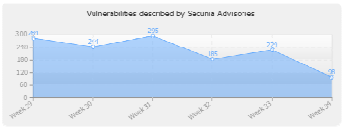
Computer Security Overview

Slides for CSC 495 / CSC 680
August 25, 2010

Scope of Problem

- Stats from the book:
  - Cybercrime proceeds in 2004 were $105 billion
  - Dealing with viruses and security problems cost businesses $67.2 billion in 2005
- Recent information on reported vulnerabilities:



Around 200 new vulnerabilities found every week!!!

What Are the Targets?

10 year ago: Targets were primarily big, visible servers

Today: Targets are individual PCs – individual, home, work desktops, …

Why? Because they can be harnessed into large, distributed "botnets" that are used for distributed attacks, spamming, and hosting illegal content

Botnets can have millions of hosts under the control of the botnet master…

UPI.com
100 YEARS OF JOURNALISTIC EXCELLENCE

Virus strikes 15 million PCs

Published: Jan. 26, 2009 at 10:34 AM

WASHINGTON, Jan. 26 (UPI) -- A virulent computer virus has infected as many as 15 million computers around the world so far, according to various estimates.

The virus -- a self-replicating computer worm known as Downadup, Conficker or Kido -- spreads across computer networks using Microsoft Windows software which have not been patched or updated properly. Microsoft issued a patch that fixes the vulnerability the virus exploits last October.

The Independent on Sunday newspaper said in London at the weekend that more than 3,000 British organizations, including hospitals and the Ministry of Defense, have been hit by the virus.

Categories of Security Problems

- Book gives six categories of security problems:
  1. Vulnerable Programs
  2. Malicious Programs
  3. Misconfigured Programs
  4. Social Engineering
  5. Physical Theft
  6. Electronic Eavesdropping

Note: There are certainly other problems/threats (such as environmental hazards, attacks through hardware, careless users, …), but these six were the main ones considered as Trusted Computing was developed

Categories of Security Problems

1. Vulnerable Programs

- By far the biggest security problem is accidentally vulnerable programs
- How can programs be vulnerable?
  1. Bad design
     - Sensitive information communicated in cleartext (telnet, ftp, …)
     - Using unverified information for authentication (rlogin, …)
  2. Bugs in code
     - Incorrect memory management
       - Buffer overflows, denial of service issues, …
     - Incomplete / improper input checking (input sanitization)
       - SQL injection, cross site scripting, …
     - Unlimited ways to have bugs!

Vulnerable Programs

The Biggie: Buffer Overflows

- Variable size data is put into fixed-size storage allocation
  - Ex: Read user input into a 10 char array, but user types 20 chars
  - What happens to extra 10 chars?
    - C, C++, Assembly: Happily write over whatever happens to be in memory after array
    - Java, C#, Perl, PHP, …: Program throws an exception (and probably stops/crashes)
- Some history:
  - Recognized as far back as 1972
  - First major use: Morris worm, 1988 – bug in "fingerd"
  - Biggest publicity: "Stack Smashing for Fun and Profit" – 1996
  - Interesting exploit: Used on X-Box game to run unauthorized software (X-Box Linux)

So 20 years later this isn't a problem, right??? …. Unfortunately, no….

Found: 3674 Secunia Security Advisories, displaying 1-25

Sort by: Match, Title, Date

Title	Date
Cisco WebEx Player ARF Parsing Buffer Overflow Vulnerability	2010-08-24
Quagga BGP Daemon Denial of Service and Buffer Overflow Vulnerabilities	2010-08-24
Wyse ThinOS LPD Service Buffer Overflow	2010-08-19
A-PDF WAV to MP3 Converter File Processing Buffer Overflow Vulnerability	2010-08-18
Explorer Suite CFF Explorer Name Identifier Buffer Overflow Vulnerability	2010-08-17
MUSE Playlist Processing Buffer Overflow Vulnerabilities	2010-08-17
Novell iPrint Server Buffer Overflow Vulnerability	2010-08-13
SigCast WebPlayer ActiveX Control "SetSopAddress" Buffer Overflow Vulnerability	2010-08-11
Microsoft Windows Movie Maker String Parsing Buffer Overflow	2010-08-10
Microsoft Windows MPEG Layer-3 Audio Decoder Buffer Overflow	2010-08-10
Microsoft Office Excel SXDB Record Parsing Buffer Overflow	2010-08-10
Amlib NetOpacs "webquery.dll" Buffer Overflow Vulnerability	2010-08-06
Microsoft Windows win32k.sys Driver "CreatePalette()" Buffer Overflow	2010-08-06
Invensys Wonderware ConfigurationAccessComponent ActiveX Control Buffer Overflow	2010-08-05
BarCodeWiz Barcode "LoadProperties()" Buffer Overflow Vulnerability	2010-08-02
MapServer "msTmpFile()" Buffer Overflow Vulnerability	2010-08-02
socat Command Line Argument Buffer Overflow Vulnerability	2010-08-02
SigPlus Pro ActiveX Control "LCDWriteString()" Method Buffer Overflow	2010-08-02
Xion Audio Player Playlist File Parsing Buffer Overflow	2010-08-02
UPlusFtp Server Web Interface Buffer Overflow Vulnerability	2010-07-29
QuickTime Player Streaming Debug Error Logging Buffer Overflow	2010-07-26
HP OpenView Network Node Manager "nnmRptConfig" Buffer Overflow	2010-07-22
QQPlayer Playlist Processing Buffer Overflow Vulnerabilities	2010-07-21
HP OpenView Network Node Manager "execvp_nc()" Buffer Overflow	2010-07-21
Apple iTunes "ftpc:" Handling Buffer Overflow	2010-07-20

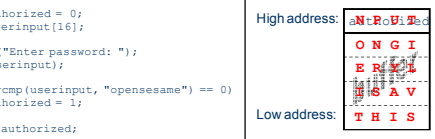
Next 25 matches >>

Results of a recent search for "buffer overflow" in a database of security advisories

Vulnerable Programs

A Simple Buffer Overflow

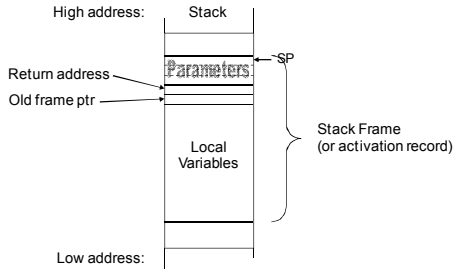
```
int checkauth()
{
    int authorized = 0;
    char userinput[16];

    printf("Enter password: ");
    gets(userinput);

    if (strcmp(userinput, "opensesame") == 0)
        authorized = 1;

    return authorized;
}
```



- Bad code:
  - Idea: Set auth flag only if user enters the correct password
  - Works fine if nothing unusual entered
  - But: What happens if more than 16 characters are entered?

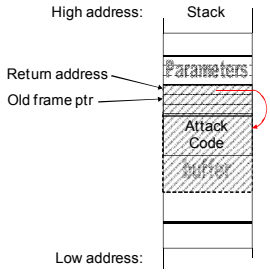
Vulnerable Programs

"Stack Smashing" Illustration



Vulnerable Programs

"Stack Smashing" Illustration



- Input from user contains machine code
- Keeps writing past end of buffer
- Overwrites return address with pointer to user-produced code

Result: User can execute whatever code they want!!!

Note: "Data" used as transport for executable statements!

Categories of Security Problems

1. Vulnerable Programs

- Will we ever eliminate bugs?
  - Not until we get perfect programmers… (so no, we won't)
- How prevalent are these bugs?
  - A large scale study showed that a typical large system will have on average one security-sensitive bug per 1,000 lines of code
  - A modern system like a Windows PC has over 100 million lines of code
  - So… expect *100,000 security-sensitive bugs*?!?!?

Vulnerable Programs

What happens when systems are full of bugs and the bad guys know it?

InformationWeek

Unpatched PC "Survival Time" Just 16 Minutes

The average unpatched Windows PC lasts less than 20 minutes on the Internet before it's compromised, according to data from the Internet Storm Center.

By Gregg Keizer, TechWeb News, InternetWeek
Aug. 18, 2004
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=29106061

The average unpatched Windows PC lasts less than 20 minutes on the Internet before it's compromised, according to data from the Internet Storm Center.

Part of the SANS Institute, the Storm Center calculated the average "lifespan" of an unpatched, unprotected PC by listening to IP addresses and tallying the number of probes run against them.

"If you are assuming that most of these reports are generated by worms that attempt to propagate, an unpatched system would be infected by such a probe," the Storm Center said in a statement.

In June 2003, the "survival time" of an unpatched PC was approximately 40 minutes. As of Wednesday, the average was less than half that: only 16 minutes.

Note: Not as big a problem after XP SP2 (and Vista)

Categories of Security Problems

2. Malicious Programs

- Some programs intentionally do bad things!
  - Viruses, worms, spyware, …
- How do these get on your system?
  - One way: By first exploiting a vulnerable program
  - Another way: See category 4, "Social Engineering"
    - Can pretend to be a game, cool app, or even an anti-virus program!
- Often take efforts to conceal their presence
  - Can't "uninstall"
  - Can't see processes or files
  - Sometimes called a "rootkit"

Categories of Security Problems

2. Malicious Programs – Current Example

TECHWORLD

Fake antivirus software is most costly security scam of 2010

McAfee reports 400% increase in reported incidents

By Carrie-Ann Skinner | PC Advisor | Published: 12:20 GMT, 11 March 10

Fake antivirus programs that encourage web users to part with their hard-earned cash and download hoax security software is likely to be the most costly scam of 2010, says McAfee.

According to the security firm, cybercriminals make upwards of $300m from conning web users worldwide into downloading scareware.

The security firm also said it had seen a 660 percent rise in scareware over the past two years, and a 400 percent increase in reported incidents in the last 12 months.

"Even the savviest of computer users fall victim to online threats because cybercriminals have become so sophisticated," said Jeff Green, senior vice president of McAfee Labs.

The scareware scam starts with a pop-up that claims the web user's PC is infected with malware and then prompts the user to purchase the fake 'security software' which is actually malware in disguise. Cybercriminals also obtain the user's computer and bank details.

Categories of Security Problems

3. Misconfigured Programs

- How can a program or device be misconfigured?
  - User mistakes – particularly with very complex configurations
    - sendmail was notorious for this
  - Insecure default settings
    - Wireless routers distributed with security disabled
    - Network servers by default serving the world
  - Predictable default passwords
    - DSL routers
    - Database systems
    - System maintenance passwords
- Developers are much smarter about this now than they used to be

Categories of Security Problems

4. Social Engineering

- Basically: Talking people into giving information or doing something that they shouldn't!
- Some common types (other than talking people out of info):
  - Phishing: Email that claims to be from a legitimate company (bank, etc.), but following links takes you to a web site run by attacker
    - Big warning flag: Web site URL uses IP address rather than name
    - Protection: Make sure SSL is on and site verified – or don't follow email links!
  - Pharming: Similar to phishing, but with legitimate URLs – accompanied by DNS hijacking to direct to attacker's site
- Technical solutions can help with awareness, but can't cure stupidity…

Categories of Security Problems

4. Social Engineering

Some have turned this into a game…

What's your take: Is this ethical?

NETWORKWORLD

This story appeared on Network World at http://www.networkworld.com/news/2010/072210-defcon-social-engineering-contest-stirs.html

Defcon social engineering contest stirs concerns

Challenge that requires contests to target companies and obtain information is making some organizations uneasy
By Joan Goodchild, CSO
July 21, 2010 08:11 PM ET

A capture-the-flag-style competition slated to take place at Defcon later this month has raised eyebrows at a number of companies who are concerned they will be embarrassed or negatively impacted in some way. CSO first reported the CTF challenge earlier this month in Defcon contest to spotlight social engineering. The challenge asks contestants to collect information about a "target" company, which they are assigned to by contest coordinators at the web site social-engineer.org.

"In the excitement some have expressed concern that contestants might act improperly or that government, companies or individuals might be adversely impacted. We want to put these concerns to rest," officials with social-engineer.org said in a release, reacting to the fervor over the event.

Chris Hadnagy, one of the site's founders, said he decided to issue the statement after hearing that due to the fear generated, many contestants who work for larger corporations were threatened with termination if they participated in the CTF.

Categories of Security Problems

5. Physical Theft

- Particularly laptops, netbooks, portable storage, …
  - But not entirely! August 27, 2003, thieves gave false names and got into a top-security mainframe room at Sydney International Airport – and *crated up and stole a mainframe*!
- Some countermeasures:
  - BIOS password/lock
    - OK to protect against casual access, but not against actual theft
  - Encrypted disk
    - Enter password at boot, or rely on bootstrap to supply (e.g., Microsoft's Bitlocker)
  - Theft recovery systems
    - Might help retrieve hardware and/or prosecute, but might be too late for sensitive information!

Categories of Security Problems

6. Electronic Eavesdropping

- This is exactly what cryptography was originally designed for
- Big remaining issue: Key management
  - How/where are keys stored?
  - Are they backed up?
  - Does a user have to provide a passphrase?
  - How often are they changed?

Categories of Security Problems

Homework Exercise!

- Teams of students will be given a particular category, and should find a news story about a real-world security incident in that category
- Next Monday: Each team will give a brief (3-5 minute) synopsis of your news story
  - Can use electronic displays
    - Either PPT with main points or can just pull up the story online
  - Can have handouts
    - Send them to me before class and I'll print and copy

How Can a TPM Help?

- Focus on most valuable items (cryptographic keys, integrity measurements) and limit functionality so device can be verified
  - Important: Valuable items remain secure even if rest of system is compromised
- Some TPM design goals:
  - Private keys can't be stolen or given away (protect against stupidity!)
  - Malicious code is always detected
  - Malicious code can be kept from using keys (note: different than copying)
  - Keys not easily available even to a physical attacker (tamper resistant)

How Can a TPM Help?

Why is malicious code detection so hard without hardware changes?

Blue Pill Prototype Creates 100% Undetectable Malware

By: Ryan Naraine
2006-06-28
Article Rating: ★★★☆☆ / 9
Share This Article

There are user comments on this Windows & Interoperability story.

A security researcher with expertise in rootkits has created a working prototype of new technology that is capable of creating undetectable malware, even on Windows Vista x64 systems.

A security researcher with expertise in rootkits has built a working prototype of new technology that is capable of creating malware that remains "100 percent undetectable," even on Windows Vista x64 systems.

Joanna Rutkowska, a stealth malware researcher at Singapore-based IT security firm COSEINC, says the new Blue Pill concept uses AMDs SVM/Pacifica virtualization technology to create an ultra-thin hypervisor that takes complete control of the underlying operating system.

Rutkowska plans to discuss the idea and demonstrate a working prototype for Windows Vista x64 at the SyScan Conference in Singapore on July 21 and at the Black Hat Briefings in Las Vegas on Aug. 3.

The Black Hat presentation will occur on the same day Microsoft is scheduled to show off some of the key security features and functionality being fitted into Vista.

Rutkowska said the presentation will deal with a "generic method" of inserting arbitrary code into the Vista Beta 2 kernel (x64 edition) without relying on any implementation bug.

Rate This Article:
Poor Best
Rate
e-mail
PDF Version
Print

How Can a TPM Help?

TPM Capabilities

- Some TPM capabilities:
  - Public key authentication (keys generated and usable only inside TPM)
  - Integrity measurement
    - Uses "Platform Configuration Registers" (PCRs) that contain measurements of machine configuration and what software is running – can't be faked to show a specific value!
    - Note that even a virtual machine hypervisor would not go undetected
    - Secrets can be "sealed" so that they are only available under certain PCR values
  - Attestation (assurance to remote parties)

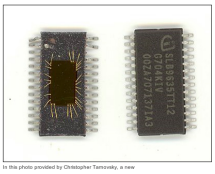
Does a TPM Stop a Dedicated Attacker?

No, nothing is perfect….

Security chip that does encryption in PCs hacked

By JORDAN ROBERTSON AP Technology Writer

STORY



In this photo provided by Christopher Tarnovsky, a new unopened Infineon TPM part, right, alongside a part opened by Tarnovsky are shown.

SAN FRANCISCO (AP) - Deep inside millions of computers is a digital Fort Knox, a special chip with the locks to highly guarded secrets, including classified government reports and confidential business plans. Now a former U.S. Army computer-security specialist has devised a way to break those locks.

The attack can force heavily secured computers to spill documents that likely were presumed to be safe. This discovery shows one way that spies and other richly financed attackers can acquire military and trade secrets, and comes as worries

Privacy Issues with TPMs

TPMs contain unique keys that can allow tracking and correlation of activities.

Does this concern people? *Yes*!

Was an embarrassing debacle when Intel put in unique processor serial numbers in the Pentium III processor

- Intel removed this feature after massive protests and the "Big Brother Inside" campaign.

TPM designers were (very!) sensitive to this, so included privacy features:

- Can create multiple "pseudonym" keys that are used in different interactions – however are linkable through a "Privacy CA"
- Version 1.2 introduced "Direct Anonymous Attestation"

GREENSBORO

Some Interesting Privacy Quotes

... or: Not everyone feels the same way about your privacy

- You already have zero privacy. Get over it.
  - Scott McNealy, CEO of Sun Microsystems
- We know roughly who you are, roughly what you care about, roughly who your friends are.
  - Eric Schmidt, CEO of Google
- A lot of companies would be trapped by the conventions and their legacies of what they've built, doing a privacy change for 350 million users is not the kind of thing that a lot of companies would do. But we viewed that as a really important thing … and decided that these would be the social norms now and we just went for it.
  - Mark Zuckerberg, Facebook founder, on Facebook's privacy changes that opened up previously-private information of its users.

GREENSBORO

Discussion Topic

Reflections on Trusting Trust

- For discussion:
  - Ken Thompson's Turing Award Lecture: "*Reflections on Trusting Trust*"
  - 20-year follow up by Diomidis Spinellis: "*Reflections on Trusting Trust Revisited*"
- Questions:
  - What do you trust in a computer system?
  - How can your level of trust be raised?

GREENSBORO