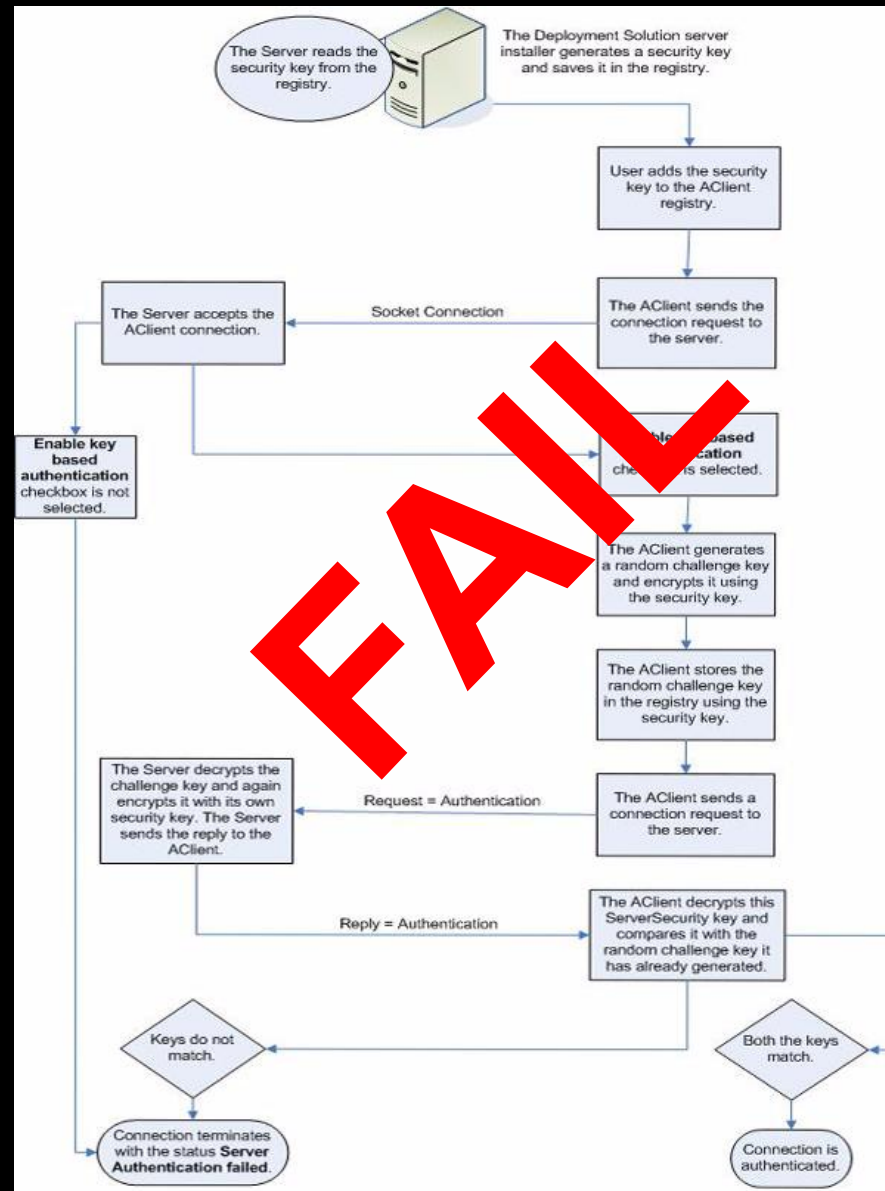


New Vulns: Server Impersonation

- Key-based server authentication was added
- I found this was simple to bypass
- Leads to two valid attack vectors
- Worse due to multicast

New Vulns: Server Impersonation

```
Stream Content
Request=SendFile
Filename="c:\mwrtest1234.exe"
Date=1207643970
Attributes=32
Size=115712
Port=6666
Schedule-ID=100000008
Task-Sequence-ID=0
Task-Type=CopyFile
Allow-Defer=5
CurrentFilecount=1
TotalFileCount=1
TotalFileCopySize=115712
ID=5000001
.Request=Authenticate
CipherText=GuzSLH_DAV`zy|sFDZLYYKYCxa[IQIU.PRVK~LAXSgMzoz.gMnys@HIKz`{S0dj{UlwzPyu_cg.Mux
[gsPj_M{]BGE|Kmlc\WMAXunZoJtQvTikoIDE_nwprnuaY{jkAlx_noHUA|s^f{]sPLE~dAu|`a.KOec{e`
{Q@b`vvt]hh{gPf\vn{g}nFwAIFtBzGGg_CEWYnetxkebrHEbxamZQ}hovI[IN~hopCJHjOBFDLji]}
BRfLxm_KSaPI@.YI~|xxpngd@x@toFq[csJrpsa^gv@w]lUw|PxiUuUFjPX|sAMo@\LF@Y_asj@frGCTA|
yAvMVz^zo_xUG\pLMqZrF@jxrUC|J\tqJixKAAqQ{RMTZiipp_fVQfzi{YQdw.max}|eAPZRxFZAlqCTEY`\
\MnJzxNT@}yTYRYlo^xJH}Fe\bg@ztQreuoCC@vVfPrJNSAR.KB_@eiI]C|]rBBatba~U@dHgILcpo^\uTcmAoLsJM|
[VrL}_vyvAFwGfha_qomLcmN~@xptA}mr~H|@r~vfNkOw_{}GnhPLXSdv.K{It|`KD__CPIEdmtBKACQxw]]
vvr_ako||Y]fn|ZoYKpogtT|NaqkmsRQf.H\]SUSOL|n|]qa@Fe]IO\gpjFvpwowUEYY
[NtwSSbzTgbPAZANP.g.wAOBp
.Reply=SendFile
Schedule-ID=100000008
Task-Sequence-ID=0
Result=Success
Status-Code=0
Status-Module=AClient
.Request=LiveEvent
Event=Execute
```



Attack #1 – Compromising Laptops Outside the Network

- Server Impersonation
- Redirect Traffic at Wi-Fi hotspots
- **DEMO**

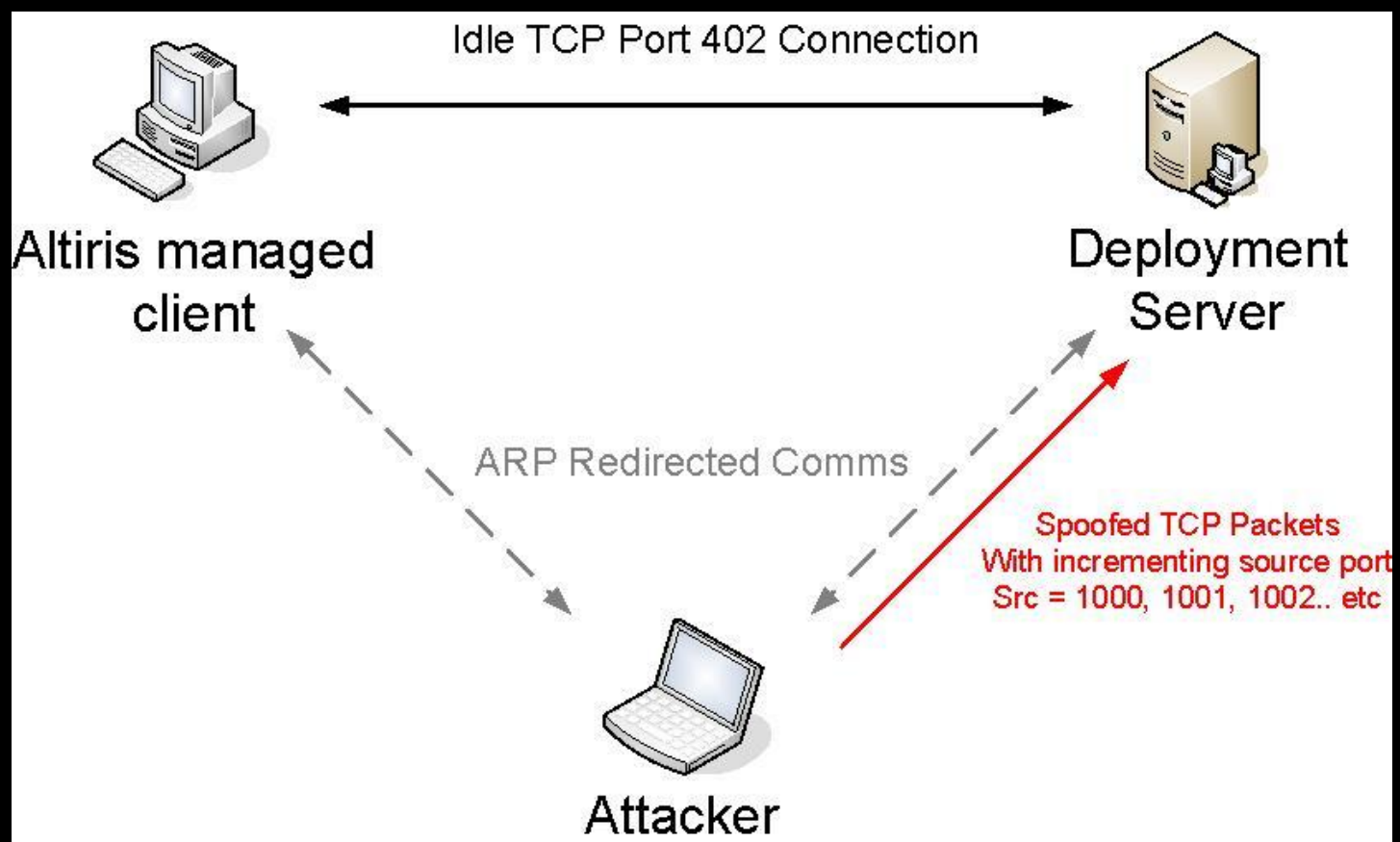


Attack #2 – Compromising <any> Inside the Network

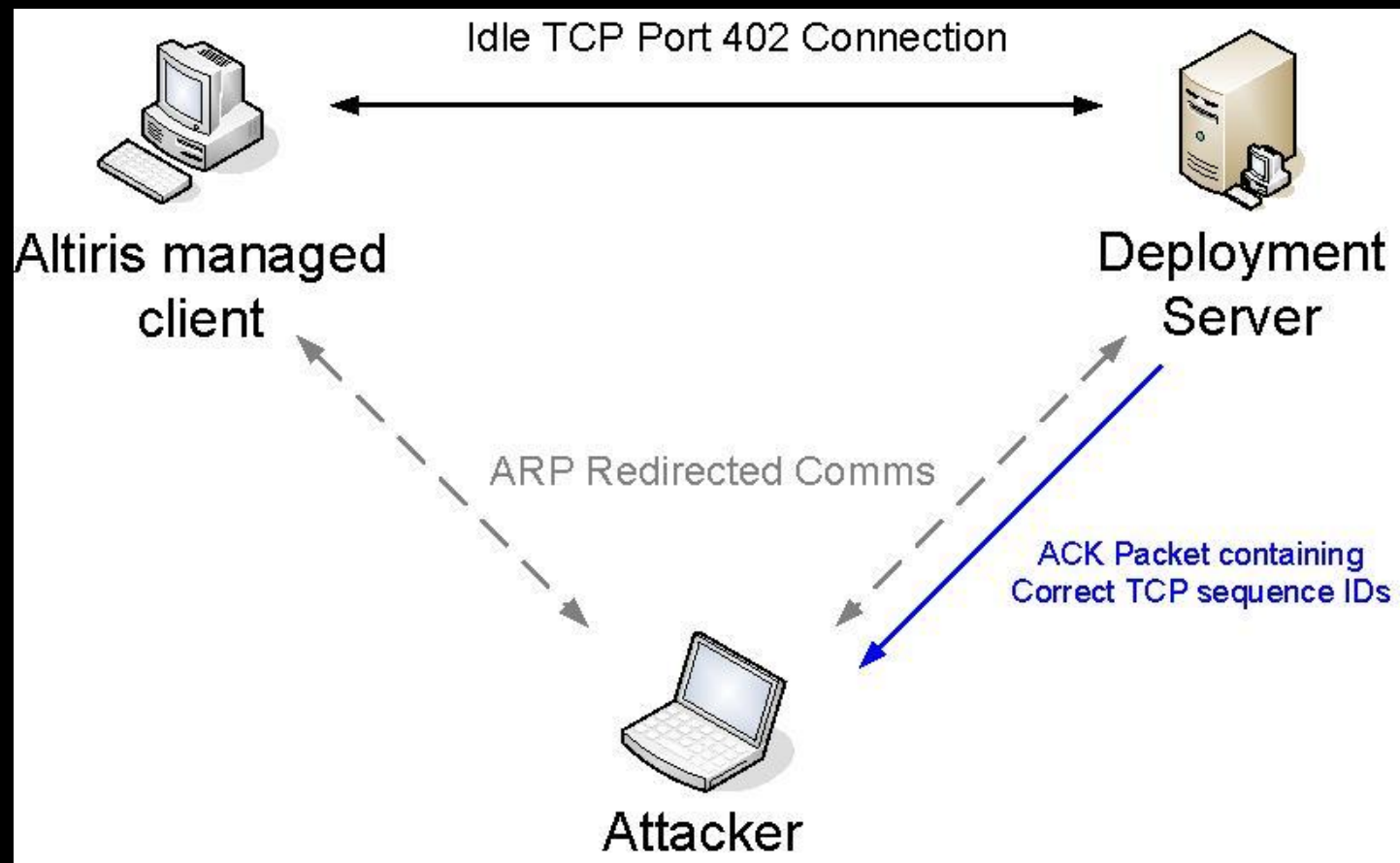
- Connection Hijacking
- Forced TCP Connection Termination
- DEMO



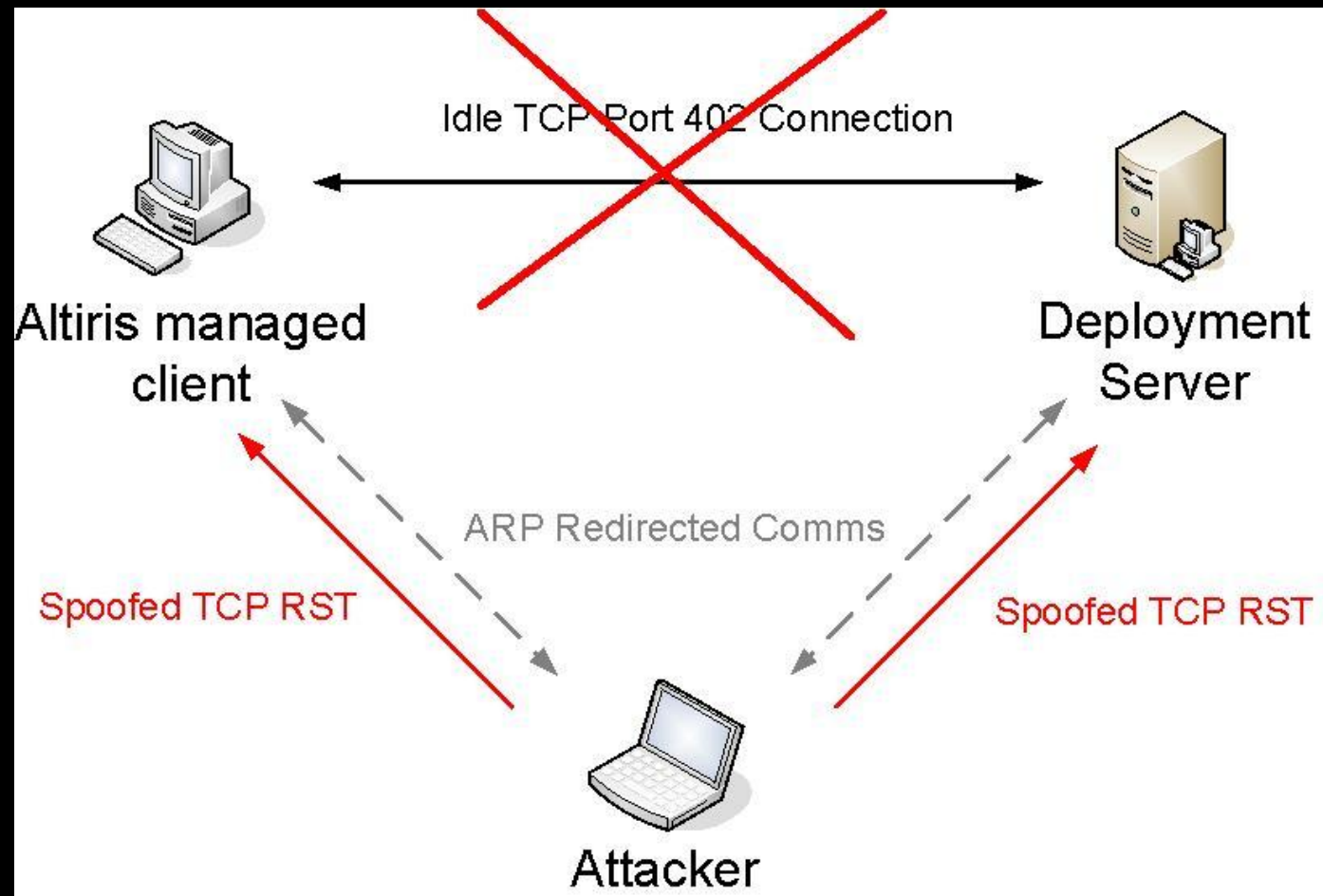
Killing an Idle TCP Connection (1)



Killing an Idle TCP Connection (2)



Killing an Idle TCP Connection (3)





New Vulns: DB Management Authentication Bypass

- “Middle Man”
- Listens externally by default
- Similar coding error to before



New Vulns: DB Management Authentication Bypass

- A bit of IDA Pro use reveals...
- ScheduleEvent, AddUser, SetPrivilege, UpdatePXEBootOptions etc...

Attack #3: Full Server Compromise

- Turns out further vulns in DB Management are more useful...
- **DEMO**

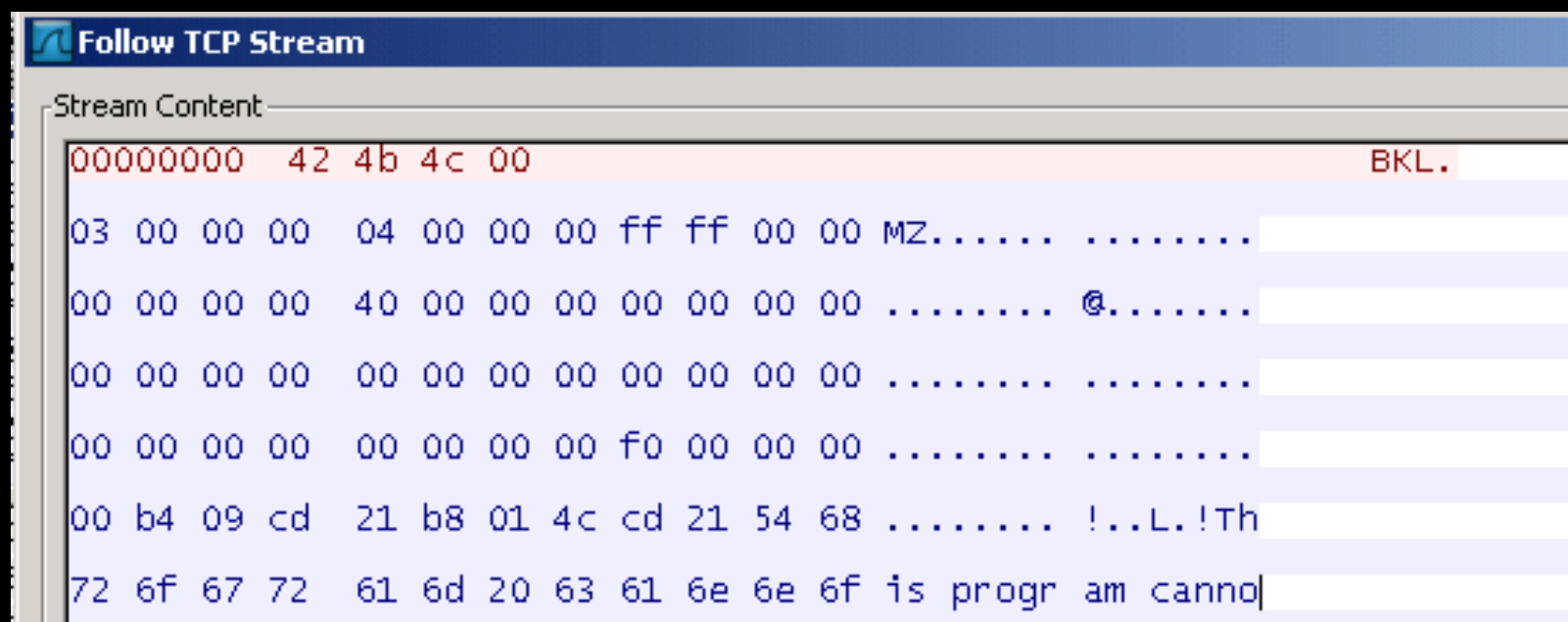




New Vulns: Unauthorised File Disclosure/DoS

- Dynamic Port used for file transfer
- No session control
- Encryption prevents file disclosure
- DoS still prevents patching etc...

New Vulns: Unauthorised File Disclosure/DoS



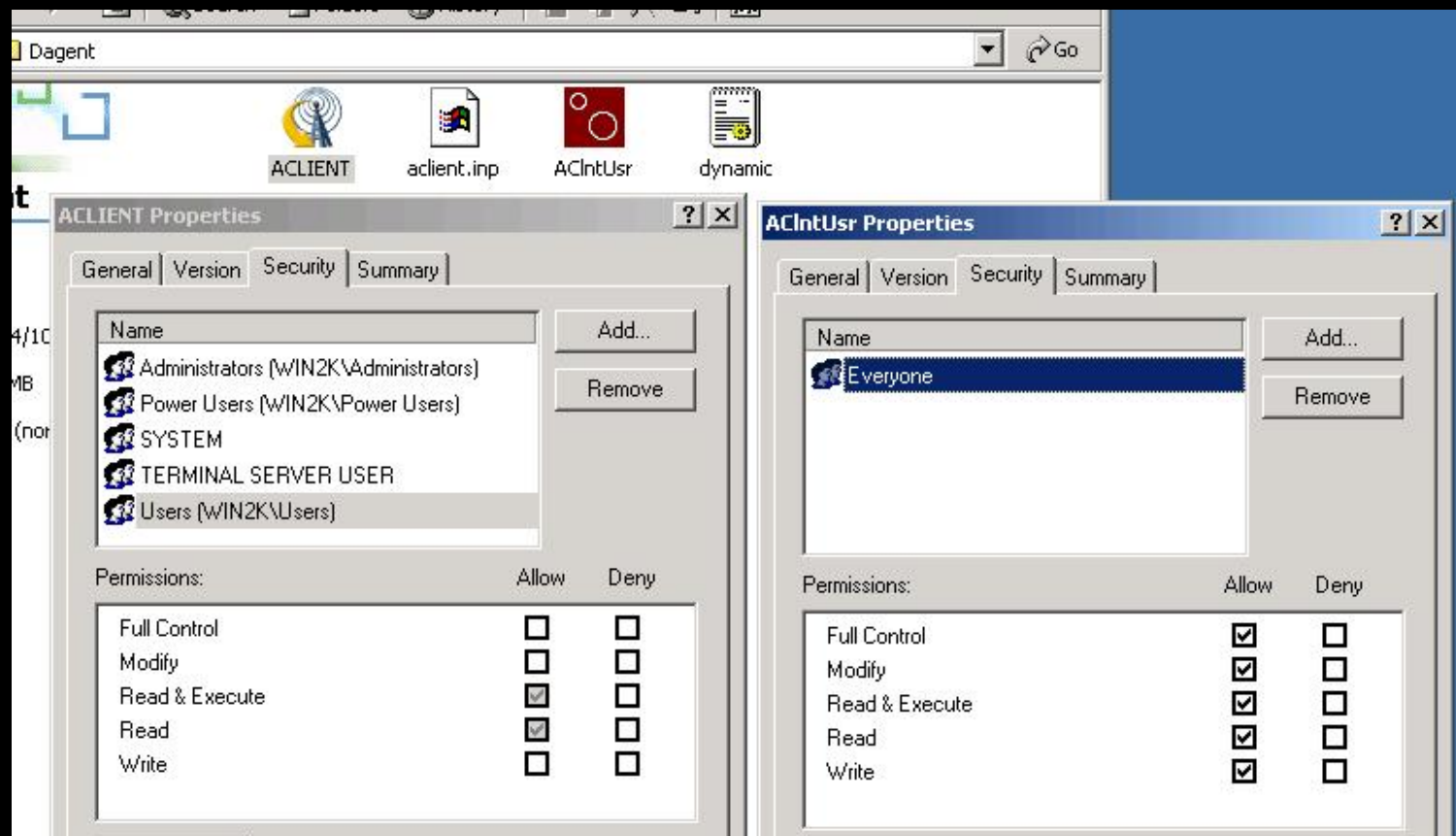
```
Follow TCP Stream
Stream Content:
00000000  42 4b 4c 00                                     BKL.
03 00 00 00  04 00 00 00 ff ff 00 00 MZ.....
00 00 00 00  40 00 00 00 00 00 00 00 ..... @.....
00 00 00 00  00 00 00 00 00 00 00 00 .....
00 00 00 00  00 00 00 00 f0 00 00 00 .....
00 b4 09 cd  21 b8 01 4c cd 21 54 68 ..... !..L.!Th
72 6f 67 72  61 6d 20 63 61 6e 6e 6f is progr am canno|
```



New Vulns: Client Privilege Escalation

- ACLIENT.EXE = SYSTEM service
- ACIntUsr.exe = GUI control client
- “Everyone:Full Control”
- Can you say Trojan?

New Vulns: Client Privilege Escalation





What I (and others) are not telling you

- There are significant issues I have discovered that are not yet public
- There are 0-day exploits available for sale (VulnDisco)
- My personal opinion is there are more to find



Further Work

- Architectural investigation of PXE and automation environment
- LOTS of implementation level work to be done
- Numerous network services not yet touched



Further Work – Network Services

Component	Service	Port	Protocol	Where is this port connected?	Is this port configurable?
PXE MTFTP	Altiris PXE MTFTP Server	69	UDP	PXE Client	No (Industry standard port)
	Altiris PXE MTFTP Server	1758	UDP	PXE Client	Yes
		1759	(Multicast)		
PXE Server	Altiris PXE Server	67	UDP	PXE Client	No
	Altiris PXE Server	68	UDP	PXE Client	No
	Altiris PXE Server	4011	UDP	PXE Client	No
PXE Manager	Altiris PXE Manager	405	TCP	PXEConfig	Yes
	Altiris PXE Manager	406	TCP	PXECfg Service	Yes
PXECfg Service	Altiris PXE Config Helper	407	TCP	PXE Server and PXE MTFTP	Yes
Deployment Web Console (Web Console)	Altiris Deployment Server Console Manager	8081	HTTP	DSWeb	Yes
	Altiris Deployment Server Data Manager	8080	HTTP	DSWeb, Console Manager	Yes
DB Management (Middle Man)	Altiris Deployment Server DB Management	505	TCP	Win32 console, Axengine, PXEManager	Yes

Page 1 of 2!

14 ports on server alone!



Outline

- Introduction
- Threat Vectors
- Environment Concerns
- Case Study: Altiris Deployment Solution
- Defence
- Q&A



Defence



General Deployment Solution Advice

- Consider the impact on your environment
- Pay attention to configuration and privilege assignment
- Consider independent testing
- Analyse security trade off
- **PROTECT THE DEPLOYMENT SERVER**

Altiris Specific Defence

- Patch!
- Patch!
- Patch!





Communications Security

- Use a well tested encrypted tunnel for client/server comms
- IPSec through group policy
- Stunnel (probably difficult)



Defence in Depth

- Lots of services exposed by default
- Firewall, firewall, firewall!
- Dynamic file port makes deny all tricky...
- At the very least block TCP 505, 8080 and 8081



Configuration

- Altiris opens a file share by default
- Pay attention to the permissions you set on it
- Insecure write permissions = trojaned deployment server and/or clients!



Conclusion

- Deployment solutions can heavily impact security
- Altiris in particular has very significant vulnerabilities
- If you haven't considered the issues outlined today, your entire network is at risk
- Get thinking!



Questions?

