



How to attack and disrupt enterprise networks



Łukasz Bromirski
lbromirski@cisco.com



Confidence 5.1, Warsaw, XI.2009

Disclaimer

Attacking or even doing any kind of reconnaissance in corporate network may be against your company security policy, terms of use policy or any other „regulations“. It usually is. So simply - don't do that.

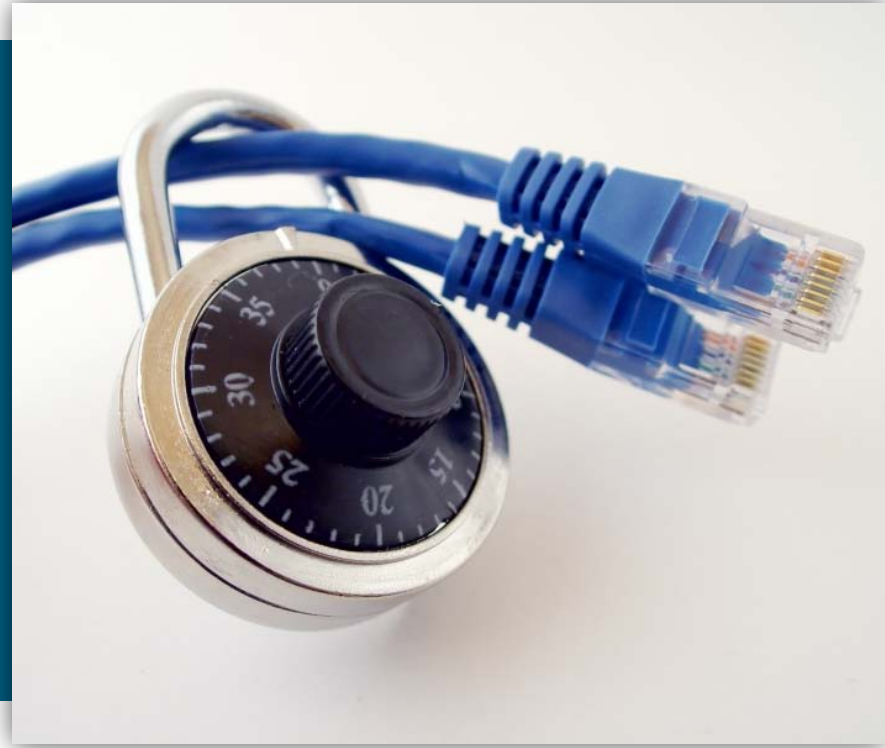
I'm not encouraging you to use the information in any way against live installations. Tests should be performed in controlled environment, in labs etc.

YMMV. You may not be able to do what I describe, you may get different results, you may destroy the world as we know it.

The flight plan for today

- Network security – „we all know the drill”
- If you don't have a plan, you plan to fail
- Attacking the network – steps to success

Network security – „we all know the drill”



Five stages of...

...typical networking team engagement in... somewhere...

- **Denial** – ‘this can’t be happening to me and it is not happening to me! no! nooooooo!’
- **Anger** – ‘this switch is broken! this firewall is lousy! this VPN AAA system was designed by idiots!’
- **Bargaining** – ‘could we just by chance have someone to look at the configs we have to discuss with us a way to optimize our network?’
- **Depression** – ‘nobody f* cares if my life and my network is broken, nobody f* cares! I’m not going to build any network in my life! Do you hear me - life? Die!’
- **Acceptance** – ‘OK, we’ve learned something, now let’s switch vendors’

Two sides of story



Security by duct tape

Because failure is always an option.



Łukasz Bromirski | Channel Systems Engineer
lbromirski@cisco.com



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

- „All the problems listed seem to be to **obvious to miss in real networks**” – life is not a criminal movie with a plot taken from blockbusters – a lot of things may happen and they don’t always follow the model of being very spectacular or visible or interesting
- „I wouldn’t want to **configure my network in a way that would permit such attacks to happen**” – propably nobody would
- „You want us to **buy more of your gear**” – I’m not selling anything, I’m discussing the way we should approach security – in a more friendly, open manner
- „**Turbodymoman will always be better than you anyway**” – Yes he will be ☺



Two sides of story



Security by duct tape

Because failure is always an option.



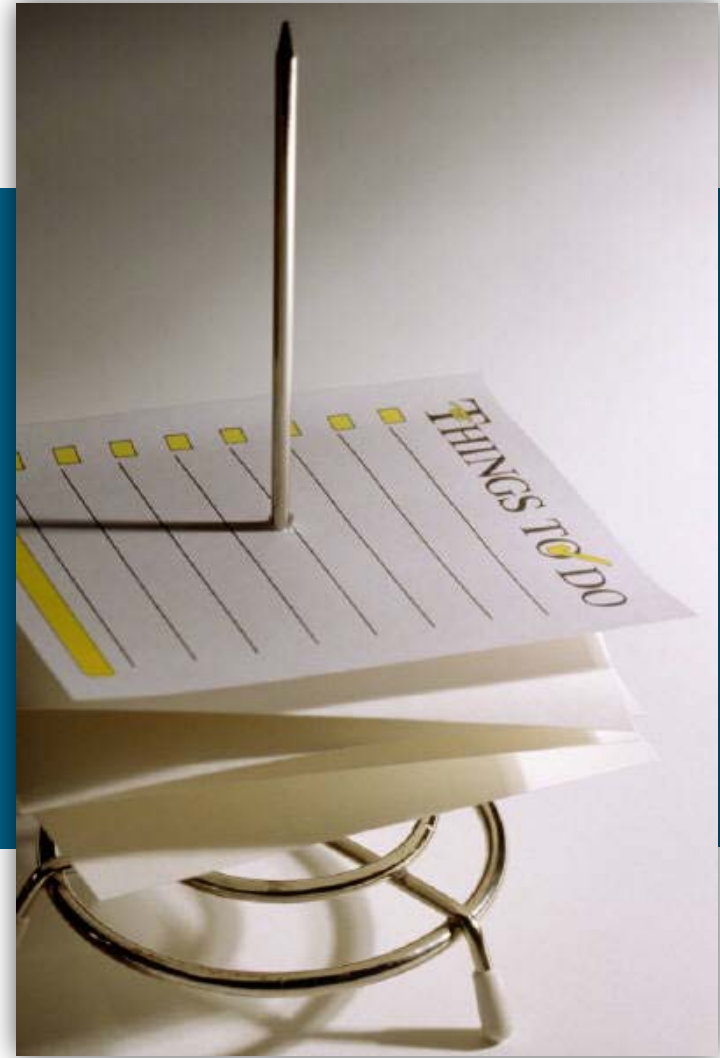
Łukasz Bromirski | Channel Systems Engineer
lbromirski@cisco.com



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

- „This taught me a lot – I hired two guys and they made over 400 changes in our network during a month to secure it” – a CTO of a small company

Plan to fail



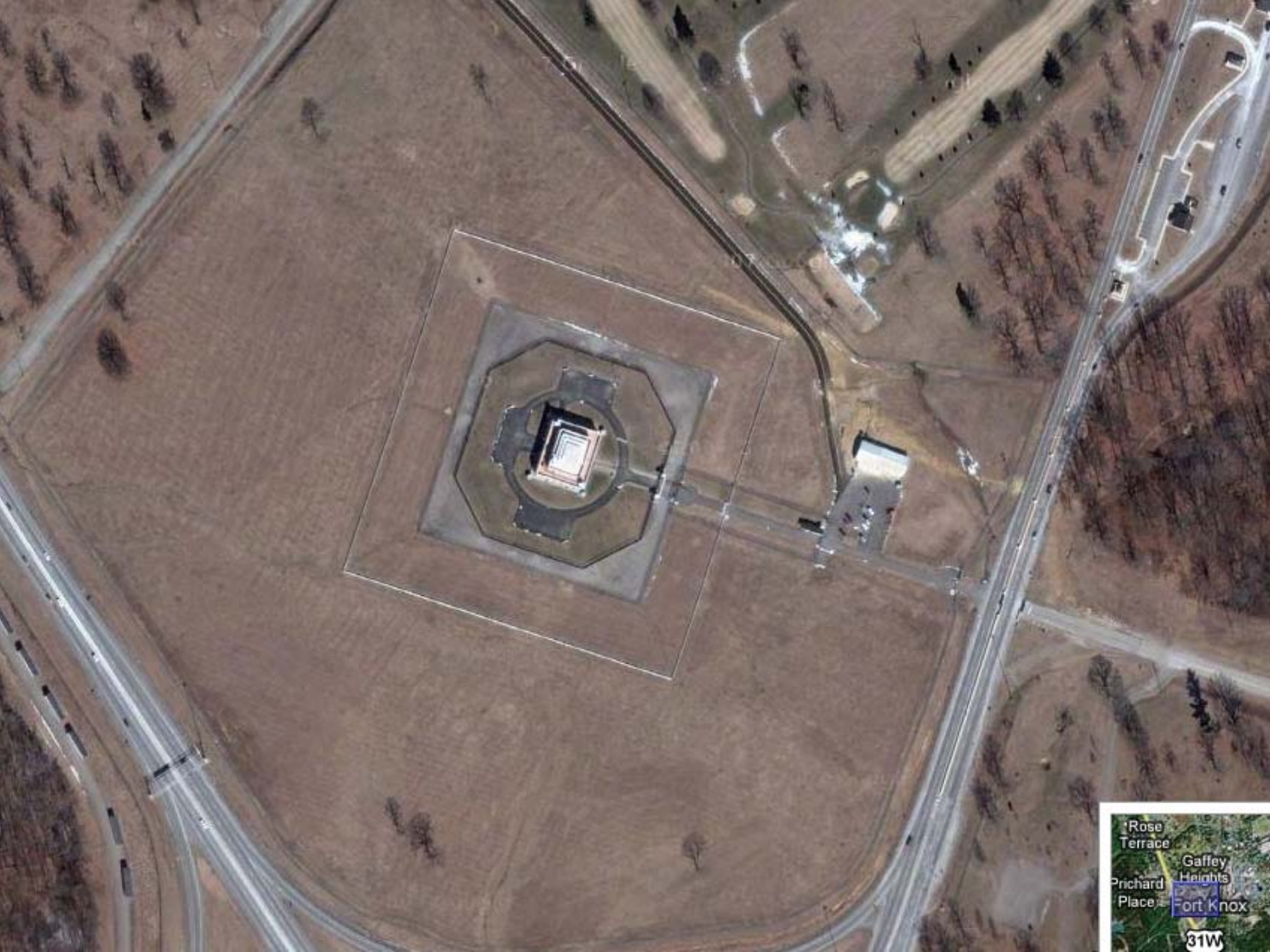
How we build our networks?

- Our own IT team, staffed with specialized networking gurus, that can handle everything, at any speed and with any troubles that may happen without even <1%
- A group of people „doing networking and stuff, including but not limited to phones, browsers, drivers installation, fax troubleshooting.... we can even deliver pizza! 😊” as a part of their normal duties ~30%
- A group of people letting the specialized companies (aka „integrators”) do the dirty work and present them shiny document with everything specified, documented and working (at least on the surface) ~69%

Best practices, anyone?

- Build a layered defense
- Every layer should slow the attacker down, drain his strength, power, will to fight, eventually stop him and possibly – destroy, redirect him to other target
- The layering of the defense is widely supported by:
 - common sense
 - a set of „industry” standards, public documents, white papers
 - vendors, willing to sell, sell, sell and if in doubt – sell again 😊

<http://www.google.com/search?q=network+security+layered+defense>





The Cisco SAFE Security Reference Architecture

The Foundation for Secure E-Business

Cisco's SAFE is a security reference architecture that provides detailed design and implementation guidelines to assist organizations looking to build highly secure and reliable networks. SAFE's modular design takes advantage of cross-platform network integration and collaboration between Cisco security and network devices to better address the unique security and business needs of different places within the network, and interoperability between network segments, including campus, data center, branches, partners, and remote workers. The result is a greater visibility into devices and network security events, and enhanced control of users, devices, and traffic for coordinated threat response. SAFE's comprehensive security strategy improves an organization's ability to identify, prevent, and respond to threats, and securely deploy critical business applications and services.

High-Level View

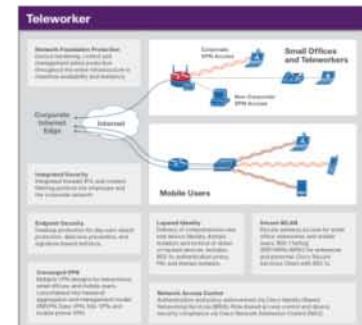
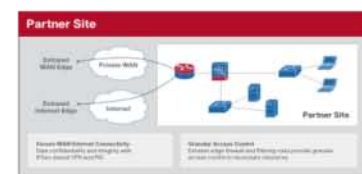
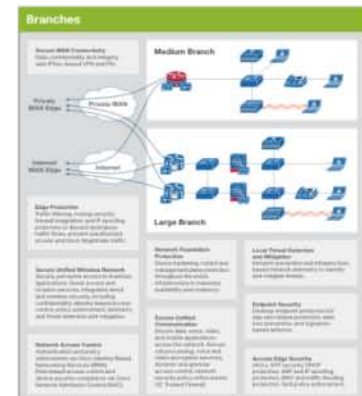
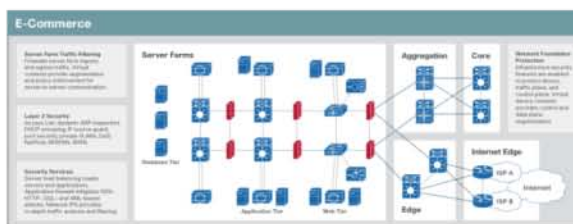
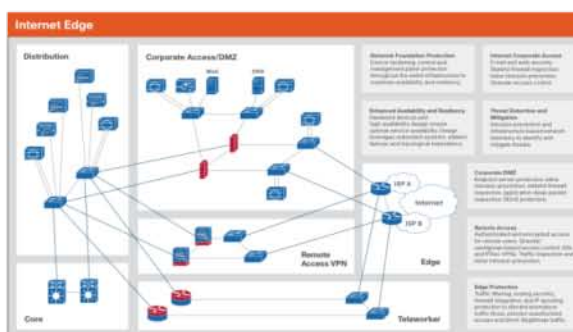
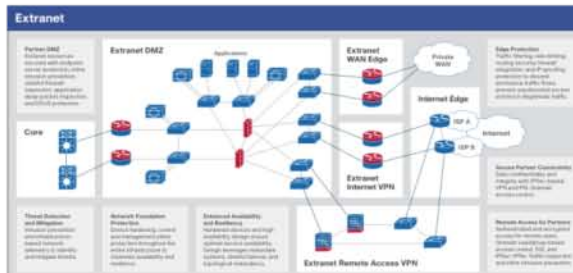
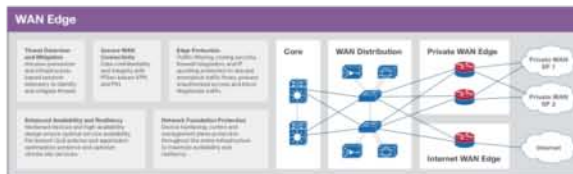
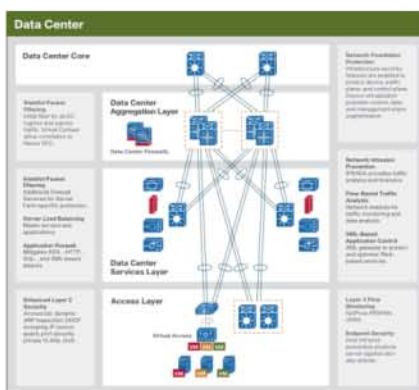
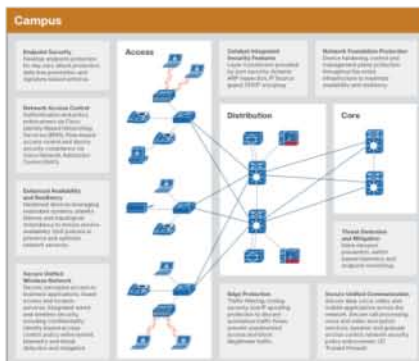
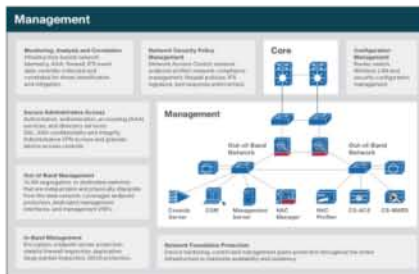


Icon Key



For More Information

cisco.com/go/safe cisco.com/go/security



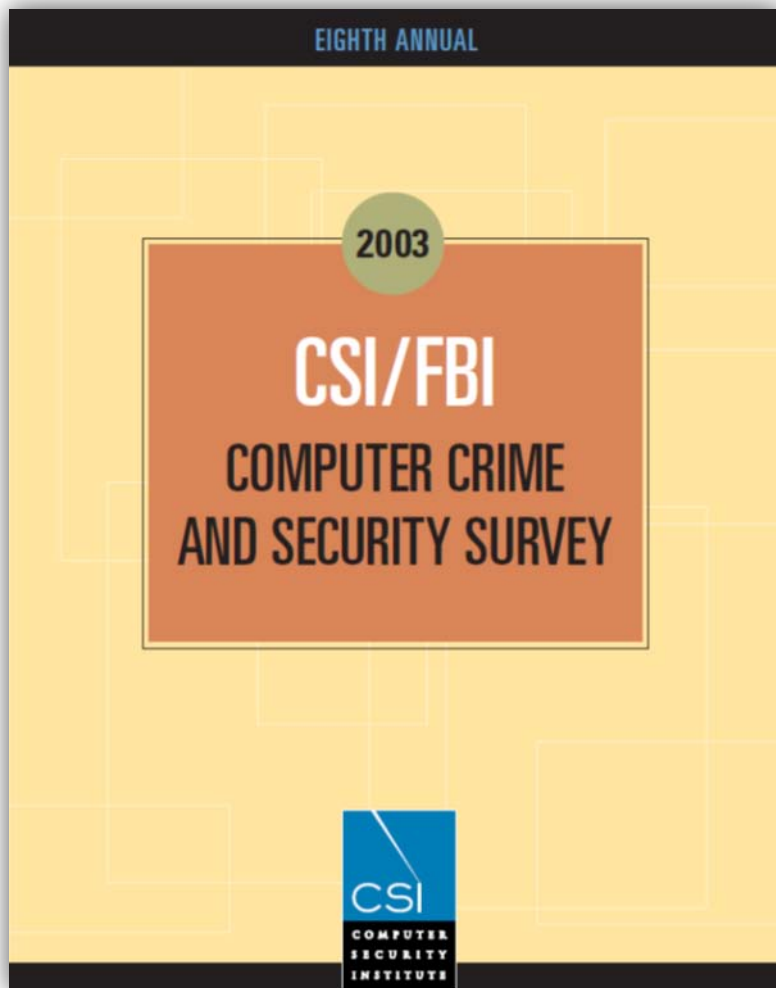
Who needs best practices, anyway?



- „The modern network looks like a Moebius strip
- Interactions with the outside happen at the desktop, the server, the laptop, the disks, the applications, and somewhere out there in the CLOUD
- So, where **is the depth?**
- **There is none. A modern network throws all its fight out at once.”**

http://www.isecom.org/events/The_Mobius_Defense.pdf
http://toxygen.x86.sk/pdf/The_Mobius_Defense.pdf

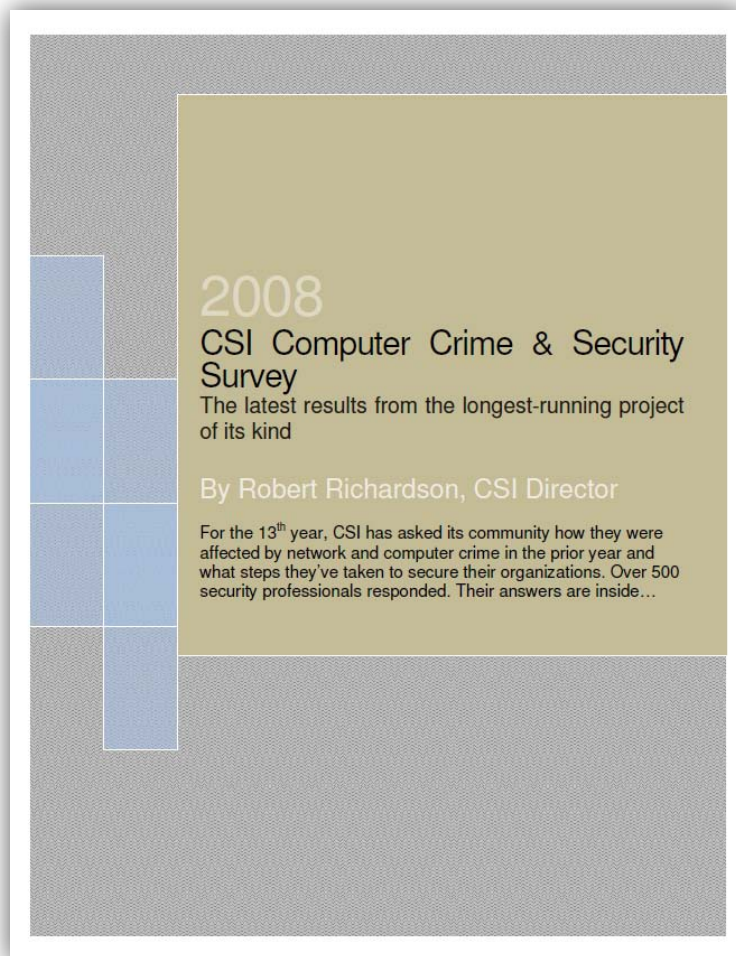
It's popular, and so often misquoted



- Out of 490 respondents, **220 the insider attack or stole the information**, 103 had a laptop or other important mobile devices stolen
- That's hardly a „over 80%” or „almost 95%”

http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

It's popular, and so often misquoted #2



- Out of 522 respondents, **230 had the insider attack or stole the information**, 222 had a laptop or other important mobile devices stolen
- In 52 cases, DNS was attacked
- In 141 cases, the networks were penetrated by targeted attack – specially crafted trojan, virus or other form of attack
- That's, again, hardly a „over 80%” or „almost 95%”

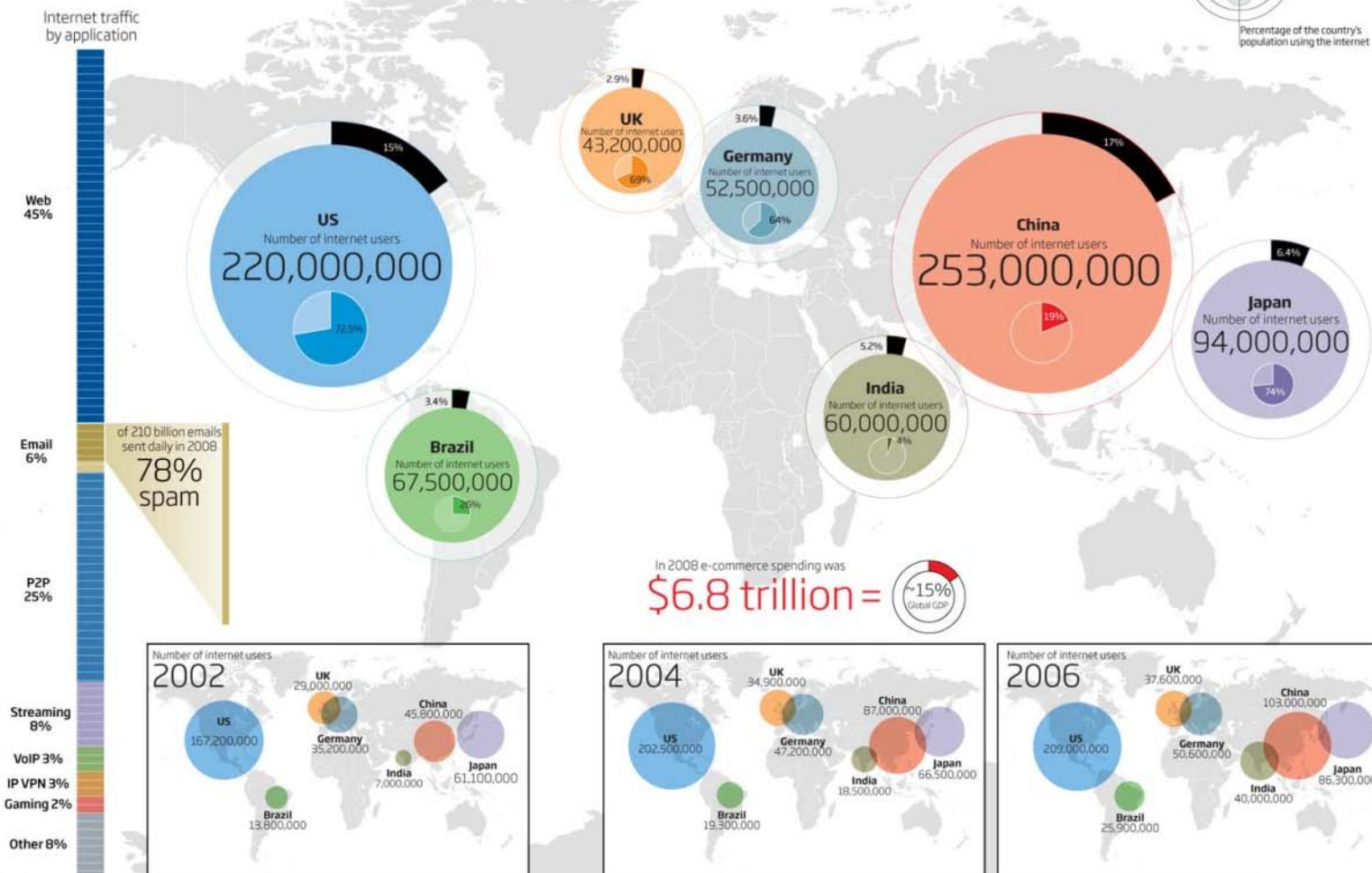
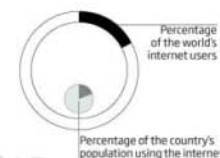
<http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>

Anyone can be an attacker...

The exploding internet 2008

Internet traffic is growing by about 50 per cent annually, with video and music streaming rising fastest. At the same time, the web is becoming divided along language lines

By 2012, Asian web surfers, including about 490 million Chinese, will outnumber North Americans by 3 to 1 and Indians will become the third-largest group online. Tomorrow's web will probably be dominated by a mixture of the English, Mandarin, Hindi, Portuguese and Russian languages



P2P = Peer-to-peer file sharing, Streaming = Video and music downloads
VoIP = Voice over Internet Protocol, IP VPN = Internet Protocol virtual private network

Common sense in security...

- When all you do for last 5-10 years with new system is to just bring up the favorite firewall suite and that's all...
- And the whole world around you is screaming that the IT technologies rush forward with the speed close to the speed of light...
- „Insanity - doing the same thing over and over again and expecting different results.” – Albert Einstein

Attacking the network – „steps to success”



Ways to do it

- **Random** – scan, attack random services and try to obtain meaningful response/data – very often ends with success
- **A sort of ‘unpaid audit’** – „we will just do a checklist based on our best practices model”
- **Interesting** – „work out” the target network along with services, try to plant a bug/trojan horse, install back door or „just have an entry”
- **Focused** – Own the n3t – sometimes for years, without anyone noticing the fact data is leaking

Attack vectors

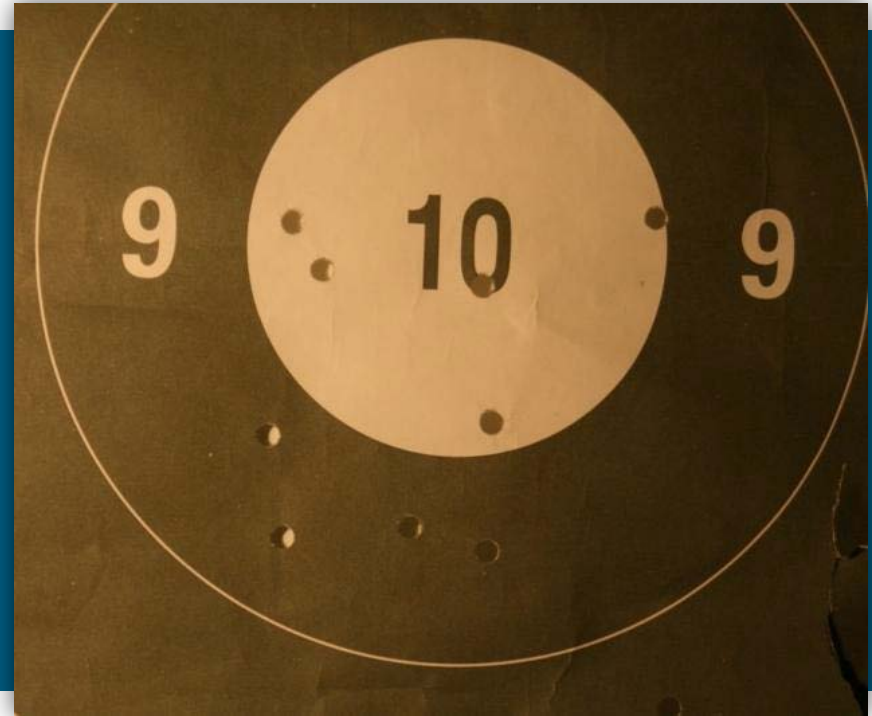
- How much **time** you have? How much **exposure** you're willing to have?
- Go after the people – their knowledge or their laptop*, cell phone, etc.
- Go after the remote access
- Go after the AAA part
- Try to be physically connected (WLAN/Ethernet) and map the network
- Remotely disrupt their work – DNS, DoS BGP sessions or hijack their prefixes, deface their web or make it infect people PCs, spam from their domain

* <http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html>

I'll focus on...

- ...security from the **network point of view**
- Trillions of attacks exist that work from the application layer – MitM attacks on browsers, DNS caches, applications, exploits and trojan horses working as an e-mail and web site attachments or simply faked torrent files, including broadly pirated software – like Windows 7 („with addons”) or Adobe software („with addons”), the magic WMV files („[XXX] She did it for real! Awesome!”) or PDF files („The EBook of everything – 5MB!”)
- The DEFCON, HITB, CCC, BlackHat, HAR and other sites host a tons of material for anyone curious enough to read or watch & listen

Own the core infrastructure



You can attack a lot of things

- „Control plane” of the network

Signalling protocols used by L2: Spanning Tree (and variations of it), port aggregation (LACP and PAgP), automation protocols (CDP, LLDP and DTP), management protocols (VTP, RADIUS, TACACS+), security features (802.1x)

Redundancy and management protocols used by L3: HSRP/VRRP/GLBP, DHCP, routing protocols, both IGP and BGP, multicast control plane (PIM) or new attack vector – IPv6

- „Data plane” of the network

injecting or gaining access to networks you should not be permitted to access: VLAN hopping, MVR/multicast registration

A lot of was told already about it

...and I won't repeat this again and again – it's important, learn it!

- Download and use:

Backtrack: <http://www.remote-exploit.org/backtrack.html>

Pentoo: <http://www.pentoo.ch/>

- Tools to use:

yersinia: <http://www.yersinia.net/>

nmap: <http://www.nmap.org>

hping: <http://www.hping.org/>

kismet: <http://www.kismetwireless.net/>

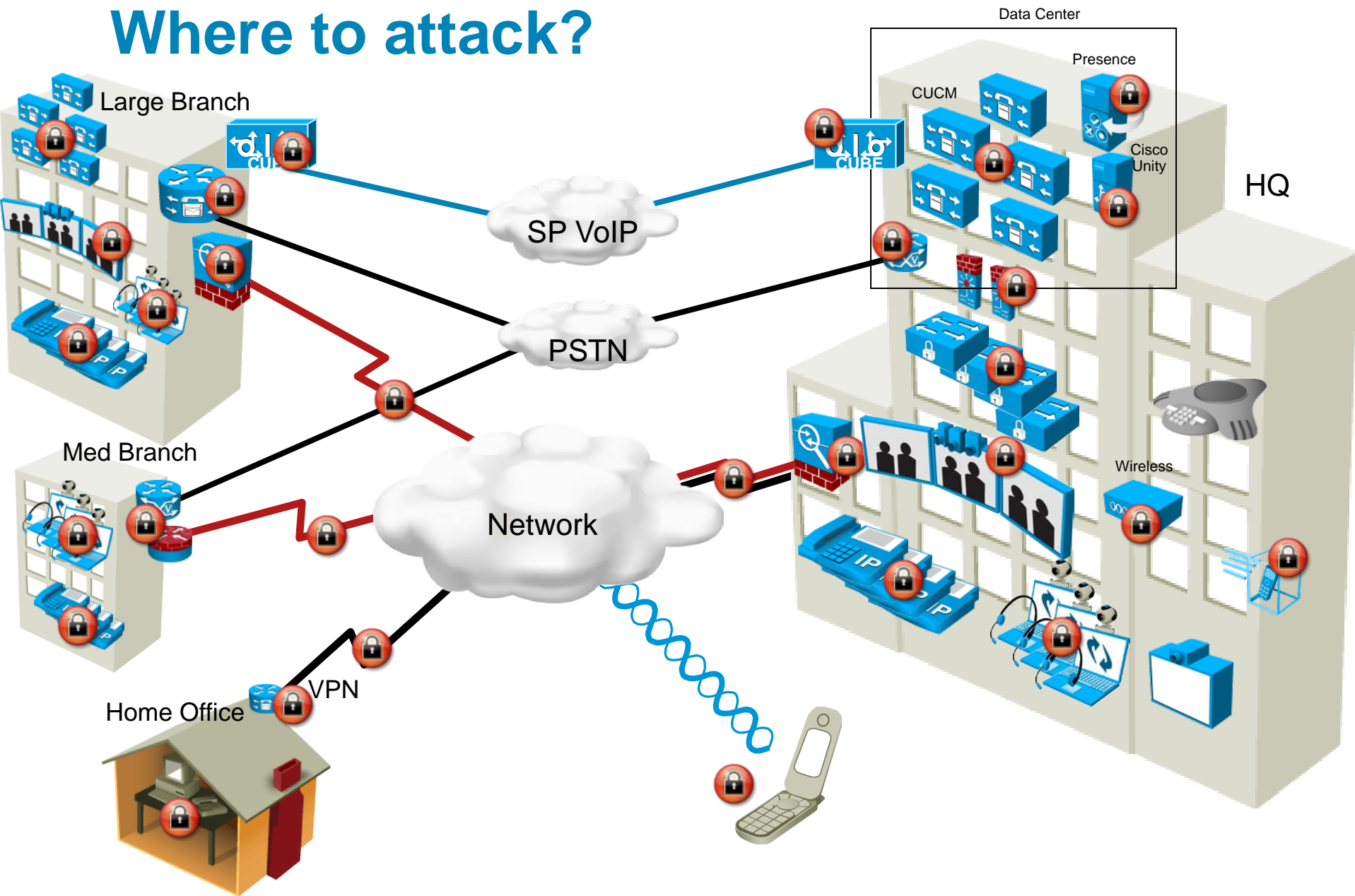
- Use google to look for references, examples, howtos

<http://lukasz.bromirski.net/docs/prezos/>

Own the IP telephony network



Where to attack?



Attack Prevention

Cisco CallManager security complexity in eyes of Cisco Engineers

	Phones	Switches	Routers	Network/ Firewall	CUCM	Servers
Eavesdropping	E - C	E - I	E - I	NA	E - C	NA
Denial of Service	E	E - I	E - I	I - E	E	E
Impersonation	E	C	NA	C	E	NA
UC Applications Security	NA	NA	NA	NA	E/I	E
Soft Client	NA	NA	NA	E/I	E	NA
Toll Fraud	NA	NA	E	NA	E	NA

E = Easy; I = Intermediate; C = Complex

Eavesdropping Protection – phone setting

- Turning on the Settings Access to the phone
- Keeps a phone from displaying useful information to non-IT person
- Call Managers IP, VLAN ID, etc.
- Usually enabled by default

Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="password"/>

Product Specific Configuration ?	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Eavesdropping Protection – Voice VLAN


- Phones have the ability to prevent Voice VLAN access
- Will prevent someone plugged into the phone getting access
- Usually enabled by default

Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="password"/>

Product Specific Configuration	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Eavesdropping Protection - MitM

- Phones have the capability to protect their data streams from Man in the Middle Attacks
- Only protects data from the phone
- Usually enabled by default
- If devices are not Layer 2 adjacent it is much harder to run a MITM attack

Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="password"/>
Product Specific Configuration 	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

Eavesdropping Protection – phone access

- Control web access to phones with ACLs

Default gateway

DHCP server

DNS server

TFTP server


CUCM(s)

Directory server

etc.

- Disable the phone's web server

Disabling web access
also breaks XML
pushing apps

		Network Configuration	
		Cisco Systems, Inc. IP Phone CP-7960 (SEP003094C25E70)	
<u>Device Information</u>		DHCP Server	10.27.15.1
<u>Network Configuration</u>		BOOTP Server	No
<u>Network Statistics</u>		MAC Address	003094C25E70
<u>Ethernet</u>		Host Name	SEP003094C25E70
<u>Port 1 (Network)</u>		Domain Name	
<u>Port 2 (Access)</u>		IP Address	10.27.15.27
<u>Port 3 (Phone)</u>		Subnet Mask	255.255.255.0
<u>Device Logs</u>		TFTP Server 1	10.27.11.12
<u>Debug Display</u>		Default Router	10.27.15.1
<u>Stack Statistics</u>		1	

Eavesdropping Protection – phones load

- Signed images

Software images signed at the factory to make sure someone can not install a rogue image on a phone

- Signed config files

Config files signed locally by the CUCM and then checked when downloaded to the phone to verify the config file

- TFTP is used as the transport of the signed files

Eavesdropping Protection - crypto

- Signed images & signed config files
- Does prevent them from playing back the conversation

The system uses new keys for every conversation

X.509v3 digital certificates

TLS

RSA signatures

HMAC-SHA1 authentication

AES-128 CBC encryption

SRTP

HMAC-SHA1 and AES-128 CM

- Does not prevent someone from being able to capture the streams

MITM attacks still work, unable to replay the voice because of the encryption

It's more than just a IP terminal in hand...

Overview of the Unified CM SIP Trunk
Technology Basics — Security

SIP Trunk Security Profile Information

Name* Secure SIP Trunk

Description With TLS and SRTP

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

☐ Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name

Incoming Port* 5062

☐ Enable Application Level Authorization

☐ Accept Presence Subscription

☐ Accept Out-of-Dialog REFER

☐ Accept Unsolicited Notification

☐ Accept Replaces Header

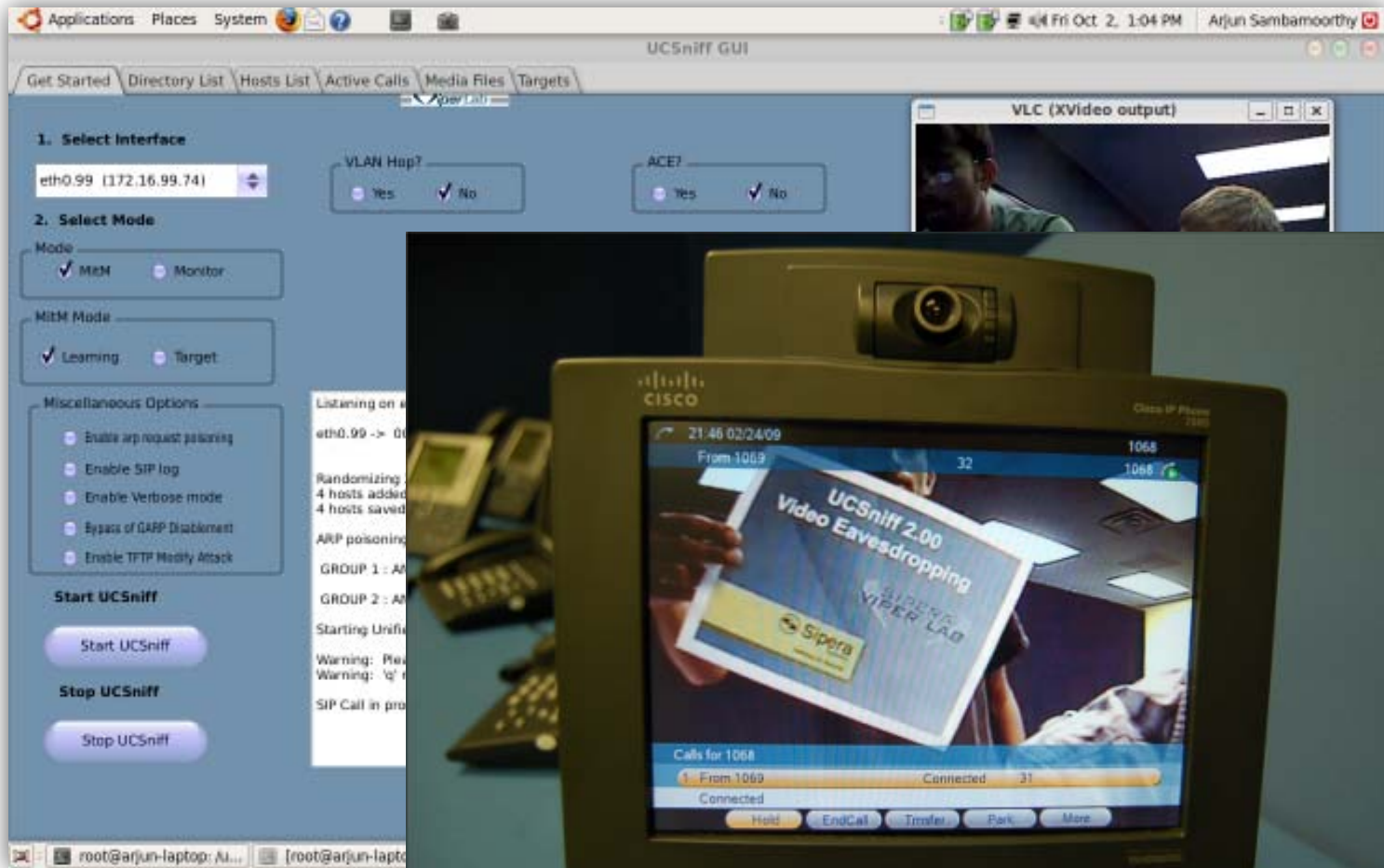
- Done through **SIP Security Profile** associated with trunk
- **Device Security Mode** set to Encrypted for AES-128 crypto string
- **Transport Type** set to TLS for signaling security
- **Digest Authentication** for SIP message level challenge
- **X.509 Subject Name** set to correspond to peer name
- Media Encryption (**SRTP**) done if transport type is TLS and both sides offer compatible capabilities

- We all* connect via H.323 and SIP to external IP voice providers
- Is the softswitch platform secure? Was it audited? Ever? Or just installed and left „because it works”?
- Is the authentication secure? No known MitM attacks?
- Is the signalization secure? There's AES y'know?
- Is the media secure? SRTP is a standard for that, do you use it?

* If you're not doing it directly, probably your provider is doing it for you, for your own good of course

<http://www.google.com/search?q=voip+sniffing+tool>

Sniffing both audio and video...



<http://ucsniff.sourceforge.net/ss.html>

Own the remote access network



Virtual Private Network (VPN) Overview

IP security (IPsec) and SSL

- Mechanism for secure communication over IP

 - Authenticity (unforged/trusted party)

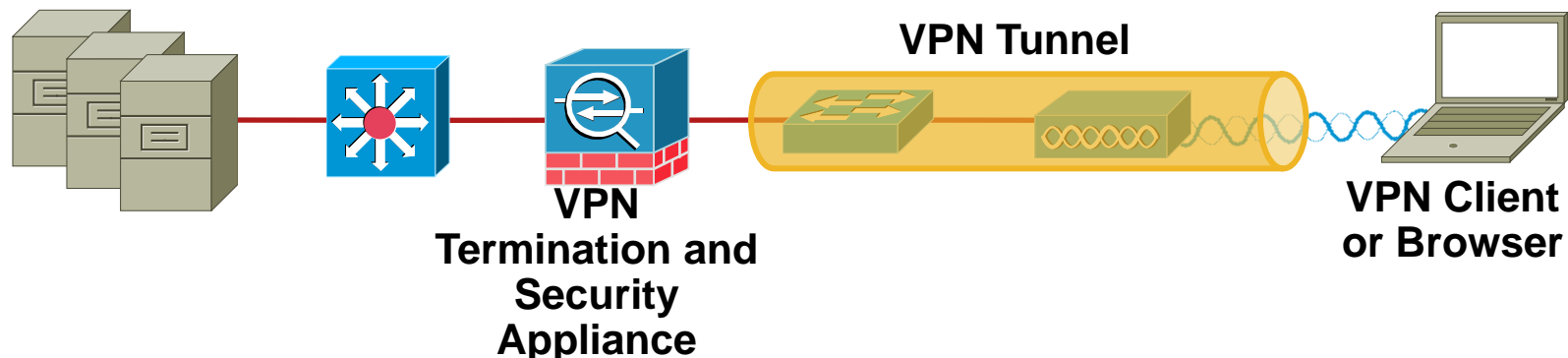
 - Integrity (unaltered/tampered)

 - Confidentiality (unread)

- Remote Access (RA) VPN components

 - Client (mobile or fixed)

 - Termination device (high number of endpoints)



Remote Access VPNs

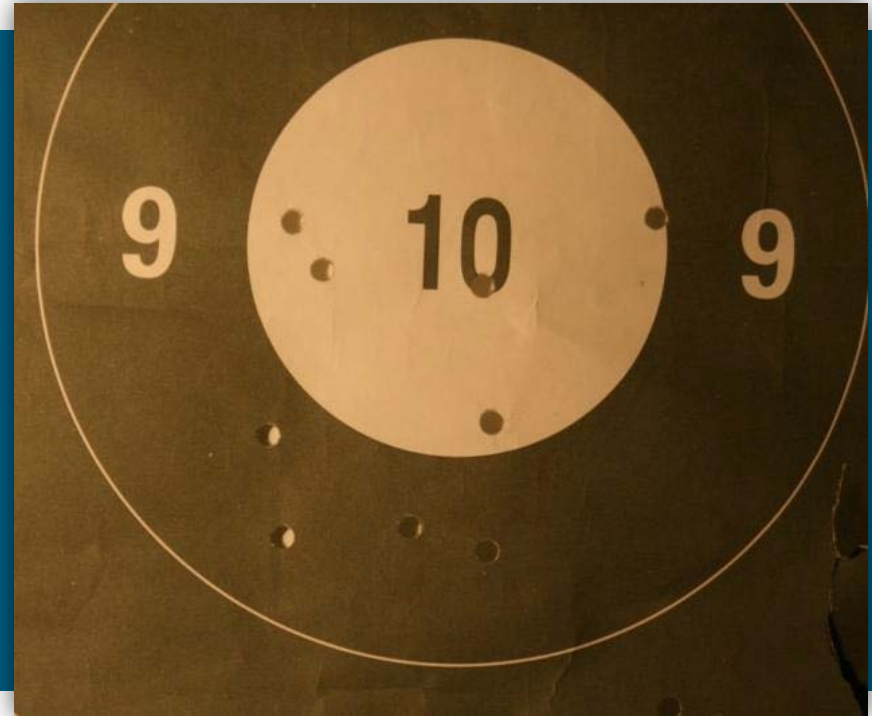
- Do you use OTPs? Or just a static password?
- Maybe because you're authenticating based on the Active Directory, you're using a username and password that is stored there?
- Guessing a valid username/password is easier than finding a VPN concentrator

guest/guest, test/test, test/test123, jank/jank, dupa/dupa.8, snmp/snmp.... the list just goes and goes

how many of you did check if the VPN device supports locking down after X unsuccessful authentications?

if you know the config names for popular VPN software, it's wonderful what Google can do for you!

Own the 'cloud'



From silos to clouds – a long journey

Today: 'Accidental Architecture'

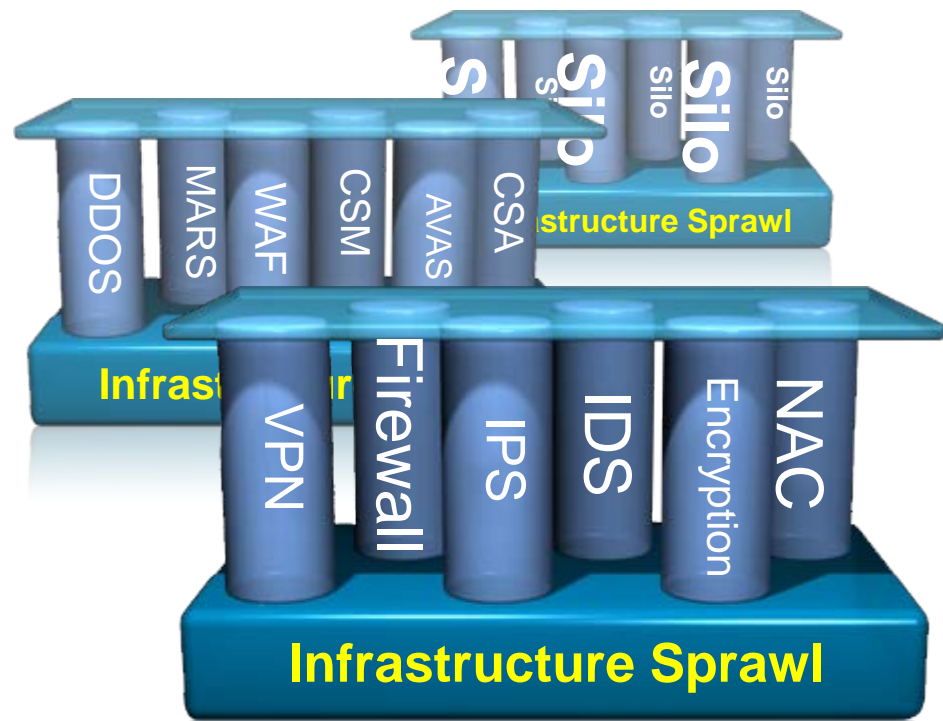
- Silo'd IT resources
- Complex, heterogeneous infrastructure
 - Fragmented security
- Branch offices —'mini data centers'

Benefits to Business

- Cost containment
- Service velocity
- Diversified portfolio
- Adjacent markets

Network Enabled Cloud

- Building on existing investments a "Cloud" with Video, UC and other services
- Leverages Cisco core strength in infrastructure consolidation
- Differentiation – network is the platform yet visibility to application level



Cloud by...

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.

Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

[Sign Up For Amazon EC2](#)

1.5 million success stories and counting



[See all of our success stories](#)

And the 'cloud' always comes down to...



The
one

The

rate to
er and

o get

Own the WAN



My WAN connections are secure!

- My FR/ATM PVCs are secure!

Network of my SP is übersecure and they have übergeeks working überalles!

- SP network is as secure as the people working there, and secure only up to the moment when somebody will have an opportunity to listen to, record, redirect or otherwise modify the traffic flowing through the network

...or somebody will do a mistake

...exchanging traffic of a L2VPN and L3VPNs between pair of customers, after the service migration to new devices was carried on is one example

Mistakes happen, but...

- ...if You're not protecting your own traffic, everything can happen, now, in five minutes or in a year
- You may not even notice that 'it is happening!'
 - ...but some portal may announce it to the world
- Most obvious problems are:
 - exchanging control plane traffic (Spanning Tree, VTP, IGP routing information – OSPF, EIGRP, IS-IS) with either service provider or other companies
 - exchanging the user traffic with other companies
 - being victim of prefix hijacking

Network protocol fuzzing

- Ever heard of protocols like

LDP

RSVP

BFD

802.1ah

OSPFv2/v3

SDP

IS-IS

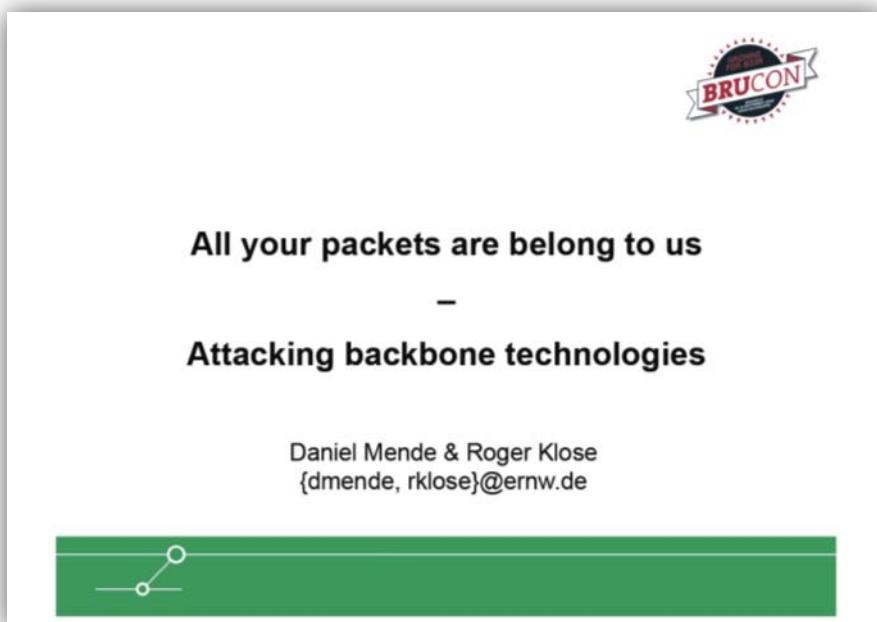
LLDP

802.3ah OAM?

- You probably don't know them inside out, your favorite network protocol fuzzer also, but miracles will come...
- They don't need mpps to drop on your box, sometimes single packet or a slow, steady stream of them will do

<http://www.google.com/search?q=network+protocol+fuzzing>

Is my L2/L3 service secure?



- Another session meant as an eye opener for crowds, but went mainly unnoticed
- Active attacks on BGP (password, prefix injection)
- Active attacks on MPLS (LDP sessions establishment, label exchange and MD5 protection)
- Actually, they only touched around 1% of the points the SP network can be attacked, including the MPLS network, but still, if you don't cover basics, you're [...] anyway!

http://www.ernw.de/content/e7/e181/e1370/download1432/ERNW_BruCon_All_your_packets_ger.pdf

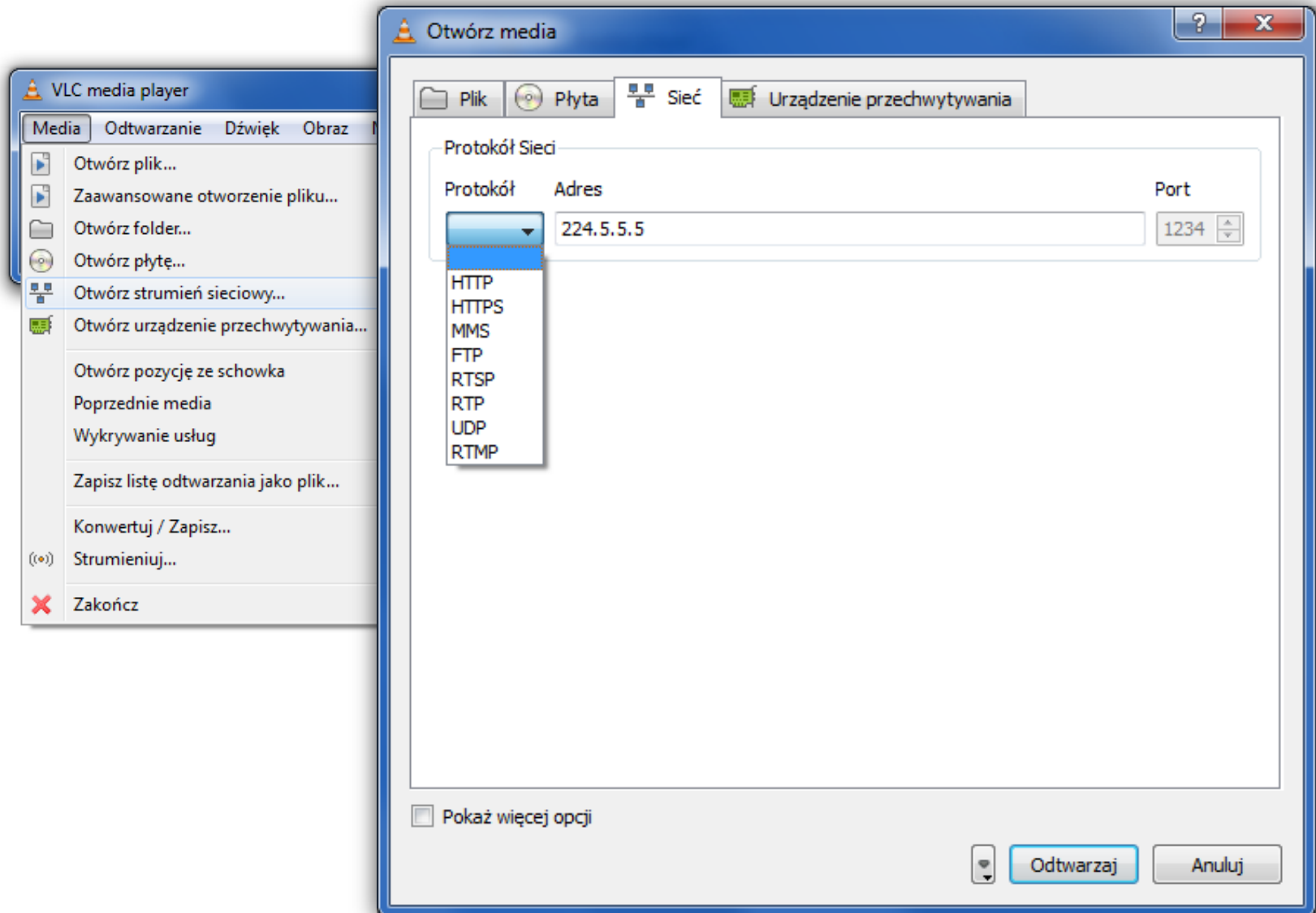
Own the service!



Corporate IPTV? Board teleconferences?

- More and more companies are using IP multicast for
 - corporate IPTV
 - content caching/content delivery networks
 - teleconferences (if running over IP)
 - some of the security camers, personal cameras and other gear uses multicast also (some of which may be...disturbing to see)
- It's often **trivial** to get access to that information by...
 - ...just joining the proper group
- Some dedicated tools exist to do it in one click
 - <http://code.google.com/p/multicast-scanner/>

Corporate IPTV?



Own the IPv6!



IPv6 tools ready to be used

Let the Games Begin

- Sniffers/packet capture

- Snort
- TCPdump
- Sun Solaris snoop
- COLD
- Wireshark
- Analyzer
- Windump
- WinPcap

- Scanners

- IPv6 security scanner
- Halfscan6
- Nmap
- Strobe
- Netcat

- DoS Tools

- 6tunneldos
- 4to6ddos
- Imps6-tools

- Packet forgers

- Scapy6
- SendIP
- Packit
- Spak6

- Complete tool

- <http://www.thc.org/thc-ipv6/>



The Hacker's Choice

Reconnaissance In IPv6

Subnet Size Difference

- Default subnets in IPv6 have 2^{64} addresses
10 Mpps = more than 50 000 years
- NMAP doesn't even support ping sweeps on IPv6 networks



$$\frac{2^{128}}{6.5 \text{ Billion}} = 52 \text{ Trillion Trillion IPv6 addresses per person}$$

World's population is approximately 6.5 billion

Reconnaissance In IPv6

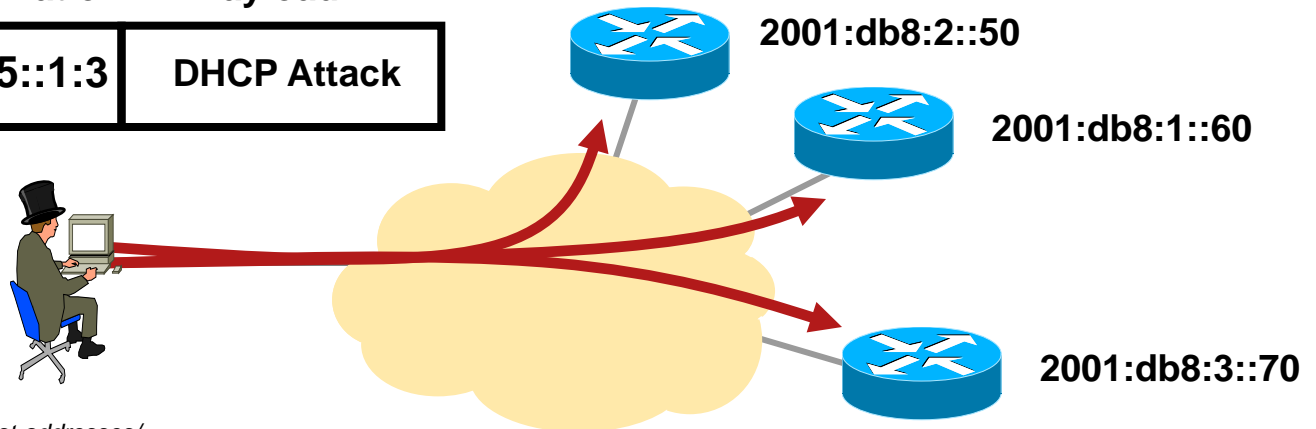
Scanning Methods Are Likely to Change

- Public servers will still need to be DNS reachable
 - More information collected by Google...
- Increased deployment/reliance on dynamic DNS
 - More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses
(::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques (see further) derive IPv6 address from IPv4 address
 - can scan again

Reconnaissance In IPv6? Easy With Multicast!

- No need for reconnaissance anymore
- 3 site-local multicast addresses
 - FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
- Several link-local multicast addresses
 - FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, ...
- Some deprecated (RFC 3879) site-local addresses but still used
 - FEC0:0:0:FFFF::1 DNS server

Source	Destination	Payload
Attacker	FF05::1:3	DHCP Attack



Dual Stack Host Considerations

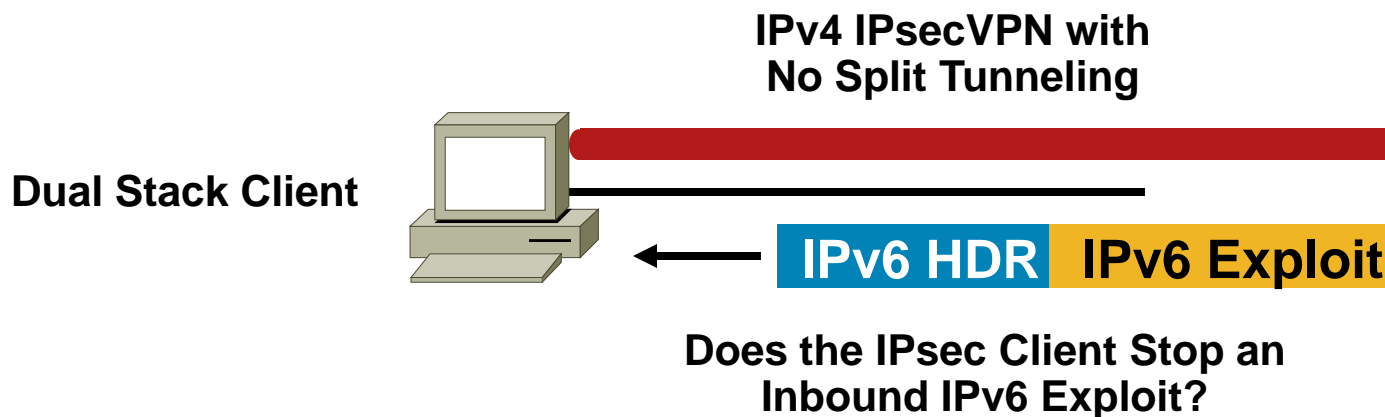
- Host security on a dual-stack device

Applications can be subject to attack on both IPv6 and IPv4

Fate sharing: as secure as the least secure stack...

- Host security controls should block and inspect traffic from both IP versions

Host intrusion prevention, personal firewalls, VPN clients, etc.



Dual Stack With Enabled IPv6 by Default

- Your host:
 - IPv4 is protected by your favorite personal firewall...
 - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- Your network:
 - Does not run IPv6
- Your assumption:
 - I'm safe
- Reality
 - You are **not** safe
 - Attacker sends Router Advertisements
 - Your host configures silently to IPv6
 - You are now under IPv6 attack
- => Probably time to think about IPv6 in your network

Enabling IPv6 on a Remote Host

(in this Case Mac OS/X)

2) Hacker: I'm the Router

1) Dual-Stack MacOS:
any IPv6 Router?

	Destination	Protocol	Info
3 1.568197	2001:db8::1	ICMPv6	Neighbor solicitation
4 99.069381	fe80::215:58ff:fe21:1	ICMPv6	Neighbor solicitation
5 455.573664	fe80::215:58ff:fe21:1	ICMPv6	Router advertisement
6 880.382347	fe80::20d:93ff:fe3	ICMPv6	Router advertisement
7 880.388487	fe80::20d:93ff:fe3	MDNS	standard query response SRV
8 880.578883	fe80::215:58ff:fe2	ICMPv6	Router advertisement
9 880.583454	::	ICMPv6	Neighbor solicitation
10 880.583602	fe80::20d:93ff:fe3	ICMPv6	Multicast listener report
11 880.694784	fe80::20d:93ff:fe3	ICMPv6	Multicast listener report
12 883.604742	fe80::20d:93ff:fe3	ICMPv6	Multicast listener done
13 1476.586161	fe80::215:58ff:fe2	ICMPv6	Router advertisement
14 1716.588901	fe80::215:58ff:fe2	ICMPv6	Router advertisement
15 1806.190418	2001:db8:dead::1	ICMPv6	Neighbor solicitation

⊕	Frame 9 (78 bytes on wire, 78 bytes captured)
⊕	Ethernet II, Src: AppleCom_38:c8:74 (00:0d:93:38:c8:74), Dst: IPv6-Neighbor-Discovery_ff
⊕	Internet Protocol Version 6
⊖	Internet Control Message Protocol v6
	Type: 135 (Neighbor solicitation)
	Code: 0
	Checksum: 0x48da [correct]
	Target: 2001:db8:dead:0:20d:93ff:fe38:c874

3) Newly Enabled IPv6
MacOS does DAD

4) The Full IPv6 Address
of the MacOS

Transition Threats—ISATAP

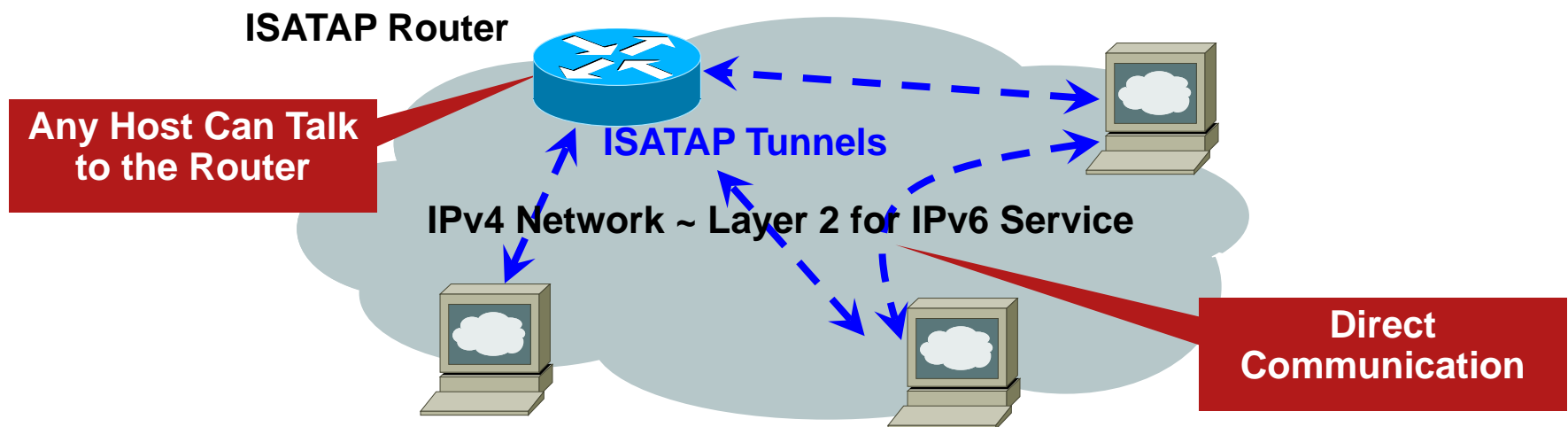
- Unauthorized tunnels—firewall bypass (protocol 41)
- IPv4 infrastructure looks like a Layer 2 network to ALL ISATAP hosts in the enterprise

This has implications on network segmentation and network discovery

- No authentication in ISATAP—rogue routers are possible

Windows default to isatap.example.com

- Ipv6 addresses can be guessed based on IPv4 prefix



6to4 Relay Security Issues

- Traffic injection & IPv6 spoofing

 - Prevent spoofing by applying uRPF check

 - Drops 6to4 packets whose addresses are built on IPv4 bogons

 - Loopback

 - RFC 1918

- Redirection and DoS

 - Block most of the ICMPv6 traffic:

 - No Neighbor Discovery

 - No link-local traffic

 - No redirect

- Traffic is asymmetric

 - 6to4 client/router -> 6to4 relay -> IPv6 server:

 - client IPv4 routing selects the relay

 - IPv6 server -> 6to4 relay -> 6to4 client/router:

 - server IPv6 routing selects the relay

 - Cannot insert a stateful device (firewall, ...) on any path

TEREDO?

- **Teredo navalis**

A shipworm drilling holes
in boat hulls

- **Teredo Microsoftis**

IPv6 in IPv4 punching holes
in NAT devices

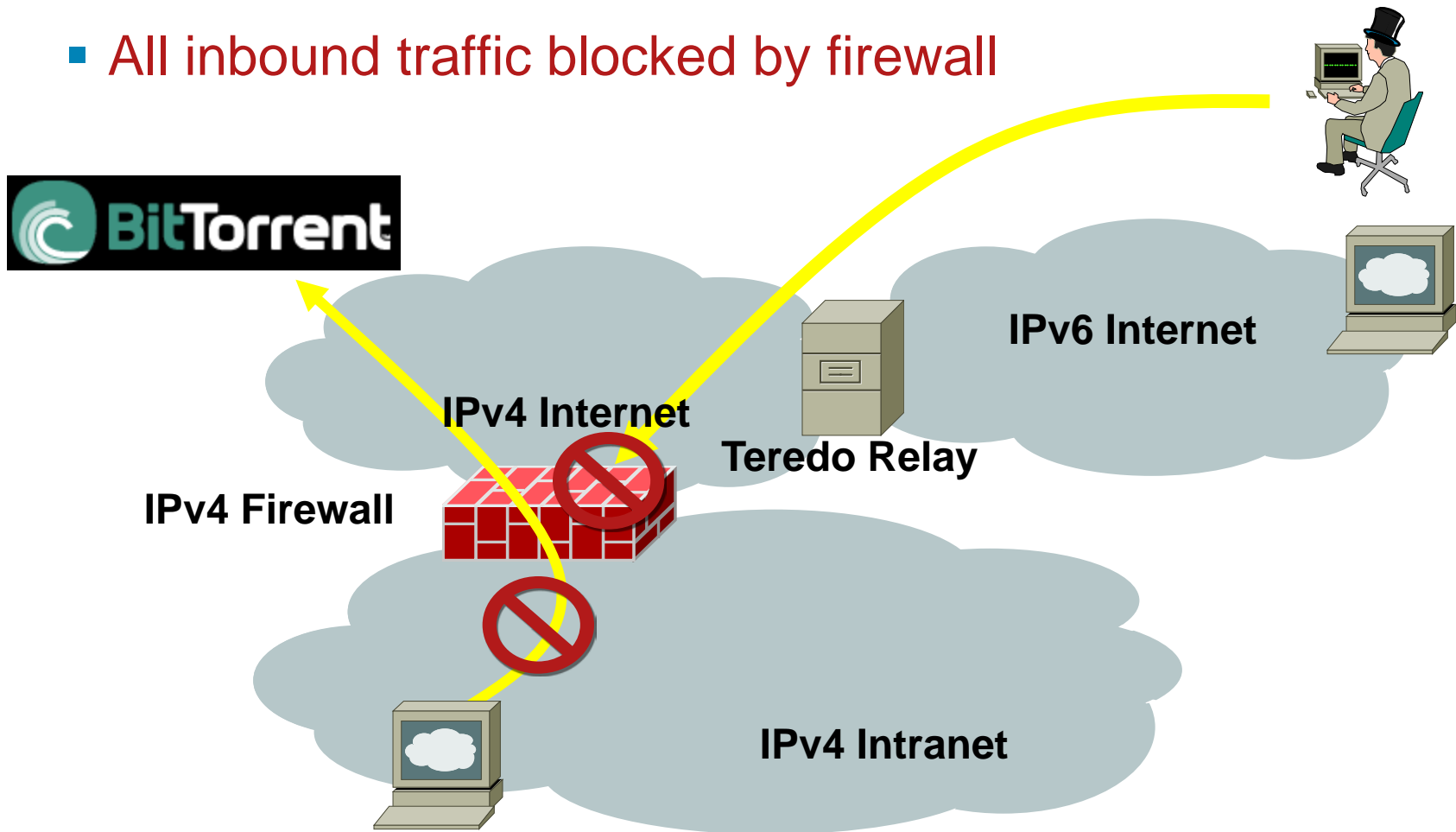


Source: United States Geological Survey

Teredo Tunnels (1/3)

Without Teredo: Controls Are In Place

- All outbound traffic inspected: e.g., P2P is blocked
- All inbound traffic blocked by firewall

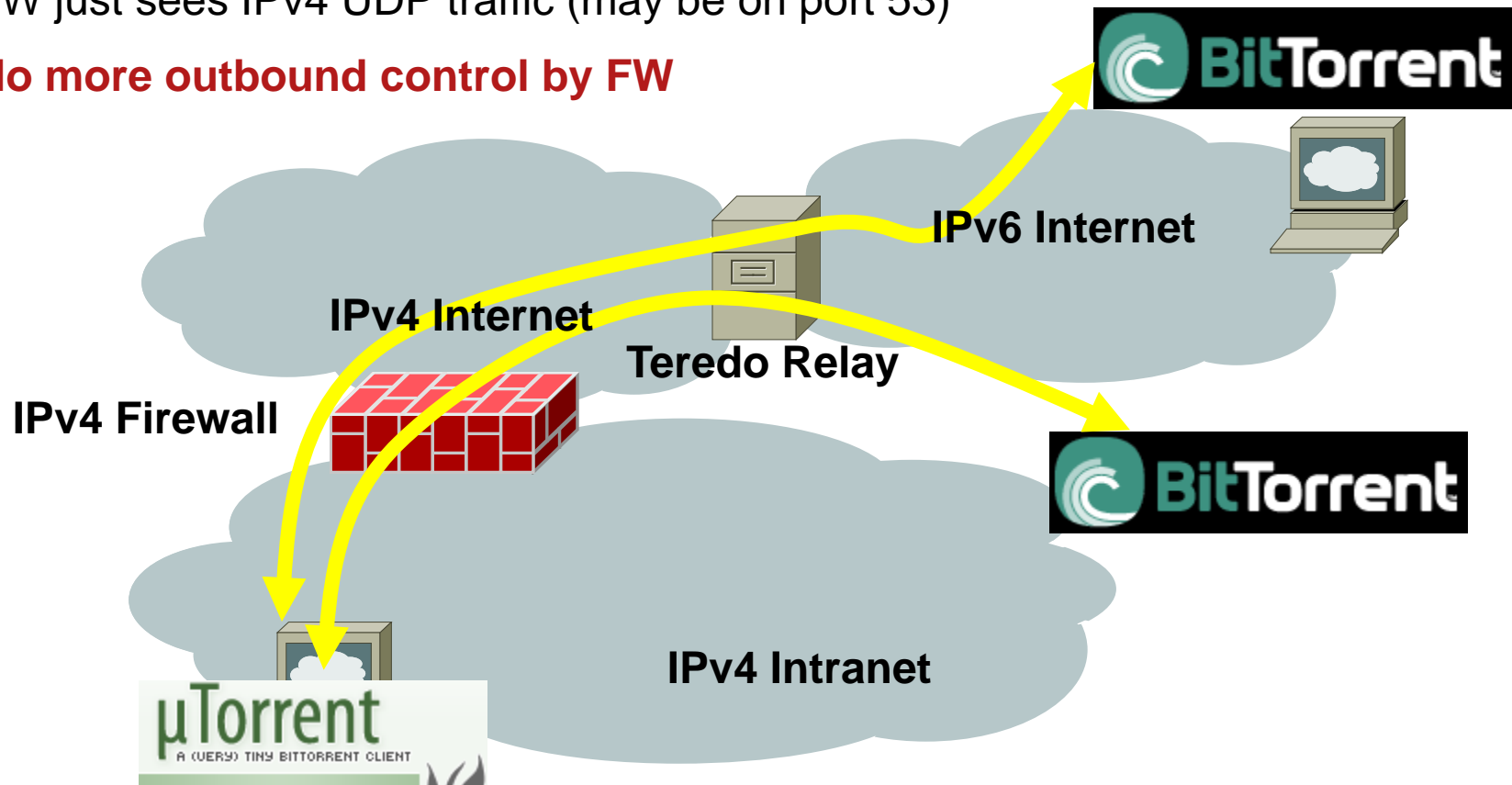


Teredo Tunnels (2/3)

No More Outbound Control

Teredo threats—IPv6 Over UDP (port 3544)

- Internal users want to get P2P over IPv6
- Configure the Teredo tunnel (already enabled by default!)
- FW just sees IPv4 UDP traffic (may be on port 53)
- **No more outbound control by FW**

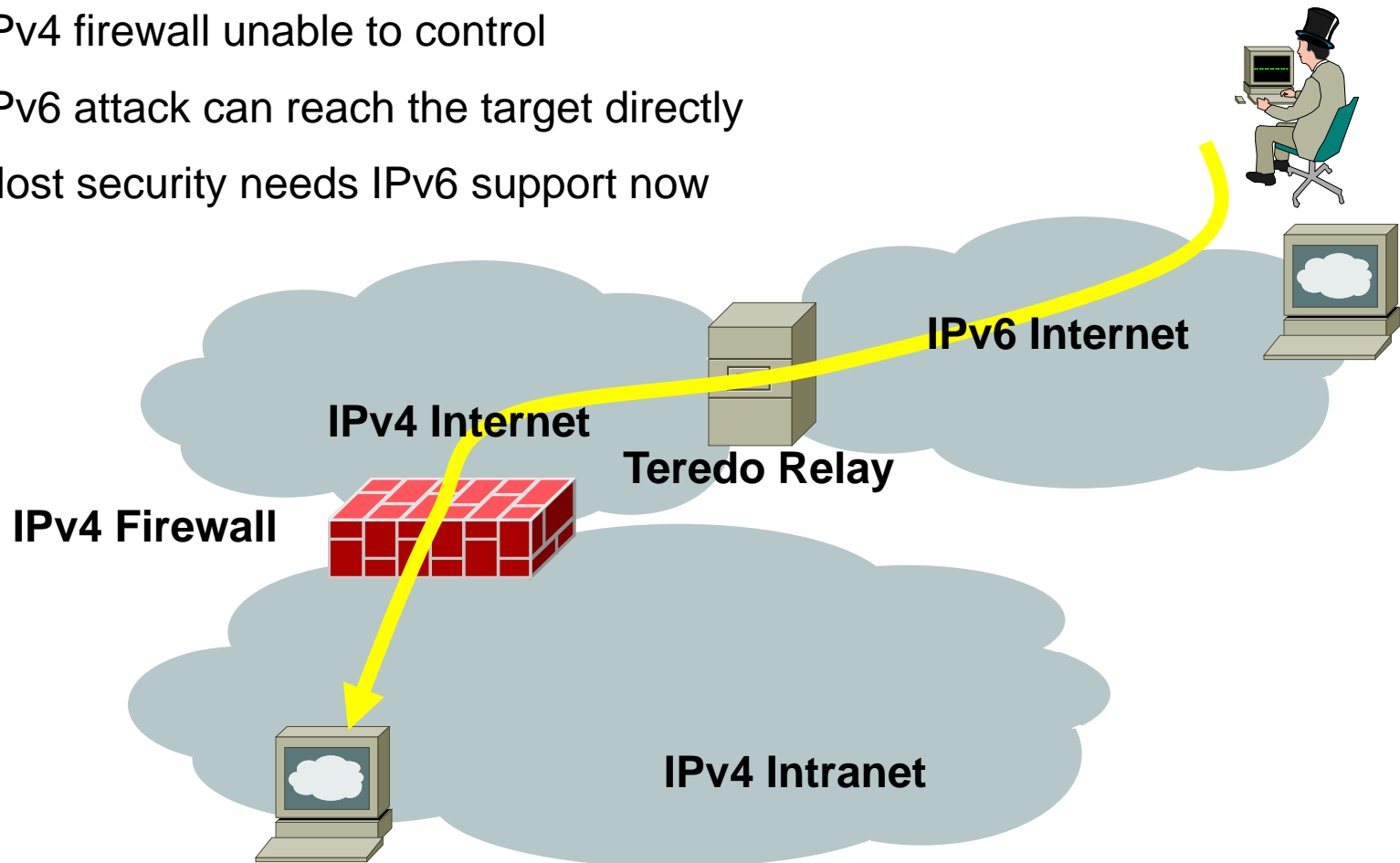


Teredo Tunnels (3/3)

No More Outbound Control

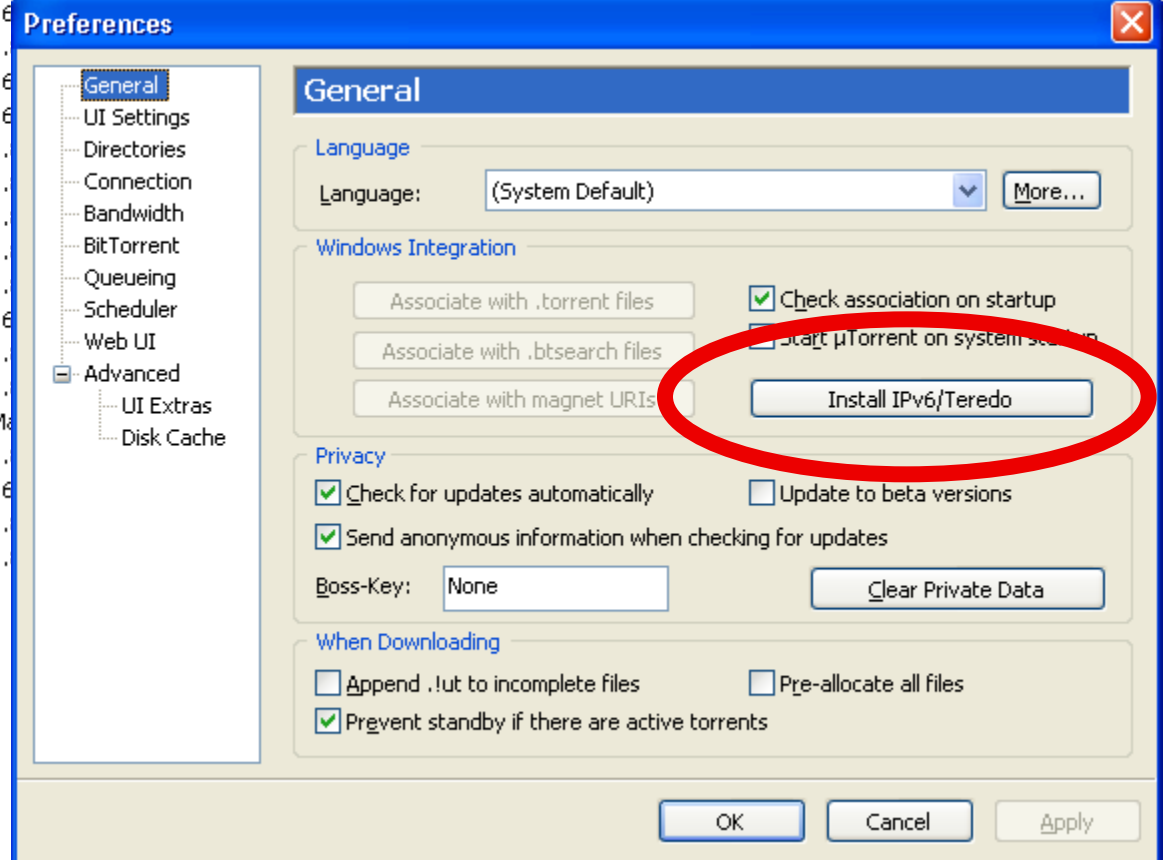
Once Teredo Configured

- **Inbound** connections are allowed
- IPv4 firewall unable to control
- IPv6 attack can reach the target directly
- Host security needs IPv6 support now



µTorrent 1.8 (Released Aug. '08)

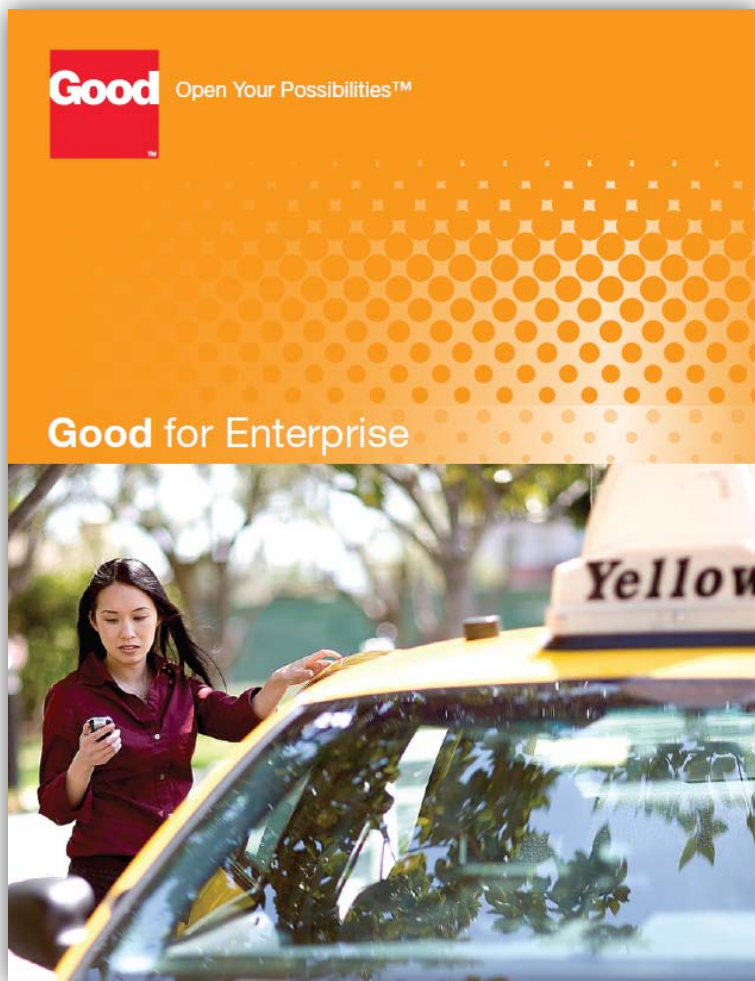
Général		Trackers	Clients	Pièces	Fichiers	Grat
IP		Logiciel client				
2002:53e1:661c::53e1:661c	µTorrent 1.8.2					
2002:5853:3a0f:0:20a:95ff:fed1:5c2e	Transmission 1.51					
2002:59d4:b885::59d4:b885	µTorrent 1.8.2					
2002:7730:ce96::7730:ce96	µTorrent 1.8.2					
2002:bec5:9619::bec5:9619	BitTorrent 6					
2a01:e34:ee07:a7d0:687a:e559:4aaf:556f	µTorrent 1.					
2a01:e34:ee4b:b570:45c1:5889:9c6b:a9d2	BitTorrent 6					
2a01:e35:1380:d200:a13e:1919:8e4e:be93	BitTorrent 6					
2a01:e35:242c:e500:1087:f807:2aa3:64e6	µTorrent 1.					
2a01:e35:243e:b430:29eb:c2f9:f86d:329b	µTorrent 1.					
2a01:e35:2e37:5670:25ef:9941:1d10:c6bc	µTorrent 1.					
2a01:e35:2e58:bd30:2c5e:c2c2:d040:8d0	µTorrent 1.					
2a01:e35:2e60:89b0:96:8b64:1b3c:dcac	µTorrent 1.					
2a01:e35:2e76:d200:7888:4fb8:6adc:54a9	BitTorrent 6					
2a01:e35:2e87:f40:c947:2f74:f5c7:cc99	µTorrent 1.					
2a01:e35:2e9d:ce10:389a:378:a7c7:a715	µTorrent 1.					
2a01:e35:2eb5:2820:221:e9ff:fee5:a32d	µTorrent Ma					
2a01:e35:2f24:7990:ad15:fc01:6907:4b07	µTorrent 1.					
2a01:e35:8a17:4c70:6c5b:3560:b117:49a5	BitTorrent 6					
2a01:e35:8a85:e8f0:d514:7e66:7db:81c8	µTorrent 1.					
2a01:e35:8b43:4c80:e516:cab2:f9af:beec	µTorrent 1.					



**Own the mobile
communication...**



Sort of „two-factor” auth



- You get the e-mail with the PIN
- The PIN let's you install the GoodLink application
- ...which has a access to many applications you use 'in corporate environment'
 - e-mail
 - calendar
- You don't have to break any network security to get the PIN
- Many instances of the same GoodLink app (at least with 5.x) can run at the same time

Own... anything?



The world...

...is full of errors. In software, in hardware, in processes, in people behavior, in documents, in web pages, in documentation... There are no 100% perfect vendors, nor the 90% perfect...

Attack by botnet, a skilful hacker or a script kiddie will hurt just like the same – there's no magic that will save your network, there's only hard work, blood, tears (and Żubrówka)

I encourage You to learn by practice. Don't trust – verify. And have fun!

Questions?



