Access Control and Privacy Policies (6)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)

Slides: KEATS (also homework is there)

1st Week

- What are hashes and salts?

1st Week

- What are hashes and salts?
- ...can be use to store securely data on a client, but you cannot make your protocol dependent on the presence of the data

1st Week

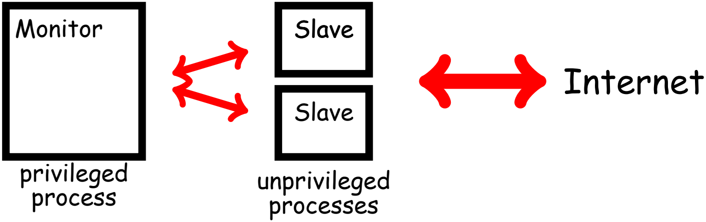
- What are hashes and salts?
- . . . can be use to store securely data on a client, but you cannot make your protocol dependent on the presence of the data
- . . . can be used to store and verify passwords

2nd Week

- Buffer overflows
- choice of programming language can mitigate or even eliminate this problem

3rd Week

- defence in depth
- privilege separation afforded by the OS



4th Week

- voting. . . has security requirements that are in tension with each other

  integrity vs ballot secrecy
  authentication vs enfranchisment

- electronic voting makes 'whole sale' fraud easier as opposed to 'retail attacks'

5th Week

- access control logic

- formulas
- judgements
- inference rules

Access Control Logic

Formulas

$$
\begin{array}{lcll}
F & ::= & \text{true} & \\
 & | & \text{false} & \\
 & | & F \wedge F & \\
 & | & F \vee F & \\
 & | & F \Rightarrow F & \\
 & | & p\,(t_1,\ldots,t_n) & \\
 & | & P \text{ says } F & \text{“saying predicate”}
\end{array}
$$

Judgements

$$\Gamma \vdash F$$

Inference Rules

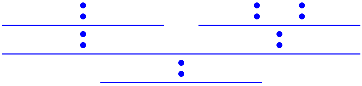
$$\overline{\Gamma, F \vdash F}$$

$$\frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_2}{\Gamma \vdash F_2} \qquad \frac{F_1, \Gamma \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2}$$

$$\frac{\Gamma \vdash F}{\Gamma \vdash P \text{ says } F}$$

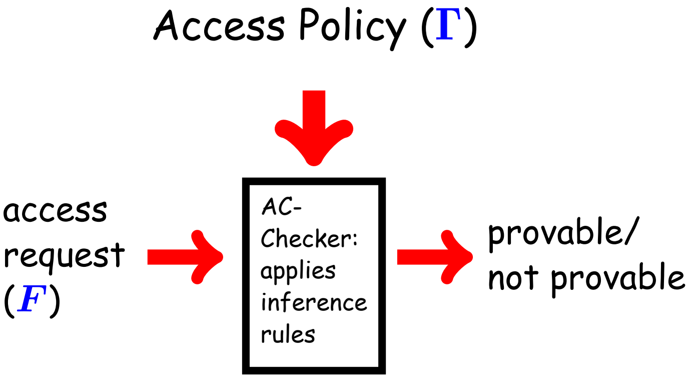
$$\frac{\Gamma \vdash P \text{ says } (F_1 \Rightarrow F_2) \quad \Gamma \vdash P \text{ says } F_1}{\Gamma \vdash P \text{ says } F_2}$$

Proofs



$$\Gamma \vdash F$$

The Access Control Problem



Recall the following scenario:

- If Admin says that file should be deleted, then this file must be deleted.
- Admin trusts Bob to decide whether file should be deleted.
- Bob wants to delete file.

$$\Gamma = \begin{array}{l} (\text{Admin says del\_file}) \Rightarrow \text{del\_file}, \\ (\text{Admin says } ((\text{Bob says del\_file}) \Rightarrow \text{del\_file})), \\ \text{Bob says del\_file} \end{array}$$

$$\Gamma \vdash \text{del\_file}$$

How to prove $\Gamma \vdash F$?

$$\overline{\Gamma, F \vdash F}$$

$$\frac{F_1, \Gamma \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2}$$

$$\frac{\Gamma \vdash F}{\Gamma \vdash P \text{ says } F}$$

$$\frac{\Gamma \vdash F_1}{\Gamma \vdash F_1 \vee F_2} \qquad \frac{\Gamma \vdash F_2}{\Gamma \vdash F_1 \vee F_2}$$

$$\frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \wedge F_2}$$

I want to prove $\Gamma \vdash$ Pred

I want to prove $\Gamma \vdash \mathsf{Pred}$

1. I found that Γ contains the assumption $F_1 \Rightarrow F_2$

I want to prove $\Gamma \vdash Pred$

1. I found that Γ contains the assumption $F_1 \Rightarrow F_2$
2. If I can prove $\Gamma \vdash F_1$,

I want to prove $\Gamma \vdash$ Pred

1. I found that Γ contains the assumption $F_1 \Rightarrow F_2$
2. If I can prove $\Gamma \vdash F_1$, then I can prove
$$\Gamma \vdash F_2$$

$$\frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_1}{\Gamma \vdash F_2}$$

I want to prove $\Gamma \vdash$ Pred

1. I found that Γ contains the assumption $F_1 \Rightarrow F_2$
2. If I can prove $\Gamma \vdash F_1$, then I can prove

$$\Gamma \vdash F_2$$

3. So better I try to prove $\Gamma \vdash$ Pred with the additional assumption F_2.

$$F_2, \Gamma \vdash \text{Pred}$$

- P is entitled to do F

$$P \text{ controls } F \stackrel{\text{def}}{=} (P \text{ says } F) \Rightarrow F$$

$$\frac{\Gamma \vdash P \text{ controls } F \quad \Gamma \vdash P \text{ says } F}{\Gamma \vdash F}$$

- P speaks for Q

$$P \mapsto Q \stackrel{\text{def}}{=} \forall F.(P \text{ says } F) \Rightarrow (Q \text{ says } F)$$

$$\frac{\Gamma \vdash P \mapsto Q \quad \Gamma \vdash P \text{ says } F}{\Gamma \vdash Q \text{ says } F}$$

$$\frac{\Gamma \vdash P \mapsto Q \quad \Gamma \vdash Q \text{ controls } F}{\Gamma \vdash P \text{ controls } F}$$

Protocol Specifications

The Needham-Schroeder Protocol:

Message 1 $A \rightarrow S : A, B, N_A$
Message 2 $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
Message 3 $A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$
Message 4 $B \rightarrow A : \{N_B\}_{K_{AB}}$
Message 5 $A \rightarrow B : \{N_B - 1\}_{K_{AB}}$

Trusted Third Party

Simple protocol for establishing a secure connection via a mutually trusted 3rd party (server):

Message 1 $A \to S : A, B$
Message 2 $S \to A : \{K_{AB}\}_{K_{AS}}$ and $\{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
Message 3 $A \to B : \{K_{AB}\}_{K_{BS}}$
Message 4 $A \to B : \{m\}_{K_{AB}}$

Sending Messages

- Alice sends a message m

  Alice says m

Sending Messages

- Alice sends a message m

  Alice says m

- Alice sends an encrypted message m (with key K)

  Alice says $\{m\}_K$

Sending Messages

- Alice sends a message m

$$\text{Alice says } m$$

- Alice sends an encrypted message m (with key K)

$$\text{Alice says } \{m\}_K$$

- Decryption of Alice's message

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_K \quad \Gamma \vdash K}{\Gamma \vdash \text{Alice says } m}$$

Encryption

- Encryption of a message

$$\frac{\Gamma \vdash \text{Alice says } m \quad \Gamma \vdash K}{\Gamma \vdash \text{Alice says } \{m\}_K}$$

Public/Private Keys

- Bob has a private and public key: $K_{Bob}^{pub}, K_{Bob}^{priv}$

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_{K_{Bob}^{pub}} \quad \Gamma \vdash K_{Bob}^{priv}}{\Gamma \vdash \text{Alice says } m}$$

Public/Private Keys

- Bob has a private and public key: $K_{Bob}^{pub}, K_{Bob}^{priv}$

$$\frac{\Gamma \vdash \text{Alice says } \{m\}_{K_{Bob}^{pub}} \quad \Gamma \vdash K_{Bob}^{priv}}{\Gamma \vdash \text{Alice says } m}$$

- this is **not** a derived rule!

Trusted Third Party

- Alice calls Sam for a key to communicate with Bob
- Sam responds with a key that Alice can read and a key Bob can read (pre-shared)
- Alice sends the message encrypted with the key and the second key it recieved

$$
\begin{array}{lcl}
A \text{ sends } S & : & \text{Connect}(A, B) \\
S \text{ sends } A & : & \{K_{AB}\}_{K_{AS}} \text{ and } \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}} \\
A \text{ sends } B & : & \{K_{AB}\}_{K_{BS}} \\
A \text{ sends } B & : & \{m\}_{K_{AB}}
\end{array}
$$

Sending Rule

$$\frac{\Gamma \vdash P \text{ says } F \quad \Gamma \vdash P \text{ sends } Q : F}{\Gamma \vdash Q \text{ says } F}$$

Sending Rule

$$\frac{\Gamma \vdash P \text{ says } F \quad \Gamma \vdash P \text{ sends } Q : F}{\Gamma \vdash Q \text{ says } F}$$

$$P \text{ sends } Q : F \overset{\text{def}}{=}$$
$$(P \text{ says } F) \Rightarrow (Q \text{ says } F)$$

Trusted Third Party

A sends S : Connect(A, B)
S says (Connect$(A, B) \Rightarrow$
$\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}\_K_{AS})$
S sends A : $\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
A sends B : $\{K_{AB}\}_{K_{BS}}$
A sends B : $\{m\}_{K_{AB}}$

Trusted Third Party

A sends S : Connect(A, B)
S says (Connect$(A, B) \Rightarrow$
$\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}\_K_{AS})$
S sends A : $\{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
A sends B : $\{K_{AB}\}_{K_{BS}}$
A sends B : $\{m\}_{K_{AB}}$

$\Gamma \vdash B$ says m