Pondering and Patrolling Perimeter Defenses

Bill Cheswick
ches@lumeta.com
http://www.lumeta.com
Brief personal history

• Started at Bell Labs in December 1987
  – Immediately took over postmaster and firewall duties
• Good way to learn the ropes, which was my intention
Morris worm hit on Nov 1988

• Heard about it on NPR
  – Had a “sinking feeling” about it
• The home-made firewall worked
  – No fingerd
  – No sendmail (we rewrote the mailer)
• Intranet connection to Bellcore
• We got lucky
• Bell Labs had 1330 hosts
• Corporate HQ didn’t know or care
Action items

• Shut down the unprotected connection to Bellcore
  – What we now call a “routing leak”

• Redesign the firewall for much more capacity, and no “sinking feeling”
  – (VAX 750, load average of 15)

• Write a paper on it
  – “if you don’t write it up, you didn’t do the work”
Old gateway:
New gateway:

belt  suspenders
New gateway:
(one referee’s suggestion)
“Design of a Secure Internet Gateway” – Anaheim Usenix, Jun 1990

• My first real academic paper
• It was pretty good, I think
• It didn’t have much impact, except for two pieces:
  – Coined the work “proxy” in its current use (this was for a circuit level gateway
    • Predated “socks by three years)
  – Coined the expression “crunchy outside and soft chewy center”
Why wasn’t the paper more influential?

• Because the hard part isn’t the firewall, it is the perimeter
  – I built a high security firewall for USSS from scratch in about 2 hours in Sept. 2001.

• I raised our firewall security from “low medium” to “high”
  – (that’s about as good as computer and network security measurement gets)

• The perimeter security was “dumb luck”, which we raised to “probably none”
Network and host security levels

- Dumb luck
- None
- Low
- Medium
- High = no “sinking feeling”
By 1996, AT&T’s intranet

• Firewall security: high, and sometimes quite a pain, which meant
• Perimeter security: dumb luck
• Trivestiture didn’t change the intranet configuration that much
Lucent 1997:
Circling the wagons around Wyoming

The Internet

Lucent - 130,000, 266K IP addresses, 3000 nets ann.

thousands of telecommuters

~200 business partners

SLIP
PPP
ISDN
X.25
cable
...

Lucent 16 June 2005

Pondering Perimeters: DOE
Firewalls and Internet Security
Second Edition
Repelling the Wily Hacker

William R. Cheswick
Steven M. Bellovin
Aviel D. Rubin
Highlands forum, Annapolis, Dec 1996

• A Rand corp. game to help brief a member of the new President’s Infrastructure Protection Commission

• Met Esther Dyson and Fred Cohen there
  – Personal assessment by intel profiler

• “Day after” scenario

• Gosh it would be great to figure out where these networks actually go
Perimeter Defenses have a long history
The Pretty Good Wall of China
Perimeter Defense
Flower pots
Security doesn’t have to be ugly
Delta barriers
Parliament: entrance
Parliament: exit
Edinburgh Castle
Warwick Castle
Berwick Castle
Why use a perimeter defense?

• It is cheaper
  – A man’s home is his castle, but most people can’t afford the moat
• You can concentrate your equipment and your expertise in a few areas
• It is simpler, and simpler security is usually better
  – Easier to understand and audit
  – Easier to spot broken parts
Layered Positive Measures to Assure Against Unauthorized Use

The Adversary: Humans or Accidents

Personnel

Procedures

Security

Design Features

Recapture & Recovery

PREVENT UNAUTHORIZED USE

Coded Control
Warhead & Weapon System

Use Denial Features

Accident Protection Features

Physical Security

Information Security

Emergency Action Procedures

Materials & Code Management

Operational Safety Rules

Personnel Reliability Program

Two Person Policy

Exercises & Training
What’s wrong with perimeter defenses

• They are useless against insider attacks
• They provide a false sense of security
  – You still need to toughen up the inside, at least some
  – You need to hire enough defenders
• They don’t scale well
Anything large enough to be called an ‘intranet’ is out of control
The Internet Mapping Project

An experiment in exploring network connectivity
1998
Methods - network discovery (ND)

- Obtain master network list
  - network lists from Merit, RIPE, APNIC, etc.
  - BGP data or routing data from customers
  - hand-assembled list of Yugoslavia/Bosnia
- Run a TTL-type (traceroute) scan towards each network
- Stop on error, completion, no data
  - Keep the natives happy
Methods - data collection

• Single reliable host connected at the company perimeter
• Daily full scan of Lucent
• Daily partial scan of Internet, monthly full scan
• One line of text per network scanned
  – Unix tools
• *Use a light touch, so we don’t bother Internet denizens*
TTL probes

- Used by traceroute and other tools
- Probes toward each target network with increasing TTL
- Probes are ICMP, UDP, TCP to port 80, 25, 139, etc.
- Some people block UDP, others ICMP
TTL probes
Send a packet with a TTL of 1...
…and we get the death notice from the first hop
Send a packet with a TTL of 2...
... and so on ...
Advantages

• We don’t need access (i.e. SNMP) to the routers
• It’s very fast
• Standard Internet tool: it doesn’t break things
• Insignificant load on the routers
• Not likely to show up on IDS reports
• We can probe with many packet types
Limitations

• Outgoing paths only
• Level 3 (IP) only
  – *ATM networks appear as a single node*
  – This distorts graphical analysis
• Not all routers respond
• Many routers limited to one response per second
Limitations

• View is from scanning host only
• Takes a while to collect alternating paths
• Gentle mapping means missed endpoints
• Imputes non-existent links
The data can go either way
The data can go either way
But our test packets only go part of the way
We record the hop…
The next probe happens to go the other way
...and we record the other hop...
We’ve imputed a link that doesn’t exist
Intranet implications of Internet mapping

• High speed technique, able to handle the largest networks
• Light touch: “what are you going to do to my intranet?”
• Acquire and maintain databases of Internet network assignments and usage
Data collection complaints

• Australian parliament was the first to complain
• List of whiners (25 nets)
• On the Internet, these complaints are mostly a thing of the past
  – Internet background radiation predominates
Visualization goals

• make a map
  – show interesting features
  – debug our database and collection methods
• geography doesn’t matter
• use colors to show further meaning
Visualization of the layout algorithm

Laying out the Internet graph
Map Coloring

• distance from test host
• IP address
  – shows communities
• Geographical (by TLD)
• ISPs
• future
  – timing, firewalls, LSRR blocks
Colored by IP address!
Colored by geography
Colored by distance from scanning host
Yugoslavia

An unclassified peek at a new battlefield
1999
Un film par Steve “Hollywood” Branigan...
fin
Intranets: the rest of the Internet
This was Supposed To be a VPN
Detecting perimeter leaks: not all spoofing is evil

Lumeta’s Special Sauce
2000
Types of leaks

• Routing leaks
  – Internal routes are announced externally, and the packets are allowed to flow betwixt

• Host leaks
  – Simultaneously connected inside and out, probably without firewall-functionality
  – Not necessarily a dual-homed host

• “Please don’t call them leaks”
  – They aren’t always a Bad Thing
Routing leaks

• Easily seen on maps
• Shows up in our reports
• Generally easily fixed
Host leak detection

• Developed to find hosts that have access to both intranet and Internet
• Or across any privilege boundary
• Leaking hosts do not route between the networks
• 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
Leak Detection Prerequisites

• List of potential leakers: obtained by census
• Access to intranet
• Simultaneous availability of a “mitt”
Leak Detection Layout

- Mapping host with address A is connected to the intranet.
- Mitt with address D has Internet access.
- Mapping host and mitt are currently the same host, with two interfaces.
Leak Detection

- Test host has known address B on the intranet
- It was found via census
- We are testing for unauthorized access to the Internet, possibly through a different address, C
Leak Detection

- **A** sends packet to **B**, with spoofed return address of **D**
- If **B** can, it will reply to **D** with a response, possibly through a different interface
Leak Detection

- Packet must be crafted so the response won’t be permitted through the firewall
- A variety of packet types and responses are used
- Either inside or outside address may be discovered
- Packet is labeled so we know where it came from
Inbound Leak Detection

- This direction is usually more important
- It all depends on the site policy…
- …so many leaks might be just fine.
Inbound Leak Detection

Diagram:
- mitt (D) connected to Internet
- Mapping host (A) connected to intranet
- Test host (B) connected to intranet
Leak results

• Found home web businesses
• At least two clients have tapped leaks
  – One made front page news
• From the military: “the republic is a little safer”
### Case studies: corp. networks

#### Some intranet statistics

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intranet sizes (devices)</td>
<td>7,900</td>
<td>365,000</td>
</tr>
<tr>
<td>Corporate address space</td>
<td>81,000</td>
<td>745,000,000</td>
</tr>
<tr>
<td>% devices in unknown address space</td>
<td>0.01%</td>
<td>20.86%</td>
</tr>
<tr>
<td>% routers responding to &quot;public&quot;</td>
<td>0.14%</td>
<td>75.50%</td>
</tr>
<tr>
<td>% routers responding to other</td>
<td>0.00%</td>
<td>52.00%</td>
</tr>
<tr>
<td>Outbound host leaks on network</td>
<td>0</td>
<td>176,000</td>
</tr>
<tr>
<td>% devices with outbound ICMP leaks</td>
<td>0%</td>
<td>79%</td>
</tr>
<tr>
<td>% devices with outbound UDP leaks</td>
<td>0%</td>
<td>82%</td>
</tr>
<tr>
<td>Inbound UDP host leaks</td>
<td>0</td>
<td>5,800</td>
</tr>
<tr>
<td>% devices with inbound ICMP leaks</td>
<td>0%</td>
<td>11%</td>
</tr>
<tr>
<td>% devices with inbound UDP leaks</td>
<td>0%</td>
<td>12%</td>
</tr>
<tr>
<td>% hosts running Windows</td>
<td>36%</td>
<td>84%</td>
</tr>
</tbody>
</table>
We developed lot of stuff

• Leak detection (that’s the special sauce)
• Lots of reports: the hardest part is converting data to information
• Route discovery: TTL probes plus SNMP router queries
• Host enumeration and identification: ping and xprobe-style host identification
• Server discovery: SYN probes of popular TCP ports
• Wireless base station discovery: xprobe, SNMP, HTTP
• And more…ask the sales people
• The “zeroth step in network intelligence”
  – me
Nice research result: happy clients

- Switched from service to appliance
- Developers did a nice job with GUI and productizing the software
- Priced by approx. number of active IP devices and length of time you have the appliance
- ~100 Fortune 200 clients
- Growing government use among military, spooks, and various departments
  - FAA, VA, EOP, DISA, DOD, Treasury, pilots at others including DOE
What’s next?
IPv6
2005 + 3
Pondering and Patrolling Perimeters

Bill Cheswick
ches@lumeta.com
http://www.lumeta.com

(Bill, you can go drinking now)