Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

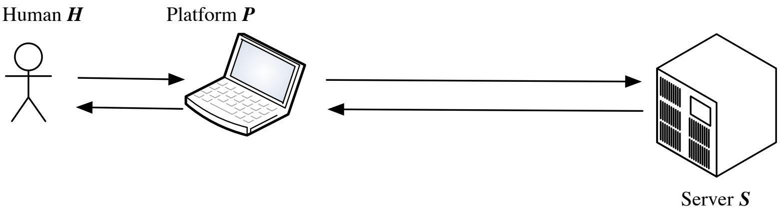
Informatik
Computer Science

# Characterization of Secure Human-Server Communication

Michael Schläpfer
Institute of Information Security
Dec 17, 2013

# Motivation

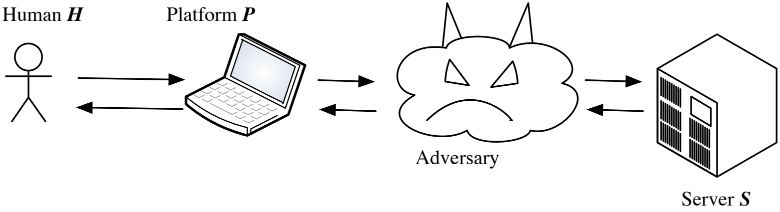
Remote (Internet) voting:




- Uncontrolled environment
- Broader attack surface
- No inherent voter privacy

# Motivation

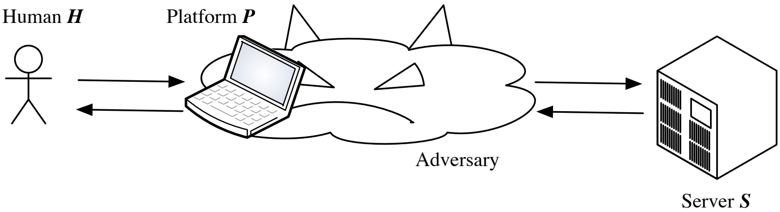
Cryptographic Internet voting protocols:




- Ballot casting assurance ✓
- Receipt freeness ✓
- Coercion resistance ✓

# Motivation

The Secure Platform Problem (SPP):




- Client-side multi-purpose platforms used
- Emerging malware infections
- General problem in electronic communication applications

# Research Questions

- What are possible approaches to solve the SPP?
- How to model these approaches and how to verify their security properties?
- What are necessary conditions to achieve specific security properties?

# Outline

State-Of-The-Art

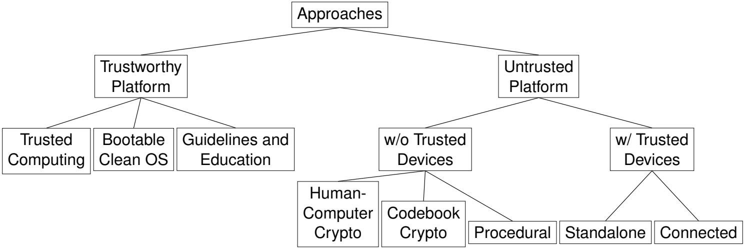
Human-Interaction Security Protocols

Characterization of Secure Human-Server Communication

Case Study

Conclusion

# Taxonomy of Solution Approaches



# Security Ceremonies [UPn03, Ell07]

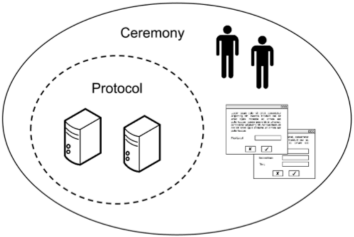
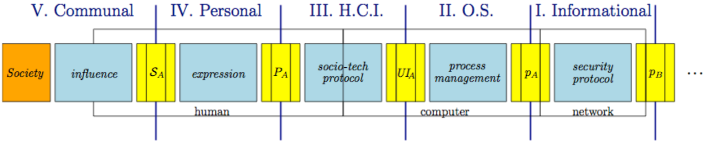



Figure: Security ceremonies. (Source: Carlos et al.)

- Nothing out-of-band
- “Special” Network connections
- Human nodes with different capabilities

# Formal Modeling of Security Ceremonies

- Bella and Coles-Kemp [BCK11, BCK12]:




- Meadows and Pavlovic [PM12, MP13] :
  Procedure Derivation Logic, Logic of moves
- Carlos et al. [CMPC12, CMPC13] :
  Weakening DY-adversary in Bluetooth-Pairing

# Outline

State-Of-The-Art

Human-Interaction Security Protocols

Characterization of Secure Human-Server Communication

Case Study

Conclusion

# Multiset Term Rewriting

- A rewriting theory $R$ consists of rewriting rules $l \rightarrow r$
- The symbol $\rightarrow$ indicates that an expression matching the left side can be rewritten to the one of the right side
- Tamarin uses labeled multiset rewriting rules. A labeled multiset rewriting rule is a triple $(l, a, r)$, denoted by $l{-}[\ a\ ]{\rightarrow}r$

## Examples

$\neg\neg A \rightarrow A$ represents a rule for double negative elimination in logic.
$A, A, B{-}[\ \ ]{\rightarrow}C, D, D, E$ is a multiset rewriting rule in Tamarin syntax.

# Traces of a Protocol

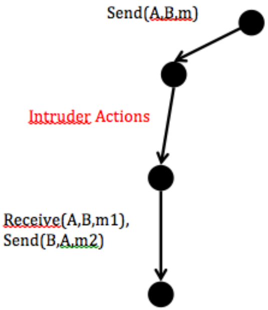
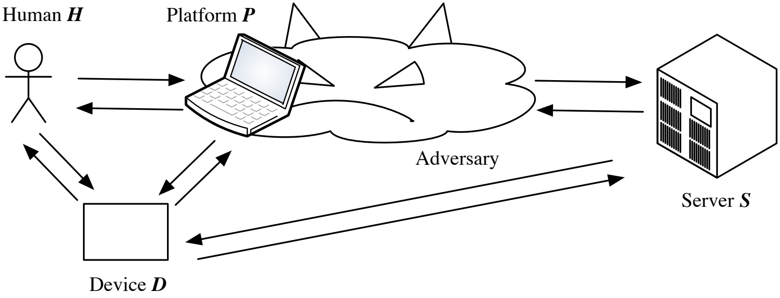


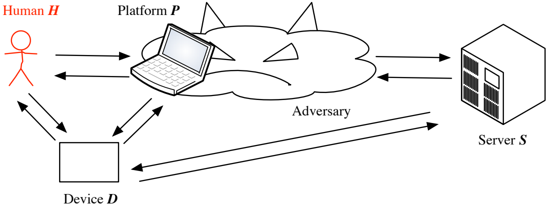

Figure: A specific trace of a protocol.

# Human-Interaction Security Protocols (HISP)



# Modeling HISPs

## Human Model

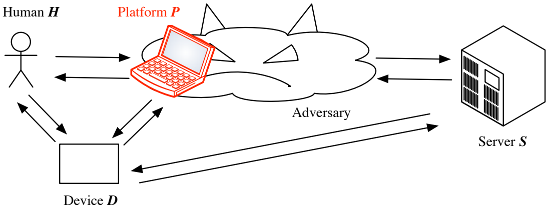



### Human capabilities

- Pairing of terms
- Projection of terms

# Modeling HISPs

## Dishonest Agents

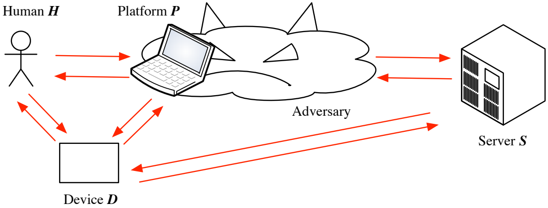



### Dishonest agents

- Leak all information, i.e., the current state
- Adversary controls them, i.e., updates the current state

# Modeling HISPs

Standard Dolev-Yao adversary and channel abstraction:




## Channels as assumptions

- Insecure
- Confidential
- Authentic
- Secure

# Modeling HISPs

Security goals

- Authentic channels
- Confidential channels
- Secure channels

between $H$ and $S$.

# Modeling HISPs

Security goals

- Authentic channels
- “Discriminating” authentic channels
- Confidential channels
- “Discriminating” confidential channels
- Secure channels
- “Discriminating” secure channels

between *H* and *S*.

# Outline

State-Of-The-Art

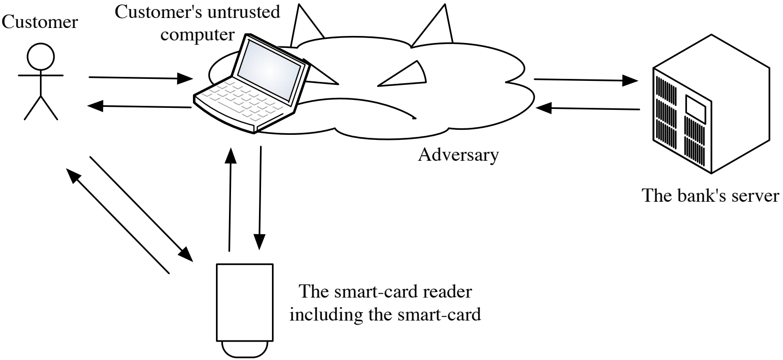
Human-Interaction Security Protocols

Characterization of Secure Human-Server Communication

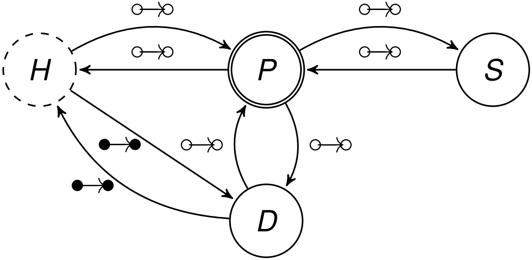
Case Study

Conclusion

# Just One Example



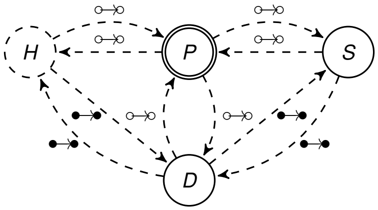
# Communication Topology Example



# Communication Topology Model

## HISP communication topology $(V, E, \eta, \mu)$

- $V = \{H, D, P, S\}$
- $\eta(H) = (\Sigma_H, \emptyset, \text{honest}), \eta(D) = (\Sigma, K_D, \text{honest}), \ldots$
- $\mu(H, P) = \mu(P, H) = \mu(D, P) = \circ\!\!\rightarrow\!\!\!\!\!/\,\circ, \ldots$



# Conditions for Secure Channel from *H* to *S*

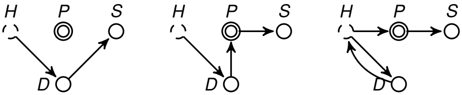



Figure: All minimal HISP topologies for which there are protocols providing a secure channel from *H* to *S*.

# Conditions for Secure Channel from *S* to *H*

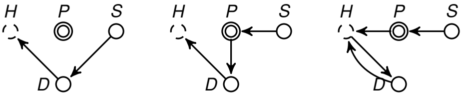



Figure: All minimal HISP topologies for which there are protocols providing a secure channel from *S* to *H*.

# Conditions for "Discriminating" Secure Channel from *H* to *S*

All minimal graphs for a "discriminating" secure channel from *H* to *S*:

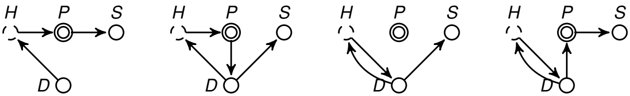



Figure: The edge from *D* to *H* and all acyclic paths from *H* to *S*.

# Conditions for "Discriminating" Secure Channel from *H* to *S*

"Discriminating" secure channels from *H* to *S*:

| | $(D,H) \notin E \wedge (H,D) \notin E$ | $(D,H) \notin E \wedge (H,D) \in E \wedge (D,S) \notin E^+$ | $(D,H) \notin E \wedge (H,D) \in E \wedge (D,S) \in E^+$ | $(D,H) \in E$ |
|---|---|---|---|---|
| $\mathrm{dauth}(\mathcal{R},H,S)$ | no (Lemma 1) | no (Lemma 2) | yes (Lemma 4) | yes (Lemma 6) |
| $\mathrm{dconf}(\mathcal{R},H,S)$ | no (Lemma 1) | no (Lemma 2) | yes (Lemma 4) | yes (Lemma 6) |
| $\mathrm{dsecure}(\mathcal{R},H,S)$ | no (Lemma 1) | no (Lemma 2) | yes (Lemma 4) | yes (Lemma 6) |

# Conditions for “Discriminating” Secure Channel from $S$ to $H$

All minimal graphs for a “discriminating” secure channel from $S$ to $H$:

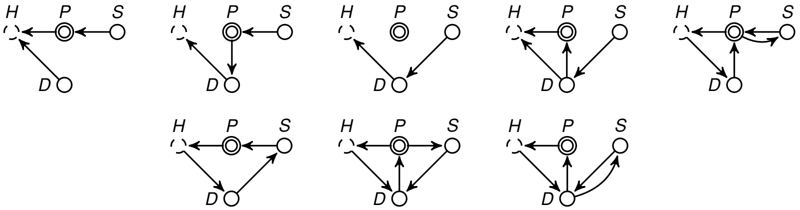



Figure: The edge from $D$ to $H$ and all acyclic paths from $S$ to $H$.

# Conditions for “Discriminating” Secure Channel from $S$ to $H$

Discriminating secure channels from $S$ to $H$:

| | $(D,H) \notin E \wedge (H,D) \notin E$ | $(D,H) \notin E \wedge (H,D) \in E \wedge (D,H) \notin E^+$ | $(D,H) \notin E \wedge (H,D) \in E \wedge (D,H) \in E^+$ | $(D,H) \in E$ |
|---|---|---|---|---|
| $\mathrm{dauth}(\mathcal{R},S,H)$ | no (Lemma 1) | no (Lemma 3) | yes (Lemma 7) | yes (Lemma 5) |
| $\mathrm{dconf}(\mathcal{R},S,H)$ | no (Lemma 1) | no (Lemma 3) | if $(H,S) \in E^+$ (Lemma 8) | yes (Lemma 5) |
| $\mathrm{dsecure}(\mathcal{R},S,H)$ | no (Lemma 1) | no (Lemma 3) | if $(H,S) \in E^+$ (Lemma 8) | yes (Lemma 5) |

# Outline

State-Of-The-Art

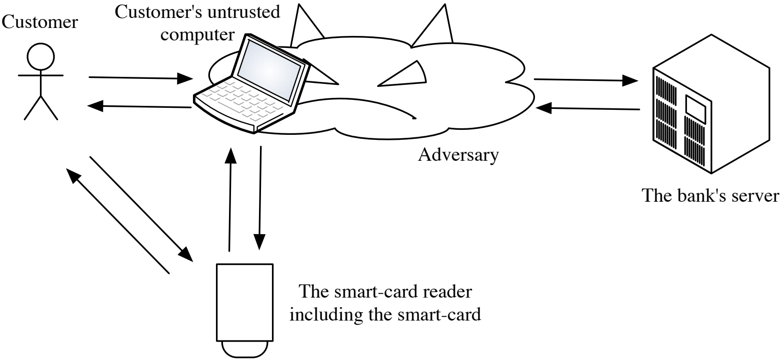
Human-Interaction Security Protocols

Characterization of Secure Human-Server Communication

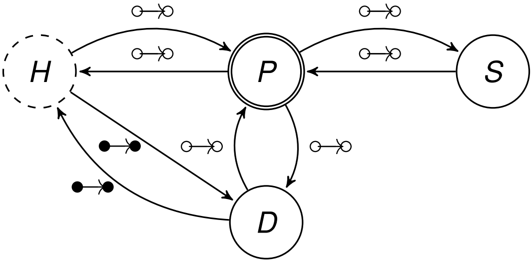
Case Study

Conclusion

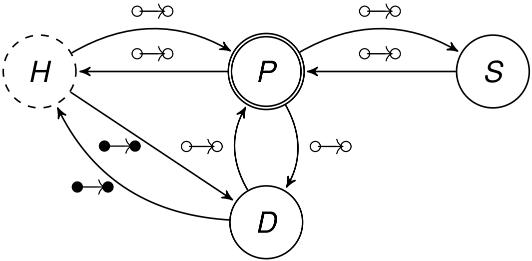
# Smart-Card-Based Transaction Authentication

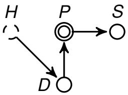


# Communication Topology



# Communication Topology




Authentic channel from *H* to *S* possible. ✓

# Transaction Authentication Protocols

Protocol Transauth a

$$H : \mathrm{knows}(\langle D, PIN \rangle)$$
$$D : \mathrm{knows}(\langle ltkD, PIN \rangle)$$
$$S : \mathrm{knows}(\langle H, D, \mathrm{pk}(ltkD) \rangle)$$
$$H \circ\!\!\rightarrow\!\!\circ P : m$$
$$P \circ\!\!\rightarrow\!\!\circ D : m$$
$$D \bullet\!\!\rightarrow\!\!\bullet H : m$$
$$H \bullet\!\!\rightarrow\!\!\bullet D : PIN$$
$$D \circ\!\!\rightarrow\!\!\circ P : \{m\}_{ltkD}$$
$$P \circ\!\!\rightarrow\!\!\circ S : \langle m, \{m\}_{ltkD} \rangle$$

# Transaction Authentication Protocols

Protocol Transauth a

$$
\begin{array}{rl}
 & H : \mathrm{knows}(\langle D, PIN\rangle) \\
 & D : \mathrm{knows}(\langle ltkD, PIN\rangle) \\
 & S : \mathrm{knows}(\langle H, D, \mathrm{pk}(ltkD)\rangle) \\
H \circ\!\!\rightarrow\!\!\circ & P : m \\
P \circ\!\!\rightarrow\!\!\circ & D : m \\
D \bullet\!\!\rightarrow\!\!\bullet & H : m \\
H \bullet\!\!\rightarrow\!\!\bullet & D : PIN \\
D \circ\!\!\rightarrow\!\!\circ & P : \{m\}_{ltkD} \\
P \circ\!\!\rightarrow\!\!\circ & S : \langle m, \{m\}_{ltkD}\rangle
\end{array}
$$

Protocol Transauth b

$$
\begin{array}{rl}
 & H : \mathrm{knows}(\langle D, PIN\rangle) \\
 & D : \mathrm{knows}(\langle ltkD, PIN\rangle) \\
 & S : \mathrm{knows}(\langle H, D, \mathrm{pk}(ltkD)\rangle) \\
H \circ\!\!\rightarrow\!\!\circ & P : m \\
P \circ\!\!\rightarrow\!\!\circ & D : m \\
D \bullet\!\!\rightarrow\!\!\bullet & H : \langle m, vc\rangle \\
H \bullet\!\!\rightarrow\!\!\bullet & D : \langle PIN, vc\rangle \\
D \circ\!\!\rightarrow\!\!\circ & P : \{m\}_{ltkD} \\
P \circ\!\!\rightarrow\!\!\circ & S : \langle m, \{m\}_{ltkD}\rangle
\end{array}
$$

# Outline

State-Of-The-Art

Human-Interaction Security Protocols

Characterization of Secure Human-Server Communication

Case Study

Conclusion

# Conclusions

- Complete characterization of necessary and sufficient conditions for the existence of security protocols that provide secure channels between a human and a remote server using an insecure network and a dishonest platform.
- Extensible and applicable on different levels of abstraction
- Efficient tool support (Tamarin)
- No bisimulation, i.e., no strong secrecy verification (yet)
- Basis for more specific models (e.g., human behavior)

# Future Work

- More detailed model and channel properties
  - Resilience as assumption
  - Verifiability as goal
- Human error modeling

# References

Giampaolo Bella and Lizzie Coles-Kemp, *Seeing the full picture: the case for extending security ceremony analysis*, Proceedings of 9th Australian Information Security Management Conference (Security Research Centre, Edith Cowan University, Perth, Western Australia), 2011, pp. 49–55.

______, *Layered analysis of security ceremonies*, Information Security and Privacy Research (Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou, eds.), IFIP Advances in Information and Communication Technology, vol. 376, Springer Berlin Heidelberg, 2012, pp. 273–286.

Marcelo Carlomagno Carlos, Jean Everson Martina, Geraint Price, and Ricardo Felipe Custódio, *A proposed framework for analysing security ceremonies.*, SECRYPT, 2012, pp. 440–445.

______, *An updated threat model for security ceremonies*, Proceedings of the 28th Annual ACM Symposium on Applied Computing, ACM, 2013, pp. 1836–1843.

Carl M Ellison, *Ceremony design and analysis.*, IACR Cryptology ePrint Archive **2007** (2007), 399.

Catherine Meadows and Dusko Pavlovic, *Formalizing physical security procedures*, Security and Trust Management (Audun Jø sang, Pierangela Samarati, and Marinella Petrocchi, eds.), LNCS, vol. 7783, Springer Berlin Heidelberg, 2013, pp. 193–208.

Dusko Pavlovic and Catherine Meadows, *Actor-network procedures*, Distributed Computing and Internet Technology (R. Ramanujam and Srini Ramaswamy, eds.), LNCS, vol. 7154, Springer Berlin Heidelberg, 2012, pp. 7–26.

UPnP Security Working Group, *UPnP™ security ceremonies design document*, October 2003.

# Questions

???