Bayesian authentication with imperfect cryptography in pervasive networks

Dusko Pavlovic
(in ongoing collaboration with Cathy Meadows)

June 2009

Outline

Problem of proximity authentication

Flavours of authentication

Proving proximity authentication

Conclusions and ongoing work

EMV payment system

Figure: Chip & Pin authentication

Problem

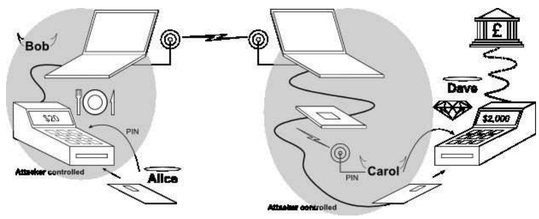


Figure: Smart card relay attack [Anderson et al.]

Problem

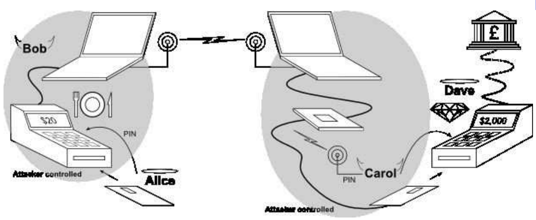


Figure: Smart card relay attack [Anderson et al.]

This will become much easier with NFC phones!

Problem

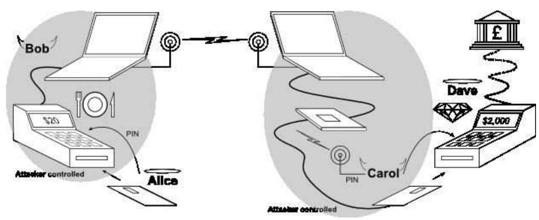


Figure: Smart card relay attack [Anderson et al.]

This will become much easier with NFC phones!

But the NFC phones have a timer!

Task

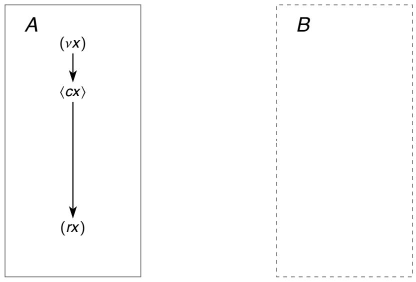
Strengthen authentication

Verify for each principal

- not only **certificates**
- but also **proximity**

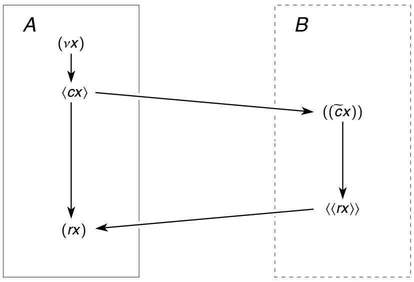
What is authentication?

Challenge-Response pattern



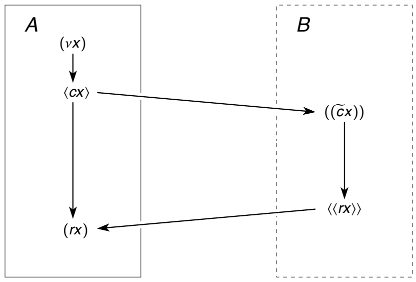
What is authentication?

Challenge-Response pattern



What is authentication?

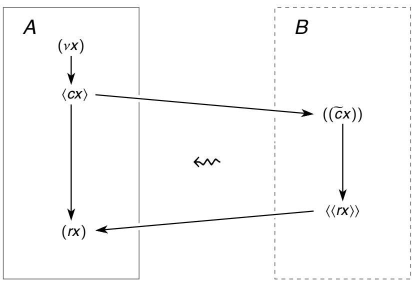
Challenge-Response pattern



$\text{Local}_A \implies \text{Global}_{AB}$

What is authentication?

Challenge-Response pattern



$\text{Local}_A \implies \text{Global}_{AB}$

Derive global from local?!

Derive global from local?!

Problem

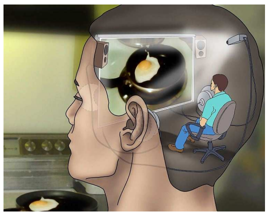
"There is no logical impossibility in the hypothesis that the world sprang into being five minutes ago, exactly as it then was, with a population that 'remembered' a wholly unreal past."

Bertrand Russell, The Analysis of Mind

Derive global from local?!

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

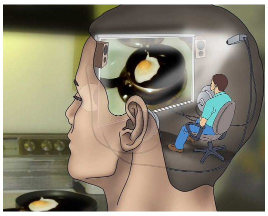
Philosophical solution: reflection



Derive global from local?!

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Philosophical solution: reflection



René to himself: "I think, therefore I exist."

Derive global from local?!

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Computational solution: cheating is hard

Derive global from local?!

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

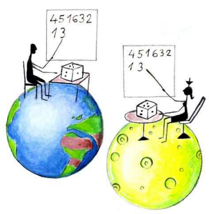
Computational solution: cheating is hard

Alan to Machine: "You are a machine."

Derive global from local?!

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Cryptographic solution: authenticity from secrecy



Alice to Bob: "Nobody else could decrypt this, therefore you exist."

Authentication with perfect cryptography

"Theorem"

Suppose that only Bob knows k^B, such that

- rx can be computed from $\widetilde{c}x$ and k^B
- this is the only way to compute rx here

Authentication with perfect cryptography

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

"Theorem"

Suppose that only Bob knows k^B, such that

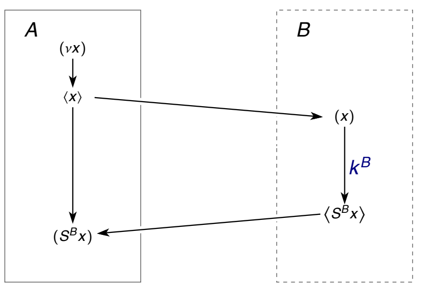
- rx can be computed from $\widetilde{c}x$ and k^B
- this is the only way to compute rx here

Then $\text{Local}_A \Longrightarrow \text{Global}_{AB}$ holds.

Authentication with perfect cryptography

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Example

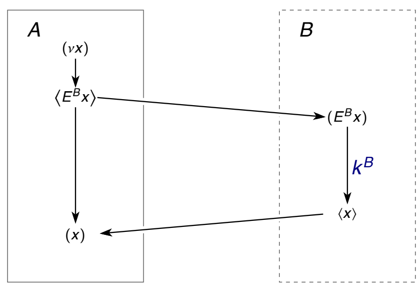


$\text{Local}_A \qquad \Longrightarrow \qquad \text{Global}_{AB}$

Authentication with perfect cryptography

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Example



$\text{Local}_A \qquad \Longrightarrow \qquad \text{Global}_{AB}$

Authentication with perfect cryptography

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

"Theorem"

Suppose that only Bob knows k^B, such that

- rx can be computed from $\widetilde{c}x$ and k^B
- this is the only way to compute rx here

Then $\text{Local}_A \Longrightarrow \text{Global}_{AB}$ holds

Authentication in Protocol Logics

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Theorem A

Suppose that only Bob knows k^B, such that

- rx can be computed from $\widetilde{c}x$ and k^B
  - $k^B, \widetilde{c}x \vdash rx$
- this is the only way to compute rx here
  - $\{\!\{k^B\}\!\}$ guards rx within CR

Then $\text{Local}_A \Longrightarrow \text{Global}_{AB}$ holds where

$$\begin{aligned} \text{Local}_A &= (\nu x)_A \to \langle cx\rangle_A \to (rx)_A \\ \text{Global}_{AB} &= (\nu x)_A \to \langle cx\rangle_A \to ((\widetilde{c}x))_B \to \langle\langle rx\rangle\rangle_B \to (rx)_A \end{aligned}$$

Authentication in Protocol Logics

Theorem A

Suppose that only Bob knows k^B, such that

- rx can be computed from $\widetilde{c}x$ and k^B
  - $k^B, \widetilde{c}x \vdash rx$
- this is the only way to compute rx here
  - $\left\{\{k^B\}\right\}$ guards rx within CR

Then $\text{Local}_A \Longrightarrow \text{Global}_{AB}$ holds where

$$\begin{aligned} \text{Local}_A &= (\nu x)_A \to \langle cx \rangle_A \to (rx)_A \\ \text{Global}_{AB} &= (\nu x)_A \to \langle cx \rangle_A \to ((\widetilde{c}x))_B \to \langle\langle rx \rangle\rangle_B \to (rx)_A \end{aligned}$$

Algebraic guards

Definition

For $s \in \mathbb{T}[V]$ and $\mathcal{G}, \mathcal{C} \in \wp\wp\mathbb{T}[V]$ with $s \not\sqsubseteq \Theta \in \mathcal{C}$ define

$$\mathcal{G} \text{ guards } s \text{ within } \mathcal{C}$$

$$\Updownarrow$$

$$\forall \Theta \in \mathcal{C}\ \exists \Gamma \in \mathcal{G}.\quad \Theta \vdash s \Longrightarrow \Theta \vdash \Gamma$$

Algebraic guards

Definition

For $s \in \mathbb{T}[V]$ and $\mathcal{G}, \mathcal{C} \in \wp\wp\mathbb{T}[V]$ with $s \not\sqsubseteq \Theta \in \mathcal{C}$ define

$$\mathcal{G} \text{ guards } s \text{ within } \mathcal{C}$$

$$\Updownarrow$$

$$\forall \Theta \in \mathcal{C}\ \exists \Gamma \in \mathcal{G}.\quad \Theta \vdash s \Longrightarrow \Theta \vdash \Gamma$$

where

$$\begin{aligned} \Theta \vdash \Gamma &\iff \forall s \in \Gamma \exists \vec{t} \subseteq \Theta \exists f(\vec{x}) \in \mathcal{F}.\ f(\vec{t}) = s \\ \Theta \sqsupseteq \Gamma &\iff \forall s \in \Gamma \exists \vec{t} \subseteq \Theta \exists j(\vec{x}) \in \mathcal{J}.\ j(\vec{t}) = s \end{aligned}$$

Algebraic guards

Examples

- $\{\{x, g^y\}, \{y, g^x\}\}$ guards g^{xy} within DH

Algebraic guards

Examples

- $\{\{x, g^y\}, \{y, g^x\}\}$ guards g^{xy} within DH
- $\left\{\{\overline{k}\}, \{m\}\right\}$ guards m within $\{A \text{ to } B : E(k, m)\}$

Perfect cryptography

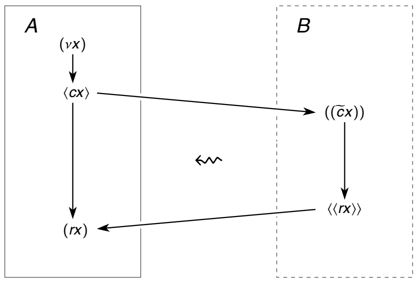
The algebraic fact that

$$\Theta \vdash s \quad \vee \quad \Theta \nvdash s$$

abstracts away partial information leaks.

Task: Refine cryptographic authentication

Challenge-Response pattern

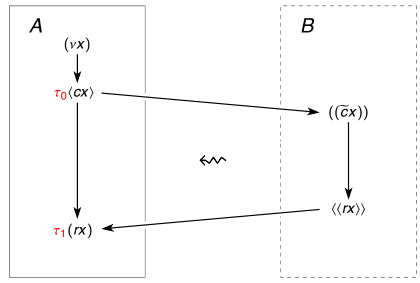


$\text{Local}_A \implies \text{Global}_{AB}$

Proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Timed Challenge-Response pattern

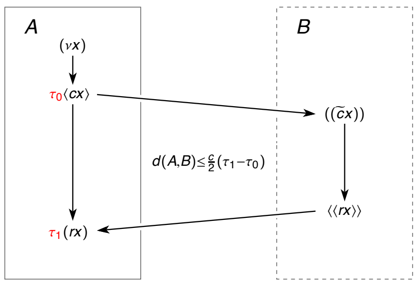


$\text{Local}^{\tau}_A \implies \text{Global}^{\tau}_{AB}$

Proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Timed Challenge-Response pattern

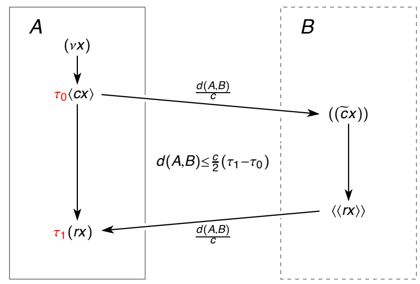


$\text{Local}^{\tau}_A \implies \text{Global}^{\tau}_{AB}$

Proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Timed Challenge-Response pattern

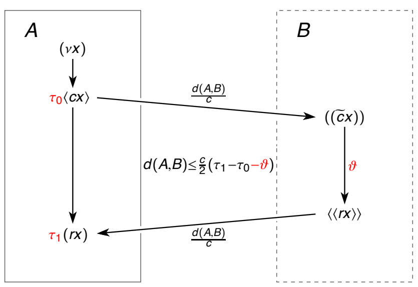


$\text{Local}^{\tau}_A \implies \text{Global}^{\tau}_{AB}$

Proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Timed Challenge-Response pattern



$\text{Local}^{\tau}_A \implies \text{Global}^{\tau}_{AB}$

Proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Problem

- Alice does not know ϑ.

Proximity authentication

Problem

- Alice does not know ϑ.
- Bob looks closer if he is faster.

Proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Problem

- Alice does not know ϑ.
- Bob looks closer if he is faster.

Task

- Minimize ϑ.
- Compute $\widetilde{c}x, k^B \vdash rx$ on-line.

On-line computation

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Definition

A boolean function $f : \mathbb{Z}_2^\ell \longrightarrow \mathbb{Z}_2^\ell$ is

- *on-line* if it returns i-th bit of the output as soon as it has received i-th bit of the input, for $i = 1, 2, \ldots, \ell$

On-line computation

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Definition

A boolean function $f : \mathbb{Z}_2^\ell \longrightarrow \mathbb{Z}_2^\ell$ is

- *on-line* if it returns i-th bit of the output as soon as it has received i-th bit of the input, for $i = 1, 2, \ldots, \ell$
- *partitioned* if i-th bit of the output only depends on the i-th bit of the input.

On-line computation

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Definition

A boolean function $f : \mathbb{Z}_2^\ell \longrightarrow \mathbb{Z}_2^\ell$ is

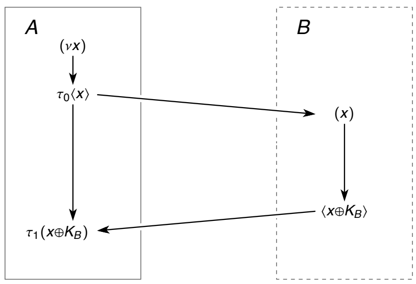
- *on-line* if it returns i-th bit of the output as soon as it has received i-th bit of the input, for $i = 1, 2, \ldots, \ell$
- *partitioned* if i-th bit of the output only depends on the i-th bit of the input.

(Blockwise versions are defined analogously.)

Implementing proximity authentication

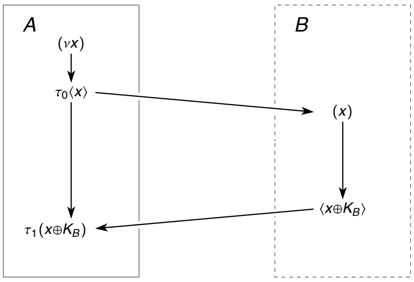
Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

First try: XOR (Brands-Chaum)



Implementing proximity authentication

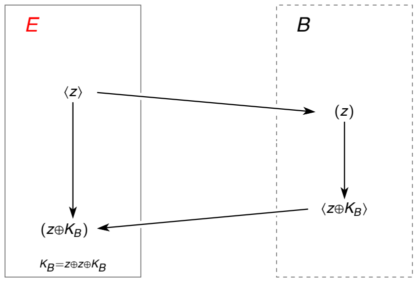
First try: XOR (Brands-Chaum)



$K_B = H(k^{AB}, y)$ where $(\nu y)_A \to \langle y\rangle_A$

Implementing proximity authentication

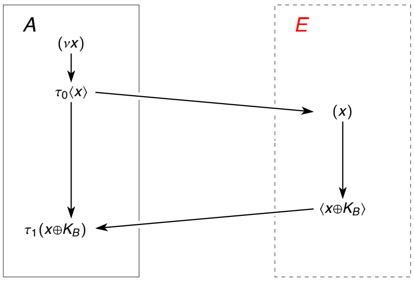
Silly attack



Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Implementing proximity authentication

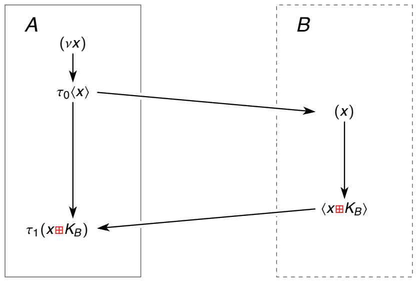
Silly attack



Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Implementing proximity authentication

Second try: the Hancke-Kuhn function

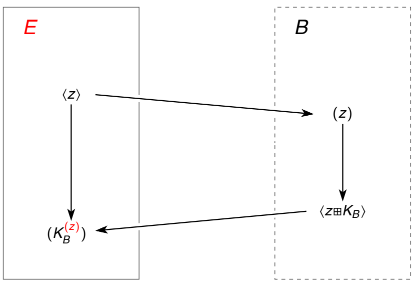


$(x \boxplus Y)_i = Y_i^{(x_i)} \qquad Y = Y^{(0)} :: Y^{(1)}$

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Implementing proximity authentication

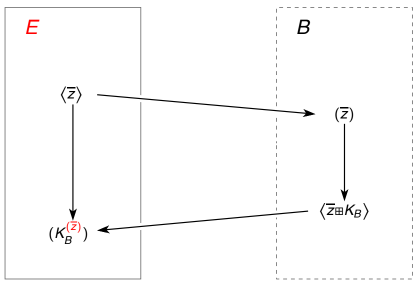
The silly attack only recovers half of the bits



Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Implementing proximity authentication

. . . and Eve needs one more challenge. . .

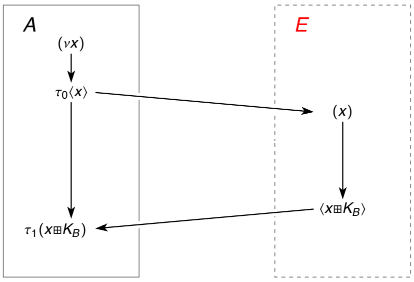


Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

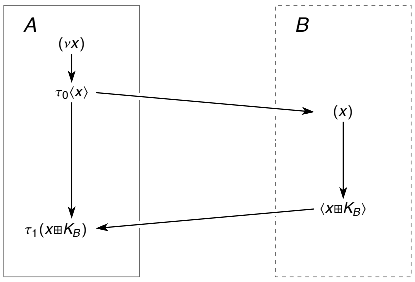
...before she can impersonate Bob



Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

The Hancke-Kuhn protocol: one-time secret

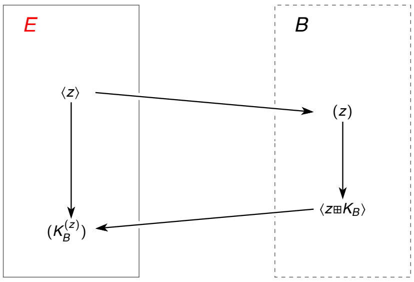


$K_B = H(k^{AB}, y)$ where $(\nu y)_B \to \langle y\rangle_B$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Eve can still get one half of the secret bits

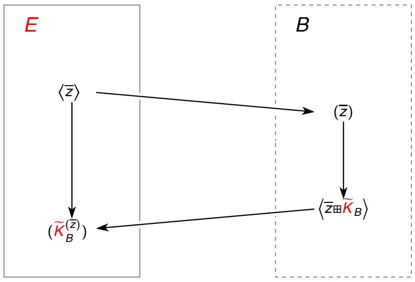


$K_B = H(k^{AB}, y)$ where $(\nu y)_B \to \langle y\rangle_B$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

...but not the other half

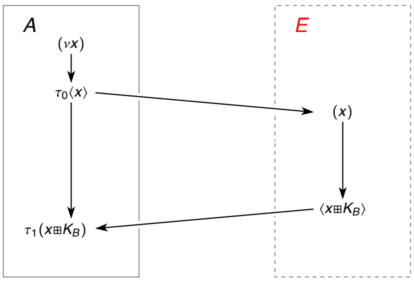


$\widetilde{K}_B = H(k^{AB}, \widetilde{y})$ where $(\nu \widetilde{y})_B \to \langle \widetilde{y}\rangle_B$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Eve's chance to guess the response

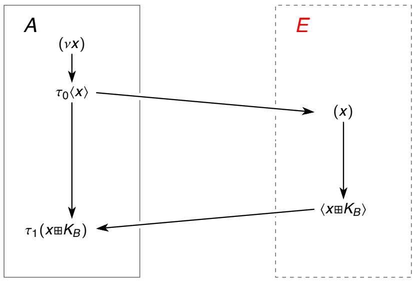


$$\left[z, z \boxplus K_B,\ x \vdash x \boxplus K_B\right] = 2^{-\Delta(z,x)}$$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

...with the expected value



$$\int_{z\in\mathbb{Z}_2^\ell}\left[z, z \boxplus K_B,\ x \vdash x \boxplus K_B\right] = \left(\frac{3}{4}\right)^\ell$$

Implementing proximity authentication

Facts

- On-line functions always leak information:

$$\left[z, fz, x \vdash fx\right] \quad > \quad \varepsilon(\ell)$$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Facts

- On-line functions always leak information:

$$\left[z, fz, x \vdash fx\right] \quad > \quad \varepsilon(\ell)$$

- On-line response can be guessed:

$$\{\{k\}, \{z, rz, x\}\}_{z \in Z} \quad \text{guards} \quad rx \quad \text{within} \quad CRP$$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Facts

- On-line functions always leak information:

$$\left[z, fz, x \vdash fx\right] \quad > \quad \varepsilon(\ell)$$

- On-line response can be guessed:

$$\{\{k\}, \{z, rz, x\}\}_{z \in Z} \quad \text{guards} \quad rx \quad \text{within} \quad CRP$$

- Protocols with on-line response do not satisfy Theorem A.

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Proposition

If $f : \mathbb{Z}_2^\ell \longrightarrow \mathbb{Z}_2^\ell$ is bitwise partitioned, then

- $\left[z, f(z), x \vdash f(x)\right] \geq 2^{-\Delta(z,x)}$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Proposition

If $f : \mathbb{Z}_2^\ell \longrightarrow \mathbb{Z}_2^\ell$ is bitwise partitioned, then

- $\left[z, f(z), x \vdash f(x)\right] \geq 2^{-\Delta(z,x)}$
- $\left[z, f(z), x \vdash f(x)\right] = 2^{-\Delta(z,x)} \iff \forall i. \left[f_i(0) \perp f_i(1)\right]$

Implementing proximity authentication

Bayesian authentication
D. Pavlovic
Problem
Flavours
What is authentication?
Crypto authentication
Theorem A
Proximity authentication
Implementing
Proving proximity
Conclusions

Proposition

If $f : \mathbb{Z}_2^\ell \longrightarrow \mathbb{Z}_2^\ell$ is bitwise partitioned, then

- $\left[z, f(z), x \vdash f(x)\right] \geq 2^{-\Delta(z,x)}$
- $\left[z, f(z), x \vdash f(x)\right] = 2^{-\Delta(z,x)} \iff \forall i. \left[f_i(0) \perp f_i(1)\right]$
- $\left[z, f(z), x \vdash f(x)\right] = 2^{-\Delta(z,x)} \iff f(x) = x \boxplus \left(f(0^\ell) :: f(1^\ell)\right)$

Implementing proximity authentication

Upshot

- The Hancke-Kuhn protocol is
  - not secure in the symbolic model
  - optimal among the partitioned implementations

Implementing proximity authentication

Upshot

- The Hancke-Kuhn protocol is
  - not secure in the symbolic model
  - optimal among the partitioned implementations
- Need a better model to evaluate its security.

Bayesian model

- *algebra encoding:* $[\![-]\!] : \mathbb{T}[V] \longrightarrow \wp\{0,1\}^*$

Bayesian model

- *algebra encoding:* $[\![-]\!] : \mathbb{T}[V] \longrightarrow \wp\{0,1\}^*$
- *feasible operations:* $\mathcal{F}$ on the codes (e.g. $\mathcal{BPP}$)

Bayesian model

- *algebra encoding:* $[\![-]\!] : \mathbb{T}[V] \longrightarrow \wp\{0,1\}^*$
- *feasible operations:* $\mathcal{F}$ on the codes (e.g. $\mathcal{BPP}$)
- *guessing chance:* $\left[\Theta \vdash \Gamma\right] = \bigvee_{\mathbb{A}\in\mathcal{F}} \mathrm{Prob}\left(\Gamma \leftarrow \mathbb{A}(\Theta)\right)$

Bayesian model

- *algebra encoding:* $[\![-]\!] : \mathbb{T}[V] \longrightarrow \wp\{0,1\}^*$
- *feasible operations:* $\mathcal{F}$ on the codes (e.g. $\mathcal{BPP}$)
- *guessing chance:* $\left[\Theta \vdash \Gamma\right] = \bigvee_{\mathbb{A}\in\mathcal{F}} \mathrm{Prob}\left(\Gamma \leftarrow \mathbb{A}(\Theta)\right)$
- *guessing advantage:* $\mathrm{Adv}\left[\Theta \vdash \Gamma\right] = \left[\Theta \vdash \Gamma\right] - \left[\Gamma\right]$

Bayesian model

- *algebra encoding:* $[\![-]\!] : \mathbb{T}[V] \longrightarrow \wp\{0,1\}^*$
- *feasible operations:* $\mathcal{F}$ on the codes (e.g. $\mathcal{BPP}$)
- *guessing chance:* $\left[\Theta \vdash \Gamma\right] = \bigvee_{\mathbb{A}\in\mathcal{F}} \mathrm{Prob}\left(\Gamma \leftarrow \mathbb{A}(\Theta)\right)$
- *guessing advantage:* $\mathsf{Adv}\left[\Theta \vdash \Gamma\right] = \left[\Theta \vdash \Gamma\right] - \left[\Gamma\right]$
- *independence:* $\left[\Theta \perp \Gamma\right] \iff \mathsf{Adv}\left[\Theta \vdash \Gamma\right] = 0$
  where $\left[\Gamma\right] = \left[\emptyset \vdash \Gamma\right]$

Bayesian model

Lemma

Guessing probability is sub-Bayesian, in the sense

$$\left[\Theta \vdash \Gamma\right] \cdot \left[\Theta, \Gamma \vdash \Xi\right] \;\leq\; \left[\Theta \vdash \Gamma, \Xi\right]$$

which for $\Theta = \emptyset$ and $\left[\Gamma\right] \neq 0$ gives

$$\left[\Gamma \vdash \Xi\right] \;\leq\; \frac{\left[\Gamma, \Xi\right]}{\left[\Gamma\right]}$$

Bayesian model

Remark

Guessing probability is not Bayesian in general:

- $\left[\Gamma\right] \cdot \left[\Gamma \vdash \Theta\right] \neq \left[\Theta\right] \cdot \left[\Theta \vdash \Gamma\right]$
- $\left[\Gamma \perp \Theta\right] \not\Leftrightarrow \left[\Theta \perp \Gamma\right]$

Guessing guards

Definition

For $s \in \mathbb{T}[V]$ and $\mathcal{G}, \mathcal{C} \in \wp\wp\mathbb{T}[V]$ with $s \notin \Theta \in \mathcal{C}$ define

$$\mathcal{G} \;\text{ guards }\; s \;\text{ within }\; \mathcal{C}$$

$$\Updownarrow$$

$$\forall \Theta \in \mathcal{C}. \left(\left[\Theta \vdash s\right] \;\leq\; \sum_{\Gamma \in \mathcal{G}} \left[\Theta \vdash \Gamma\right] \cdot \left[\Theta, \Gamma \vdash s\right] \right.$$

$$\wedge$$

$$\left. \mathsf{Adv}\left[\Theta \vdash s\right] \;\leq\; \bigvee_{\Gamma \in \mathcal{G}} \mathsf{Adv}\left[\Theta \vdash \Gamma\right] \right)$$

Authentication with imperfect cryptography

Theorem B

Suppose that only Bob knows k, such that

- $k, x \vdash rx$
- $\{\{k\}\} \cup \mathcal{X}$ guards rx within CRT

Then

$$\mathrm{Prob}(\mathsf{Global}_{AB} \mid \mathsf{Local}_A) \;\geq\; 1 - \bigvee_{\Theta \in CRT} \int_{\Xi \in \mathcal{X}} \left[\Theta, \Xi \vdash rx\right]$$

Authentication with imperfect cryptography

Theorem B

Suppose that only Bob knows k, such that

- $k, x \vdash rx$
- $\{\{k\}\} \cup \mathcal{X}$ guards rx within CRT

Then

$$\mathrm{Prob}(\mathsf{Global}_{AB} \mid \mathsf{Local}_A) \;\geq\; 1 - \bigvee_{\Theta \in CRT} \int_{\Xi \in \mathcal{X}} \left[\Theta, \Xi \vdash rx\right] \;-\; \varepsilon(\ell)$$

Authentication with imperfect cryptography

Proof

$$\exists\Theta \in \mathcal{C}.\ \Theta \vdash rx, k$$
$$\Downarrow$$
$$\Theta_B \vdash rx$$
$$\Downarrow$$
$$\mathsf{Global}_{AB}$$
$$\Downarrow$$
$$\mathsf{Local}_{A}$$
$$\Downarrow$$
$$\exists\Theta \in \mathcal{C}.\ \Theta \vdash rx$$

Authentication with imperfect cryptography

Proof

$$\mathrm{Prob}\left(\exists\Theta \in \mathcal{C}.\ \Theta \vdash rx, k\right)$$
$$\rotatebox{90}{$\geq$}$$
$$\mathrm{Prob}\left(\Theta_B \vdash rx\right) + \varepsilon(\ell)$$
$$\rotatebox{90}{$\geq$}$$
$$\mathrm{Prob}\left(\mathsf{Global}_{AB}\right)$$
$$\rotatebox{90}{$\geq$}$$
$$\mathrm{Prob}\left(\mathsf{Local}_{A}\right)$$
$$\rotatebox{90}{$\geq$}$$
$$\mathrm{Prob}\left(\exists\Theta \in \mathcal{C}.\ \Theta \vdash rx\right)$$

Authentication with imperfect cryptography

Proof

$$\begin{aligned}
\mathrm{Prob}\left(\mathsf{Global}_{AB} \mid \mathsf{Local}_A\right) &= \frac{\mathrm{Prob}\left(\mathsf{Global}_{AB} \wedge \mathsf{Local}_A\right)}{\mathrm{Prob}(\mathsf{Local}_A)} \\
&= \frac{\mathrm{Prob}\left(\mathsf{Global}_{AB}\right)}{\mathrm{Prob}(\mathsf{Local}_A)} \\
&\geq \frac{\mathrm{Prob}\left(\exists\Theta \in \mathcal{C}.\ \Theta \vdash rx, k\right)}{\mathrm{Prob}\left(\exists\Theta \in \mathcal{C}.\ \Theta \vdash rx\right)} - \varepsilon(\ell) \\
&\geq \bigwedge_{\Theta\in\mathcal{C}} \frac{\left[\Theta \vdash rx, k\right]}{\left[\Theta \vdash rx\right]} - \varepsilon(\ell)
\end{aligned}$$

Authentication with imperfect cryptography

Proof

But

$$\bigwedge_{\Theta\in\mathcal{C}} \frac{\left[\Theta \vdash rx, k\right]}{\left[\Theta \vdash rx\right]} \geq 1 - \bigvee_{\Theta\in\mathcal{C}} \int_{\Xi\in\mathcal{X}} \left[\Theta, \Xi \vdash rx\right]$$

follows from

$$\begin{aligned}
\frac{\left[\Theta \vdash rx, k\right]}{\left[\Theta \vdash rx\right]} &\geq \frac{\left[\Theta \vdash k\right]\cdot\left[\Theta, k \vdash rx\right]}{\left[\Theta \vdash k\right]\cdot\left[\Theta, k \vdash rx\right] + \sum_{\Xi\in\mathcal{X}}\left[\Theta \vdash \Xi\right]\cdot\left[\Theta, \Xi \vdash rx\right]} \\
&= 1 - \frac{\sum_{\Xi\in\mathcal{X}}\left[\Theta \vdash \Xi\right]\cdot\left[\Theta, \Xi \vdash rx\right]}{\left[\Theta \vdash rx\right]} \\
&= 1 - \int_{\Xi\in\mathcal{X}} \left[\Theta, \Xi \vdash rx\right]
\end{aligned}$$

Authentication with imperfect cryptography

The case of the Hancke-Kuhn protocol

We have seen that it admits

$$\mathcal{X} = \left\{\{z, z \boxplus K, x\} \mid z \in \mathbb{Z}_2^\ell\right\}$$

as the guessing set, and that

$$\int_{z\in\mathbb{Z}_2^\ell} \left[z, z \boxplus K, x \vdash rx\right] = \left(\frac{3}{4}\right)^\ell$$

is the expected probability of a successful guess.

Authentication with imperfect cryptography

Corollary: Security of the Hancke-Kuhn protocol

Suppose that Alice and Bob share an uncompromised key, and that Bob is honest.

If Alice receives a correct response to her challenge, then the probability that this response originates from Bob is indistinguishable from

$$1 - \left(\frac{3}{4}\right)^\ell$$

where ℓ is the length of the challenge.

Conclusions and ongoing work

- Pervasive authentication requires quantitative security evaluation
  - tradeoffs, dynamics...

Conclusions and ongoing work

- Pervasive authentication requires quantitative security evaluation
  - tradeoffs, dynamics...
- The need for quantitative evaluation leads from
  - algebraic derivability $\Gamma \vdash \Theta$ to
  - guessing probability $\left[\Gamma \vdash \Theta\right]$

Conclusions and ongoing work

- Pervasive authentication requires quantitative security evaluation
  - tradeoffs, dynamics...
- The need for quantitative evaluation leads from
  - algebraic derivability $\Gamma \vdash \Theta$ to
  - guessing probability $\left[\Gamma \vdash \Theta\right]$
- This *Bayesian extension of PDL* combines
  - cryptographic formalisms of *provable security* with
  - modules over *assemblies* and *modest sets*.

Conclusions and ongoing work

- Pervasive authentication requires quantitative security evaluation
  - tradeoffs, dynamics...
- The need for quantitative evaluation leads from
  - algebraic derivability $\Gamma \vdash \Theta$ to
  - guessing probability $\left[\Gamma \vdash \Theta\right]$
- This *Bayesian extension of PDL* combines
  - cryptographic formalisms of *provable security* with
  - modules over *assemblies* and *modest sets*.
- Similar combinations simplify reasoning about other cryptographic concepts and frameworks.