Trust Factory
architecture & security

Over-zealous Security Administrators Are Breaking the Internet

Richard van den Berg

Trust Factory

Phil Dibowitz

University of Southern California

THE PROBLEM

Trust Factory
architecture & security

http://bladeforum.wells.org.uk/
“On my sun blade netscape browser, i am not able to access all the websites. Some websites are just fine and others are talking long time and then timeout.”

comp.dcom.sys.cisco
“The client computers at my remote sites can access all but a handful of websites. From the remote routers I can telnet to the website and receive the html document. But, from the client computers (behind those remote routers), I am unable to receive the html document.”

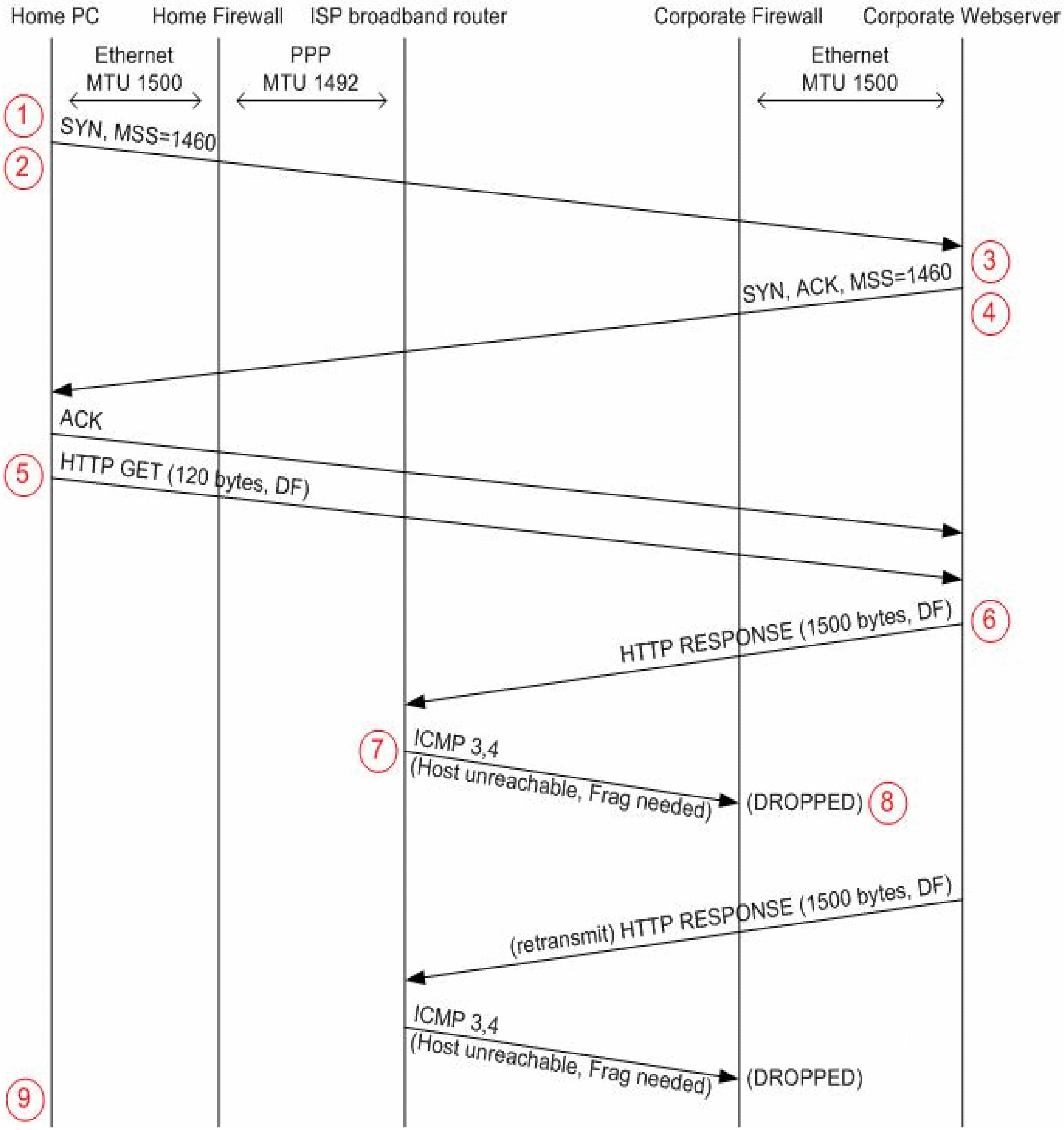
bellsouth.net.support.adsl
“I have the following setup. Machine #1 running XP-Home & SpeedTouch USB DSL modem. Machine #2 running WinME. Machine #3 running XP-Home. All machines network just fine and machine 2 & 3 can get to the interent through machine 1 just fine for about 90% of the websites. However there are a few websites that if accessed through machines 2 or 3 just will not work.”

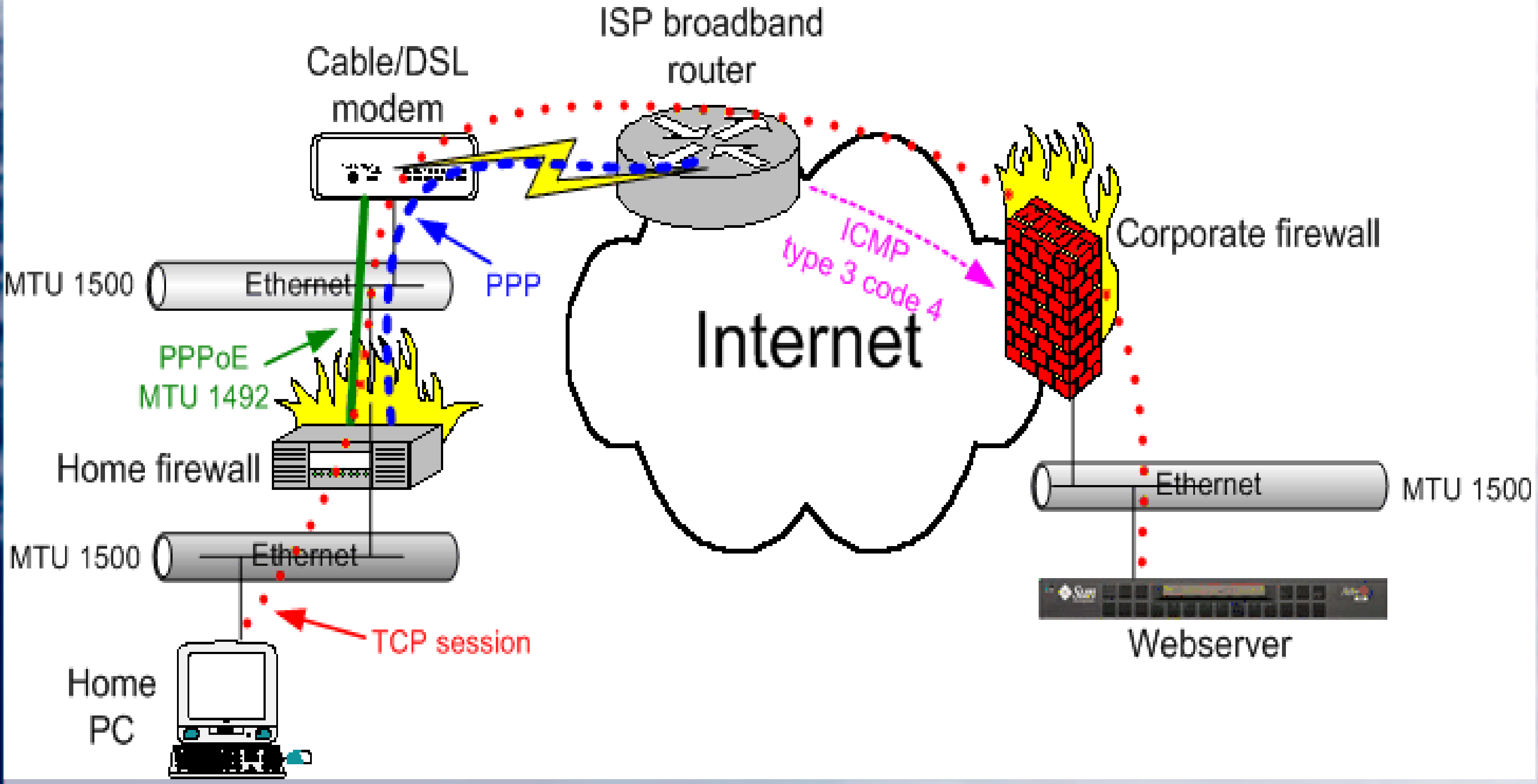
PATH MTU DISCOVERY

- use Maximum Segment Size (MSS) from TCP SYN if available, otherwise use local Maximum Transfer Unit (MTU)
- set Don't Fragment (DF) bit on all IP packets
- routers will send back ICMP type 3 code 4 (destination unreachable: fragmentation needed, but DF bit set) including MTU of the next link if packets are too big
- lower packet size to MTU indicated by ICMP 3,4 and resend the packet

PATH MTU DISCOVERY BLACKHOLE

- A Path MTU Discovery black hole occurs when the ICMP type 3 code 4 packets do not reach the system which is sending out packets too large for the smallest MTU on the end-to-end link
- Possible causes:
  - faulty routers
  - filters
  - firewalls


Home PC
Home Firewall
ISP broadband router
Corporate Firewall
Corporate Webserver
Ethernet
MTU 1500
PPP
MTU 1492
Ethernet
MTU 1500
1
SYN, MSS=1460
2
3
SYN, ACK, MSS=1460
4
ACK
5
HTTP GET (120 bytes, DF)
6
HTTP RESPONSE (1500 bytes, DF)
7
ICMP 3,4
(Host unreachable, Frag needed)
(DROPPED)
8
(retransmit) HTTP RESPONSE (1500 bytes, DF)
ICMP 3,4
(Host unreachable, Frag needed)
(DROPPED)
9


ISP broadband router
Cable/DSL modem
PPP
MTU 1500
Ethernet
PPPoE
MTU 1492
Home firewall
MTU 1500
Ethernet
TCP session
Home PC
Internet
ICMP type 3 code 4
Corporate firewall
Ethernet
MTU 1500
Webserver

HISTORY OF THE BLACK HOLE

- 1988: Path MTU Discovery proposed
- 1990: RFC 1191 recommends use of Path MTU Discovery
- 1998: oldest found website mentioning the black hole
- 2000: RFC 2923 TCP Problems with Path MTU Discovery
- 2001: sans.org: The Truth About ICMP
- 2002: The MSS Initiative

MORE HISTORY

- Affects technologies like SLIP and X.25
- Small MTUs now only at the endpoints, right?

NOT TAKEN SERIOUSLY

Prior to the recent growth in broadband...

The number affected was small, so many people ignored the problem.

Client-side fixes were considered acceptable.

RECENT HISTORY

- PPP over Ethernet (PPPoE)
- Point-to-point Tunneling Protocol (PPTP)
- Generic Route Encapsulation (GRE)
- IP version 6 (IPv6)
- 10Gb ethernet
- DSL/cable users on the rise
- Home firewalls

Trust Factory
architecture & security

AND THE PROBLEM GROWS

- With the use of broadband, and thus these protocols growing fast, many more users are affected.
- More and more questions regarding the blackhole are seen on newgroups and mailing list as time goes on.

TrustFactory
architecture & security

WHO IS (NOT) AFFECTED

1) just one workstation connected to a modem
2) home gateways with a public IP address on an Ethernet interface
3) home gateways connecting to a modem using USB
4) home gateways connecting to a modem using PPTP
5) home gateways connecting to a modem using PPPoE

SIZE OF THE PROBLEM

Sites that really should know better are broken:

www.securityfocus.com

www.cert.org

www.verisign.com

www.counterpane.com

www.ntsecurity.com

SOLUTIONS

- Allow ICMP Type 3 Code 4 Packets To Reach the Servers
- Disable Path MTU Discovery
- Path MTU Discovery Black Hole Detection
- Using a Proxy Server
- Lowering MTU/MSS of the Internal Network
- MSS Clamping

THE MSS INITIATIVE

- Started January 2002
- Contacts administrators of broken sites
- Blacklists sites that don't respond within two weeks (fix not required)
- Offers assistance in correction the problem
- Provides detection instructions for users
- Provides a list of broken sites for comparison for users

Trust Factory
architecture & security

THE MESSAGE

RFC 2923 mentions in Chapter 3:

It is vitally important that those who design and deploy security systems understand the impact of strict filtering on upper-layer protocols. The safest web site in the world is worthless if most TCP implementations cannot transfer data from it.

CONCLUSION

- Know what you are filtering and why
- Don't asume everything is okay if a simple test scenario seems to work
- Set up and publish technical points of contact
- Listen to your users

URLS

- http://www.ietf.org/rfc/rfc1191.txt
- http://www.ietf.org/rfc/rfc2923.txt
- http://rr.sans.org/threats/ICMP.php
- http://www.cisco.com/warp/public/105/38.shtml
- http://home.earthlink.net/~jaymzh666/mss/

Thank you

CLIENT-SIDE FIXES

- `--clamp-mss-to-pmtu` switch for IPTables in Linux 2.4.x kernels
- `CLAMPMSS` setting of Roaring Penguin's PPPoE Software
- `mssfixup` command of ppp for FreeBSD
- Solaris kernel module

HOW TO DETECT

- snoop / tcpdump / ethereal
- At the client end-point:
  - Verify SYN + SYN ACK + ACK work
  - Request a non-existing page (404 ares are probably small)
- At gateway inbetween client and server:
  - Watch how icmp code 3 type 4 is ignored