Access Control and Privacy Policies (11)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS (also homework is there)

- you can still send me your homework
- Unix AC question: use a terminal-based editor (vm, vim)
- exams: 2 out of 3 questions, 5 or so subquestions each, you can fill in your answers on the question sheet

Interlock Protocol

The interlock protocol ("best bet" against MITM):

1. $A \to B : K_A^{pub}$
2. $B \to A : K_B^{pub}$
3. $\{A, m\}_{K_B^{pub}} \mapsto H_1, H_2$

   $\{B, m'\}_{K_A^{pub}} \mapsto M_1, M_2$
4. $A \to B : H_1$
5. $B \to A : \{H_1, M_1\}_{K_A^{pub}}$
6. $A \to B : \{H_2, M_1\}_{K_B^{pub}}$
7. $B \to A : M_2$

Interlock Protocol

The interlock protocol ("best bet" against MITM):

1. $A \rightarrow B : K_A^{pub}$
2. $B \rightarrow A : K_B^{pub}$
3. $\{A, m\}_{K_B^{pub}} \mapsto H_1, H_2$

   $\{B, m'\}_{K_A^{pub}} \mapsto M_1, M_2$
4. $A \rightarrow B : H_1$
5. $B \rightarrow A : \{H_1, M_1\}_{K_A^{pub}}$
6. $A \rightarrow B : \{H_2, M_1\}_{K_B^{pub}}$
7. $B \rightarrow A : M_2$

m = How is your grandmother? m' = How is the weather today in London?

$$A \rightarrow C : K_A^{pub}$$
$$C \rightarrow B : K_C^{pub}$$
$$B \rightarrow C : K_B^{pub}$$
$$C \rightarrow A : K_C^{pub}$$

$$\{A, m\}_{K_C^{pub}} \mapsto H_1, H_2$$
$$\{B, n\}_{K_C^{pub}} \mapsto M_1, M_2$$

$$\{C, a\}_{K_B^{pub}} \mapsto C_1, C_2$$
$$\{C, b\}_{K_A^{pub}} \mapsto D_1, D_2$$

$$A \rightarrow C : H_1$$
$$C \rightarrow B : C_1$$
$$B \rightarrow C : \{C_1, M_1\}_{K_C^{pub}}$$
$$C \rightarrow A : \{H_1, D_1\}_{K_A^{pub}}$$
$$A \rightarrow C : \{H_2, D_1\}_{K_C^{pub}}$$
$$C \rightarrow B : \{C_2, M_1\}_{K_B^{pub}}$$
$$B \rightarrow C : M_2$$
$$C \rightarrow A : D_2$$

- you have to ask something that cannot imitated (requires A and B know each other)
- what happens if m and n are voice messages?

- the moral: establishing a secure connection from "zero" is almost impossible—you need to rely on some established trust

- that is why we rely on certificates, which however are badly, badly realised (just today a POODLE attack against SSL)