COMP 424

Purpose:

Introduction to computer security issues

Familiarization with secure software dev

Topics:

Cryptography/Auth

Access control & sec models

Secure protocols

Secure software design and programming

Network sec.: threats/countermeasures

Operating systems sec

Sec analysis and forensics

Malware, common attacks & important defenses

Privacy

Practical computer security defenses

<http://www.csun.edu/ansr/classes/comp424/>

Username:guest

Password:turing

History of the Security Problem:

In the beginning, there was no computer security prob

Later, problems, but nobody cared

Now, large problem, people care

Examples of Large Scale Security Problems:

Malicious code attacks

Distributed denial of service attacks

Vulnerabilities in commonly used systems

Distributed Denial of Service Attacks

Use large number of compromised machines to attack one target

-By exploiting vulnerabilities

-Or just generating lots of traffic

A favored tool for hacktivists

-Recent large DDoS attacks on China and others

In general form, and extremely hard problem

Vulnerabilities in Commonly Used Systems

802.11 WEP is fatally flawed

Recently, critical vulnerabilities in Intel processor microcode, Linksys routers

Popular applications:Android webview, Android OS, IE, HP backup. Office, Adobe Flash

Man security systems have vulnerabilities

GNU TLS, APPLE iOS SSL, symantec endpoint protection recently

Electronic Commerce Attacks

Credit card number theft(often via phishing)

Identity theft

Loss of valuable data from laptop theft

Manipulation of e-commerce sites

Extortion via DDoS

Cyber warfare

Nation states have developed capabilities to use computer networks for such purposes

DDoS attacks on Estonia and Georgia

Continuous cyber spying by many nations

Vulnerabilities of critical infrastructure

Legacy and Retrofitting

We are constrained by legacy issues

Core internet design

Popular programming languages

Commercial operating systems

All developed before security was a concern

With little or no attention to security

Retrofitting security works poorly

Consider the history of patching

Problems with Patching

Usually done under pressure(quick and dirty)

Tends to deal with obvious and immediate problem

Hard(sometimes impossible) to get patch to everyone

Since it's not organic security, patches sometimes introduce new security problems

Speed is increasingly killing us

Attacks are developed more quickly

Malware spreads faster

Some Important Definitions

Security and Protection

Security is a policy

Protection is a mechanism

Protection mechanisms implement security policies

Vulnerabilities and Exploits

A vulnerability is a weakness that can allow an attacker to cause problems

Not all vulnerabilities can cause all problems

Most vulnerabilities are never exploited

An exploit is an actual incident of taking advantage of a vulnerability

Allowing attacker to do something bad on some particular machine

Trust

An extremely important security concept

You do certain things for those you trust

Problems with trust

How do you express trust?

Why do you trust something?

How can you be sure who you’re dealing with?

What if trust is situational

What if trust changes?

Trust is not a theoretical Issue

Most vulnerabilities that are actually exploited are based on trust problems

Attackers exploit overly trusting elements of the computer

From the access control model to the actual human user

Taking advantage of misplaced trust

Such a ubiquitous problem that some aren’t aware of its existence