# 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)

# Access Control Logic

Formulas

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

"saying predicate"

Judgements

$$\Gamma \vdash F$$

# Inference Rules

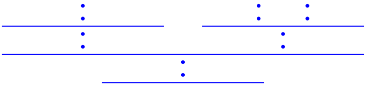
$$\frac{}{\Gamma, \boldsymbol{F} \vdash \boldsymbol{F}}$$

$$\frac{\Gamma \vdash \boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2 \quad \Gamma \vdash \boldsymbol{F}_1}{\Gamma \vdash \boldsymbol{F}_2} \qquad \frac{\boldsymbol{F}_1, \Gamma \vdash \boldsymbol{F}_2}{\Gamma \vdash \boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2}$$

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

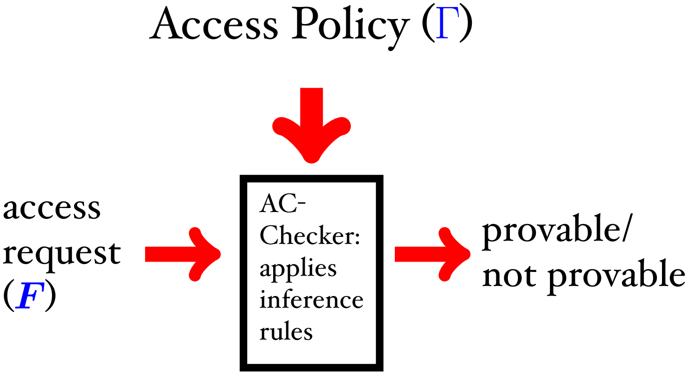
$$\frac{\Gamma \vdash \boldsymbol{P} \text{ says } (\boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2) \quad \Gamma \vdash \boldsymbol{P} \text{ says } \boldsymbol{F}_1}{\Gamma \vdash \boldsymbol{P} \text{ says } \boldsymbol{F}_2}$$

# Proofs



$$\Gamma \vdash \boldsymbol{F}$$

# 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 $\Gamma \vdash \boldsymbol{F}$?

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

$$\frac{\boldsymbol{F}_1, \Gamma \vdash \boldsymbol{F}_2}{\Gamma \vdash \boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2}$$

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

$$\frac{\Gamma \vdash \boldsymbol{F}_1}{\Gamma \vdash \boldsymbol{F}_1 \vee \boldsymbol{F}_2} \qquad \frac{\Gamma \vdash \boldsymbol{F}_2}{\Gamma \vdash \boldsymbol{F}_1 \vee \boldsymbol{F}_2}$$

$$\frac{\Gamma \vdash \boldsymbol{F}_1 \quad \Gamma \vdash \boldsymbol{F}_2}{\Gamma \vdash \boldsymbol{F}_1 \wedge \boldsymbol{F}_2}$$

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

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

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

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

1. I found that $\Gamma$ contains the assumption $\boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2$
2. If I can prove $\Gamma \vdash \boldsymbol{F}_1$,

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

1. I found that $\Gamma$ contains the assumption $\boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2$
2. If I can prove $\Gamma \vdash \boldsymbol{F}_1$, then I can prove

$$\Gamma \vdash \boldsymbol{F}_2$$

$$\frac{\Gamma \vdash \boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2 \quad \Gamma \vdash \boldsymbol{F}_1}{\Gamma \vdash \boldsymbol{F}_2}$$

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

1. I found that $\Gamma$ contains the assumption $\boldsymbol{F}_1 \Rightarrow \boldsymbol{F}_2$

2. If I can prove $\Gamma \vdash \boldsymbol{F}_1$, then I can prove

$$\Gamma \vdash \boldsymbol{F}_2$$

3. So better I try to prove $\Gamma \vdash \text{Pred}$ with the additional assumption $\boldsymbol{F}_2$.

$$\boldsymbol{F}_2, \Gamma \vdash \text{Pred}$$

- $P$ is entitled to do $F$

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

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

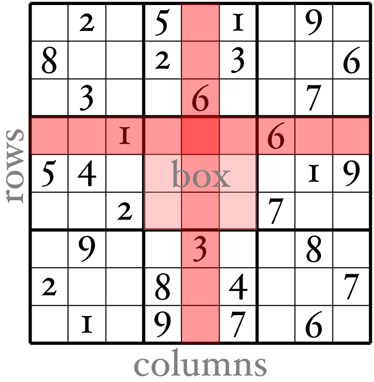
- $P$ speaks for $Q$

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

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

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

# Sudoku




1. **Row-Column:** each cell, must contain exactly one number
2. **Row-Number:** each row must contain each number exactly once
3. **Column-Number:** each column must contain each number exactly once
4. **Box-Number:** each box must contain each number exactly once

# Solving Sudokus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 7 | | | | 5 | 8 |
| | 5 | 6 | 2 | 1 | 8 | 7 | 9 | 3 |
| | | | | | | 1 | | |
| | | | | | | | 8 | 1 |
| | | | 3 | 7 | 6 | | | |
| 9 | 6 | | | | | | | |
| | | 5 | | 3 | | | | |
| | | 4 | | 2 | 1 | 8 | 3 | |
| 8 | 7 | | | | 3 | | | |

**single position rules**

$$\frac{\{1..9\} - \{4\} \text{ in one row}}{4 \text{ in empty position}}$$

# Solving Sudokus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 7 | | | | 5 | 8 |
| | 5 | 6 | 2 | 1 | 8 | 7 | 9 | 3 |
| | | | | | | 1 | | |
| | | | | | | | 8 | 1 |
| | | | 3 | 7 | 6 | | | |
| 9 | 6 | | | | | | | |
| | | 5 | | 3 | | | | |
| | | 4 | | 2 | 1 | 8 | 3 | |
| 8 | 7 | | | | 3 | | | |

**single position rules**

$$\frac{\{1..9\} - \{4\} \text{ in one row}}{4 \text{ in empty position}}$$

$$\frac{\{1..9\} - \{x\} \text{ in one column}}{x \text{ in empty position}}$$

$$\frac{\{1..9\} - \{x\} \text{ in one box}}{x \text{ in empty position}}$$

# Solving Sudokus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 7 | | | 2 | 5 | 8 |
| | 5 | 6 | 2 | 1 | 8 | 7 | 9 | 3 |
| | | | | | | 1 | 2 | 2 |
| | | | | | | | 8 | 1 |
| | | | 3 | 7 | 6 | | | |
| 9 | 6 | | | | | | | |
| | | 5 | | 3 | | | | |
| | | 4 | | 2 | 1 | 8 | 3 | |
| 8 | 7 | | | | 3 | | | |

**candidate rules**

$$\frac{X - \{x\} \text{ in one box} \quad X \subseteq \{1..9\}}{x \text{ candidate in empty positions}}$$

# Solving Sudokus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 7 | | | 2 | 5 | 8 |
| 4 | 5 | 6 | 2 | 1 | 8 | 7 | 9 | 3 |
| | | | | | | 1 | 2 | 2 |
| | | | | | | | 8 | 1 |
| | | | 3 | 7 | 6 | | | |
| 9 | 6 | | | | | | | |
| | | 5 | | 3 | | | | |
| | | 4 | | 2 | 1 | 8 | 3 | |
| 8 | 7 | | | | 3 | | | |

$$\frac{\{1..9\} - \{4\} \text{ in one row}}{4 \text{ in empty position}}$$

$$\frac{X - \{2\} \text{ in one box} \quad X \subseteq \{1..9\}}{2 \text{ candidate in empty positions}}$$

# Solving Sudokus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 7 | | | 2 | 5 | 8 |
| 4 | 5 | 6 | 2 | 1 | 8 | 7 | 9 | 3 |
| | | | | | | 1 | 2 | 2 |
| | | | | | | | 8 | 1 |
| | | | 3 | 7 | 6 | | | |
| 9 | 6 | | | | | | | |
| | | 5 | | 3 | | | | |
| | | 4 | | 2 | 1 | 8 | 3 | |
| 8 | 7 | | | | 3 | | | |

$$\frac{\{1..9\} - \{4\} \text{ in one row}}{4 \text{ in empty position}}$$

$$\frac{X - \{2\} \text{ in one box} \quad X \subseteq \{1..9\}}{2 \text{ candidate in empty positions}}$$

# Solving Sudokus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 7 | | | | 5 | 8 |
| | 5 | 6 | 2 | 1 | 8 | 7 | 9 | 3 |
| | | | | | | 1 | | |
| | | | | | | | 8 | 1 |
| | | | 3 | 7 | 6 | | | |
| 9 | 6 | | | | | | | 2 |
| | | 5 | | 3 | | | | |
| | | 4 | | 2 | 1 | 8 | 3 | |
| 8 | 7 | | | | 3 | | | |

$$\frac{X - \{2\} \text{ in one box} \quad X \subseteq \{1..9\}}{2 \text{ candidate}}$$

# Sudoku

Are there sudokus that cannot be solved?

# Sudoku

Are there sudokus that cannot be solved?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| | | | | | | | | 2 |
| | | | | | | | | 3 |
| | | | | | | | | 4 |
| | | | | | | | | 5 |
| | | | | | | | | 6 |
| | | | | | | | | 7 |
| | | | | | | | | 8 |
| | | | | | | | | 9 |

Sometimes no rules apply at all....unsolvable sudoku.

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

# Sending Messages

- Alice sends a message $m$

  Alice says $m$

# Sending Messages

- Alice sends a message $m$

$$\text{Alice says } m$$

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

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

# 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

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

# Encryption

- Encryption of a message

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

# 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

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

# Sending Rule

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

# Sending Rule

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

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

# Trusted Third Party

$$
\begin{array}{l}
A \text{ sends } S : \mathit{Connect}(A, B) \\
S \text{ says } (\mathit{Connect}(A, B) \Rightarrow \\
\qquad\qquad \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}) \\
S \text{ sends } A : \{K_{AB}\}_{K_{AS}} \wedge \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}} \\
A \text{ sends } B : \{K_{AB}\}_{K_{BS}} \\
A \text{ sends } B : \{m\}_{K_{AB}}
\end{array}
$$

# Trusted Third Party

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