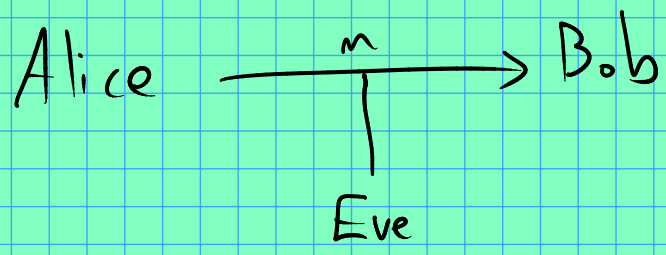
Outline / Topics

- Cryptography ⊛
- Network Security
- Software security (Meltdown, Spectre, ROP...)
- Practical stuff — How to improve your own security on Linux/BSD.

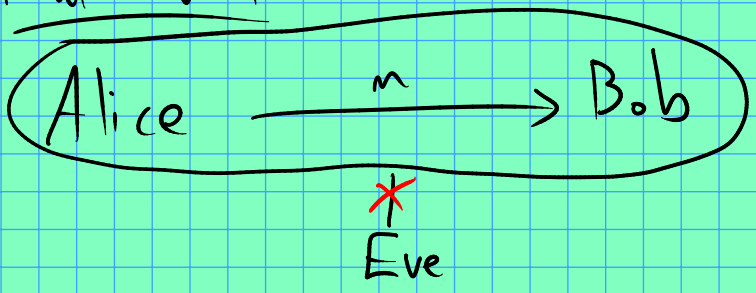
Crypto time...

Encryption Schemes

Goal, abstractly, is to take the real world situation:



to the ideal world:



Idea: can Alice + Bob modify their communication method to "implement" the ideal world in the real world?

Alice can transform her message through some encoding function $E(\cdot)$.

Bob will decode via some process $D(\cdot)$.

Say $M \equiv$ space of all possible messages

$C \equiv$ space of possible encoded messages.

$$E: M \to C, \quad D: C \to M.$$

Ground rules / desirable properties:

① E, D algorithms are public knowledge.

(No "security via obscurity")

Rationale: algorithms are hard to come up with! Ideally secrets should be essentially random strings.

② Decryption should always "work":

$D \circ E$ = identity map

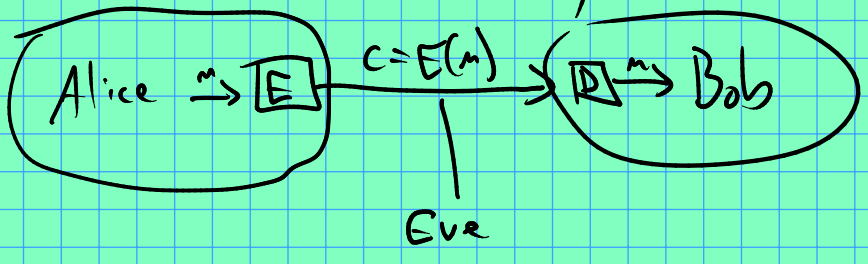
(i.e., $D(E(m)) = m \quad \forall m \in M$)

③ Scheme resists an <u>unbounded</u> adversary Eve.

(Eve can perform any computation <u>instantly</u>.)

Consequences of ①, ②, ③:

for one, Alice must have some secret info that Eve does not know. Why?



Eve could compute $E(m)$ $\forall m \in M$.

If Alice has no secret, this reveals the message to Eve.

Let's introduce keys: Say $E: M \times K \to C$ and

$D: C \times K \to M$

K = space of all keys.

Turns out that Bob must also keep a secret from Eve. Furthermore, Bob must <u>share</u> secret info w/Alice! (Public key crypto impossible in this model!)

Note that Eve can compute all "explanations" of a ciphertext c:

$$X_c = \{ m \in M \mid E(m,k) = c \text{ for some } k \in K \}$$

Say $|X_c| = 1$. Then Eve at once knows the message!

So it must look like this:

$$c = E(m_0, k_0) = E(m_1, k_1) = E(m_2, k_2) \cdots$$

$$(X_c = \{m_0, m_1, \ldots\})$$

So Bob must know something about k, or he won't be able to properly decrypt! (requirement ②)

Intuitively, want large $|X_c|$ to maximize uncertainty in Eve's mind.

Security definitions

Models "a priori knowledge" Eve might have

Shannon Security: For all probability distributions on M, the induced distribution on C is independent (choose random $m \in M$ and random $k \in K$. Then output $c = E(m,k)$):

$$\Pr_{m,k}(M = m \mid C = c) = \Pr_{m}(M = m).$$

I.e., C is independent from M!

(Note: we will usually assume messages are of a fixed length...)

Alternate definition:

Perfect security: $\forall\, m, m' \in M$, $c \in C$

$$\Pr_{k \in K}(E(m,k) = c) = \Pr_{k \in K}(E(m',k) = c)$$

Example: "one time pad" (OTP)

$$M = \{0,1\}^l, \quad C = \{0,1\}^l, \quad K = \{0,1\}^l$$

For $m \in M$, $k \in K$

$$E(m,k) \triangleq m \oplus k \qquad (\text{"}\oplus\text{"} \equiv \text{bitwise XOR})$$

For $c \in C$, $k \in K$

$$D(c,k) \triangleq c \oplus k$$

Clearly "correct": $D(\underbrace{m \oplus k}_{c}) = m \oplus k \oplus k = m \oplus (\underbrace{k \oplus k}_{=0^l}) = m$

Security? Let's think about the distribution induced on C by encrypting $m \in M$ w/ a random key:

For any fixed $c \in C$,

$$\Pr_{k \in K}(E(m,k) = c) = \frac{1}{|\text{keys}|} = \frac{1}{2^l}$$

If $m \oplus k = c$, then $k = m \oplus c$.

I.e., there is a unique key k that produces c.

This already shows OTP is perfectly secure:

$\forall m, m' \in M$, $c \in C$,

$$\Pr_{k \in K}(E(m,k) = c) = 2^{-l} = \Pr_{k \in K}(E(m',k) = c) \quad \checkmark$$

Practical concerns: can't reuse key k!

Say $c = E(m,k)$, $c' = E(m',k)$.

Then $c \oplus c' = m \oplus m'$

That is, key must be as long as message and cannot be reused!

Claim: if $|K| < |M|$ (and say each $m \in M$ might occur w/ nonzero probability), then the encryption scheme cannot be perfectly secure. (or Shannon)

(So OTP (with $|K| = |M|$) is in some sense optimal.)

Proof: Say Eve observes ciphertext c, and suppose $|K| < |M|$.

She can compute

$$X_c = \{ D(c,k) \mid k \in K \}$$

$$|X_c| \leq |K| \lneq |M|.$$

Then $M \setminus X_c \neq \{\}$ $\quad (A \setminus B = A \cap \bar{B})$

s.t. $\exists\, m^* \in M$ s.t. $m^* \notin X_c$.

$\therefore \quad Pr(M = m^* \mid C = c) = 0$ ⊛

$\neq Pr(M = m^*) > 0$ by assumption.

So scheme is not secure. ✓

(Eve "learned" that message from Alice was not m^*.)

Sort of disappointing, but requirement ③ (unbounded Eve) seems quite strong. Maybe with some assumptions on computational bounds for Eve we can do better?

E.g. what if we assume it it "hard" for Eve to factor huge integers? What does "hard" even mean?...