Principles of Security — Part 5: Pervasive security Sections 1 and 2

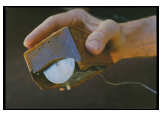
Dusko Pavlovic

Oxford
Michaelmas Term 2008

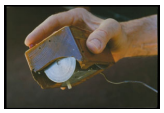
Outline

Outline

Mouse

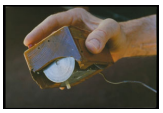


Mouse



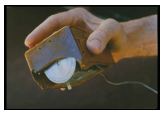
Symbols with which the human represents the concepts can be arranged before his eyes; moved, stored, recalled, operated upon according to extremely complex rules. . .

Mouse



In the limit of what we might now imagine, this could be a computer which could construct sophisticated images in automatic response to human direction. . .

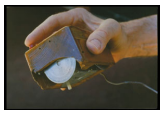
Mouse



. . . and could involve concepts that we have never yet imagined.

Douglas C. Engelbart
Augmenting Human Intellect (1962)

Mouse



Computation as evolution of concepts depends on the human-computer interaction:

- screen
- windows
- icons (objects)
- printouts

The mouse manages real estate of computation.

Computational spaces

Computer in a black box

- 80 character line interface
- input strings and output strings

Computational spaces

Computer in a black box

- 80 character line interface
- input strings and output strings

Computer in a space of interaction

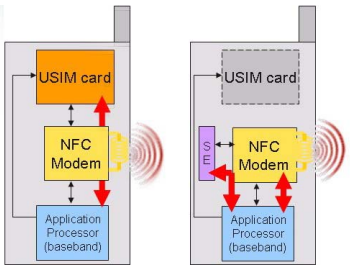
- concepts are symbols, icons, objects
- computation pervades physical space

Pervasive computation

- ubiquitous devices
- programmable environment — disappearing computer
- **computation is coevolution of computational agents**

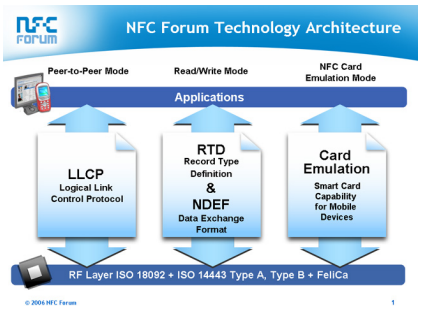
Example: Near Field Communication (NFC)

Phone with a contactless smart card:



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

NFC modes of operation: standards



NFC applications: 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

- 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

- 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 URLs
  - **drag and drop local links**

NFC applications

Proximity social networking: Beyond the address book

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

NFC applications

Proximity social networking: Beyond the address book

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

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

NFC applications

Proximity social networking: Beyond the address book

- P2P mode: support local networks
  - exchange public keys, personal (business) cards
- RW mode: generate local networks
  - check in selected personal data[1] 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. . .

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

NFC applications

Proximity social networking: Beyond the address book

- P2P mode: support local networks
  - exchange public keys, personal (business) cards
- RW mode: generate local networks
  - check in selected personal data[1] 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. . .

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

Security 5: Pervasive
Dusko Pavlovic
Introduction
Pervasive computation
Security landscape
Tools
Timed authentication
Social authentication
Conclusions

NFC applications

Proximity social networking: Beyond the address book

- P2P mode: support local networks
  - exchange public keys, personal (business) cards
- RW mode: generate local networks
  - check in selected personal data[1] 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"

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

Security 5: Pervasive
Dusko Pavlovic
Introduction
Pervasive computation
Security landscape
Tools
Timed authentication
Social authentication
Conclusions

New security capabilities

Theorem (Even-Yacobi, 1980)

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

Security 5: Pervasive
Dusko Pavlovic
Introduction
Pervasive computation
Security landscape
Tools
Timed authentication
Social authentication
Conclusions

New security capabilities

Theorem (Even-Yacobi, 1980)

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

Security 5: Pervasive
Dusko Pavlovic
Introduction
Pervasive computation
Security landscape
Tools
Timed authentication
Social authentication
Conclusions

Why?

New security capabilities

Theorem (Even-Yacobi, 1980)

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

Why?

Security 5: Pervasive
Dusko Pavlovic
Introduction
Pervasive computation
Security landscape
Tools
Timed authentication
Social authentication
Conclusions

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

New security capabilities

Pervasive solution

New security capabilities

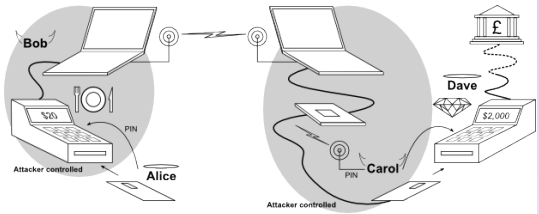
Pervasive solution
Swap the horses!

New security capabilities

Pervasive solution
Swap the horses!

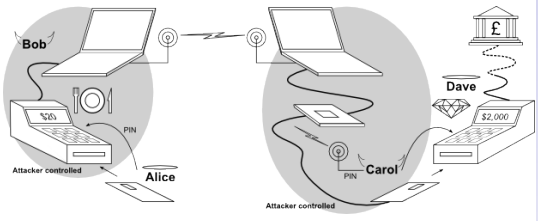
. . . i.e. swap the devices, or the send buttons.

New security problems



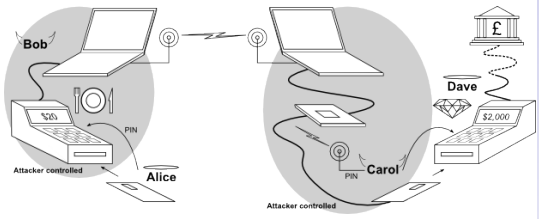
New security problems

The attack requires a long range link.



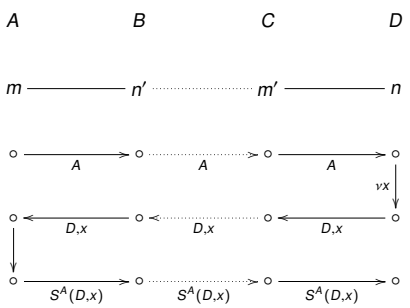
New security problems

The attack requires a long range link.



The NFC phones provide just that!

Agreement is not enough



Summary

Pervasive computation is
- not in cyberspace
  - not distance-free

Summary

Pervasive computation is
- not in cyberspace
  - not distance-free
- but in physical space
  - **principal's position needs to be authenticated**.

Proximity authentication

Degrees of authentication:
- ping authentication: matching records of the messages
- agreement: matching records of intent
- proximity authentication: matching views of the positions

Tools of authentication

You authenticate yourself by leveraging over:

- what you know: secrets, digital keys
- what you have: tokens, smart cards, physical keys
- what you are: biometric properties, handwriting

Tools of authentication

You authenticate yourself by leveraging over:

- what you know: secrets, digital keys
  - can be copied and given away
- what you have: tokens, smart cards, physical keys
  - can be given away, but not copied
- what you are: biometric properties, handwriting
  - cannot be given away, or copied

Tools of authentication

You authenticate yourself by leveraging over:

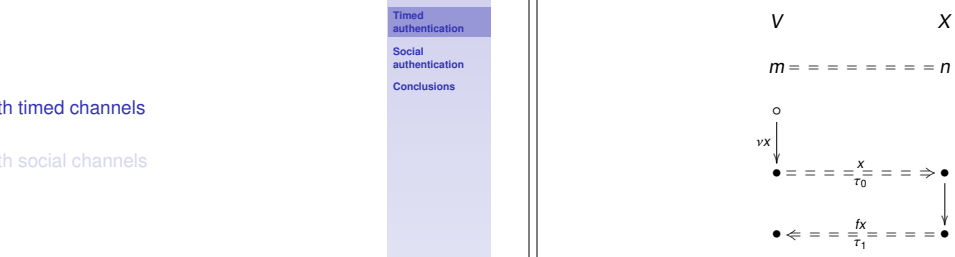
- what you know: secrets, digital keys
  - can be copied and given away
- what you have: tokens, smart cards, physical keys
  - can be given away, but not copied
- what you are: biometric properties, handwriting
  - cannot be given away, or copied

Idea of proximity authentication

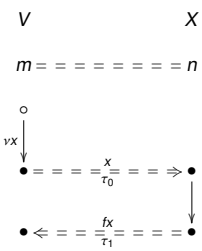
- Most security tokens do not authenticate position directly
- Their physical properties must be used to authenticate position.

Outline

Timed challenge-response



Timed challenge-response



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

Distance bounding protocols

Idea: Combine (cr) and (crt)

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

Distance bounding protocols

Idea: Combine (cr) and (crt)

- 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)

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

Distance bounding protocols

Idea: Combine (cr) and (crt)

- 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

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

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

Distance bounding protocols

Idea: Combine (cr) and (crt)

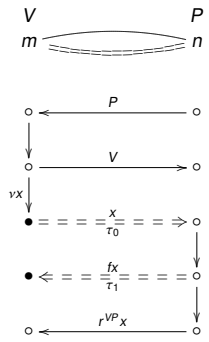
- with **one challenge and two responses**:
  - $r^{VP}x$, satisfying (cr)
  - $f^{VP}x$, satisfying (crt)
- with **two challenges and one response**:
  - $c^{VP}y$ and $fr^{VP}(x,y)$, satisfying (cr)
  - x and $fr^{VP}(x,y)$, satisfying (crt)
- with **one challenge and one response**:
  - x and $fr^{VP}x$,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

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

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

Distance bounding with two responses

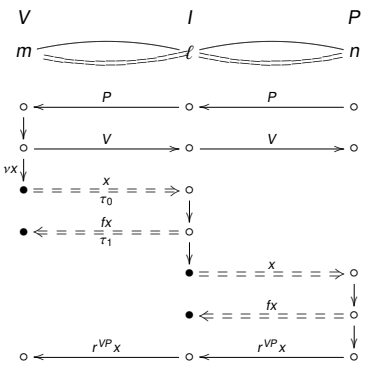
Idea



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

Distance bounding with two responses

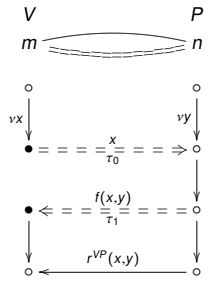
Problem



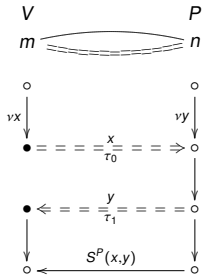
Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions

Distance bounding with two responses

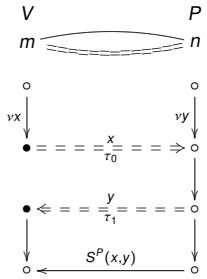
Basic template



Brands-Chaum 1

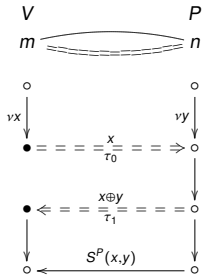


Brands-Chaum 1

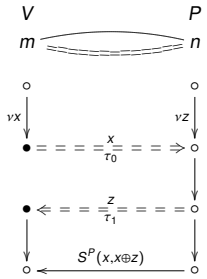


- V : P honest $\Longrightarrow$ $d(V,P) < \tau_1 - \tau_0$
- V : $\forall X.\ X$ responds $\Longrightarrow$ $d(V,X) + d(X,P) < \tau_1 - \tau_0$

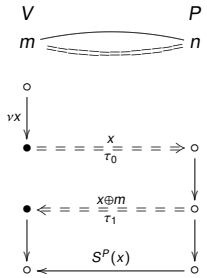
Discharge the honesty assumption?



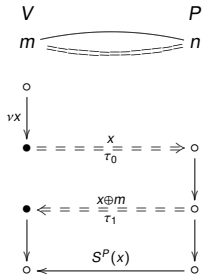
P can still cheat



Brands-Chaum 2

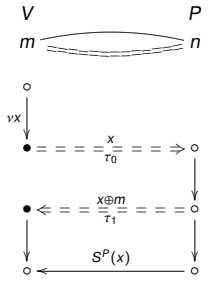


Brands-Chaum 2



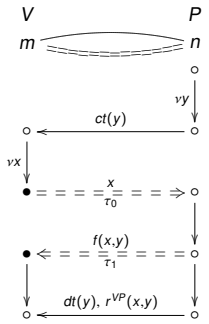
- Peggy cannot cheat

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* over a set of messages $\mathcal{T}$ consists of three publicly known functions

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

Digression: Symbolic commitment

Definition

A *commitment schema* over a set of messages $\mathcal{T}$ consists of three publicly known functions such that

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

Digression: Symbolic commitment

Definition

A *commitment schema* over a set of messages $\mathcal{T}$ consists of three publicly known functions such that

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

Use of commitment

- Alice commits to w by sending $u = ct(w)$.
- Later, Alice decommits by sending $v = dt(w)$.
- Bob verifies that $ct\,(ot(u, v)) = u$.

Digression: Symbolic commitment

Examples

$ct(w) = H(w)$	$ct(w) = H(w)_0$	$ct(w) = E(w_0, w_1)$
$dt(w) = w$	$dt(w) = w::H(w)_1$	$dt(w) = w_0$
$ot(u, v) = v$	$ot(u, v) = v_0$	$ot(u, v) = v::D(v, u)$

Digression: Symbolic commitment

Examples

$$ct(w) = H(w) \qquad ct(w) = H(w)_0 \qquad ct(w) = E(w_0, w_1)$$
$$dt(w) = w \qquad dt(w) = w::H(w)_1 \qquad dt(w) = w_0$$
$$ot(u,v) = v \qquad ot(u,v) = v_0 \qquad ot(u,v) = v::D(v,u)$$

where

- $H : \mathcal{T} \longrightarrow \mathcal{T}$ is a one-way collision free function,
- $(-)_0, (-)_1 : \mathcal{T} \longrightarrow \mathcal{T}$ and $(-::-) : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ satisfy
  - $(u::v)_0 = u$ and $(u::v)_1 = v$
  - $(w_0::w_1) = w$
- $E, D : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ satisfy
  - $E(x, D(x,y)) = y$, and
  - $E(x,-) : \mathcal{T} \longrightarrow \mathcal{T}$ is one-way for all $x \in \mathcal{T}$.

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

Digression: Symbolic commitment

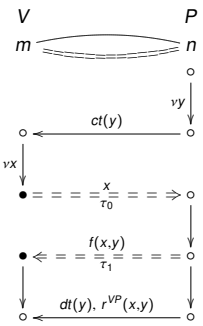
Homework

1. Verify that each of the above triples of functions satisfies the requirements for a commitment schema.
2. Given a projection-pairing system $(-)_0, (-)_1, (-::-)$ as in the preceding slide, set
   - $ct(w) = w_0$
   - $dt(w) = w_1$
   - $ot(u,v) = (u::v)$

   Is this a commitment schema? The other way around, does every commitment schema provide a projection-pairing system?

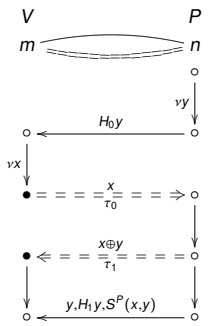
Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions

Solution 1: Commitment



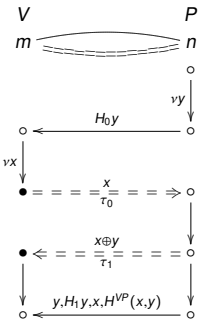
Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions

Brands-Chaum 3



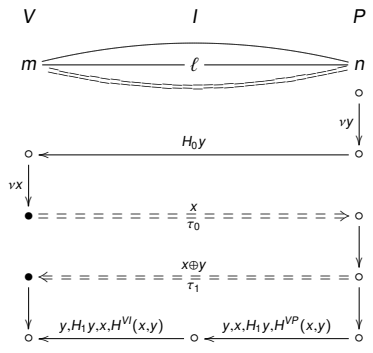
Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions

Čapkun-Hubaux

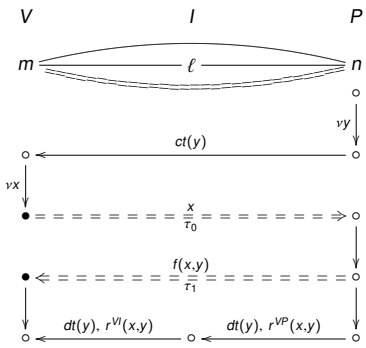


Security 5: Pervasive
Dusko Pavlovic
Introduction
Timed authentication
Social authentication
Conclusions

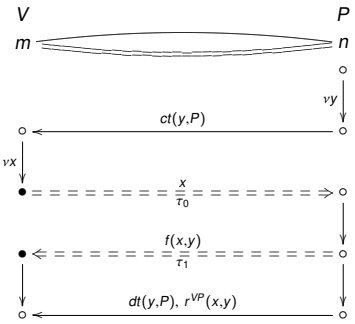
. . . but Peggy's identity can be spoofed



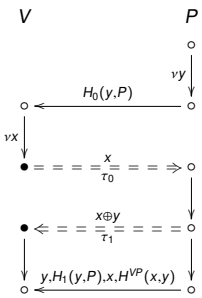
. . . and in general



. . . so we need

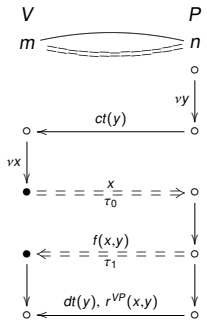


Meadows et al



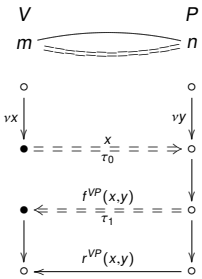
Solution 1: Commitment

This was an implementation of



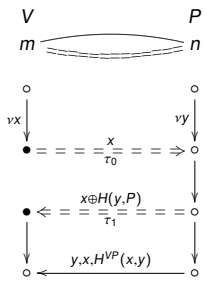
Solution 2: One-way response

Another idea is to commit in the timed response:

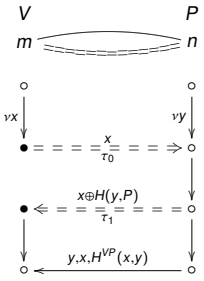


where $f^{VP}(x,-)$ is a one-way function for every x.

Meadows et bo

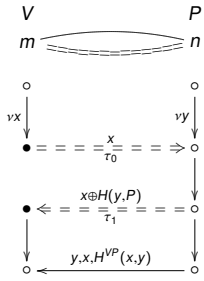


Meadows et bo



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

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 protocols

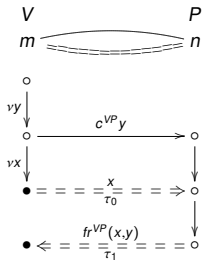
Idea: Combine (cr) and (crt)

- 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

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

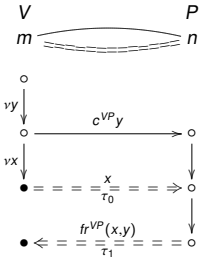
Distance bounding with two challenges

Idea



Distance bounding with two challenges

Idea

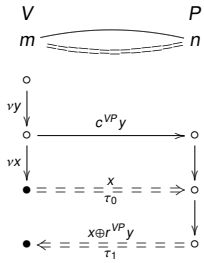


where

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

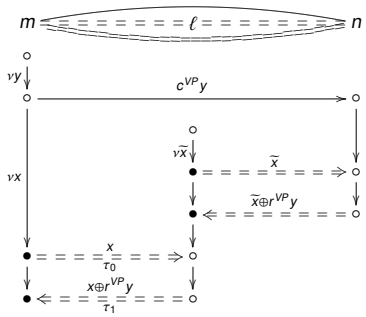
Distance bounding with two challenges

Try



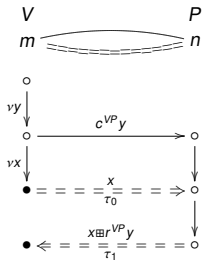
Distance bounding with two challenges

Problem



Distance bounding with two challenges

Idea 2: Find $\boxplus$

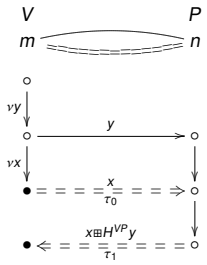


where

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

Hancke-Kuhn

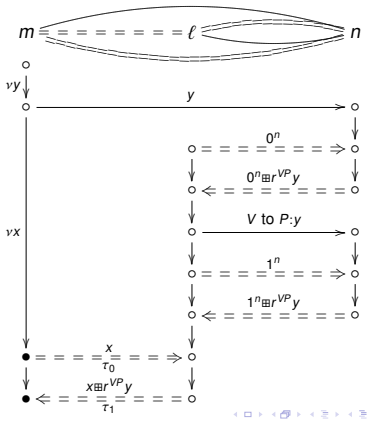
Candidate



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

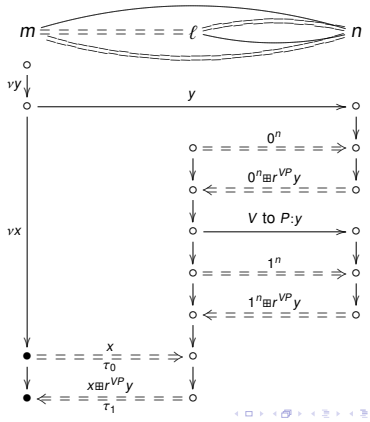
Hancke-Kuhn

Problem



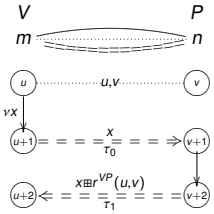
Hancke-Kuhn

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



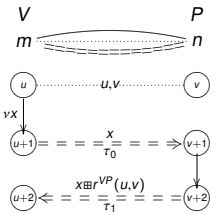
Simple distance bounding template

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



Simple distance bounding template

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

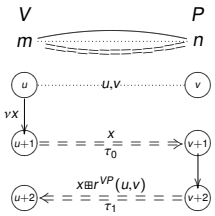


where

- 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

Outline