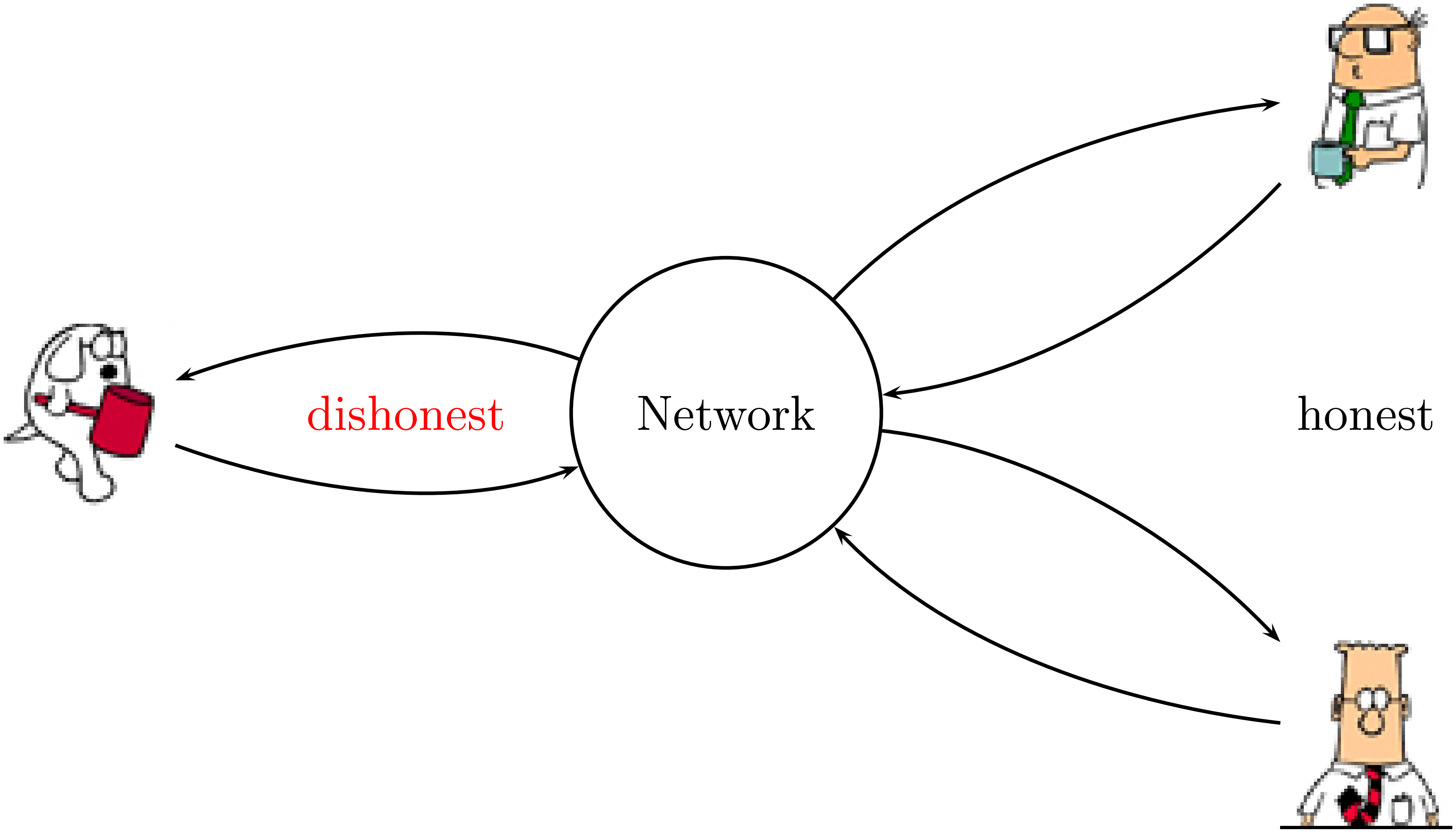
Easy Intruder Deductions

Hubert Comon et Ralf Treinen
LSV
CNRS, INRIA Futurs projet SECSI, and ENS de Cachan
Cachan, France

Cryptographic protocols on an insecure network



The Intruder Deduction Problem

- *Active attack* : Attacker can send messages and initiate new sessions

- *Passive attack* : Attacker can only observe the messages that pass on the network

Intruder Deduction Problem: Given a finite set of messages (the messages that pass over a network during a protocol session) and a given term (a secret), can the intruder deduce the term from the set of messages?

The Perfect Cryptography Assumption

The cipher is perfect: there is no way to obtain knowledge about the plaintext pertaining to a ciphertext without knowing the key.

This allows to separate security analysis into

1. cryptography ($\rightarrow$ mathematics)
2. protocol analysis ($\rightarrow$ computer science)

The Dolev-Yao Model of Intruder Capabilities

(A) $\dfrac{u \in T}{T \vdash u}$

(P) $\dfrac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v \rangle}$

(UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

(UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

(C) $\dfrac{T \vdash u \qquad T \vdash v}{T \vdash \{u\}_v}$

(D) $\dfrac{T \vdash \{u\}_v \qquad T \vdash v}{T \vdash u}$

(F) $\dfrac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)}$

Intruder Deduction in the Dolev-Yao Model

1. the Dolev-Yao rules are Horn clauses

2. the Dolev-Yao clauses are *local* in the sense of [McAllester '93] : If $T \vdash t$, then there is a proof that uses only subterms of terms in $T \cup \{t\}$ [Comon & Shmatikov, 2003].

Consequence : Intruder Deduction in the Dolev-Yao Model is polynomial.

Weakening of the Perfect Cryptography Assumption

Take into account algebraic properties of the cryptographic primitives :

- Properties that are exploited by the protocol, like commutativity of encryption in Diffie-Hellman key exchange.
- Inherent (accidental) properties of the encryption, like homomorphism properties of RSA.

Example of an Attack Using Laws of Homomorphism

Key exchange protocol [Tatebayashi, Matsuzuki, Newmann '89]

- two participants A and B want to agree on a session key
- they use a trusted server S
- participants A, B have limited computing resources :
  1. generation of random numbers
  2. *encryption* by public key cryptography : $m \mapsto m^3 \bmod n$
  3. bitwise xor

The TMN Protocol

Public key encryption : n is public, but only S can compute cubic roots modulo n.

$$
\begin{array}{llll}
(1) & A \rightarrow S & \text{“I want to talk to B”}, r_A^3 \bmod n \\
(2) & S \rightarrow B & \text{“A wants to talk to you”} \\
(3) & B \rightarrow S & {r_B}^3 \bmod n \\
(4) & S \rightarrow A & r_A \oplus r_B
\end{array}
$$

Now, participant A can compute $r_B = r_A \oplus (r_A \oplus r_B)$.

Attack on the TMN Protocol [Simmons '94]

- Attacker C has seen $r_B^3 \bmod n$ on the network.
- The value r_D is known to both attackers C and D.

$$
\begin{array}{llll}
(1) & C \rightarrow S & \text{“D”}, (r_C^3 * (r_B^3 \bmod n)) \bmod n = (r_C * r_B)^3 \bmod n \\
(2) & S \rightarrow D & \text{“C wants to talk to you”} \\
(3) & D \rightarrow S & r_D^3 \bmod n \\
(4) & S \rightarrow C & r_D \oplus r_C * r_B
\end{array}
$$

Attacker C can now calculate

- $r_C * r_B = r_D \oplus (r_D \oplus (r_C * r_B))$
- $r_B = r_C^{-1} * (r_C * r_B)$

The Dolev-Yao Attacker Model Modulo E

(A) $$\frac{u \in T}{T \vdash u}$$

(P) $$\frac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v \rangle}$$

(UL) $$\frac{T \vdash \langle u, v \rangle}{T \vdash u}$$

(UR) $$\frac{T \vdash \langle u, v \rangle}{T \vdash v}$$

(C) $$\frac{T \vdash u \qquad T \vdash v}{T \vdash \{u\}_v}$$

(D) $$\frac{T \vdash \{u\}_v \qquad T \vdash v}{T \vdash u}$$

(F) $$\frac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)}$$

(E) $$\frac{T \vdash u \qquad u =_E v}{T \vdash v}$$

Problems of the Naive Dolev-Yao Model Modulo E

1. Allows derivation of too many terms

2. In general *locality* is lost

Solution?

1. Use a *terminating and confluent rewriting system* $\rightarrow_E$ for E, only compute with normal forms

2. Extend carefully the notion of subterm

Example: Homomorphism

Equational theory:

$$\{\langle u, v\rangle\}_k = \langle \{u\}_k, \{v\}_k\rangle$$

Rewrite system:

$$\{\langle u, v\rangle\}_k \rightarrow \langle \{u\}_k, \{v\}_k\rangle$$

When working with normal forms only, the *decryption rule* must apply to

$$\langle \{u\}_k, \{v\}_k\rangle$$

Dolev-Yao Modulo E

(A) $$\frac{u \in T}{T \vdash u\!\downarrow}$$

(P) $$\frac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v\rangle\!\downarrow}$$

(UL) $$\frac{T \vdash r}{T \vdash u\!\downarrow} \quad \text{if } \exists v\ \langle u, v\rangle \to^! r$$

(UR) $$\frac{T \vdash r}{T \vdash v\!\downarrow} \quad \text{if } \exists u\ \langle u, v\rangle \to^! r$$

(C) $$\frac{T \vdash u \qquad T \vdash v}{T \vdash \{u\}_v\!\downarrow}$$

(D) $$\frac{T \vdash r \qquad T \vdash v}{T \vdash u\!\downarrow} \quad \text{if } \{u\}_v \to^! r$$

(F) $$\frac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)\!\downarrow}$$

How to define the set $S(T)$?

- closed under subterm,
- must allow *proof normalization*: If there is a proof of $T \vdash t$ then there is a proof that uses only terms in $S(T, t)$
- If T finite then $S(T)$ must be finite
- *What else ?*

Example: Homomorphism

$$
\dfrac{
  \dfrac{\langle u, v \rangle \in T}{T \vdash \langle u, v \rangle}\,A
  \qquad
  \dfrac{k \in T}{T \vdash k}\,A
}{
  \dfrac{T \vdash \langle \{u\}_k, \{v\}_k \rangle}{T \vdash \{u\}_k}\,UL
}\,C
$$

The intermediate term $\langle \{u\}_k, \{v\}_k \rangle$ does not belong to $subterms(\langle u, v \rangle, k, \{u\}_k)$.

Example: Homomorphism (cntd.)

This proof can be rewritten into

$$
\dfrac{\dfrac{\dfrac{\langle u, v\rangle \in T}{T \vdash \langle u, v\rangle}\,A}{T \vdash u}\,UL \qquad \dfrac{k \in T}{T \vdash k}\,A}{T \vdash \{u\}_k}\,C
$$

All nodes of this proof are in $subterms(\{u\}_k, \langle u, v\rangle, k)$.

Proof Normalization

In general: we must push decompositions to the leaves of the tree :

$$\dfrac{\dfrac{T \vdash r_1 \quad \cdots \quad T \vdash r_n}{T \vdash f(r_1, \ldots, r_n)} \quad \to^! r \leftarrow^! \langle u, v \rangle}{T \vdash u}$$

must be rewritten into

$$\dfrac{\dfrac{T \vdash \langle s_1, t_1 \rangle \to^! r_1}{T \vdash s_1} \quad \cdots \quad \dfrac{T \vdash \langle s_i, t_i \rangle \to^! r_i}{T \vdash s_i} \quad T \vdash r_{i+1} \quad \cdots \quad T \vdash r_n}{T \vdash C[s_1, \ldots, s_i, r_{i+1}, \ldots, r_n] \to^! u}$$

where $C[\ldots]$ is a *context* (maybe empty).

Reduced Proofs

Data Path in a proof tree : any path that does not pass through the key of a decryption node.

Reduced Tree : Any Data Path departing from a decomposition node has only decompositions (i.e., all decompositions have been pushed to the leaves, except for decryption keys)

Condition on the rewrite system : Must allow proof normalization.

Lemma 1 *If* $T \vdash t$ *then there is a reduced proof tree for* $T \vdash t$*.*

Proof Normalization

Condition: S must be closed under inverse rewriting:

If $f(t_1, \ldots, t_n) \rightarrow^! t$ then $t_1, \ldots, t_n \in S(t)$

(In fact, one can also allow rules like $x \oplus x \oplus y \rightarrow y$.)

Theorem 1 *If S satisfies the above conditions, then if $T \vdash t$ then there is a normal proof for $T \vdash t$.*

Example: Homomorphism (cntd.)

$S(t)$ is the smallest set of terms which

1. contains t;
2. is closed under subterm;
3. if $\langle \{u\}_z, \{v\}_z \rangle \in S(t)$ then $\langle u, v \rangle \in S(t)$.

Theorem 2 *In case of the homomorphism axiom, $T \vdash t$ can be decided in linear time provided that t and all elements of T are in normal form.*

Open questions

- many interesting theories can not yet be treated by this approach, including the cases of [Comon & Shmatikov 2003]: Abelian groups, and xor

- classify the interesting theories according to the decidability/undecidability, and complexity of the intruder deduction problem

- *active* attacker: constraint solving for equational theories