Internet Security

Nan Niu (nn@cs.toronto.edu)
CSC309 -- Summer 2008

In the News

Articles in the news from the past month

- "Security shockers: 75% of US bank websites have flaws"
- "Blank robbers swipe 3,000 'fraud-proof' UK passports"
- "Korean load sharks feed on hacked data"
- "Worms spread via spam on Facebook and MySpace"
- "Beloved websites riddled with crimeware"
- "Google gives GMail always-on encryption"

http://www.theregister.co.uk

New Targets of 2007

- Cyber criminals and cyber spies have shifted their focus again
  - Facing real improvements in system and network security
- The attackers now have two new targets
  - users who are easily misled
  - custom-built applications
- Next, 4 exploits scenarios…
  - Reported by SANS (SysAdmin, Audit, Network, Security), http://www.sans.org

Scenario 1

- The Chief Information Security Officer of a medium sized, but sensitive, federal agency learned that his computer was sending data to computers in China.
- He had been the victim of a new type of spear phishing attack highlighted in this year's Top 20.
- Once they got inside, the attackers had freedom of action to use his personal computer as a tunnel into his agency's systems.

Scenario 2

- Hundreds of senior federal officials and business executives visited a political think-tank website that had been infected and caused their computers to become zombies.
- Keystroke loggers, placed on their computers by the criminals (or nation-state), captured their user names and passwords when their stock trading accounts and their employers computers, and sent the data to computers in different countries.
- Bank balances were depleted; stock accounts lost money; servers inside their organizations were compromised and sensitive data was copied and sent to outsiders.
- Back doors were placed on some of those computers are still there.

Scenario 3

- A hospital's website was compromised because a Web developer made a programming error.
- Sensitive patient records were taken.
- When the criminals proved they had the data, the hospital had to choose between paying extortion or allowing their patients health records to be spread all over the Internet.

Scenario 4

- A teenager visits a website that exploits the old version of her media player that she never updated.
- She didn't do anything but visit the site; the video started up automatically when the page opened.
- The attackers put a keystroke logger on her computer.
- Her father used the same computer to access the family bank account.
- The attackers got his user name and password and emptied his bank account (the bank reimbursed him).
- US law enforcement officials followed the money and found that it ended up in an account being used by a terrorist group that recruits suicide bombers.

7

Top 20 Internet Security Risks of 2007 Reported by SANS

- Client-side Vulnerability in:
  - C1. Web Browsers
  - C2. Office Software
  - C3. Email Client
  - C4. Media Players
- Server-side Vulnerability in:
  - S1. Web Applications
  - S2. Windows Services
  - S3. Unix and Mac OS Services
  - S4. Backup Software
  - S5. Anti-virus Software
  - S6. Management Servers
  - S7. Database Software

8

Top 20 of 2007 (Cont'd)

- Security Policy and Personnel:
  - H1. Excessive User Rights and Unauthorized Devices
  - H2. Phishing/Spear Phishing
  - H3. Unencrypted Laptops and Removable Media
- Application Abuse:
  - A1. Instant Messaging
  - A2. Peer-to-peer Programs
- Network Devices:
  - N1. VoIP Servers and Phones
- Zero Day Attacks:
  - Z1. Zero Day Attacks

9

C1. Web Browsers

- Microsoft Internet Explorer (IE)
  - World's most popular Web browser
  - Un-patched or older versions of IE: memory corruption, spoofing and execution of arbitrary scripts or code
  - The most critical issue: allowing remote code execution without any user interaction when a user visits a malicious Web page or reads a malicious email
  - IE has been leveraged to exploit vulnerabilities in other core Windows components such as HTML Help and the Graphics Rendering Engine and hundreds of vulnerabilities in ActiveX controls installed by Microsoft and other software vendors
- Mozilla Firefox, the 2nd most popular browser, has its fair share of vulnerabilities too

10

C1. Web Browsers (Cont'd)

- Increase in the number of Browser Helper Object and third-party plug-ins
  - Inspired by the offering of rich content in websites
  - Used to access various MIME file types (multimedia documents)
  - Plug-ins often support client-side Web scripting languages
    - Macromedia Flash or Shockware
  - Installed (semi-)transparently by a website
- Users may not even be aware that an at-risk helper object or plug-in is installed on his/her system
- The additional plug-ins introduce more avenues for hackers to exploit and compromise users' computers while visiting malicious websites

11

S1. Web Applications

- Web application/framework security defects
  - Ranging from insufficient validation to application logic errors
  - Frameworks: PHP, .NET, J2EE, ColdFusion, etc.
- Most exploited types of vulnerabilities
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgeries (CSRF)
  - PHP Remote File Inclusion

12

S7. Database Software

- The most common vulnerabilities in database systems are:
  - Use of default configurations with default user names and passwords
  - SQL Injection via the database's own tools, third-party applications or Web front-ends added by users
    - Huge number of vulnerabilities in this class are announced every year
- Use of weak passwords for privileged accounts
- Buffer overflows in processes that listen on well-known ports

13

Z1. Zero-day Attack

- A computer threat that exposes undisclosed or unpatched computer application vulnerabilities
- Zero-day attack take advantage of computer security holes for which no solution is currently available
- A.k.a. Zero-hour Attack

14

Common Attacks Overview

- What is it?
- What are commonly used techniques?
- What are the damages caused by the attack?
- What are the responses to the attack?
  - Social
  - Technical
  - Legal
  - …

15

Passerby Attack (Shouler-surfing)

- Using direct observation techniques, such as looking over someone's shoulder, to get information

16

Malware and Spam

- Distribution of malware
  - Virus, Trojans, keyloggers, spyware, adware, rootkits
- Spam
  - Unsolicited or undesired bulk of electronic messages
  - Email spam
  - Mobile phone spam
  - Forum spam
  - Messaging spam (SPIM)
  - …

17

Denial of Service (DoS) Attacks

- Common attack method
  - Saturating the target (victim) machine with external communications requests
  - Such that it cannot respond to legitimate traffic in reasonable time
- Common implementations
  - Forcing the targeted computer(s) to reset, or consume its resources such that it can no longer provide its intended service
  - Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately

18

Spoofing Attacks

- A situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage
  - In the network security context
- Sample methods
  - Man-in-the-Middle attack
  - Phishing
  - Login spoofing

19

Phishing Attack

- Attempts to lure users into revealing her passwords or other confidential information by masquerading as a trustworthy entity in an electronic communication
  - The word "phishing" was first used around 1996 when hackers began stealing AOL accounts by sending email to AOL users, that appeared to come from AOL
  - Variant of "fishing": alludes to baits used to "capture" financial information and passwords
- A form of Identity Theft
  - Most major banks in US, UK, and AUS have been hit
- Phishing technqiues
  - Link manipulation
  - Filter evasion
  - Phone phishing
  - …

20

Identity Theft

- Describe an action where a person uses the identity of another to fraudulently obtain credit, goods, services, or to commit crimes
- Examples of these crimes are bank and credit card fraud, wire fraud, mail fraud, money laundering, bankruptcy fraud, and computer crimes
- Anti-phishing

21

Spear Phishing Attack

- A highly targeted phishing attack
- Spear phishers send emails that include information about stuff or current organizational issues that make it appear genuine to employees or members within a certain company, government agency, organization, or group
- UofT alert (http://www.news.utoronto.ca/campus-news/u-of-t-computer-staff-warn-of-phishing-scams.html)
  - April-May 2008, more than 2,000 UTORmail customers received an email that looked as if it came from the university's help desk
  - Asking for user IDs and passwords

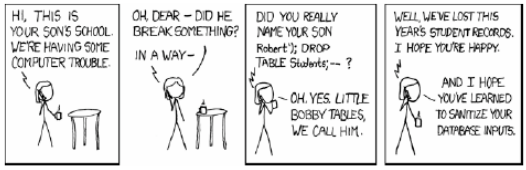
22

SQL Injection

- Injections are possible due to intermingling of user supplied data within dynamic queries or within poorly constructed stored procedures
  - Incorrectly filtered escape characters
  - Incorrect type handling
- Examples
  - statement := "SELECT * FROM users WHERE name = ' " + userName + " '; "
  - userName being " a'; DROP TABLE users' "
- SQL injections allow attackers:
  - To create, read, update, or delete any arbitrary data available to the application
  - In the worst case, to completely compromise the database system and systems around it

23

A Picture is Worth a Thousand Words



24

Attack Prevention Measures

- You cannot control that which you cannot measure!
  - JavaScript Security Model
  - Secure Sockets Layer (SSL)
  - Secure Java Programming

25

JavaScript Security Policy

- Set of rules governing what scripts can do under what circumstances
  - For example, to prohibit JavaScript Web pages from accessing to the local file system
    - If not, any Web page you visit could potentially steal or destroy all your files
- We examine the security policies browsers enforce on JavaScript embedded in Web page
  - The fundamental premise is that there is no reason to trust randomly encountered code such as that found on Web pages

26

JavaScript Security Model

- Downloaded scripts are run by default in a restricted "sandbox" environment
  - Isolated from the rest of the OS
- Scripts are permitted access only to data in the current document or closely related documents
  - Generally those from the same site as the current document
- No access is granted to
  - The local file system
  - The memory space of other running programs
  - The OS's networking layers

27

The Same-Origin Policy

- To prevent scripts loaded from one website from getting or setting properties of a document loaded from a different site
  - Prevents hostile code from one site from "taking over" or manipulating documents from another
  - Without it, JavaScript from a hostile site could do any number of undesirable things such as
    - Snoop key-presses while you're logging in to a site in a different window
    - Wait for you to go to your online banking site and insert spurious transactions
    - Steal login cookies from other domains

28

Browser Security Problems with JavaScript

- Bombing browsers with JavaScript
  - Denial-of-Service attacks
    - "services" refers to access to a functioning operating system
  - Examples
    - Infinite Loops
    - Memory Hogs
    - Using the Browser's Functionality
    - Deceptive Practices

29

Infinite Loops

- Some modern browsers will catch and halt the execution of the most obvious infinite loops
- But seldom would they stop something like this:

```
function tag()
{
    you_are_in();
}
function you_are_in()
{
    tag();
}
tag();
```

30

Memory Hogs

- Doubling string
  - Grows exponentially in size, crashing many browsers within seconds

```
var a_str = "random value";
while(true)       a_str += a_str;
```

- Stack overflow

```
function recurse()
{
    var x=1;
    recurse();
}
```

31

Using the Browser's Functionality

- Writes <frameset> elements referencing itself
  - Thereby creating an infinite recursion of document fetches
- Open up an endless series of dialog boxes

```
function ask_me_again()
{
    alert("Ouch!");
    ask_me_again();
}
```

- Continually call window.open() until the client's resources are exhausted

32

Deceptive Practices

- To trick or annoy users in one way or another
- Pop-up ads
  - Create a small, minimized window
  - Immediately send it to the background by bringing the original window into focus()
  - The ads window comes with
    - an event handler that will blur() it when it receives focus
    - and an onunload handler to respawn it if it is closed
- Trick a user into changing the default home page
  - Supported in IE 5+: DHTML Behaviors

```
<a onclick="this.style.behavior='url(#default#homepage)';
    this.setHomePage('http://www.example.com')" href=""> Click here
    to see our list of products! </a>
```

- Disguised windows or dialog boxes

33

Secure Sockets Layer (SSL)

- Cryptographic protocols
  - Provide secure communications on the Internet
    - Web browsing, e-mail, Internet faxing, instant messaging
- More recently, Transport Layer Security (TLS)
  - A modification of SSL version 3
- HTTP running over SSL is referred to as *secure* HTTP
  - https:// instead of http://
  - The default port for HTTPS is 443

34

SSL: Basics

- Server authentication
  - SSL-enabled browser includes public keys for trusted Certificate Authorities (CAs)
  - Browser requests server certificate, issued by trusted CA
  - Browser uses CA's public key to extract server's public key from certificate
- Visit your browser's security menu to see its trusted CA's

35

Secure Java Programming

- Data Handling
  - e.g., SQL Injection
- Authentication and Session Management
  - e.g., Phishing, Passerby Attack
- Access Control (Authorization)
  - Unauthorized Access
- Other Aspects
  - Java Types & JVM Management
  - Application Faults & Logging
  - Encryption Services
  - Secure Architecture & Coding Principles

36

CSC309H1Y Course Evaluation

- Instructor
  - Nan Niu
- TAs
  - Timothy Fowler
    - Tutorial: Client-side programming & Pointbase
    - Marking: A1, A3
  - Ali Juma
    - Tutorial: Tomcat
    - Marking: A2
  - Torsten Hahmann
    - Tutorial: Apache
    - Marking: A4

37