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

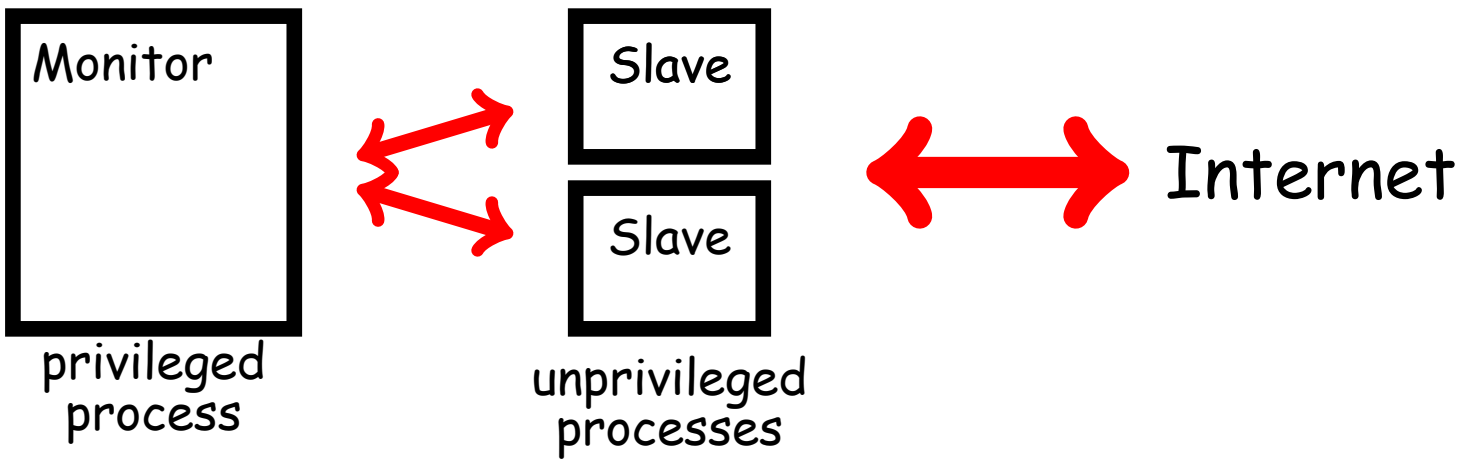
- What are hashes and salts?
- ...can be use to store securely data on a client, but you cannot make your protocol dependent on the presence of the data
- ...can be used to store and verify passwords

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

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

Judgements

$$\Gamma \vdash F$$

Inference Rules

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

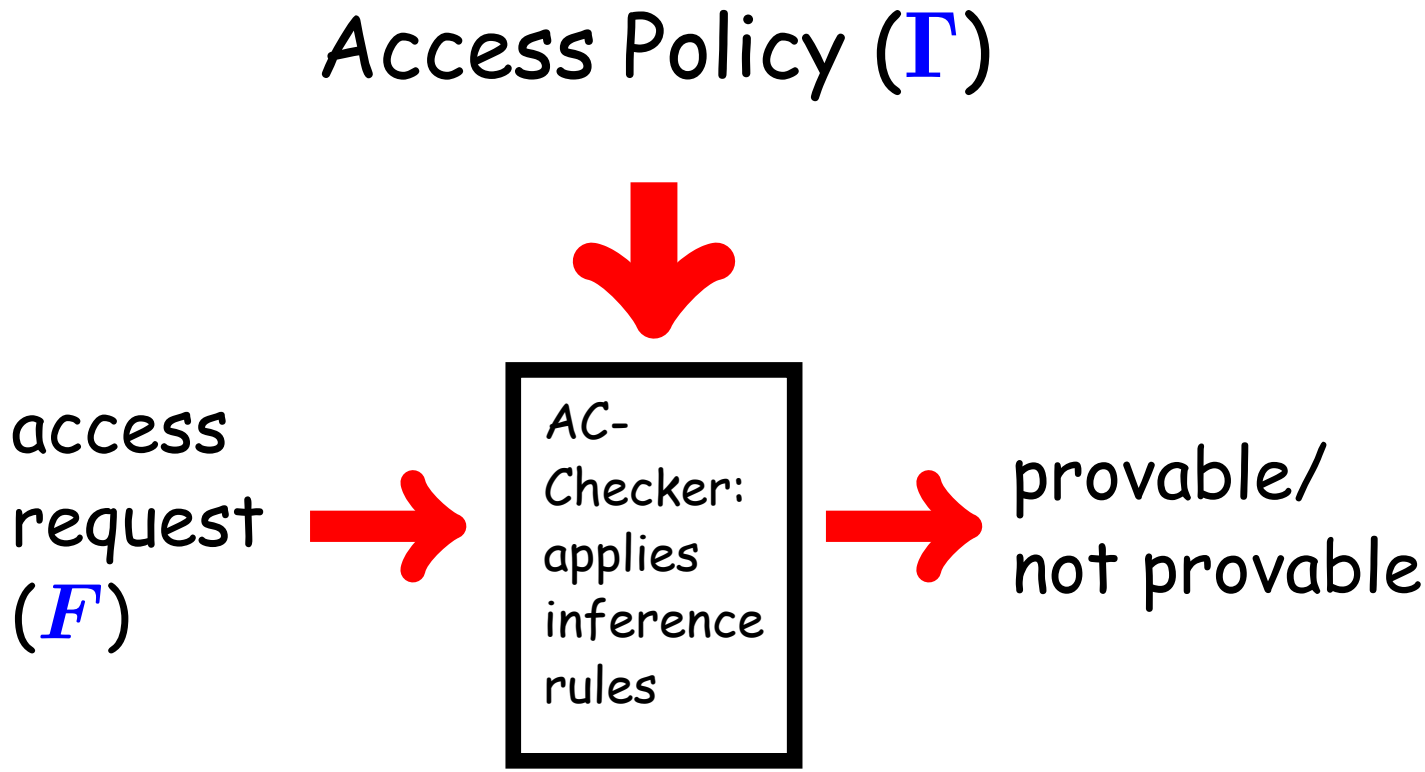
$$\frac{\Gamma \vdash F_1 \Rightarrow F_2 \quad \Gamma \vdash F_2}{\Gamma \vdash F_2} \qquad \frac{F_1, \Gamma \vdash F_2}{\Gamma \vdash F_1 \Rightarrow F_2}$$

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

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

Proofs

The Access Control Problem



Recall the following scenario:

- If Admin says that file_1 should be deleted, then this file must be deleted.
- Admin trusts Bob to decide whether file_1 should be deleted.
- Bob wants to delete file_1.

$$\begin{array}{ll} & (\text{Admin says del\_file}_1) \Rightarrow \text{del\_file}_1, \\ \Gamma = & (\text{Admin says } ((\text{Bob says del\_file}_1) \Rightarrow \text{del\_file}_1)), \\ & \text{Bob says del\_file}_1 \end{array}$$

$$\Gamma \vdash \text{del\_file}_1$$

How to prove $\Gamma \vdash F$?

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

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

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

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

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

I want to prove $\Gamma \vdash Pred$

I want to prove $\Gamma \vdash$ 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
$$\Gamma \vdash F_2$$

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

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 $\Gamma \vdash \text{Pred}$ with the additional assumption F_2.
$$F_2, \Gamma \vdash \text{Pred}$$