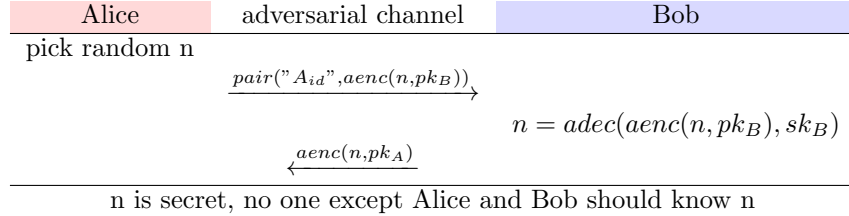


Lecture Notes: Dolev-Yao Model

Introduction

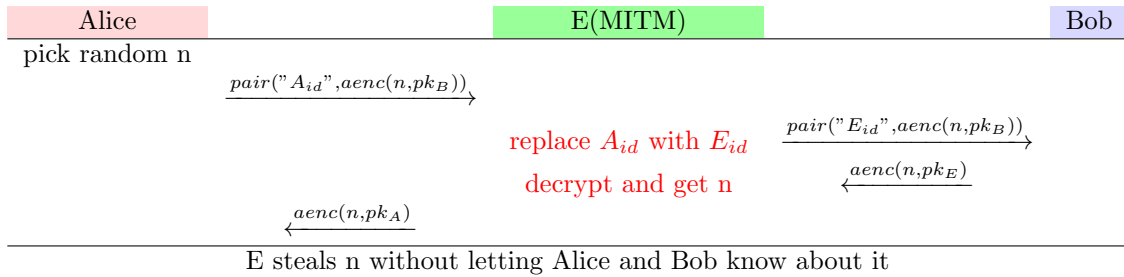
The Dolev-Yao model was given by D. Dolev and A. Yao in their paper titled: On the security of public key protocols. The model is used to mathematically prove(or disprove) that a cryptographic protocol is secure or not.

We have discussed the following protocol in class:



Question : Can n come into the knowledge-base of the adversary(E)?

Yes, E can act as a man-in-the-middle & can easily infer the secret n , although it is encrypted:



Clearly, this protocol is not secure. Try proving it using the Dolev-Yao model.

What is structure of the knowledge-base?

The knowledge-base includes:

1. terms := keys | messages | nonces ; Any operator applied to a term(s) gives a term.
2. operators := hash | aenc | adec | senc | sdec | sign | ver ; etc..
 Term grammar $t := m \mid n \mid id \mid k \mid \text{hash}(t) \mid \text{aenc}(t, k) \mid \text{adec} \mid \text{sign}(t, id) ; \text{etc} \dots$
3. Equations := $\text{adec}(\text{aenc}(m, k), k^{-1}) = m$, $\text{ver}(\text{sign}(t, id), t, id) = \text{true}$ etc..
 Term algebra := terms & how they are related to equations.

Expanding the knowledge-base

How do agents expand their knowledge-base? – using derivation rules.

A few derivation rules are given below:

1. $\frac{}{X \cup \{t\} \vdash t} ax$
2. $\frac{X \vdash \text{pair}(t_0, t_1)}{X \vdash t_i} \text{split}_i$
3. $\frac{X \vdash \text{enc}(t, k) \quad X \vdash \text{inv}(k)}{X \vdash t} \text{dec}$
4. $\frac{X \vdash t \quad X \vdash k}{X \vdash \text{enc}(t, k)} \text{enc}$
5. $\frac{X \vdash t_0 \quad X \vdash t_1}{X \vdash \text{pair}(t_0, t_1)} \text{pair}$

Read $\frac{X \vdash t \quad X \vdash k}{X \vdash \text{enc}(t, k)} \text{enc}$ as : If X derives t and X derives k , then X can derive $\text{enc}(t, k)$; X is the knowledge-base.

Rules 1, 2 and 3 are called elimination rules and 4, 5 are called introduction rules.

Derivability Problem : Given $\{X, t\}$, does $X \vdash t$ according to the derivation rules?

Proving the security of cryptographic protocols

A cryptographic protocol is secure when throughout the protocol, at every state, $X_I \not\vdash t$.

The problem is undecidable for active adversaries (but why? – read yourself).

We discuss the case of passive adversaries.

$t := m \mid \text{pair}(t_0, t_1) \mid \text{aenc}(t, k)$

Define **Subterm**: A subterm $st(t)$ is a set S such that:

i $t \in S$

ii $\text{pair}\{t_1, t_2\} \in S, \{t_1, t_2\} \subseteq S$

iii $\text{aenc}(t', k) \in S, \{t', k\} \subseteq S$

What are the subterms in $\text{pair}(\text{aenc}(t, k), \text{pair}(t', t''))$?

Property: $|st(t)| \leq |t|$ and $st(X) = \cup_{t \in X} st(t)$, X is the set of terms.

Define **Normal derivation**: Major premise (numerator) of elimination rule must be the conclusion of an elimination rule.

Theorem: If there is a derivation $X \vdash t$, then there also exists a normal derivation $X \vdash t$.

Fact: shortest proofs are always normal.

Subterm property: In a normal derivation $X \vdash t$, $X \vdash S$ occurs, then $S \in st(X \cup \{t\})$

Can $X \vdash t$?

The following algorithm decides this for a passive intruder:

Let $N = |st(X \cup \{t\})|$, $Y := X$, $i = 0$

while $i \leq N$ **do**:

$Z :=$ All terms derivable from Y in one step

$Y := Z$

$i := i + 1$

check if $t \in Y$?

If at all possible, a passive intruder can know the secret(t) in N steps.

But if it cannot infer in more than N steps, then it cannot infer the secret(t) any how.