






Basic Security Concepts

- n Introduction
- n Basic Security Concepts
- n Next Lecture



Course Objective

- n Understanding of Information Security
- n Industry + Academics
- n Managerial + Technical
- n DEFENSE!



Incidents

ZDNet (08/14/02)

Tech's 'dirty little secret' -- cybersecurity

It's the industry's "dirty little secret": If you use your company's networks or the Internet, your daily online communication activity—from sending and receiving e-mail and instant messages to using the Web--can be, and in all likelihood are, trivially monitored by others.

*Source: Counterpane Internet Security
(<http://www.counterpane.com/incidents.html>, 2002)*



Incidents (cont.)

Computer World (08/12/02): NASA Investigates Theft by Hacker

NASA cybercrime investigators are looking into the theft of militarily significant design documents pertaining to the next generation of reusable space vehicles. The documents, which are restricted by export laws from being shared with foreign nationals or governments and are also strictly controlled under the International Trafficking in Arms

*Source: Counterpane Internet Security
(<http://www.counterpane.com/incidents.html>, 2002)*



Incidents (cont.)

ComputerWire 08/07/02):

Database security breaches on the increase

Direct security breaches against databases appear to be on the rise, according to the recently released Summer 2002 Database Developers survey from research firm Evans Data Corp. The report revealed that one in five respondents have experienced a direct breach in security, up significantly from the winter survey six months ago when 12% reported direct breaches.

*Source: Counterpane Internet Security
(<http://www.counterpane.com/incidents.html>, 2002)*



Security Concerns

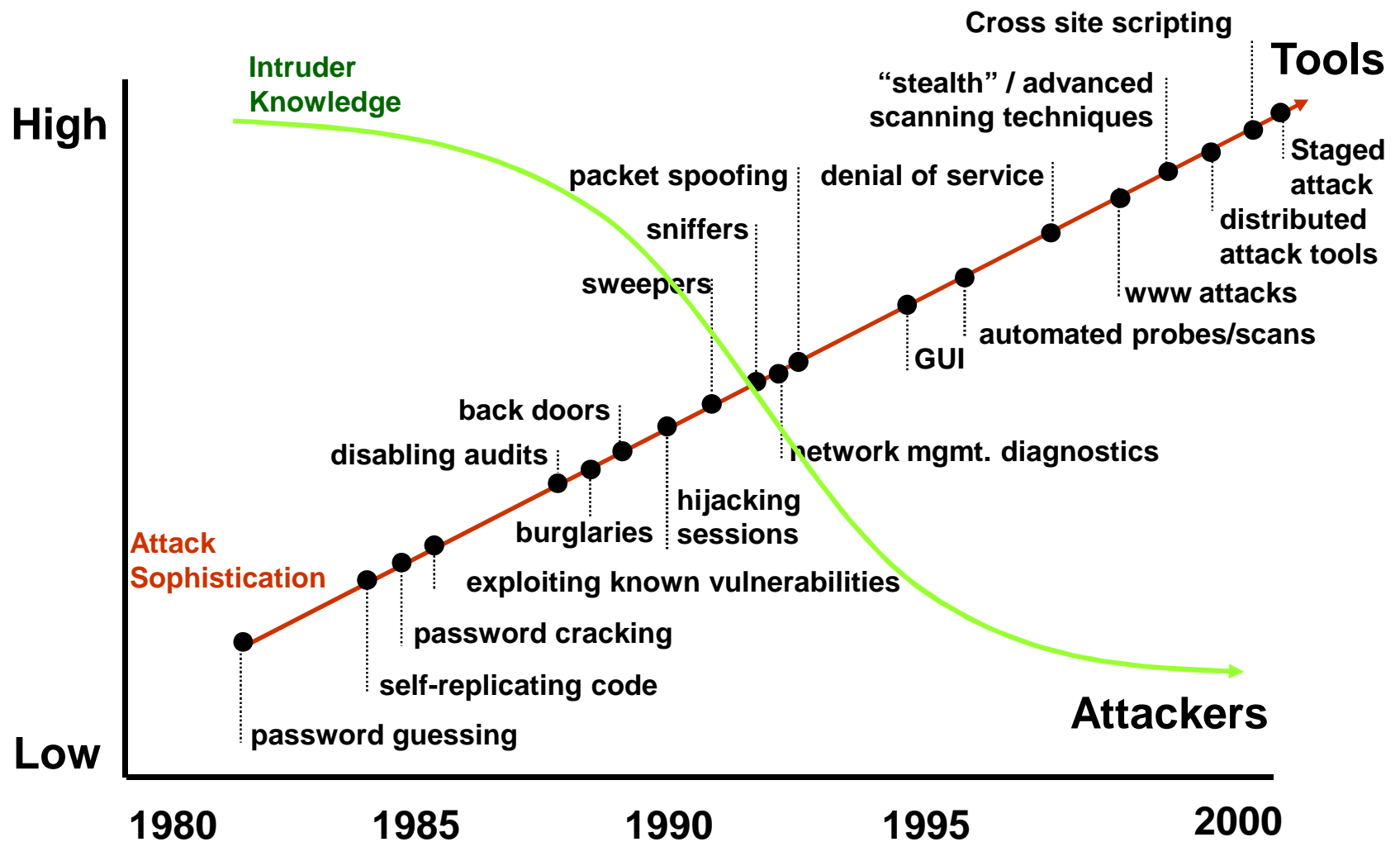
- n Monitoring and capture network traffic
- n Exploitation of software bugs
- n Unauthorized access to resources
- n Masquerade as authorized user or end system
- n E-mail forgery
- n Malicious attacks
- n Etc.



Contributing Factors

- n Increased Internet Usage
(<http://news.bbc.co.uk/2/hi/science/nature/2207259.stm>, 2002)
- n Lack of awareness of threats and risks
- n Wide-open network policies
- n Unencrypted network traffic
- n Complexity of security measurements and administration
- n Software bugs
- n Availability of cracking tools

Attack Sophistication vs. Intruder Technical Knowledge





Security Objectives

- n **Confidentiality**: prevent/detect/deter improper **disclosure** of information
- n **Integrity**: prevent/detect/deter improper modification of information
- n **Availability**: prevent/detect/deter improper **denial of access** to services



Military Example

- n **Confidentiality:** target coordinates of a missile should not be improperly disclosed
- n **Integrity:** target coordinates of missile should be correct
- n **Availability:** missile should fire when proper command is issued



Commercial Example

- n **Confidentiality:** patient's medical information should not be improperly disclosed
- n **Integrity:** patient's medical information should be correct
- n **Availability:** patient's medical information can be accessed when needed for treatment



Fourth Objective

- n **Securing computing resources:**
prevent/detect/deter improper **use** of
computing resources
 - .. Hardware
 - .. Software
 - .. Data
 - .. Network



Achieving Security

n Policy

- .. What to protect?

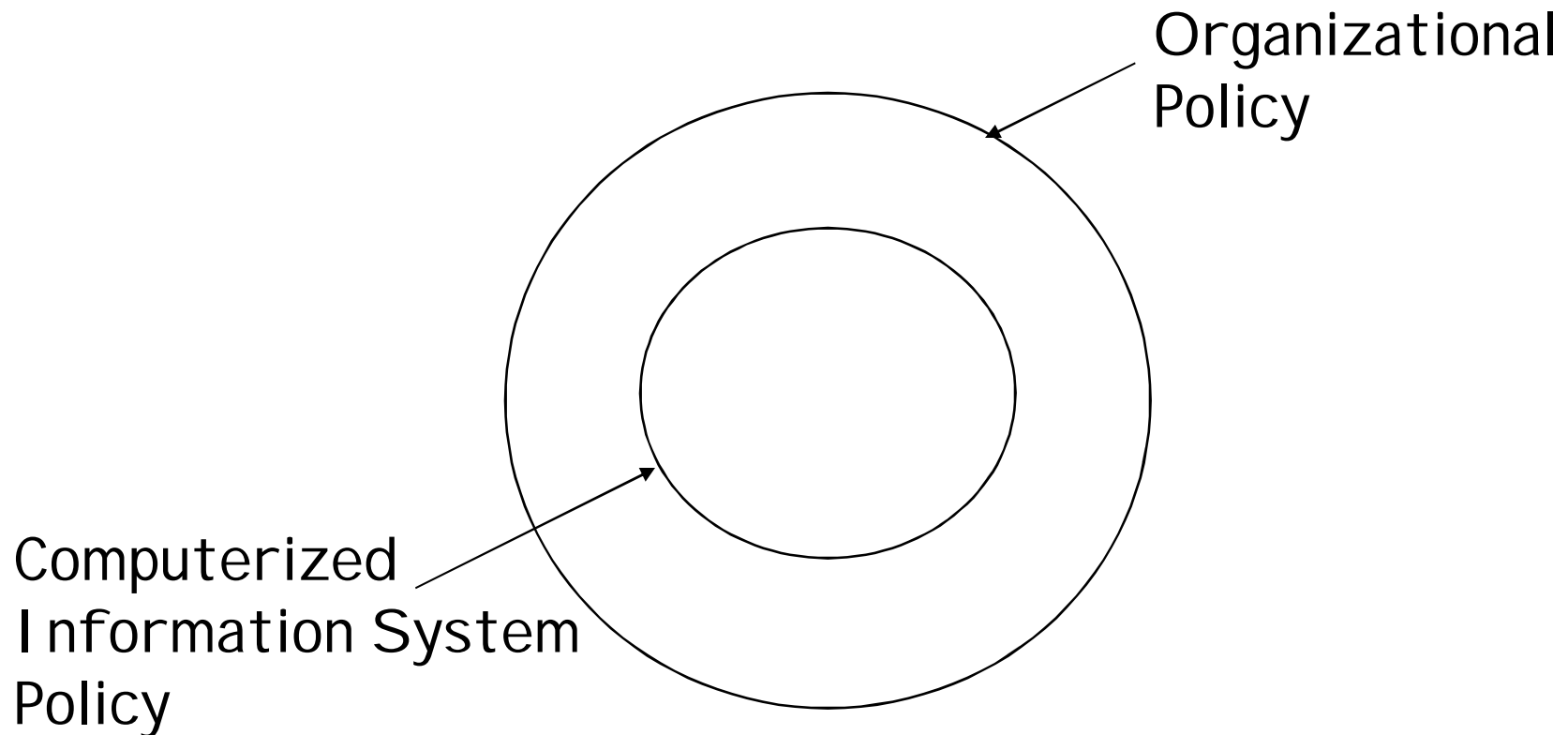
n Mechanism

- .. How to protect?

n Assurance

- .. How good is the protection?

Security Policy





Security Mechanism

- n Prevention
- n Detection
- n Tolerance/Recovery



Security by Obscurity

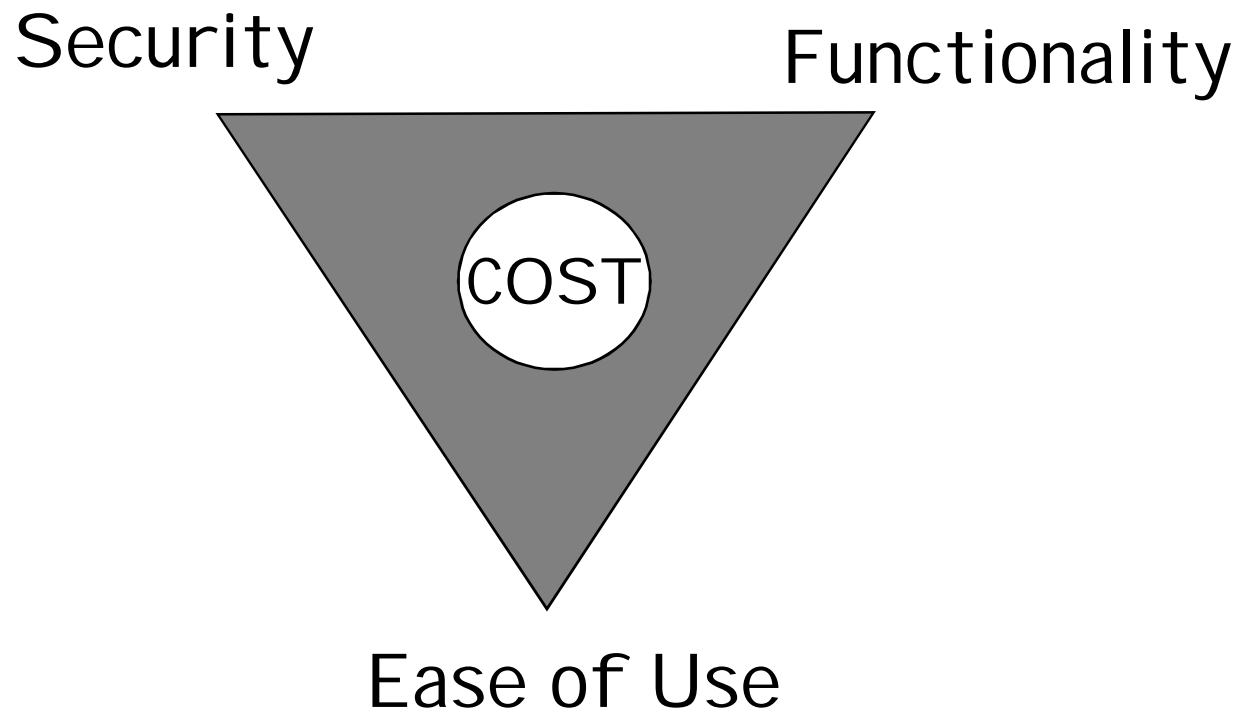
- # Hide inner working of the system
- # Bad idea!
 - n Vendor independent open standard
 - n Widespread computer knowledge

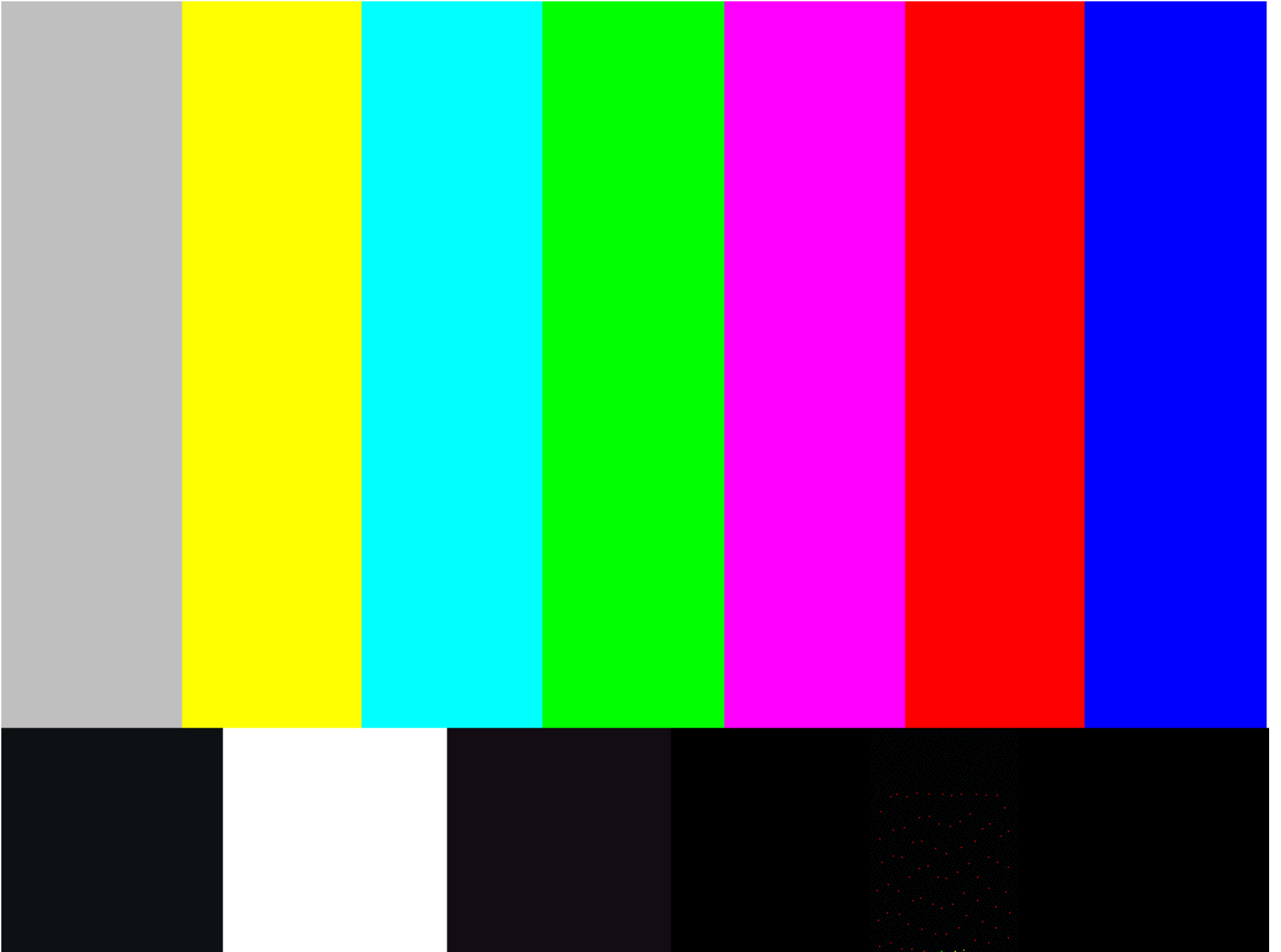


Security by Legislation

- Instruct users how to behave
- Not good enough!
 - n Important
 - n Only enhance security
 - n Targets only some of the security problems

Security Tradeoffs







Basic Security Concepts

- n Threats, Attacks, etc.
- n Computer Criminals
- n Defense Techniques
- n Security Planning



Threat, Vulnerability, Risk

- § **Threat:** potential occurrence that can have an undesired effect on the system
- § **Vulnerability:** characteristics of the system that makes it possible for a threat to potentially occur
- § **Attack:** action of malicious intruder that exploits vulnerabilities of the system to cause a threat to occur
- § **Risk:** measure of the possibility of security breaches and severity of the damage



Types of Threats (1)

- § Errors of users
- § Natural/man-made/machine disasters
- § Dishonest insider
- § Disgruntled insider
- § Outsiders



Types of Threats (2)

- § **Disclosure** threat – dissemination of unauthorized information
- § **Integrity** threat – incorrect modification of information
- § **Denial of service** threat – access to a system resource is blocked



Types of Attacks (1)

- § **Interruption** – an asset is destroyed, unavailable or unusable (*availability*)
- § **Interception** – unauthorized party gains access to an asset (*confidentiality*)
- § **Modification** – unauthorized party tampers with asset (*integrity*)
- § **Fabrication** – unauthorized party inserts counterfeit object into the system (*authenticity*)
- § **Denial** – person denies taking an action (*authenticity*)



Types of Attacks (2)

§ **Passive attacks:**

- § Eavesdropping

- § Monitoring

§ **Active attacks:**

- § **Masquerade** – one entity pretends to be a different entity

- § **Replay** – passive capture of information and its retransmission

- § **Modification** of messages – legitimate message is altered

- § **Denial of service** – prevents normal use of resources



Computer Crime

- n Any crime that involves computers or aided by the use of computers
- n U.S. Federal Bureau of Investigation: reports uniform crime statistics



Computer Criminals

- n **Amateurs:** regular users, who exploit the vulnerabilities of the computer system
 - Motivation: easy access to vulnerable resources
- n **Crackers:** attempt to access computing facilities for which they do not have the authorization
 - Motivation: enjoy challenge, curiosity
- n **Career criminals:** professionals who understand the computer system and its vulnerabilities
 - Motivation: personal gain (e.g., financial)



Methods of Defense

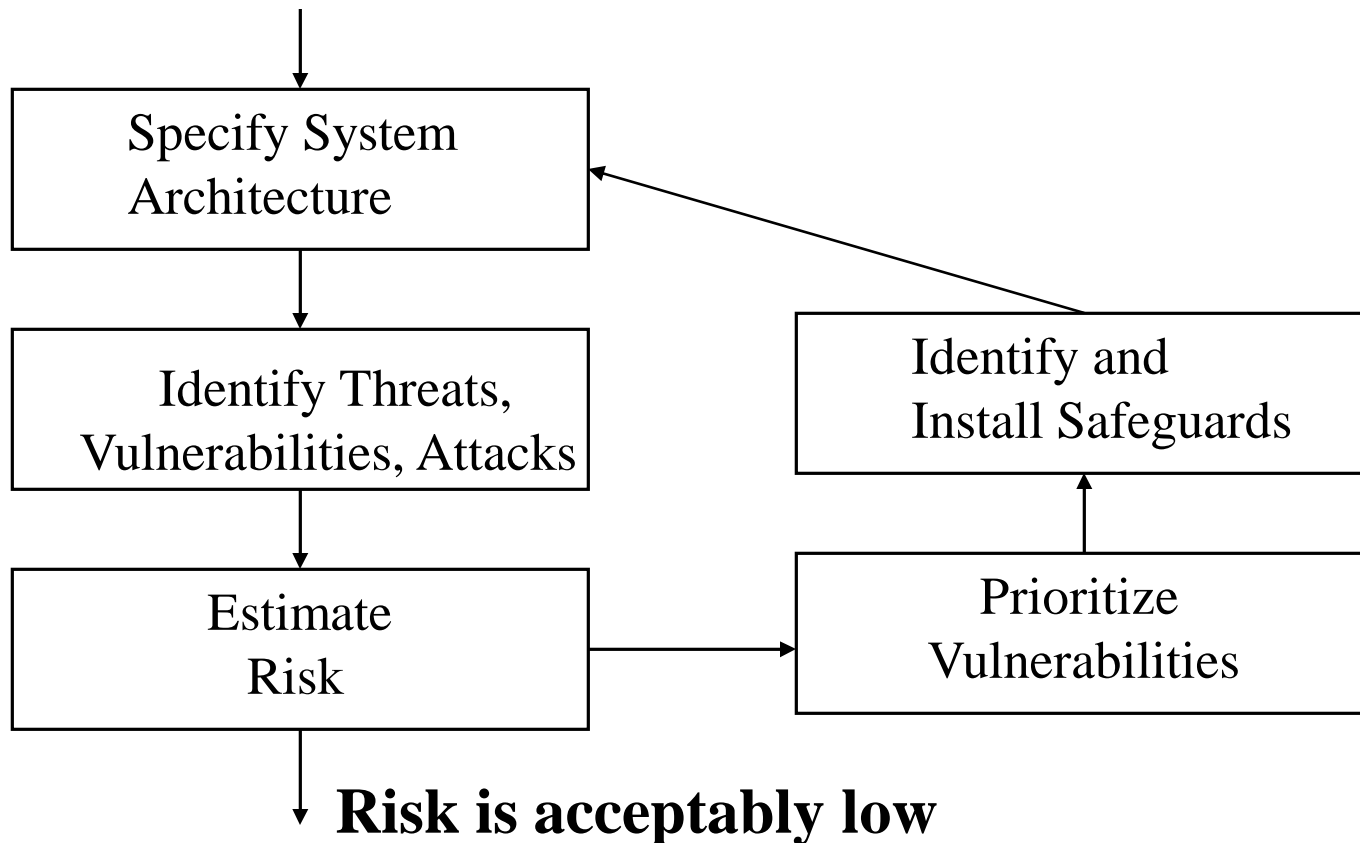
- n **Prevent:** block attack
- n **Deter:** make the attack harder
- n **Deflect:** make other targets more attractive
- n **Detect:** identify misuse
- n **Tolerate:** function under attack
- n **Recover:** restore to correct state



Information Security Planning

- n Organization Analysis
- n Risk management
- n Mitigation approaches and their costs
- n Security policy
- n Implementation and testing
- n Security training and awareness

System Security Engineering





Risk Management

- # Risk analysis
- # Risk reduction
- # Risk acceptance



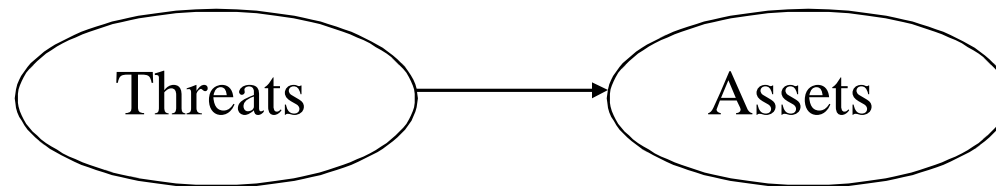
Risk Analysis Methods

n Risk Analysis

- .. Threats and relevance
- .. Potential for damage
- .. Likelihood of exploit

Assets-Threat Model (1)

- # Threats compromise assets
- # Threats have a probability of occurrence and severity of effect
- # Assets have values
- # Assets are vulnerable to threats





Assets-Threat Model (2)

Risk: expected loss from the threat against an asset

$R = V * P * S$

n R risk

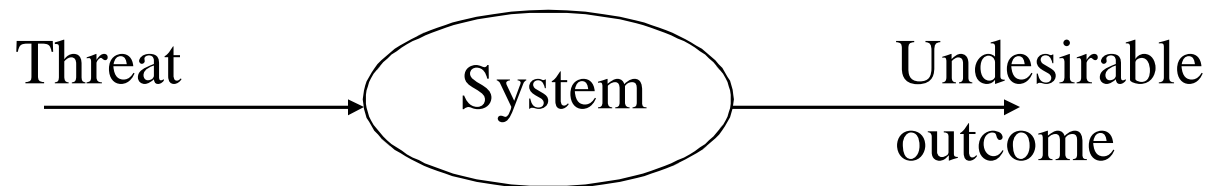
n V value of asset

n P probability of occurrence of threat

n V vulnerability of the asset to the threat

System-Failure Model

- # Estimate probability of highly undesirable events
- # Risk: likelihood of undesirable outcome





Risk Acceptance

Certification

- n How well the system meet the security requirements (technical)

Accreditation

- n Management's approval of automated system (administrative)



Mitigation Approach

n Security safeguards

- .. Protection
- .. Assurance



Cryptography

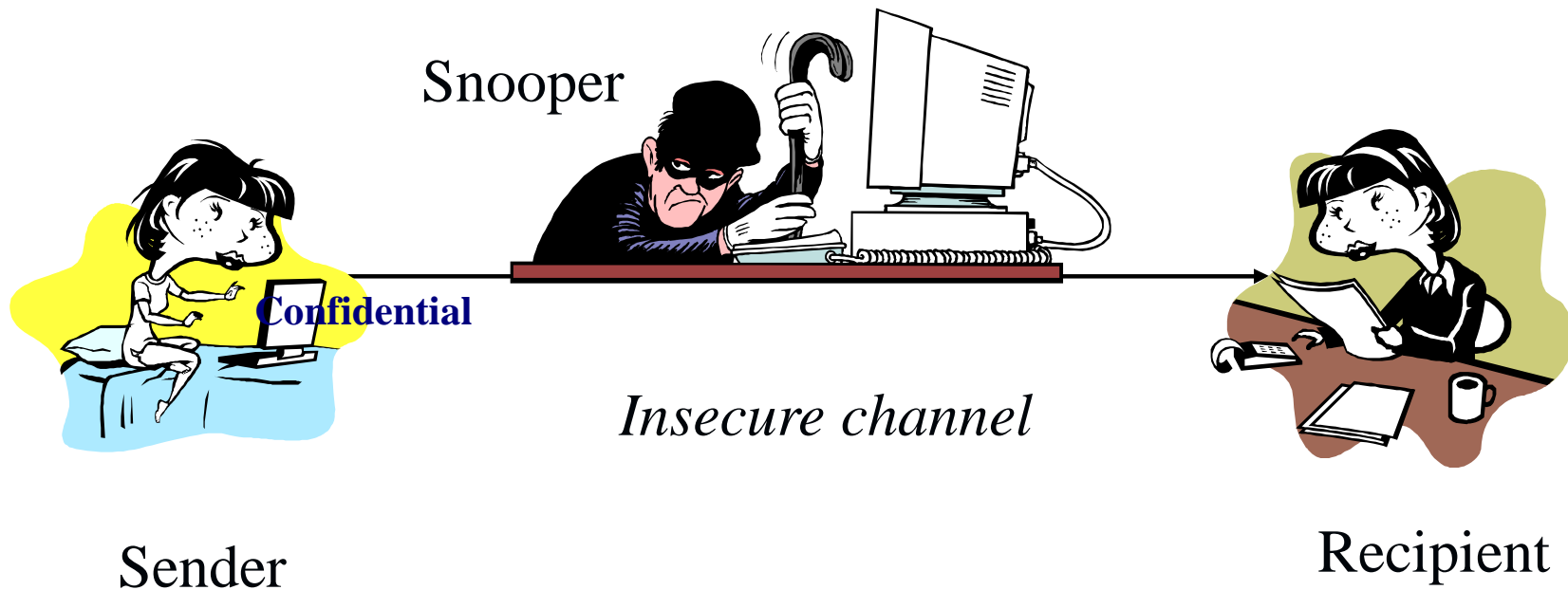
- n Cryptography
- n Terminology
- n Secret-Key Encryption
- n Public-Key Encryption



Cryptography Tools

- n Crypt Breaker's Workbench,
<http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Crypt+Breakers+Workbench>
- n PGP, <http://web.mit.edu/network/pgp.html>
- n Crypto and Security,
<http://www.programmersheaven.com/zone16/cat731/index.htm>

Insecure communications





Cryptographic Protocols

- § Messages should be transmitted to destination
- § Only the recipient should see it
- § Only the recipient should get it
- § Proof of the sender's identity
- § Message shouldn't be corrupted in transit
- § Message should be sent/received once only



Terminology

- § **Plaintext (cleartext):** a message in its original form
- § **Ciphertext (cyphertext):** an encrypted message
- § **Encryption:** transformation of a message to hide its meaning
- § **Cipher:** cryptographic algorithm. A mathematical function used for encryption (encryption algorithm) and decryption (decryption algorithm).



Terminology

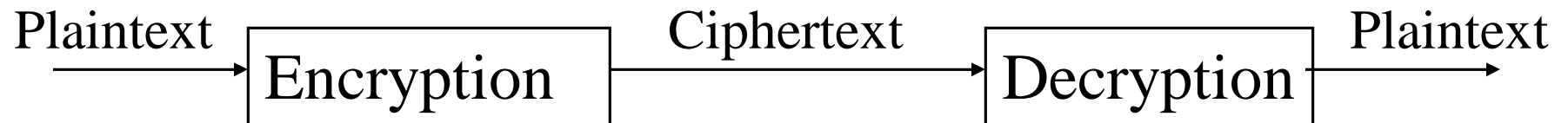
§Decryption: recovering meaning from ciphertext

§Cryptography: art and science of keeping messages secure

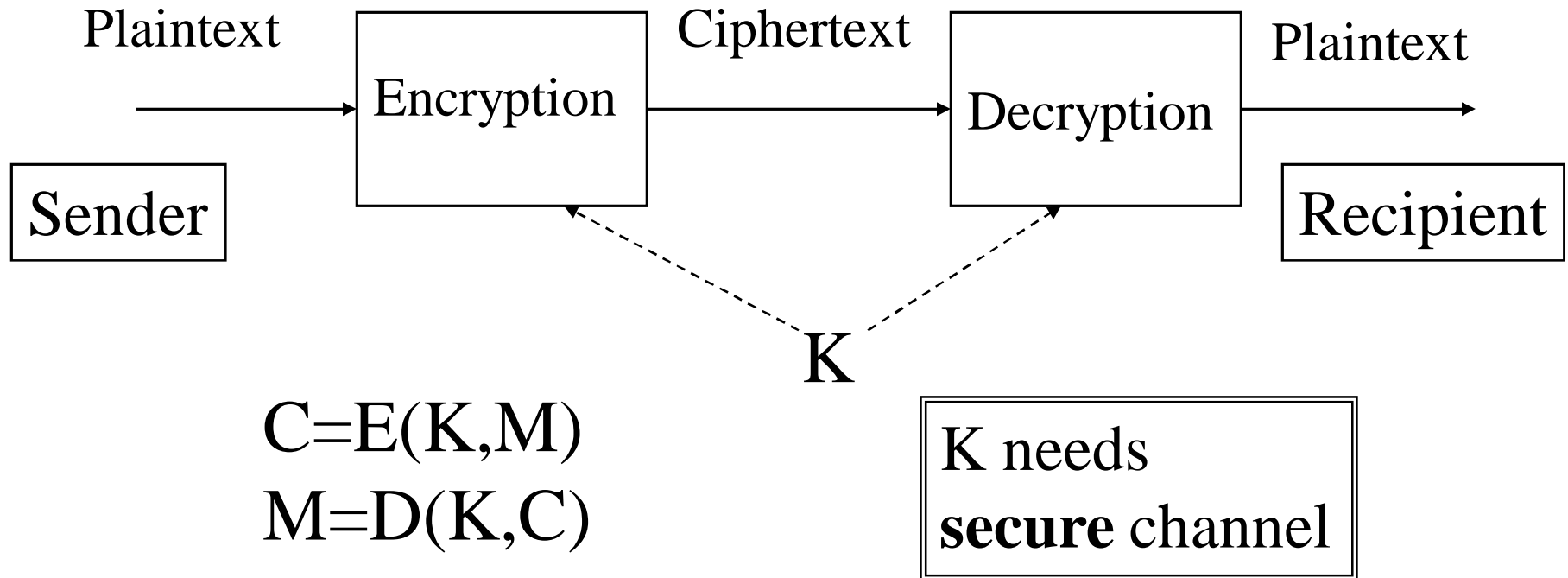
§Cryptanalysis: art and science of breaking ciphertext

§Cryptology: study of both cryptography and cryptanalysis

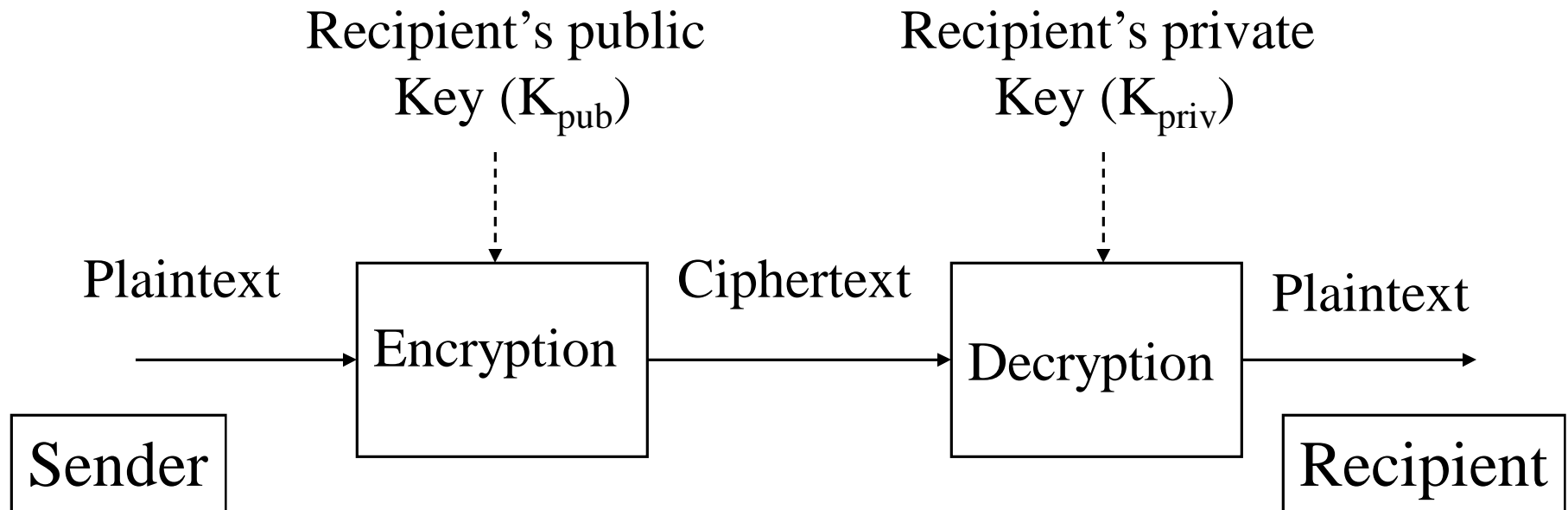
Encryption and Decryption



Conventional (Secret Key) Cryptosystem



Public Key Cryptosystem



$$C = E(K_{pub}, M)$$
$$M = D(K_{priv}, C)$$

K_{pub} needs
reliable channel



Cryptanalysis

Cryptanalyst's goal:

- .. Break message
- .. Break key
- .. Break algorithm



Taxonomy of Attacks

- n **Ciphertext-only attack:** attacker has ciphertext for messages encrypted with E . Deduce *keys* and/or *plaintext* messages.
- n **Known plaintext attack:** attacker additionally knows the plaintext of the messages. Deduce *keys* or a *decryption algorithm*.
- n **Chosen plaintext attack:** attacker can obtain the ciphertext for selected plaintext messages. Deduce *as above*.
- n **Chosen ciphertext attack:** attacker can obtain decrypted (plaintext) versions of selected ciphertext. Deduce *as above*.



Breakable versus Practically breakable

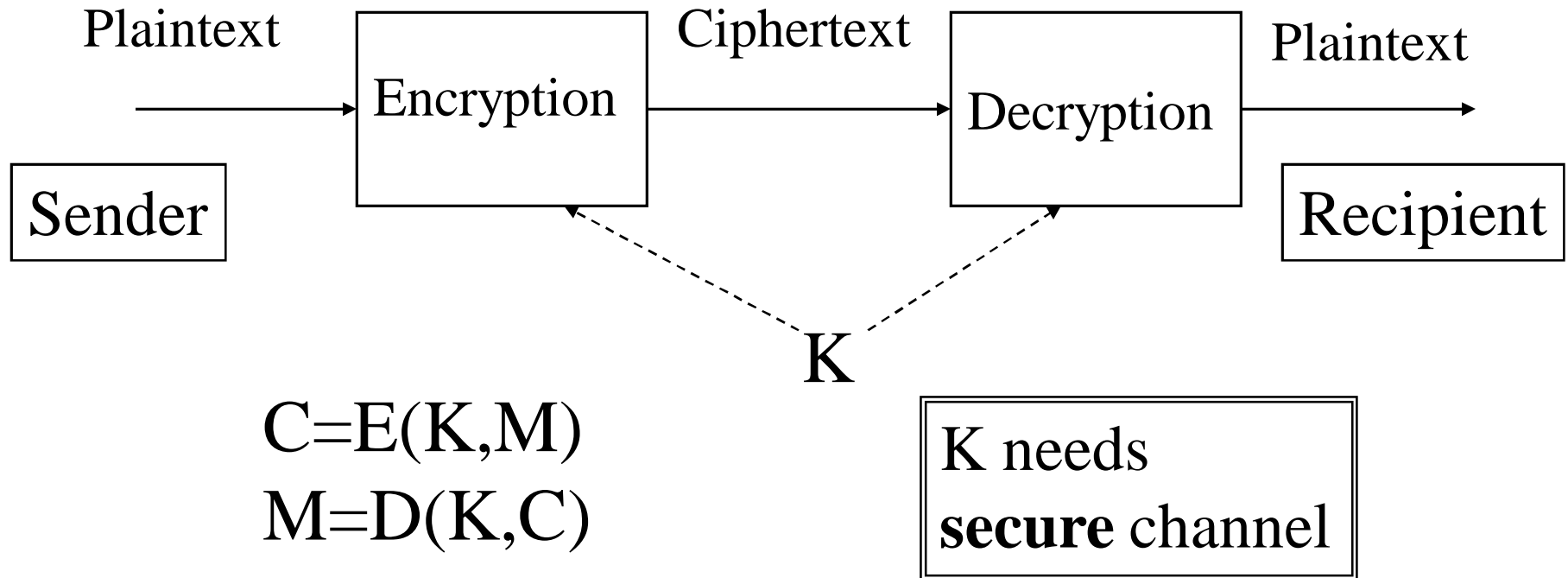
- n Unconditionally secure:** impossible to decrypt. No amount of ciphertext will enable a cryptanalyst to obtain the plaintext
- n Computationally secure:** an algorithm that is not breakable in practice based on worst case scenario
- n Breakable:** all algorithms (except one-time pad) are theoretically breakable



What makes a good cryptosystem?

- § A good cryptosystem is one whose security *does not depend* upon the secrecy of the algorithm.
- § From Bruce Schneier:
 - § “Good cryptographers rely on peer review to separate the good algorithms from the bad.”

Secret Key Cryptosystem





Secret Key Cryptosystem Vulnerabilities (1)

Passive Attacker (Eavesdropper)

- n Obtain and/or guess key and cryptosystem use these to decrypt messages
- n Capture text in transit and try a ciphertext-only attack to obtain plaintext.



Secret Key Cryptosystem Vulnerabilities (2)

Active Attacker

- n Break communication channel (denial of service)
- n Obtain and/or guess key and cryptosystem and use these to send fake messages



Inherent Weaknesses of Symmetric Cryptography

- § **Key distribution** must be done secretly (difficult when parties are geographically distant, or don't know each other)
- § Need a **key for each pair of users**
 - § n users need $n*(n-1)/2$ keys
- § If the **secret key** (and cryptosystem) is **compromised**, the adversary will be able to decrypt all traffic and produce fake messages



Basic Encryption Techniques

- n Substitution
- n Permutation
- n Combinations and iterations of these

Caesar cipher

n $C=E(K,M)$, e.g., $C=(M+n) \bmod 26$

plaintext placement:

A B C D E ...

ciphertext placement:

A B C D E F ...

e.g., $M=CAB$

$C=ECD$

n **Advantages:** simple to implement

n **Disadvantages:** easy to break (25 possibilities for English alphabet)



Simple Alphabetic Substitution

n Assign a new symbol to each plain text symbol randomly, e.g.,

C → K, A → H, B → L

M=CAB

C =KHL


§ **Advantages:** large key space 26!

§ **Disadvantages:** trivially broken for known plaintext attack



One-Time Pad

- n Perfect Secrecy!
- n Large, non-repeating set of keys
- n Key is larger than the message
- n **Advantages:** immune to most attacks
- n **Disadvantages:**
 - .. Need total synchronization
 - .. Need very long, non-repeating key
 - .. Key cannot be reused



Summary of Substitution

n Advantages:

- Simple
- Easy to encrypt

n Disadvantages:

- Easy to break!!!

