Authentication in pervasive and social computation

Dusko Pavlovic

Kestrel Institute
and
Oxford University

January-May 2008

with thanks to Cathy Meadows, Mike Mislove, John Mitchell, Bill Roscoe

Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Outline

Introduction

Model of network computation

Authentication with timed channels

Symbolic model with partial information and guessing

Authentication with social channels

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Outline

Introduction
- Problem of security engineering
- Approach: Protocol derivations
- Example: Deriving CR
- Task

Model of network computation

Authentication with timed channels

Symbolic model with partial information and guessing

Authentication with social channels

Trust & reputation

Deriving location authentication protocols

Problem of security engineering

Problem of security engineering

Verified protocols often fail

Problem of security engineering

Verified protocols often fail

Bull's protocol

- *Isabelle:* secure for $E(k, m; n)$
- *Ryan & Schneider:* not for $E(k, m; n) = n \oplus H_k(m)$

Problem of security engineering

Verified protocols often fail

Bull's protocol

- *Isabelle:* secure for $E(k, m; n)$
- *Ryan & Schneider:* not for $E(k, m; n) = n \oplus H_k(m)$

IPSec GDoI

- *IETF MSec WG:* secure, verified
- *Cathy & Dusko:* GDoI_PoP attack

Pervasive authentication
Dusko Pavlovic
Introduction
Problem
Approach
Example
Task
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Problem of security engineering

Verified protocols often fail

Bull's protocol

- *Isabelle:* secure for $E(k, m; n)$
- *Ryan & Schneider:* not for $E(k, m; n) = n \oplus H_k(m)$

IPSec GDoI

- *IETF MSec WG:* secure, verified
- *Cathy & Dusko:* GDoI_PoP attack

MQV

- *NSA:* "MQV is critical for national security of US"
- *Krawczyk:* MQV insecure

Pervasive authentication
Dusko Pavlovic
Introduction
Problem
Approach
Example
Task
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Problem of security engineering

Verified protocols often fail

Bull's protocol

- *Isabelle:* secure for $E(k, m; n)$
- *Ryan & Schneider:* not for $E(k, m; n) = n \oplus H_k(m)$

IPSec GDoI

- *IETF MSec WG:* secure, verified
- *Cathy & Dusko:* GDoI_PoP attack

MQV

- *NSA:* "MQV is critical for national security of US"
- *Krawczyk:* MQV insecure, HMQV proven secure

Pervasive authentication
Dusko Pavlovic
Introduction
Problem
Approach
Example
Task
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Problem of security engineering

Verified protocols often fail

Bull's protocol

- *Isabelle:* secure for $E(k, m; n)$
- *Ryan & Schneider:* not for $E(k, m; n) = n \oplus H_k(m)$

IPSec GDoI

- *IETF MSec WG:* secure, verified
- *Cathy & Dusko:* GDoI_PoP attack

MQV

- *NSA:* "MQV is critical for national security of US"
- *Krawczyk:* MQV insecure, HMQV proven secure
- *Menezes:* HMQV insecure

Pervasive authentication
Dusko Pavlovic
Introduction
Problem
Approach
Example
Task
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Problem of security engineering

Thesis: Informal reasoning is error prone.

Pervasive authentication
Dusko Pavlovic
Introduction
Problem
Approach
Example
Task
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Problem of security engineering

Thesis: Informal reasoning is error prone.

Antithesis: Formal reasoning hides some attacks

Pervasive authentication
Dusko Pavlovic
Introduction
Problem
Approach
Example
Task
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Problem of security engineering

Thesis: Informal reasoning is error prone.

Antithesis: Formal reasoning hides some attacks, and becomes error prone as it gets complicated.

Derivational approach

Thesis: Informal reasoning is error prone.

Antithesis: Formal reasoning hides some attacks, and becomes error prone as it gets complicated.

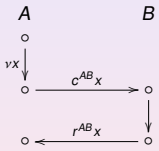
Synthesis: Incremental formalization:
Do not try to say all at once.

Derivational approach

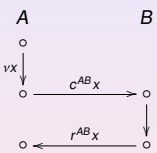
Problem
Incompleteness is the central concern in security engineering.

Solution
Protocol derivations manage it interactively.

Example: Deriving authentications

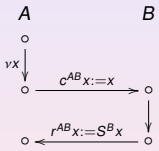


Example: Deriving authentications



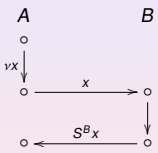
$$A:\ (\nu x)_A\Big(\langle\langle c^{AB}x\rangle\rangle_A \quad \triangleright \quad ((r^{AB}x))_A$$
$$\Longrightarrow\ \langle\langle c^{AB}x\rangle\rangle_A \triangleright ((c^{AB}x))_B \triangleright \langle\langle r^{AB}x\rangle\rangle_B \triangleright ((r^{AB}x))_A\Big) \quad \text{(cr)}$$

Signature-based challenge-response (CRS)



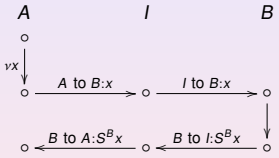
$$S^Bt = S^Bu \implies t = u \qquad \text{(sig1)}$$
$$V^B(y,t) \iff y = S^Bt \qquad \text{(sig2)}$$
$$\langle\langle S^Bt\rangle\rangle_X \implies X = B \qquad \text{(sig3)}$$

Signature-based challenge-response (CRS)

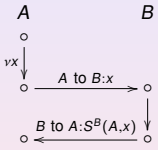


$(sig1\text{-}3) \wedge (B \text{ honest}) \vdash (cr)_{[c^{AB}x:=x,\ r^{AB}x:=S^B x]}$

Problem

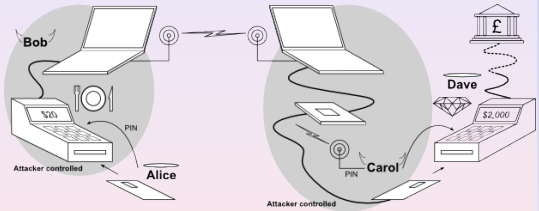


Signature-based challenge-response (CRS)

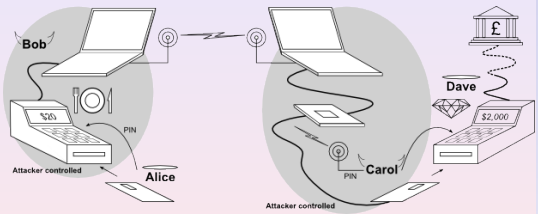


$(sig1\text{-}3) \wedge (B \text{ honest}) \vdash (cr)_{[c^{AB}x:=x,\ r^{AB}x:=S^B(A,x)]}$
$\wedge$ "B to A : $S^B(A,x)$"...

Problem



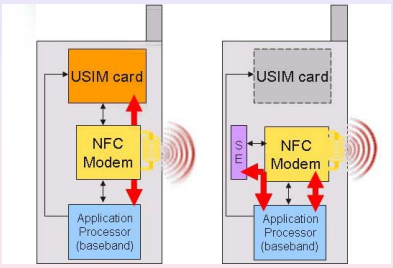
Problem



This becomes much easier with NFC phones!

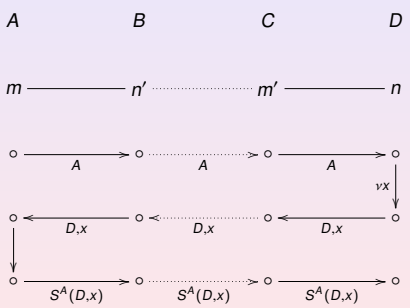
Near Field Communication (NFC)

Phone with a contactless smart card:



Secure Element (SE) is a miniSD flash memory, or a USIM card, or a separate microcontroller.

Agreement without proximity



Task

Study proximity authentication.

Outline

Introduction

Model of network computation
- Process model
- Network model

Authentication with timed channels

Symbolic model with partial information and guessing

Authentication with social channels

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Process model

terms $(\mathcal{T}, \sqsubseteq)$,

principals $(\mathcal{W}, \leqslant)$,

actions $\mathcal{A}$ generated by:

action	constructor	form
send	$\mathcal{W}^2 \times \mathcal{T} \overset{\langle\rangle}{\hookrightarrow} \mathcal{A}$	$\langle A \text{ to } B : t \rangle$
receive	$\mathrm{Var}^2_{\mathcal{W}} \times \mathrm{Var}_{\mathcal{T}} \overset{()}{\hookrightarrow} \mathcal{A}$	$(Y \text{ to } Z : x)$
match	$\mathcal{T} \times \mathrm{Op}_{\mathcal{T}} \times \mathrm{Var}_{\mathcal{W}} \overset{(/)}{\hookrightarrow} \mathcal{A}$	$(t/p(x))$
new	$\mathrm{Var}_{\mathcal{T}} \overset{(\nu)}{\hookrightarrow} \mathcal{A}$	(νx)
$\cdots$	$\cdots$	$\cdots$

Process model

processes $\mathbb{P} \xrightarrow{P} \mathcal{A} \times \mathcal{W}$ where
- $(\mathbb{P}, \triangleright)$ is a well-founded partial order
- $P_{\mathcal{W}}(p) \# P_{\mathcal{W}}(q) \;\Rightarrow\; p \# q$

runs $\big(P,\ \surd :\ \mathrm{recvs}(P) \longrightarrow \mathrm{sends}(P)\big),\ (x) \not\vdash \surd(x)$
- $\mathbb{P}^{\surd} = \mathbb{P} / \left(\surd(x) \triangleright (x)\right)$

Network model

A *communication network* consists of

network graph $\mathcal{N} = (L \underset{\varrho}{\overset{\delta}{\rightrightarrows}} N)$, where
- N is the set of nodes,
- $L = \sum_{N \times N} \mathcal{N}_{mn}$ is the set of links,
- $\mathcal{N}_{mn} = \langle \delta, \varrho \rangle^{-1}(m, n)$

Network model

A *communication network* consists of

network graph $\mathcal{N} = (L \underset{\varrho}{\overset{\delta}{\rightrightarrows}} N)$, where

- N is the set of nodes,
- $L = \sum_{N\times N} \mathcal{N}_{mn}$ is the set of links,
- $\mathcal{N}_{mn} = \langle \delta, \varrho \rangle^{-1}(m, n)$

control assignment $\copyright : \mathcal{W} \longrightarrow \wp N$, satisfying

$$A \leqslant B \implies \copyright A \subseteq \copyright B$$
$$A \# B \implies \copyright A \cap \copyright B = \emptyset$$

Network model

A *communication network* consists of

network graph $\mathcal{N} = (L \underset{\varrho}{\overset{\delta}{\rightrightarrows}} N)$, where

- N is the set of nodes,
- $L = \sum_{N\times N} \mathcal{N}_{mn}$ is the set of links,
- $\mathcal{N}_{mn} = \langle \delta, \varrho \rangle^{-1}(m, n)$

control assignment $\copyright : \mathcal{W} \longrightarrow \wp N$, satisfying

$$A \leqslant B \implies \copyright A \subseteq \copyright B$$
$$A \# B \implies \copyright A \cap \copyright B = \emptyset$$

channel typing $\theta : L \longrightarrow C$,

Outline

Introduction

Model of network computation

Authentication with timed channels
- Timed challenge-response
- Distance bounding with two responses
  - Solution 1: Commitment
  - Solution 2: One-way response
- Distance bounding with two challenges
- Simple distance bounding

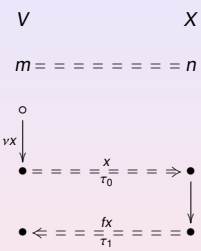
Symbolic model with partial information and guessing

Authentication with social channels

Trust & reputation

Timed challenge-response

Timed challenge-response



$$V : (\nu x)_V \Big(\tau_0 \langle x \rangle_V \triangleright \tau_1 (fx)_V \implies \exists X.\, d(V, X) \leq \frac{c}{2}(\tau_1 - \tau_0) \Big) \quad \text{(crt)}$$

Distance bounding protocols

Idea

Combine (cr) and (crt).

Distance bounding protocols

Idea

Combine (cr) and (crt).

Three families

Distance bounding protocols

Idea

Combine (cr) and (crt).

Three families

- with **one challenge and two responses**:
  - $r^{VP}x$, satisfying (cr)
  - $f^{VP}x$, satisfying (crt)

Distance bounding protocols

Idea

Combine (cr) and (crt).

Three families

- with **one challenge and two responses**:
  - $r^{VP}x$, satisfying (cr)
  - $f^{VP}x$, satisfying (crt)
- with **two challenges and one response**:
  - $c^{VP}y$ and $fr^{VP}(x,y)$, satisfying (cr)
  - x and $fr^{VP}(x,y)$, satisfying (crt)

Distance bounding protocols

Idea

Combine (cr) and (crt).

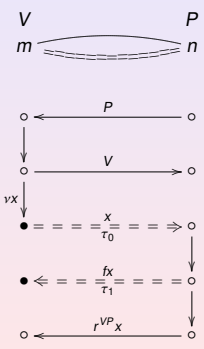
Three families

- with **one challenge and two responses**:
  - $r^{VP}x$, satisfying (cr)
  - $f^{VP}x$, satisfying (crt)
- with **two challenges and one response**:
  - $c^{VP}y$ and $fr^{VP}(x,y)$, satisfying (cr)
  - x and $fr^{VP}(x,y)$, satisfying (crt)
- with **one challenge and one response**:
  - x and $fr^{VP}x$, satisfying

$$V:\ (\nu x)_V\Big(\tau_0\langle x\rangle_V \quad \triangleright \quad \tau_1(fr^{VP}x)_V$$
$$\Longrightarrow\ \tau_0\langle x\rangle_V \triangleright (x)_P \triangleright \langle fr^{VP}x\rangle_P \triangleright \tau_1(fr^{VP}x)_V \qquad \text{(crp)}$$
$$\wedge \quad d(V,P) \le \tau_1 - \tau_0\Big)$$

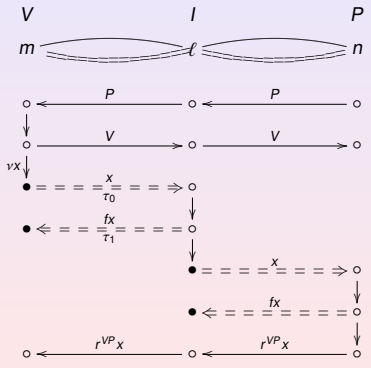
Distance bounding with two responses

Idea



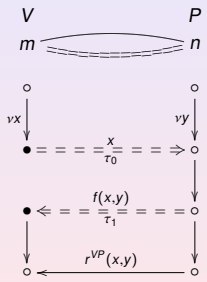
Distance bounding with two responses

Problem

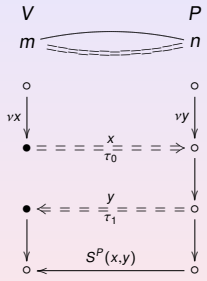


Distance bounding with two responses

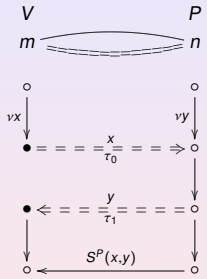
Basic template



Brands-Chaum 1

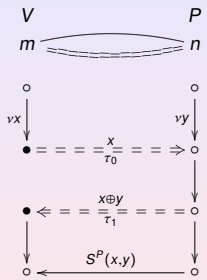


Brands-Chaum 1

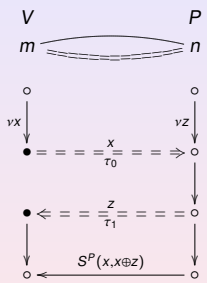


- V : P honest $\implies d(V,P) < \tau_1 - \tau_0$
- V : $\forall X.\ X$ responds $\implies d(V,X) + d(X,P) < \tau_1 - \tau_0$

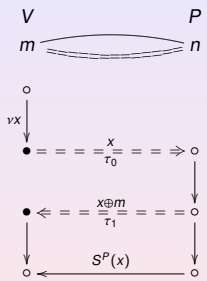
Discharge the honesty assumption?



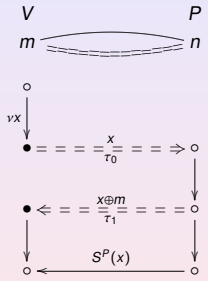
P can still cheat



Brands-Chaum 2

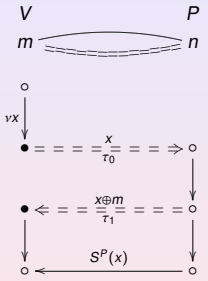


Brands-Chaum 2



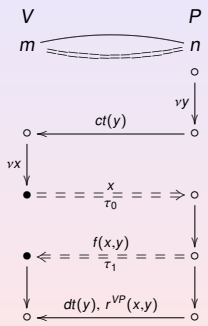
- Peggy cannot cheat

Brands-Chaum 2



- Peggy cannot cheat
- Ivan can impersonate her, and relay $S^P(x)$

Solution 1: Commitment



Digression: Symbolic commitment

Definition

A *commitment schema* consists of three publicly known functions over the space of messages $\mathcal{T}$,

- *commitment* $ct : \mathcal{T} \longrightarrow \mathcal{T}$,
- *decommitment* $dt : \mathcal{T} \longrightarrow \mathcal{T}$, and
- *open commitment* $ot : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$,

such that

- ct is a one-way collision-free function,
- $ot\,(ct(x), dt(x)) = x$.

Digression: Symbolic commitment

Definition

A *commitment schema* consists of three publicly known functions over the space of messages $\mathcal{T}$,

- *commitment* $ct : \mathcal{T} \longrightarrow \mathcal{T}$,
- *decommitment* $dt : \mathcal{T} \longrightarrow \mathcal{T}$, and
- *open commitment* $ot : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$,

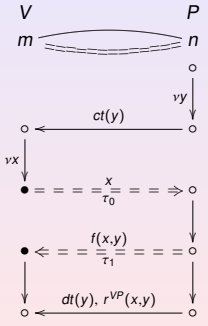
such that

- ct is a one-way collision-free function,
- $ot\,(ct(x), dt(x)) = x$.

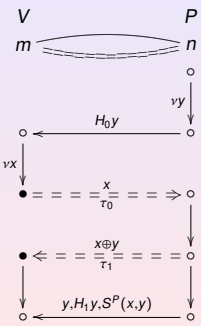
E.g.,

$ct(x) = H(x)$	$ct(x) = H_0(x)$	$ct(x) = E(x_0, x_1)$
$dt(x) = x$	$dt(x) = x::H_1(x)$	$dt(x) = x_0$
$ot(y,z) = z$	$ot(y,z) = z_0$	$ot(y,z) = D(z,y)$

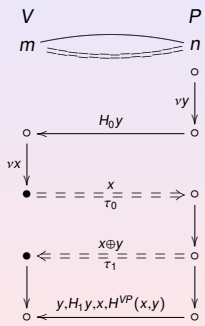
Solution 1: Commitment



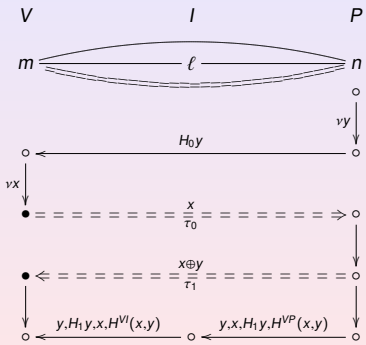
Brands-Chaum 3



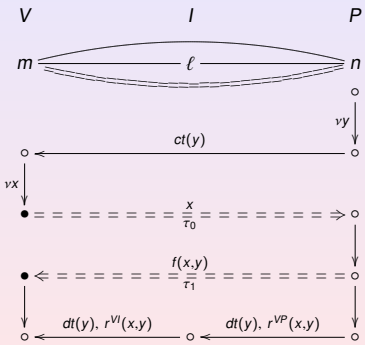
Čapkun-Hubaux



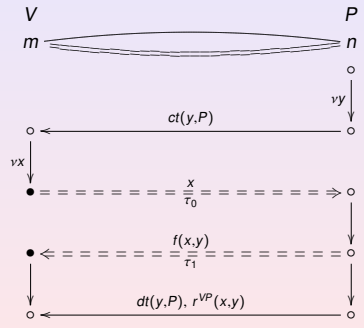
. . . but Peggy's identity can be spoofed



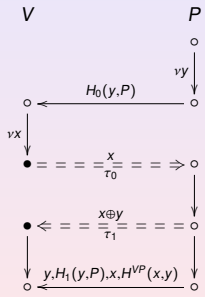
. . . and in general



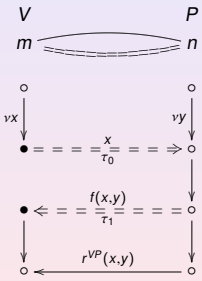
. . . so we need



Meadows et al

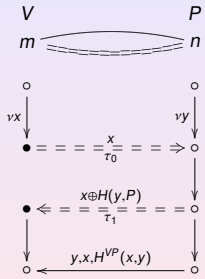


Solution 2: One-way response

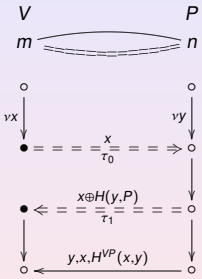


where $f^{VP}(x,-)$ is a one-way function for every x.

Meadows et bo

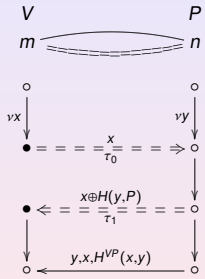


Meadows et bo



- $V:\ \exists X.\ d(V,X) < \tau_1 - \tau_0 \wedge X \sim P$

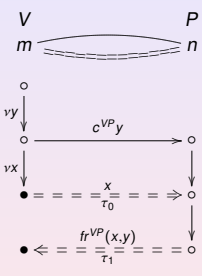
Meadows et bo



- $V:\ \exists X.\ d(V,X) < \tau_1 - \tau_0 \wedge X \sim P$
- $V:\ \forall X.\ X \text{ responds} \Longrightarrow d(V,X) + d(X,P) < \tau_1 - \tau_0$

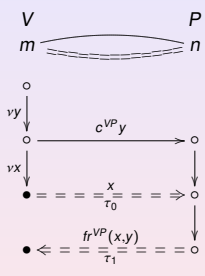
Distance bounding with two challenges

Idea



Distance bounding with two challenges

Idea

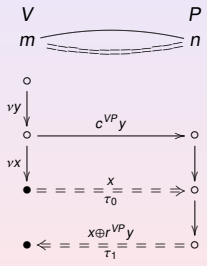


where

- $fr^{VP}(x,-)$ satisfies (cr) for all x
- $fr^{VP}(-,y)$ satisfies (crt) for all y

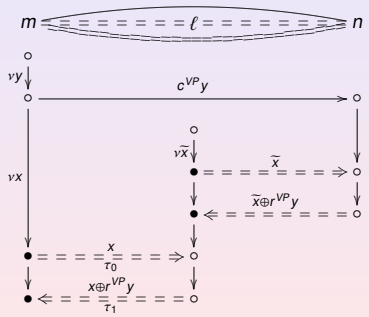
Distance bounding with two challenges

Try



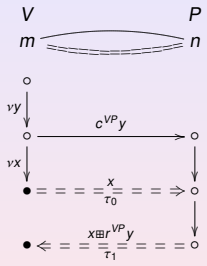
Distance bounding with two challenges

Problem



Distance bounding with two challenges

Idea 2: Find $\boxplus$

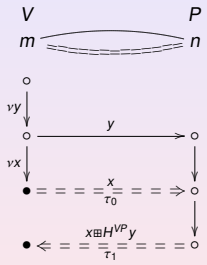


where

- r^{VP} satisfies (cr)
- $x \boxplus (-)$ is one-way function for every x
- $(-) \boxplus y$ satisfies (crt) for every y

Hancke-Kuhn

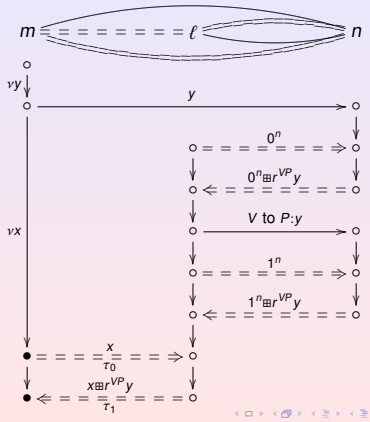
Candidate



$$x \boxplus z \;=\; [z_i^{(x_i)}] \quad \text{where } z = z^{(0)}::z^{(1)}$$

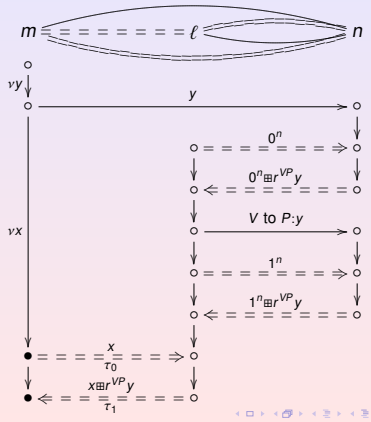
Hancke-Kuhn

Problem



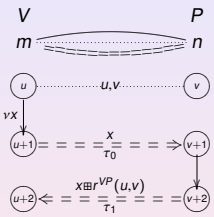
Hancke-Kuhn

Problem: $a \boxplus z, \overline{a} \boxplus z \;\vdash\; (-) \boxplus z$, for any a



Simple distance bounding template

Idea 3: Use **counters** to disable querying of $(-) \boxplus r^{VP} y$



Simple distance bounding template

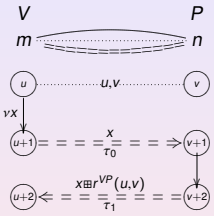
Idea 3: Use **counters** to disable querying of $(-) \boxplus r^{VP} y$

where

- r^{VP} satisfies (cr)
- $x \boxplus (-)$ is one-way function for every x
- $(-) \boxplus z$ satisfies (crt) for every z

Simple distance bounding template

Idea 3: Use **counters** to disable querying of $(-) \boxplus r^{VP} y$



where

- r^{VP} satisfies (cr)
- $x \boxplus (-)$ is one-way function for every x
- $(-) \boxplus z$ satisfies (crt) for every z
- the counters u, v are public, but never reused

Outline

Introduction

Model of network computation

Authentication with timed channels

Symbolic model with partial information and guessing
- Algebra coding
- Guessing
- Base and dimension

Authentication with social channels

Trust & reputation

Deriving location authentication protocols

Algebra coding

- $\mathcal{T}$ be a term algebra over a clone T
- $\mathcal{L}$ a language over an alphabet Σ

Algebra coding

- $\mathcal{T}$ be a term algebra over a clone T
- $\mathcal{L}$ a language over an alphabet Σ

Definition

An *encoding* (or *implementation*) of $\mathcal{T}$ in $\mathcal{L}$ is a pair of maps

$$\begin{aligned} [\![-]\!] &: \mathcal{T} \to \mathcal{L} \\ \surd &: \mathcal{L} \rightharpoonup \mathcal{T} \end{aligned}$$

such that $\surd[\![t]\!] = t$.

Feasible algebra

Notation and terminology

- $\Sigma_\perp = \Sigma + \{\perp\}$, where $\perp \sqsubset s$ for $s \in S$

Feasible algebra

Notation and terminology

- $\Sigma_\perp = \Sigma + \{\perp\}$, where $\perp \sqsubset s$ for $s \in S$
- $\mathcal{L}_\perp = \{\alpha \in \Sigma_\perp^* \mid \exists \xi \in \mathcal{L}.\ \alpha \sqsubseteq \xi\}$

Feasible algebra

Notation and terminology

- $\Sigma_\perp = \Sigma + \{\perp\}$, where $\perp \sqsubset s$ for $s \in S$
- $\mathcal{L}_\perp = \{\alpha \in \Sigma_\perp^* \mid \exists \xi \in \mathcal{L}.\ \alpha \sqsubseteq \xi\}$
- $\alpha \sqsubseteq \beta \iff |\alpha| \leq |\beta| \wedge \forall i \leq |\alpha|.\ \alpha_i \sqsubset \beta_i \vee \alpha_i = \beta_i$

Feasible algebra

Notation and terminology

- $\Sigma_\perp = \Sigma + \{\perp\}$, where $\perp \sqsubset s$ for $s \in S$
- $\mathcal{L}_\perp = \{\alpha \in \Sigma_\perp^* \mid \exists \xi \in \mathcal{L}.\ \alpha \sqsubseteq \xi\}$
- $\alpha \sqsubseteq \beta \iff |\alpha| \leq |\beta| \wedge \forall i \leq |\alpha|.\ \alpha_i \sqsubset \beta_i \vee \alpha_i = \beta_i$
- $\mathcal{F} \subseteq [\mathcal{L}_\perp \Rightarrow \mathcal{L}_\perp]_{\sqcup\uparrow}$, a submonoid of *feasible* maps

Feasible algebra

Definition

An algebraic operation $\varphi \in T$ is called *feasible* if the partial map

$$\begin{array}{rcl} [\![\varphi]\!] : \mathcal{L} & \rightharpoonup & \mathcal{L} \\ [\![t]\!] & \mapsto & [\![\varphi t]\!] \end{array}$$

can be extended to a feasible map.

Feasible algebra

Definition

An algebraic operation $\varphi \in T$ is called *feasible* if the partial map

$$\begin{array}{rcl} [\![\varphi]\!] : \mathcal{L} & \rightharpoonup & \mathcal{L} \\ [\![t]\!] & \mapsto & [\![\varphi t]\!] \end{array}$$

can be extended to a feasible map.

Example

Hohenberger-Rivest: pseudo-free groups

Derivability

Definition

For $\alpha_1, \ldots, \alpha_n, \beta \in \mathcal{L}_\perp$ define the *derivability* relation

$$\alpha_1, \ldots, \alpha_n \vdash \beta \iff \exists f_1, \ldots f_n \in \mathcal{F}.\ \bigsqcup_{i=1}^{n} f_i \alpha_i \sqsupseteq \beta$$

Derivability

Definition

For $\alpha_1, \ldots, \alpha_n, \beta \in \mathcal{L}_\perp$ define the *derivability* relation

$$\alpha_1, \ldots, \alpha_n \vdash \beta \iff \exists f_1, \ldots f_n \in \mathcal{F}.\ \bigsqcup_{i=1}^{n} f_i \alpha_i \sqsupseteq \beta$$

For a multiset of terms $s_1, \ldots, s_n, t \in \mathcal{T}$, we abbreviate

$$s_1, \ldots, s_n \vdash t \iff [\![s_1]\!], \ldots, [\![s_n]\!] \vdash [\![t]\!]$$

Frequency distribution

Assumption

Suppose that $\mathcal{L}$ is given with a probability measure

$$\mathrm{Prob} \ : \ \mathcal{M}(\mathcal{L}) \longrightarrow [0,1]$$

Frequency distribution

Assumption

Suppose that $\mathcal{L}$ is given with a probability measure

$$\mathrm{Prob} \ : \ \mathcal{M}(\mathcal{L}) \longrightarrow [0,1]$$

For simplicity, take

- $\mathcal{L} = \{0,1\}^*$
- $\mathcal{M}\{0,1\}^* = \left[\alpha^\uparrow \subseteq \{0,1\}^*\right]$
  - where $\alpha^\uparrow = \{\xi \in \{0,1\}^* \mid \alpha \sqsubseteq \xi\}$
- $\mathrm{Prob}(\alpha^\uparrow) = 2^{-|\alpha|}$

Derivability with guessing

Guessing a term

- $\mathrm{Prob}(t|A) \ = \ \frac{\mathrm{Prob}\left([\![t]\!]^\uparrow \cap A^\uparrow\right)}{\mathrm{Prob}(A^\uparrow)}$

Derivability with guessing

Guessing a term

- $\mathrm{Prob}(t|A) \ = \ \frac{\mathrm{Prob}\left([\![t]\!]^\uparrow \cap A^\uparrow\right)}{\mathrm{Prob}(A^\uparrow)}$
- $\mathrm{Prob}(t|\alpha) \ = \ \frac{\mathrm{Prob}\left([\![t]\!]^\uparrow \cap \alpha^\uparrow\right)}{\mathrm{Prob}(\alpha^\uparrow)} \ = \ \begin{cases} 2^{\|\alpha\| - \|[\![t]\!]\|} & \text{if } \alpha \sqsubseteq [\![t]\!] \\ 0 & \text{otherwise} \end{cases}$
  - where $\|\alpha\| = |\alpha \restriction_\Sigma|$

Derivability with guessing

Guessing a term

- $\mathrm{Prob}(t|A) = \frac{\mathrm{Prob}\left(\llbracket t \rrbracket^{\uparrow} \cap A^{\uparrow}\right)}{\mathrm{Prob}(A^{\uparrow})}$
- $\mathrm{Prob}(t|\alpha) = \frac{\mathrm{Prob}\left(\llbracket t \rrbracket^{\uparrow} \cap \alpha^{\uparrow}\right)}{\mathrm{Prob}(\alpha^{\uparrow})} = \begin{cases} 2^{\|\alpha\|-\|\llbracket t \rrbracket\|} & \text{if } \alpha \sqsubseteq \llbracket t \rrbracket \\ 0 & \text{otherwise} \end{cases}$
  - where $\|\alpha\| = |\alpha\restriction_{\Sigma}|$

Definition

For $\alpha_1, \ldots, \alpha_n, \beta \in \mathcal{L}_{\perp}$ and $\delta \geq 0$ define

$$\alpha_1, \ldots, \alpha_n \vdash_{\delta} \beta \iff \exists f_1, \ldots f_n \in \mathcal{F}.\ \mathrm{Prob}\left(\beta \mid f_1\alpha_1, \ldots, f_n\alpha_n\right) \geq \delta$$

Base and dimension

Base

Let $\varphi \in T$ be an algebraic operation and $B = \{b_1, \ldots, b_k\} \subseteq \mathcal{T}$. Define

- $\varphi[B]_{\delta} = \left\{t \in \mathcal{T} \mid t, B, \varphi(B) \vdash_{\delta} \varphi(t)\right\}$

Base and dimension

Base

Let $\varphi \in T$ be an algebraic operation and $B = \{b_1, \ldots, b_k\} \subseteq \mathcal{T}$. Define

- $\varphi[B]_{\delta} = \left\{t \in \mathcal{T} \mid t, B, \varphi(B) \vdash_{\delta} \varphi(t)\right\}$
- $\mathrm{base}_{\delta\epsilon}(\varphi) = \left\{B \in \wp_{<\omega}\mathcal{T} \mid \mathrm{Prob}\left(\varphi[B]_{\delta}\right) \geq \epsilon\right\}$

Base and dimension

Base

Let $\varphi \in T$ be an algebraic operation and $B = \{b_1, \ldots, b_k\} \subseteq \mathcal{T}$. Define

- $\varphi[B]_{\delta} = \left\{t \in \mathcal{T} \mid t, B, \varphi(B) \vdash_{\delta} \varphi(t)\right\}$
- $\mathrm{base}_{\delta\epsilon}(\varphi) = \left\{B \in \wp_{<\omega}\mathcal{T} \mid \mathrm{Prob}\left(\varphi[B]_{\delta}\right) \geq \epsilon\right\}$

Dimension

- $\dim_{\delta\epsilon}(\varphi) = \bigwedge_{B \in \mathrm{base}_{\delta\epsilon}(\varphi)} |B|$

Examples

eXclusive OR

Refine $b, b \oplus c \vdash x \oplus c$ for all $b, c, x \in \{0,1\}^{\ell}$ to show

- $\mathrm{base}_{\delta\epsilon}(- \oplus c) = \begin{cases} \{0,1\}^{*} & \text{if } \epsilon \leq 2^{-k} \wedge \delta \leq 2^{\ell-k} \\ \{0,1\}^{k} & \text{if } \epsilon > 2^{-k} \wedge \delta \leq 2^{\ell-k} \end{cases}$
- $\dim_{\delta\epsilon}(- \oplus c) = \begin{cases} 0 & \text{if } \epsilon \leq 2^{-k} \wedge \delta \leq 2^{\ell-k} \\ 1 & \text{if } \epsilon > 2^{-k} \wedge \delta \leq 2^{\ell-k} \end{cases}$

Examples

One-way XOR

For $\Sigma = \{0, 1, \ldots, n-1\}$ and $d = d^{(0)}::d^{(1)}::\ldots d^{(n-1)} \in \Sigma^{n\ell}$ define

$$\begin{array}{rcl} (-) \boxplus d : \Sigma^{\ell} & \longrightarrow & \Sigma^{\ell} \\ z & \mapsto & \left[d_1^{(z_1)}, d_2^{(z_2)}, \ldots, d_{\ell}^{(z_{\ell})}\right] \end{array}$$

Examples

One-way XOR

Refine
$0^\ell, 1^\ell, \ldots, (n-1)^\ell, 0^\ell \boxplus d, \ldots, (n-1)^\ell \boxplus d \vdash x \boxplus d$
to show

$$\dim_{\delta\epsilon}(- \boxplus d) = \begin{cases} 1 & \text{if } \epsilon \in \left[0, 2^{-nk}\right] \\ 2 & \text{if } \epsilon \in \left(2^{-nk}, 2^{(1-n)k}\right] \\ \vdots & \\ i+1 & \text{if } \epsilon \in \left(2^{(i-1-n)k}, 2^{(i-n)k}\right] \\ \vdots & \\ n & \text{if } \epsilon \in \left(2^{-k}, 1\right] \end{cases}$$

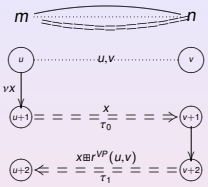
Upshot

Proposition

For all $\delta, \epsilon \geq 0$, and any $A \subseteq \mathcal{T}$ holds

$$|A| < \dim_{\delta\epsilon}(\varphi) \implies \mathrm{Prob}\big(t \in \mathcal{T} \mid t, A, \varphi(A) \vdash_\delta \varphi(t)\big) < \epsilon$$

Corollary



satisfies

$$V: (\nu x)_V\Big(\tau_0\langle x\rangle_V \triangleright \tau_1(fr^{VP}x)_V \implies \tau_0\langle x\rangle_V \triangleright (x)_P \triangleright \langle fr^{VP}x\rangle_P \triangleright \tau_1(fr^{VP}x)_V \wedge d(V,P) \leq \tau_1 - \tau_0\Big)$$

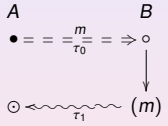
with probability $1 - 2^{-|x|}$.

Outline

Introduction
Model of network computation
Authentication with timed channels
Symbolic model with partial information and guessing
Authentication with social channels
- Social channel and its use
- Social commitment
- Authentication before decommitment
- Authentication after decommitment
- Socially authenticated key exchange
- Security homology

Trust & reputation

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."

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

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."

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Social actions

- $\ll B$ to $A : \beta \gg$ — B shows an action β to A

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Social actions

- $\ll B$ to $A : \beta \gg$ — B shows an action β to A

axiomatized as follows:

- $\ll B$ to $A : \beta \gg \implies A : \beta_B$
  - "If A sees B perform β, then A knows that B has performed β."

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Social actions

- $\ll B$ to $A : \beta \gg$ — B shows an action β to A

axiomatized as follows:

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

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Social actions

- $\ll B$ to $A : t \gg$ — B shows a term t to A

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Social actions

- $\lessdot B$ to $A : t \gtrdot$ — B shows a term t to A

axiomatized as follows:

- $\lessdot B$ to $A : t \gtrdot \implies \sigma t \in \Gamma_A$
  - "If B shows A a term t, then A sees the digest σt."

Social actions

- $\lessdot B$ to $A : t \gtrdot$ — B shows a term t to A

axiomatized as follows:

- $\lessdot B$ to $A : t \gtrdot \implies \sigma t \in \Gamma_A$
  - "If B shows A a term t, then A sees the digest σt."
- $\lessdot B$ to $A : t \gtrdot \implies A : \exists u.\ \sigma u = \sigma t \wedge \lessdot A$ to $B : u \gtrdot_B$
  - "If B shows A a term t, then A knows that B has shown her some term with the digest σt."

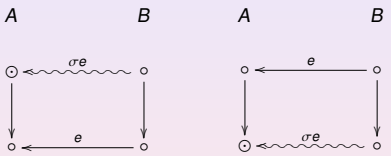
Social actions

Graphic notation

- $\beta_B \rightsquigarrow \odot_A$ represents $\lessdot B$ to $A : \beta \gtrdot$
- $\circ_B \overset{\sigma t}{\rightsquigarrow} \odot_A$ represents $\lessdot B$ to $A : t \gtrdot$

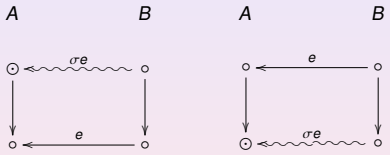
Socially authenticated key distribution

Bob announces his public key



Socially authenticated key distribution

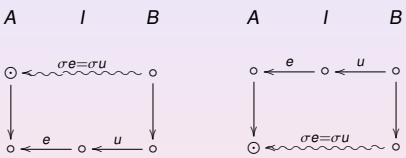
Bob announces his public key



- $e, \sigma e \in \Gamma_A$
- $A :\ B$ honest $\implies \exists u.\ \sigma u = \sigma e \wedge \langle B$ to $A : u \rangle_B$

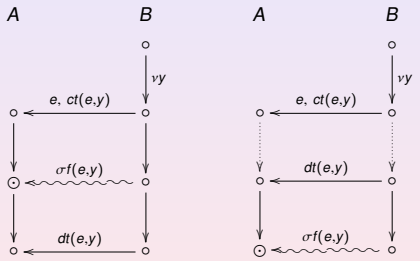
Socially authenticated key distribution

. . . but Ivan may have replaced it

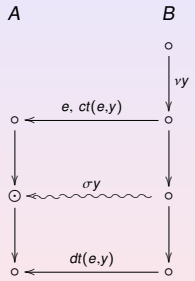


- $e, \sigma e \in \Gamma_A$
- $A :\ B$ honest $\implies \exists u.\ \sigma u = \sigma e \wedge \langle B$ to $A : u \rangle_B$

Social commitment

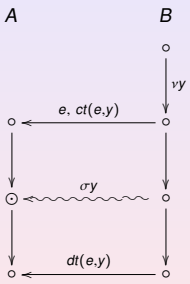


Authentication before decommitment



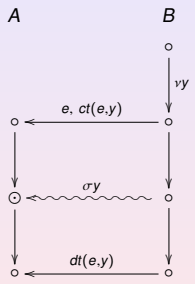
- $A:\ \exists y.\ \sigma y = s \wedge \lessdot B \text{ to } A : s \gtrdot_B$

Authentication before decommitment



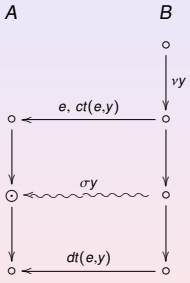
- $A:\ B \text{ honest} \Longrightarrow \exists y.\ \lessdot B \text{ to } A : \sigma y \gtrdot_B$

Authentication before decommitment



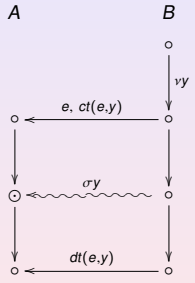
- $A:\ B \text{ honest} \Longrightarrow \exists u \exists y.\ \langle u, ct(u,y)\rangle_B \trianglerighteq \lessdot \sigma y \gtrdot_B$

Authentication before decommitment



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

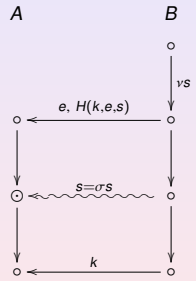
Authentication before decommitment



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

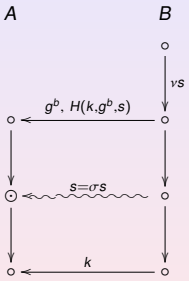
Authentication before decommitment

Wong-Stajano template



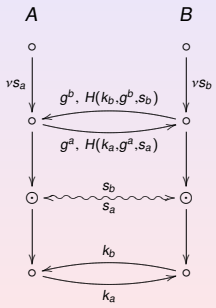
Authentication before decommitment

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



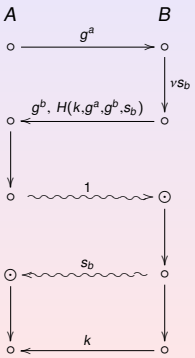
Authentication before decommitment

Wong-Stajano

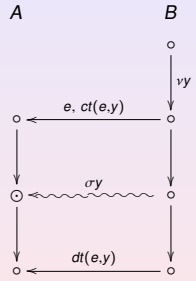


Authentication before decommitment

Wong-Stajano 3



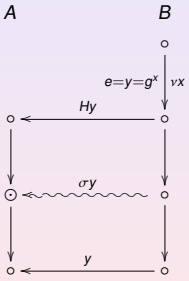
Authentication before decommitment



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

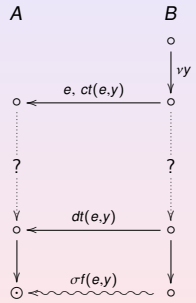
Authentication before decommitment

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

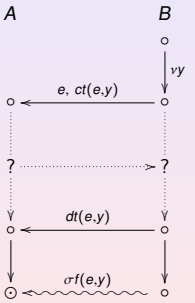


- $A:\ B$ honest $\Longrightarrow (\nu x)_B \trianglerighteq \langle H(g^x)\rangle_B \trianglerighteq \ll\sigma(g^x)\gg_B \trianglerighteq \langle g^x\rangle_B$

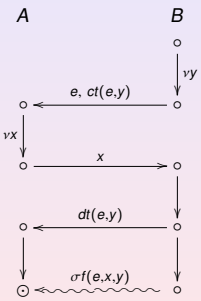
Authentication after decommitment



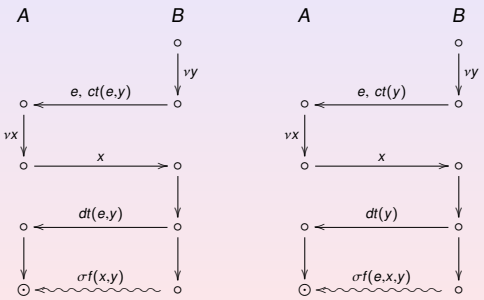
Authentication after decommitment



Authentication after decommitment

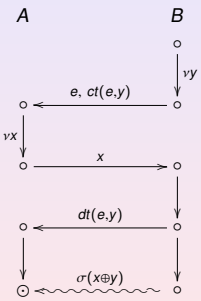


Authentication after decommitment



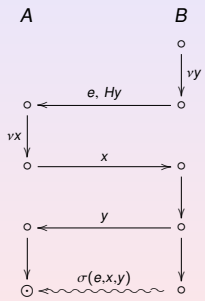
Authentication after decommitment

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



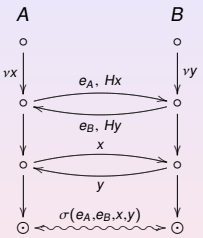
Authentication after decommitment

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



Mutual authentication after decommitment

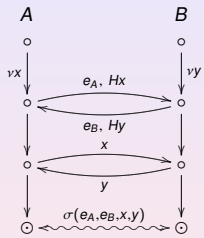
Nguyen-Roscoe: HCBK (2-party)



Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)



Assumption: Initiator establishes the order

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)

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

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

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Multi-party authentication after decommitment

Nguyen-Roscoe: HCBK

Assumptions (to be discharged)

- agreed ordering of the principals

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

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

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Multi-party authentication after decommitment

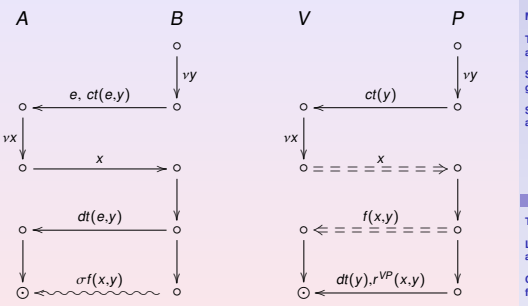
Nguyen-Roscoe: HCBK

Assumptions (to be discharged)

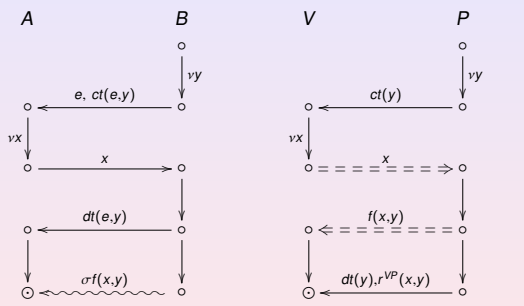
- agreed ordering of the principals
  - all principals must digest at the same payload
- social protocol to compare the digests

Pervasive authentication
Dusko Pavlovic
Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

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
Model of network computation
Authentication with timed channels
Symbolic model with partial information and guessing
Authentication with social channels
Trust & reputation
Deriving location authentication protocols
Conclusions and future work

Trust and reputation

NOT PRESENTED

Outline

Introduction
Model of network computation
Authentication with timed channels
Symbolic model with partial information and guessing
Authentication with social channels
Trust & reputation
Deriving location authentication protocols
Conclusions and future work

Deriving location authetication: Mobile IP

NOT PRESENTED

Outline

Introduction

Model of network computation

Authentication with timed channels

Symbolic model with partial information and guessing

Authentication with social channels

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Summary

Conclusions

- space security for pervasive and social computation
  - E2E model does not suffice

Pervasive authentication

Dusko Pavlovic

Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Summary

Conclusions

- space security for pervasive and social computation
  - E2E model does not suffice
- bootstrap distance, proximity, routing. . .

Pervasive authentication

Dusko Pavlovic

Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Summary

Conclusions

- space security for pervasive and social computation
  - E2E model does not suffice
- bootstrap distance, proximity, routing. . .
  - derivational approach *sine qua non*

Pervasive authentication

Dusko Pavlovic

Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Summary

Conclusions

- space security for pervasive and social computation
  - E2E model does not suffice
- bootstrap distance, proximity, routing. . .
  - derivational approach *sine qua non*

Future work

- embed Social Web 2.0 in physical space
  - enable the export of authenticated social links
  - make the Web into a social channel
- **electronic pheromones**

Pervasive authentication

Dusko Pavlovic

Introduction
Model
Timed authentication
Symbolic guessing
Social authentication
Trust & reputation
Location authentication
Conclusions and future work