Topics in Security
Aug – Nov 2017
Assignment 1

Due: October 8, 2017. 11 pm. Submit on Moodle.

---

1. Assume a set of basic terms $\mathscr{B} = \mathscr{A} \cup \mathscr{N} \cup \mathscr{K}$. We assume that each key k has an inverse $inv(k)$. The syntax for terms $\mathscr{T}$ is given as usual:

   $$t, t' ::= m \mid (t, t') \mid \{t\}_k$$

   where $m \in \mathscr{B}$, $k \in \mathscr{K}$.

   Sometimes, particular implementations of the cryptographic operations admit more properties (even accidentally). For instance, many common implementations of encryption in terms of modular exponentiation satisfy the following rule (which we call *simplify*).

   $$\frac{X \vdash \{\{t\}_k\}_{inv(k)}}{X \vdash t}\ simplify$$

   Consider a derivation system with the rules *ax*, *pair*, *split*, *enc*, *dec* and *simplify*. Define a notion of normal proofs, prove normalization and the subterm property, and modify the linear time algorithm to account for this new rule.

2. Consider now a derivation system with encryption, pairing, and *blind signatures*. This is a method to get someone to sign a message for you without letting that person look at the message itself. (As a physical example, think of sealing your message – written on a piece of paper – inside a special envelope which allows writing on top to seep through. If the seal is secure, the message gets signed while still being secret.)

   One way of modelling this logically is as follows. Enhance the syntax of terms by allowing terms of the form $[t, m]$, where $t \in \mathscr{T}$ and $m \in \mathscr{N}$ (in addition to pairing and encryption), and add the following two rules (*blind* corresponds to sealing in a secure envelope, *unblind* corresponds to taking a signed envelope and extracting the signed message inside it by breaking the seal):

   $$\frac{X \vdash t \quad X \vdash m}{X \vdash [t, m]}\ blind \qquad \frac{X \vdash \{[t, m]\}_k \quad X \vdash m}{X \vdash \{t\}_k}\ unblind$$

   Give a proof of $X \vdash \{t\}_k$ in this system, for $X = \{[t, m], m, k\}$. Does the term $\{[t, m]\}_k$ occur in the proof? Is it a subterm of some term in $X \cup \{\{t\}_k\}$?

Give two proofs of $Y \vdash \{t\}_k$ for $Y = \{t, m, k\}$, one in which $\{[t, m]\}_k$ occurs, and one in which it does not occur. Are either of the proofs minimal, in the sense that no term occurs on the same branch twice?

As suggested by these examples, if one desires the subterm property to hold, the notion of "subterm" has to be modified. Specifically, $\mathbf{st}(t)$ is now defined to be the smallest $X \subseteq \mathscr{T}$ such that:

- $t \in X$;
- if $(t, t') \in X$ then $\{t, t'\} \subseteq X$;
- if $\{t\}_k \in X$ then $\{t, k\} \subseteq X$;
- if $[t, m] \in X$ then $\{t, m\} \subseteq X$; and
- if $[t, m] \in X$ and $\{t\}_k \in X$ then $\{[t, m]\}_k \in X$.

With this definition, $|\mathbf{st}(X)| \leq |X|^2$, in general. For example, if

$$X = \{[t, m_1], \ldots, [t, m_p], \{t\}_{k_1}, \ldots, \{t\}_{k_n}\},$$

then $\mathbf{st}(X)$ contains all the *pn* terms of the form $\{[t, m_i]\}_{k_j}$.

Nevertheless, one can define a notion of normal proofs, and prove the normalization theorem and the subterm property (using the above definition), and modify the linear time algorithm presented for the basic system. (The algorithm is now linear in $|\mathbf{st}(X)|$, and thus quadratic in $|X|$.)

3. Suppose one adds the following extra rule to the system in the previous question.

$$\frac{X \vdash [t, m] \quad X \vdash m}{X \vdash t}\ \mathit{unblind}'$$

For $X = \{[t, m], k, m\}$, is there a proof of $X \vdash \{t\}_k$ in which $\{[t, m]\}_k$ does not occur?

Modify the definition of normal proofs from the previous question, so that the subformula property holds for the usual definition of $\mathbf{st}(t)$ (without the fifth clause in the definition given earlier). Also modify the linear time procedure to work for this system.

4. Recall our favourite protocol

$$A \to B : (n)\{n\}_B$$
$$B \to A : \{n\}_A$$

n is meant to be a fresh nonce, and $\{t\}_C$ means encrypting t with C's public key, for any $t \in \mathscr{T}$ and $C \in \mathscr{A}$.

We know that this admits an attack where m, generated freshly by A intended for B, ends up being known to I. We fixed the protocol by modifying the first message to $\{A, n\}_B$. Here is a seemingly more secure fix.

$$A \to B : (n)\{A, \{n\}_B\}_B$$
$$B \to A : \{n\}_A$$

But unfortunately this admits a violation of secrecy when the intruder is allowed to substitute any term for a nonce (leading to a non well-typed run). Can you find it?

Can you show a similar violation of secrecy for the following protocol?

$$A \to B : (n)\{A, \{A, \{n\}_B\}_B\}_B$$
$$B \to A : \{n\}_A$$

Finally, prove that even allowing for non well-typed runs, there is no secrecy violation in the original amendment:

$$A \to B : (n)\{A, n\}_B$$
$$B \to A : \{n\}_A$$