Principles of Security — Part 5: Pervasive security Sections 3 and 4

Dusko Pavlovic

Oxford
Michaelmas Term 2008

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

Outline

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

Outline

Introduction

Authentication with timed channels

Authentication with social channels

Conclusions

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

Outline

Introduction

Authentication with timed channels

Authentication with social channels

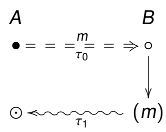
Conclusions

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

Outline

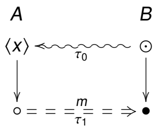
Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions

Preliminary example: a timed social protocol



Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions

Preliminary example: a timed social protocol



Social channel bandwidth

- $\sigma : \mathcal{T} \longrightarrow \mathcal{T}$: a short digest (hash) function

Social channel bandwidth

- $\sigma : \mathcal{T} \longrightarrow \mathcal{T}$: a short digest (hash) function

such that

- $\sigma\sigma t = \sigma t$
  - "The digest does not change short terms."

Social channel bandwidth

- $\sigma : \mathcal{T} \longrightarrow \mathcal{T}$: a short digest (hash) function

such that

- $\sigma\sigma t = \sigma t$
  - "The digest does not change short terms."
- $\forall s\ \exists t.\ s \neq t\ \wedge \sigma s = \sigma t\ \wedge\ s \vdash t$
  - "For every term s, it is feasible to find a different term t with the same digest."

Social actions

- <B to A : β> — B shows an action β to A

Social actions

- <B to A : β> — B shows an action β to A

axiomatized as follows:

- <B to A : β> $\Longrightarrow A : \beta_B$
  - "If A sees B perform β, then A knows that B has performed β."

Social actions

- $\langle B \text{ to } A : \beta \rangle$ — B shows an action β to A

axiomatized as follows:

- $\langle B \text{ to } A : \beta \rangle \implies A : \beta_B$
  - "If A sees B perform β, then A knows that B has performed β."
- $\langle B \text{ to } A : \beta \rangle \triangleright \langle C \text{ to } A : \gamma \rangle \implies A : \beta_B \triangleright \gamma_C$
  - "If A sees β_B before γ_C, then she knows that β_B occurred before γ_C."

Social actions

Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions

- $\langle B \text{ to } A : t \rangle$ — B shows a term t to A

Social actions

Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions

- $\langle B \text{ to } A : t \rangle$ — B shows a term t to A

axiomatized as follows:

- $\langle B \text{ to } A : t \rangle \implies \sigma t \in \Gamma_A$
  - "If B shows A a term t, then A sees the digest σt."

Social actions

Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions

- $\langle B \text{ to } A : t \rangle$ — B shows a term t to A

axiomatized as follows:

- $\langle B \text{ to } A : t \rangle \implies \sigma t \in \Gamma_A$
  - "If B shows A a term t, then A sees the digest σt."
- $\langle B \text{ to } A : t \rangle \implies A : \exists u.\ \sigma u = \sigma t \wedge \langle B \text{ to } A : u \rangle_B$
  - "If B shows A a term t, then A knows that B has shown her some term with the digest σt."

Social actions

Graphic notation

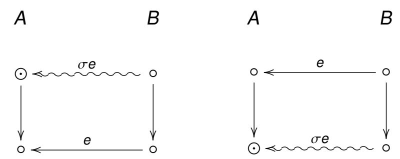
Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions

- $\beta_B \rightsquigarrow \odot_A$ represents $\langle B \text{ to } A : \beta \rangle$
- $\circ_B \overset{\sigma t}{\rightsquigarrow} \odot_A$ represents $\langle B \text{ to } A : t \rangle$

Socially authenticated key distribution

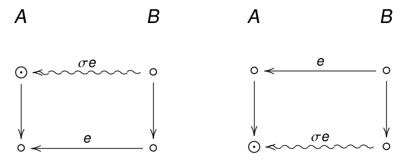
Bob announces his public key

Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Conclusions



Socially authenticated key distribution

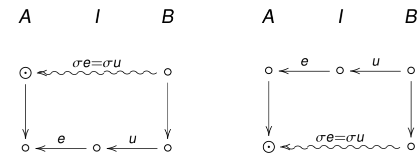
Bob announces his public key



- $e, \sigma e \in \Gamma_A$
- $A: \; B$ honest $\Longrightarrow \exists u.\ \sigma u = \sigma e \wedge \langle B \text{ to } A : u\rangle_B$

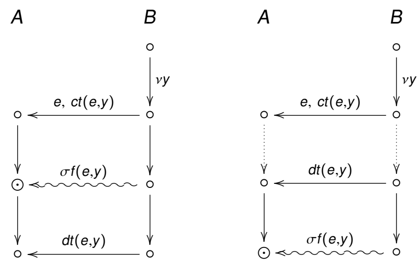
Socially authenticated key distribution

. . . but Ivan may have replaced it

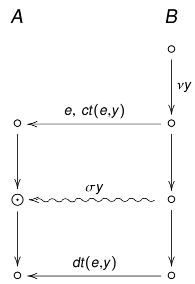


- $e, \sigma e \in \Gamma_A$
- $A: \; B$ honest $\Longrightarrow \exists u.\ \sigma u = \sigma e \wedge \langle B \text{ to } A : u\rangle_B$

Social commitment

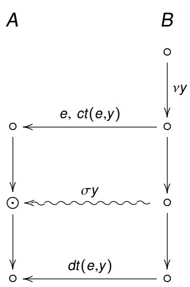


Authentication before decommitment



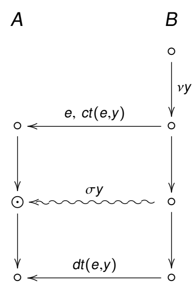
- $A: \; \exists y.\ \sigma y = s \wedge \text{<}B \text{ to } A : s\text{>}_B$

Authentication before decommitment



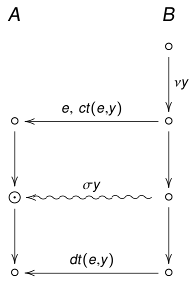
- $A: \; B$ honest $\Longrightarrow \exists y.\ \text{<} B \text{ to } A : \sigma y\text{>}_B$

Authentication before decommitment



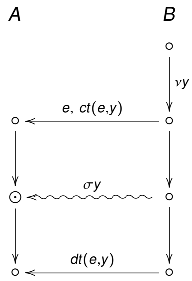
- $A: \; B$ honest $\Longrightarrow \exists u \exists y.\ \langle u, ct(u,y)\rangle_B \trianglerighteq \text{<}\sigma y\text{>}_B$

Authentication before decommitment



- $A: B$ honest $\Longrightarrow \exists u.\ (\nu y)_B \trianglerighteq \langle u, ct(u,y)\rangle_B \trianglerighteq \lessdot \sigma y \gtrdot_B$

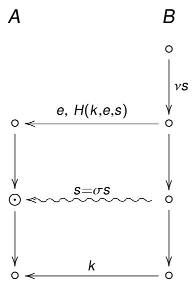
Authentication before decommitment



- $A: B$ honest $\Longrightarrow (\nu y)_B \trianglerighteq \langle e, ct(e,y)\rangle_B \trianglerighteq \lessdot \sigma y \gtrdot_B \trianglerighteq \langle dt(e,y)\rangle_B$

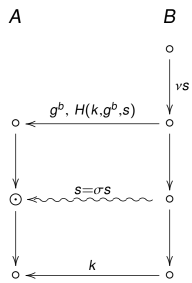
Authentication before decommitment

Wong-Stajano template



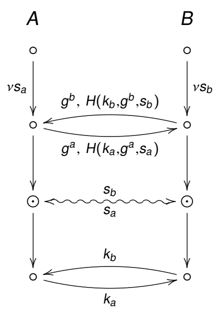
Authentication before decommitment

Wong-Stajano-$\frac{1}{2}$



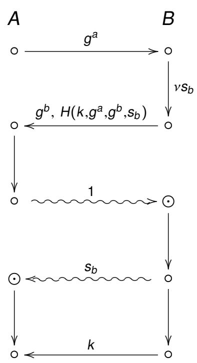
Authentication before decommitment

Wong-Stajano

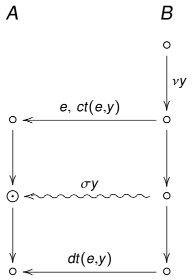


Authentication before decommitment

Wong-Stajano 3



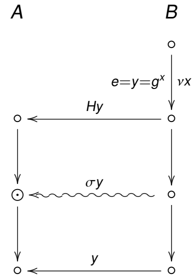
Authentication before decommitment



- $A : B$ honest $\Longrightarrow (\nu y)_B \trianglerighteq \langle e, ct(e,y)\rangle_B \trianglerighteq \lessdot \sigma y \gtrdot_B \trianglerighteq \langle dt(e,y)\rangle_B$

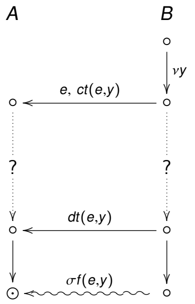
Authentication before decommitment

Hoepman-$\frac{1}{2}$

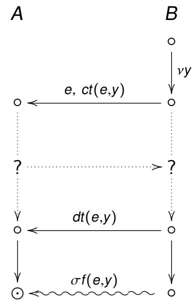


- $A : B$ honest $\Longrightarrow (\nu x)_B \trianglerighteq \langle H(g^x)\rangle_B \trianglerighteq \lessdot \sigma(g^x) \gtrdot_B \trianglerighteq \langle g^x\rangle_B$

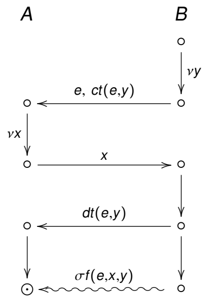
Authentication after decommitment



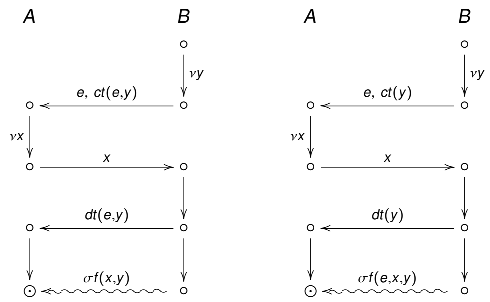
Authentication after decommitment



Authentication after decommitment

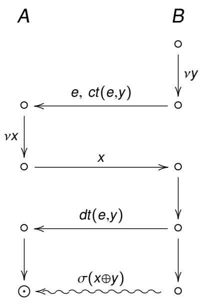


Authentication after decommitment



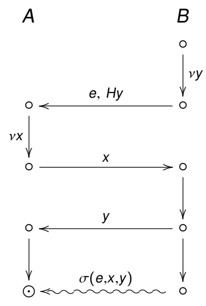
Authentication after decommitment

Vaudenay: SAS-$\frac{1}{2}$



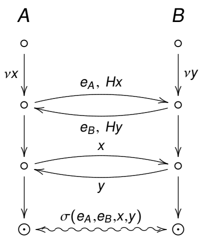
Authentication after decommitment

Nguyen-Roscoe: HCBK-$\frac{1}{2}$



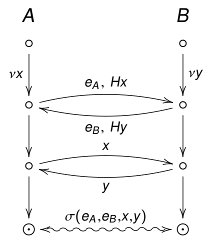
Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)



Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)



Assumption: Initiator establishes the order

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)

$$\Big((\nu x)_A\ \langle e_A, Hx\rangle_A\ (u_1,u_2)_A\ \otimes\ (\nu y)_B\ \langle e_B, Hy\rangle_B\ (v_1,v_2)_B\Big)\ ;$$

$$\Big(\langle x\rangle_A\ (u_3)_A\ (u_1,u_2/e_B,Hu_3)_A\ <\sigma(e_A,e_B,x,u_3)>_A\ \otimes\ \langle y\rangle_B\ (v_3)_B\ (v_1,v_2)/e_A,Hv_3)_B\ <\sigma(e_A,e_B,v_3,y)>_B\Big)$$

Multi-party authentication after decommitment

Nguyen-Roscoe: HCBK

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

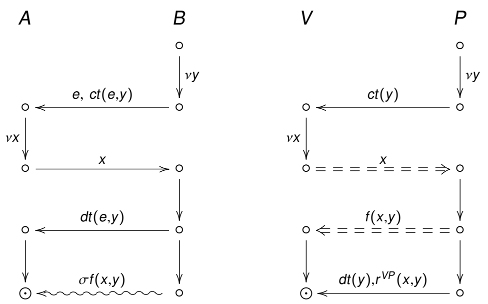
Multi-party authentication after decommitment

Nguyen-Roscoe: HCBK

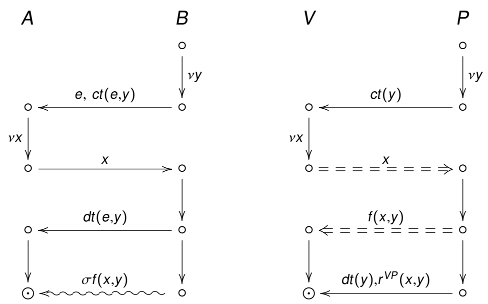
Assumptions (to be discharged)

- agreed ordering of the principals
  - all principals must digest at the same payload
- social protocol to compare the digests

Structural similarity — conceptual difference



Structural similarity — conceptual difference



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...