Preliminary example: a timed social protocol

\[
A \xrightarrow{(m)} B
\]

\[\odot \xrightarrow{\tau} \odot\]
Preliminary example: a timed social protocol

\[ A \xrightarrow{\text{\(\alpha\)}} B \]

$s = m \xrightarrow{\text{\(\alpha\)}} \exists t$

\[ \alpha : T \rightarrow T : \text{a short digest (hash) function} \]

such that

\[ \forall s \exists t : \alpha(t) = \alpha(s) \]

"The digest does not change short terms."

Security: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social commitment
Integrity
Decommit then auth.
Social channel bandwidth

Social actions

\[ \langle B \rightarrow A : \beta \rangle \]

\[ \langle B \rightarrow A : \beta \rangle \xrightarrow{\text{\(\beta\)}} A \]

axiomatized as follows:

\[ \langle B \rightarrow A : \beta \rangle \xrightarrow{\beta} A \]

"If A sees B perform \(\beta\), then A knows that B has performed \(\beta\)."
Social actions

- **\(<B \rightarrow A \mid \beta\rangle \rightarrow B\) shows an action \(\beta\) to \(A\)**

  axiomatized as follows:
  - **\(<B \rightarrow A \mid \beta\rangle \rightarrow A \rightarrow B\)**
    - "If \(A\) sees \(B\) perform \(\beta\), then \(A\) knows that \(B\) has performed \(\beta\)."
  - **\(<B \rightarrow A \mid \beta\rangle \rightarrow C \rightarrow A \mid \gamma\rangle \rightarrow A \rightarrow \beta\gamma\)**
    - "If \(A\) sees \(\beta\) before \(\gamma\), then she knows that \(\beta\) occurred before \(\gamma\)."

Social actions

- **\(<B \rightarrow A \mid t\rangle \rightarrow B\) shows a term \(t\) to \(A\)**

  axiomatized as follows:
  - **\(<B \rightarrow A \mid t\rangle \rightarrow c \in \Gamma_{\alpha}\)**
    - "If \(B\) shows \(A\) a term \(t\), then \(A\) sees the digest \(c\)."

Social actions

- **\(<B \rightarrow A \mid \beta\rangle \rightarrow B\) shows an action \(\beta\) to \(A\)**

  axiomatized as follows:
  - **\(<B \rightarrow A \mid \beta\rangle \rightarrow A \rightarrow B\)**
    - "If \(A\) sees \(B\) perform \(\beta\), then \(A\) knows that \(B\) has performed \(\beta\)."
  - **\(<B \rightarrow A \mid \beta\rangle \rightarrow C \rightarrow A \mid \gamma\rangle \rightarrow A \rightarrow \beta\gamma\)**
    - "If \(A\) sees \(\beta\) before \(\gamma\), then she knows that \(\beta\) occurred before \(\gamma\)."

Social actions

- **\(<B \rightarrow A \mid t\rangle \rightarrow B\) shows a term \(t\) to \(A\)**

  axiomatized as follows:
  - **\(<B \rightarrow A \mid t\rangle \rightarrow c \in \Gamma_{\alpha}\)**
    - "If \(B\) shows \(A\) a term \(t\), then \(A\) sees the digest \(c\)."
  - **\(<B \rightarrow A \mid t\rangle \rightarrow A \rightarrow \beta\gamma\)**
    - "If \(B\) shows \(A\) a term \(t\), then \(A\) knows that \(B\) has shown her some term with the digest \(\beta\gamma\)."

Socially authenticated key distribution

Bob announces his public key

```
A
```

```
B
```

```
A
```

```
B
```
Socially authenticated key distribution
Bob announces his public key

\[ e, r \in \Gamma_A \]
\[ A : B \text{ honest } \implies \exists u. cu = r e \land (B \text{ to } A : u)_A \]

Socially authenticated key distribution
... but Ivan may have replaced it

\[ e, r \in \Gamma_A \]
\[ A : B \text{ honest } \implies \exists u. cu = r e \land (B \text{ to } A : u)_A \]

Social commitment

\[ e_1, c_1 \in \Gamma_A \]
\[ c_1 = c(y) \]
\[ d(x) = c_1(x) \]
\[ A : B \text{ honest } \implies \exists y. c(y) = s \land (B \text{ to } A : s)_B \]

Authentication before decommitment

\[ A : B \text{ honest } \implies \exists y. (u, c(y))_A \equiv (u)_y \]

Authentication before decommitment

\[ A : B \text{ honest } \implies \exists y. (u, c(y))_A \equiv (u)_y \]
Authentication before decommitment

\[ A \xrightarrow{e, cf(e, y)} B \]

\[ d(e, y) \]

\[ \sigma(y) \implies (\forall y)[(e, cf(e, y)]_2 \equiv \sigma(y)]_2 \equiv (d(e, y))_2 \]

Authentication after decommitment

\[ A \xrightarrow{e, cf(e, y)} B \]

\[ d(e, y) \]

\[ \sigma(y) \]

Authentication before decommitment

\[ A \xrightarrow{e, cf(e, y)} B \]

\[ a = y = g^x \]

\[ B \]

\[ B \xrightarrow{e, cf(e, y)} A \]

\[ d(e, y) \]

\[ \sigma(y) \]

\[ (\forall y)[(e, cf(e, y)]_2 \equiv \sigma(y)]_2 \equiv (g^y)_2 \]

Authentication after decommitment

\[ A \xrightarrow{e, cf(e, y)} B \]

\[ d(e, y) \]

\[ \sigma(y) \]

Authentication after decommitment

\[ A \xrightarrow{e, cf(e, y)} B \]

\[ d(e, y) \]

\[ \sigma(y) \]

Authentication after decommitment

\[ A \xrightarrow{e, cf(e, y)} B \]

\[ d(e, y) \]

\[ \sigma(y) \]
Authentication after decommitment

Vaudenay: SAS

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK

Vaudenay: SAS-

Authentication after decommitment

Nguyen-Roscoe: HCBK

Assumption: Initiator establishes the order

Assumptions (to be discharged)

* agreed ordering of the principals
Multi-party authentication after decommitment
Nguyen-Roscoe: HCBK

Assumptions (to be discharged)
- agreed ordering of the principals
  - all principals must digest at the same payload

Multi-party authentication after decommitment
Nguyen-Roscoe: HCBK

Assumptions (to be discharged)
- agreed ordering of the principals
  - all principals must digest at the same payload
- social protocol to compare the digests

Structural similarity — conceptual difference

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>V</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>e. df(x/y)</td>
<td>1y</td>
<td>df(y)</td>
<td>f(x/y)</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>f</td>
<td>x/y</td>
</tr>
<tr>
<td>df(x/y)</td>
<td>f(x/y)</td>
<td>df(y)/f(x/y)</td>
<td></td>
</tr>
</tbody>
</table>

Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions

Historical

Social protocol to compare the digests

Social authentication is not challenge-response:
- x on the left is not a challenge, but a binder, analogous to y.

Outline

Introduction
Authentication with timed channels
Authentication with social channels
Conclusions

Summary

- computation is becoming pervasive: in physical space
- new security landscape
  - need stronger authentication: proximity...
  - weaker cryptography: low power devices
  - bootstrap distance, proximity, routing...

Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions