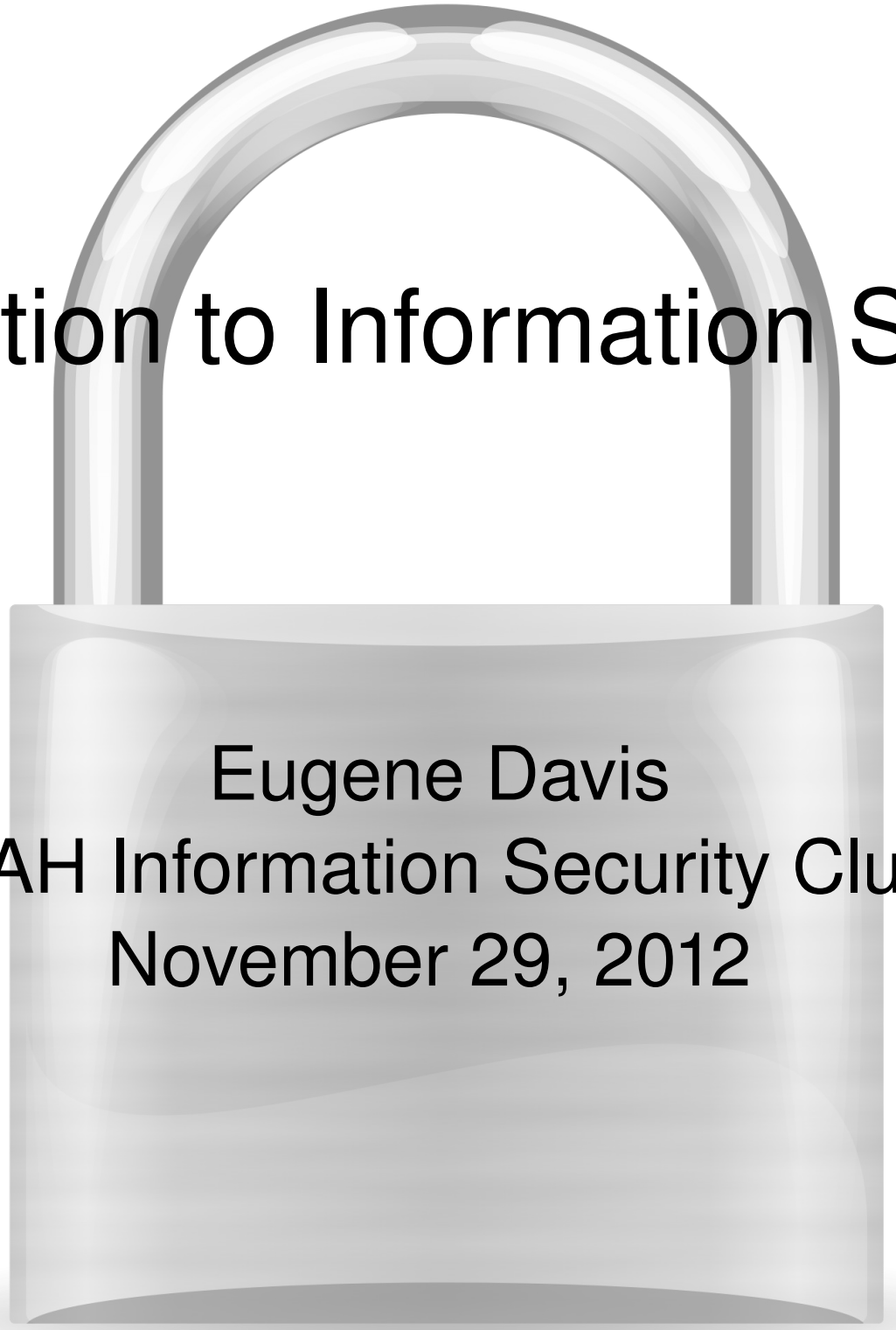
Introduction to Information Security



Eugene Davis
UAH Information Security Club
November 29, 2012

What is Information Security?

- Protecting information, data and computer systems from attackers
- Areas include:
  - Protecting the confidentiality of data and information
  - Protecting the integrity of data and computer systems
  - Ensuring the availability of data and computer systems

Black Hat vs White Hat

- **Black Hat** – commonly called a hacker, more precisely a criminal attempting to compromise a system
- **White Hat** – uses penetration testing (aka “ethical hacking”) to determine a system's weaknesses before it is attacked

- **Grey Hat –** straddling the line of legality, often outright breaking the law, they attempt to compromise systems for reasons other than personal gain

Cryptography

- Cryptography forms the basis for many aspects of security.
- Three forms of cryptography exist
  - **Symmetric Cryptography** – in which there is a key which must be directly exchanged between the communicating parties
  - **Asymmetric Cryptography** – developed in the 1970s, this allows two parties to communicate without ever having to exchange secret keys.
    - Each party maintains two keys, a secret key that they keep to themselves and a public key that anyone can access.
    - This process allows Internet commerce (and more) to exist
  - **Hashes** – one way functions that provide a fixed length output for any input, with a low chance of collision
- Tip: XORing your data and key only provides secure encryption if the key is the same length as the data and is **never** reused

Classification of Security
Basic Model

- Two basic categories of security
  1. **Integrity** – concerned with protecting the data and the system the data resides on from being damaged, e.g. tampered with or destroyed.
     - This includes dealing with write (but not read) permissions on files
  2. **Confidentiality** – concerned with keeping data (and information) secret and making sure that only those with proper permissions may read data
     - Information is distinct from data – information can be gained from unreadable data, through attacks of varying sophistication

Classification of Security
Examples

- A denial of service (DOS) attack is an integrity attack because it compromises the system
- Changing a field in a database (without reading it) is an integrity attack
- Stealing credit card records is a confidentiality attack
- Intercepting and reading an email is a confidentiality attack
- Compromising a system in order to read emails is an integrity attack (reading the emails is still a confidentiality attack)

Alternative Classifications of Security

CIA Triad (not Langley) – A Security Acronym

1. **Confidentiality** – see previous
2. **Integrity –** see previous
3. **Availability –** ensuring that the system is available when needed (part of integrity in the first definition, includes things such as DOS)

Alternative Classifications of Security

STRIDE – A Microsoft Acronym for Threats

1. **Spoofing Identity** – when an attacker impersonates a legitimate user
2. **Tampering with Data** – modification of data
3. **Repudiation** – when a malicious user can successfully deny responsibility for an attack. Repudiation also concerns itself with ensure that data is genuine and the originator cannot repudiate it.
4. **Information Disclosure** – when information or data leaks to unauthorized users
5. **Denial of Service** – attacks which prevent valid users from using the service
6. **Elevation of Privilege** – when an unprivileged user gains privileged access that allows them to cause some form of harm

Attacks: Malware

- **Viruses** – self-replicating programs that are capable of spreading from computer to computer, usually through human aid
- **Worms** – a type of virus capable of spreading from computer to computer without human aid (i.e. through vulnerabilities)
- **Trojan Horses** – programs that appear to be legitimate, but once installed by the user have additional nefarious uses
- **Rootkits** - malware that modifies the host operating system
- **Backdoors** – software or part of software that allows remote access to the machine.
- **Botnets** – networks of compromised computers controlled by a nefarious entity for activities such as DDOS (Distributed Denial of Service) attacks, spam, and more.

Attacks: Exploits

- Exploits take advantage of inherent problems in software/firmware/hardware to gain control or do damage to a system
- Examples
  - Buffer overflows – an array is passed too much data and other memory is overwritten with malicious content
  - Operating system design flaws – allowing a user to get unauthorized access (or elevate privileges) on a system

Attacks: Social Engineering

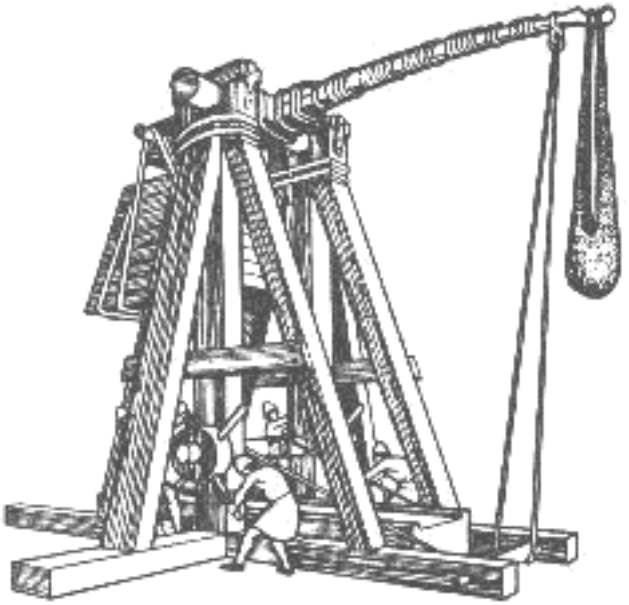
- Social Engineering - non-technical approach to gaining access to a system by tricking legitimate users into granting access to the attacker
- Relatively common (and effective) form of attack
- Examples
  - Dressing up as a janitor or IT person
  - Impersonating a legitimate user
  - Phishing - emails or other communications that appear to come from a legitimate source

Attacks: Repudiation

- An attacker can cover their tracks such that no action can be taken by the compromised organization
- Examples
  - Attacks performed through anonymizers
  - Attacks performed by compromised computers
  - Attacks where all input and output by the attacker is done through side channels

Attacks: Physical Access

- Physical Access – when the attacker has direct access to the system in question.
- One of the hardest things to defend against
- Examples
  - Attacker can plant a key logger
  - Attacker can steal the hard drive
  - Attacker can recover encryption keys from memory

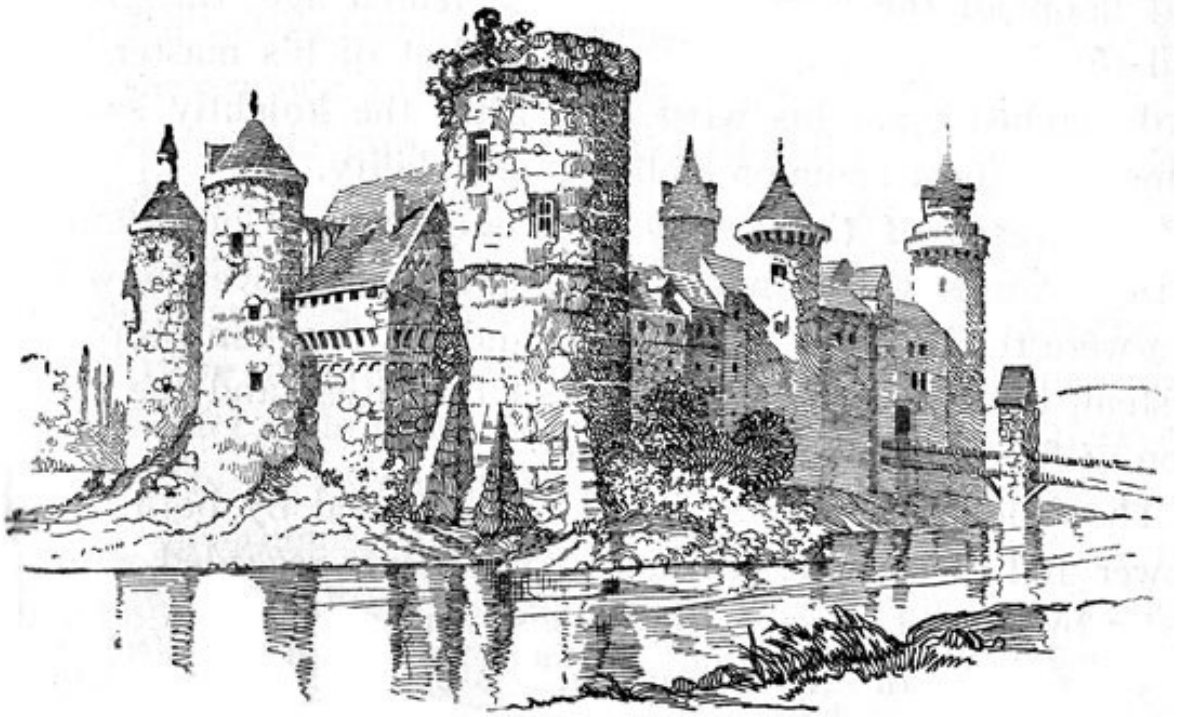


Defenses: Cryptography - Confidentiality

- Original use for cryptography – to keep your opponent from reading your messages
- Modern cryptography with a well selected key should take huge amounts of time to crack
- AES (Advanced Encryption Standard) is the current standard algorithm for symmetric cryptography
- Developing your own encryption algorithm is not a task to be undertaken lightly – it requires years of research, testing as well as a deep understanding of mathematics to prove its security
  - Accepting an algorithm as secure requires peer review by acknowledged experts in the field
  - As a developer, you should never attempt to develop your own algorithm, but use the current standards instead

Defenses: Cryptography - Integrity

- In some ciphers, it is possible to detect tampering (or errors) because the message will not decrypt
- In other cases, a hash of the original message is included to detect tampering
  - Usually this is called “signing” a message



Defenses: User and File Permissions

- By assigning identifiers to users and files, each can be assigned a listing a what they can access
  - Programs will often be associated with the running user and have their permissions
- A more complex system uses a partially ordered set or lattice as the structure to define access controls
- Many models exist for implementing permissions, such as the Bell-LaPadula model (BLP)

Defenses: Secure Architecture and Coding

- Secure Architecture – ensure that the system as a whole is designed with security in mind
- Examples
  - Connections over the network should be encrypted
  - Sensitive data should be encrypted
- Securing Coding – follow best practices for security in programming
- Examples
  - No dangling pointers
  - Use tested encryption libraries

Defenses: At the Individual Computer Level

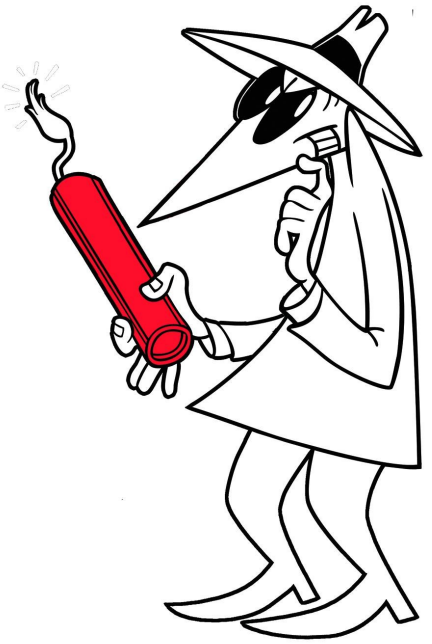
- Known as system hardening
- Antivirus – a good antivirus should be heuristic, and thus able to detect new “mutations” of old viruses
- Firewall – blocks incoming and outgoing traffic to IP and ports which are not allowed in its configuration
- Run as a non-admin user to prevent malware from getting elevated privileges
- Require software to notify and get permission before making changes to the system or other software (prevents malware from taking hold)
  - Example: Windows UAC

Defenses:
At the Network Level

- Network firewalls (often available in routers)
- Proxies to avoid direct contact between machines and to do a variety of scanning on the data (including virus scanning)
- Network intrusion systems – look for suspicious activity and alert the network administrator
- Careful assignment of permissions

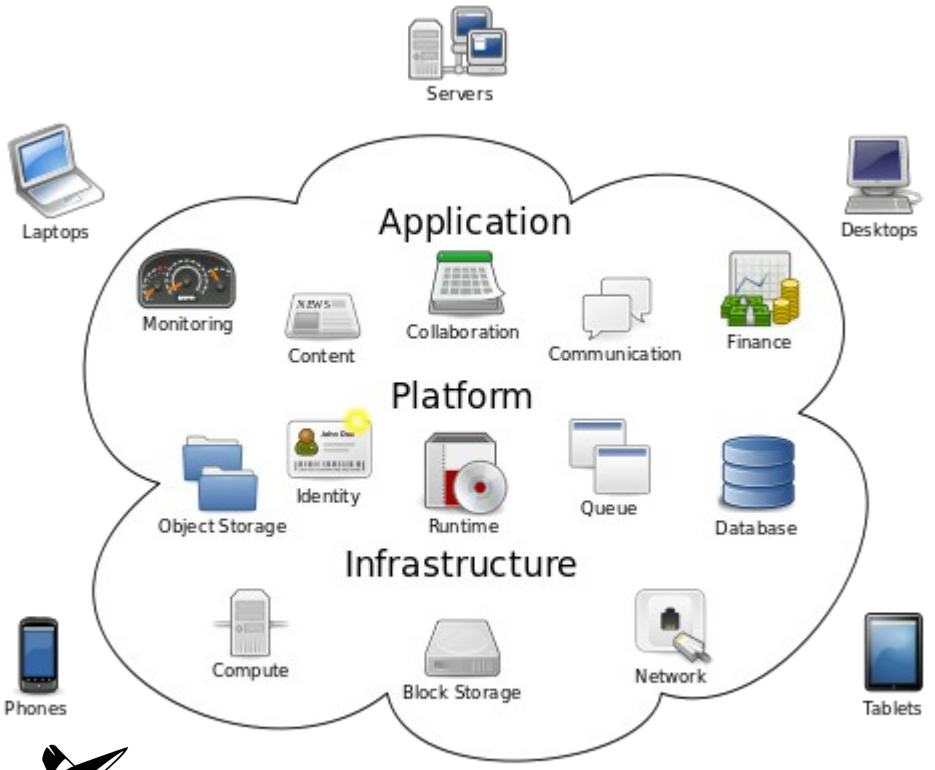
Defenses:
Penetration Testing

- **Penetration Testing or "Ethical Hacking"** - when white hats attempt to find vulnerabilities in systems in order that they can be fixed
- At the very least this should catch the obvious errors in a system



Areas of Current Activity

- **Cloud Computing** – moving everything to remote servers means that there is a single point of failure for total compromise of the system
- **Mobile Computing** – Android has regular issues with malicious apps, and periodically something happens to the iPhone as well
- **Encryption** – encryption is and always has been a constant battle between the attackers trying to read the messages and the defenders trying to keep them hidden. Lately the defenders seem to have the upper hand.



Suggested Reading

- For Encryption:
  - “The Code Book” by Simon Singh
  - “Applied Cryptography” by Bruce Schneier
  - Coursera's Introduction to Cryptography Course
- General Security:
  - “The Art of Computer Virus Research and Defense” by Peter Szor
  - “Computer Security” by Dieter Gollmann
  - “The Cryptogram” newsletters by Bruce Schneier
  - “Security Now!” podcast and associated websites