

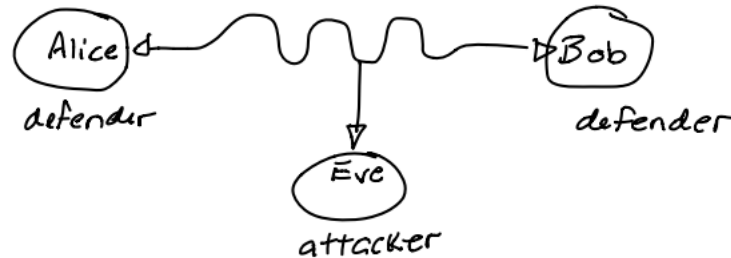
Lecture 2.1

1. What is IT Security?
 - IT security is the prevention of, or protection against
 - access to info by unauthorized recipients
 - intentional but unauthorized destruction or alteration of that info
2. What's at stake?
 - Computer systems make up assets that have value to it
 - Time sensitive value:
 - At one point it means something but at another it doesn't
 - Valuable assets deserve security protection
 - Preserve value -> expressed as a *security property*
 - * Personal photos should always be accessible by their owner
 - Prevent harm -> examined as a concrete *attack*
 - * Permanent destruction of irreplaceable photos
3. What are the players?
 - Defender:
 - System owners (users, admins)
 - Attackers:
 - Hackers or possibly owners
4. Security properties
 - CIA Triad: Confidentiality, Integrity, Availability
5. The CIA Triad
 - Comp security seeks to prevent unauthorized viewing (confidential) or modification (integrity) of data while preserving access (availability)
6. Confidentiality
 - An asset is viewed only by authorized parties
 - Through encryption etc.
7. Integrity
 - An asset is modified only by authorized parties
 - Beyond the normal "write" access-control rules
 - Precise, accurate, unmodified, modified in acceptable way by authorized people or processes, consistent, meaningful and usable
 - * Consistency: the same file you have gets updated with every push/change, it's not an old file that didn't stage changes
8. Availability
 - An asset can be used by any authorized party
 - Timely response, fairness, concurrency
 - Tools: redundancy, fault tolerance, distributed architectures
 - DDOS attacks this specifically

Lecture 2.2 - Symmetric Key Encryption

1. Recall - Confidentiality

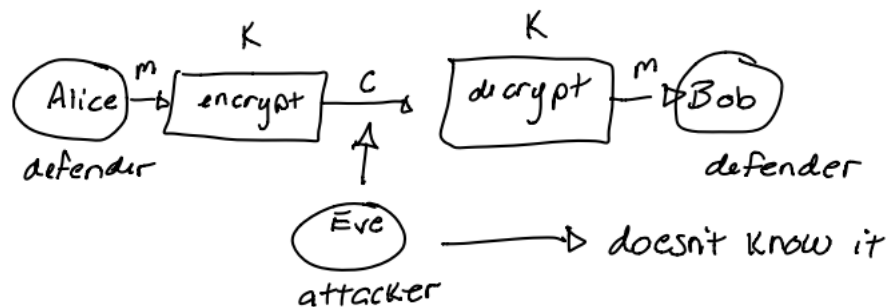
- Eavesdropping
 - Main threat against confidentiality of in-transit data



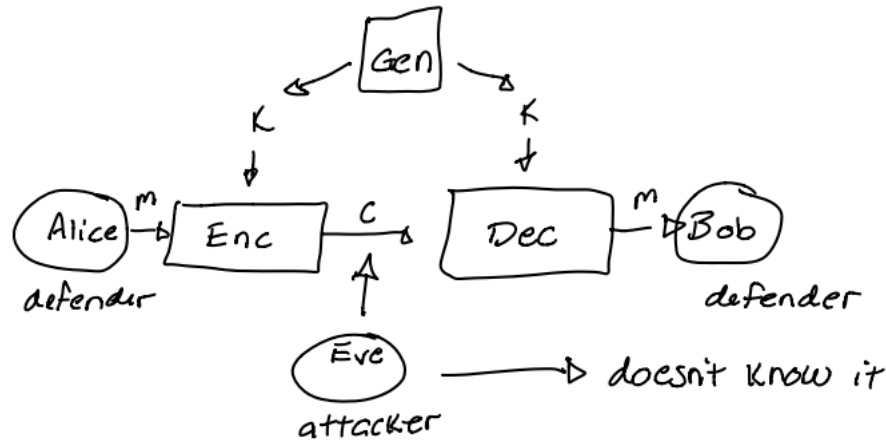
- Attacker: packet sniffing over networked or wireless communications

2. Solution concept: Symmetric-key encryption

- Main idea:
 - Secretly transform message so that it is unintelligible while in transit
 - Alice encrypts her message (m) to ciphertext (c), which is sent instead of plaintext (m)
 - Eve can intercept (c) but won't know (m)
 - Alice and Bob share secret key (k) that is used for both message transformations



- Abstract cryptographic primitive (**cipher**) defined by:
 - A message space M and a triplet of algorithms (Gen, Enc, Dec)
 - Gen, Enc are probabilistic algorithms, whereas Dec is deterministic
 - * Probabilistic employs some sort of randomness (variable output) whereas deterministic does not use any randomness (always the same output)
 - Gen outputs a uniformly random key (k) (from some key space K - all possible key values)



3. Desired Properties for Symmetric-key encryption solution

- Should satisfy:
 - Efficiency: key generation & message transformations “are fast”
 - Correctness: For all m and k , it holds that $\text{Dec}(\text{Enc}(m, k), k) = m$
 - Security: one “cannot learn” plaintext m from ciphertext c

4. Kirchoff’s Principle

- “The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.”
- Reasoning:
 - Due to security & correctness, Alice and Bob must share some secret info
 - If no shared key captures this secret info, it must be captured by Enc and Dec
 - But keeping Enc, Dec secret is problematic
 - * Harder to keep secret an algorithm than a short key (eg. after user revocation)
 - * Harder to change an algorithm than a short key (eg. after secret info exposed)
 - * Riskier to rely on custom/ad-hoc schemes than publicly scrutinized/standardized ones

5. Main Application Areas

- Secure communication
 - Encrypt messages sent among parties
 - Assumption:
 - * Alice and Bob securely generate, distribute, and store shared key k
 - * Attacker does not learn key k
- Secure storage
 - Encrypt files outsourced to the cloud
 - Assumption:
 - * Alice securely generates and stores key k
 - * Attacker does not learn key k

6. Brute Force Attack

- Generic attack
 - Given a captured ciphertext c and known key space K , Dec
 - Strategy is an exhaustive search
 - * For all possible keys k in K
 - Determine if $\text{Dec}(c, k)$ is a likely plaintext m
 - Requires some knowledge on the message space M
 - * ie. Structure of the plaintext (eg. PDF file or email message)
- Countermeasure
 - Key should be a random value from a **sufficiently large** key space K to make exhaustive search attacks infeasible

7. Substitution Ciphers

- Large class of ciphers
 - Each letter is uniquely replaced by another
 - There are $26!$ possible substitution ciphers
- 8. Classical Ciphers
 - Cryptanalysis
 - No secret key issued
 - Thus the code is trivially insecure once someone knows Enc or Dec