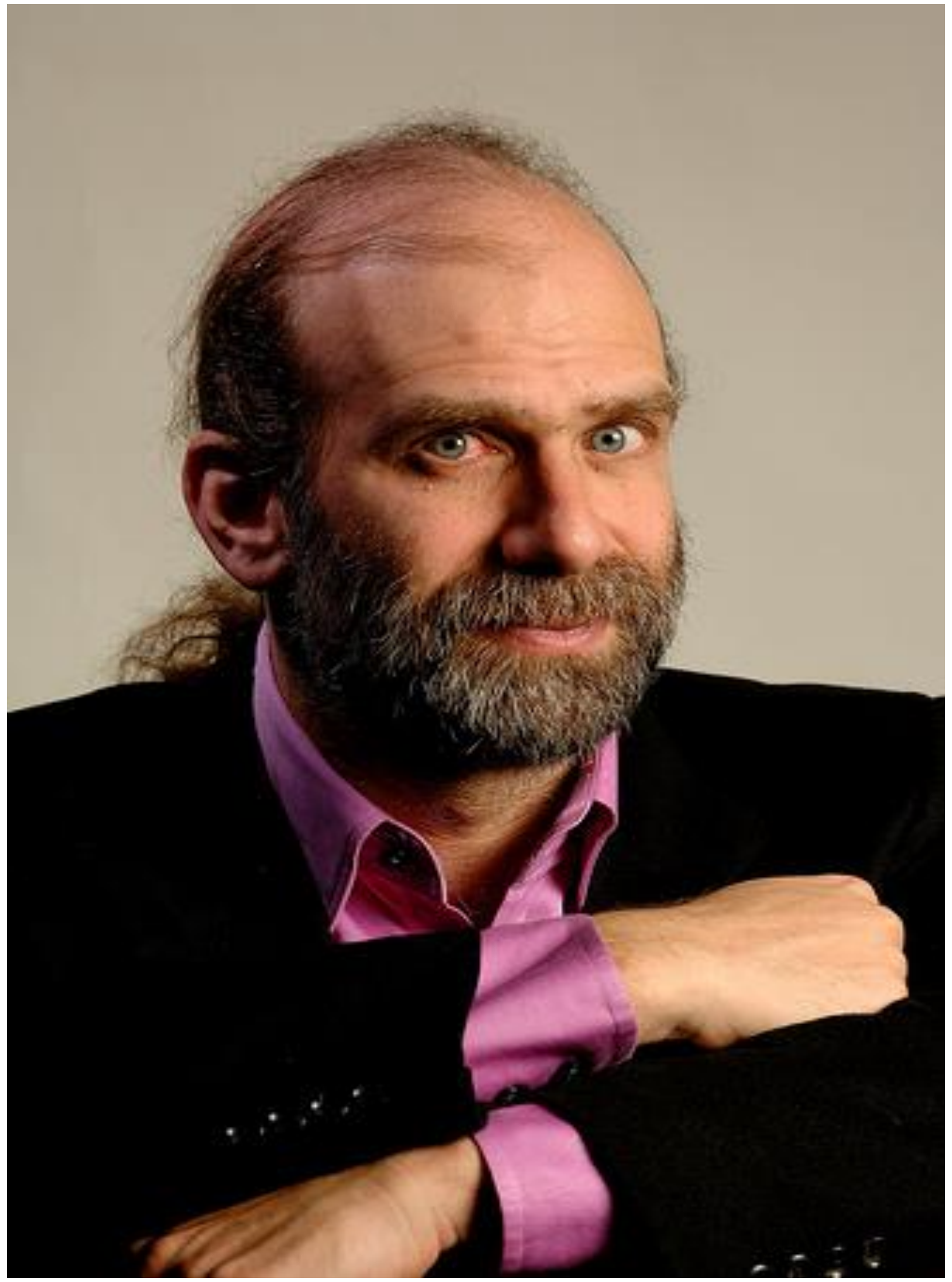
Critical Infrastructure Protection

Why Network Security Fails

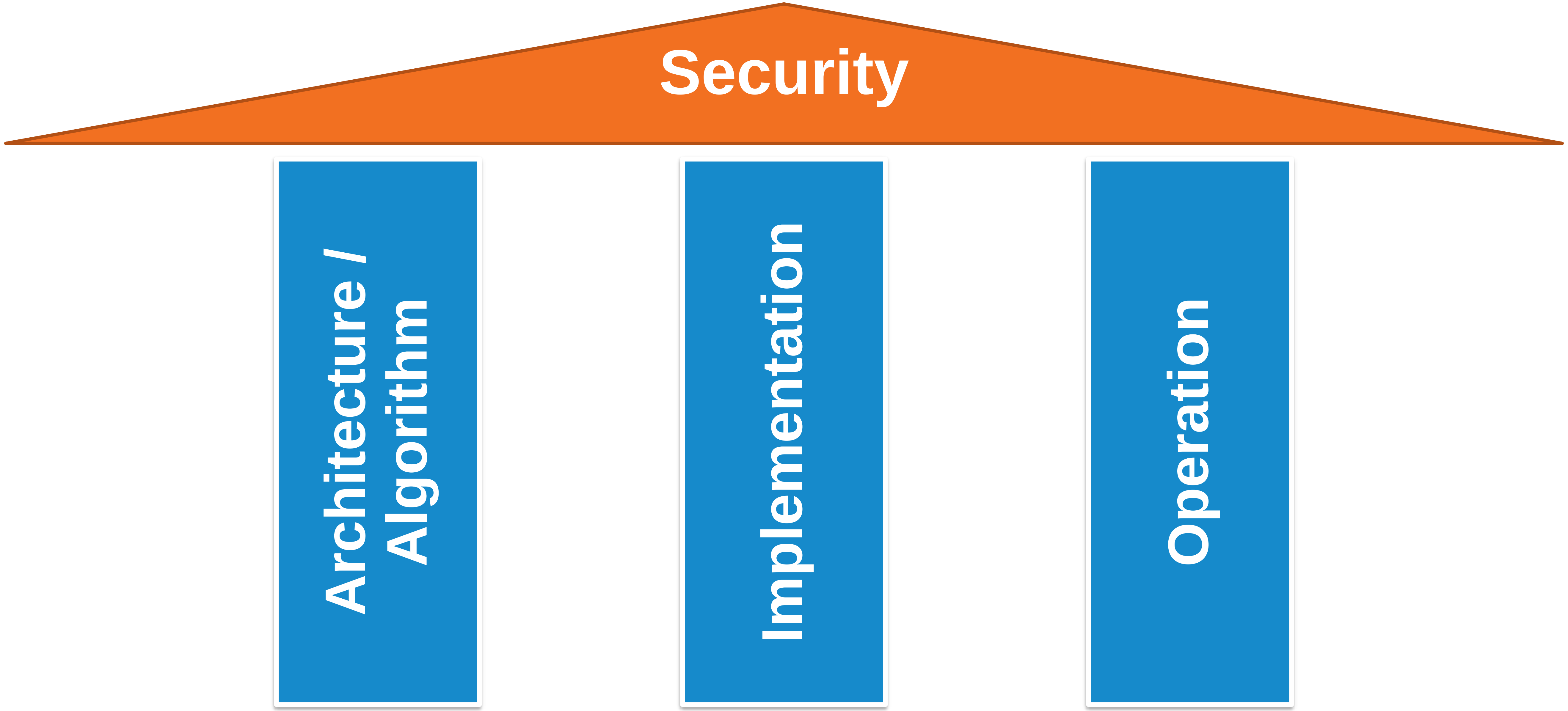
Michael H. Behringer

If you think technology CLI can solve your security problems, then you don't understand the problems and you don't understand the technology CLI.

- Bruce Schneier

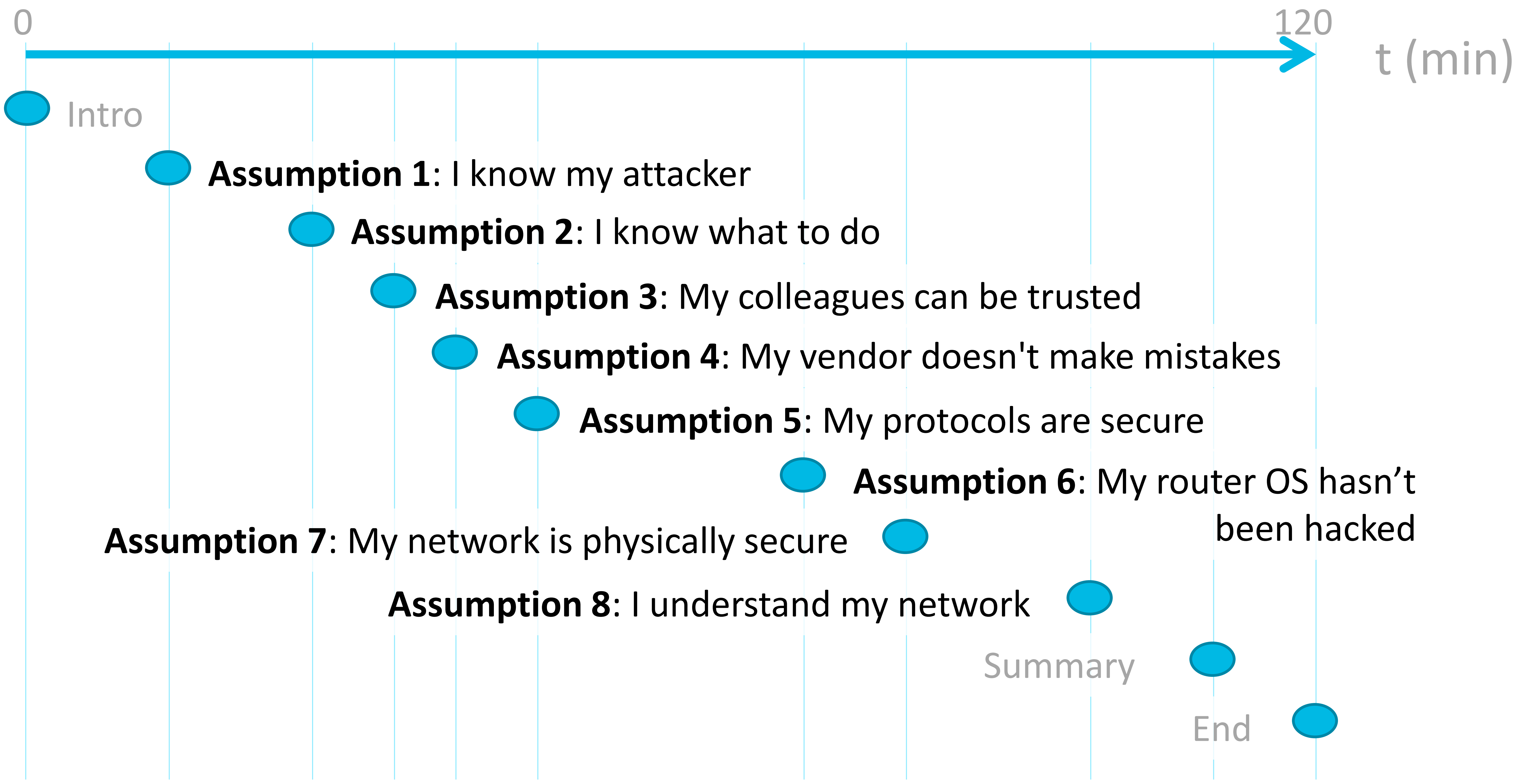


Security Relies on Three Pillars



Break one, and all security is gone!

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

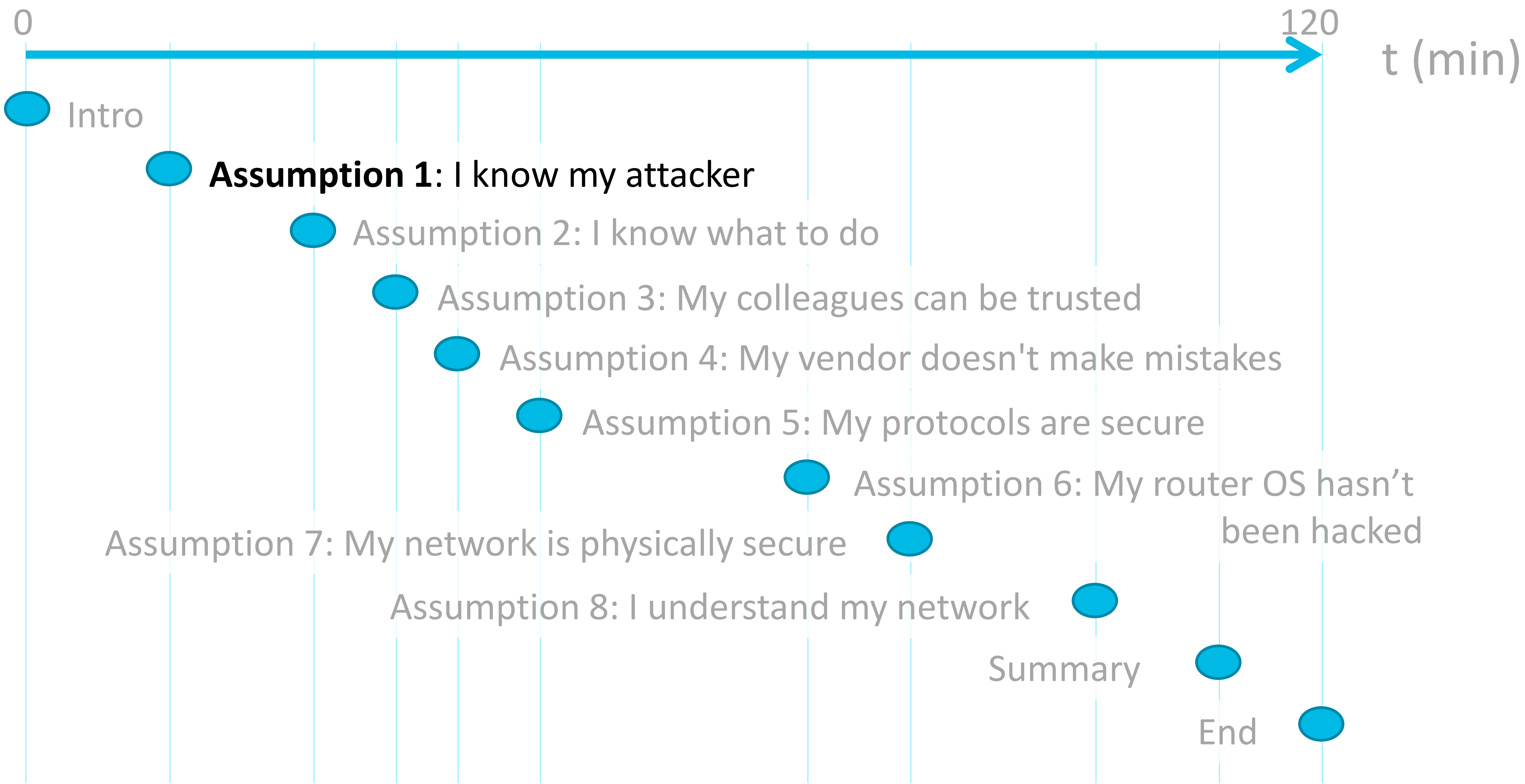
Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

End

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

End

Survey: Who Is Your Most Likely Attacker?

A – Leisure

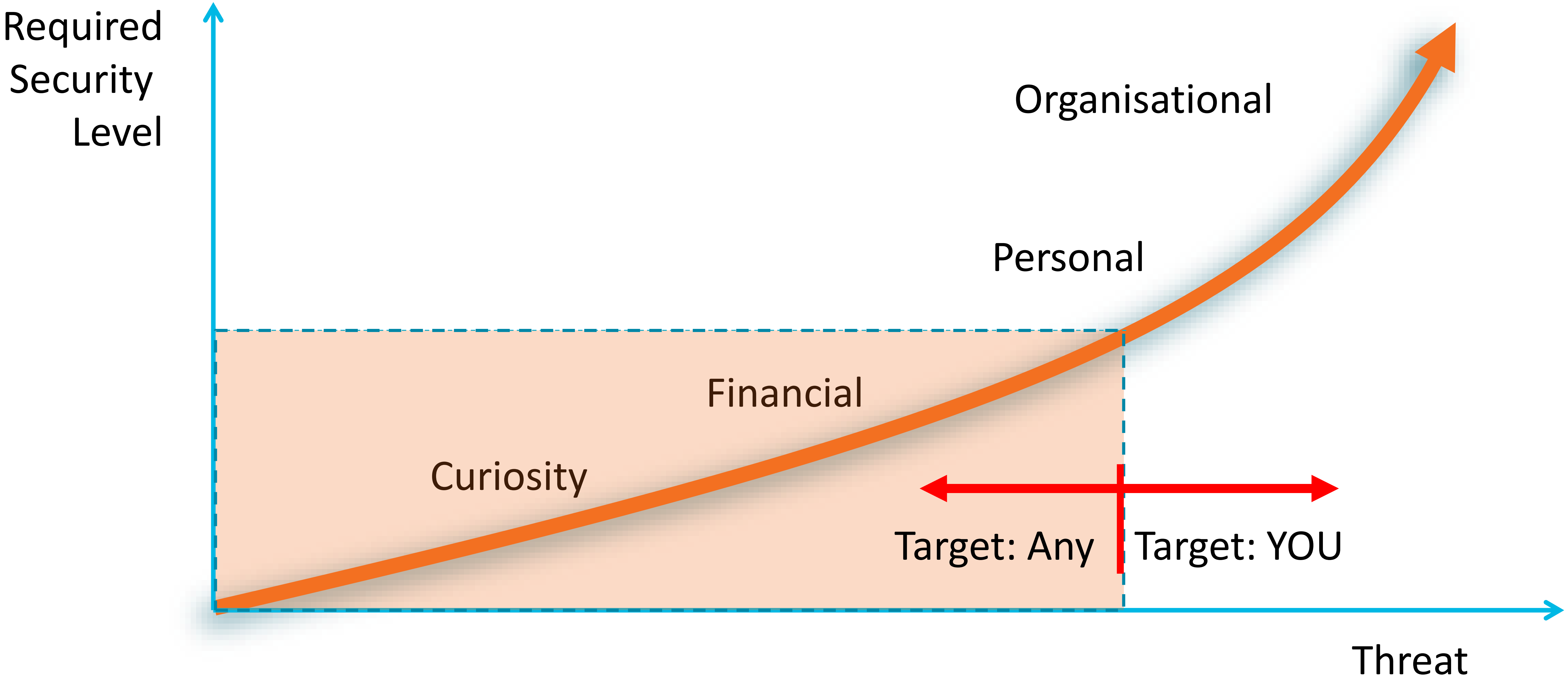
B – Financial motives

C – Insider attacks

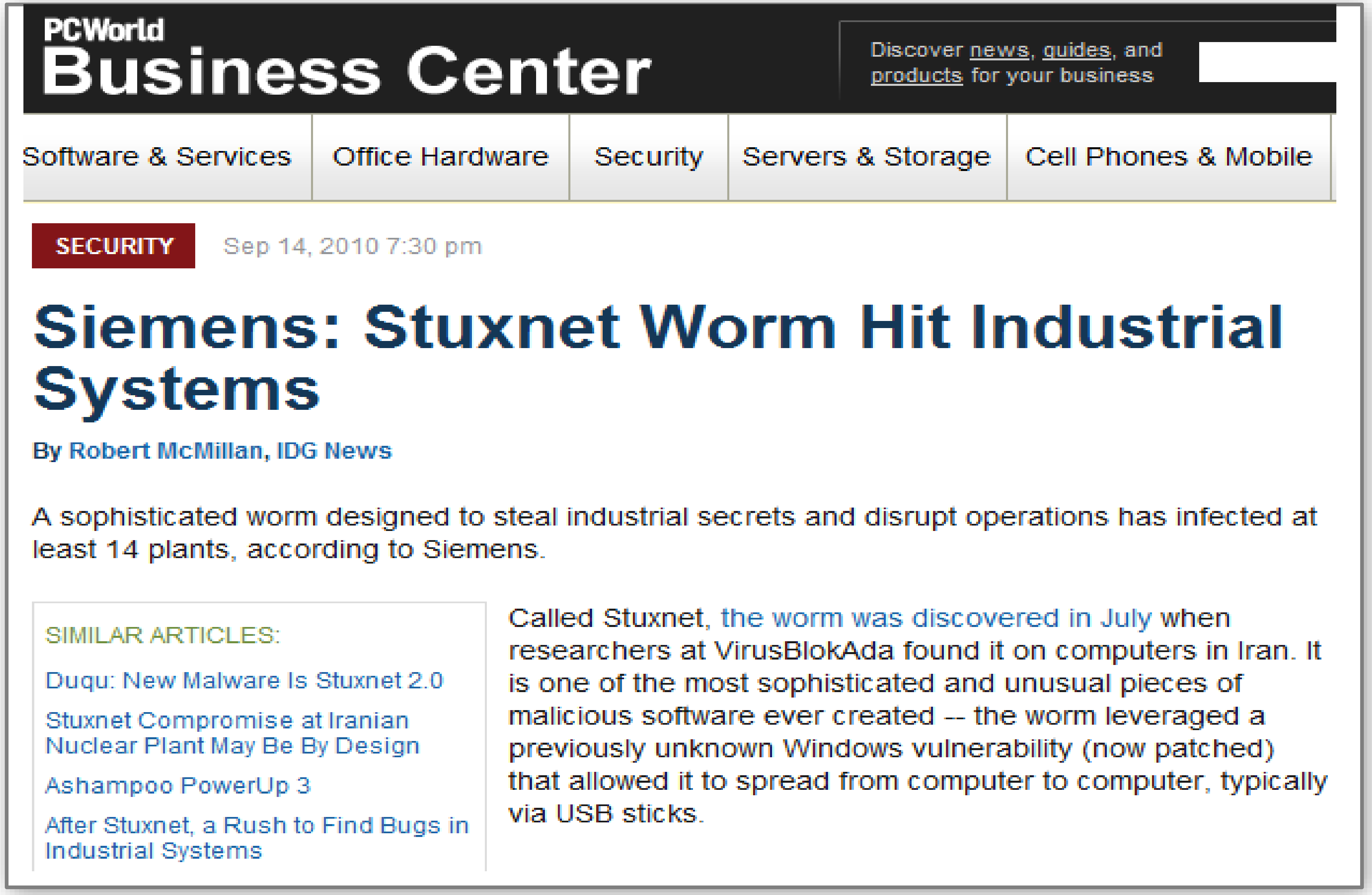
D – “Idealistic” motives

E – Government agencies

Threat Model



2010



PCWorld Business Center

Discover news, guides, and products for your business

Software & Services | Office Hardware | Security | Servers & Storage | Cell Phones & Mobile

SECURITY Sep 14, 2010 7:30 pm

Siemens: Stuxnet Worm Hit Industrial Systems

By Robert McMillan, IDG News

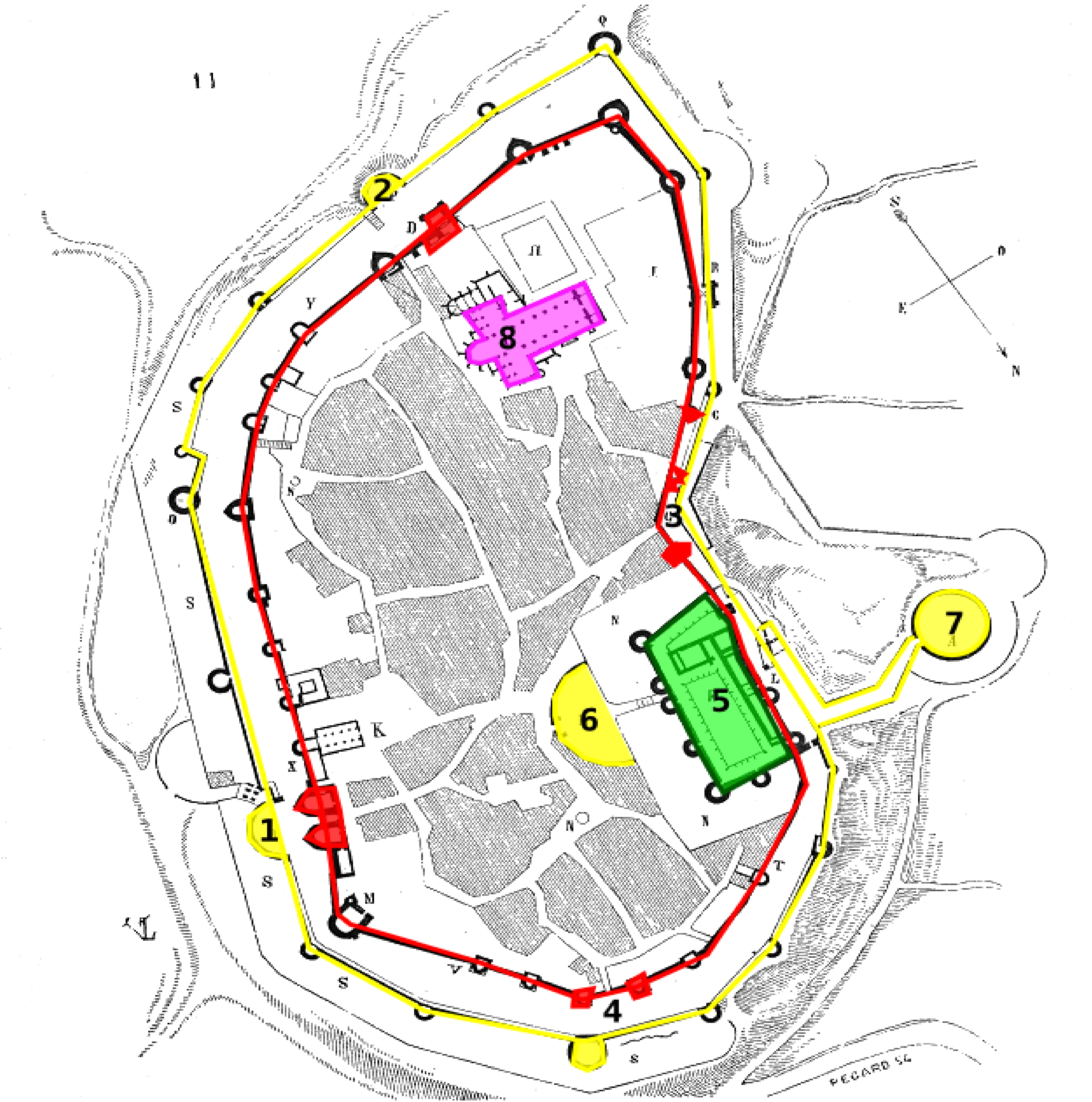
A sophisticated worm designed to steal industrial secrets and disrupt operations has infected at least 14 plants, according to Siemens.

Called Stuxnet, the worm was discovered in July when researchers at VirusBlokAda found it on computers in Iran. It is one of the most sophisticated and unusual pieces of malicious software ever created -- the worm leveraged a previously unknown Windows vulnerability (now patched) that allowed it to spread from computer to computer, typically via USB sticks.

SIMILAR ARTICLES:

- Duqu: New Malware Is Stuxnet 2.0
- Stuxnet Compromise at Iranian Nuclear Plant May Be By Design
- Ashampoo PowerUp 3
- After Stuxnet, a Rush to Find Bugs in Industrial Systems

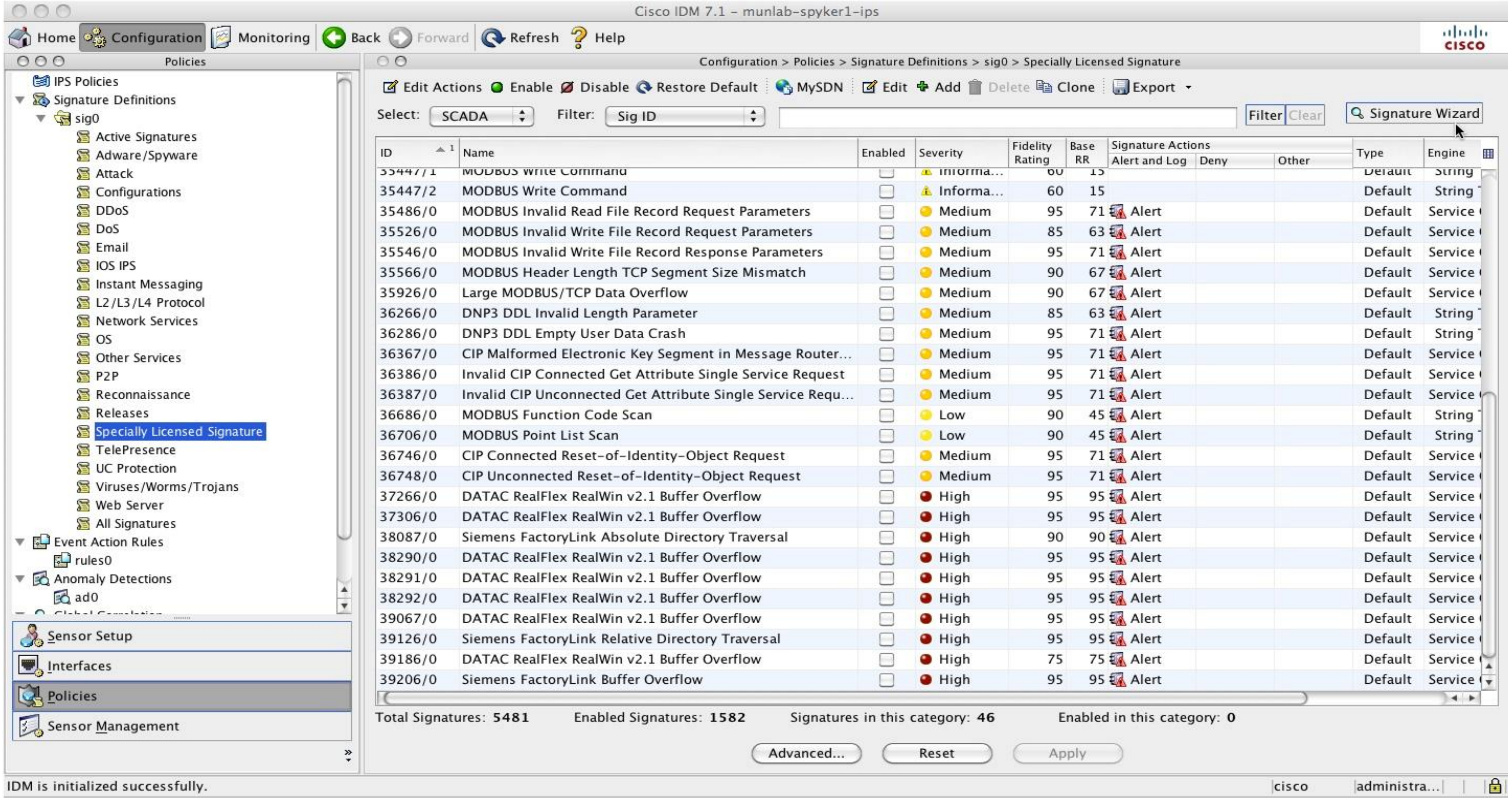
http://www.pcworld.com/businesscenter/article/205420/siemens_stuxnet_worm_hit_industrial_systems.html



Source: http://commons.wikimedia.org/wiki/User:Pinpin

Dusseldorf
Wuppertal
Bruxelles
Brussel
Aachen
Cologne
gium
Verviers
Bonn
Wetzlar
Koblenz
Wiesbaden
Fra
Luxembourg
Sankt Wendel
Mannh
Luxembourg
Saarbrücken
Neustadt
Karlsruhe
Nancy
Baden-Baden
Strasbourg
Reutl
Freiburg
Belfort
Mulhouse
Dijon
Besançon
Basel
Zur
Biel/Bienne
Lucerne
on-sur-Saône
Switzerla
Lausanne
Geneva
Lyon
Annecy
Chambéry
Vares
Nov
ienne
Grenoble
Turin
Valence
Aless
Avignon
Aix-en-Provence
Monaco
Cannes
arseille
Toulon

Industrial Automation: Only “Passive” Security!



- IPS Policies
- Signature Definitions
  - sig0
    - Active Signatures
    - Adware/Spyware
    - Attack
    - Configurations
    - DDoS
    - DoS
    - Email
    - IOS IPS
    - Instant Messaging
    - L2/L3/L4 Protocol
    - Network Services
    - OS
    - Other Services
    - P2P
    - Reconnaissance
    - Releases
    - Specially Licensed Signature
    - TelePresence
    - UC Protection
    - Viruses/Worms/Trojans
    - Web Server
    - All Signatures
- Event Action Rules
  - rules0
- Anomaly Detections
  - ad0
- Global Correlation

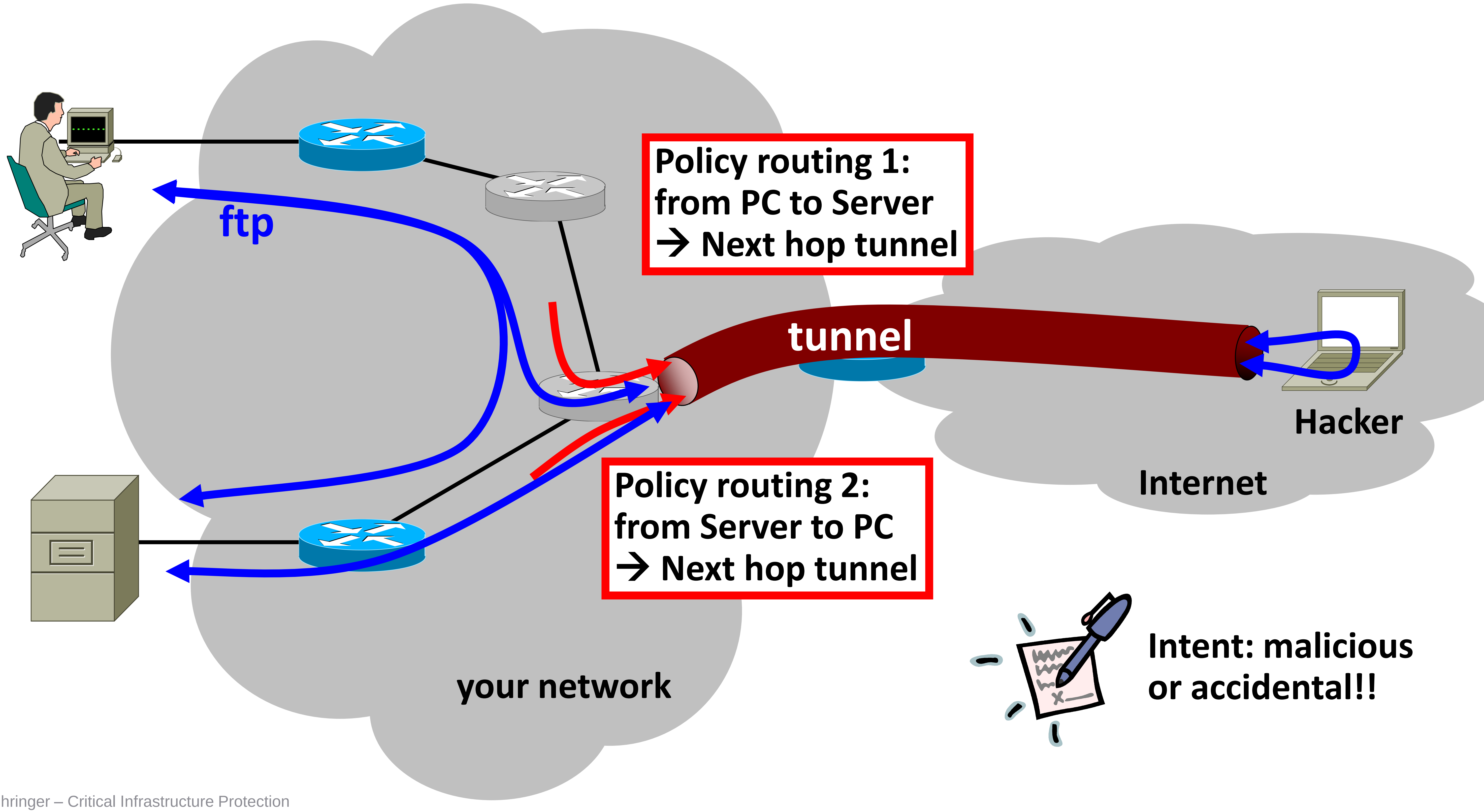
Select: SCADA Filter: Sig ID

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions: Alert and Log	Deny	Other	Type	Engine
35447/1	MODBUS Write Command	□	Informa...	60	15				Default	String
35447/2	MODBUS Write Command	□	Informa...	60	15				Default	String
35486/0	MODBUS Invalid Read File Record Request Parameters	□	Medium	95	71	Alert			Default	Service
35526/0	MODBUS Invalid Write File Record Request Parameters	□	Medium	85	63	Alert			Default	Service
35546/0	MODBUS Invalid Write File Record Response Parameters	□	Medium	95	71	Alert			Default	Service
35566/0	MODBUS Header Length TCP Segment Size Mismatch	□	Medium	90	67	Alert			Default	Service
35926/0	Large MODBUS/TCP Data Overflow	□	Medium	90	67	Alert			Default	Service
36266/0	DNP3 DDL Invalid Length Parameter	□	Medium	85	63	Alert			Default	String
36286/0	DNP3 DDL Empty User Data Crash	□	Medium	95	71	Alert			Default	String
36367/0	CIP Malformed Electronic Key Segment in Message Router...	□	Medium	95	71	Alert			Default	Service
36386/0	Invalid CIP Connected Get Attribute Single Service Request	□	Medium	95	71	Alert			Default	Service
36387/0	Invalid CIP Unconnected Get Attribute Single Service Requ...	□	Medium	95	71	Alert			Default	Service
36686/0	MODBUS Function Code Scan	□	Low	90	45	Alert			Default	String
36706/0	MODBUS Point List Scan	□	Low	90	45	Alert			Default	String
36746/0	CIP Connected Reset-of-Identity-Object Request	□	Medium	95	71	Alert			Default	Service
36748/0	CIP Unconnected Reset-of-Identity-Object Request	□	Medium	95	71	Alert			Default	Service
37266/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	95	95	Alert			Default	Service
37306/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	95	95	Alert			Default	Service
38087/0	Siemens FactoryLink Absolute Directory Traversal	□	High	90	90	Alert			Default	Service
38290/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	95	95	Alert			Default	Service
38291/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	95	95	Alert			Default	Service
38292/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	95	95	Alert			Default	Service
39067/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	95	95	Alert			Default	Service
39126/0	Siemens FactoryLink Relative Directory Traversal	□	High	95	95	Alert			Default	Service
39186/0	DATAC RealFlex RealWin v2.1 Buffer Overflow	□	High	75	75	Alert			Default	Service
39206/0	Siemens FactoryLink Buffer Overflow	□	High	95	95	Alert			Default	Service

Total Signatures: 5481 Enabled Signatures: 1582 Signatures in this category: 46 Enabled in this category: 0

IDM is initialized successfully. cisco administra...

“Why Would Anyone Hack Into My Router?”



Policy routing 1:
from PC to Server
→ Next hop tunnel

Policy routing 2:
from Server to PC
→ Next hop tunnel

Intent: malicious
or accidental!!

You Know Your Attacker?

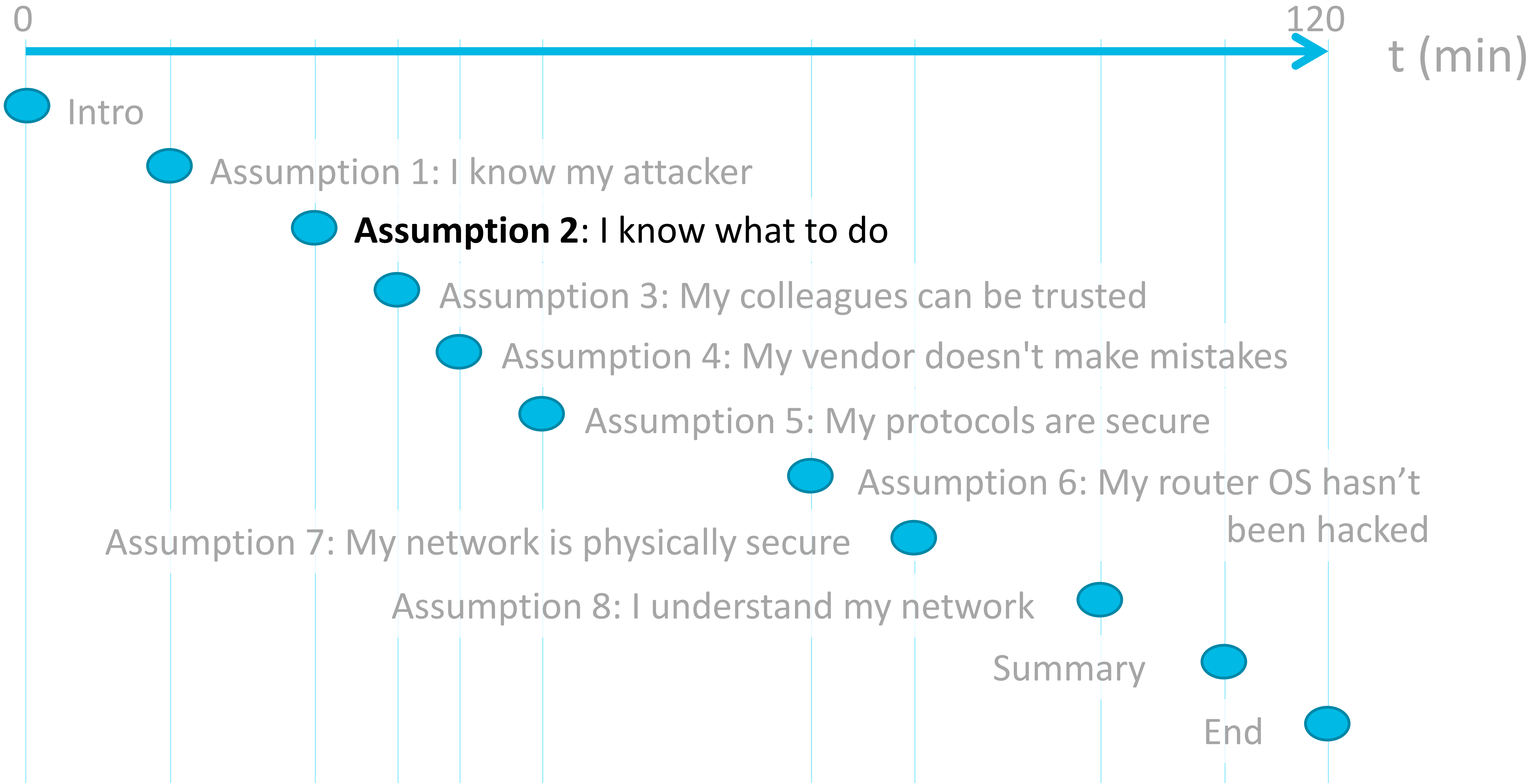
Source: http://www.flickr.com/photos/dseneste/5912382808/

- Motives are hard to predict
- Can change fast
- Network is a target

THEREFORE

- Write threat model
- List attack types:
  - you defend against
  - you do NOT defend against (accept risk)
- Secure according to threat model
- Review regularly

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

End

http://www.cisco.com/security

Security Intelligence Operations

Security Intelligence Operations Best Practices

Security Operations | Network Security | Host Security | Application Security | IPv6

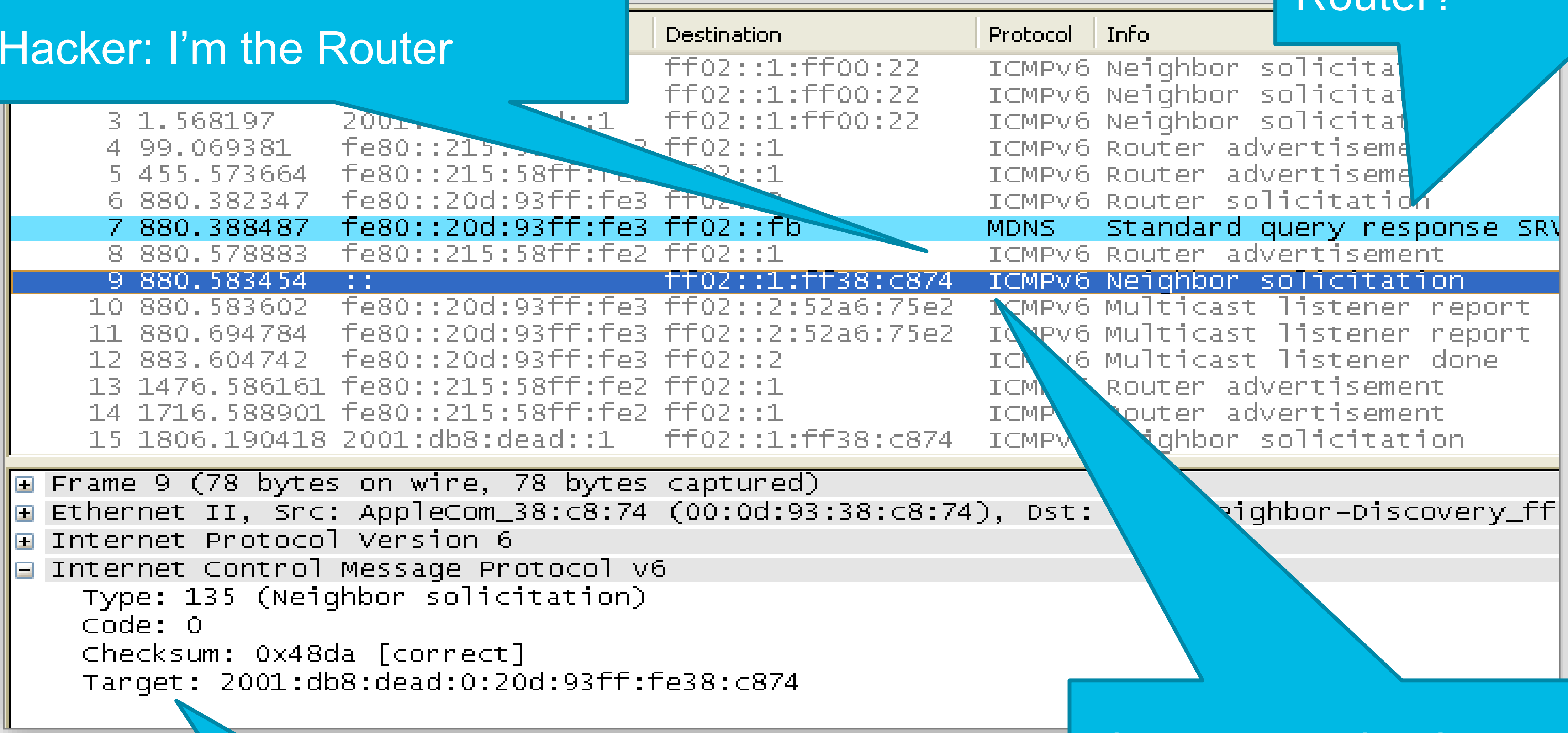
Best Practices and Co

Cisco Guide to Securing Ci
Cisco Guide to Harden Cisc
Cisco TelePresence Harde
Integrating Cisco Anomaly
Lawful Interception for 3G
Protecting Border Gateway
Network Security Baseline
Protecting Your Core: Infra
Cisco IPS Mitigation Capabi
Cisco Guide to Harden Cisc
Service Provider Infrastruc
Understanding Control Plan
Control Plane Policing Imple
Understanding and Using S
Deploying RSVP in Multiple
The Multicast Security Tool
Understanding Unicast Rev
Unicast Reverse Path Forw
Securing Tool Command La

Attack Identification an

Cisco Intrusion Prevention
Cisco Intrusion Prevention
Writing Custom Signatures
Preventing ActiveX Exploits
TTL Expiry Attack Identification and Mitigation

You Know What To Do. Right?



```
                                      Destination          Protocol Info
                                      ff02::1:ff00:22      ICMPv6   Neighbor solicita
                                      ff02::1:ff00:22      ICMPv6   Neighbor solicita
  3 1.568197     2001:           :1   ff02::1:ff00:22      ICMPv6   Neighbor solicitat
  4 99.069381    fe80::215:           ff02::1              ICMPv6   Router advertiseme
  5 455.573664   fe80::215:58ff:        02::1              ICMPv6   Router advertiseme
  6 880.382347   fe80::20d:93ff:fe3   ff02                 ICMPv6   Router solicitation
  7 880.388487   fe80::20d:93ff:fe3   ff02::fb             MDNS     Standard query response SRV
  8 880.578883   fe80::215:58ff:fe2   ff02::1              ICMPv6   Router advertisement
  9 880.583454   ::                   ff02::1:ff38:c874    ICMPv6   Neighbor solicitation
 10 880.583602   fe80::20d:93ff:fe3   ff02::2:52a6:75e2    ICMPv6   Multicast listener report
 11 880.694784   fe80::20d:93ff:fe3   ff02::2:52a6:75e2    IC  v6   Multicast listener report
 12 883.604742   fe80::20d:93ff:fe3   ff02::2              IC  v6   Multicast listener done
 13 1476.586161  fe80::215:58ff:fe2   ff02::1              ICM      Router advertisement
 14 1716.588901  fe80::215:58ff:fe2   ff02::1              ICMP      outer advertisement
 15 1806.190418  2001:db8:dead::1     ff02::1:ff38:c874    ICMPv       ighbor solicitation

⊞ Frame 9 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: AppleCom_38:c8:74 (00:0d:93:38:c8:74), Dst:          eighbor-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
```

1) Dual-Stack MacOS: any IPv6 Router?

2) Hacker: I'm the Router

3) Newly Enabled IPv6 MacOS does Duplicate Address Detection

4) The Full IPv6 Address of the MacOS

Source: Eric Vyncke

Network Security Overview

1. Basic Security
   - AAA, SSH, SNMPv3, rACL, CoPP, etc…

   Individual router security

2. Don’t let packets into (!) the core

   → No way to attack core, except through routing, thus:

   Still “open”: routing protocol

3. Secure the routing protocol
   - Neighbor authentication, maximum routes, route filters, dampening, GTSM, …

   Only attack vector: Transit traffic

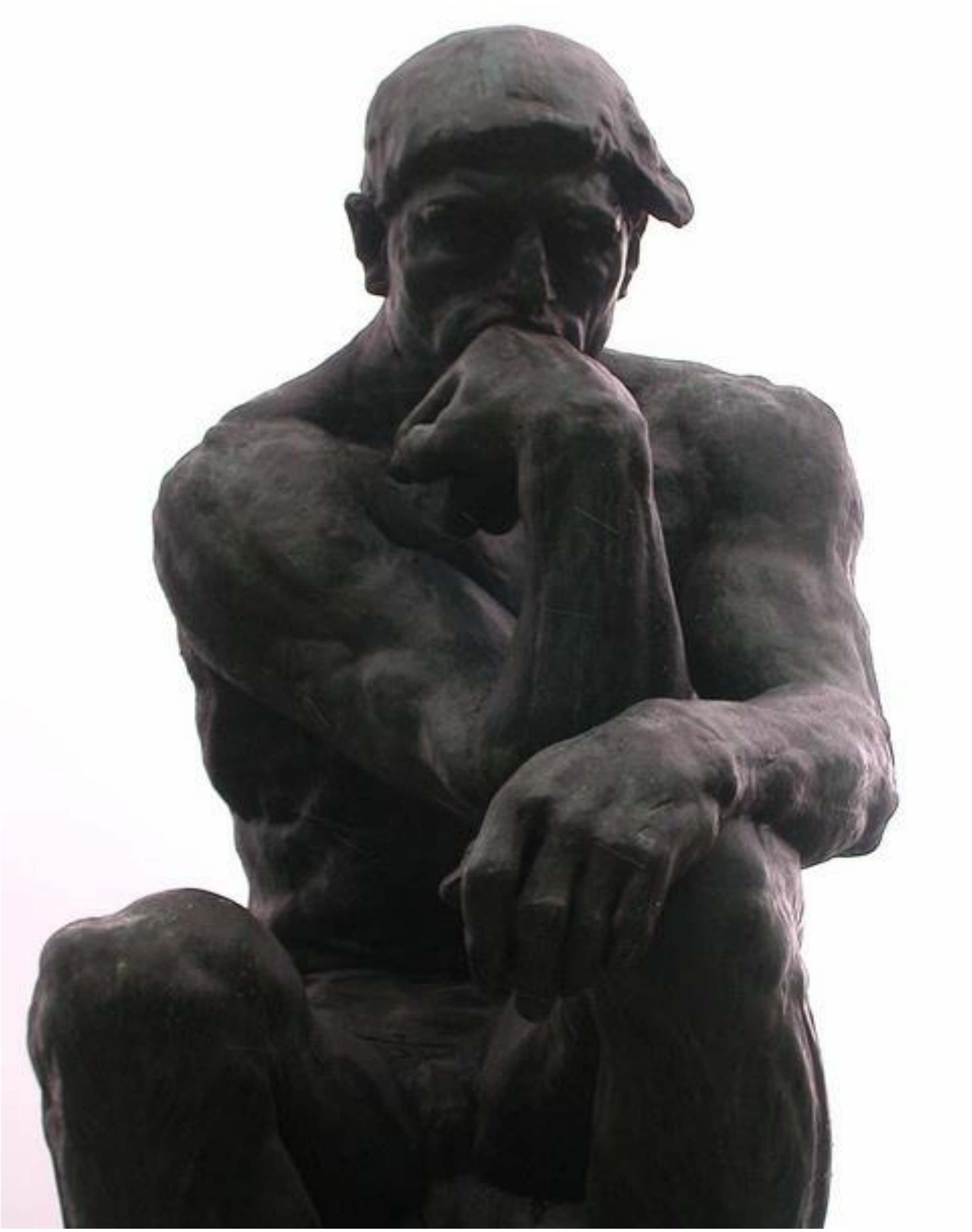
4. Design for transit traffic
   - Correct Core Design (Capacity / QoS)
   - Bogon filters (RFCs 2827, 3330, 3704)
   - Choose correct router for bandwidth

   Now only insider attacks possible

5. Operate Securely

   Avoid insider attacks

You Know What To Do?



Source: http://www.flickr.com/photos/dseneste/5912382808/

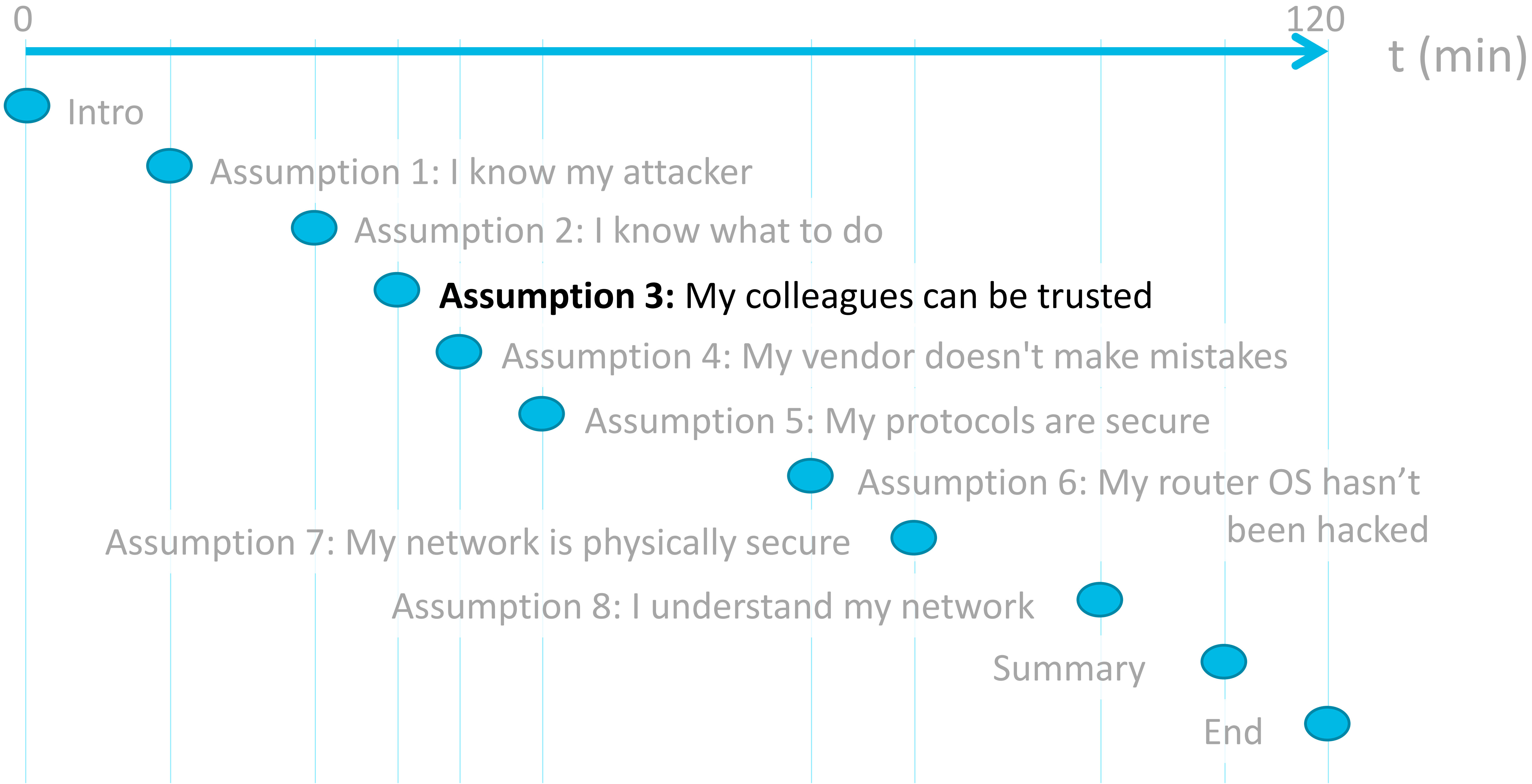
- Assume you don’t
- Assume you forgot something

THERFORE

- Defence in depth:
  More than one type of protection
- Monitoring:
  Detect abnormal conditions
  (AAA, NetFlow, Syslog, SNMP, ...)
- Audits
- Penetration Tests

One of the main detection tools for SP!!

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

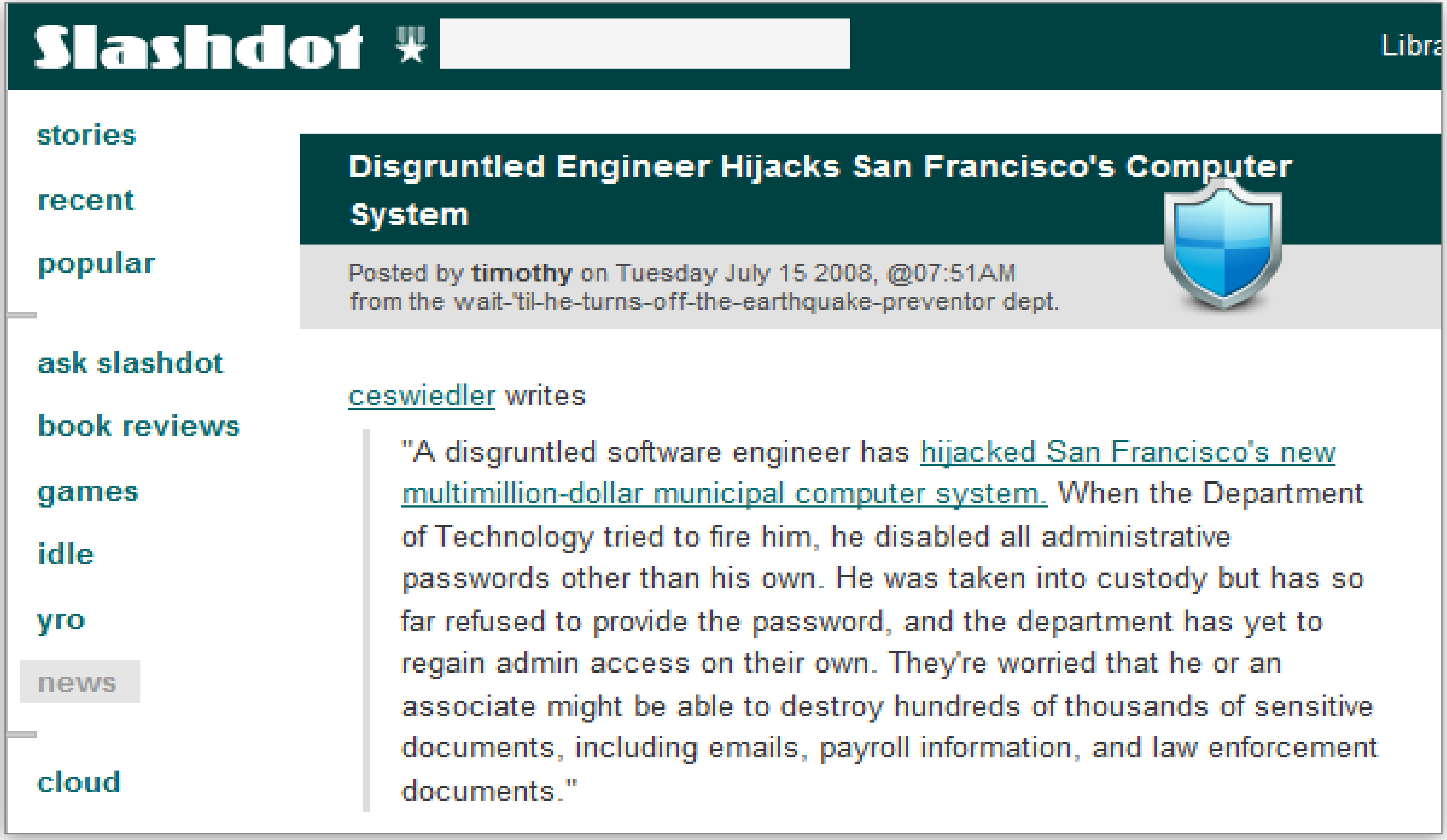
Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

End

2008



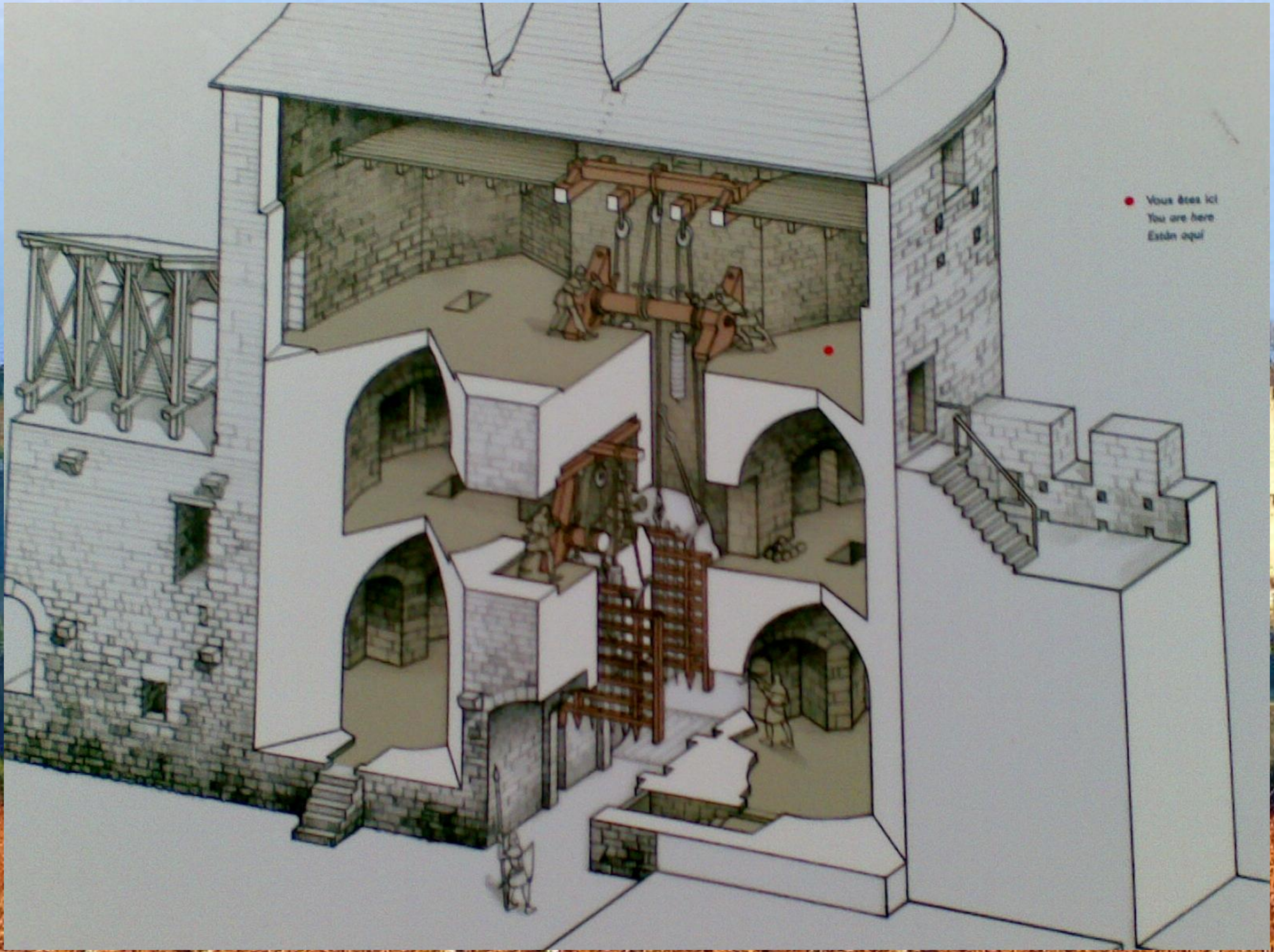
Disgruntled Engineer Hijacks San Francisco's Computer System

Posted by **timothy** on Tuesday July 15 2008, @07:51AM
from the wait-'til-he-turns-off-the-earthquake-preventor dept.

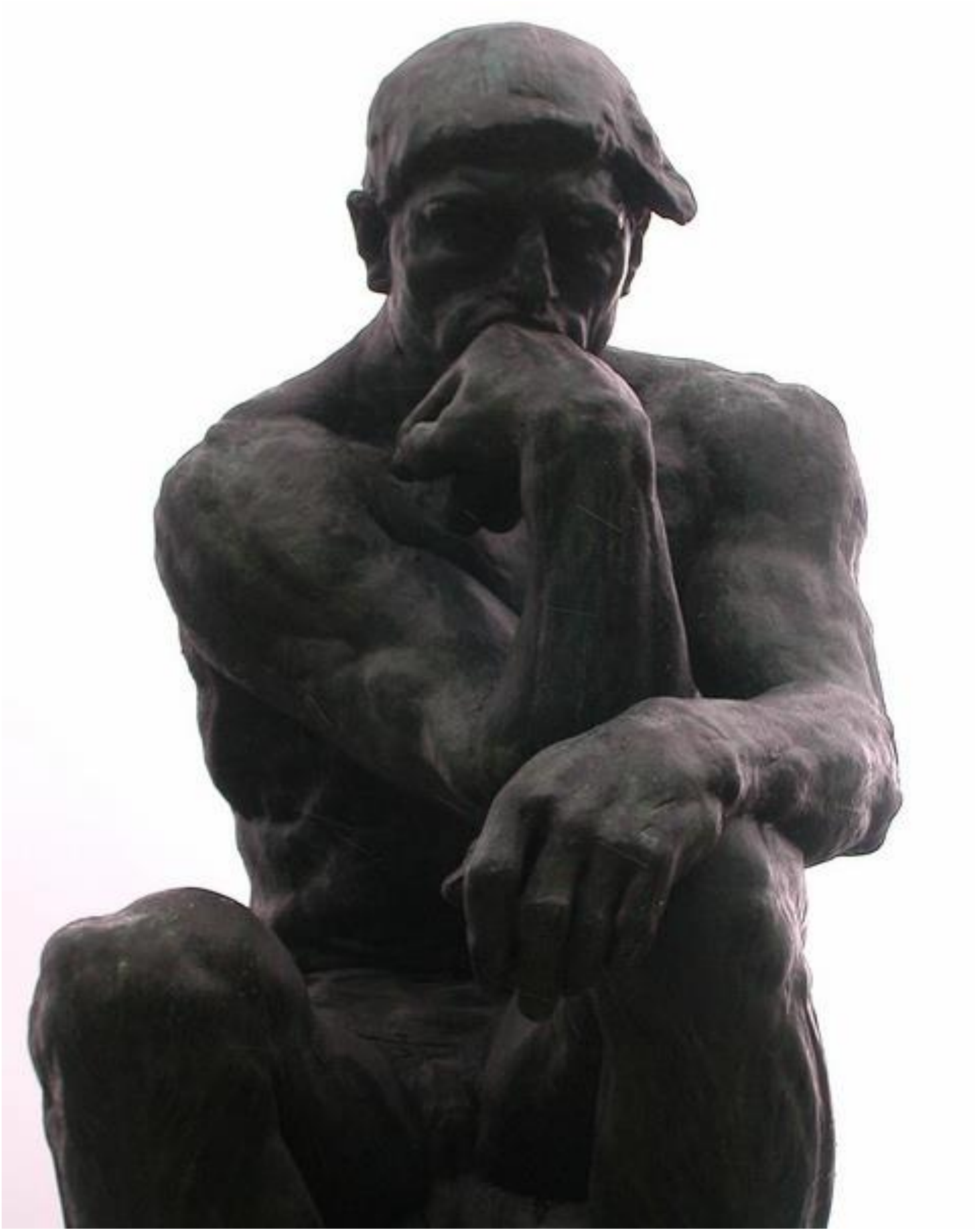
ceswiedler writes

> "A disgruntled software engineer has hijacked San Francisco's new multimillion-dollar municipal computer system. When the Department of Technology tried to fire him, he disabled all administrative passwords other than his own. He was taken into custody but has so far refused to provide the password, and the department has yet to regain admin access on their own. They're worried that he or an associate might be able to destroy hundreds of thousands of sensitive documents, including emails, payroll information, and law enforcement documents."

http://news.slashdot.org/story/08/07/15/120220/disgruntled-engineer-hijacks-san-franciscos-computer-system


● Vous êtes ici
You are here
Están aquí

Your Colleagues Can Be Trusted?



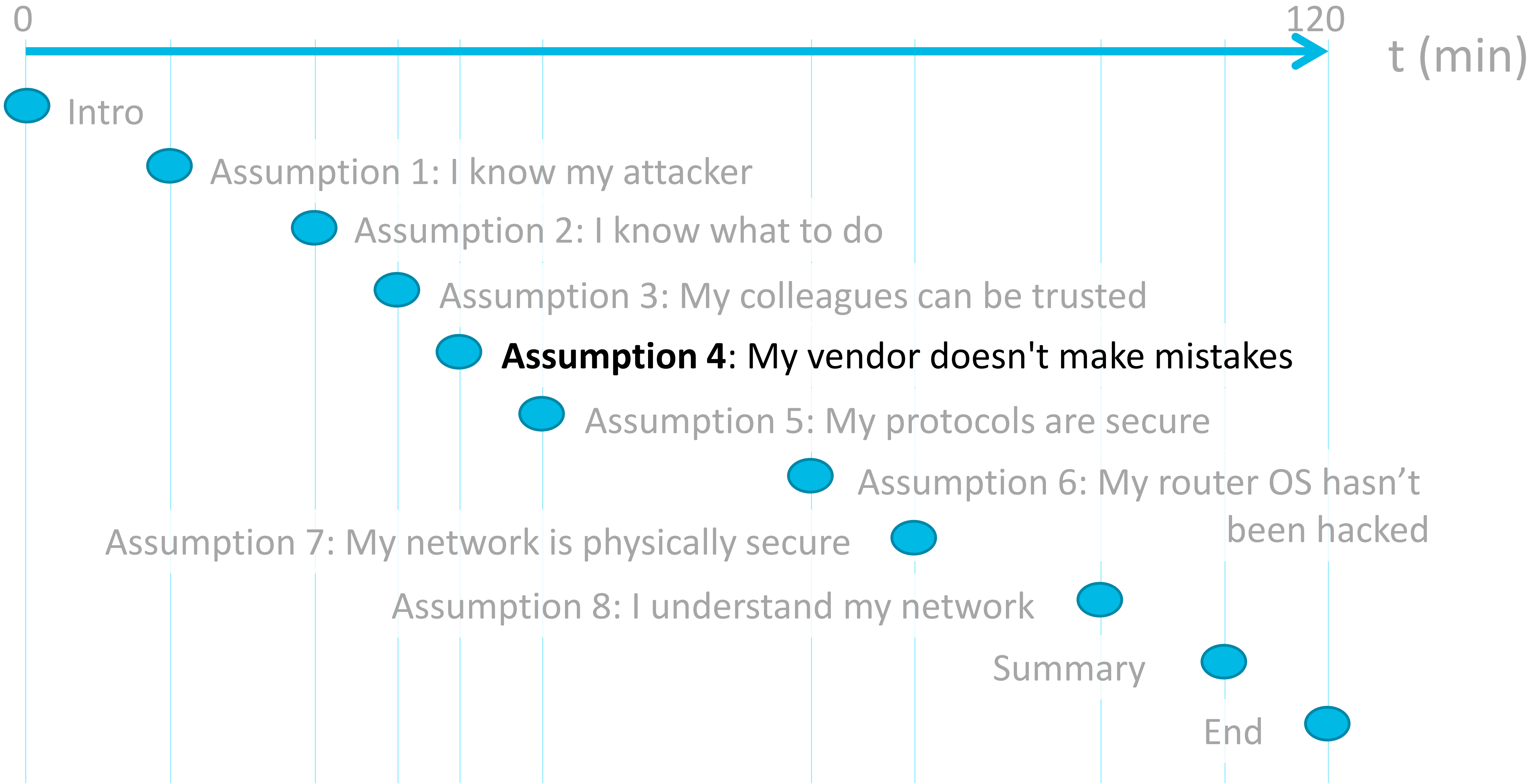
Source: http://www.flickr.com/photos/dseneste/5912382808/

- Hopefully... But:
- Everybody makes mistake
- Think: sabotage

THEREFORE

- Dual control
- Least privilege

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

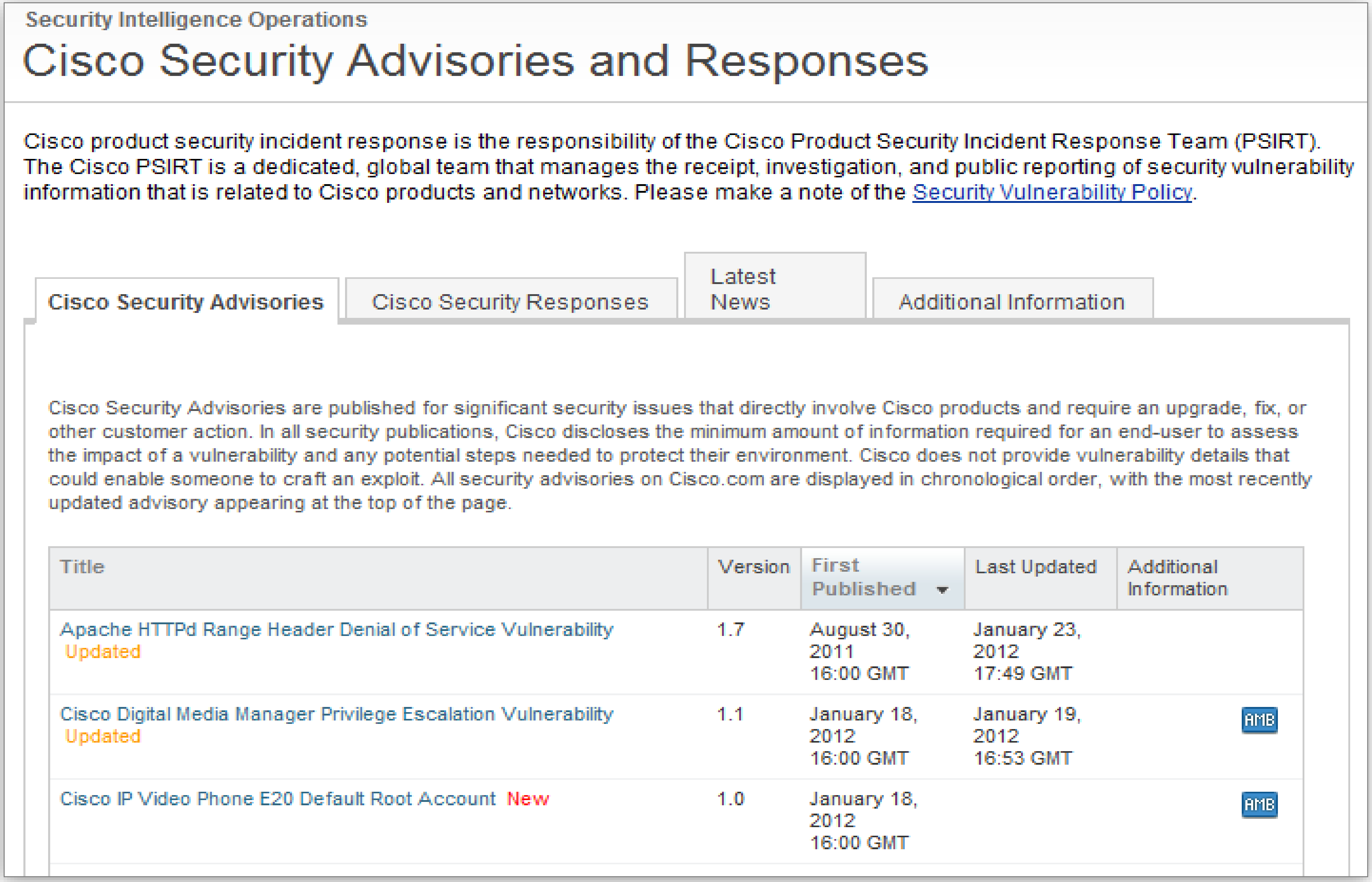
Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

End

www.cisco.com/go/psirt



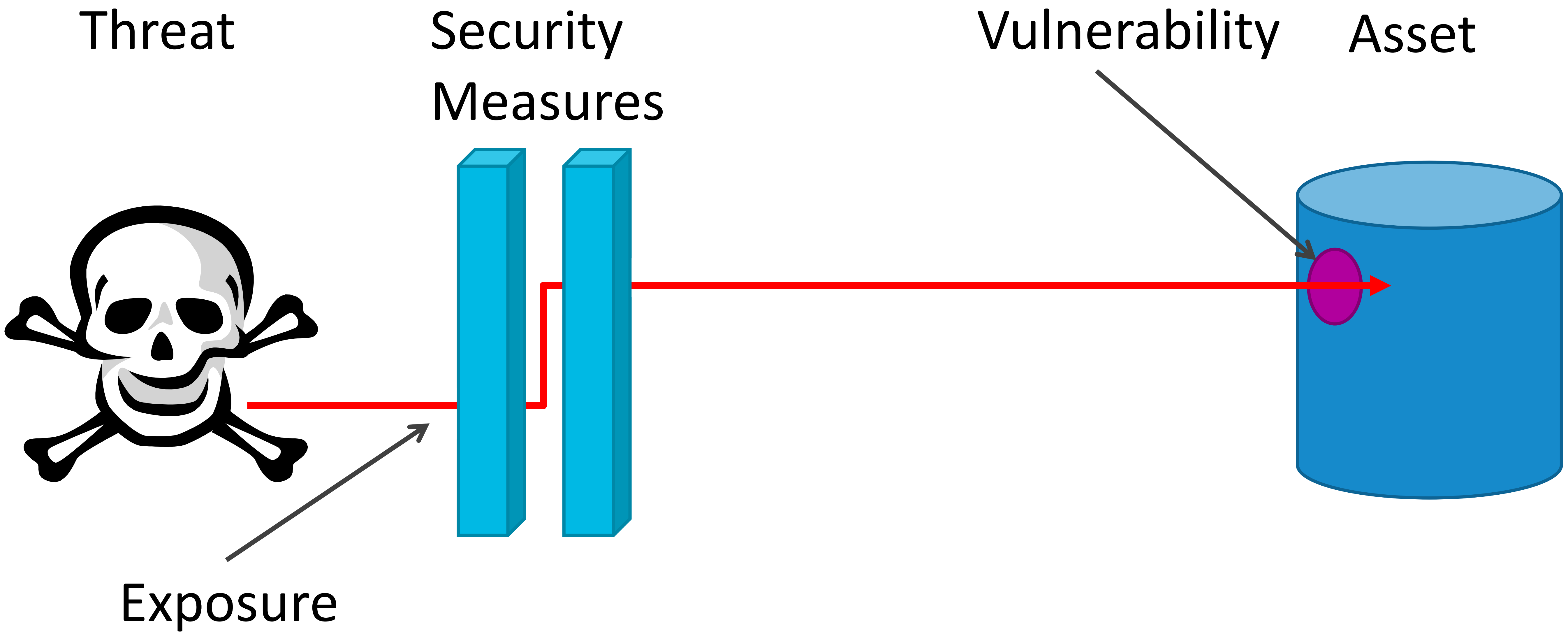
Security Intelligence Operations

Cisco Security Advisories and Responses

Cisco product security incident response is the responsibility of the Cisco Product Security Incident Response Team (PSIRT). The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks. Please make a note of the Security Vulnerability Policy.

Cisco Security Advisories are published for significant security issues that directly involve Cisco products and require an upgrade, fix, or other customer action. In all security publications, Cisco discloses the minimum amount of information required for an end-user to assess the impact of a vulnerability and any potential steps needed to protect their environment. Cisco does not provide vulnerability details that could enable someone to craft an exploit. All security advisories on Cisco.com are displayed in chronological order, with the most recently updated advisory appearing at the top of the page.

Title	Version	First Published ▾	Last Updated	Additional Information
Apache HTTPd Range Header Denial of Service Vulnerability Updated	1.7	August 30, 2011 16:00 GMT	January 23, 2012 17:49 GMT	
Cisco Digital Media Manager Privilege Escalation Vulnerability Updated	1.1	January 18, 2012 16:00 GMT	January 19, 2012 16:53 GMT	AMB
Cisco IP Video Phone E20 Default Root Account New	1.0	January 18, 2012 16:00 GMT		AMB



Threat

Security Measures

Vulnerability

Asset

Exposure

Your Vendor Doesn’t Make Mistakes?

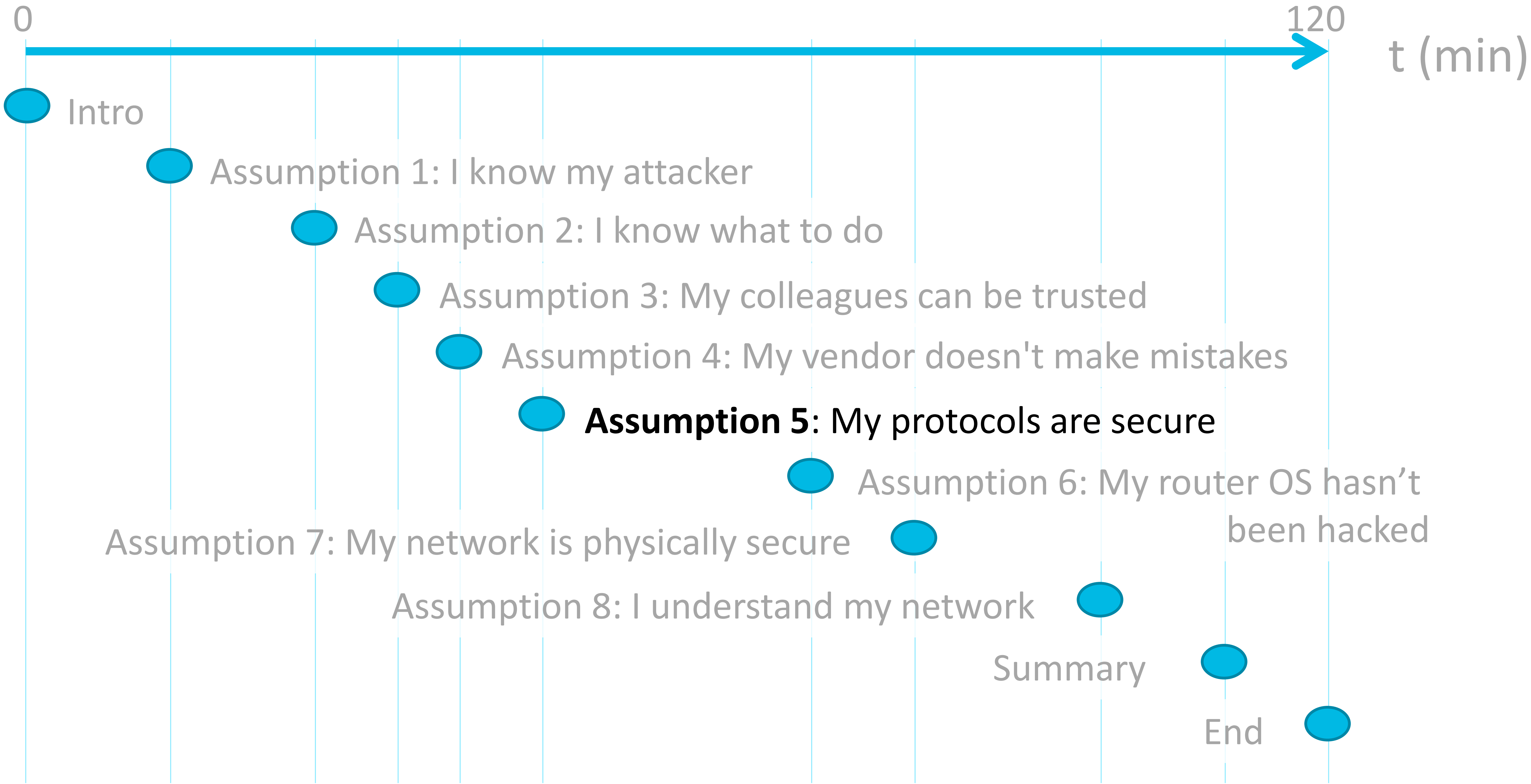
Source: http://www.flickr.com/photos/dseneste/5912382808/

- He does
- Security bugs exist

THEREFORE

- Make network devices unreachable (iACL)
- Insist on vendor having a vulnerability management process (RFP)
- Integrate into your processes
- Have an upgrade policy

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

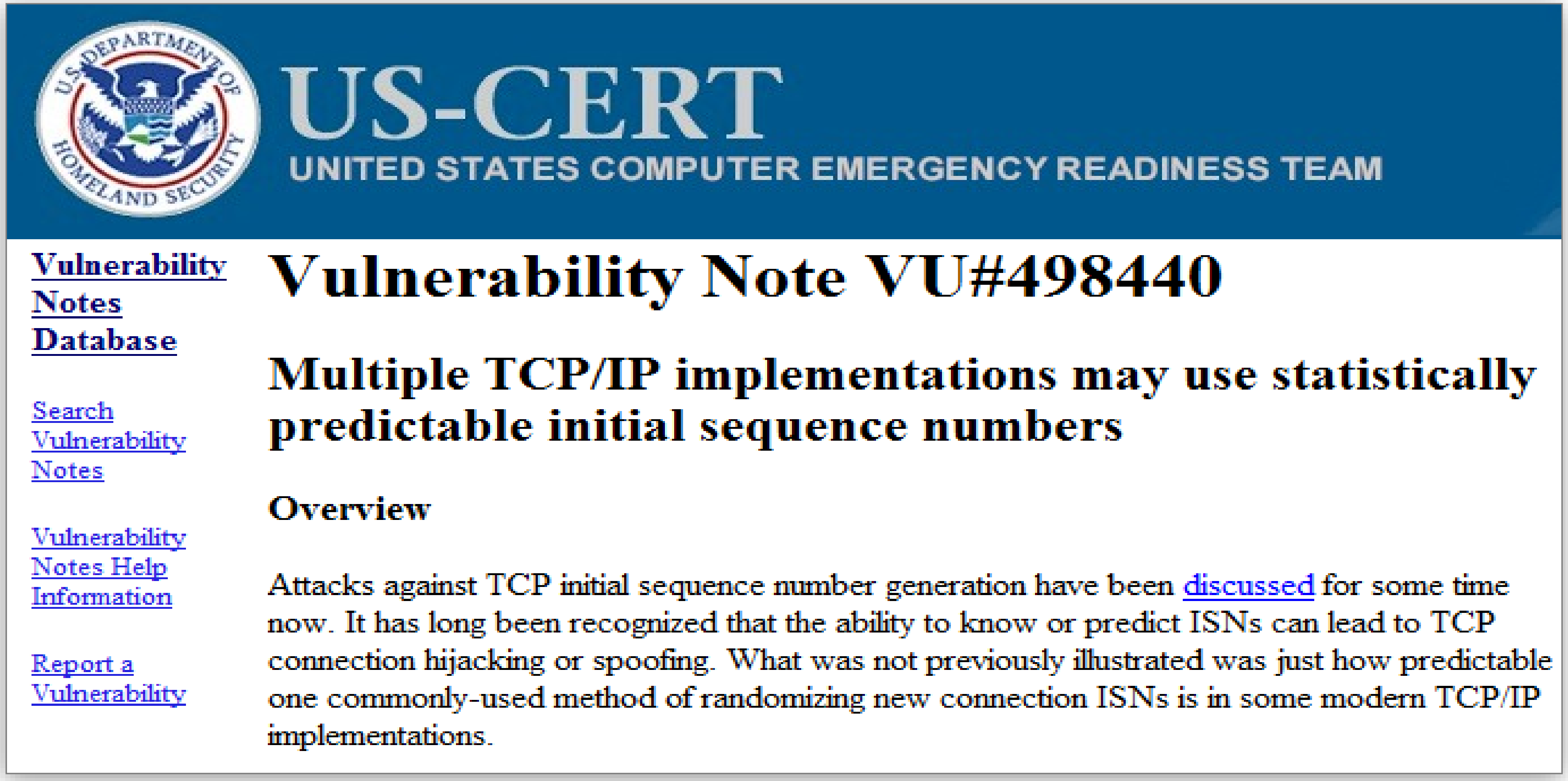
Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

End

2001



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

Report a Vulnerability

Vulnerability Note VU#498440

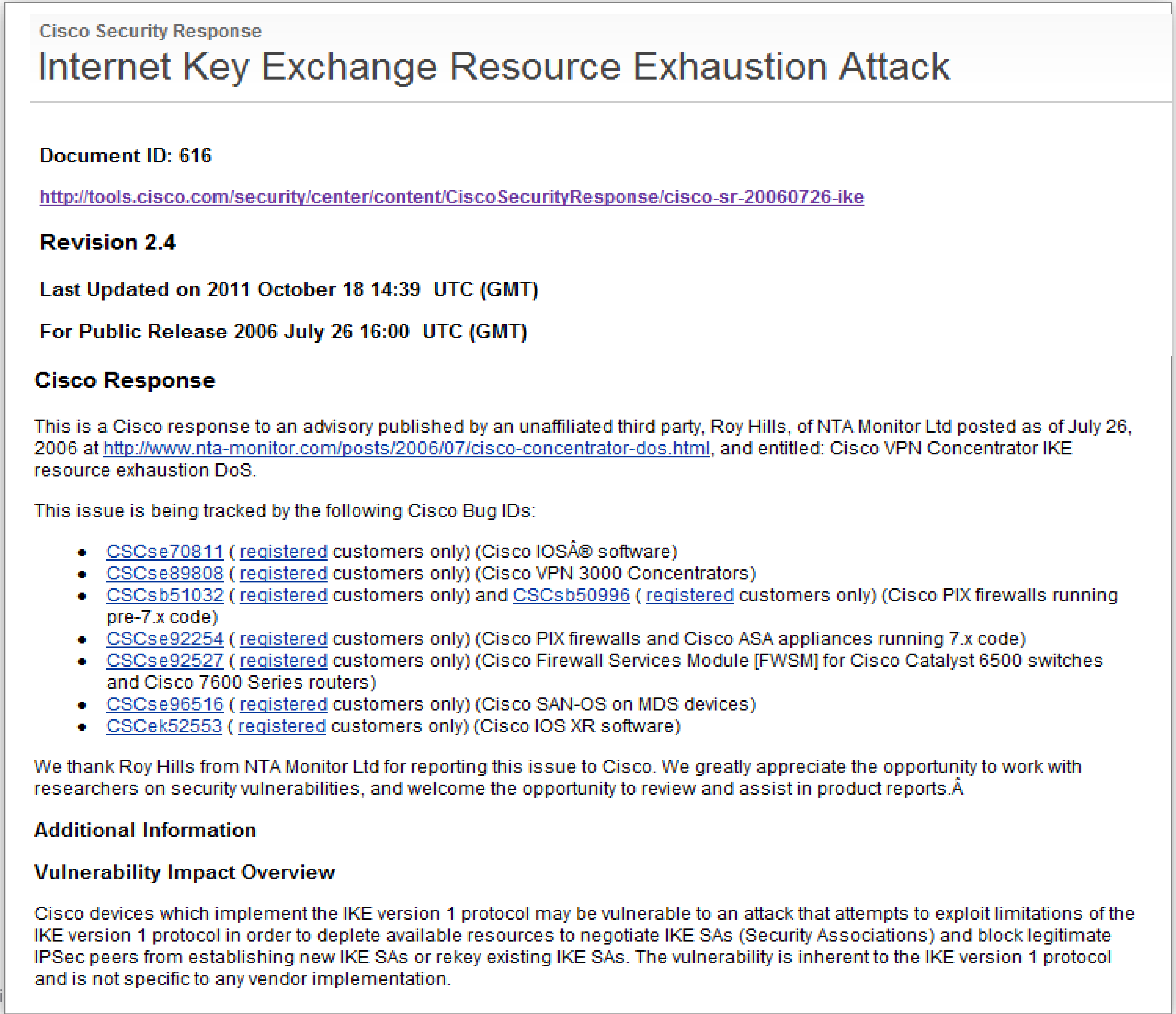
Multiple TCP/IP implementations may use statistically predictable initial sequence numbers

Overview

Attacks against TCP initial sequence number generation have been discussed for some time now. It has long been recognized that the ability to know or predict ISNs can lead to TCP connection hijacking or spoofing. What was not previously illustrated was just how predictable one commonly-used method of randomizing new connection ISNs is in some modern TCP/IP implementations.

Source: http://www.kb.cert.org/vuls/id/498440

2006



Cisco Security Response

Internet Key Exchange Resource Exhaustion Attack

Document ID: 616

http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20060726-ike

Revision 2.4

Last Updated on 2011 October 18 14:39 UTC (GMT)

For Public Release 2006 July 26 16:00 UTC (GMT)

Cisco Response

This is a Cisco response to an advisory published by an unaffiliated third party, Roy Hills, of NTA Monitor Ltd posted as of July 26, 2006 at http://www.nta-monitor.com/posts/2006/07/cisco-concentrator-dos.html, and entitled: Cisco VPN Concentrator IKE resource exhaustion DoS.

This issue is being tracked by the following Cisco Bug IDs:

- CSCse70811 (registered customers only) (Cisco IOSÂ® software)
- CSCse89808 (registered customers only) (Cisco VPN 3000 Concentrators)
- CSCsb51032 (registered customers only) and CSCsb50996 (registered customers only) (Cisco PIX firewalls running pre-7.x code)
- CSCse92254 (registered customers only) (Cisco PIX firewalls and Cisco ASA appliances running 7.x code)
- CSCse92527 (registered customers only) (Cisco Firewall Services Module [FWSM] for Cisco Catalyst 6500 switches and Cisco 7600 Series routers)
- CSCse96516 (registered customers only) (Cisco SAN-OS on MDS devices)
- CSCek52553 (registered customers only) (Cisco IOS XR software)

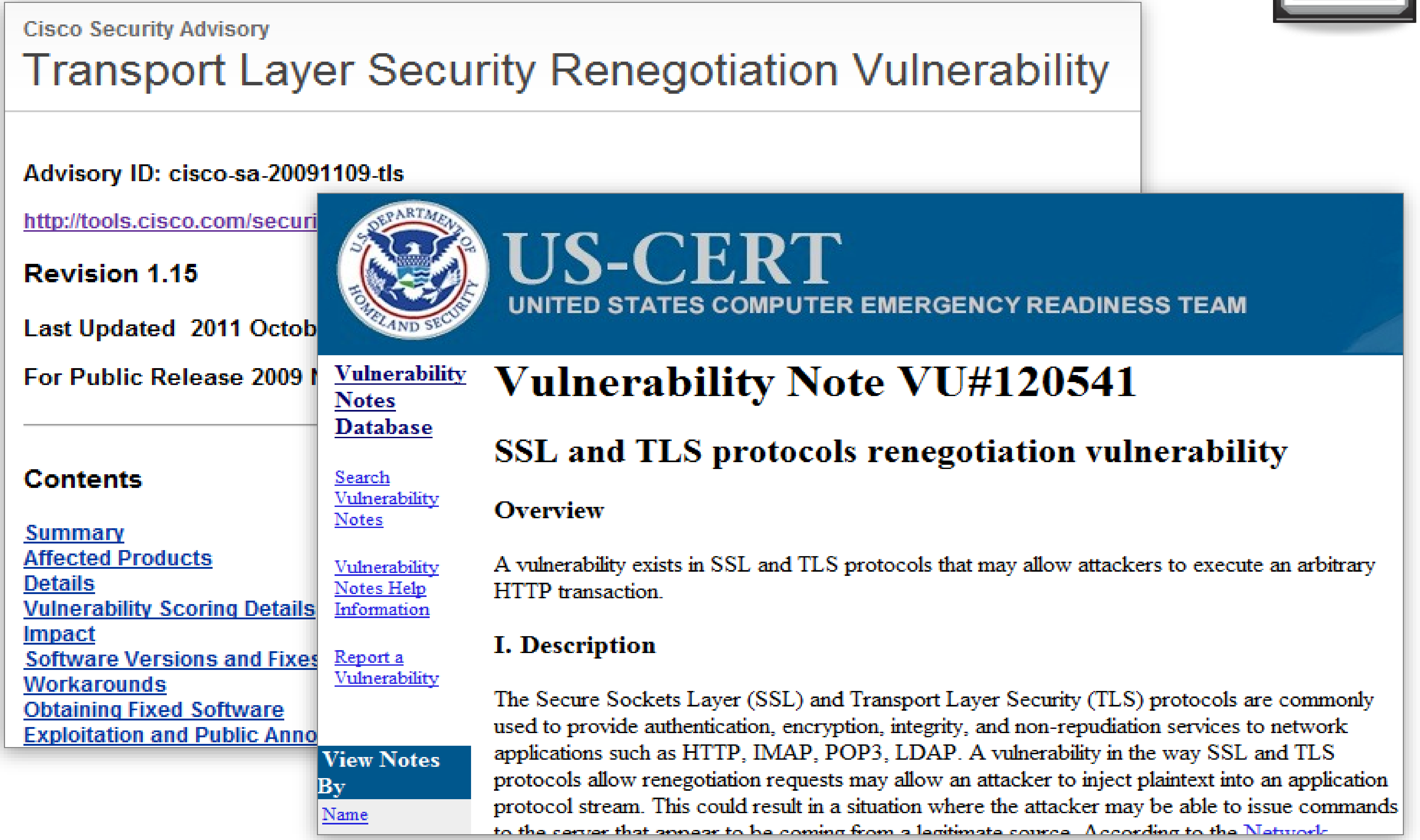
We thank Roy Hills from NTA Monitor Ltd for reporting this issue to Cisco. We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.Â

Additional Information

Vulnerability Impact Overview

Cisco devices which implement the IKE version 1 protocol may be vulnerable to an attack that attempts to exploit limitations of the IKE version 1 protocol in order to deplete available resources to negotiate IKE SAs (Security Associations) and block legitimate IPSec peers from establishing new IKE SAs or rekey existing IKE SAs. The vulnerability is inherent to the IKE version 1 protocol and is not specific to any vendor implementation.

2009



Cisco Security Advisory

Transport Layer Security Renegotiation Vulnerability

Advisory ID: cisco-sa-20091109-tls

http://tools.cisco.com/securi

Revision 1.15

Last Updated 2011 Octob

For Public Release 2009 N

Contents

Summary
Affected Products
Details
Vulnerability Scoring Details
Impact
Software Versions and Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Anno

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

Report a Vulnerability

View Notes By

Name

Vulnerability Note VU#120541

SSL and TLS protocols renegotiation vulnerability

Overview

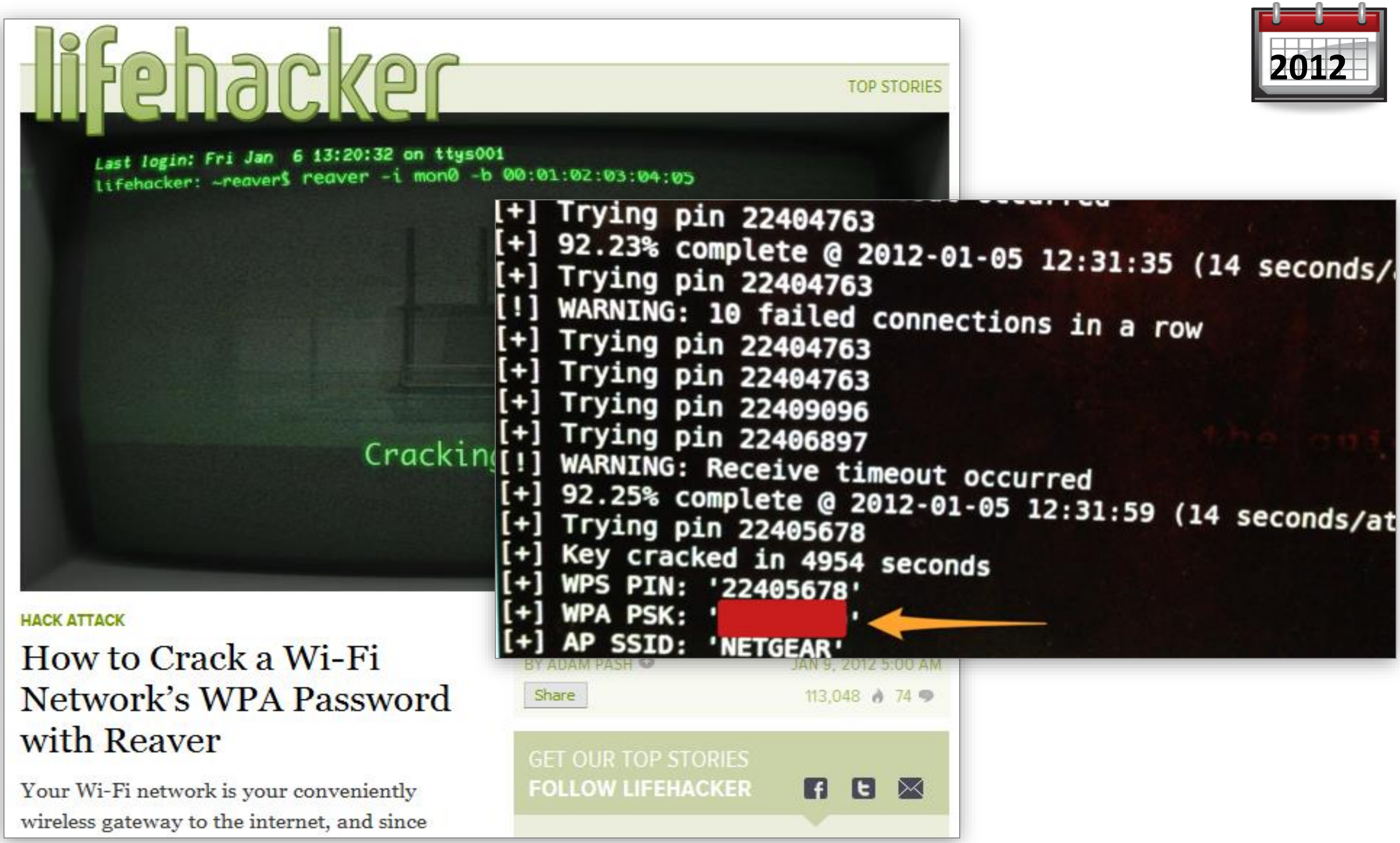
A vulnerability exists in SSL and TLS protocols that may allow attackers to execute an arbitrary HTTP transaction.

I. Description

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to provide authentication, encryption, integrity, and non-repudiation services to network applications such as HTTP, IMAP, POP3, LDAP. A vulnerability in the way SSL and TLS protocols allow renegotiation requests may allow an attacker to inject plaintext into an application protocol stream. This could result in a situation where the attacker may be able to issue commands to the server that appear to be coming from a legitimate source. According to the Network

Source: http://www.kb.cert.org/vuls/id/120541

2012



```
Last login: Fri Jan  6 13:20:32 on ttys001
lifehacker: ~reaver$ reaver -i mon0 -b 00:01:02:03:04:05
```

```
[+] Trying pin 22404763
[+] 92.23% complete @ 2012-01-05 12:31:35 (14 seconds/
[+] Trying pin 22404763
[!] WARNING: 10 failed connections in a row
[+] Trying pin 22404763
[+] Trying pin 22404763
[+] Trying pin 22409096
[+] Trying pin 22406897
[!] WARNING: Receive timeout occurred
[+] 92.25% complete @ 2012-01-05 12:31:59 (14 seconds/at
[+] Trying pin 22405678
[+] Key cracked in 4954 seconds
[+] WPS PIN: '22405678'
[+] WPA PSK: '[redacted]'
[+] AP SSID: 'NETGEAR'
```

HACK ATTACK

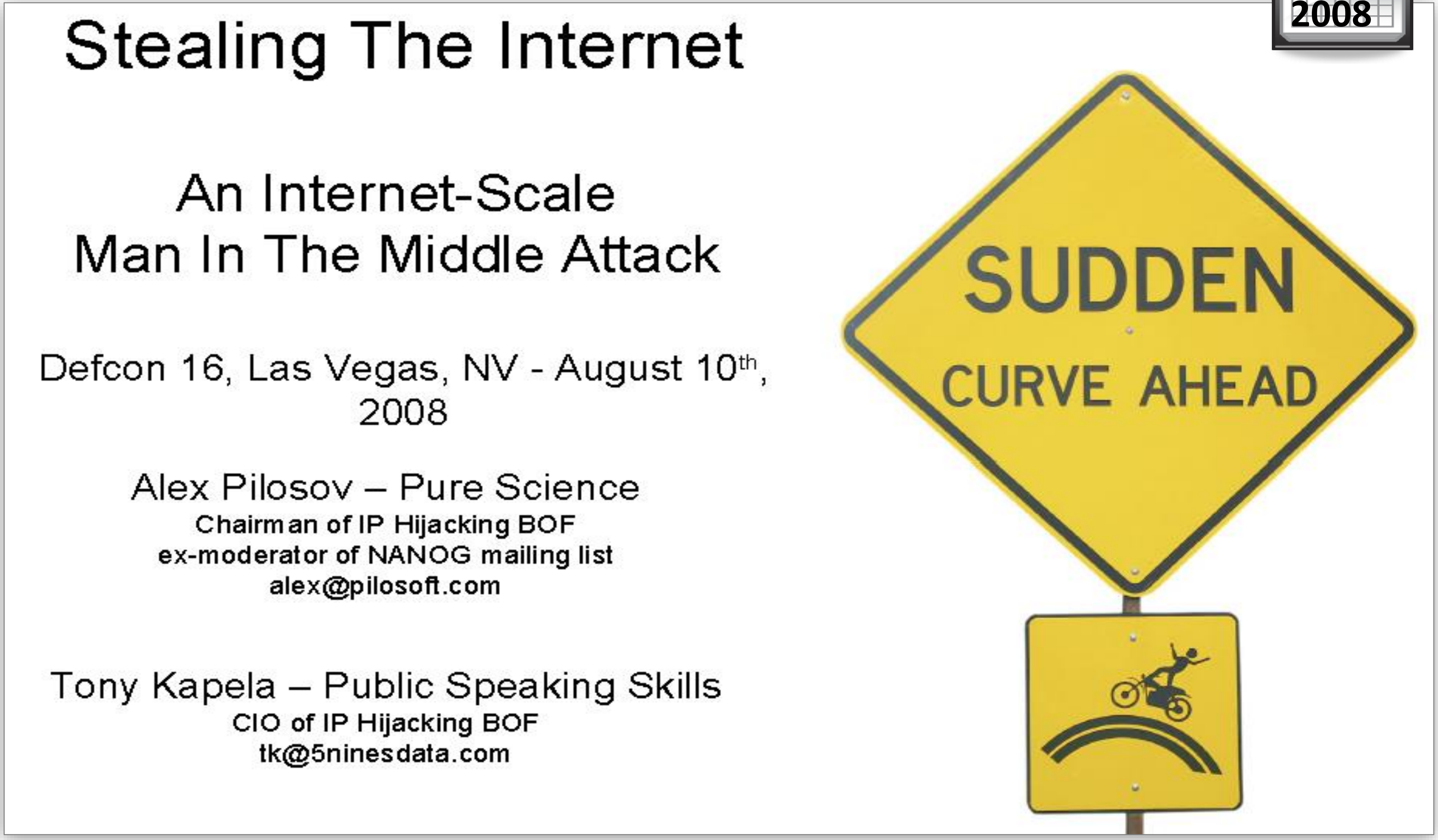
How to Crack a Wi-Fi Network's WPA Password with Reaver

BY ADAM PASH JAN 9, 2012 5:00 AM

Your Wi-Fi network is your conveniently wireless gateway to the internet, and since

Source: http://lifehacker.com/5873407/how-to-crack-a-wi+fi-networks-wpa-password-with-reaver

2008



Stealing The Internet

An Internet-Scale
Man In The Middle Attack

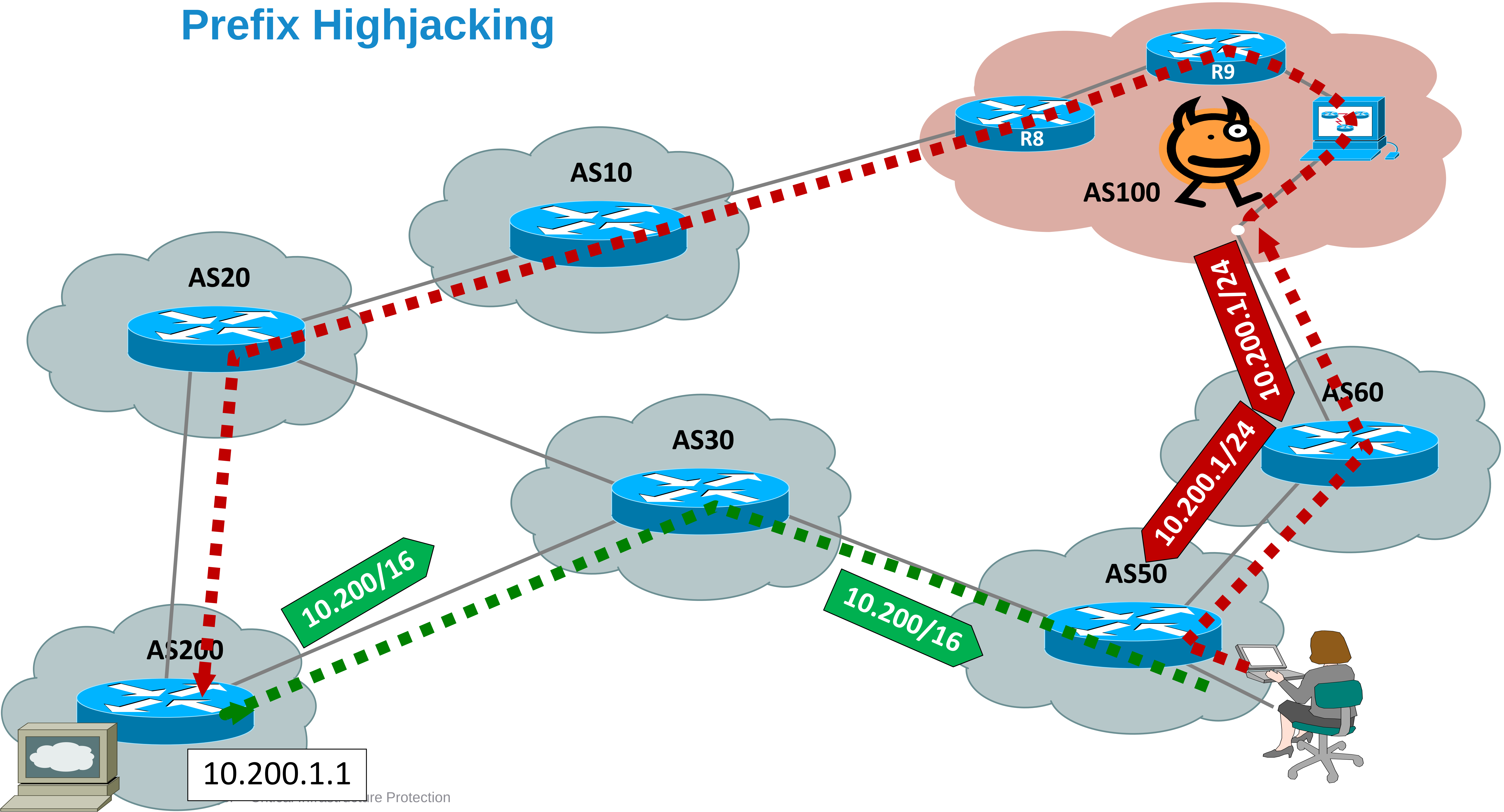
Defcon 16, Las Vegas, NV - August 10th, 2008

Alex Pilosov – Pure Science
Chairman of IP Hijacking BOF
ex-moderator of NANOG mailing list
alex@pilosoft.com

Tony Kapela – Public Speaking Skills
CIO of IP Hijacking BOF
tk@5ninesdata.com

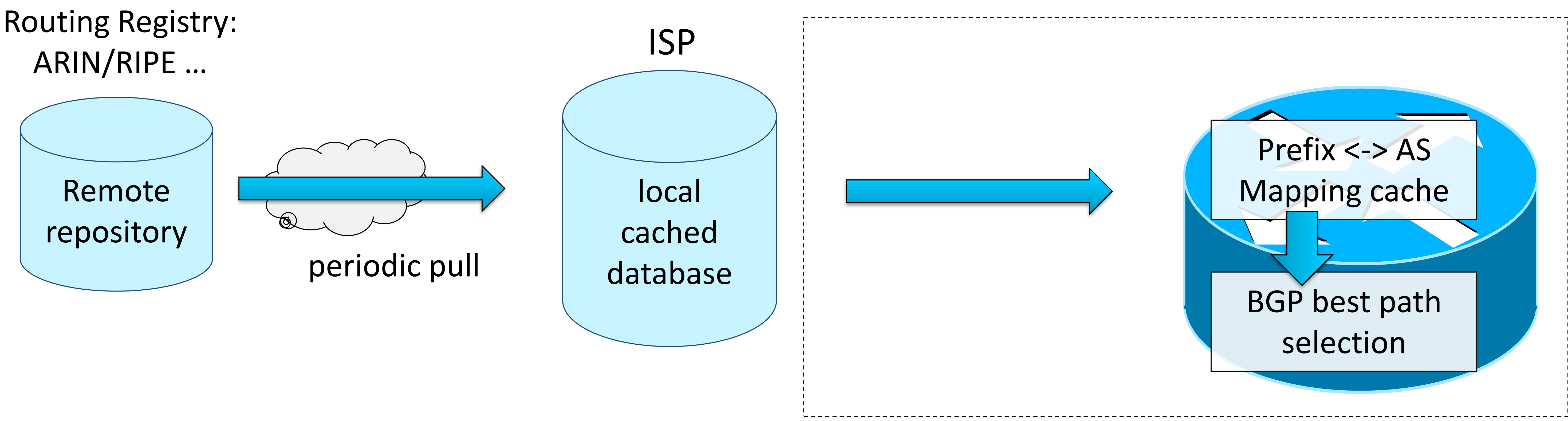
SUDDEN
CURVE AHEAD

Prefix Highjacking



Secure Inter Domain Routing (SIDR)

IOS 12.2(1)S
IOS XE 3.5
IOS XR 4.2.1



Routing Registry:
ARIN/RIPE …

Remote repository

periodic pull

ISP

local cached database

Prefix <-> AS Mapping cache

BGP best path selection

Attestation:
Prefix belongs to AS

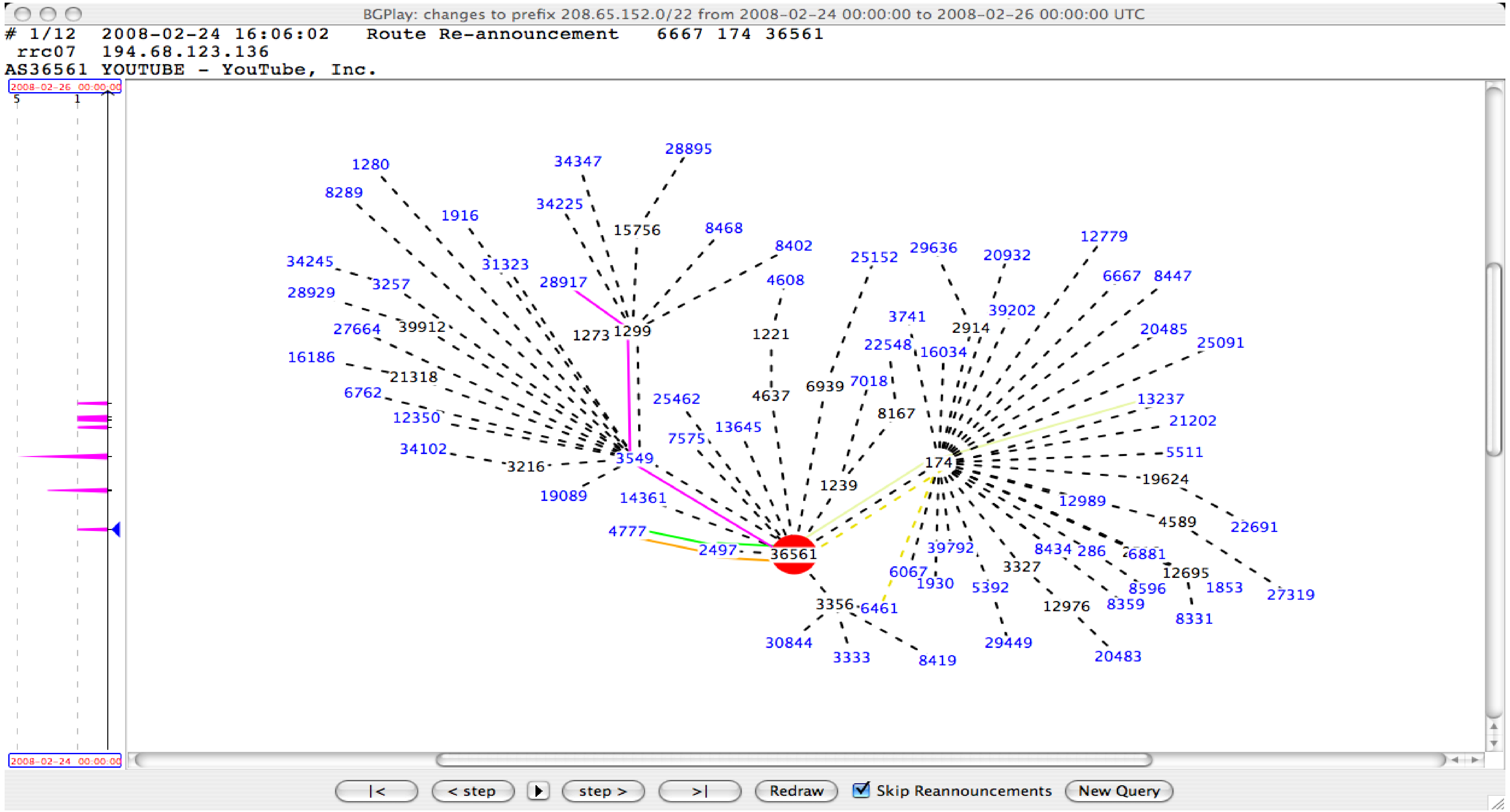
Verification
and caching

Use:
Influence BGP policy

Standardization: IETF SIDR Working Group

No Intrinsic Security in BGP Updates

2008

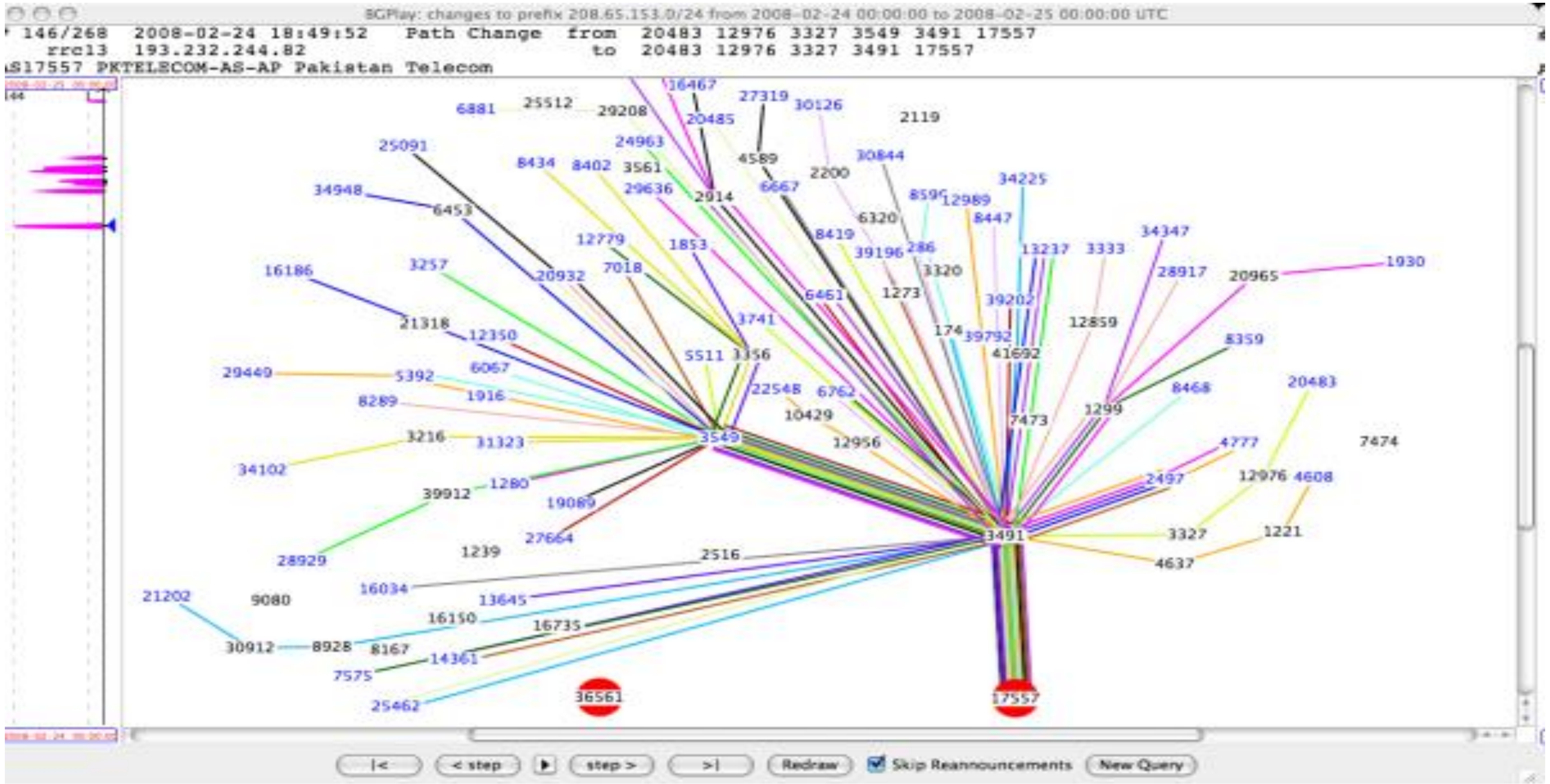


BGPlay: changes to prefix 208.65.152.0/22 from 2008-02-24 00:00:00 to 2008-02-26 00:00:00 UTC

```
# 1/12  2008-02-24 16:06:02   Route Re-announcement   6667 174 36561
 rrc07  194.68.123.136
AS36561 YOUTUBE - YouTube, Inc.
```

No Intrinsic Security in BGP Updates

2008

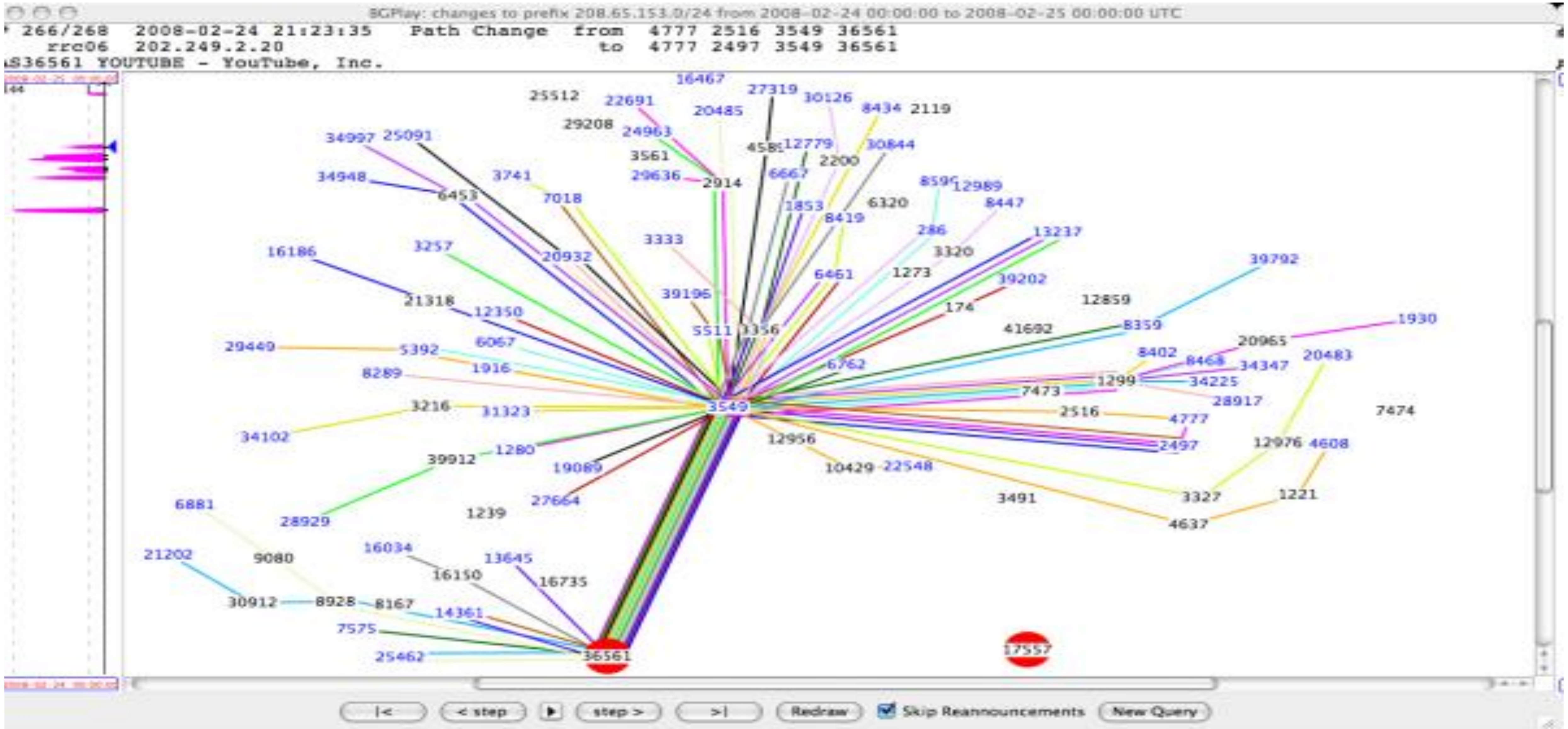


```
BGPlay: changes to prefix 208.65.153.0/24 from 2008-02-24 00:00:00 to 2008-02-25 00:00:00 UTC
 146/268   2008-02-24 18:49:52   Path Change   from  20483 12976 3327 3549 3491 17557
    rrc13  193.232.244.82                        to  20483 12976 3327 3491 17557
AS17557 PKTELECOM-AS-AP Pakistan Telecom
```

24th Feb'08, 18:47 (UTC):
AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. PT's upstream provider AS3491 (PCCW Global) propagates the announcement.
Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.

No Intrinsic Security in BGP Updates

2008



BGPlay: changes to prefix 208.65.153.0/24 from 2008-02-24 00:00:00 to 2008-02-25 00:00:00 UTC

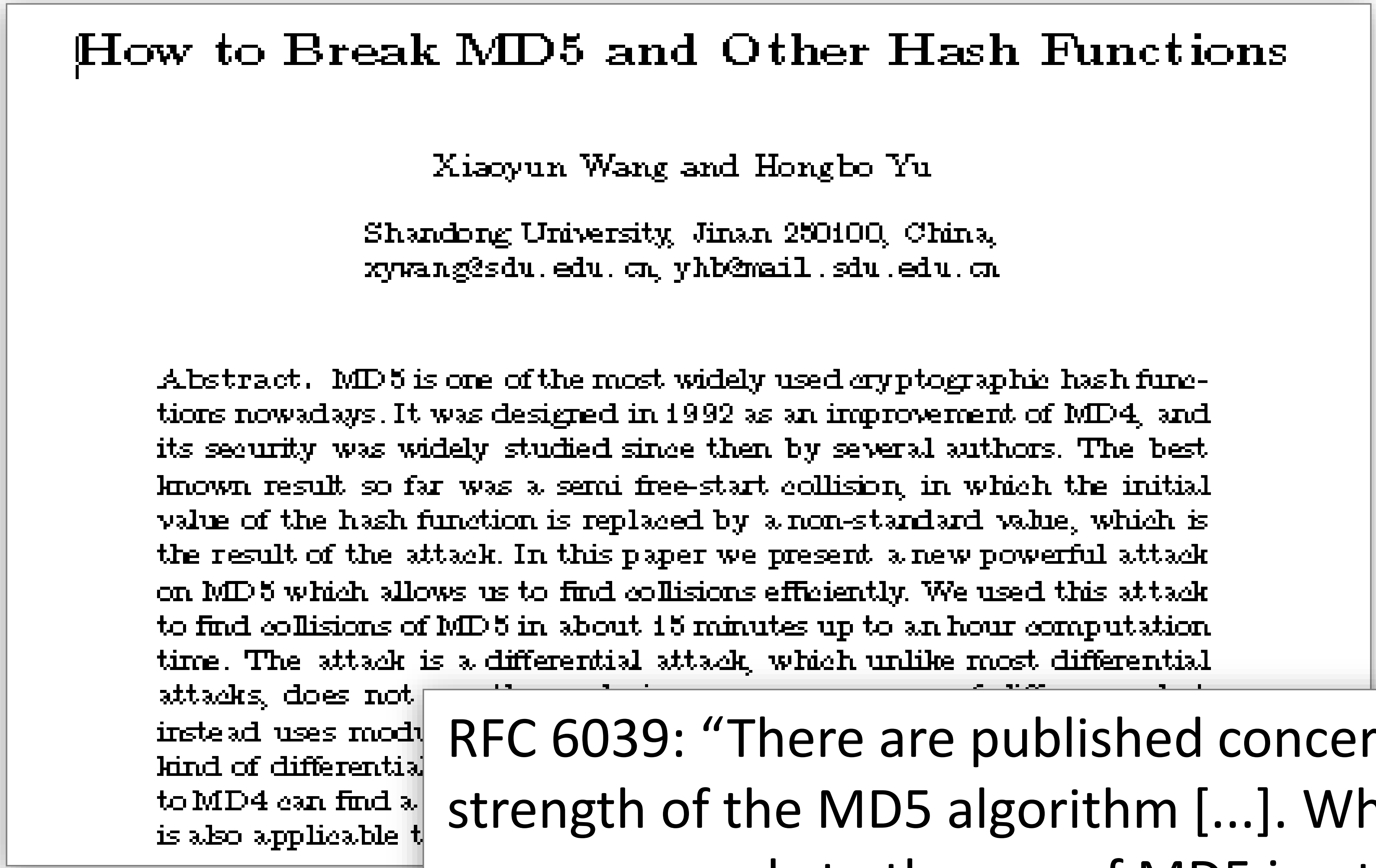
```
 266/268   2008-02-24 21:23:35   Path Change  from  4777 2516 3549 36561
   rrc06   202.249.2.20                         to  4777 2497 3549 36561
S36561 YOUTUBE - YouTube, Inc.
```

24TH Feb’08, 21:23 (UTC):

AS36561 has been announcing **208.65.153.0/24** since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to AS3656

Source: http://www.ripe.net/news/study-youtube-hijacking.html

2005



How to Break MD5 and Other Hash Functions

Xiaoyun Wang and Hongbo Yu

Shandong University, Jinan 250100, China,
xywang@sdu.edu.cn, yhb@mail.sdu.edu.cn

Abstract. MD5 is one of the most widely used cryptographic hash functions nowadays. It was designed in 1992 as an improvement of MD4, and its security was widely studied since then by several authors. The best known result so far was a semi free-start collision, in which the initial value of the hash function is replaced by a non-standard value, which is the result of the attack. In this paper we present a new powerful attack on MD5 which allows us to find collisions efficiently. We used this attack to find collisions of MD5 in about 15 minutes up to an hour computation time. The attack is a differential attack, which unlike most differential attacks, does not
instead uses modu
kind of differentia
to MD4 can find a
is also applicable t

RFC 6039: "There are published concerns about the overall strength of the MD5 algorithm [...]. While those published concerns apply to the use of MD5 in other modes (e.g., use of MD5 X.509v3/PKIX digital certificates), **they are not an attack upon Keyed MD5 and Hash-based Message Authentication Code MD5 (HMAC-MD5),** which is what the current routing protocols have specified."

Your Protocols Are Secure?

Source: http://www.flickr.com/photos/dseneste/5912382808/

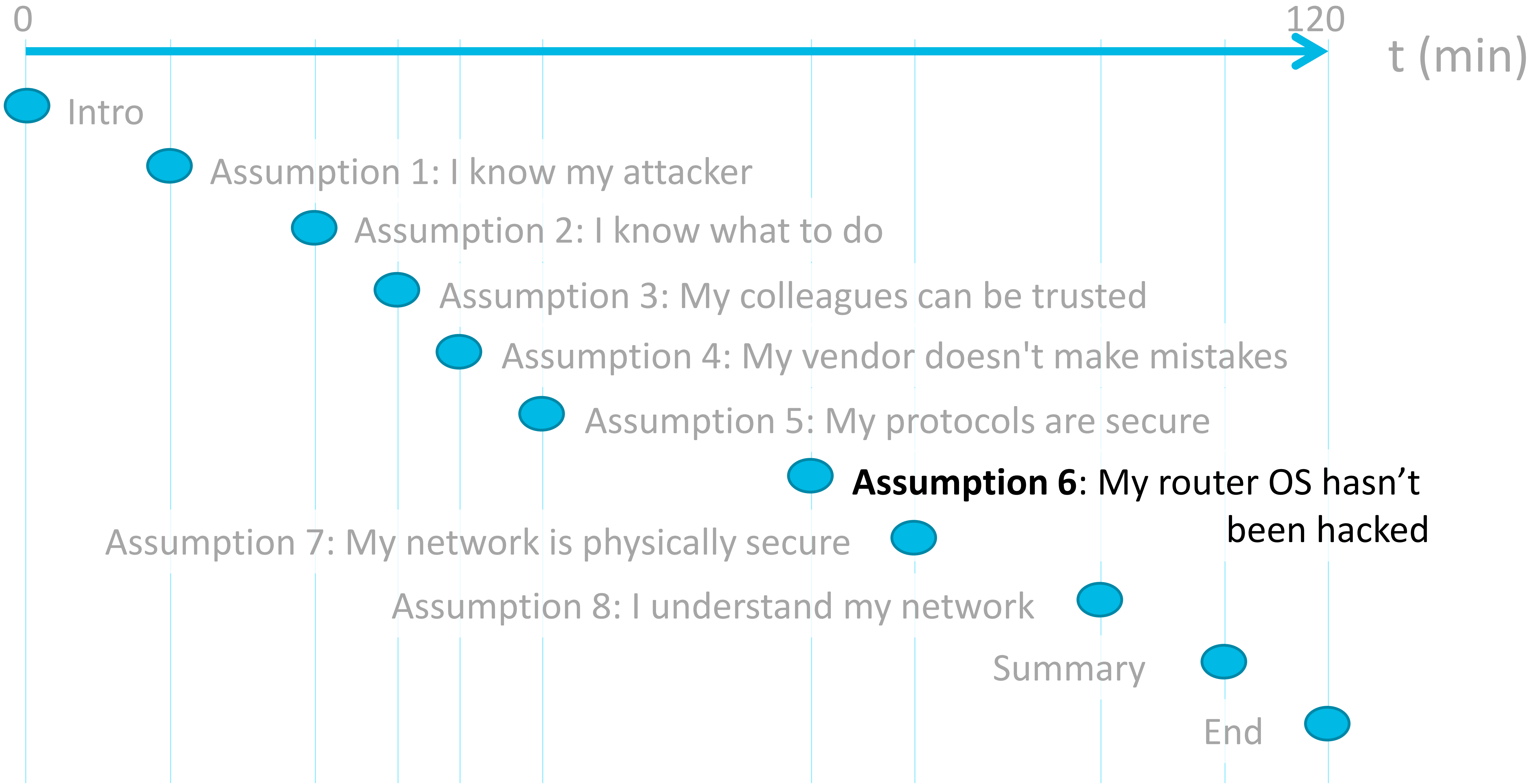
- Protocols can have vulnerabilities
- Typically cross-vendor

THEREFORE

- Use Defence in Depth

  Ex: Make network devices unreachable (iACL)
- Use up to date protocols
- Understand vendor’s vulnerability management process
- Have an upgrade policy
- For intrinsic risks, monitor and respond (eg BGP prefix hijack)

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

Assumption 7: My network is physically secure

Assumption 8: I understand my network

Summary

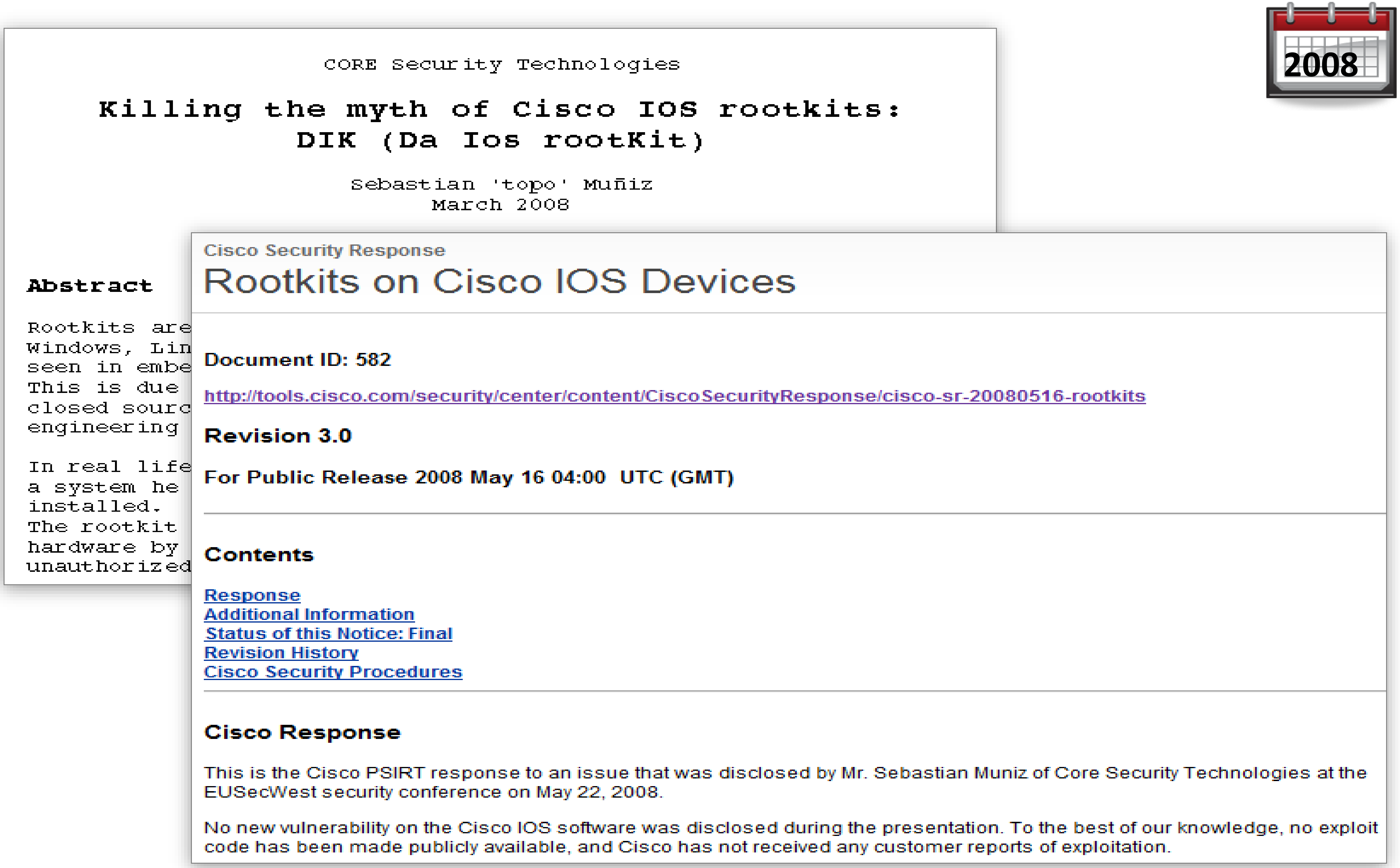
End

Detecting OS Modifications

- New IOS requires reload
  - Syslog message
  - Line down/up, routing adjacency down/up, etc: Indicating a reload → Should check OS consistency
- Two abuse cases:

  1. Different, but “clean” IOS version (original OS)
     - Detect with “show version”
  2. “Hacked” IOS version
     - Cannot check OS integrity! (“show” commands could be modified, too)
     - → Not necessarily detectable!
- IOS XR: Modules do *not* require reload
  - But: Are cryptographically signed, thus not possible to modify.
  - Module re-start: Syslog

2008



CORE Security Technologies

Killing the myth of Cisco IOS rootkits: DIK (Da Ios rootKit)

Sebastian 'topo' Muñiz
March 2008

Abstract

Rootkits are
Windows, Lin
seen in embe
This is due
closed sourc
engineering

In real life
a system he
installed.
The rootkit
hardware by
unauthorized

Cisco Security Response

Rootkits on Cisco IOS Devices

Document ID: 582

http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20080516-rootkits

Revision 3.0

For Public Release 2008 May 16 04:00 UTC (GMT)

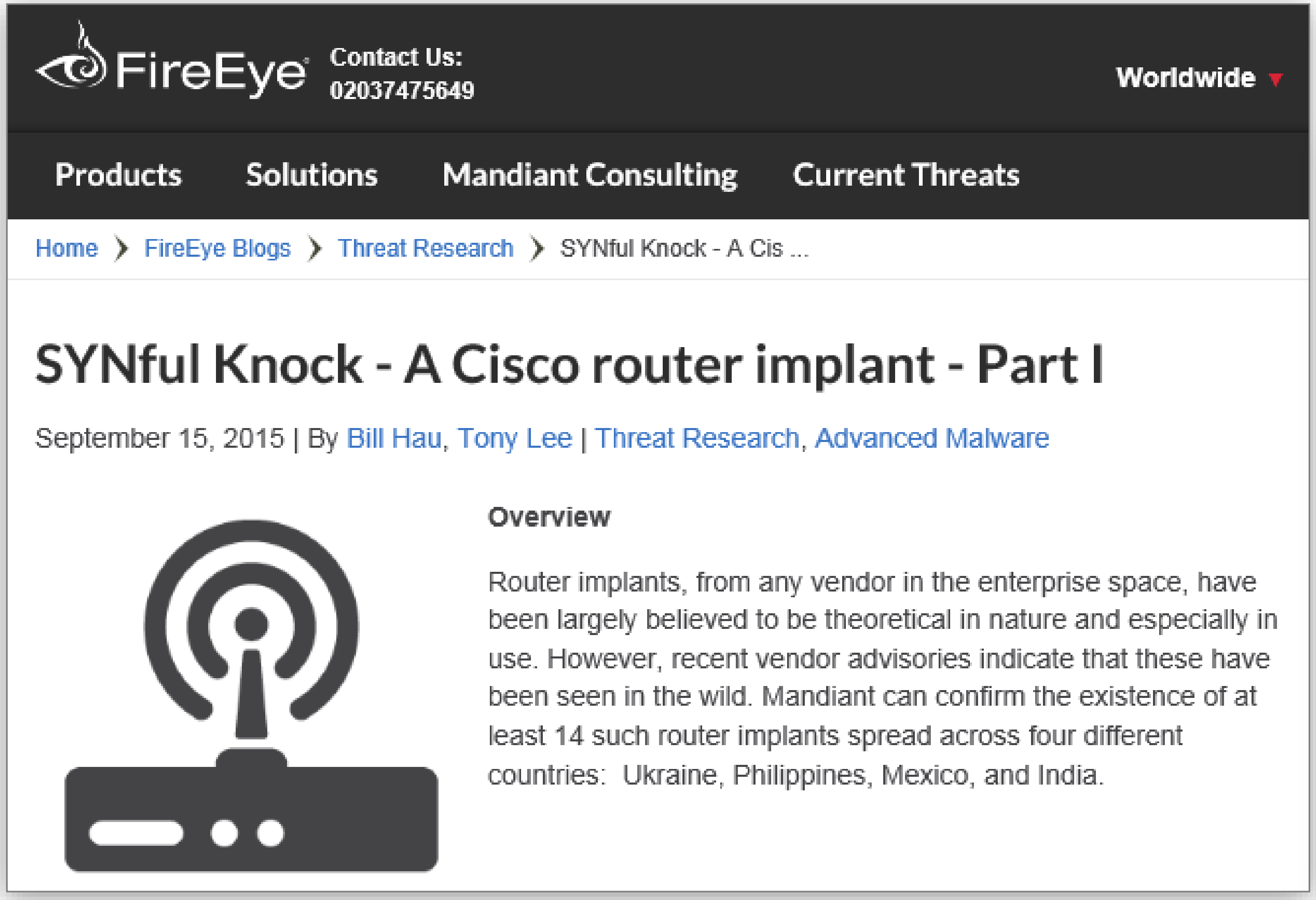
Contents

Cisco Response

This is the Cisco PSIRT response to an issue that was disclosed by Mr. Sebastian Muniz of Core Security Technologies at the EUSecWest security conference on May 22, 2008.

No new vulnerability on the Cisco IOS software was disclosed during the presentation. To the best of our knowledge, no exploit code has been made publicly available, and Cisco has not received any customer reports of exploitation.

2015



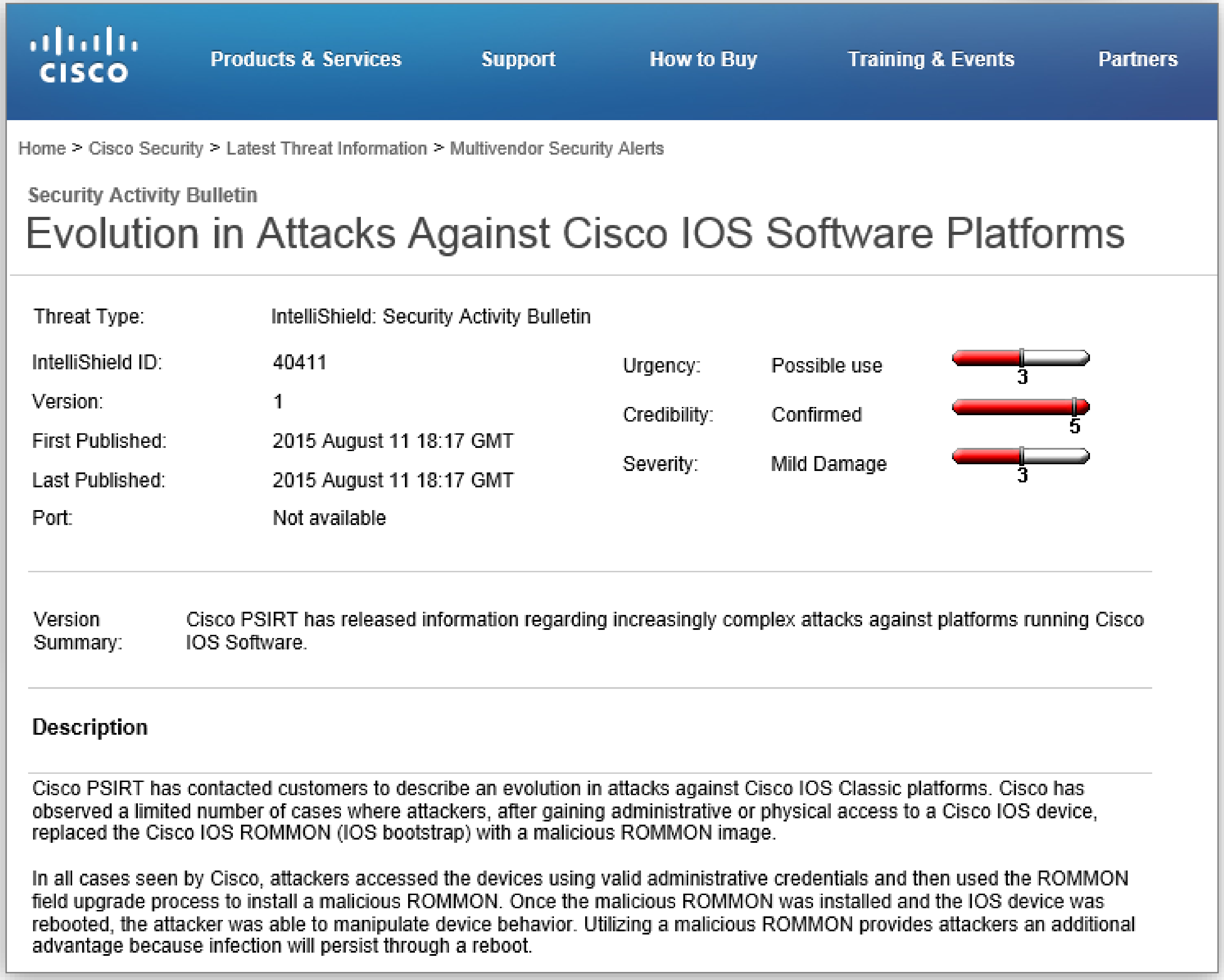
SYNful Knock - A Cisco router implant - Part I

September 15, 2015 | By Bill Hau, Tony Lee | Threat Research, Advanced Malware

Overview

Router implants, from any vendor in the enterprise space, have been largely believed to be theoretical in nature and especially in use. However, recent vendor advisories indicate that these have been seen in the wild. Mandiant can confirm the existence of at least 14 such router implants spread across four different countries: Ukraine, Philippines, Mexico, and India.

https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html


cisco
Products & Services
Support
How to Buy
Training & Events
Partners
Home > Cisco Security > Latest Threat Information > Multivendor Security Alerts

Security Activity Bulletin

Evolution in Attacks Against Cisco IOS Software Platforms

Threat Type:	IntelliShield: Security Activity Bulletin			
IntelliShield ID:	40411	Urgency:	Possible use	3
Version:	1	Credibility:	Confirmed	5
First Published:	2015 August 11 18:17 GMT	Severity:	Mild Damage	3
Last Published:	2015 August 11 18:17 GMT			
Port:	Not available			

Version Summary: Cisco PSIRT has released information regarding increasingly complex attacks against platforms running Cisco IOS Software.

Description

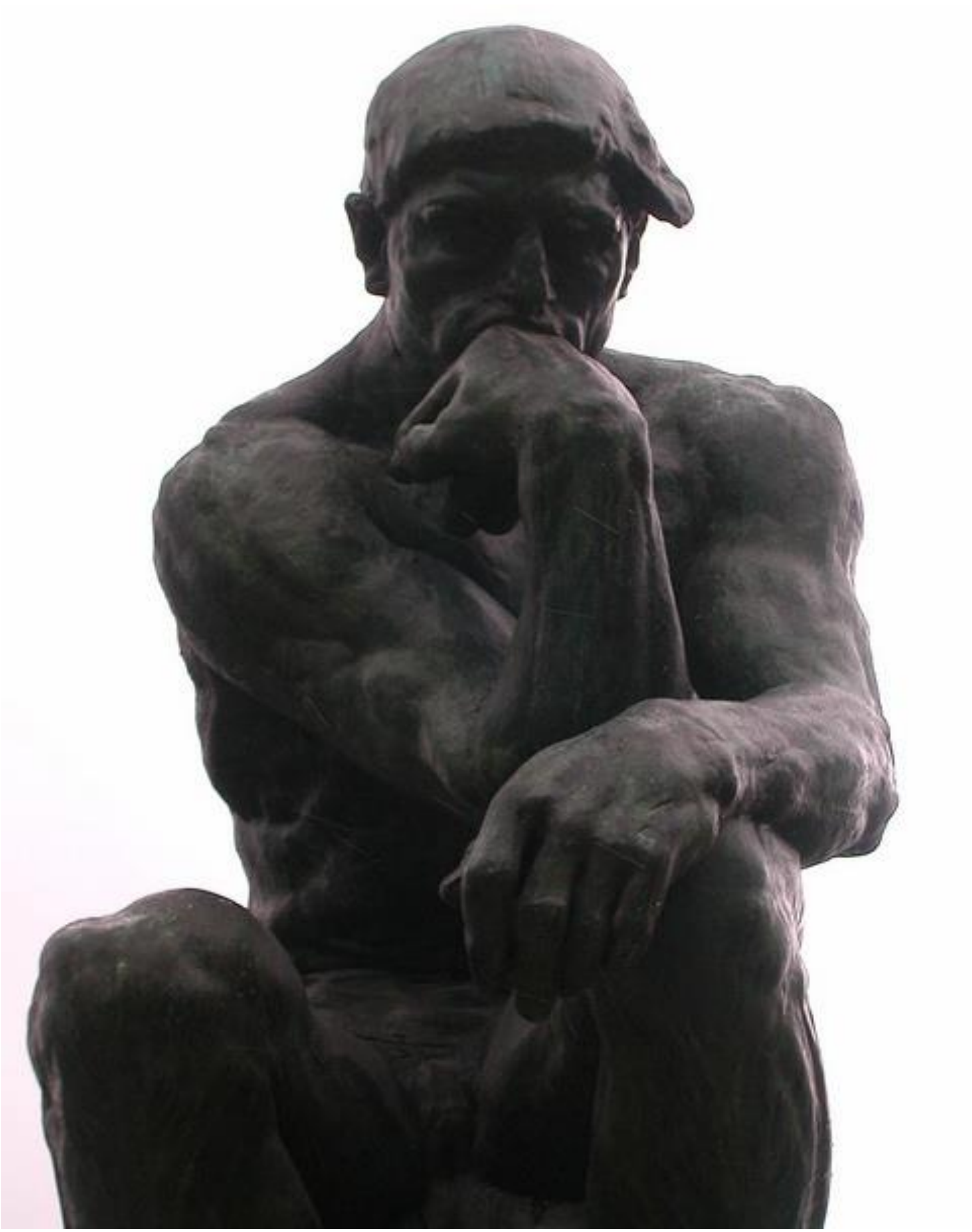
Cisco PSIRT has contacted customers to describe an evolution in attacks against Cisco IOS Classic platforms. Cisco has observed a limited number of cases where attackers, after gaining administrative or physical access to a Cisco IOS device, replaced the Cisco IOS ROMMON (IOS bootstrap) with a malicious ROMMON image.

In all cases seen by Cisco, attackers accessed the devices using valid administrative credentials and then used the ROMMON field upgrade process to install a malicious ROMMON. Once the malicious ROMMON was installed and the IOS device was rebooted, the attacker was able to manipulate device behavior. Utilizing a malicious ROMMON provides attackers an additional advantage because infection will persist through a reboot.

http://tools.cisco.com/security/center/viewAlert.x?alertId=40411

Snort Signature: https://www.snort.org/advisories/talos-rules-2015-09-15

Your Router OS Hasn't Been Hacked?



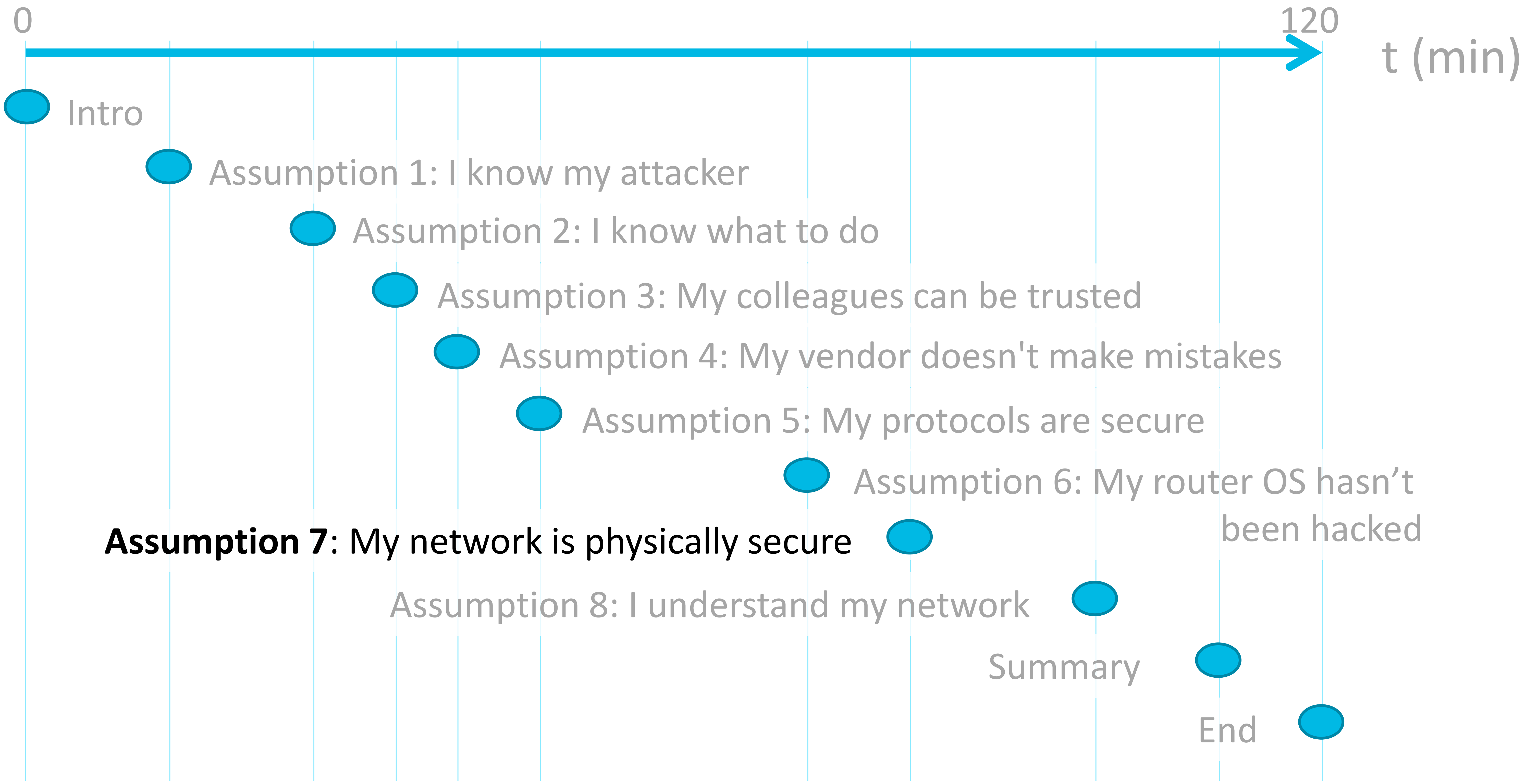
Source: http://www.flickr.com/photos/dseneste/5912382808/

- Hard to prove correctness of OS
- Rootkits exist

THEREFORE

- Optimise physical security
- Monitor for device changes (reload)
- Check correctness of OS (as good as possible)
- Have procedures to re-gain control of a modified device
- Have procedures to isolate a suspicious device

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

Assumption 7: My network is physically secure

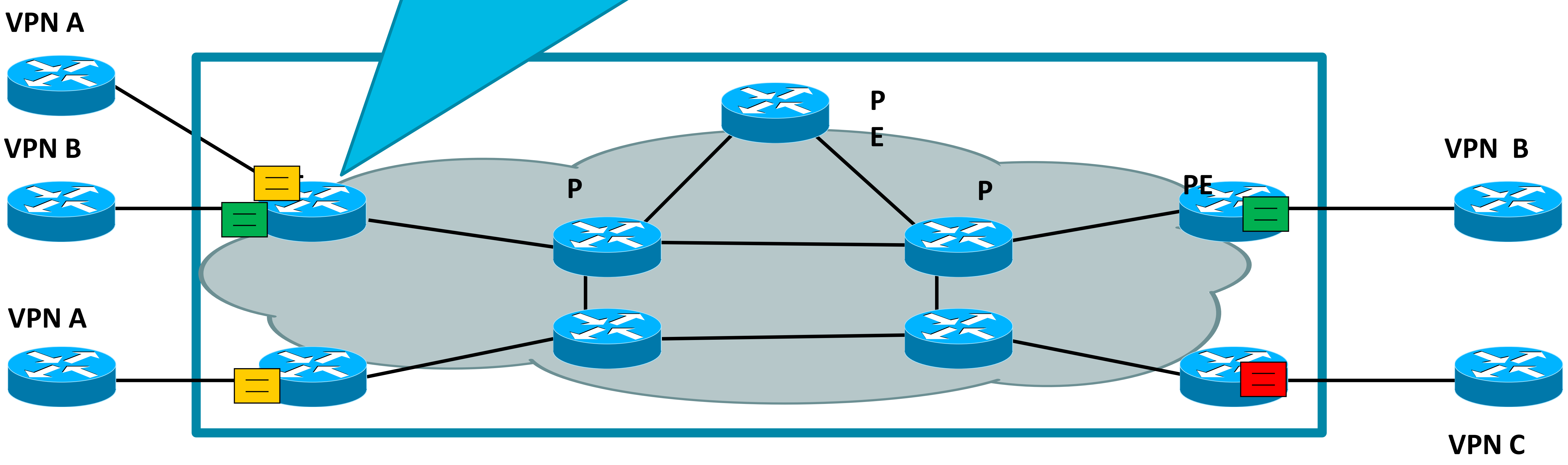
Assumption 8: I understand my network

Summary

End

PE Security: A Quiz

Assume a hacker has enable access on this PE.
What can he access?



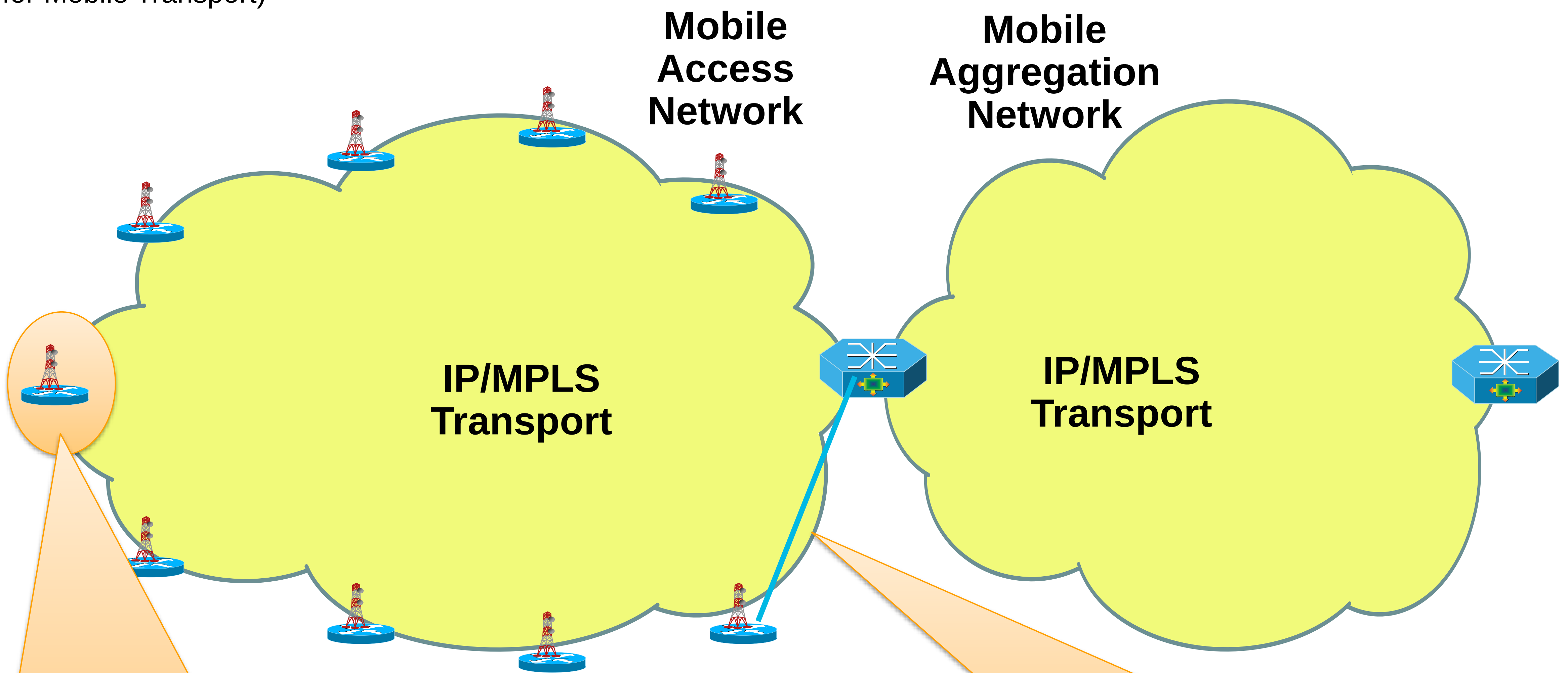
A: All locally connected sites of VPN A and B

B: All sites of VPN A and B

C: All sites of all VPNs

UMMT Mobile Access Network

(Unified MPLS for Mobile Transport)



What if one PE is physically compromised?

- **Password recovery → Anything possible**
- **Can join any VPN in that zone. Oops.**

What if link is physically compromised?

- **Sniff, modify, insert, drop:**
  Control, data and management plane traffic
- **With MACsec, no compromise!**

Operational Security

- Can detect takeover of device
  - MUST detect login of authorised admin
  - MUST detect brute force SSH attacks
  - MUST detect password recovery
  - MUST detect device replacement (UDI)
  - MUST check device integrity regularily (os, config, file system)

AAA server

syslog server

script

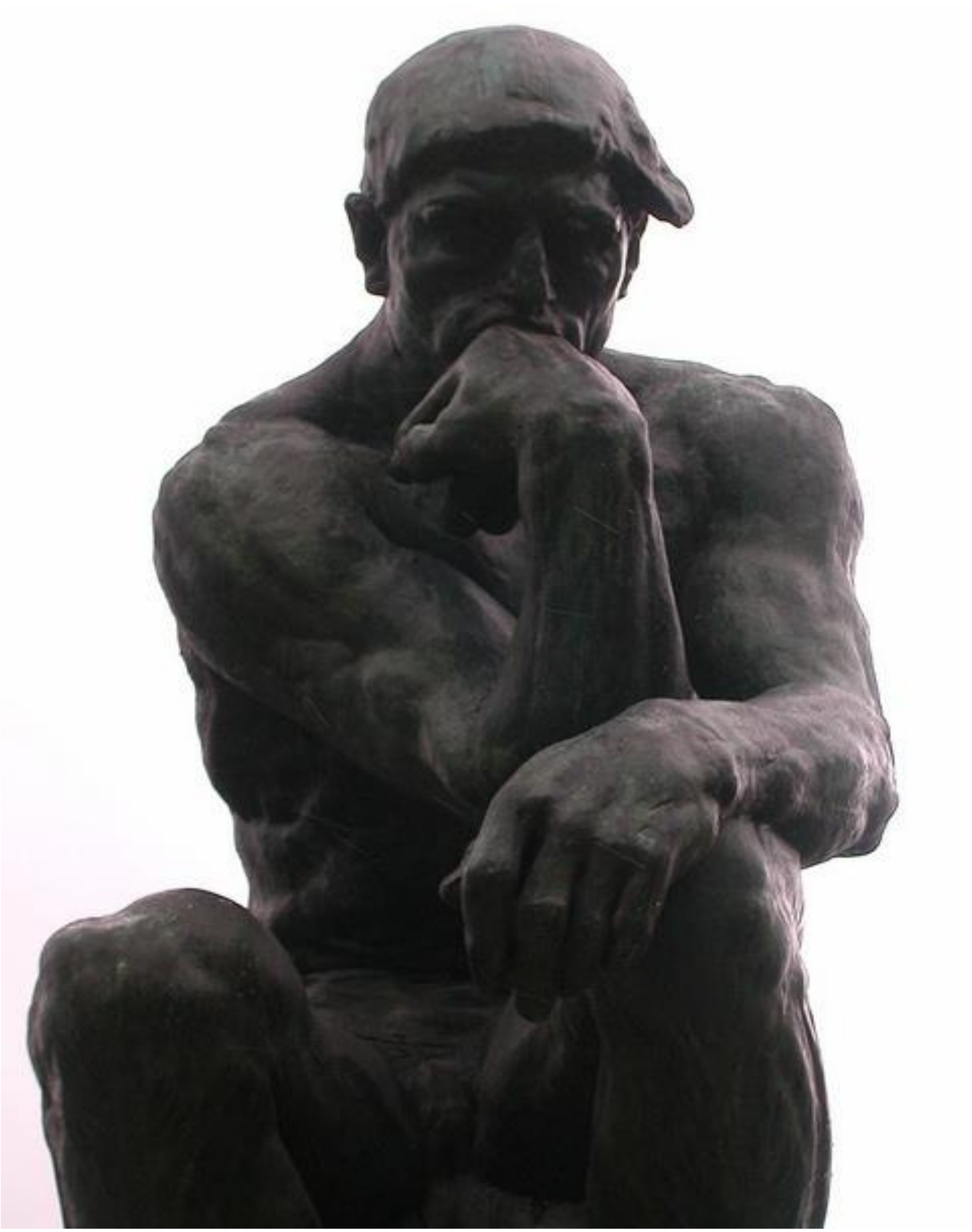
- Cannot detect wiretap
  - MUST protect all control plane protocols (BGP, IGP, LDP)
  - MUST protect all management plane protocols (SSH, SNMP, ...)

→Only data plane attacks are possible

Operational Procedures

- After each reboot, link-down event, etc:
  - Device could have been replaced
  - Password recovery could have been done
  - → Check system: Unique Device Identifier (UDI), OS, configuration, enable p/w
- After unexpected login from admin:
  - Change password for that admin
  - → Check system: OS, configuration, enable p/w
- Regularly: (ex: once in 24h)
  - → Check system: OS, configuration, enable p/w
  - (You could have missed an event)

Your Network is Physically Secure?



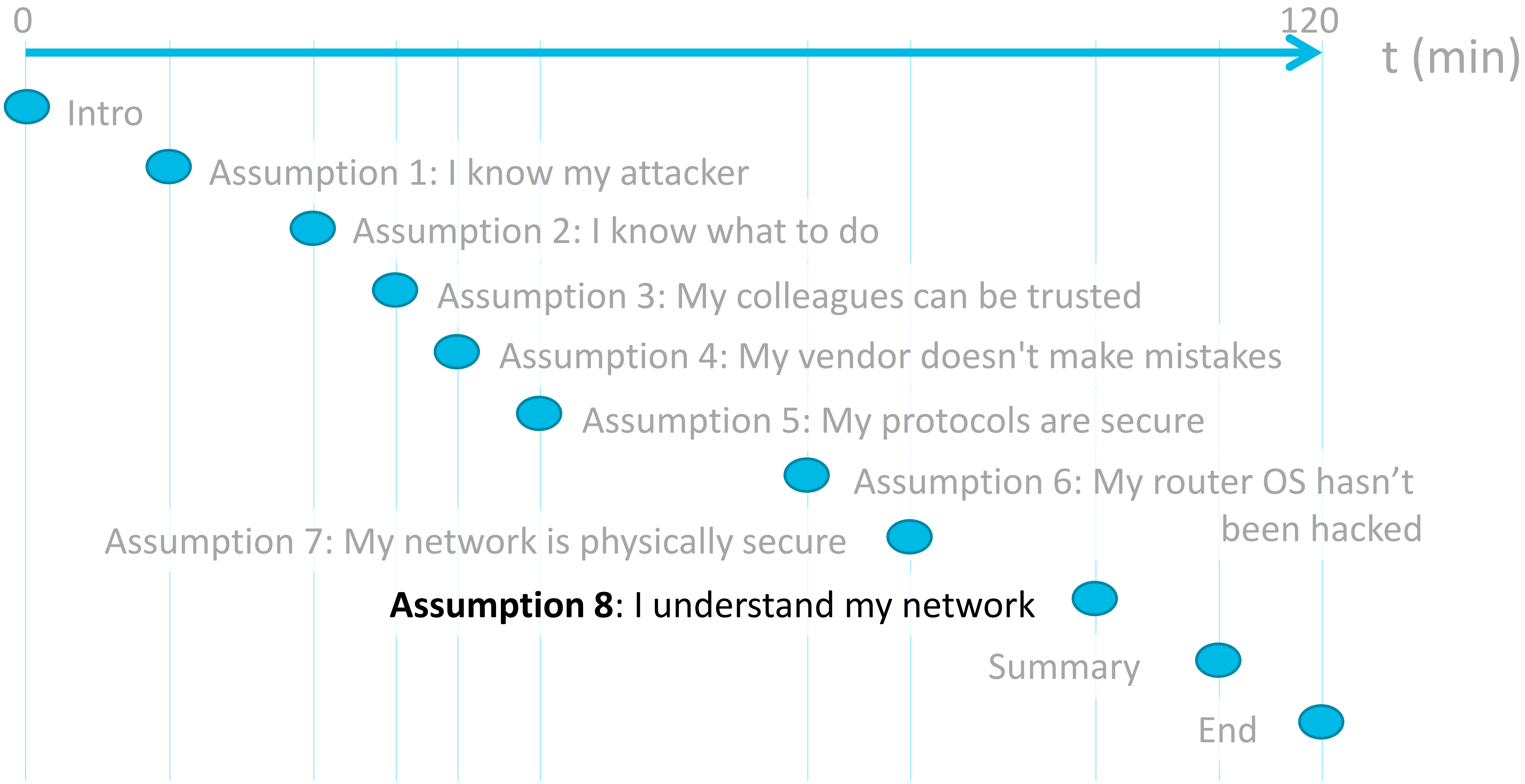
Source: http://www.flickr.com/photos/dseneste/5912382808/

- Cannot guarantee physical security
- Password recovery, device replacement, sniffing, wiretaps, man-in-the-middle are threats

THEREFORE

- Secure management + control plane
- Secure data plane (IPsec)
- Monitor for device changes (reload)
- Check UDI (sh license udi)
- Check correctness of config
- Have procedures to re-gain control of a physically intruded device
- Have procedures to isolate an intruded device

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

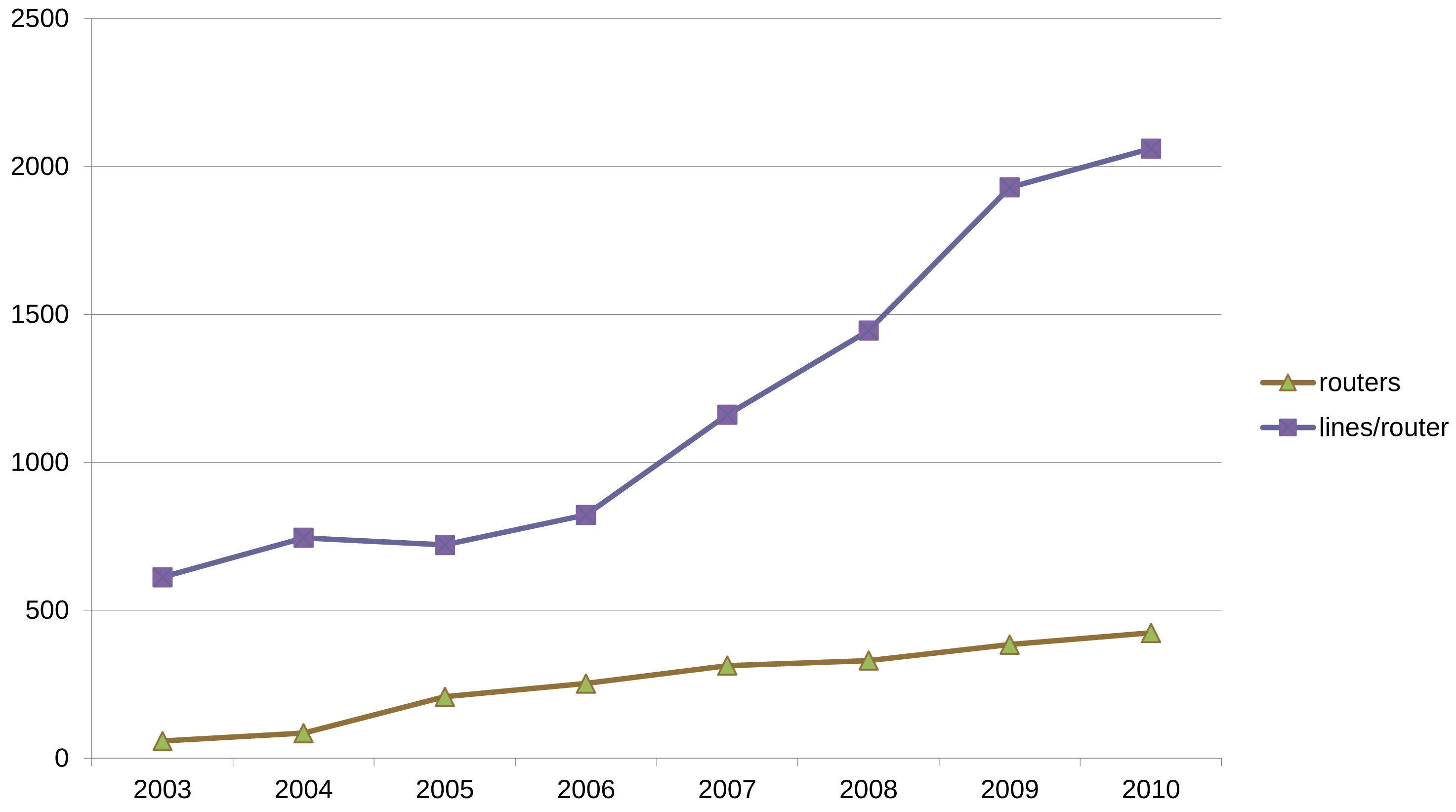
Assumption 7: My network is physically secure

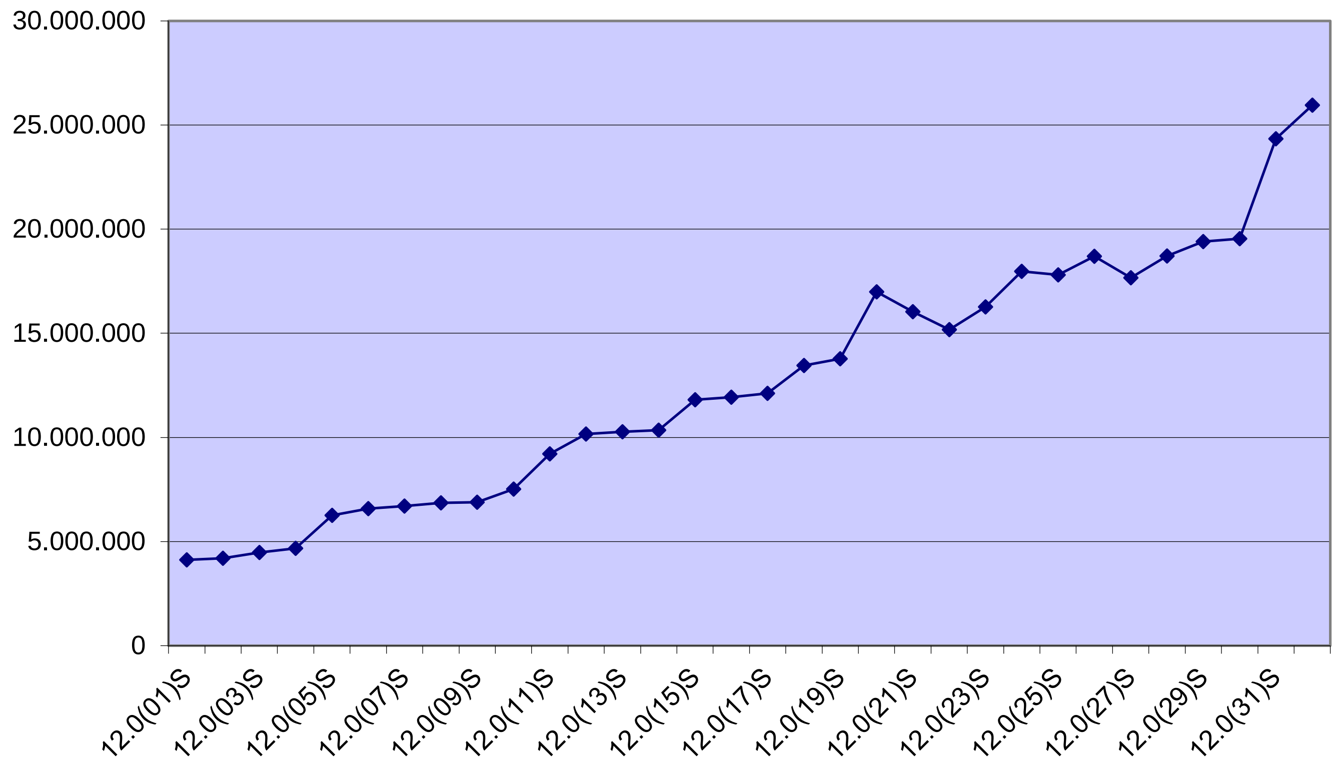
Assumption 8: I understand my network

Summary

End

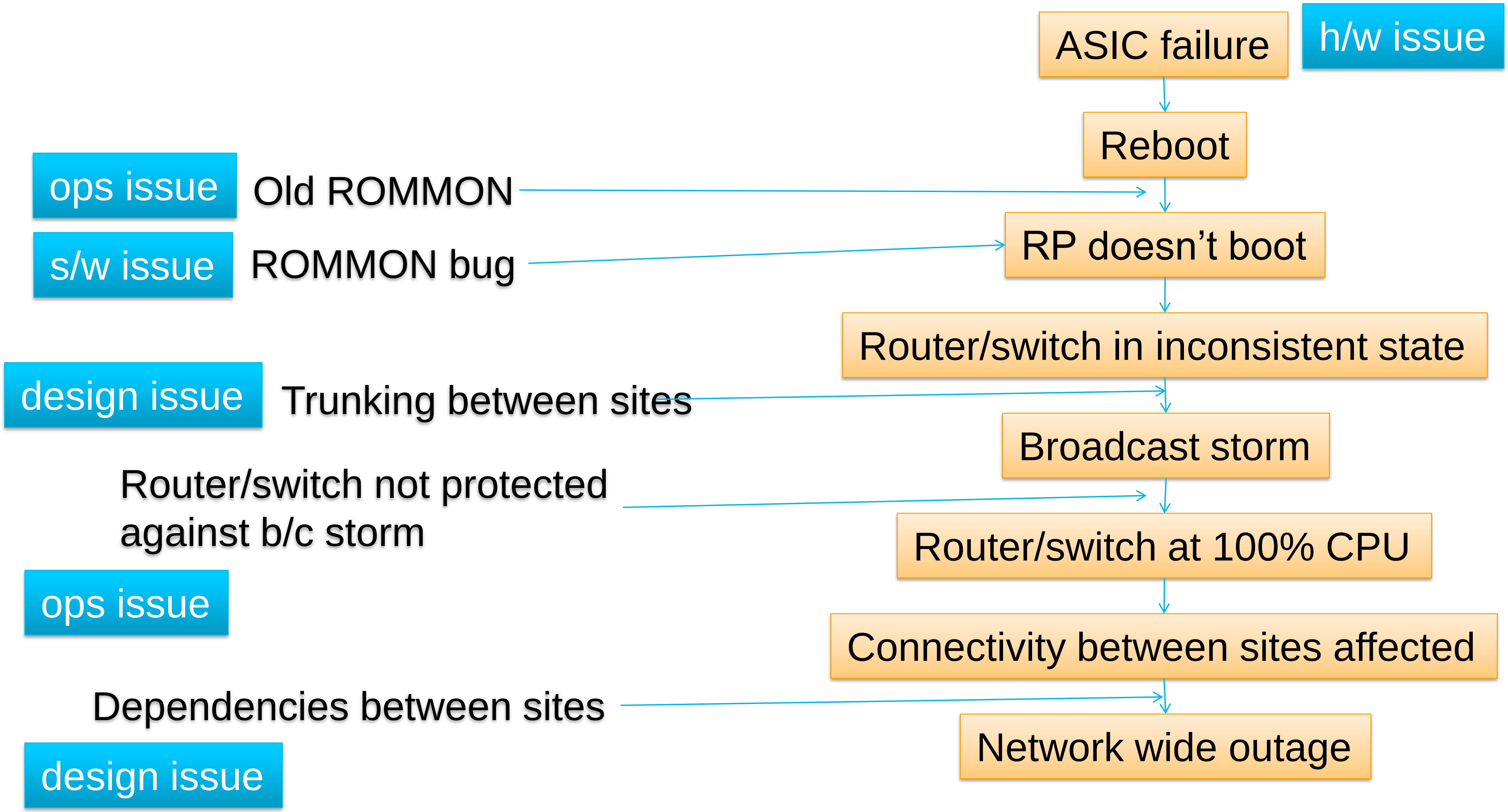
Increasing Complexity





Soon, it will not be feasible to directly configure routers

Example Of A “Catastrophic Failure” (P1 Case)



You Understand Your Network?

Source: http://www.flickr.com/photos/dseneste/5912382808/

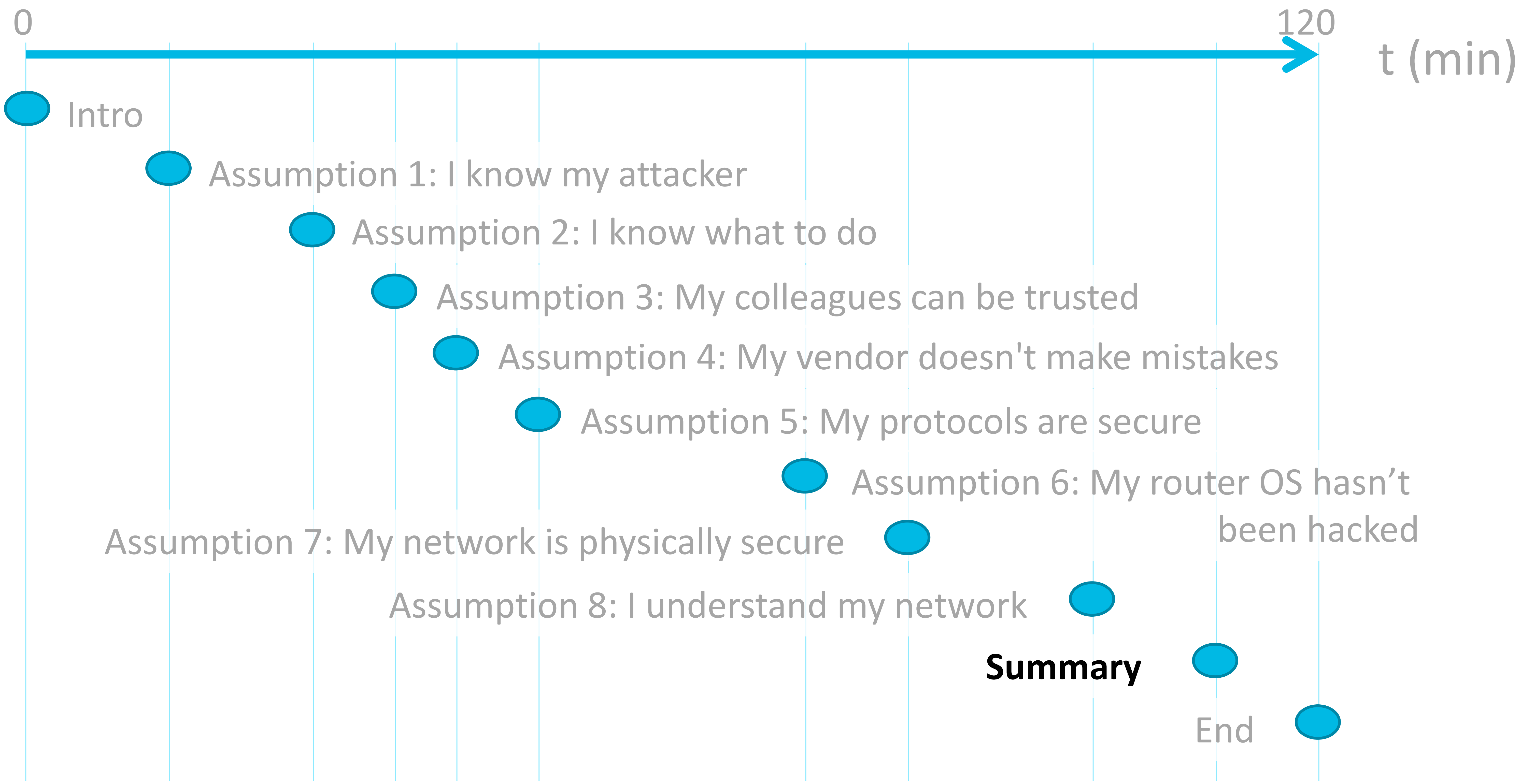
- Networks are complex
- Few (if any) admins understand the entire network, with all dependencies

THEREFORE

- Use templates and automated tools

  → Abstraction!!!
- Check dependencies, correctness
- Dual control: Two engineers in parallel propose required template changes; compare before deployment
- Minimize human intervention

Agenda: The 8 Fatal Assumptions



Intro

Assumption 1: I know my attacker

Assumption 2: I know what to do

Assumption 3: My colleagues can be trusted

Assumption 4: My vendor doesn't make mistakes

Assumption 5: My protocols are secure

Assumption 6: My router OS hasn’t been hacked

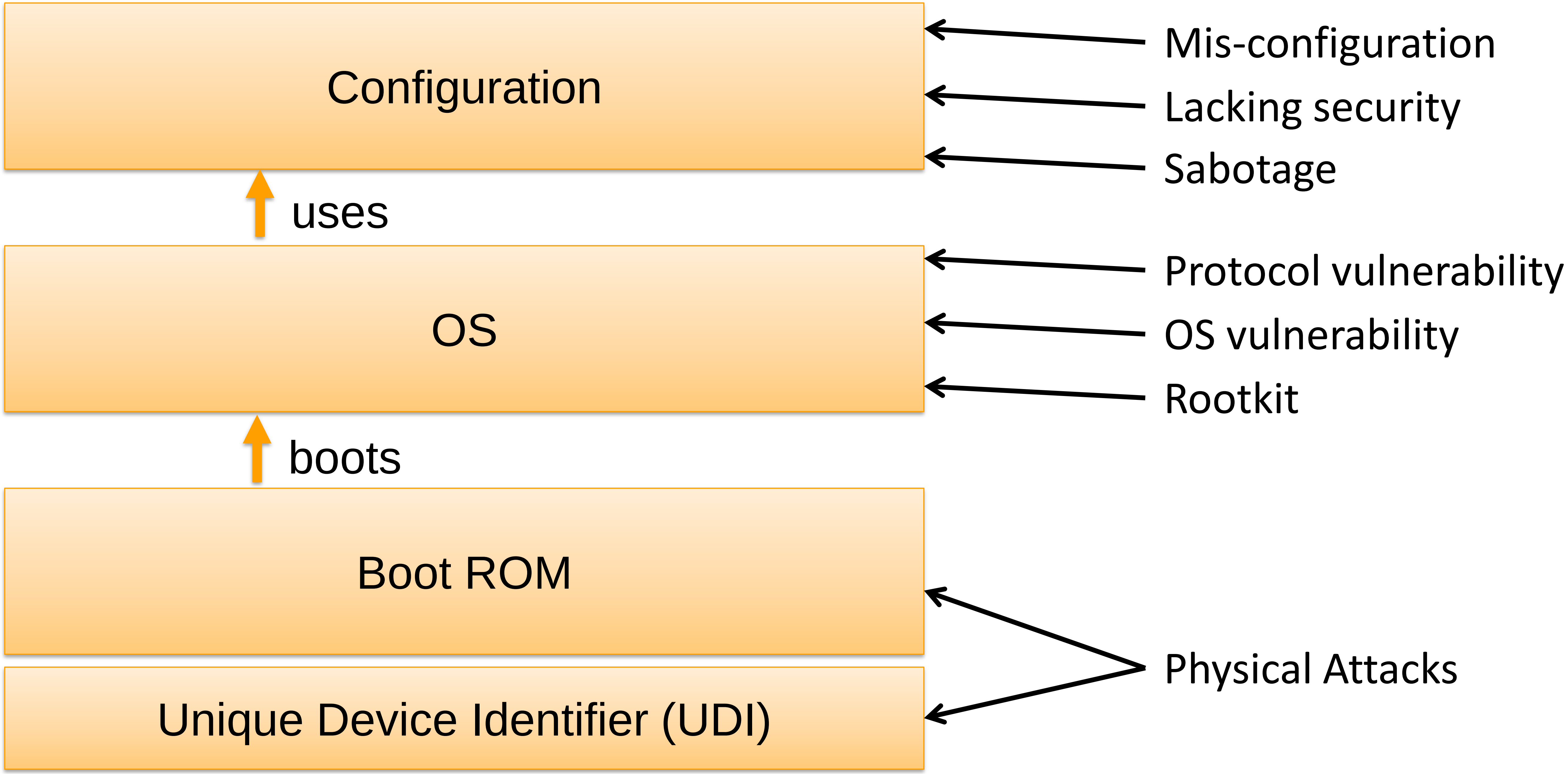
Assumption 7: My network is physically secure

Assumption 8: I understand my network

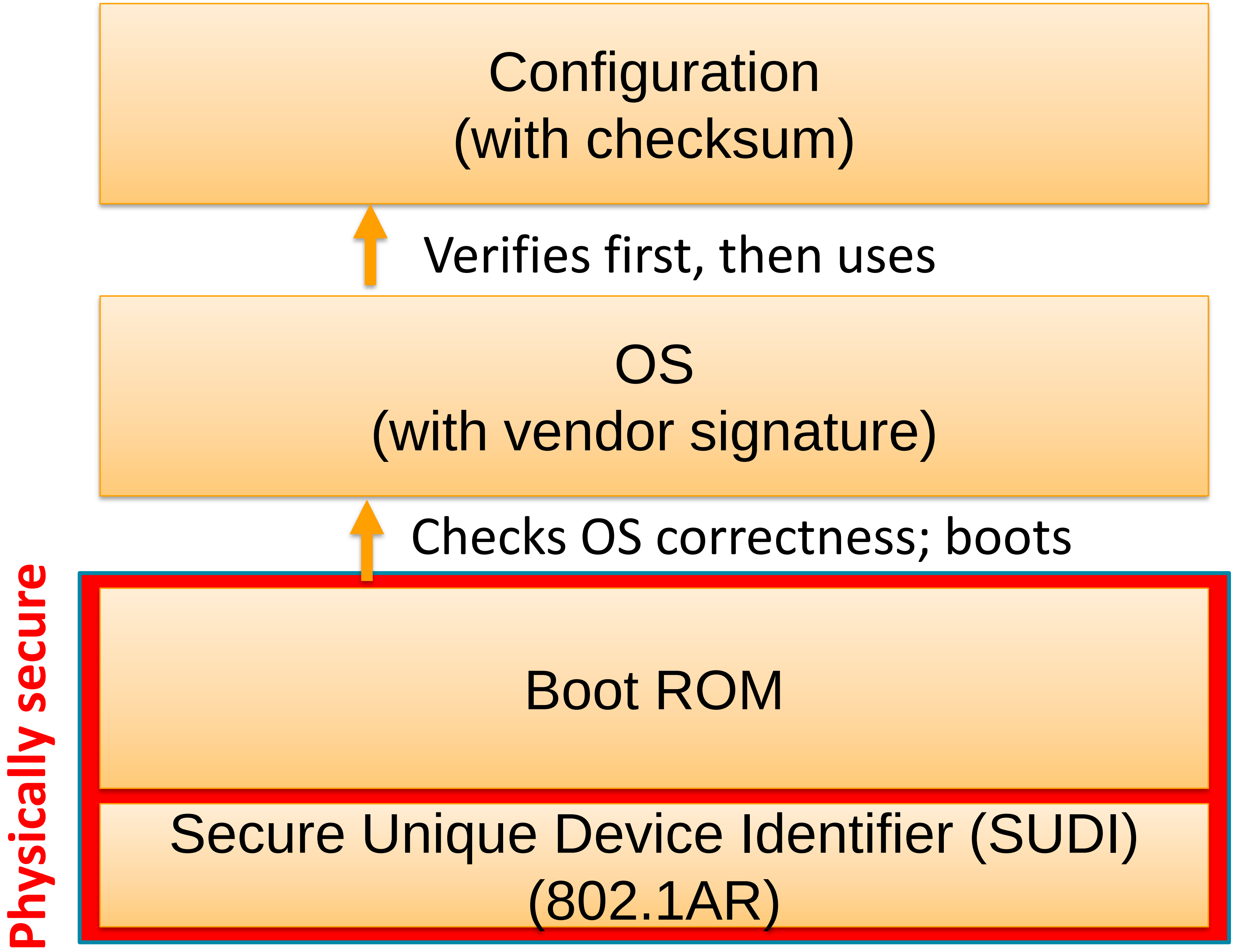
Summary

End

Depth Of Problems Today



Outlook


Configuration
(with checksum)
Verifies first, then uses
OS
(with vendor signature)
Checks OS correctness; boots
Boot ROM
Secure Unique Device Identifier (SUDI)
(802.1AR)
Physically secure

- SUDI allows for globally unique, secure device identification

  →Cannot replace device

- Boot process secured

  →Cannot modify bootrom

  →Cannot modify OS

- Secure OS coding practices

  →Reduces vulnerabilities

- Upgrade procedures

“Meta” Best Practices

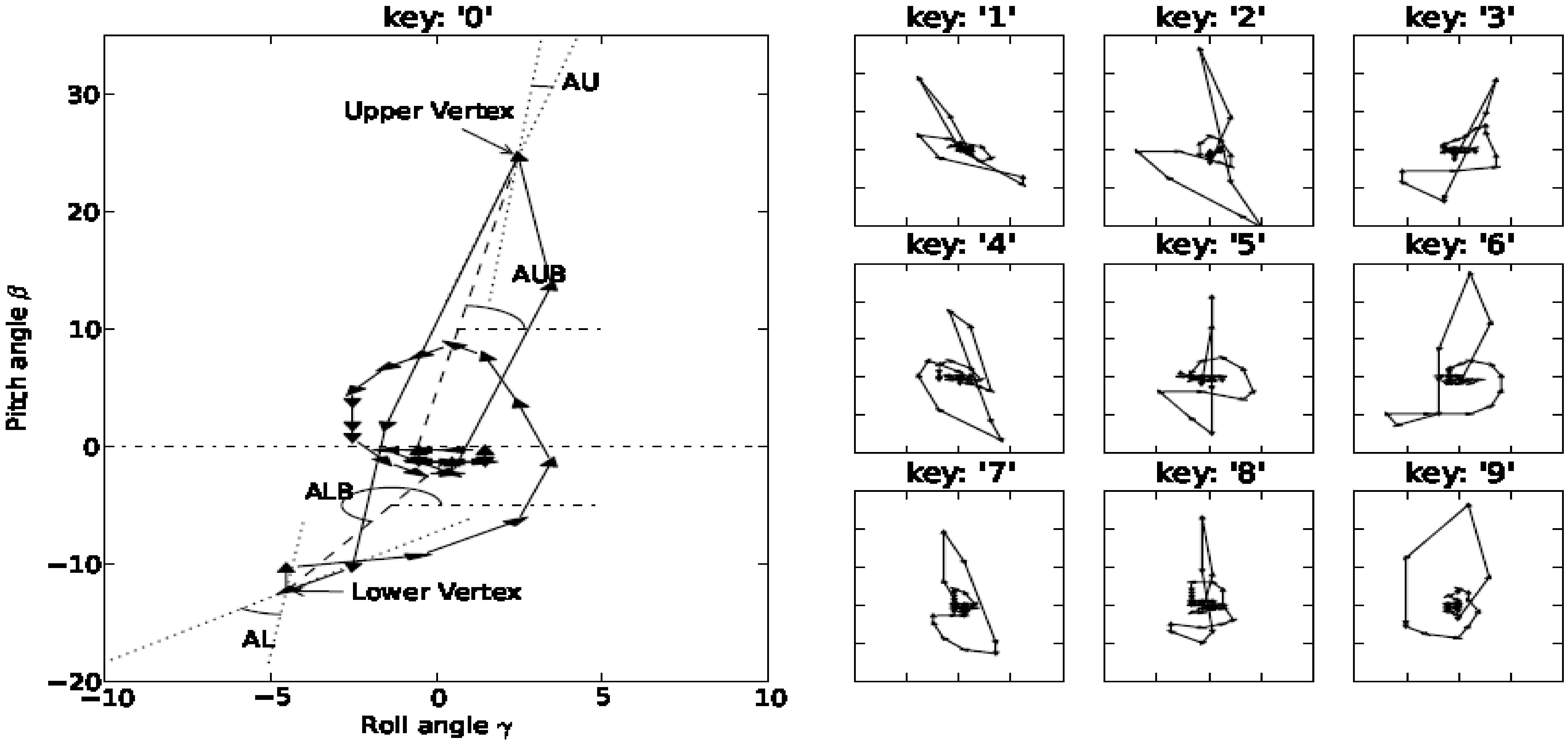
Source: http://www.flickr.com/photos/dseneste/5912382808/

- Defence in Depth
  - – Example: Infrastructure ACLs protect against SSH brute forcing
- Generic monitoring, audits
  - – Example: Detect MITM attacks through NetFlow

See: **BRKSEC-2073**: “Advanced Threat Defence using NetFlow and ISE”

- Process
  - – Example: Dual Control and Least Privilege
- Automation
  - – Example: Scripts to check correctness of OS / config

And Finally...



Source: http://www.usenix.org/event/hotsec11/tech/final_files/Cai.pdf