Problems with the Firewall Model

1

What, Me Worry?

- In the early days of the firewall market they were simple devices that were therefore easy to implement and maintain
  - Today they are complex devices that are being aggressively marketted as a panacea in a $100m/year industry

2

Types of Problems

- Incoming traffic
- Data equivalence
- Proxy-versus-whatever
- Reliance on DNS
- Content access control
- Downloadable content
- Lack of “common sense” feedback

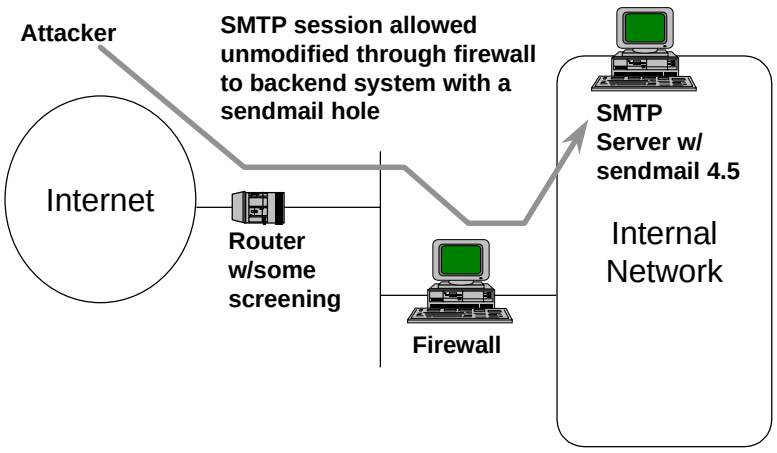
3

The Incoming Traffic Problem

- Data streams that are allowed in by firewalls may not be protected
- Some firewalls perform application specific security on data streams
  - Others do not
  - Sometimes you can’t
- Splits security between firewall and system on backend

4

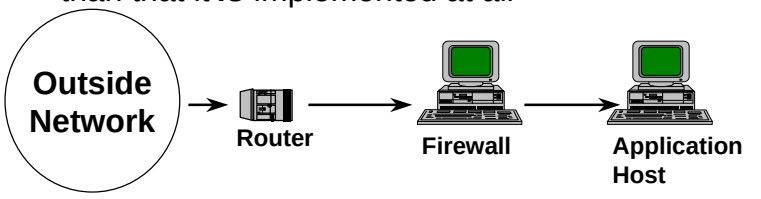
The Incoming Problem *(cont)*



5

Service Security

It is less important ***where*** security is implemented than that it ***is*** implemented at all



Router	Firewall	Application Host
Screening or network level security	Screening or network level security, possibly proxy services with additional security	Application specific configuration or host security

6

The Incoming Problem *(cont)*

- Upshot of the Incoming Traffic Problem is that firewalls are going to increasingly depend on host security at the backend
  - So why have the firewall at all?

7

Data Equivalence Problem

- Firewalls are not an effective *information control* technology
  - Covert Channel: a data transmission channel based on encoding data within another set of events
  - Overt Channel: a data transmission channel based on tunnelling one protocol within another
    - E.g.: TCP/IP over Email (don't laugh, I did it)

8

Data Equivalence Problem *(cont)*

- Eventually, if enough data is going back and forth through your firewall it is no longer a firewall

  …. it is a router

9

Data Equivalence Problem *(cont)*

- WWW is greatest example of data equivalence problem today
  - Many applications (soon to be many more) tunnel traffic over HTTP
  - PointCast includes HTTP tunnelling and automatic file/executable update
    - A firewall admin can't effectively block it

10

Proxy-Versus-Whatever

- Firewall market has grown from $1m/year to nearly $100m/year
  - Commoditization means vendors will be aggressive in searching for ways to discriminate their products
  - Mostly based on labelling: “XYZ sucks”
  - What are the technical differences?

11

Proxy-Versus-Whatever *(cont)*

- Proxy: O/S reassembles packets/TCPs and presents a stream to proxy application
  - Proxy *may* perform checks on the data crossing through it
  - Proxy *may* identify known attacks in data stream and block them

  … then again it may not

12

Proxy-Versus-Whatever *(cont)*

- Plug-board proxy
  - Reads data from one destination and copies it bit-for-bit to another
  - This is no different from a router filter
- Many organizations believe proxy is somehow better
  - Mandated use of plug-board proxy “more secure than router filtering”

13

Proxy-Versus-Whatever *(cont)*

- Stateful packet inspection
  - Engine in kernel space preserves state tables about traffic and sessions
  - Monitors traffic and updates state table
  - Permit or deny based on state and origin of traffic
  - Some application specific state hooks
  - No application specific security checks

14

Proxy-Versus-Whatever *(cont)*

- Firewalls are evolving into the same thing
- Market perception remains a big distinguisher
  - (Some of this is my fault)
- The open research question is mixing heuristic content filtering into proxy or whatever firewalls to analyse traffic

15

Reliance on DNS

- We know DNS has serious security problems
  - Most firewall vendors recommend not using DNS for security decisions: rely on IP address instead - like that's a lot harder to spoof :(
  - Firewalls still heavily reliant on DNS for operational purposes
    - Email routing
    - Web forwarding, etc.

16

Reliance on DNS *(cont)*

- Customers frequently rely on DNS within firewall rules

17

Content Access Control

- Java and ActiveX are here to stay
- Right now it is nearly impossible to meaningfully filter based on the type of content
  - E.g.: permit download and execution of Java from “trusted” sources while blocking “untrusted”
- What about plain old executables?

18

Content Access Control *(cont)*

- Many organizations attempt to block downloading executables from Internet
  - Time-wasting (Doom, Quake)
  - Viral
- Firewalls usually see such downloads as a compressed executable in a .zip file within a MIME document
  - No way to sort good from bad

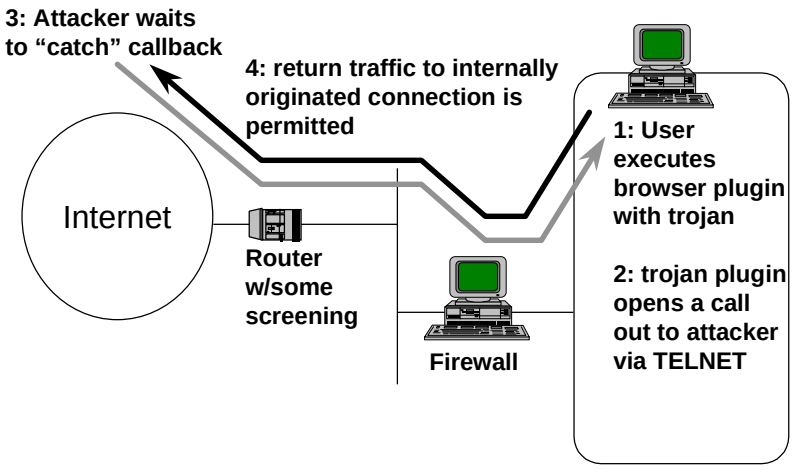
19

Downloadable Content

- Firewalls are becoming increasingly convenient about allowing outgoing access
  - Hackers have not yet developed and fielded download-trojans but they will eventually

20

Download Trojan



21

Downloadable Content *(cont)*

- Eventually if enough download content trojans are developed there will be a panic among firewall users

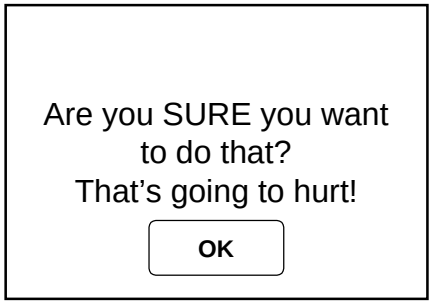
22

Lack of Feedback

- Many products do not provide “expert” feedback about what users are permitting or denying
  - 98% of users installing firewalls today have little or no security background

23

Lack of Feedback *(cont)*



24

Lack of Feedback *(cont)*

- Presently no firewall products are known to provide expert feedback
- Some come with pre-canned policies which is a good start
- Eventually we will evolve “best practices” for different categories of organizations’ firewalls

25

Summary

- Firewalls, in many ways, are losing their credibility as a defense
  - Incorrectly deployed
  - Aggressively marketted
  - Installed by clueless installers
  - Managed by unsophisticated customers
- What’s next?
  - Firewall effective design span is ending

26