Be sure to review the homework solutions for Units 2 & 3.

Security Concepts

Security Goals (NIST SP 800-12 and FIPS 199)

Know the three primary security goals

1. Confidentiality
2. Integrity
3. Availability

Some add *Non-repudiation* and *Assurance*

Know the three impact levels

1. Low
2. Medium
3. High

Apply the CIA concepts and impact levels to specific scenarios.

Threats, Attacks, Assets

Definitions of threats, attacks, and assets; vulnerabilities. What are the relationships among these concepts?

Taxonomy of Attacks (Inside/Outside, Active/Passive)

Examples of assets and threats (see, e.g., Table 1.3 in *S&B*).

Apply concepts to specific scenarios.

Standards

Interoperability, assurance of market share. Important for security *because it is hard!*

The Internet Organization

Internet Architecture Board

Internet Engineering Steering Group

Internet Engineering Task Force (IETF)

Internet Drafts are proposed standards; Requests for Comment (RFCs) are published standards.

RFCs — not just security, but many Internet standards.

National Institutes of Standards and Technology (NIST)

Publish Federal Information Processing Standards (FIPS) and Special Publications (SP)

International Telecommunications Union (ITU)

"is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis."

Stack-Buffer Overflow

Attacking the in/out package

Why is the in/out package "interesting" from a security perspective?

Owner and permissions
User Input

Find the vulnerability

Which function in the in/out package causes the buffer overflow?
Which C library function should the programmer *not* have used and why? What is an alternative that would have been better?

What does the stack look like (roughly) in the vulnerable function?

Exploitation Challenges

Knowledge of stack frame location

Where *exactly* is the function's return address?
Where *exactly* can we locate malicious code?

String processing

Malicious code must survive string processing

Exploit Components

There are three components of a basic stack-buffer overflow attack. All three components are part of a single string that will be passed to the vulnerable program as user input.

Shellcode (see sample)

What is the purpose of shellcode?

What are the two major constraints facing a shellcode writer?

Return Address

Why might an attacker include multiple copies of the return address?

NOP Sled

What is a NOP?

What is the purpose of the NOP sled (block of NOPs before the shellcode)?

Stack-Buffer Overflow Protection

Buffer overflow recap

Attacker must:

1. Overwrite values on stack
2. Execute the code on the stack.
3. Predict location of code in memory.

Modern systems protect against these things.

Stack Protection

Goal is to prevent attacker from overwriting anything important (esp. return address)

Terminator Canaries

What is a terminator canary? How is it constructed?

What type of overflow does it protect against? How?

Some weaknesses with terminator canaries

May not protect against non-string based overflow attacks

May be defeated if multiple overwrites are possible — one overwrite to modify control information on the stack, a second to fix-up the canary

Random Canaries

What is a random canary? How is it constructed?

What type of overflow does it protect against? How?

Some weaknesses with random canaries

Local variables *may* not be protected

Function arguments *may* not be protected, at least within the vulnerable function

Attacker may be able to retrieve or guess random canary value (low entropy). Some bits of canary may be derived from “guessable” sources

What overflow protection does Linux provide? How is it enabled or disabled?

Stack Execution Protection

What is it? Where is it supported — CPU or OS?

How does Linux implement stack execution protection? How is it enabled or disabled?

Some weaknesses with stack execution protection

CPU may not support it (older CPUs) or it may be disabled in BIOS
May not be enabled in virtualized environment

Attackers have developed workarounds

Return-to-libc attacks to overcome non-executable stack

How do they work; describe the approach for a specific example

Address Space Layout Randomization

What is the purpose of ASLR? What different types of ASLR are there?

What types of ASLR are supported in Ubuntu Linux? Which types of ASLR did you implement in Project 1?

Who can disable ASLR on Linux?

Classification of Malicious Software - Propagation

Viruses

Replicate by modifying other files or programs

Require *user assistance* to replicate

Give an example

Trojan Horse

Masquerades as useful or desirable software, enticing users to install

Includes malicious functionality

Give an example

Worms

Spread *without* injecting code into other applications

Typically spread *without user assistance*

Give an example

Trapdoors (or Backdoors)

Method to obtain access that bypasses usual authentication measures

A type of *Insider Attack*; may be malicious or benign

Example: Ken Thompson's *Reflections on Trusting Trust*. (linked from the Lecture 6 web page)

Logic Bombs

Code created to take destructive action given a specific *trigger*

Another form of *Insider Attack*

Give an example

Viruses in Depth

Virus Types

File viruses — what are they? Give an example.

Macro viruses — what are they? Give an example.

Boot sector viruses — what are they? Give an example.

Virus Signatures

What is a virus signature?

How are signatures used to defend against viruses?

Given a ClamAV signature, describe how it is used

Encrypted, Polymorphic, and Metamorphic Viruses

Why would a virus writer encrypt the virus code?

What limitations are there on encryption of the code?

What is a *Polymorphic Virus*?

A *Metamorphic Virus* attempts to defeat signature recognition by re-writing its own code. Know the following methods for re-writing code:

1. Garbage code insertion
2. Register Use Exchange
3. Code Block Permutation / Jump Insertion
4. Code Integration

Worms in Depth

Worms can spread without user action.

Example: The Morris Worm, 1988 (http://en.wikipedia.org/wiki/Morris_worm)

What vulnerabilities did the worm exploit in order to spread?

What design flaw turned this “experiment” into a denial-of-service?

Example: Stuxnet, 2010 (http://en.wikipedia.org/wiki/Stuxnet)

A *zero-day vulnerability* is a vulnerability that was previously unknown to the general public. What was special about Stuxnet with regard to zero-days?

Stuxnet targeted a Siemens Programmable Logic Control (PLC). Why is this a concern? Recall the TED video.

How was Stuxnet able to install device drivers that were trusted by Windows?

Was Stuxnet harmful?

Malicious Software - Payloads

System Damage

What is it?

Give an example of a virus that causes system damage.

Rootkits

What is the purpose of a rootkit?

What is the difference between kernel-mode and user-mode rootkits?

What is function hooking?

Give an example of a rootkit.

Botnets

What is a botnet and what is the purpose of a botnet?

Privacy Invasive Software

Give some examples of privacy invasive software.

Basic Virus Detection

What is a heuristic? How is it different than a signature? Give an example of a heuristic.

Block Ciphers

What is a block cipher?

Basic parameters — block size, key size, round function, number of rounds, subkey algorithm (also called *key schedule* or *key expansion*).

What is the structure of a Feistel Network? How is a Feistel network used to decrypt a message?

DES — what is it? How is it related to Feistel Networks? What are the block and key sizes? How are encryption and decryption related.Which

What is the important of the S-boxes in DES?

Why would a linear block cipher be "bad?" See the exercises.

Why is DES no longer considered to be secure?

What is Triple DES (3DES)? What are the two versions of 3DES?

Be able to compute the time to complete a brute-force attack on 3DES (or any other algorithm).

AES — what is it? What are the basic parameters (block size, etc.) for AES? Is AES a Feistel Network?

What are the components of the AES round function? What it the importance of the S-function?

What is the purpose of the subkey algorithm (also knows as *key expansion* or *key schedule*)?

Block Cipher Modes of Operation

Know the four modes discussed in class — ECB, CBC, CFB, CTR.

Be able to draw a diagrams of the four modes of operation.

Know the relative weaknesses and strengths of the four modes.

Stream Ciphers

What is a stream cipher? What is the *period* of a stream cipher?

Describe how a block cipher in CFB or CTR mode is a type of stream cipher.

Describe the attack against stream ciphers when the underlying plaintext is highly structured and known to the attacker.

Describe the function and phases of the RC4 algorithm. What does the run-up (initialization phase) produce? How is secret key used? How does the key generation phase work?

What is the problem with RC4 as used in WEP? What attack applies in this case?

Public Key — RSA

What problem does public key "solve?"

What are the requirements for a public key algorithm? What are the roles of the public and private keys?

How can a public key algorithm be used to construct a digital signature?

What is a certificate and what are certificates used for? What is the standard format for a certificate?

Both RSA and DH are susceptible to a Man-in-the-Middle attack. How do certificates protect against this?

What are the basic parameters of RSA (p, q, N, d, e)? What properties should p and q have? What is the relationship between N and p and q? How is d derived from p, q, and e? How big should p, q, an N be? What is phi(N)?

Be able to perform basic RSA computations to encrypt or decrypt data.

How would RSA be used along with a block cipher to encrypt a message?

What is the basis for the security of RSA?

Public Key — Diffie-Hellman

What mathematical problem is the basis for the security of DH?

What are the parameters of basic DH (q, alpha)? How are the public and private keys created? How are the public and private keys used?

What is a primitive rood modulo q?

Be able to compute a small DH key exchange example.

What are the parameters of “real” DH (p, q, alpha) and how are they related? What are their sizes?

How would DH be used along with a block ciphersp to encrypt data?

What is the advantage of elliptic curve DH over classical DH?

Cryptographic Hash Functions

Hash functions in general

What is a hash function?

What are some of their uses?

Three security requirements for a cryptographic hash — know these and be able to apply them to simple examples (scenario or to a simple hash function):

1. Pre-image Resistance
2. Weal Collision Resistance
3. Strong Collision Resistance

For a secure, *n*-bit hash function, what are the “costs” to find a pre-image, weak collision, or strong collision?

Standard Hash Functions

Which series of publications defines the SHA hashes?

Which SHA algorithm family is the current standard for US Government systems? What are some of the digest sizes supported by this algorithm family?

Describe the operation of SHA-512 on a multi-block message requiring padding. Sketch a diagram.

SHA-3 is still in DRAFT. Why did NIST believe another algorithm was needed even though the current generation of hashes is still believed to be secure? What sort of construction is SHA-3 based upon?

Problems with MD5

What is the problem with MD5? I.e., what type of attack is possible?

What did Lenstra, Wang, and de Weger do to demonstrate that the weakness could be exploited?

How did the Flame malware use this weakness?

HMAC

What is an HMAC used for? Describe how Alice and Bob can use an HMAC.

Why is HMAC better than a keyed hash?

Pseudo-random Number Generation

What are some of the uses of PRNGs?

What are the requirements of a cryptographic PRNG?

Is an LCG acceptable for cryptographic applications? If not, which requirement does it not satisfy?

Be able to do simple LCG computations.

Which NIST document describes several good cryptographic PRNGs?

Describe, in general terms, the operation of the NIST PRNG that was discussed in class.

Describe the BBS generator and be able to do simple computations.

What is the security of BBS based on? What is the main disadvantage of BBS?