SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 4: Cybersecurity Tools

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

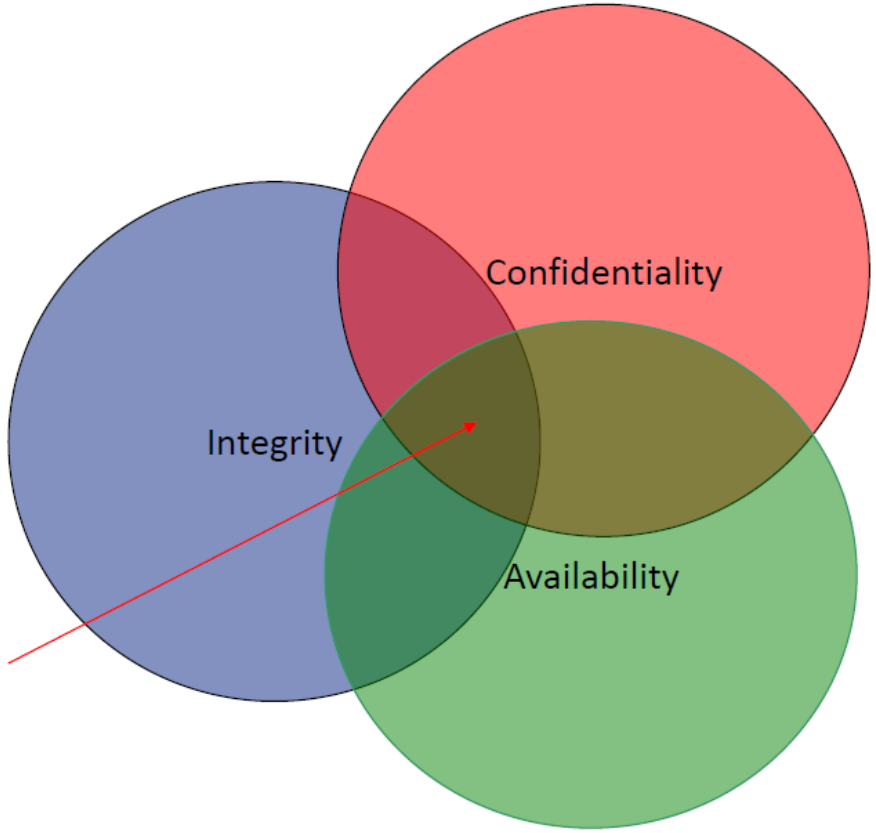
Cryptography

- Encryption
  - Symmetric
  - Asymmetric

Recall: Cybersecurity goals

CIA Triad:

- Confidentiality
- Integrity
- Availability

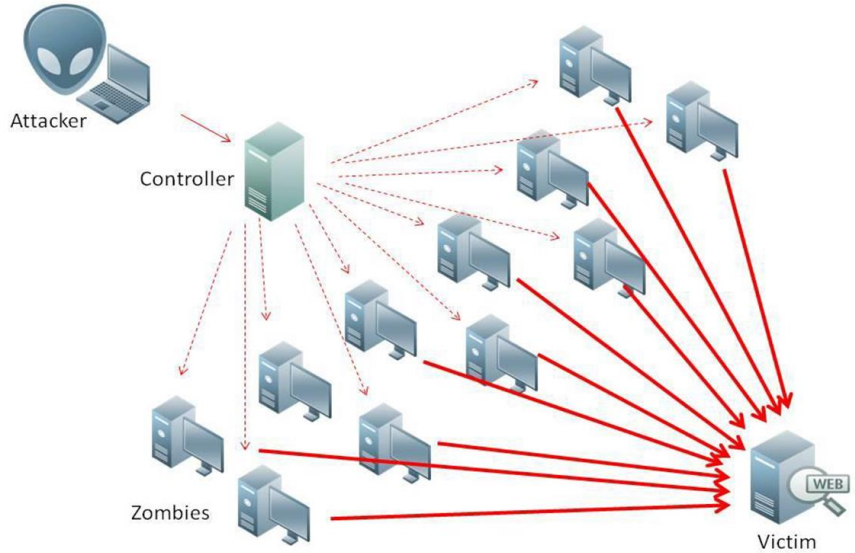


DoS and DDoS

DoS attack overwhelms a system's resources so that it cannot respond to service requests

DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker

- TCP SYN flood attack, etc.



Goals of Security

Prevention

- Prevent attackers from violating security policy
- Ideal Solution

Detection

- Detect attackers' violation of security policy
- Occurs after the attack

Recovery

- Stop attack, assess and repair damage
- Continue to function correctly even if attack succeeds

Cryptography

Cryptography is the study of mathematical techniques in the provision of information security services

- It is the strongest and most widely used tool for defending against many kinds of security threats

Goals of cryptography

- Confidentiality: keeping information secret from all but those who are authorized to see it
- Integrity: ensuring information has not been altered by unauthorized or unknown means
- Authentication: is the message from the expected source?
- Non-repudiation: preventing the MiTM

Encryption

Symmetric

Asymmetric

Symmetric Encryption

Technique for providing confidentiality for transmitted or stored data

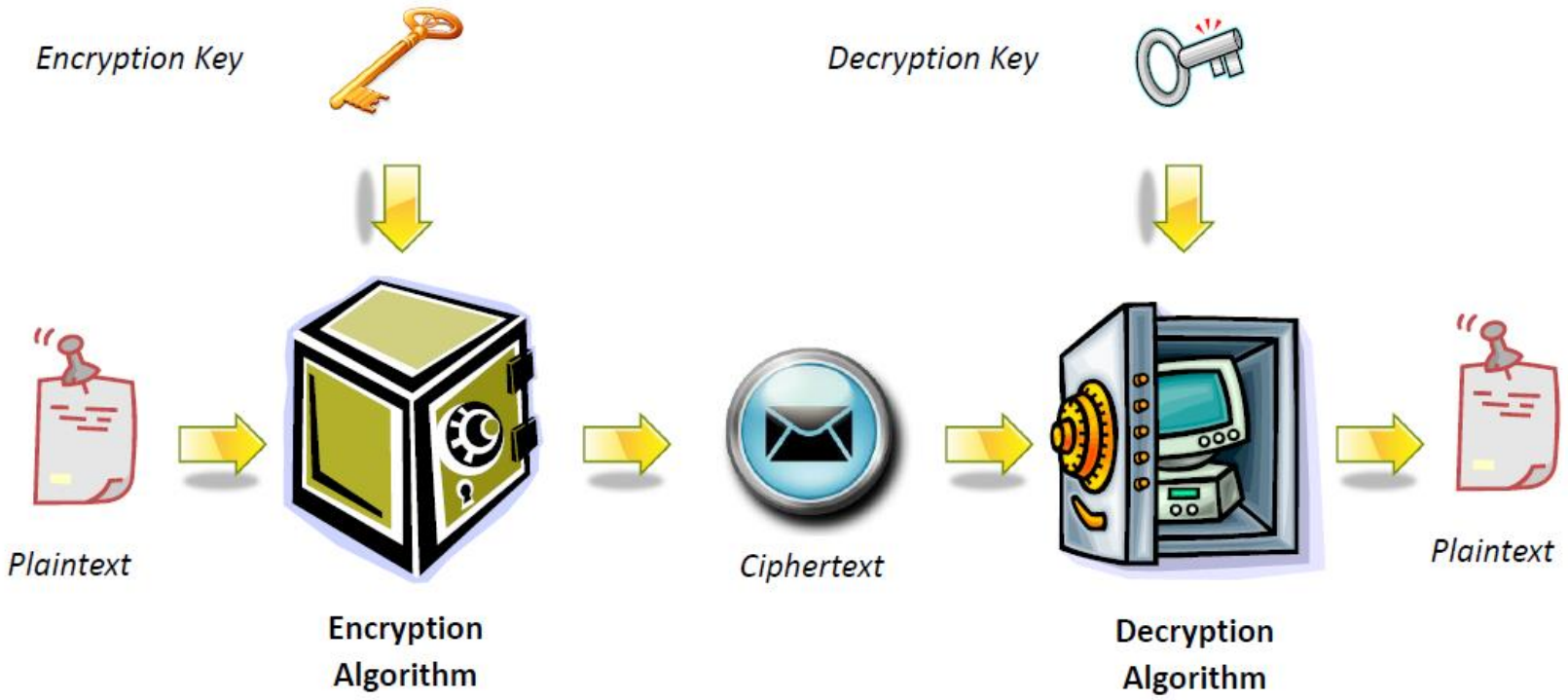
Also referred to as conventional encryption or single-key encryption

Two requirements for secure use:

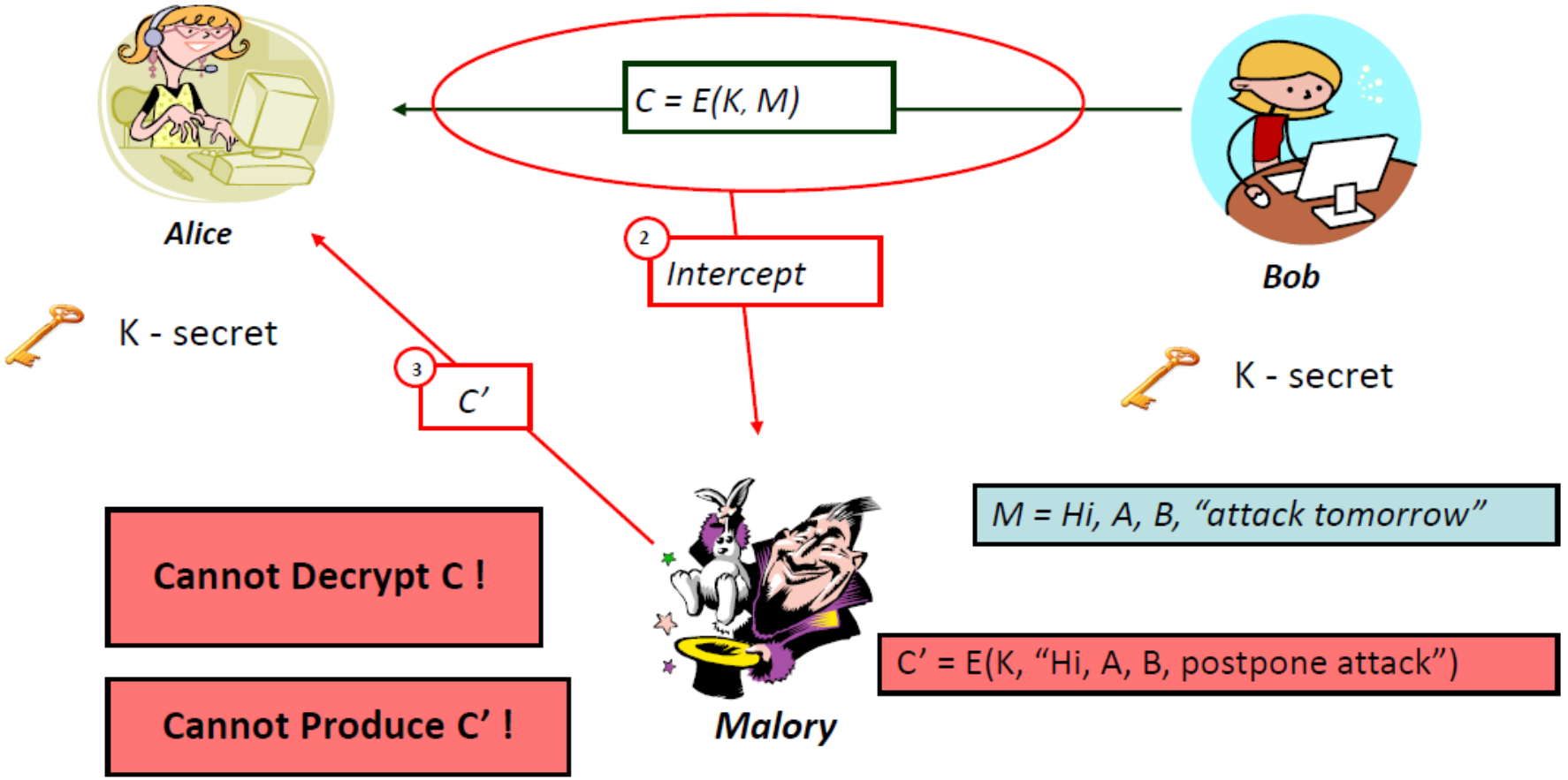
- Need a strong encryption algorithm
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

Symmetric Encryption

Secret key known only to sender / receiver



MiTM in encrypted scenario

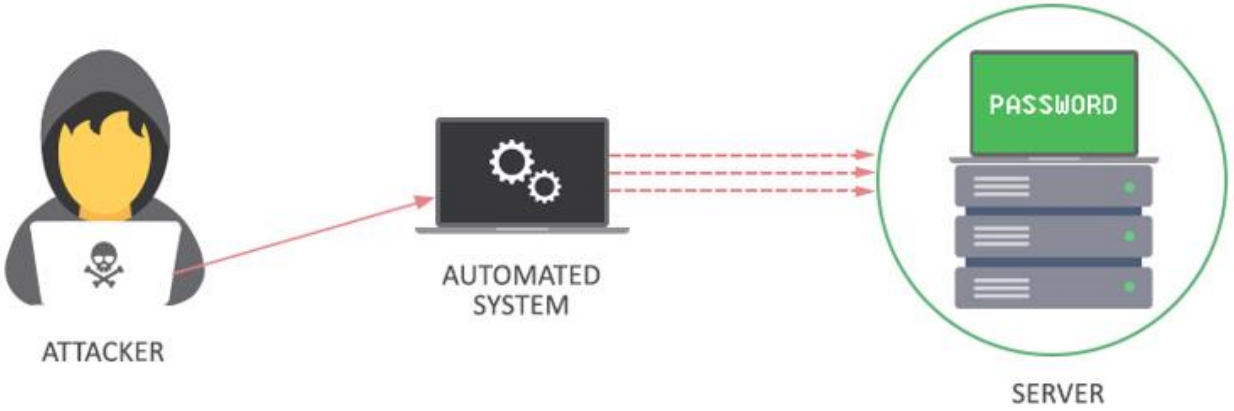


Attacking Symmetric Encryption

Brute-Force Attack:

Try all possible keys on some ciphertext (encrypted text) until an intelligible translation into plaintext (regular text) is obtained

- On average half of all possible keys must be tried to achieve success



Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful; all future and past messages encrypted with that key are compromised

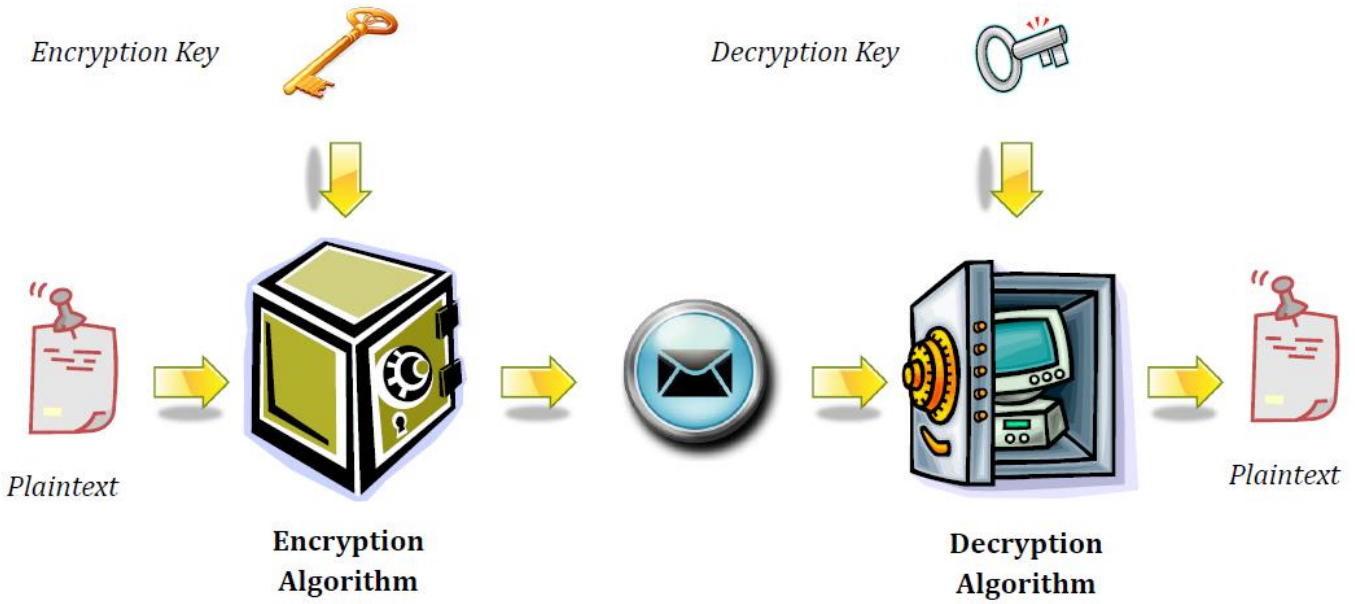
Asymmetric Encryption

Uses two keys – **a public and a private key**

Asymmetric: parties are <u>not equal</u>

User encrypts data using his or her own private key

Anyone who knows the corresponding public key will be able to decrypt the message (or vice versa)



Asymmetric Encryption: Requirements

Useful if either key can be used for each role

Computationally easy for sender knowing public key to encrypt messages

Computationally easy for receiver knowing private key to decrypt ciphertext

Computationally infeasible for opponent to determine private key from public key

Computationally infeasible for opponent to otherwise recover original message

Why Public Key

Addresses two key issues:

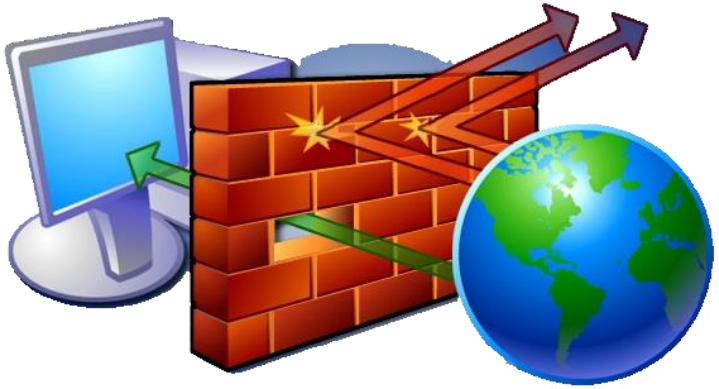
- Key distribution – how to have secure communications in general without having to trust a KDC (key distribution center) with your key
- Digital signatures – how to verify a message comes intact from the claimed sender

Ensure Both Security and Identity

Cyberattack Prevention Tools: Firewall

Network security device that

- Monitors incoming and outgoing network traffic
- Permits or blocks data packets based on a set of security rules



Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic

Cyberattack Prevention Tools: Intrusion Prevention System

Actively analyzes and takes automated actions on all traffic flows that enter the network. Specifically, these actions include:

- Sending an alarm to the administrator
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

Cyberattack Prevention Tools: Intrusion Prevention System

IPS must work efficiently to avoid degrading network performance

- It must also work fast because exploits can happen in near real-time
- The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

It often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content

Cyberattacks Detection Mechanisms

Anomaly Detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic Based Detection Methods

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Intrusion Detection System vs. Intrusion Prevention System