Recent Security Threats & Vulnerabilities

Computer  security

Bob Cowles

bob.cowles@slac.stanford.edu

HEPiX, Spring 2006 – CASPUR

Work supported by U. S. Department of Energy contract DE-AC03-76SF00515

Skype Security

http://www.secdev.org/conf/skype_BHEU06.handout.pdf

http://www.networkworld.com/reviews/2005/121205-skype-test.html?page=1

- Extremely difficult to block
- Assessments show encryption is good
- No known backdoors (now US-based ?)
- No bandwidth concern for calls
- Supernode concerns
  - User agreement
  - Network impact
  - Not done for NAT-ed systems

Flu Pandemic

http://www.csoonline.com/read/020106/planning_pandemic.html

- Employees required to stay home – 10 days
- Need to know where critical employees live
- Be prepared for work from home
- Implications of home computers accessing critical applications on network

Port Knocking

http://www.portknocking.org/

- Server has no open ports but monitors connection attempts
- Client sends SYN (the “knock”)
- Ports must be “knocked” in proper sequence to be allowed application access
- The sequence can also be used a covert channel

Bumping Locks

http://www.toool.nl/bumping.pdf

- File the shoulder of a key
- Insert and use impact to jar pins
- Works best with expensive locks
- Works with “dimple” locks

Passwords

- POP3
  - kastela3, Romania2, ecdMJee4dD, baum2kid, ghbghb, 1@roma06, ubc789, 84relax, 4q63wbg, light2484, tDsfCxJs
- IMAP
  - Dadoes63, cal1pat0 dnow12i, Bruck5BD * hoFK87, 1etsg0, 21 filipch ckmckmir, obheyto, authum1808 R2gsumb0, rugbybear v3sm9r-EGEE, k7u0na Dad123Red345, 123456 Tuesday, ippin, nk0
- SMTP
  - lworib4u, iosara44, tuesday, **ha66il33**
- ICQ
  - gg147231, lalamisi xircom12, power0 123stell, B7A8
- FTP
  - !!

Passwords (http) - 2

- auradoo
- indovina
- mrakovnjacha
- 268jld823
- hepix
- ovidVM1
- sebastian
- 123pirla
- bazzy
- 637xre286
- argxb@$$
- e4077a97
- rl57ux27
- pfstef
- fireball
- frump
- 585tnc172
- anais
- admin
- cband
- tig4yet
- pincopallino
- JSAjNTU=
- st1mpy3483

Passwords (http) - 3

- d115872m
- Hammerhead
- S0ph0S
- 268jld823
- bravodb
- monkies
- fifth
- r0|01010
- figarek
- 844dbc784
- aK`5huHn
- e4077a97
- 1hepix
- sonia
- 637xre286
- fin_maggie
- frump
- elijah
- anais
- courier
- cband
- tig4yet
- pincopallino
- Mammoths

Instant Messaging

http://internet.newsforge.com/internet/05/10/07/1521221.shtml?tid=13

- OTR – variety of IM clients and platforms
- Encrypts data on IM channel – independent of central server (AIM, Gtalk, etc.)
- Authenticates IM partner
  - First communication – user/computer requires fingerprint verification
  - Subsequently – exchanges encryption key

Wireless Configuration Issues

http://www.theta44.org/karma/

- Client remembers previous networks
- Custom WAP can get client to associate
- T-mobile, linksys, netgear …..
- Works with Windows, MAC OS X

Stealth by Design malware

http://invisiblethings.org/

- Use private file infector (survive reboot)
- Inject thread into existing process
- Passive covert channels to avoid sockets
- Relocate into block of storage & unload
- Not detectable by normal rootkit detectors
- Coming soon to a PC near you ….

10 Best for Security

http://www.cio.com.au/index.php/id;1449363213;fp;16;fpid;0

- Assess your risk
- Define you boundaries
- Rely on multiple solutions
- Market your program
  - User awareness
- Take your measure
  - Define metrics and measure continually
- Set your standard
  - (NIST 800-xx, ISO 17799, etc._
- Train and mentor
- Use biometrics
- Avoid common mistakes
- Don’t forget Process Control Networks (PCN)

TAN Codes

http://www.theregister.co.uk/2006/03/24/trojan_captures_token/

- Thought to be safe against phishing – sent via SMS or paper mail
- Trojan-Spy.Win32.Bancos.pw intercepts https traffic to obtain passcode
- Displays error message to user – scammer can quickly enter passcode themselves

Computing Dragons

- DNA just a program
- Use computer to design (evolve) lizard DNA and tweak results based on simulations.
- Produce designer pets

- http://www.economist.com/science/displayStory.cfm?story_id=6740040

Computing Dragons

- DNA just a program
- Use computer to design (evolve) lizard DNA, test results based on simulations
- Produce designer pets
- http://www.economist.com/science/displayStory.cfm?story_id=6740040

April Fool