



DIMENSIONS OF INFORMATICS & COMPUTING: CYBER-SECURITY

Matt Hottell



SECURITY: THE CIA

- Three principles underline Information Security:
 - Confidentiality
 - Integrity
 - Availability

CONFIDENTIALITY

- Achieving this goal means that only appropriately authorized entities can get access to resources.
- Applies to communications as well as computer resources
 - Techniques:
 - Authentication (CAS)
 - Encryption
 - Access controls and classification levels

INTEGRITY

- This goal is the prevention of unauthorized alteration of data, regardless of accidental or malicious intent.
- If a change occurs, we should be able to recognize that it has happened and hopefully have a backup.
 - Techniques:
 - Algorithmic validation (checksums, hashing)
 - Access logs

AVAILABILITY

- Authorized users should be allowed to access resources when needed.
- To do this, we need to make sure that attacks or other scenarios are not preventing access.
 - Denial of service or server overload
 - Hacking
 - Accidents/disasters/outages

PICK THE PRINCIPLE

- Which of the CIA principles do each of the following violate:
 - A **virus** attack deletes most of the documents on a computer.
 - A **virus** attack bogs down a computer so that it is running too slowly to service requests.
 - An attacker uses a logged-in computer of someone who has gone off to a meeting to change grades on Oncourse.
 - A **distributed denial of service** attack shuts down Amazon.com for 4 hours.
 - An attacker calls a worker and pretends to be from the IT Helpdesk and convinces that worker to give the attacker his password.

MANAGING RISK


- Managing risk is the way we make decisions about each of the CIA principles
- Risk = Threat x Vulnerability x Cost
 - Threat is the frequency of a particular adverse event happening
 - Vulnerability is the likelihood of a particular threat being effective against a particular organization.
 - i.e. a weakness that can be exploited
 - Cost is the potential impact of a threat acting on a vulnerable organization.

EXAMPLE RISK: VIRUS ATTACK ON A PC

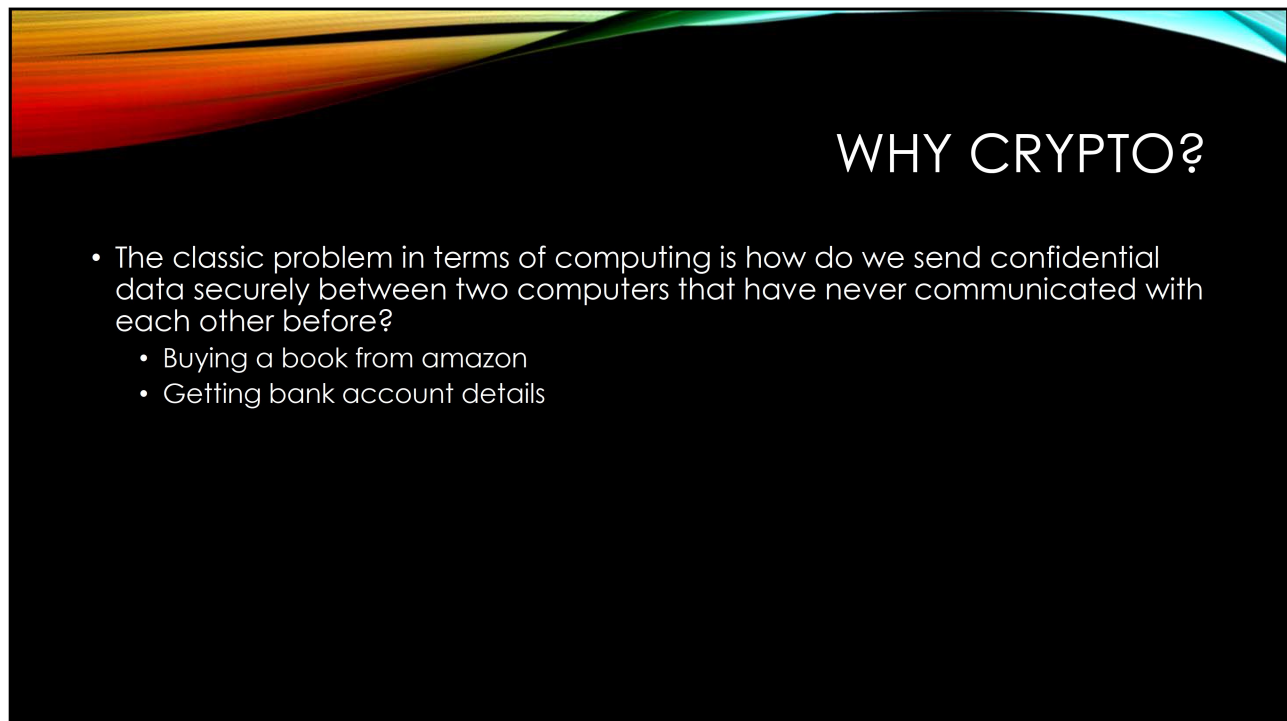
- The threat of a virus attack is approximately 88 per 1,000 users per day.



SECURITY: THE BROAD PICTURE



SECURITY APPLICATION: ENCRYPTION





DEFINITIONS

- **Plaintext** – the message
- **Ciphertext** – the encrypted message
- **Encryption** – process of converting **plaintext** into **ciphertext**
- **Decryption** – process of converting **ciphertext** into **plaintext**

METHODS OF ENCRYPTION

- Transposition
 - Switching the symbols within the plaintext
- Substitution
 - Substituting different symbols for the symbols in the plaintext

TRANSPOSITION EXAMPLE

- Rail fence cipher:
one if by land two if by sea - **plaintext**

o e f y a d w i b s a
n i b l n t o f y e

oefyadwibsanibln tofye - **ciphertext**

TRANSPOSITION EXAMPLE

- Decrypt the following 3-rail fence cipher:
FROASEESOOSRNENAAUCEDVYRG

ICE 1

When the ephors send out an admiral or a general, they make two round pieces of wood exactly alike in length and thickness, so that each corresponds to the other in its dimensions, and keep one themselves, while they give the other to their envoy.

These pieces of wood they call scytalae. Whenever, then, they wish to send some secret and important message, they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their scytale, leaving no vacant space thereon, but covering its surface all round with the parchment.

After doing this, they write what they wish on the parchment, just as it lies wrapped about the scytale; and when they have written their message, they take the parchment off and send it, without the piece of wood, to the commander.

He, when he has received it, cannot otherwise get any meaning out of it, -- since the letters have no connection, but are disarranged, -- unless he takes his own scytale and winds the strip of parchment about it, so that, when its spiral course is restored perfectly, and that which follows is joined to that which precedes, he reads around the staff, and so discovers the continuity of the message. And the parchment, like the staff, is called scytale, as the thing measured bears the name of the measure.

-Plutarch, *Lives*



SUBSTITUTION EXAMPLE

- Julius Caesar Cipher
 - Substitute each letter in the plaintext by the letter that is 3 down from it.
 - $\text{Encode}(\text{letter}) = (\text{letter} + 3) \bmod 26$
 - $\text{Decode}(\text{letter}) = (\text{letter} - 3) \bmod 26$

CAESAR CIPHER EXAMPLE

- Plaintext:
One if by land two if by sea
- Ciphertext:
Rqh li eb odqg wzr li eb vhd

CAESAR CIPHER EXAMPLE

- Decode the following message:
vhqg pruh slccd

ICE 2

SUBSTITUTION CIPHERS

- There are 4.0×10^{26} possible arrangements of the 26 letters.
- At one arrangement per sec it would take a billion people the lifetime of the universe to check all possibilities.
- Yet they are surprisingly easy to break...

FREQUENCY ANALYSIS

- Check frequency of symbols in the ciphertext and compare them to "normal" frequency of letters in that language.
- Issues...

SYMMETRIC KEY ENCRYPTION

- Knowledge of the same key provides the ability to both encode and decode.
- Traditional forms of encryption

WHIT DIFFIE IN 1975

- Proposed the first **asymmetric** encryption scheme.
- Alice and Bob each have a private key that only they know and a public key that anyone can know.
- The private key cannot be calculated using the public key

WHIT DIFFIE IN 1975

- Messages encrypted with Bob's public key can only be decrypted using his private key
- Messages encrypted using Bob's private key can only be decrypted using Bob's public key.
- This is also known as **Public Key Encryption**



RSA

- In April, 1977 a group of 3 MIT professors figured out mathematically how to implement Whit Diffie's concept of asymmetric key encryption
- They formed RSA, named for the last names of the 3 researchers (Rivest, Shamir, and Adleman)

CRYPTOGRAPHY

- So how is crypto used in web browsers today?

ICE 3

What is ONE thing that you found to be interesting during today's lecture? Why was it interesting to you? Discuss in your group and record your thoughts.

(You MUST complete this activity to receive attendance, a blank page with only your name and username will NOT count towards attendance)

ICE 3

INFO I101

Any questions?



On your way out...

1. Bring your **ICE Sheet** to the front and set it on the pile.
2. Scan your **CrimsonCard** for attendance.

