

Computer and Network Investigations

Steve Romig, The Ohio State University
September, 2005

Agenda

- Computer investigations
- Who we're investigating and what they are doing (briefly)
- Computer security (briefly)
- Current and future challenges and trends

My Background

- 12 years experience as a Unix/network sysadmin
- 10 years experience in computer security and especially incident response
- I've overseen 1000's of incidents involving compromised computers
- I've assisted on a number of criminal investigations

Who and What

Any Computer User

- Our suspect could be anyone who uses a computer to commit a crime
- Murder, fraud, drug transactions, extortion, insider trading...
- Disgruntled employees, upset spouses, roommates...

Miscreants

- Mostly teenage
- High interest in technology
- Plenty of free time
- Morals aren't well developed
- Little or no fear of being caught
- Skilled, but typically NOT geniuses

Miscreants' Motives

- They want to learn, experiment
- To gain social standing in the computer underground (by demonstrating skills or through barter)
- To support their passion (file sharing, denial of service, building a base...)

Crooks

- Motives: \$\$\$ for spam, denial of service, identity theft, espionage, harassment
- Botnets are a real business now - for spam, denial of service attacks especially (and building other botnets)
- They have more at risk, and are more motivated to use tools and techniques to hide their tracks than miscreants

Terrorism

- Terrorists certainly use computers
- They can certainly target physical infrastructure through the Internet
- Attacking the Internet itself may not be easy or attractive
 - No “BOOM”
 - The Internet is robust - global outages are hard

Computer Crime Prevention

Securing Computers

- Anti-virus, anti-spyware, and up to date
- “Personal” firewall
- “Personal” intrusion detection
- Good, changing passwords
- Keep up with patches
- Backups and disaster recovery

Securing Computers

- Increase log levels and retention
- “Lock it down” - often you need to “bump up” the security level by changing settings
- Apple’s MacOS X and Microsoft’s Windows XP SP2 do a lot of this by default, which is GREAT

Securing Networks

- Firewalls, VPN
- Network Access Control (authorized users, secured computers, including wireless)
- Intrusion detection and prevention
- Vulnerability scanning and remediation
- Think long and hard about whether and how to provide remote access!!

Securing Organizations

- Policies - acceptable use, privacy, PDAs and laptops, etc.
- Procedures - incident response, patching, host and network configuration
- Awareness, education, training

Securing People

- Password security - use complex passwords, change them regularly
- Train against social engineering
- Teach about phishing, identity theft, attacks through email and IM
- This is the hardest nut to crack...

Computer Crime Investigation

Forensics Defined

- “Forensic” means “of or pertaining to the law”.
- Forensic Anthropology: applying the science and techniques of anthropology to a criminal investigation
- Computer Forensics, Network Forensics, Software Forensics...

Computer Forensics

- Looking at what's on the computer: contents of the disks, programs running, active network connections, contents of memory, log files
- The eternal question: dead or alive?

Computer Forensics

- We don't want to risk corrupting the contents of the disk, so we turn the system off and image the drives. But then we lose the "live" state (memory, programs, network connections).
- If we need the "live" state, we need to use the computer, but we risk corrupting the disk contents.

Computer Forensics

- What's the right answer? Whatever you need to do for the situation at hand.
- This can be tough to answer for a new investigation where you don't know what to expect.

Common Tools

- Guidance Software's EnCase, Brian Carrier's TASK (aka Autopsy, aka SleuthKit), FTK, SMART
- Special purpose tools: Scalpel, Foremost, others
- OnLineDFS, RootKitRevealer, Microsoft's Malicious Software Removal Tool, sysinternals.com, BlackLight

Network Forensics

- There's potentially a wealth of evidence available from the network
- “Transaction” logs, such as Cisco NetFlow or Argus logs
- Packet captures
- Authentication, firewall, DHCP, and router logs.

Common Tools

- Cisco NetFlow, flow-tools, nprobe
- Argus
- Ethereal, tcpdump
- Various efforts at integrated log analysis

Software Forensics

- Given a piece of software, what does it do, and who wrote it?
- Static analysis: examine the software without running it
- Dynamic analysis: run it in a test environment and see what it does

Software Forensics

- Some parts of static analysis are easy (get the strings, symbol table, etc.)
- The job gets progressively harder: disassemble, decompile...
- Made difficult by packers, encoders, encryption (UPX, burneye, morphine)
- Tools: IDA-pro

Software Forensics

- Dynamic analysis: you want a safe environment where you can reproduce your results
- VMWare is a great environment for running malware. You can set up fake DNS, web and etc.
- Note that the malware may not run correctly in the test environment (burneye)

Incident Response vs. Crime Investigation

- Goals of incident response include determining: how we were compromised, what other systems were affected or could be affected, how do we detect this better, how do we prevent this more effectively, how do we clean up...
- Facilitating criminal investigation might not be on the radar...

Anatomy of a Security Incident

Terminology

- Scan: probing through the network to find vulnerable systems
- Vulnerability: a weakness that might lead to something “bad”, often found by analyzing patches
- Exploit: using a vulnerability to gain access to a system

Terminology

- Backdoor: intruders often insert hidden entrances to your system
- Rootkit: tools used to hide an intruder's presence
- Virus, worm, trojan: old names for different sorts of “bad software”. These have all sort of blended together

Terminology

- Malware: new name for viruses, worms, adware, spyware, trojans...
- Adware, spyware: “commercial” software that invades your privacy, displays pop-ups and undermines your security

Terminology

- Bot: (short for robot) a computer running software that makes it part of a botnet which allows others to control it
- Botnet: a network of 10's, 100's or 10,000's of bots that can be used for scanning, exploiting, denial of service attacks, spamming, file sharing and so on

Rootkits

Rootkits

- The term “rootkit” refers to software that is used to hide an intruders tracks on a computer.
- Rootkits sometimes include other functionality, like setting up backdoor access.
- Rootkits have been around since 1995 or so.

Hacker Defender

- Hacker Defender is a Windows kernel rootkit.
- HD allows you to hide files, processes, services, drivers, registry keys, and open ports.
- HD creates a backdoor that piggy-backs on existing network services, like web or email.
- HD creates a powerful proxy services.

Hacker Defender

- HD is being used in the wild.
- It can be detected, though it is “difficult”.
- For this and other rootkits, see www.rootkit.com.

Botnets

Botnets

- A “bot” is an IRC or MUD (or, these days, also chat room) user which is actually a program.
- There are good and bad uses for bots.
- A “botnet” is a group of bots that can be controlled by a single person or group.

Botnets

- Botnets have been around since the early 90's, at least.
- Today, botnets are a *huge* problem.
- At any given time, there are thousands of botnets on the Internet, with tens or hundreds of thousands of bots on them (at least!)

Botnets

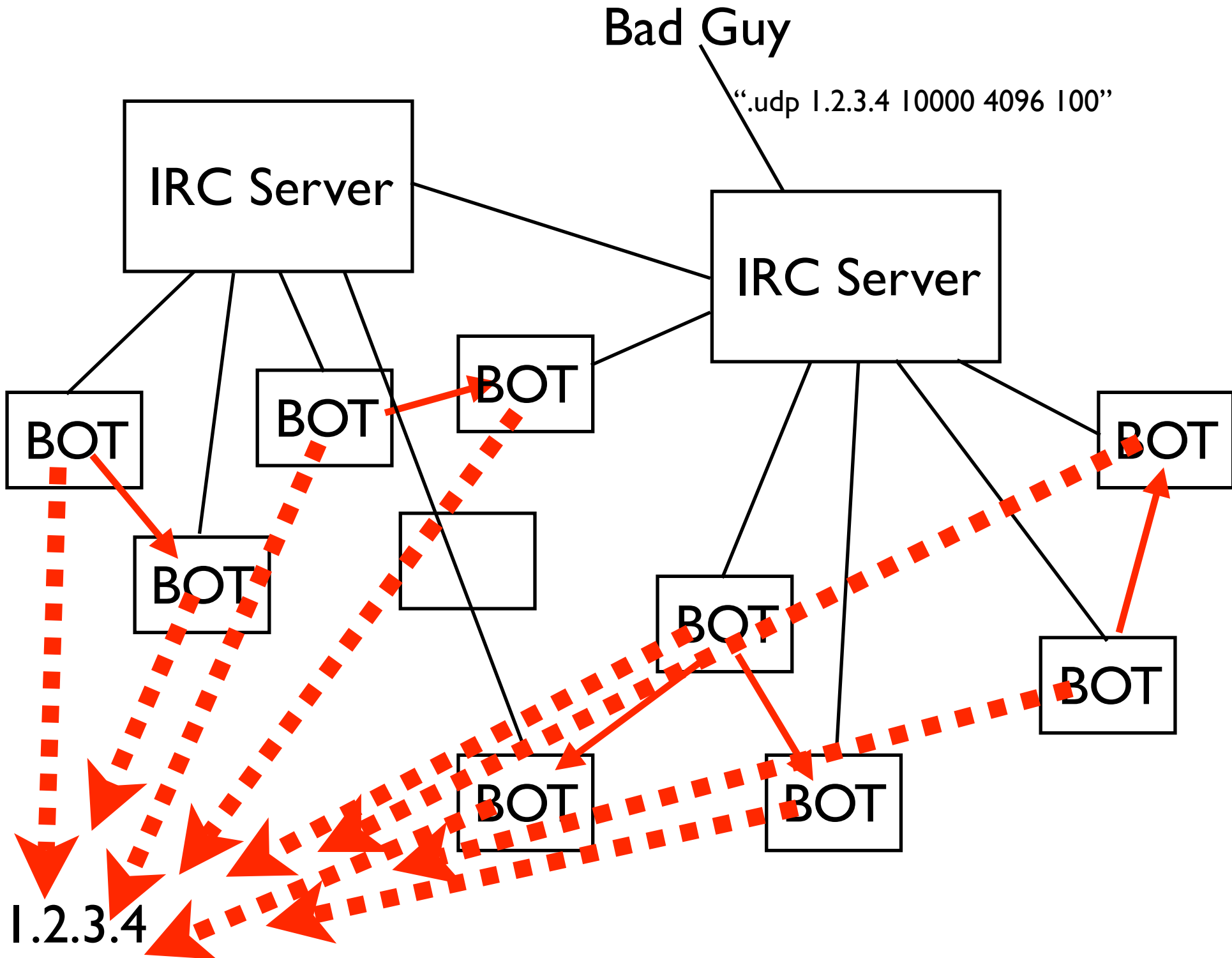
- Botnets can be used for many things:
 - File sharing
 - Denial of service attacks
 - Spam
 - Scan and exploit attacks to build botnets

Recent bots can...

- Install, open, execute files
- Update themselves with new versions
- Start simple denial of service attacks
- Create backdoors
- Create proxies

Recent bots can...

- Forward email
- Log keystrokes
- Scan for software keys, passwords, credit card numbers...
- Spread in numerous ways: missing/weak passwords, open shares, bugs, backdoors from other malware (e.g. Bagle, MyDoom)



Sniffing and Keystroke Logging

Keystroke Logging

- Hardware
 - Hard to spot
 - Have to install, retrieve in person
- Software
 - Most bots, much of the recent malware includes keystroke loggers

Sniffing Network Traffic

- This was common back in the 90's, not so much now that we encrypt lots of traffic and use switches rather than hubs (not that that does much to secure anything).
- This seems to be making at least a minor comeback.

Replace the Client

- If the intruder can replace the client software used for remote access, they can contrive to grab passwords.
- Example: replace the ssh client with a version that grabs host, user and password. Some will also grab secret keys and their passphrases!

Replace the Client

- If someone logs into my system from a compromised system, then their account is known to the intruder.
- The intruder will use this to access my system, elevate privs and replace the client.
- Etc. They can capture very large numbers of accounts for many systems very quickly.

Sniffing

- Illustrates the need for better authentication (two factor or one time), especially for remote access.
- Remote access systems should be isolated from critical systems, though that's often what you are trying to reach remotely.

But even then...

- Some intruders are using tools that allow them to take control of a session after the user has already logged in using two-factor authentication.

Metasploit

Metasploit

- An open-source exploit development framework.
- Useful for vulnerability testing
- Designed for exploit development

Metasploit

- Multiple interfaces: msfconsole, msfweb, msfcli
- Could be adapted for IM, IRC with groups of people

Metasploit

- Choose an exploit
- Set global and exploit specific options
- Choose a payload
- Exploit away

Developing Exploits

- Can also be used to develop exploits (see “Sockets, Shellcode, Porting and Coding” chapter 12, by James Foster and Mike Price)
- Metasploit doesn't remove the need for poking around, knowing what you are doing
- But it automates some of the tedious parts and lowers the bar for everyone once new exploits are integrated into Metasploit

Developing Exploits

- Pick an attack vector, get the offset (e.g. a new buffer overflow in IIS)
- Pick a control vector (return to stack, DLL trampoline)
- Trampoline technique is harder, but see the Metasploit Opcode Database

Developing Exploits

- Find “bad” characters
- Determine your Nop sled
 - Metasploit’s Nop generators
- Determine your payload
- Determine your encoding

Developing Exploits

- msfpayload
 - 65 payloads for 9 operating systems on 4 architectures
 - bind, reverse, execute, VNC, meterpreter

Developing Exploits

- Determine your encoding
 - msfencode
 - Bad characters?
 - Output format (C, Perl, etc)

Meterpreter

- A dynamically extendable, in-memory command interpreter (read: “powerful and stealthy exploit payload”)
- Solves 3 problems: avoid known shells, get around chroot, ability to do “what you want”
- Modules: Process, Fs, Net, Sys, plus whatever you write

Redirection

Proxies

- Most bots include proxies that allow miscreants to “bounce” connections through the machine
- Sweden to Korea to France to Argentina to Cleveland

Onion Routers

- TOR (The Onion Router) makes it easy to use proxies in a distributed network of servers
- Supports encryption
- Supports anonymous services

Trends and Challenges

Increasing Incidents

1994	2
1995	11
1996	102
1997	308
1998	348
...	...
2002	1145
2003	786/4039
2004	7,686/2,484

Increasing Automation

- Easy for them to infect 100's of thousands of hosts
- 200,000 hosts picking up agobot from OSU in 3 days...
- On the other hand, we're more automated also

Increasing Sophistication

- Better rootkits (HackerDefender), backdoors
- Encryption
- Better exploit development tools and books
- Tools, books are enabling technologies that let more people enter the “game”

Increasing Variations

- Agobot - hundreds of versions, hard to analyze them all
- If you don't have time to really analyze them, how do you know what they do, how to clean it up, etc?
- Morphine makes it possible to create unique versions for every compromised system

Increased Economic Incentives

- Bots
- Spam
- Industrial espionage
- Identity theft
- Extortion, denial of service

The Stakes Are Higher

- The Internet isn't just a "cool toy" any more
- Our y2k survival plan: use paper forms
- In 2004, the paper forms don't exist
- The Internet is a must-have: distance education, business processes, communication...

Challenges

- Securing user-owned computers and keeping the “bad” ones off our net (Network Access Control)
- Education people so they don't do Stupid Things
- Figuring out how to provide remote access in a “safe” way

Resources

Resources

- www.net.ohio-state.edu/security/talks.shtml
- romig.1@osu.edu

Start Here

- Secrets & Lies
 - Schneier

Firewalls

- Internet Firewalls
 - Cheswick and Bellovin
- Building Internet Firewalls
 - Chapman and Zwicky

Unix

- Practical Unix Security
 - Garfinkle and Spafford

Windows

- Microsoft Windows 2000 Security Handbook
 - Schmidt
- NSA Security Guides
 - www.nsa.gov
- SANS Security Guides
 - www.sans.org

Miscellaneous

- Applied Cryptography
 - Schneier
- Incident Response
 - Van Wyk
- Building Secure Software
 - Viega, McGraw

Web sites, mailing lists

- www.securityfocus.com
 - bugtraq
 - focus-*
 - forensics
 - search papers, tools
- cftt@yahogroups.com
- SANS
 - www.sans.org

Web sites, mailing lists

- CERT
 - Computer Emergency Response Team
 - www.cert.org
- FIRST
 - Forum of Incident Response and Security Teams
 - www.first.org

Tools

- Forensics
 - Encase – www.guidancesoftware.com
 - TCT – www.fish.com
 - Task – www.atstake.com
 - www.sysinternals.com