Midterm Exam Review - Part 2

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.

Protection Against Malicious Software

Basic Virus Detection

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

Metamorphic Virus Detection with HMMs

What is a Markov Model?

What is “hidden” in a Hidden Markov Model?

What data is used to build (“train”) a Hidden Markov Model to detect evolutions of a metamorphic virus?

What are the two components of an HMM to detect evolutions of a metamorphic virus? Describe them in words (i.e. what information to they contain).

Suppose you have built an HMM for a particular metamorphic virus. You find a program that you suspect is an evolution of the virus. What quantity can you compute using the HMM that helps you decide whether it is in fact an evolution of the virus?

Best Practices / Software Engineering

What do these mean:

1. Diversity of systems
2. Robustness of software
3. Limit user privilege
4. Improve authentication
5. Monitor networks
6. Use malicious software detection
7. Prepare for recovery

What is the single most effective development practice for reducing the number of security weaknesses in software?

Access Control in General Purpose OSs

Memory and Address Protection

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?

Protection of General Objects

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

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?

Passwords and Authentication

Hashes and Passwords

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.

Password Cracking

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 $N^{1/3}$ 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}?