Secure Internet Communications, and Why Yours Probably are Not

Bill Cheswick

ches@lumeta.com

LUMETA CORPORATION

50 slides

Fighting FUD

- Good security is about relaxing…with good reason
- “Best block is not be there” – Pat Morita in *Karate Kid*
- This talk is about problems, some solutions, and some unrequited yearnings

POP3 alternatives

- **APOP authentication: at least requires dictionary attack to discover the password, and several of these would be resistant to all but brute force attacks**
- **SSL/TLS transport would fix this**
  - **Does the ISP offer the service?**
  - **Does the client support this access?**
- **You might think you have already selected one of these. You must check.**
- **You may not care (the passwords suggest otherwise)**

Why do these breaches happen?

- **Technical: good solutions may be unavailable**
- **Economic: solution gets in the way of getting the job done**
- **Psychological**
  - **“security is inconvenient”**
  - **“this account isn’t important”**
  - **“nobody wants to attack me”**

Secure Communications Requirements

- Secure endpoints
  - Only authorized users have access to clients and servers
  - Only trusted software is running
- Secure link between the endpoints
  - Physically secure link (I.e. intranets) or
  - Cryptography

Cryptography
v.
Cryptology

50 slides

Cryptography

- Deals with the technology for concealing the traffic
- It is hard to design your own cryptographic protocols, even if you think you know what you are doing
  - Numerous public embarrassing failures
- Today’s strong crypto may be immune to attack even by motivated government agencies

You don’t go through security, you go around it

50 slides

Cryptology

- Deals with the use of cryptography in the larger context
- E.g. It doesn’t matter how good a password you choose if someone is willing to beat that password out of you with a rubber hose
- Cipher machines that leak plaintext
- E.g. you use SSL to protect a credit card number, but the credit card database is on a weak computer

Probably good enough cryptography: on the wire

- Ipsec
  - Hardware VPN devices (
  - Doesn’t work through NAT (e.g. out of hotel rooms)
- SSL v3
- Ssh V2

…and authentication

- Kerberos
- Authentication tokens such as SecureID and SecureNet key

Probably not good enough cryptography

- WEP
- MS-PPTP
- Plain text
- Any proprietary, secret protocol

If the cryptography is good enough

- You can focus on the endpoints
- Thanks to Moore’s law, there is plenty of compute power available for strong crypto on client hosts
- Server hosts may need hardware assist for heavy traffic loads

Resistance to crypto

- **Takes time and expertise to set up**
- **Cryptographic authentication may take an extra user step**

Good security can still be convenient

- This is an engineering problem
- Hotel locks
- Automobile locks
- User expectation: I need a key to use my car or get into my hotel room

Endpoints are computers

- We don’t have very good tools for securing endpoints
- We rely on the software in the computers
- TCB: Trusted Computing Base

TCB

- **Reliable hardware**
- **Reliable boot mechanism**
- **Reliable operating system**
- **Reliable libraries**
- **Reliable applications**
- **Reliable software source**
- **Reliable software updates**

Microsoft/Intel as a TCB

- Reliable hardware
- Reliable boot mechanism
- Reliable operating system
- Reliable libraries
- Reliable applications
- Reliable software source
- Reliable software updates

Building our houses on sand

- **Insecure operating systems and applications**
- **Poor security models**
- **Complex standards**

Reliability of MSFT operating systems

- ***HUGE* code base**
- **History of unreliability**
  - **Buggy software has security bugs**

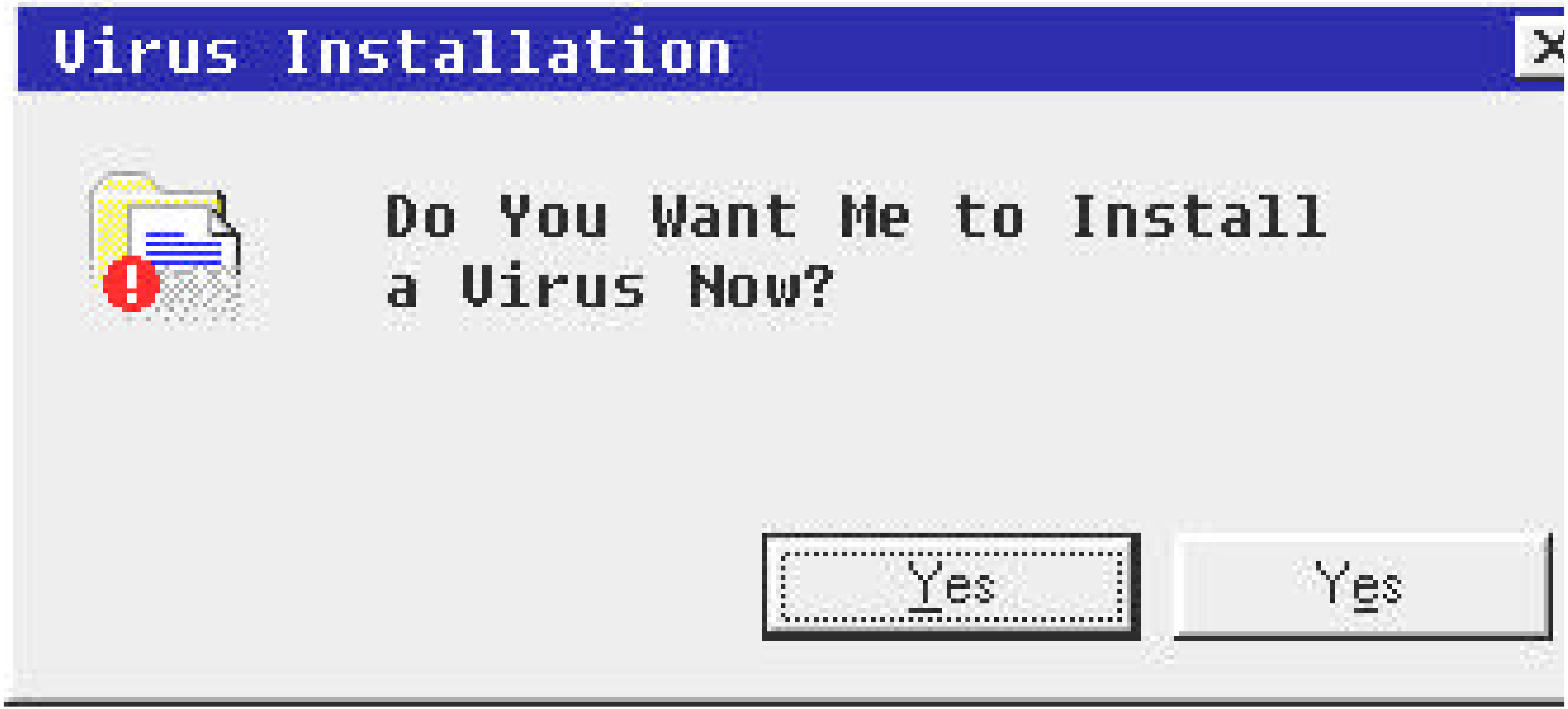
Poor engineering

- Potent, unnecessary features
  - Word macros
  - ActiveX components
  - .DLLs change the trusted base
- Ineffective sand-boxing
- Story about 20-year old email readers

Poor security models

- In general, users are not equipped to make security decisions
- Defaults should favor security and…
- Common practice should favor security
  - Javascript? Java? Plug-bins?

Click ***here*** to infect your computer.



Virus Installation

Do You Want Me to Install
a Virus Now?

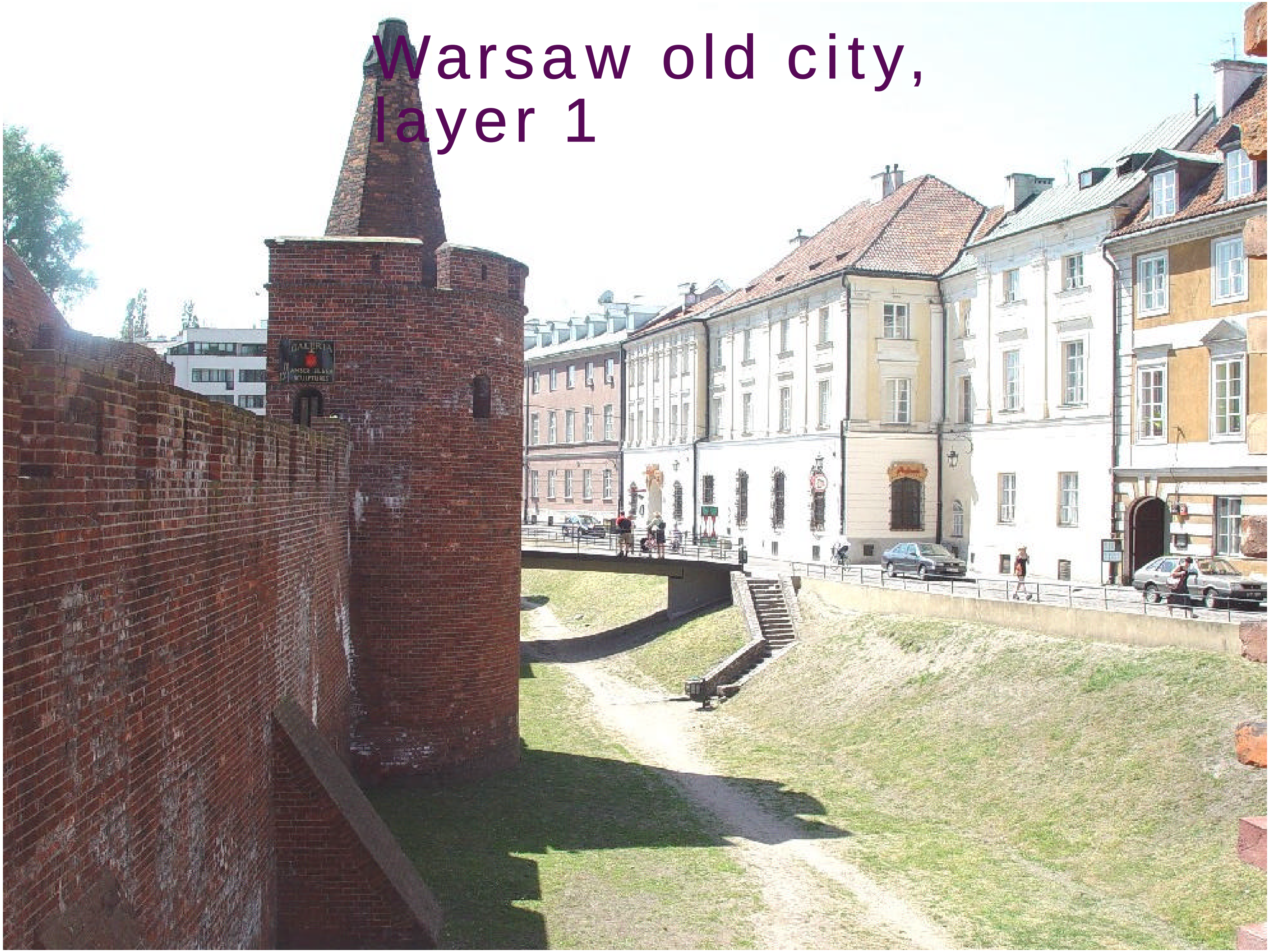
Complex standards

- ASN.1
- X.509
  - Uses ASN.1
- SNMP MIBs
  - Uses ASN.1
- LDAP
  - Uses ASN.1, X.509
- Often the code is the standard
- KISS

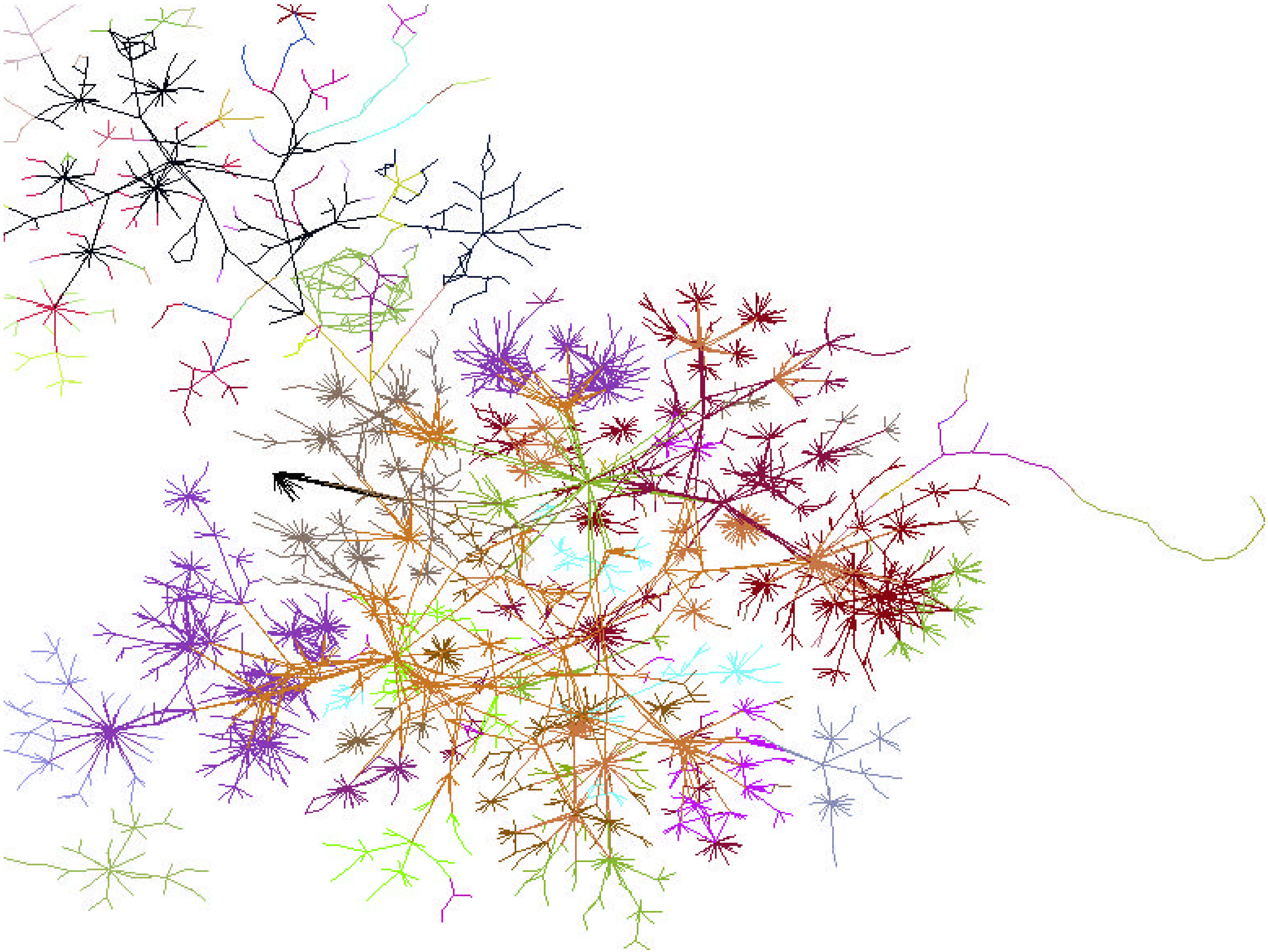
Perimeter defenses: trying to get out of the game

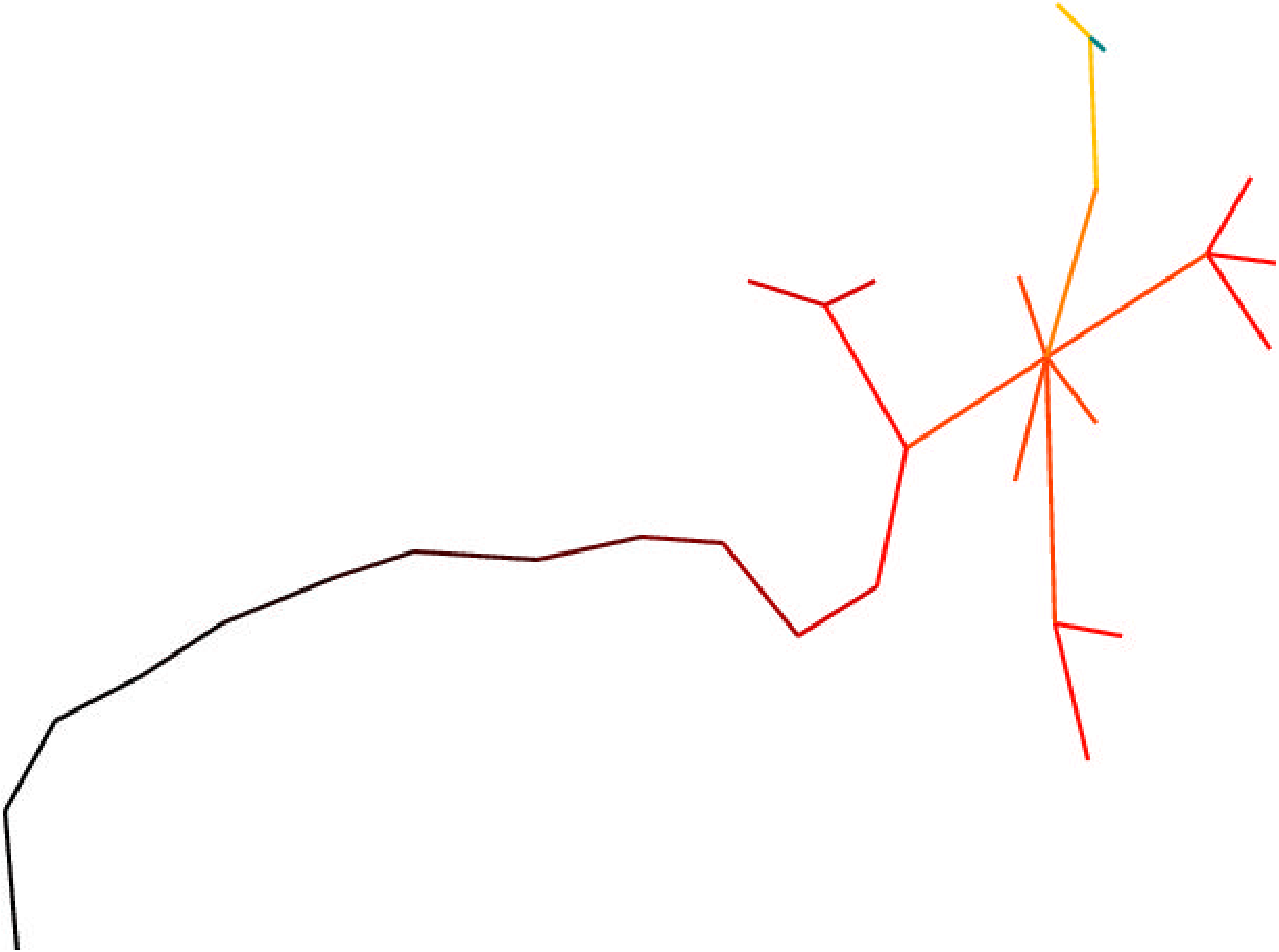
50 slides

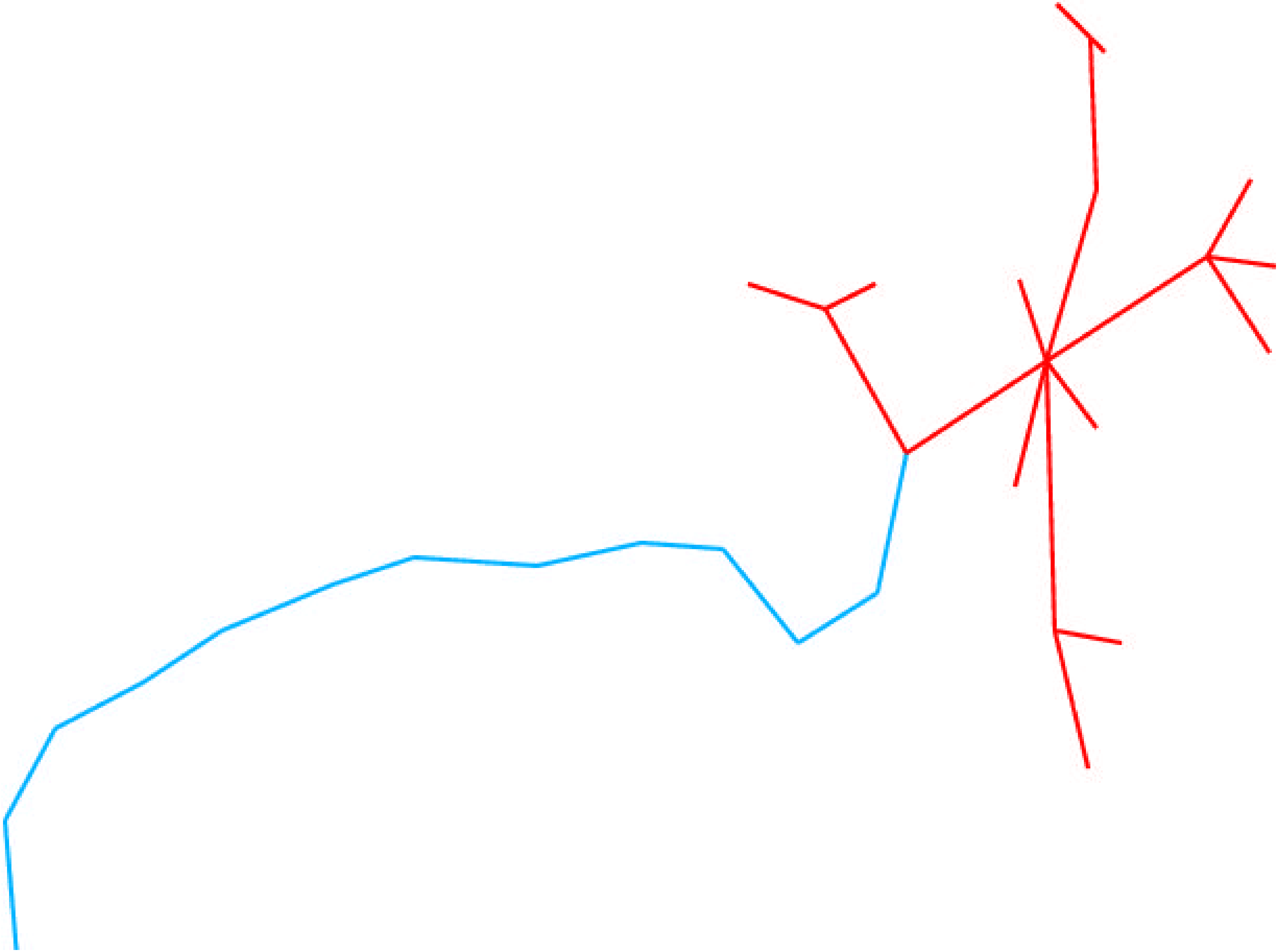
Warsaw old city, layer 1



Parliament: entrance







We call these “routing leaks”

- Easily-found holes in the intranet perimeter
- Show up nicely on the maps
- Leaking hosts or routers announce routes to other networks or the Internet
- Sometimes left over from an old corporate split
- Non-functional VPNs can show up

Slammer was a surprise audit of your perimeter security

LUMETA CORPORATION

50 slides

Host leaks

- Leaking hosts do not route between the networks
- May be a dual-homed host
- Not always a bad thing
- Technology didn't exist to find these

Possible host leaks

- Miss-configured telecommuters connecting remotely
- VPNs that are broken
- DMZ hosts with too much access
- Business partner networks
- Internet connections by rogue managers
- Modem links to ISPs

Some intranet statistics from Lumeta clients

Intranet sizes (devices)	7,900	365,000
Corporate address space	81,000	745,000,000
Address space usage efficiency		
% devices in unknown address space	0.01%	20.86%
% routers responding to "public"	0.14%	75.50%
% routers responding to other	0.00%	52.00%
Outbound host leaks on network	0	176,000
% devices with outbound ICMP leaks	0%	79%
% devices with outbound UDP leaks	0%	82%
Inbound UDP host leaks	0	5,800
% devices with inbound ICMP leaks	0%	11%
% devices with inbound UDP leaks	0%	12%
% hosts running Windows	36%	84%

Leak results

- Found home web businesses
- At least two clients have tapped leaks
  - One made front page news

Strong host security is possible

LUMETA CORPORATION

50 slides

...but not with Microsoft, yet...

- The new security focus announced in Feb. 2002 seems to be real
- Massive retraining effort
- Huge code review effort
- Already reported to be having an effect
- But they have a long way to go

How I do it

- **Routine, strong security**
  - **Ssh and IPsec only**
- **Servers running Unix-like operating systems**
  - **Only run the network services absolutely needed**
  - **Jail those services in chroot partitions (see below)**
- **Clients run minimal client software**
  - **Text email processors**
  - **Text browser**
  - ***We need a jailed browser…seems to be quite hard***

Chroot: Unix belt-and-suspenders

- **Confines software to a portion of the file tree**
- ***Root* can probably escape**
- **Newer experiments restrict network and other access to the host**
- **Failure in the chroot environment does not mean that the computer system is lost**
- **Security completely orthogonal to the security in the server**
- **My confident openssl server**

My life without a firewall

- Like skinny-dipping
- Have to turn on Javascript and Java from time to time
- Seldom read html attachments (most spam has these), and Word, PowerPoint, and Excel attachments
  - – "I can't run like that"
- Ssh breaches always a worry
- Transitive trust of my machines always a worry.

What did I choose for Lumeta?

- **For the technical people and our scanning product:**
  - **FreeBSD and all the hard rules. We gotta be state-of-the-art secure**
- **For the sales and support staff**
  - **The usual MSFT configurations**
- **A firewall provides belt-and-suspenders**

You probably made the same decision

- **Many applications run only on Microsoft operating systems**
- **Other solutions are inviting, but have unknowns**
  - **Is Openoffice ready for prime time?**
  - **Does your computer have enough memory to support VMware?**
  - **How hard is it to support 50,000 hosts running Linux?**
- **Your server farms may well be running non-Microsoft software**

What I'd like to see from Microsoft

- **Sandboxes for network servers**
- **Default settings that are secure**
- **No foreign macros**
- **No executable code in .ppt, .doc, .xls**
- **Prominent buttons on IE to enable/disable scripting and other such features**
- **A TCB that can't be changed casually by any process with "admin" privileges**

What I'd like to see from Microsoft

- The ability to tunnel the smb protocol through an ssh TCP tunnel
- Documentation and adherence to a standard of remote file system support that can be implemented freely without reverse engineering
- Complete and accurate documentation of NTFS for the same purpose
- IPsec that can use a shared secret, which is simpler than the current certificate

What I'd like to see from the world

- Simple, tested, certified network servers
  - Samba, apache are too large
- More work on a general TCB
  - Linux, *BSD are working on this
  - Adopt some Orange book requirements
- I'd like Don Knuth to write the software
  - We can all benefit from the contributions of single geniuses

What I'd like to see from standards bodies

- Rigorous definition of standards
- Simpler standards
  - Easy enough to implement that we avoid a monoculture
- Proven reference implementation of the standard
  - This is where Orange Book A1 certification would be cost-effective

Internet Security, Second Edition

...of *Firewalls and Internet Security* became the bible of Internet security ... think about threats and solutions. This completely updated and expanded ... security problems companies face in today's Internet, identifies the ... ular security technologies, and illustrates the ins and outs of deploying ... will learn how to plan and execute a security strategy that allows easy ... hile defeating even the wiliest of hackers.

...rity, Second Edition, draws upon the authors' experiences as researchers ... since the beginning of the Internet explosion.

...roduction to their philosophy of Internet security. It progresses quickly ... tacks on hosts and networks and describes the tools and techniques used ... [illegible] attacks. The focus then shifts to firewalls and virtual private ... a step-by-step guide to firewall deployment. Readers are immersed in ... ternet security through a critical examination of problems and practices ... l as discussions on the deployment of a hacking-resistant host and on ... IDS). The authors scrutinize secure communications over insecure ... their predictions about the future of firewalls and Internet security.

...ide an introduction to cryptography and a list of resources (which will ... Web site and updated throughout so that readers can rely on the ... rts in Internet security.

...d-won knowledge of how to fight off hackers, readers of *Firewalls and ... Edition*, can make security the [illegible] that will make the Internet ... and

...ef Scientist at Lumeta Corporation, which explores and maps clients' ... find perimeter leaks. Formerly he was a senior researcher at AT&T Bell ... pioneering work in the areas of firewall design and implementation, PC ... uitions, and the Plan 9 operating system.

...the creator of Netnews, is a Fellow at AT&T Labs Research. He is a ... ademy of Engineering and a frequent participant in National Research ... rently one of the Security Area directors of the Internet Engineering

...bin.com) is an Associate Professor in the Computer Science Department ... and serves as the Technical Director of the Information Security ... Principal Researcher in the Secure Systems Research Department at ... e author of *White-Hat Security Arsenal* (Addison-Wesley, 2001).

...com

... & Wesley [illegible]. Distributed by ... [illegible]. All rights reserved.

...paper

54999
9 780201 634662
ISBN 0-201-63466-X
$49.99 US
$77.99 CANADA

7 85342 63466 2

Firewalls and Internet Security

Second Edition

Cheswick
Bellovin
Rubin

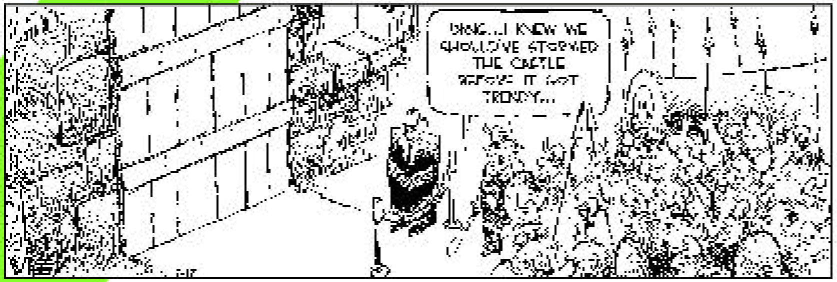
Addison
Wesley

Firewalls and Internet Security

Second Edition

Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin


DANG...I KNEW WE SHOULD'VE STORMED THE CASTLE BEFORE IT GOT TRENDY...

ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES