Final Exam Review

Security Concepts

Know the basic terms and definitions:

1. Vulnerability
2. Threat (within threat, we also consider Method, Opportunity, and Motive)
3. Attack
4. Control

Know the three primary security goals

1. Confidentiality
2. Integrity
3. Availability

Apply the CIA concepts to specific examples.

Standards

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

What makes a 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?

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

There are three components of a basic stack-buffer overflow attack: shellcode, return adress block, and NOP sled. 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

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

Stack Canaries

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 / return-to-system — describe and indicate how it bypasses stack execution protection

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?

Viruses in Depth

What are the differences among file viruses, macro viruses, boot sector viruses.

What is a virus signature? How are signatures used to defend against viruses?

Given a ClamAV signature, describe how it is used.

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

Access Control in General Purpose OSs

What are the goals of memory protection?

Know the evolution of memory protection techniques:

1. Fences
2. Base/Bounds Registers
3. Tagging

4. Segmentation
5. Paging
6. Paging with segmentation

Which protection schemes are supported by current Intel architectures?

Which protection schemes are used by current versions of Linux?

What is an Access Control Matrix (ACM)? How are directories and Access Control Lists (ACLs) just different ways of looking at the ACM? Describe.

What is Role-Based Access Control (RBAC)? What are the four levels of RBAC as described in the NIST RBAC model?

Cryptographic Hash Functions

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. Weak 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?

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

Why is HMAC better than a keyed hash?

Passwords and Authentication

Why should a system only store hashed passwords? What is “salt” and how is it used? What are the benefits of salting a password hash?

How do current *nix-based systems hash and store user passwords? Give a specific example.

Windows has used two different hash functions: LAN Manager (LM) Hash and the NT Hash. Describe the weaknesses in the LM Hash.

What flaw in the implementation of the NTLM protocol allowed for remote access to Windows systems for a period of 17 years? Explain how the vulnerability could be exploited.

What is a dictionary attack? What is the effect of salt on the cost of a dictionary attack?

For an N-word password space, a Time-Memory Tradeoff (TMTO) attack requires one-time work on the order of N hash computations, storage on the order of $N^{2/3}$ words and per-attack computation on the order of $N^{2/3}$ hash computations.

Describe a scenario in which such an attack would be useful.

Illustrate the costs with a specific example, e.g. what are the storage and computational requirements for a password space of size 2^{36}?

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.

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.

Recognize the A5/1 algorithm. What was it used for? What sort of pseudo-random stream does it produce (bits or bytes)?

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 cipher to encrypt data?

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

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?

Basic Network Security

What is ARP spoofing and what good is it to an attacker? What limitations or constraints are placed on the attacker (e.g. must be on the same network segment)? What are some defenses against ARP spoofing?

What is IP spoofing and what good is it to an attacker? What limitations or constraints are placed on the attacker (e.g. won't be able to see target's response)? What are some defenses against IP spoofing?

What is TCP Session Prediction and what good is it to an attacker? What limitations or constraints are placed on the attacker?

What is Session Hijacking and what good is it to an attacker? What limitations or constraints are placed on the attacker (e.g. must "silence" legitimate client)? What are some defenses against session hijacking?

What is DNS Cache Poisoning and what good is it to an attacker? What limitations or constraints are placed on the attacker (e.g. must provide fake query response very quickly)?

How is the Birthday Paradox relevant to DNS cache poisoning?

How does DNSSEC prevent DNS cache poisoning? What cryptographic technique does it use?

Secure Shell

What is the purpose of secure shell (ssh)? What attacks does it protect against?

What are the three SSH protocols (transport, authentication, connection)? Which two are security-related?

What is the role of the server host keys? In a typical ssh installation, how does the client acquire the host keys? What are more secure ways to distribute host keys?

What is accomplished by the transport protocol? That is, the goal of ssh is to set-up an encrypted, authenticated connection; does the transport protocol initiate encryption? authenticate the server? authenticate the host?

What public key algorithm is used by the transport protocol?

What are the allowed methods for client authentication (password or public key)? How is the client authenticated using the public key method?

When password authentication is used, is the user password protected?

What are some encryption algorithms that are supported by SSH (symmetric and authentication algorithms)?

What was the “Debian Fiasco?” Explain the vulnerability that was created in the Debian Linux distribution and how it could be exploited by an attacker. How was the vulnerability introduced?

Needham-Schroeder Protocol and Kerberos

Explain the use of *tickets* in the N-S and Kerberos protocols.

What is the role of the Authentication Server (AS)?

In N-S, what part of the protocol assures Bob that he is not receiving a re-played ticket?

What is the role of the Ticket Granting Server in Kerberos?

Why does Kerberos include a timestamp in an *authenticator.*

Why did I talk about Quantum Computing in the same lecture as N-S and Kerberos?