NFC and authentication in pervasive and social computation

Dusko Pavlovic

Kestrel Institute
and
Oxford University

January 2008

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols

Deriving social authentication protocols

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Outline

Introduction: NFC and pervasive security

Near Field Communication

Problems of pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols

Deriving social authentication protocols

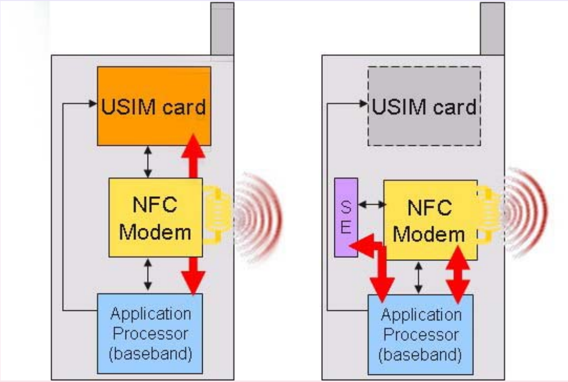
Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Near Field Communication (NFC)

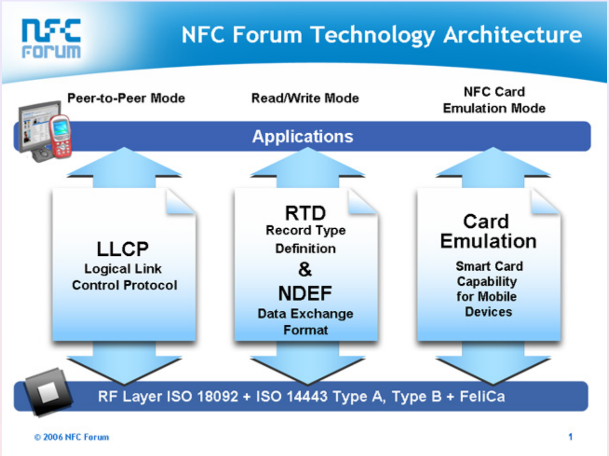
Phone with a contactless smart card:



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

Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

NFC modes of operation: standards



Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

NFC stakeholders

- mobile operators:

  pro: revenue from card issuers, targeted advertising, social networking

  con: no revenue from P2P transactions[1]

- card issuers:

  pro: increased availability and overall transaction value,

  con: dependency on mobile operators

- banks:

  pro: increased availability and overall transaction value

  con: lost revenue to P2P digital cash transactions

[1] cf. Bluetooth disabling

NFC deployment

Australia:	Telstra, National Australia Bank
China:	China Mobile, Philips, Nokia, Xiamen e-Tong card
France:	CIC, Credit Mutuel, Gemalto, LaSer, Pegasus (multi-operator, multi-bank, multi-card), RATP, SFR
Germany:	Deutsche Bahn, Rhein-Main Vb (Frankfurt), Nokia, Philips, Vodafone
India:	Delta Technologies
Japan:	DoCoMo
UK:	Barklays, Orange, O2, TfL Oyster, Wireless Fest in Hyde Park
USA:	Cingular, Discover, Inside Contactless, Nokia, NXP, NY subway, Venyon ZTar,

NFC applications

Contactless payment and exchange

- card mode (← Chip & Pin, EMV)

  2008 transaction value: $ 2.4 billion (Juniper)

  2011 transaction value: $ 24-36 billion (Juniper, Strategy Analytics)
- RW mode:
  - electronic tickets, transportation systems
  - off-line micropayments (← Chip-Knip)
- P2P mode:
  - digital cash transactions
  - electronic barter
  - street markets and transient merchants
  - vending

NFC applications

Proximity commercial networking

- RW mode: RFID-based shopping
  - discount coupons, mobile rewards distribution
  - warehouse navigation
  - dynamic pricing
    - shop auction
    - shopping derivatives: futures, calls, boolean betting. . .
    - discount for social hubs, celebrities
    - discount for viral marketing, C2C assistance, shop help
  - general shopping assistance

NFC applications

Proximity commercial networking

- RW mode: RFID-based shopping
  - discount coupons, mobile rewards distribution
  - warehouse navigation
  - dynamic pricing
    - shop auction
    - shopping derivatives: futures, calls, boolean betting...
    - discount for social hubs, celebrities
    - discount for viral marketing, C2C assistance, shop help
  - general shopping assistance
- RW mode: bootstrap other networks
  - distribute relevant URLs
  - establish Bluetooth, WLAN connections to local resources

NFC applications

Proximity social networking

Beyond address book:

- P2P mode: support local networks
  - exchange public keys, personal (business) cards

[2] e.g., a fragment of a personal page, reputation certificate, "electronic pheromone"

NFC applications

Proximity social networking

Beyond address book:

- P2P mode: support local networks
  - exchange public keys, personal (business) cards
- RW mode: generate local networks
  - check in selected personal data[2] at a smart place
    - club, school, shopping mall. . .
  - local recommender system forms clusters
    - sport partners, homework help, one-night stands. . .
    - queryless social search
    - social navigation assistance: friends, foes, fashion. . .

[2] e.g., a fragment of a personal page, reputation certificate, "electronic pheromone"

Introduction: NFC

NFC perspective

Pervasive security problems

Deriving authentication

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

NFC applications

Proximity social networking

Beyond address book:

- P2P mode: support local networks
  - exchange public keys, personal (business) cards
- RW mode: generate local networks
  - check in selected personal data[2] at a smart place
    - club, school, shopping mall. . .
  - local recommender system forms clusters
    - sport partners, homework help, one-night stands. . .
    - queryless social search
    - social navigation assistance: friends, foes, fashion. . .
  - receive other *relevant* information
    - *recommendation driven* advertising in physical space

[2] e.g., a fragment of a personal page, reputation certificate, "electronic pheromone"

NFC applications

Proximity social networking

Beyond address book:

- P2P mode: support local networks
  - exchange public keys, personal (business) cards
- RW mode: generate local networks
  - check in selected personal data[2] at a smart place
    - club, school, shopping mall. . .
  - local recommender system forms clusters
    - sport partners, homework help, one-night stands. . .
    - queryless social search
    - social navigation assistance: friends, foes, fashion. . .
  - receive other *relevant* information
    - *recommendation driven* advertising in physical space
  - point-and-click
    - drag one proximity link to another: introduce friends
    - bootstrap Bluetooth, WLAN networks: "silent concert"
    - . . . (mouse in space)

[2] e.g., a fragment of a personal page, reputation certificate, "electronic pheromone"

Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Security problems

"On the Internet, nobody knows you're a dog."

Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC
- NFC perspective
- Pervasive security problems

Deriving authentication

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

NFC applications

Proximity social networking

Task.

Study authentication methods for

- proximity social networking, in particular, and

NFC applications

Proximity social networking

Task.

Study authentication methods for

- proximity social networking, in particular, and
- pervasive computation in general

NFC applications

Proximity social networking

Task.

Study authentication methods for

- proximity social networking, in particular, and
- pervasive computation in general

Method.

Derivational approach:

- taxonomy of channels and of their applications
- incremental analysis of channel interactions
- protocol patterns
- tool support

Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

New security landscape

Example 1: Fair exchange (contract signing)

Theorem (Even-Yacobi, 1980)

Every deterministic fair exchange protocol must involve a trusted third party: it is always an escrow protocol.

New security landscape

Example 1: Fair exchange (contract signing)

Theorem (Even-Yacobi, 1980)

Every deterministic fair exchange protocol must involve a trusted third party: it is always an escrow protocol.

Why?

Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

New security landscape

Example 1: Fair exchange (contract signing)

Theorem (Even-Yacobi, 1980)

Every deterministic fair exchange protocol must involve a trusted third party: it is always an escrow protocol.

Why?

Exchange is like a race where the winning horse is the **last** to finish.

New security landscape

Example 1: Fair exchange (contract signing)

Pervasive solution

Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

New security landscape

Example 1: Fair exchange (contract signing)

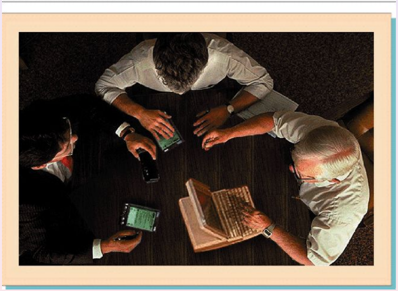
Pervasive solution

Swap the horses!

Pervasive solution

Swap the horses!

Figure 1 Design session in a mediated space

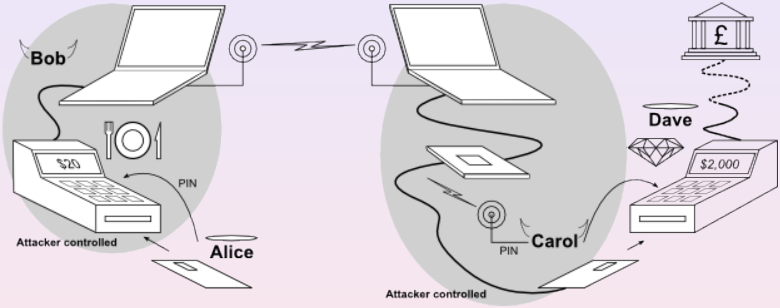


. . . i.e. swap the devices, or the send buttons.

Pervasive authentication protocols
Dusko Pavlovic
Introduction: NFC
NFC perspective
Pervasive security problems
Deriving authentication
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

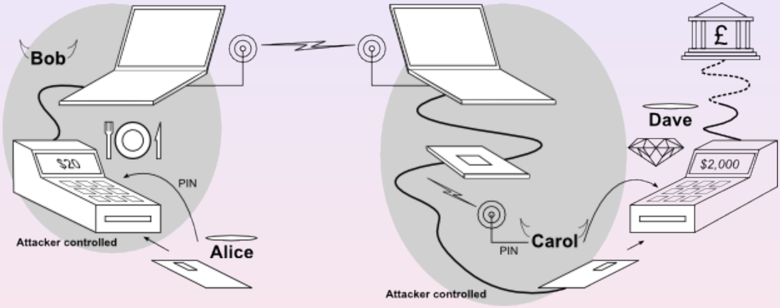
New security landscape

Example 2: Smart card relay attacks



New security landscape

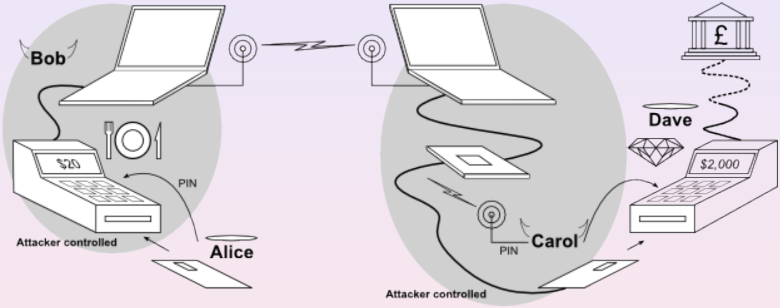
Example 2: Smart card relay attacks



This becomes much easier with NFC phones!

New security landscape

Example 2: Smart card relay attacks



This becomes much easier with NFC phones!

Solution: distance bounding,
social authentication (sign receipt)

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation
- Basic ideas
- Deriving challenge-response
- Real example: GDOI

Deriving distance bounding authentication protocols

Deriving social authentication protocols

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Basics of information flow security

Secrecy: bad information flows do not happen

Authenticity: good information flows do happen

Basics of program dependability

Safety: bad things do not happen

Liveness: good things do happen

Basics of information flow security

Secrets must be authenticated

Authentications are based on secrets

Introduction: NFC

Deriving authentication

Basics

Challenge-response

Real example: GDOI

Timed authentication

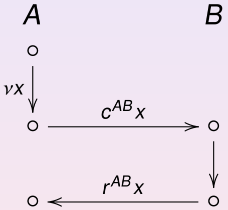
Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Authentication by challenge-response (CR)



Introduction: NFC

Deriving authentication
- Basics
- Challenge-response
- Real example: GDOI

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Authentication by challenge-response (CR)

$$
\begin{tikzcd}
A & B \\
\circ \arrow[d, "\nu x"'] & \\
\circ \arrow[r, "c^{AB}x"] & \circ \arrow[d] \\
\circ & \circ \arrow[l, "r^{AB}x"']
\end{tikzcd}
$$

$$
\begin{aligned}
A \; : \; (\nu x)_A \Big(\langle\langle c^{AB}x \rangle\rangle_A \quad & \rhd \quad ((r^{AB}x))_A \\
\Longrightarrow \; \langle\langle c^{AB}x \rangle\rangle_A \rhd ((c^{AB}x))_B \rhd \langle\langle r^{AB}x \rangle\rangle_{B\rhd} & \rhd ((r^{AB}x))_A \Big) \qquad \text{(cr)}
\end{aligned}
$$

Introduction: NFC

Deriving authentication
- Basics
- Challenge-response
- Real example: GDOI

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Signature-based challenge-response (CRS)

$$
\begin{tikzcd}
A & B \\
\circ \arrow[d, "\nu x"'] & \\
\circ \arrow[r, "c^{AB} x{:=}x"] & \circ \arrow[d] \\
\circ & \circ \arrow[l, "r^{AB} x{:=}S^B x"']
\end{tikzcd}
$$

$$S^B t = S^B u \quad \Longrightarrow \quad t = u \qquad \text{(sig1)}$$

$$V^B(y, t) \quad \Longleftrightarrow \quad y = S^B t \qquad \text{(sig2)}$$

$$\langle\langle S^B t \rangle\rangle_{X\triangleright} \quad \Longrightarrow \quad X = B \qquad \text{(sig3)}$$

Introduction: NFC

Deriving authentication
- Basics
- Challenge-response
- Real example: GDOI

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Signature-based challenge-response (CRS)

$$
\begin{tikzcd}
A & B \\
\circ \arrow[d, "\nu x"'] & \\
\circ \arrow[r, "x"] & \circ \arrow[d] \\
\circ & \circ \arrow[l, "S^B x"']
\end{tikzcd}
$$

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

Introduction: NFC
Deriving authentication
Basics
Challenge-response
Real example: GDOI
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Intruder-in-the-Middle attack on CRS

$$
\begin{tikzcd}
A & I & B \\
\circ \arrow[d, "\nu x"'] & & \\
\circ \arrow[r, "A \text{ to } B{:}x"] & \circ \arrow[r, "I \text{ to } B{:}x"] & \circ \arrow[d] \\
\circ & \circ \arrow[l, "B \text{ to } A{:}S^B x"'] & \circ \arrow[l, "B \text{ to } I{:}S^B x"']
\end{tikzcd}
$$

Introduction: NFC

Deriving authentication
Basics
Challenge-response
Real example: GDOI

Timed authentication

Social authentication

Trust & reputation

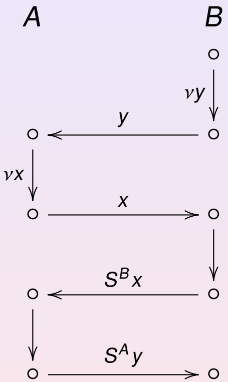
Location authentication

Conclusions and future work

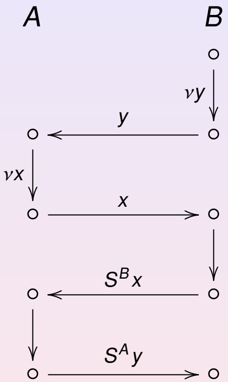
Signature-based challenge-response (CRS)

$$\begin{tikzcd}
A & B \\
\circ \arrow[d, "\nu x"'] & \\
\circ \arrow[r, "x"] & \circ \arrow[d] \\
\circ & \circ \arrow[l, "S^B x"']
\end{tikzcd}$$

Signature-based **nested** challenge-response (CRSN)



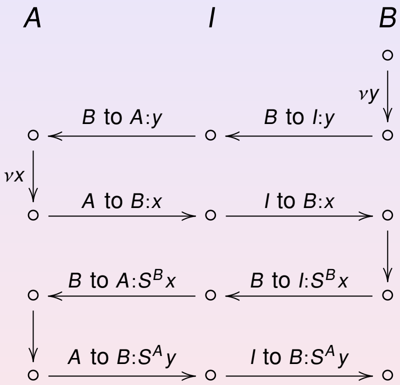
Signature-based **nested** challenge-response (CRSN)



assumptions: (sig1-3), (A honest), (B honest)

guarantee: using (cr) A and B derive matching views

Intruder-in-the-Middle attack on CRSN



Introduction: NFC

Deriving authentication
Basics
Challenge-response
Real example: GDOI

Timed authentication

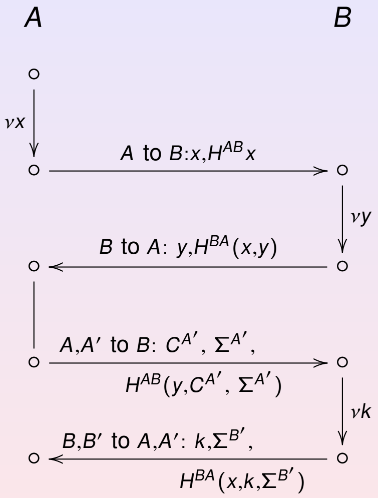
Social authentication

Trust & reputation

Location authentication

Conclusions and future work

IPSec GDOI protocol



$$\Sigma^X = S^X(x,y)$$

Introduction: NFC
Deriving authentication
Basics
Challenge-response
Real example: GDOI
Timed authentication
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Intruder-in-the-middle attack on GDOI

$$
\begin{tikzcd}[column sep=huge]
A & I & B \\
\circ \arrow[d, "\nu x"'] & & \\
\circ \arrow[r, "A \text{ to } I{:} x{,}H^{AI}x"] & \circ \arrow[r, "I \text{ to } B{:}\ x{,}H^{IB}x"] & \circ \arrow[d, "\nu y"] \\
\circ \arrow[d, dash] & \circ \arrow[l, "I \text{ to } A{:}\ y{,}H^{IA}(x{,}y)"'] & \circ \arrow[l, "B \text{ to } I{:}\ y{,}H^{BI}(x{,}y)"'] \\
\circ \arrow[r, "\begin{array}{c} A{,}A' \text{ to } I{:}\ C^{A'},\ \Sigma^{A'}, \\ H^{AI}(y{,}C^{A'},\ \Sigma^{A'}) \end{array}"] & \circ \arrow[r, "\begin{array}{c} I{,}A' \text{ to } B{:}\ C^{A'},\ \Sigma^{A'}, \\ H^{IB}(y{,}C^{A'},\ \Sigma^{A'}) \end{array}"] & \circ \arrow[d, "\nu k"] \\
 & \circ & \circ \arrow[l, "\begin{array}{c} B{,}B' \text{ to } I{,}A'{:}\ k{,}\Sigma^{B'}, \\ H^{BI}(x{,}k{,}\Sigma^{B'}) \end{array}"']
\end{tikzcd}
$$

$$\Sigma^X = S^X(x, y)$$

Introduction: NFC

Deriving authentication

Basics

Challenge-response

Real example: GDOI

Timed authentication

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols
- Timed challenge-response
- Binding timed response and crypto response
- Binding timed response and crypto challenge
- Mixing timed channels

Deriving social authentication protocols

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Timed challenge-response

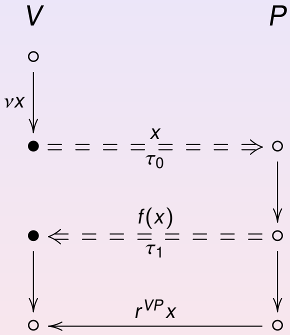
$$
\begin{tikzcd}
V & X \\
\circ \arrow[d, "\nu x"'] & \\
\bullet \arrow[r, Rightarrow, dashed, "x", "\tau_0"'] & \bullet \arrow[d] \\
\bullet & \bullet \arrow[l, Rightarrow, dashed, "f(x)"', "\tau_1"]
\end{tikzcd}
$$

supports the axiom

$$V : \ (\nu x)_V \Big(\tau_0 \langle x \rangle_V \triangleright \tau_1 ((x))_V \Longrightarrow \exists X.\ d(V, X) \le \tau_1 - \tau_0 \Big)$$

Pervasive authentication protocols
Dusko Pavlovic
Introduction: NFC
Deriving authentication
Timed authentication
Timed challenge-response
Timed/crypto response
Timed/crypto challenge
Mixing timed
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Combining timed response and cryptographic response



Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

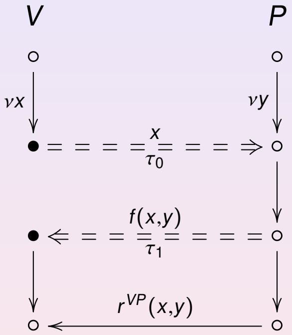
Social authentication

Trust & reputation

Location authentication

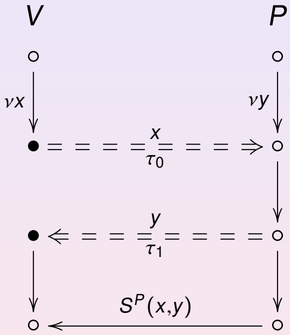
Conclusions and future work

Binding timed response to cryptographic response



Binding timed response to cryptographic response

Brands-Chaum 1



Binding timed response to cryptographic response

Brands-Chaum 1

$$\begin{tikzcd}[column sep=huge]
V & P \\
\circ \arrow[d, "\nu x"'] & \circ \arrow[d, "\nu y"'] \\
\bullet \arrow[r, Rightarrow, dashed, "x", "\tau_0"'] & \circ \arrow[d] \\
\bullet \arrow[d] & \circ \arrow[l, Rightarrow, dashed, "y"', "\tau_1"] \arrow[d] \\
\circ & \circ \arrow[l, "S^P(x{,}y)"']
\end{tikzcd}$$

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

Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

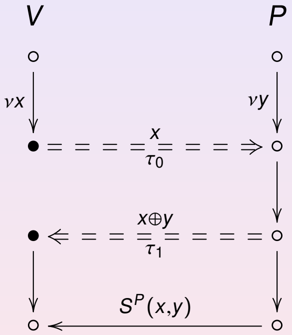
Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

Discharge the honesty assumption?



Introduction: NFC

Deriving authentication

Timed authentication
- Timed challenge-response
- Timed/crypto response
- Timed/crypto challenge
- Mixing timed

Social authentication

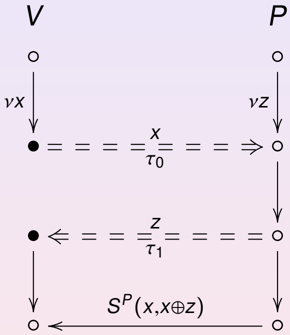
Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

P can still cheat



Introduction: NFC

Deriving authentication

Timed authentication

- Timed challenge-response
- Timed/crypto response
- Timed/crypto challenge
- Mixing timed

Social authentication

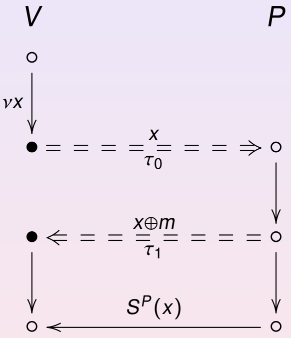
Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

Brands-Chaum 2



Introduction: NFC
Deriving authentication
Timed authentication
Timed challenge-response
Timed/crypto response
Timed/crypto challenge
Mixing timed
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Binding timed response to cryptographic response

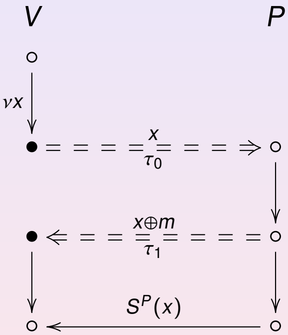
Brands-Chaum 2

$$
\begin{tikzcd}
V & P \\
\circ \arrow[d, "\nu x"'] & \\
\bullet \arrow[r, Rightarrow, dashed, "x", "\tau_0"'] & \circ \arrow[d] \\
\bullet \arrow[d] & \circ \arrow[l, Rightarrow, dashed, "x\oplus m"', "\tau_1"] \arrow[d] \\
\circ & \circ \arrow[l, "S^P(x)"']
\end{tikzcd}
$$

- Peggy cannot cheat

Binding timed response to cryptographic response

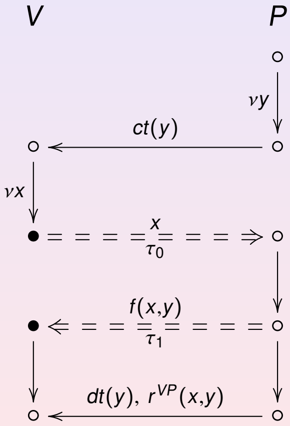
Brands-Chaum 2



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

Binding timed response to cryptographic response

— with commitment



Introduction: NFC

Deriving authentication

Timed authentication

- Timed challenge-response
- Timed/crypto response
- Timed/crypto challenge
- Mixing timed

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

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,
- $ot\,(ct(x), dt(x)) = x$.

Introduction: NFC
Deriving authentication
Timed authentication
Timed challenge-response
Timed/crypto response
Timed/crypto challenge
Mixing timed
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

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.,

$$
\begin{aligned}
ct(x) &= H(x) & \qquad ct(x) &= H_0(x) & \qquad ct(x) &= E(x_0, x_1)\\
dt(x) &= x & dt(x) &= H_1(x)::x & dt(x) &= x_0\\
ot(y,z) &= z & ot(y,z) &= z_1 & ot(y,z) &= D(z,y)
\end{aligned}
$$

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

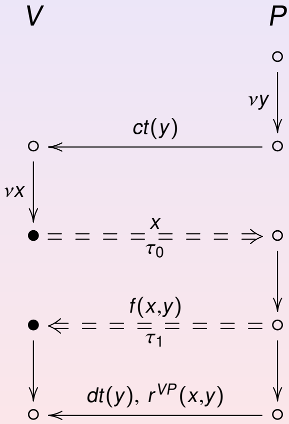
Trust & reputation

Location authentication

Conclusions and future work

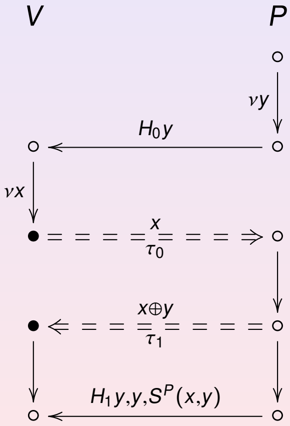
Binding timed response to cryptographic response

— with commitment



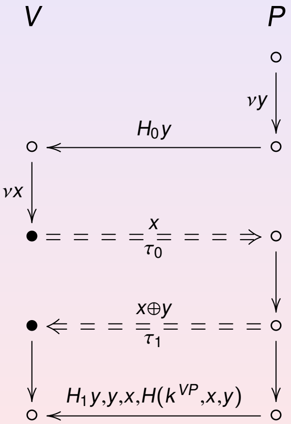
Binding timed response to cryptographic response

Brands-Chaum 3



Binding timed response to cryptographic response

Čapkun-Hubaux



Introduction: NFC

Deriving authentication

Timed authentication

- Timed challenge-response
- Timed/crypto response
- Timed/crypto challenge
- Mixing timed

Social authentication

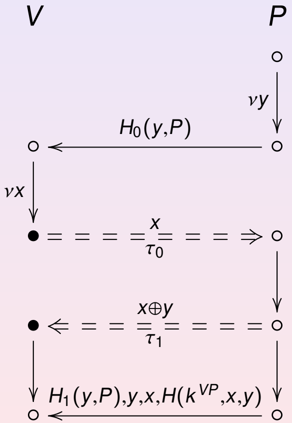
Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

Meadows-Syverson



Introduction: NFC

Deriving authentication

Timed authentication

- Timed challenge-response
- Timed/crypto response
- Timed/crypto challenge
- Mixing timed

Social authentication

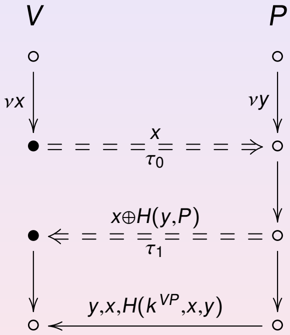
Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

Meadows-P-Syverson



Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

Meadows-P-Syverson

$$
\begin{tikzcd}
V & & P \\
\circ \arrow[d, "\nu x"'] & & \circ \arrow[d, "\nu y"] \\
\bullet \arrow[rr, Rightarrow, dashed, "x", "\tau_0"'] & & \circ \arrow[d] \\
\bullet \arrow[d] & & \circ \arrow[ll, Rightarrow, dashed, "x\oplus H(y,P)"', "\tau_1"] \arrow[d] \\
\circ & & \circ \arrow[ll, "{y,x,H(k^{VP},x,y)}"']
\end{tikzcd}
$$

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

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

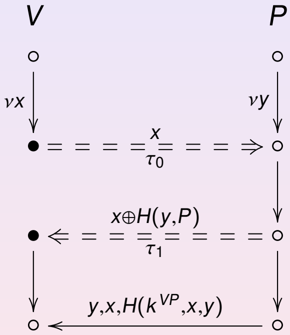
Trust & reputation

Location authentication

Conclusions and future work

Binding timed response to cryptographic response

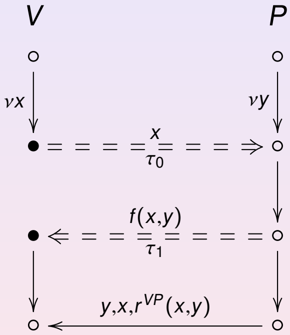
Meadows-P-Syverson



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

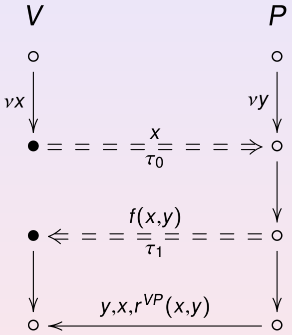
Binding timed response to cryptographic response

. . . and in general



Binding timed response to cryptographic response

. . . and in general



- $f(x, y)$ one-way function in y
- only P could generate $r^{VP}(x, y)$.

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

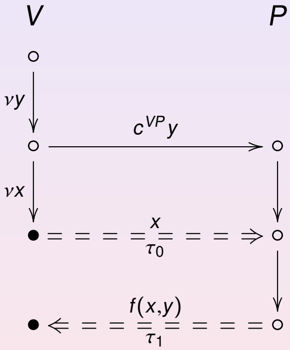
Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Binding timed response and cryptographic **challenge**



Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

Trust & reputation

Location authentication

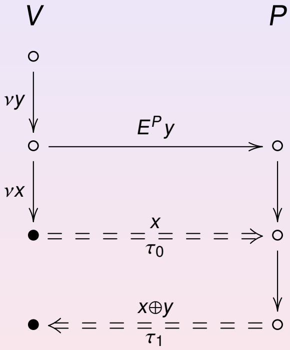
Conclusions and future work

Binding timed response and cryptographic **challenge**

$$
\begin{tikzcd}
V & P \\
\circ \arrow[d, "\nu y"'] & \\
\circ \arrow[r, "c^{VP}y"] \arrow[d, "\nu x"'] & \circ \arrow[d] \\
\bullet \arrow[r, Rightarrow, dashed, "x", "\tau_0"'] & \circ \arrow[d] \\
\bullet & \circ \arrow[l, Rightarrow, dashed, "f(x,y)"', "\tau_1"]
\end{tikzcd}
$$

(more convenient when P is a smart card)

Binding timed response and cryptographic challenge

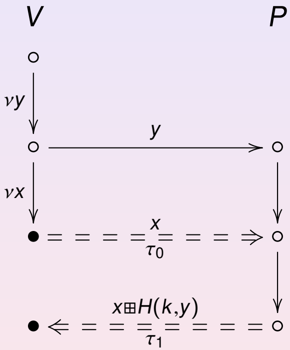


(if P has a public key)

Introduction: NFC
Deriving authentication
Timed authentication
Timed challenge-response
Timed/crypto response
Timed/crypto challenge
Mixing timed
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Binding timed response to cryptographic challenge

Hancke-Kuhn



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

Introduction: NFC

Deriving authentication

Timed authentication

- Timed challenge-response
- Timed/crypto response
- Timed/crypto challenge
- Mixing timed

Social authentication

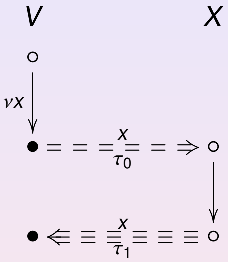
Trust & reputation

Location authentication

Conclusions and future work

Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner



Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

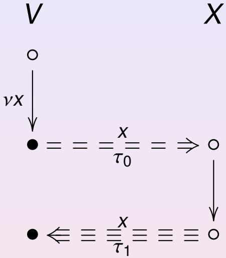
Trust & reputation

Location authentication

Conclusions and future work

Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner



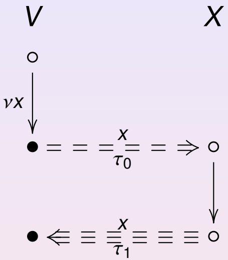
$$V:\ (\nu x)_V\Big(\tau_0\langle\langle x\rangle\rangle_V \triangleright \tau_1((x))_V \Longrightarrow \exists X.\ d(V,X) \le (\tau_1-\tau_0)\frac{c+s}{cs}\Big)$$

- where c is the speed of light and s the speed of sound

Pervasive authentication protocols
Dusko Pavlovic
Introduction: NFC
Deriving authentication
Timed authentication
Timed challenge-response
Timed/crypto response
Timed/crypto challenge
Mixing timed
Social authentication
Trust & reputation
Location authentication
Conclusions and future work

Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner



$$V: \ (\nu x)_V \left(\tau_0 \langle\langle x \rangle\rangle_V \triangleright \tau_1 ((x))_V \Longrightarrow \exists X.\ d(V,X) \leq (\tau_1 - \tau_0) \frac{c+s}{cs} \right)$$

- where c is the speed of light and s the speed of sound
- the reasoning boils down to (crt)), because $s \ll c \Longrightarrow \frac{c+s}{cs} \approx 1$

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

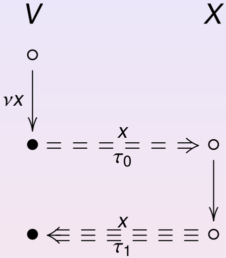
Trust & reputation

Location authentication

Conclusions and future work

Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner



$$V : \; (\nu x)_V \left(\tau_0 \langle\langle x \rangle\rangle_V \triangleright \tau_1 ((x))_V \Longrightarrow \exists X.\; d(V, X) \leq (\tau_1 - \tau_0) \frac{c+s}{cs} \right)$$

- where c is the speed of light and s the speed of sound
- the reasoning boils down to (crt)), because $s \ll c \implies \frac{c+s}{cs} \approx 1$
- **pro:** measuring longer response times requires less precision
- **con:** s less robust, due to the influences of the environment

Introduction: NFC

Deriving authentication

Timed authentication

Timed challenge-response

Timed/crypto response

Timed/crypto challenge

Mixing timed

Social authentication

Trust & reputation

Location authentication

Conclusions and future work

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols

Deriving social authentication protocols

- Social channel and its use
- Social commitment
- Authentication before decommitment
- Authentication after decommitment
- Socially authenticated key exchange
- Security homology

Trust & reputation

Deriving location authentication protocols

Preliminary example: a timed social protocol

$$\begin{tikzcd}
A & B \\
\bullet \arrow[r, Rightarrow, dashed, "m", "\tau_0"'] & \circ \arrow[d] \\
\odot & (m) \arrow[l, squiggly, "\tau_1"]
\end{tikzcd}$$

Introduction: NFC
Deriving authentication
Timed authentication
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

Introduction: NFC

Deriving authentication

Timed authentication

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."

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."

Introduction: NFC

Deriving authentication

Timed authentication

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 $A : \beta \gtrdot$ — B shows an action β to A

Introduction: NFC

Deriving authentication

Timed authentication

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 $A : \beta \gtrdot$ — B shows an action β to A

axiomatized as follows:

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

Social actions

- $\lessdot B$ to $A : \beta\gtrdot$ — B shows an action β to A

axiomatized as follows:

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

Introduction: NFC

Deriving authentication

Timed authentication

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

Introduction: NFC

Deriving authentication

Timed authentication

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

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

axiomatized as follows:

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

Introduction: NFC

Deriving authentication

Timed authentication

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

Graphic notation

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

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

Social channel and its use

Social commitment

Auth. then decommit

Decommit then auth.

Social KE

Security homology

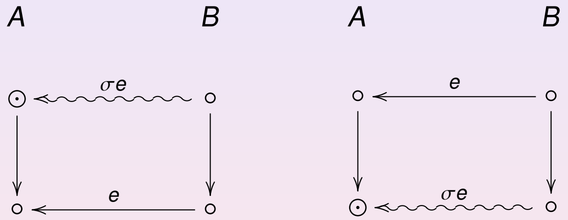
Trust & reputation

Location authentication

Conclusions and future work

Socially authenticated key distribution

Bob announces his public key



Introduction: NFC

Deriving authentication

Timed authentication

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

Socially authenticated key distribution

Bob announces his public key

$$\begin{tikzcd}[column sep=huge, row sep=huge]
A & B \\
\odot & \circ \arrow[l, squiggly, "\sigma e"'] \\
\circ \arrow[from=2-1, d] & \circ \arrow[from=2-2, d] \arrow[l, "e"']
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=huge, row sep=huge]
A & B \\
\circ & \circ \arrow[l, "e"'] \\
\odot \arrow[from=2-1, d] & \circ \arrow[from=2-2, d] \arrow[l, squiggly, "\sigma e"']
\end{tikzcd}$$

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

Introduction: NFC

Deriving authentication

Timed authentication

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

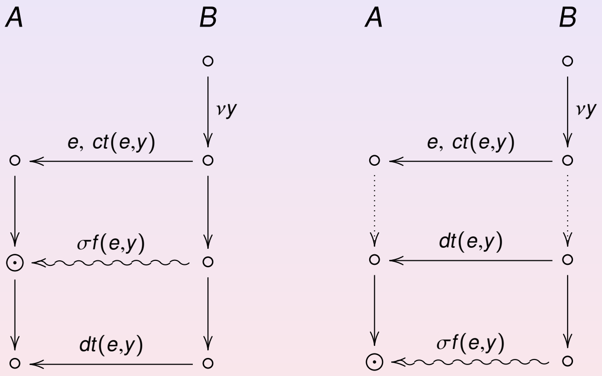
Socially authenticated key distribution

...byt Ivan may have replaced it

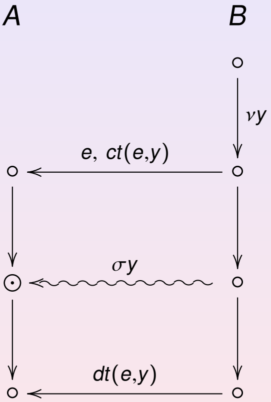
$$
\begin{tikzcd}
A & I & B \\
\odot \arrow[d] & & \circ \arrow[ll, squiggly, "\sigma e{=}\sigma u"'] \arrow[d] \\
\circ & \circ \arrow[l, "e"'] & \circ \arrow[l, "u"']
\end{tikzcd}
\qquad
\begin{tikzcd}
A & I & B \\
\circ \arrow[d] & \circ \arrow[l, "e"'] & \circ \arrow[l, "u"'] \arrow[d] \\
\odot & & \circ \arrow[ll, squiggly, "\sigma e{=}\sigma u"']
\end{tikzcd}
$$

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

Social commitment

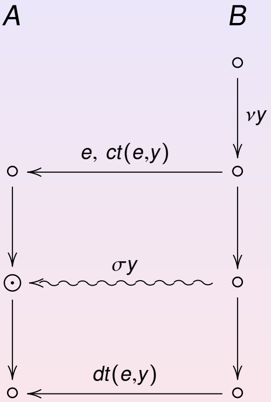


Authentication before decommitment



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

Authentication before decommitment



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

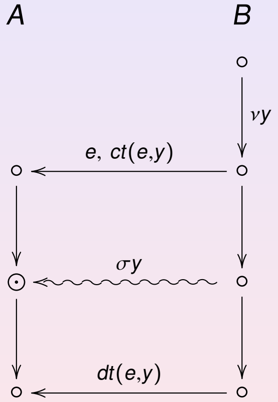
Introduction: NFC
Deriving authentication
Timed authentication
Social authentication
Social channel and its use
Social commitment
Auth. then decommit
Decommit then auth.
Social KE
Security homology
Trust & reputation
Location authentication
Conclusions and future work

Authentication before decommitment

$$
\begin{tikzcd}
A & B \\
& \circ \arrow[d, "\nu y"] \\
\circ \arrow[d] & \circ \arrow[l, "{e,\ ct(e,y)}"'] \arrow[d] \\
\odot \arrow[d] & \circ \arrow[l, squiggly, "\sigma y"'] \arrow[d] \\
\circ & \circ \arrow[l, "dt(e,y)"']
\end{tikzcd}
$$

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

Authentication before decommitment



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

Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

Social channel and its use

Social commitment

Auth. then decommit

Decommit then auth.

Social KE

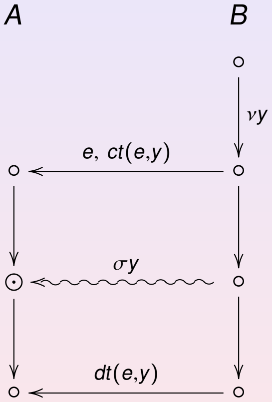
Security homology

Trust & reputation

Location authentication

Conclusions and future work

Authentication before decommitment



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

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication
- Social channel and its use
- Social commitment
- Auth. then decommit
- Decommit then auth.
- Social KE
- Security homology

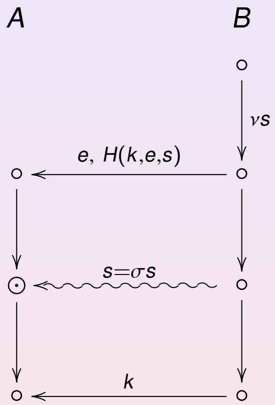
Trust & reputation

Location authentication

Conclusions and future work

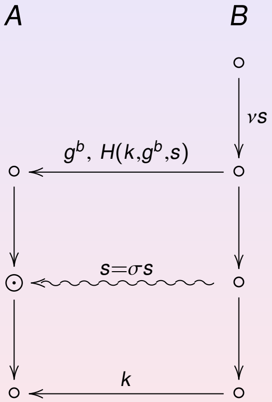
Authentication before decommitment

Wong-Stajano template



Authentication before decommitment

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



Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

- Social channel and its use
- Social commitment
- Auth. then decommit
- Decommit then auth.
- Social KE
- Security homology

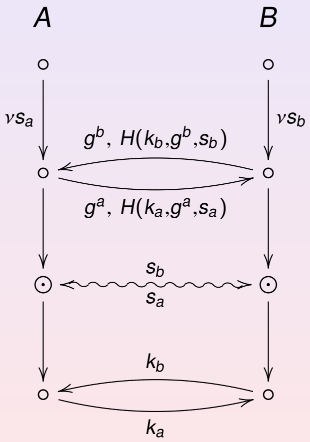
Trust & reputation

Location authentication

Conclusions and future work

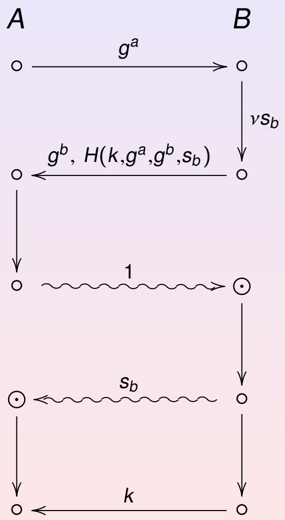
Authentication before decommitment

Wong-Stajano



Authentication before decommitment

Wong-Stajano 3



Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

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

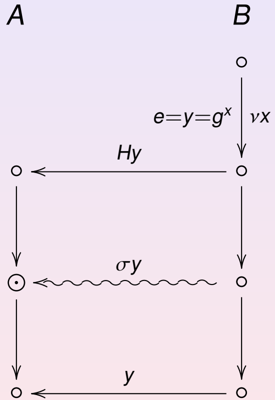
Authentication before decommitment

$$
\begin{tikzcd}
A & B \\
 & \circ \arrow[d, "\nu y"] \\
\circ \arrow[d] & \circ \arrow[l, "{e,\ ct(e,y)}"'] \arrow[d] \\
\odot \arrow[d] & \circ \arrow[l, squiggly, "\sigma y"'] \arrow[d] \\
\circ & \circ \arrow[l, "{dt(e,y)}"']
\end{tikzcd}
$$

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

Authentication before decommitment

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



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

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

Social channel and its use

Social commitment

Auth. then decommit

Decommit then auth.

Social KE

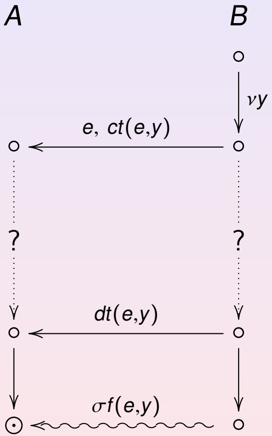
Security homology

Trust & reputation

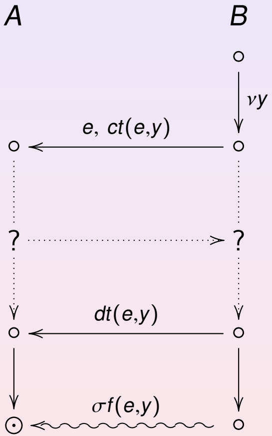
Location authentication

Conclusions and future work

Authentication after decommitment

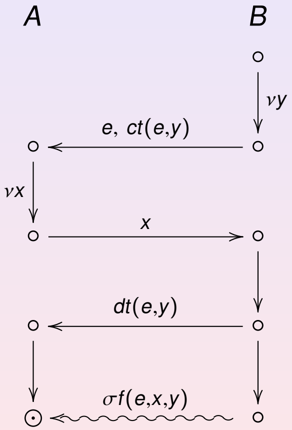


Authentication after decommitment



Introduction: NFC
Deriving authentication
Timed authentication
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

Authentication after decommitment



Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

Social channel and its use

Social commitment

Auth. then decommit

Decommit then auth.

Social KE

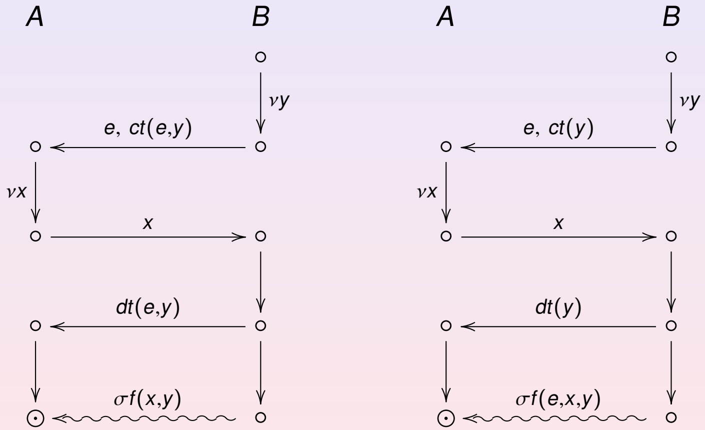
Security homology

Trust & reputation

Location authentication

Conclusions and future work

Authentication after decommitment



Pervasive authentication protocols
Dusko Pavlovic
Introduction: NFC
Deriving authentication
Timed authentication
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

Authentication after decommitment

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

$$
\begin{tikzcd}
A & B \\
 & \circ \arrow[d, "\nu y"] \\
\circ \arrow[d, "\nu x"'] & \circ \arrow[l, "{e,\ ct(e,y)}"'] \\
\circ \arrow[r, "x"] & \circ \arrow[d] \\
\circ \arrow[d] & \circ \arrow[l, "dt(e,y)"'] \arrow[d] \\
\odot & \circ \arrow[l, squiggly, "\sigma(x \oplus y)"']
\end{tikzcd}
$$

Introduction: NFC

Deriving authentication

Timed authentication

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

Authentication after decommitment

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

$$
\begin{tikzcd}
A & B \\
& \circ \arrow[d, "\nu y"] \\
\circ \arrow[d, "\nu x"'] & \circ \arrow[l, "{e,\ Hy}"'] \\
\circ \arrow[r, "x"] & \circ \arrow[d] \\
\circ \arrow[d] & \circ \arrow[l, "y"'] \arrow[d] \\
\odot & \circ \arrow[l, squiggly, "{\sigma(e,x,y)}"']
\end{tikzcd}
$$

Pervasive authentication protocols

Dusko Pavlovic

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication
- Social channel and its use
- Social commitment
- Auth. then decommit
- Decommit then auth.
- Social KE
- Security homology

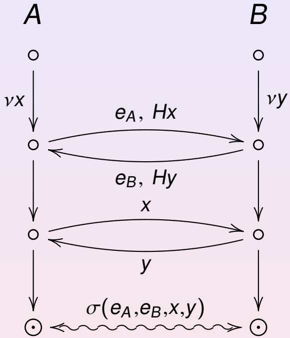
Trust & reputation

Location authentication

Conclusions and future work

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)



Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

- Social channel and its use
- Social commitment
- Auth. then decommit
- Decommit then auth.
- Social KE
- Security homology

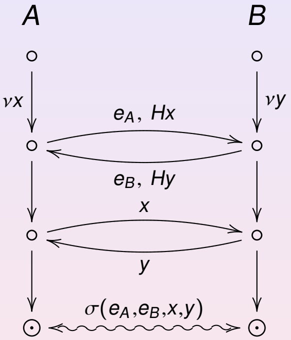
Trust & reputation

Location authentication

Conclusions and future work

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)



Assumption: Initiator establishes the order

Mutual authentication after decommitment

Nguyen-Roscoe: HCBK (2-party)

$$\Big((\nu x)_A \ \langle e_A, Hx\rangle_A \ (u_1, u_2)_A \ \otimes$$

$$(\nu y)_B \ \langle e_B, Hy\rangle_B \ (v_1, v_2)_B\Big) \ ;$$

$$\Big(\langle x\rangle_A \ (u_3)_A \ (u_1, u_2/e_B, Hu_3)_A \ \lessdot \sigma(e_A, e_B, x, u_3) \gtrdot_A \ \otimes$$

$$\langle y\rangle_B \ (v_3)_B \ (v_1, v_2)/e_A, Hv_3)_B \ \lessdot \sigma(e_A, e_B, v_3, y) \gtrdot_B\Big)$$

Multi-party authentication after decommitment

Nguyen-Roscoe: HCBK

Assumptions (to be discharged)

- agreed ordering of the principals

Introduction: NFC

Deriving authentication

Timed authentication

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

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

Introduction: NFC

Deriving authentication

Timed authentication

Social authentication

Social channel and its use

Social commitment

Auth. then decommit

Decommit then auth.

Social KE

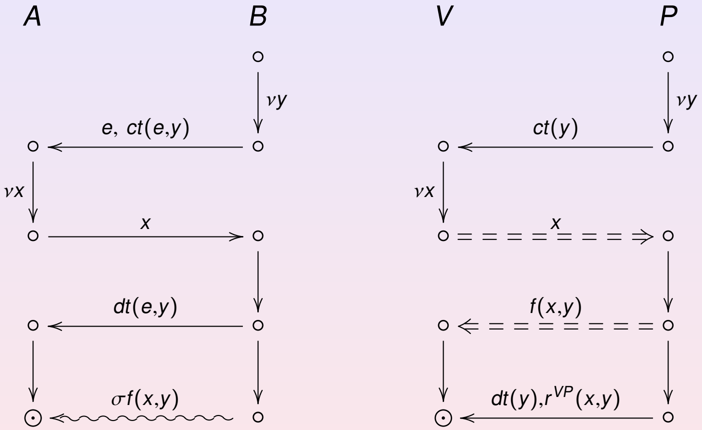
Security homology

Trust & reputation

Location authentication

Conclusions and future work

Structural similarity — conceptual difference



Structural similarity — conceptual difference

$$
\begin{tikzcd}[column sep=huge]
A & B \\
 & \circ \arrow[d, "\nu y"] \\
\circ \arrow[d, "\nu x"'] & \circ \arrow[l, "{e,\ ct(e,y)}"'] \\
\circ \arrow[r, "x"] & \circ \arrow[d] \\
\circ \arrow[d] & \circ \arrow[l, "{dt(e,y)}"'] \arrow[d] \\
\odot & \circ \arrow[l, squiggly, "{\sigma f(x,y)}"']
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=huge]
V & P \\
 & \circ \arrow[d, "\nu y"] \\
\circ \arrow[d, "\nu x"'] & \circ \arrow[l, "{ct(y)}"'] \\
\circ \arrow[r, Rightarrow, dashed, "x"] & \circ \arrow[d] \\
\circ \arrow[d] & \circ \arrow[l, Rightarrow, dashed, "{f(x,y)}"'] \arrow[d] \\
\odot & \circ \arrow[l, "{dt(y), r^{VP}(x,y)}"']
\end{tikzcd}
$$

Social authentication is not challenge-response:

x on the left is not a challenge, but a binder, analogous to y.

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols

Deriving social authentication protocols

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Trust and reputation

NOT PRESENTED

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols

Deriving social authentication protocols

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Deriving location authetication: Mobile IP

NOT PRESENTED

Outline

Introduction: NFC and pervasive security

Derivational approach to authentication and impersonation

Deriving distance bounding authentication protocols

Deriving social authentication protocols

Trust & reputation

Deriving location authentication protocols

Conclusions and future work

Summary

Conclusions

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

Summary

Conclusions

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

Summary

Conclusions

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

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**