Lecture 2

Quantitative Definition and Evaluation of Security

2/10/2020

Nicola Laurenti October 2, 2020

Lecture 2— Contents

Randomized attacks and defenses

Unconditional vs computational security

Composition of security mechanisms

Security against a single attack

We model a single attack as a randomized algorithm A, characterized by:

- a success event S_A
- its execution time T_A, (which is a random variable, in general)

Similarly, we model a security mechanism as a randomized algorithm M, characterized by its execution time T_M, (which may also be a random variable)

Security measure

The security provided by mechanism M against attack A can be measured by the conditional probability

$$\mathrm{P}\left[S_A | A, M\right]$$

that the success event S_A is achieved by attack A with mechanism M.

Security against a class of attacks

Consider a class $\mathcal{A}$ of attacks with a common success event $S_{\mathcal{A}}$.
Then, the security of a mechanism M against the class $\mathcal{A}$ of attacks is measured by

$$\sup_{A \in \mathcal{A}} \mathrm{P}\left[S_{\mathcal{A}} | A, M\right]$$

It is also customary to measure the security level of M against $\mathcal{A}$, in bits, as

$$\mathrm{SL}(M) = \log_{1/2} \sup_{A \in \mathcal{A}} \mathrm{P}\left[S_{\mathcal{A}} | A, M\right] \qquad \text{[bits]}$$

Typically, the mechanism is designed with the aim of being secure against the widest possible class of attacks.

Unconditional security

Definition

A security mechanism is said to offer ε-unconditional security against a class $\mathcal{A}$ of attacks, for some $\varepsilon > 0$, if

$$\mathrm{P}\left[S_{\mathcal{A}} | A, M\right] \leq \varepsilon \quad , \qquad \forall A \in \mathcal{A}$$

that is, all attacks in $\mathcal{A}$ succeed against M with probability no more than ε

Computational security, concrete formulation

Definition

A security mechanism is said to offer (ε, T_0)-computational security against a class $\mathcal{A}$ of attacks, for some $\varepsilon > 0, T_0 > 0$, if

$$\mathrm{P}\left[S_{\mathcal{A}} \cap \{T_A \leq T_0\} \,|A, M\right] \leq \varepsilon \quad , \quad \forall A \in \mathcal{A}$$

that is, all attacks in $\mathcal{A}$ succeed against M within time T_0 with probability no more than ε

Note

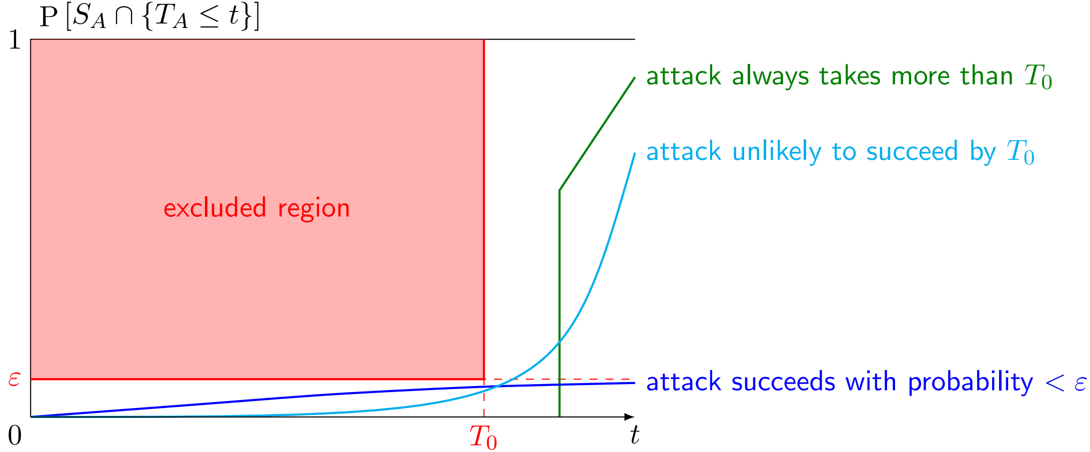
The above definition is equivalent to saying that

$$\mathrm{P}\left[S_{\mathcal{A}}|A, M\right] \leq \varepsilon \quad , \quad \forall A \in \mathcal{A} \text{ such that } T_A \leq T_0 \text{ surely}$$

that is, all attacks in $\mathcal{A}$ that take up to T_0 time succeed against M with probability no more than ε

Graphical interpretation of concrete computational security

Success probability vs running time



Computational security, asymptotic formulation

The problem with the concrete formulation is that the definition depends on the state of technological maturity

To overcome this problem, we allow the mechanism to depend on a security parameter $n \in \mathbb{N}$ (e.g., the length of cryptographic keys, the entropy of signatures, the number of rounds in an interactive protocol) that can be increased at will so that

- the legitimate operation is still feasible (complexity depends on n polynomially)
- the adversary operation soon becomes infeasible (superpolynomial complexity increase or success probability decrease)

Computational security, asymptotic formulation

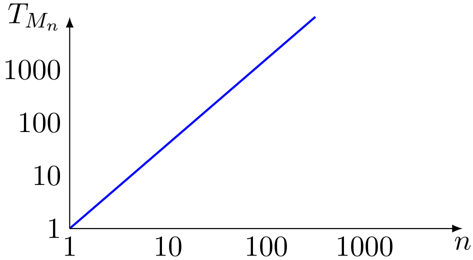
Definition

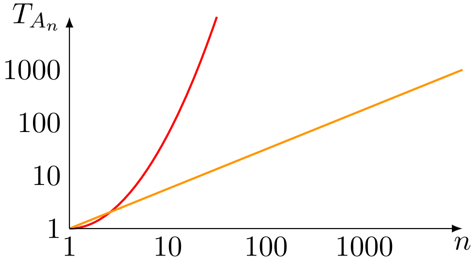
A sequence of security mechanisms $\{M_n\}$, indexed by some parameter $n \in \mathbb{N}$ is said to offer asymptotic security against a class $\mathcal{A}$ of attacks, if

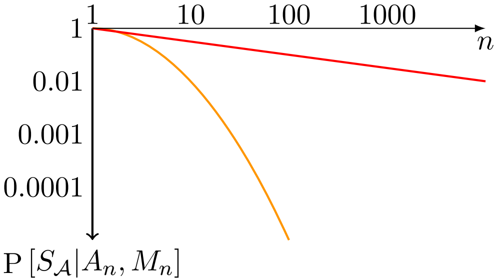
1. $\exists$ polynomial $p(\cdot)$, such that,
$$\forall n \quad , \quad T_{M_n} \leq p(n)$$
2. $\forall q(\cdot), s(\cdot)$ polynomials and sequence of attacks $\{A_n\} \subset \mathcal{A}$, $\exists\, n_0$ such that
$$\forall n > n_0 \quad , \quad \mathrm{P}\left[S_{\mathcal{A}} \cap \{T_{A_n} \leq q(n)\} \,|A_n, M_n\right] < \frac{1}{s(n)}$$

It is also said that the probability of the attack succeeding in polynomial time vanishes super polynomially, i.e. that it is asymptotically negligible

Graphical interpretation of asymptotic computational security







$\{M_n\}$ has polynomial complexity

$\{A_n\}$ has superpolynomial complexity and polynomially vanishing success probability in n

$\{A_n\}$ has polynomial complexity and super polynomially vanishing success probability in n

Review question

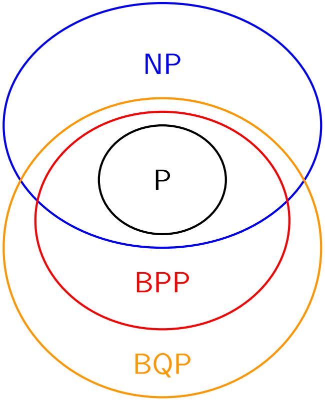
Problem

Which of the following would disprove the statement
"Mechanism M is (ε, T_0)-computationally secure with $\varepsilon = 10^{-10}$ and $T_0 = 3$ years"?

- A_1 : An attack $A_1 \in \mathcal{A}$ which has a deterministic running time $T_{A_1} = 1$ year and success probability $P[S_{\mathcal{A}}|A_1, M] = \varepsilon^2$
- A_2 : An attack $A_2 \in \mathcal{A}$ that succeeds against M with certainty and has a deterministic running time $T_A = 10$ years
- A_3 : An attack $A_3 \in \mathcal{A}$ that succeeds against M with certainty and has a random running time T_{A_3} exponentially distributed with mean $\mathrm{E}\left[T_{A_3}\right] = 10$ years

Answer (anonymously) on the Moodle page

Relationship with computational complexity classes



Briefly, and informally, speaking

- **P** are problems that can be solved by a deterministic algorithm in polynomial time
- **NP** are problems for which a candidate solution can be verified by a deterministic algorithm in polynomial time
- **BPP** are problems that can be solved with "good" success probability by a probabilistic algorithm in polynomial time
- **BQP** are problems that can be solved with "good" success probability by a quantum algorithm in polynomial time

Relationship

Asymptotic computational security $\Leftrightarrow$ attacking $\{M_n\} \notin$ BPP

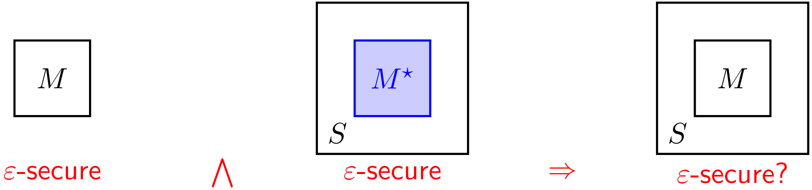
Composition of security mechanisms

Consider a security mechanism S that makes use of another mechanism M, and denote this occurrence by $S[M]$.

Let $S[M^\star]$ denote the same mechanism S where M is replaced by its ideal counterpart $M^\star$.

The *composability* question

Is it possible to derive the security of $S[M]$ from those of M and $S[M^\star]$?



Not with the definitions so far! (based on attack success probability)

We will need a different security metric. . . stay tuned for the next lecture!

A trivial counterexample

Consider the following mechanisms:

- S an encryption system employing a L-bit key but actually making use only of the first $L/2$ bits → usa $L/2$
- M a key generation mechanism that outputs a L-bit key where the first $L/2$ bits are deterministic and only the last $L/2$ bits are uniform
- $M^\star$ an ideal key generation mechanism that outputs a perfectly uniform L-bit key ← tutto uniform

with the metric based on attack success probability

- $S[M^\star]$ is (at least) ε-unconditionally secure against eavesdropping with $\varepsilon = 1/2^{L/2}$
- M is ε-unconditionally secure against guessing the key with $\varepsilon = 1/2^{L/2}$

yet $S[M]$ is totally insecure because it employs the deterministic key bits. ← usa solo quelli det.

