Stupid Net Tricks

Bill Cheswick
Bell Laboratories, Lucent Tech.
ches@bell-labs.com

Some Topics

- Characteristics of the Net
- Security
  - Exponential tricks
  - Denial-of-service attacks (no time for it today)
- Names on the net
- Silicon snake oil - can the net replace the library?
- Web search engine games

The Net

- The Net probably started around 1991
  - We were just messing around before then
- Accessible to the common man
  - pick your port and go
- Fairly homogeneous
  - same OS
  - same hardware

Some net attributes: Performance

- We are currently all in one performance pot
- Slow at 3PM
- Lots of extra capacity for Saturday breakfast
- Isochronous data works only if the load is very light
  - net phone
  - Mbone

More attributes: It's easy to be anonymous

- Finland remailer is gone
- Easy to launder IP connections
- Thousands of volunteer sites
- National laws vary
- It takes a lot of effort to chase someone down

Security - Some lessons so far

- It is very hard to write software that is safe
- Simple is good, big is bad, but even the TCP discard service can be part of a successful attack
- The space of targets is fairly homogenous, and growing like crazy
- System administrators are clueless: they don't have time or tools to get a clue

Past targets

- sendmail
- anything using gets(2) or sprintf(2)
- password guessing and sniffing
- use and abuse of trust (rlogin, rsh)
- social engineering

The Security Arms Race

- We knew about sniffing in the early ‘80s
  - massive sniffing attacks in 1994 (1992?)
- We knew about sequence-guessing attacks in 1984
  - common in 1994
- We knew about IP spoofing and address-based authentication in the 80s
  - tools available in 1994

The “Latest”

- We’ve known about denial-of-service attacks since IP was invented
- Phrack and 2600 published SYN attack code this summer
  - we left it out of our book: no clear solution
- Denial-of-service is the final net problem

Attacks on the infrastructure

- Swamp routers
- Divert packet flows
- BGP4 hijacking?
- DNS cache contamination
- Swamp the technical support staff?

Infrastructure Problems Claffy’s Law

- How do you simulate the backbones?
- Can it become unstable?
  - seen it at Netcom and others
  - AT&T phone system had it on MLK
  - Net 18
- Shiller’s law: there is a constant amount of Clue on the net
  - Tracebacks require Clue.

Exponential tricks- Morris worm

- AT&T’s Intranet is larger than the net the worm attacked
- How would it spread?
  - CERN server bug (gets)?
  - Java?

Click *here* to infect your system.

Impact of future net attacks

- It would be much worse today
  - "space" is larger and more homogenous
  - the net is more important now
- Encryption ***is*** a munition
- Ping(1) is a munition!

The Traveling Program Problem

- Every feature can be a bug
  - CPU time
  - screen access
  - file system access
  - net access
  - email access
- Security requires discipline
  - market leaders have little discipline: other goals

Telescript

- Return receipt implemented?
- Program lifetime and "teleclicks"
  - "Mail not delivered: out of teleclicks"
- Teleclick regeneration
- A virus uses fewer clicks than a real mailing list

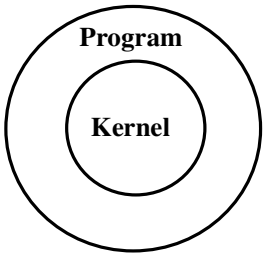
Java

- Derived from a set-top box project
  - Mid-course goal changes are a bad security sign
- I have no particular quarrel with the language
- Byte-code verifier is probably OK
  - Too fancy for my tastes
  - I solve the halting problem with ^C

Trust

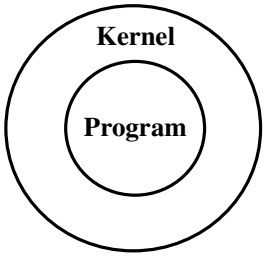
- I put my trust in these things
  - they are running as me
  - they act on my behalf
  - they have access to my files
- I prefer source code, please
- I vet and "decode" critical software, when I can

Where Do Programs Run?



This model is wrong

What it should be



Execution Environmental Choices

- Untrusted dirty machine, with firewall enforcing network restrictions
- Software containment
  - operating system
  - interpretive environment

Fears

- Average web users can't be expected to understand the security consequences of their actions.
- Applets make execution of alien programs routine
- There are a lot of aliens out there
- Jackpot - exponential growth into a space
- Theorem prover is complex security

Big Fears

- "Native Methods" aren't standardized
- All the security effort went into the language -- the environment is an afterthought
- A single security fault makes me suspect the approach
- We've had a number of very bad holes shown.

Java has let Eric Allman off the Hook

maybe

Stupid URLS

- http://www.
- file:/etc/passwd
- file:/dev/mouse
- ftp://localhost
- http://localhost:19
- http://sadflkajsdlfjalsdkjflksdjflkasdjflksdjflksdjflksdjflakjsdlkfajslkf...

Stupid Domain Names

- com.com, comdotcom.com, comdotcomdotcom.com
- macdonalds.com
- bell-labs.com, belllabs.com
- att.org, mci.org
- bell-labs.com.au?
- localhost.com

Stupid Web Tricks

- Secret pages
  - My photo album
  - Lost friends page
- http://counter.digits.com
- web awards - I haven't over 180 of them!
- Free search engines! Free indexing!
- On-line white pages
- Free home pages! (Netscape)

Stupid Web Tricks: Secret Web Pages

- My family photo albums
  - is it published?
  - chessecretword
- test.html and test/index.html

Stupid Search Engine Tricks- keywords

- They make reference librarians of us all
- Keyword searches can be very easy
- It's useful to have a unique name, like Avolio, Ranum, Bellovin, or Cheswick
- Lost friends page

Keyword ideas

- proprietary, top secret, company confidential
- d00dz, stup1d, warez, eleet, appz, hack3r
- rootkit
- "stupid net tricks"
- make your own: chesupdatetime

Snake Oil?

- The hype may have us firing librarians
- It is better to touch a book
- The net is the 1990 equivalent of filmstrips: you don't have to think!
- My stupid test: the web as a reference librarian
  - no netnews
  - no hard work

Web Questions

- How does cyanuric acid stabilize the chlorine in a swimming pool?
- What is the meaning and etymology of intinction?
- Who plays Heidi on Home Improvement?
- What is a "global learner?"
- What is the hyperfine interaction?
- How do you throw a "four seamer?"
- What are the hand signals used in baseball like?

More web questions

- What is "lumbago"?
- What is the current and historic price of cobalt oxide, used as a paint pigment?
- What do Mayan hieroglyphics look like?
- What wavelengths stimulate photochromism?
- What is the rate of colorblindness (bichromatism) in the general population?

Web Answers

- How does cyanuric acid stabilize the chlorine in a swimming pool? Unknown - Olin.
- What is the meaning and etymology of intinction? Found in a dictionary in Belgium
- Who plays Heidi on Home Improvement? Learned all about her.
- What is a "global learner?" No useful answers.
- What is the hyperfine interaction? Found: there are physics texts on the net.

More Web Answers

- How do you throw a "four seamer?" Discussed but not described.
- What are the hand signals used in baseball like? Discussed, but not answered.
- What is "lumbago"? Found in a dictionary.
- What is the current and historic price of cobalt oxide, used as a paint pigment? US Bureau of Mines had it.

More web Answers

- What do Mayan hieroglyphics look like? Found some excellent photos and descriptions.
- What wavelengths stimulate photochromism? Found at ppg.com.
- What is the rate of colorblindness (bichromatism) in the general population? Not found. Plenty of racial rants, though.

The Score

- 8 answered
- 4 not answered
- This was better than I expected
- Netnews would have yielded thousands of answers. Many would even be right
- Stupid research.

Web marketing tricks: top of the list

- hidden text
  - used cars used cars used cars used cars
  - same as background color
  - very tiny font
  - way below the first screen
- CONTENT="used cars used cars"
- Arms race: altavista.digital.com is more experienced than www.infoseek.com

Conclusions

- If you want to see some of these efforts, check out my web page.
- (Ask the search engine for the address)
- Keep experimenting!