A Complete Characterization of Secure Human-Server Communication

David Basin **Saša Radomirović** Michael Schläpfer

Institute of Information Security, ETH Zürich

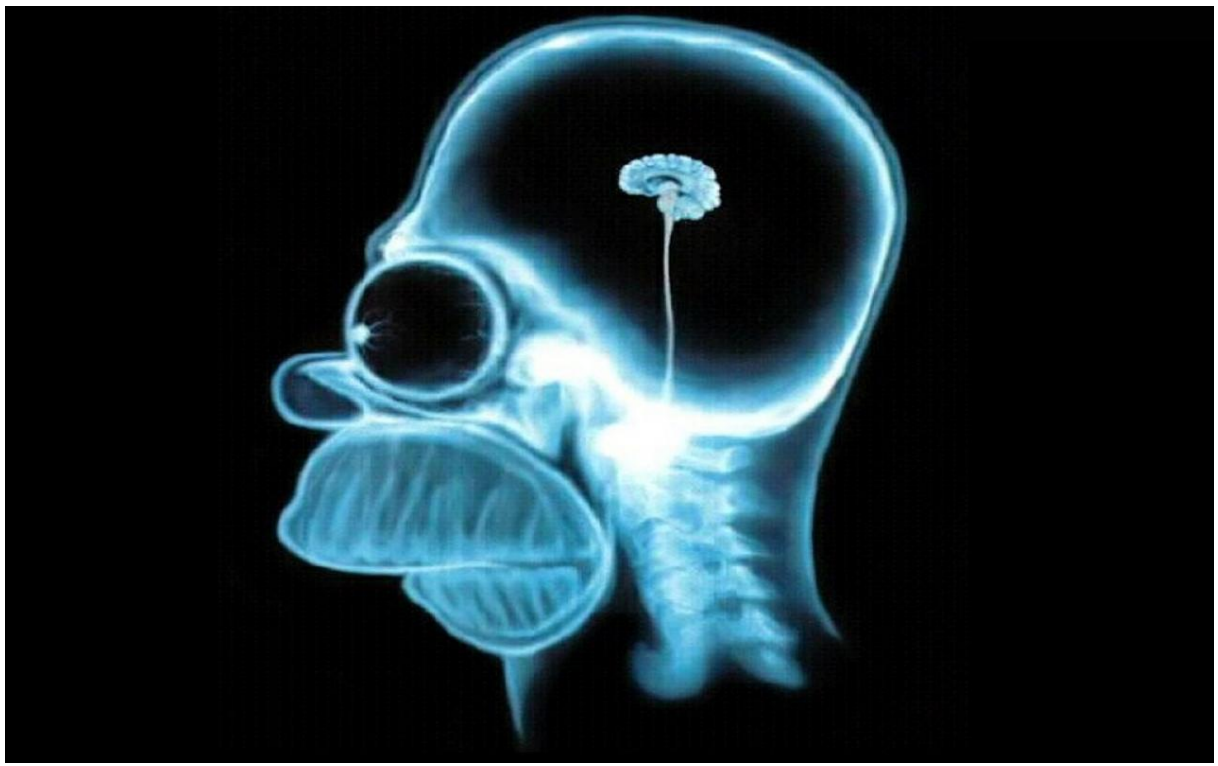
July 15, 2015

Three Observations

- Security protocols are unavoidable.

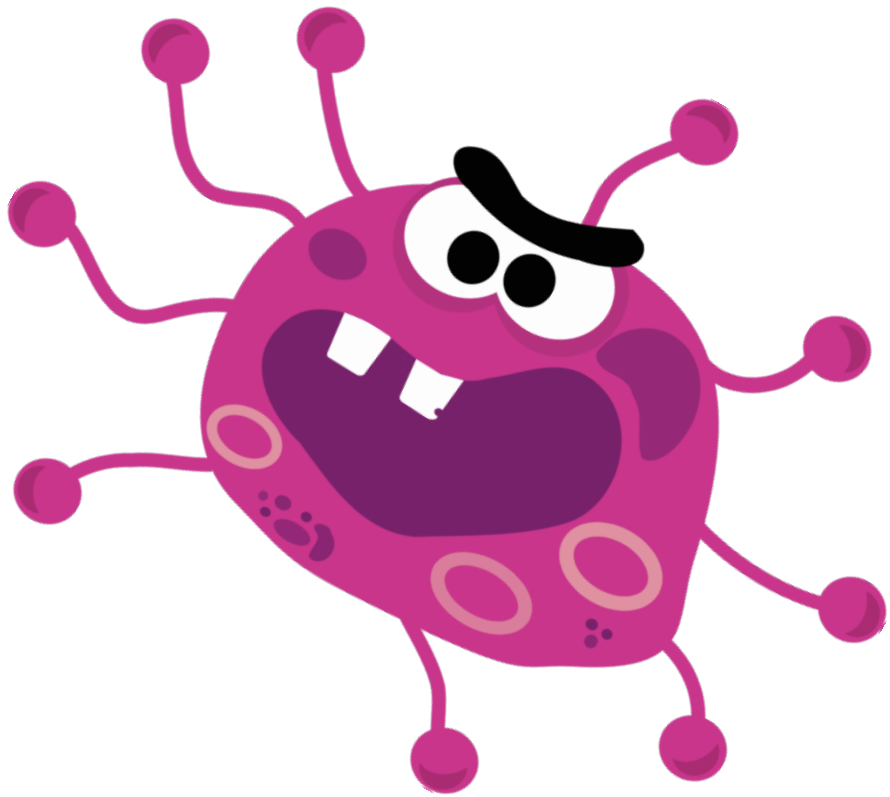
Three Observations

- Security protocols are unavoidable.
- People are terrible at computing.



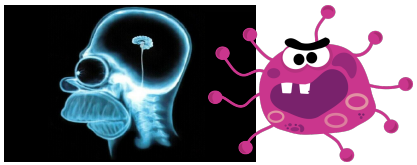
Three Observations

- Security protocols are unavoidable.
- People are terrible at computing.
- Home computers are frequently infiltrated by malware.



Question

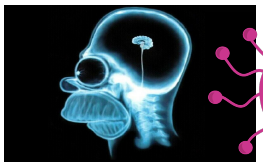
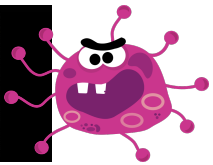
Under these circumstances:



How can we achieve secure (authentic + confidential) communication between a person and a remote server?

Question

Under these circumstances:

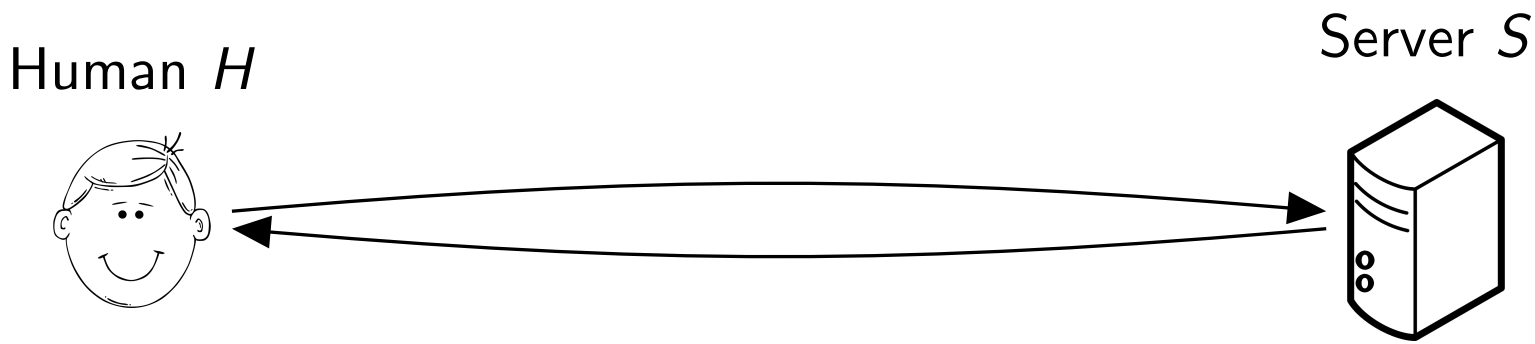
How can we achieve secure (authentic + confidential) communication between a person and a remote server?

- This is a practical problem (e.g., online banking, E-voting)
- and it is wide-spread, since humans rely on computers and smart phones.

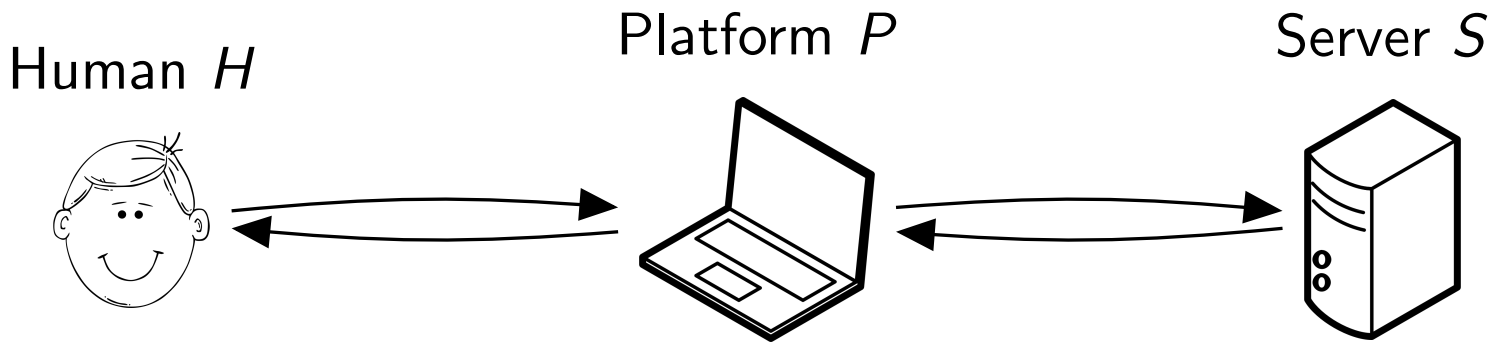
$\rightarrow$ We need a foundation for modeling and reasoning about interaction between humans and computers.

Contributions

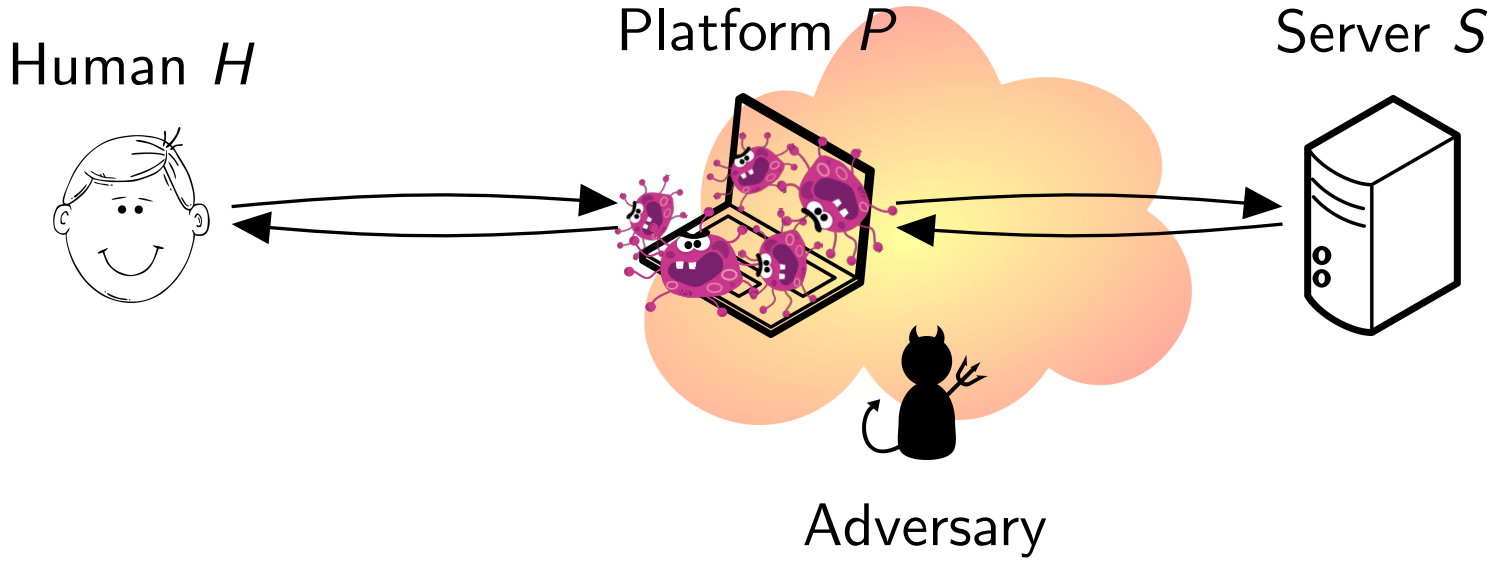
- Simple, intuitive graph-theoretic model to represent and reason about communication between humans, dishonest agents, and honest agents.
- Definitions of protocol properties that capture functionality and safety requirements, taking human agents into account.
- Necessary and sufficient conditions for the existence of security protocols that provide secure channels.



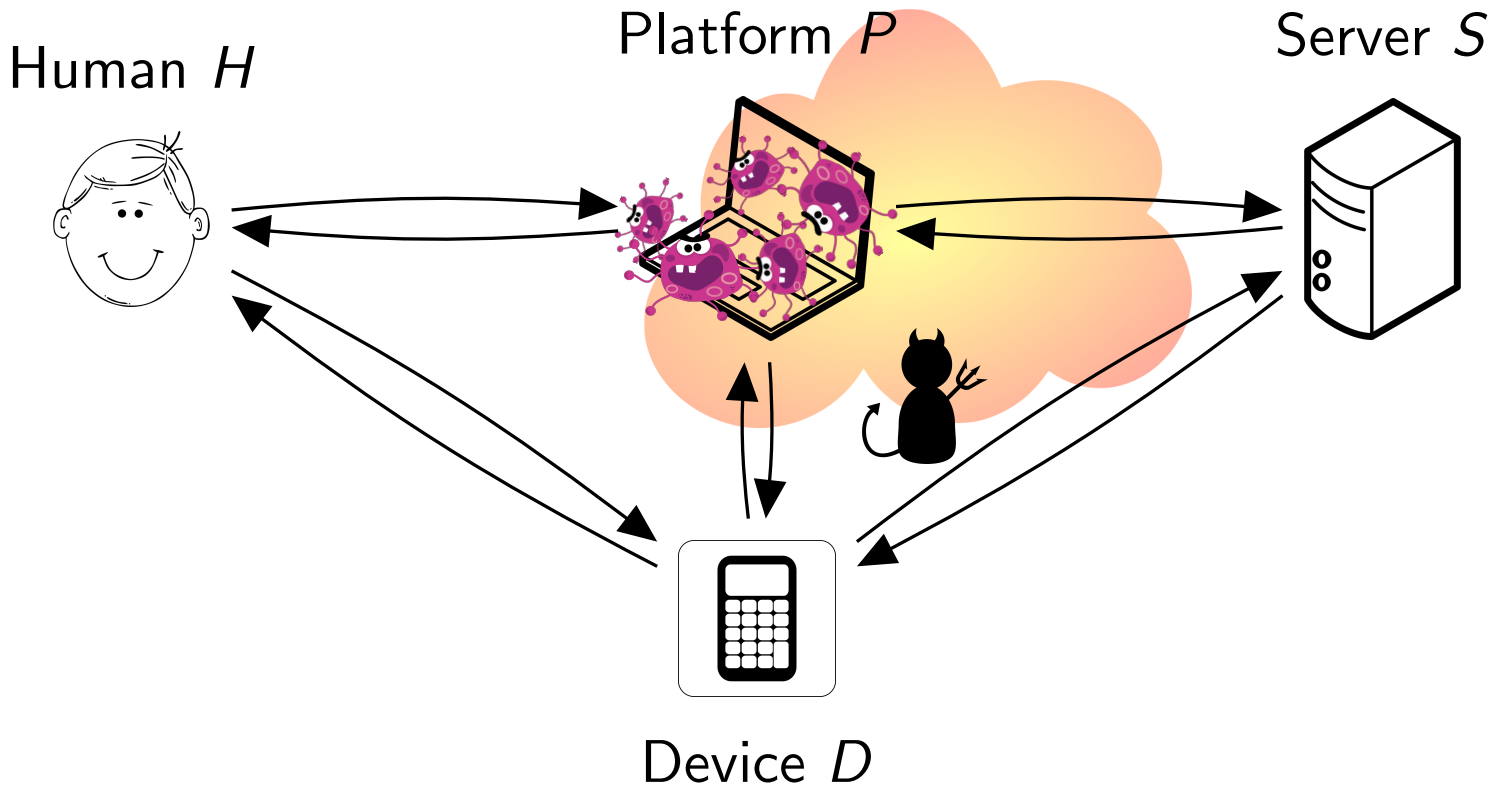
Goal: Secure Communication



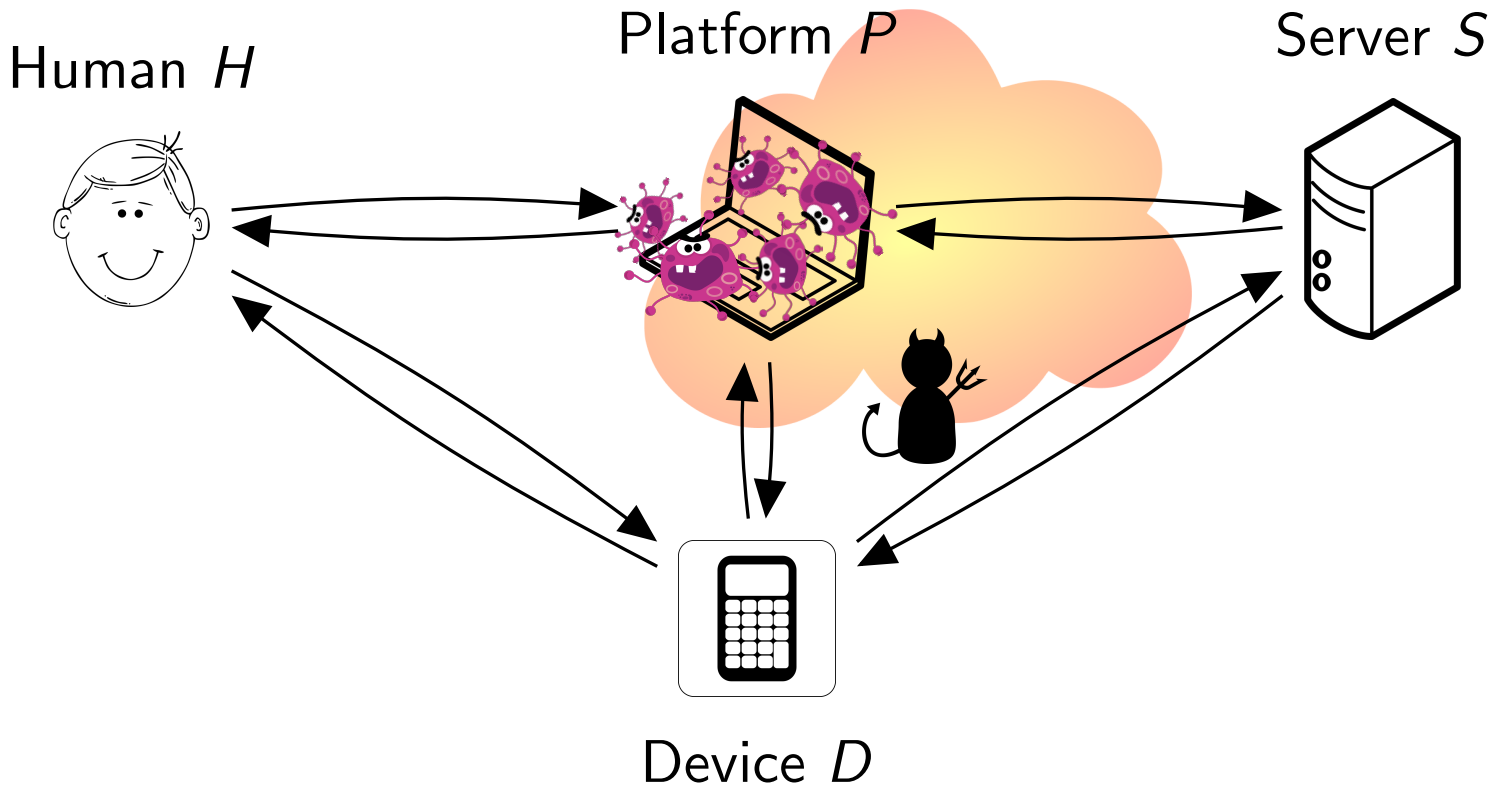
People's capabilities are limited



No useful, secure communication possible



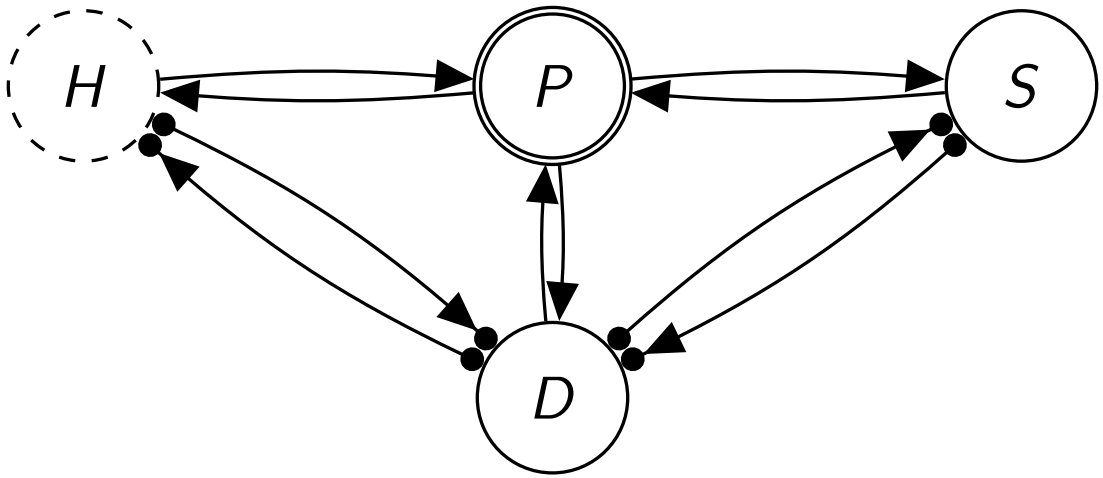
Trusted device necessary



Trusted device necessary

E.g.:





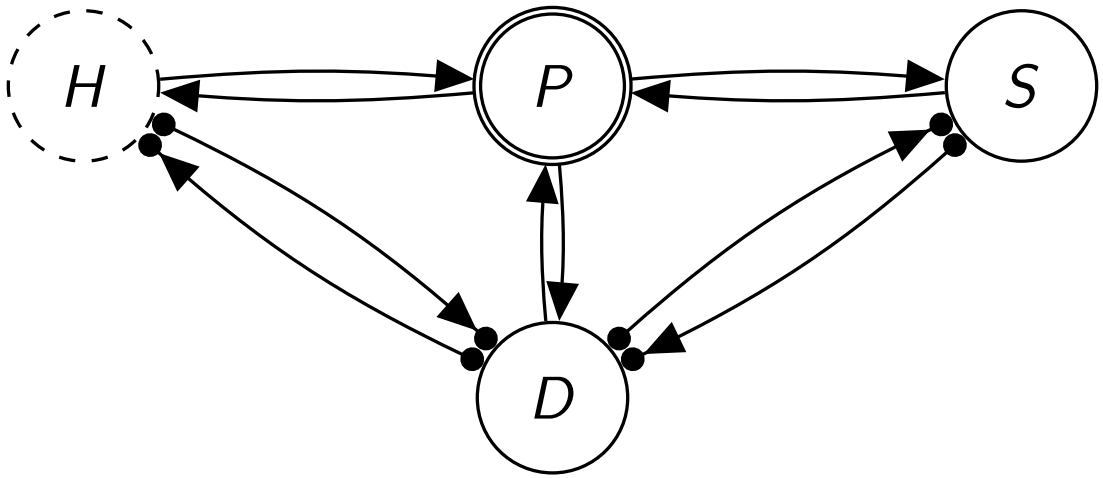
Node Properties:

- honest, unrestricted
- dishonest, unrestricted
- honest, restricted to pairing, projection

Link Properties:

- $\rightarrow$ insecure channel
- $\bullet\!\!\rightarrow\!\!\bullet$ secure channel

Human Interaction Security Protocols (HISP) Topology



Node Properties:

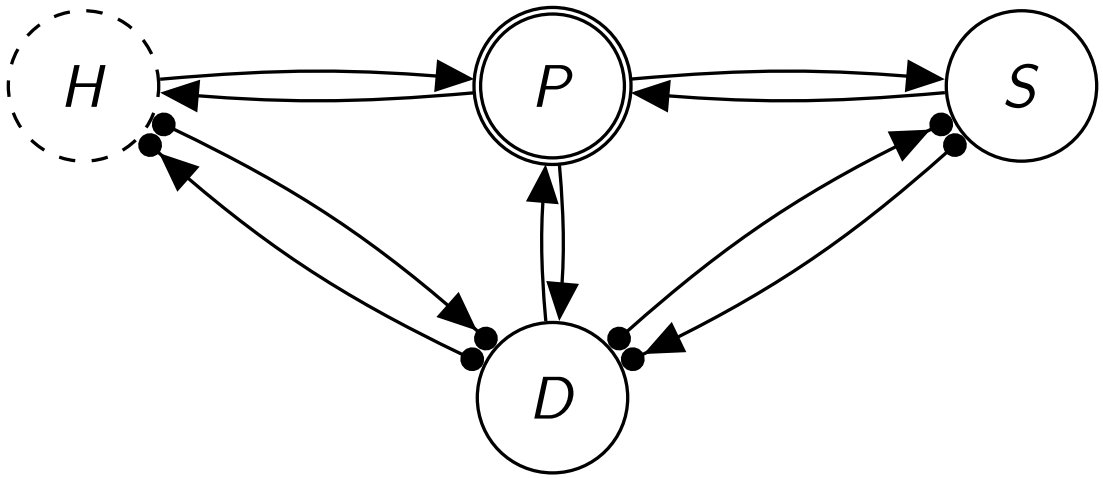
- honest, unrestricted
- dishonest, unrestricted
- honest, restricted to pairing, projection

Link Properties:

- $\rightarrow$ insecure channel
- $\bullet\!\!\rightarrow\!\!\bullet$ secure channel

A HISP topology is a subgraph of the above graph.

Human Interaction Security Protocols (HISP) Topology



Node Properties:

- honest, unrestricted
- dishonest, unrestricted
- honest, restricted to pairing, projection

Link Properties:

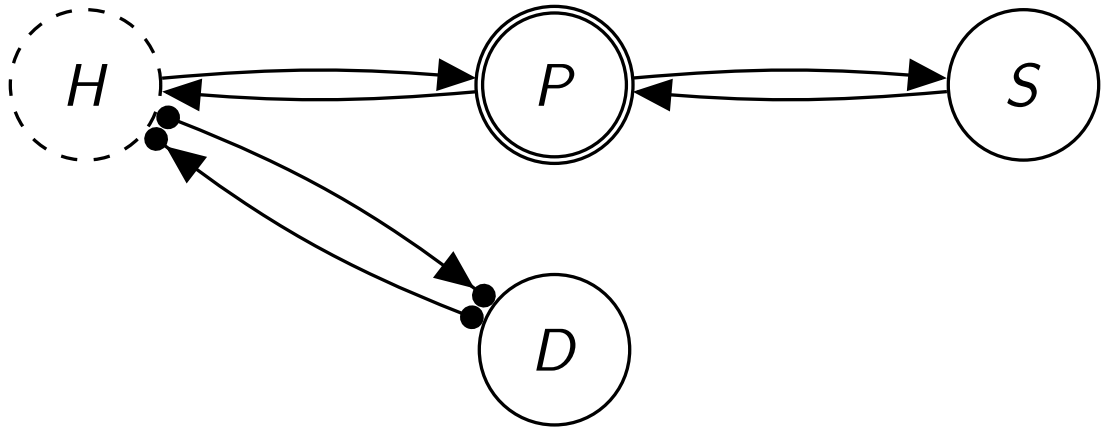
- $\rightarrow$ insecure channel
- $\bullet\!\!\rightarrow\!\!\bullet$ secure channel

A HISP topology is a subgraph of the above graph.
It represents assumptions about

- protocol participants' abilities and their trustworthiness,
- available communication links and their security properties.

Example

Online banking scenario with smart card reader (chip TAN)



Node Properties:

- honest, unrestricted
- dishonest, unrestricted
- honest, restricted to pairing, projection

Link Properties:

- $\rightarrow$ insecure channel
- $\bullet\!\!\rightarrow\!\!\bullet$ secure channel

Is secure communication from H to S possible in this topology?

Formal Model

- To reason about possibility of secure communication channels between H and S we need a security protocol model.
- Our model is based on existing security protocol model (Tamarin prover).

Our extensions:

- Authentic, confidential, and secure channel rules.
- Dishonest agent rules.
- Definitions of HISP security properties.

Security Properties (1/2)

Security properties are composed of existential and universal predicates over traces.

E.g., a protocol provides a confidential channel, if

(1) $\exists$ trace: S sends message m and R receives m.

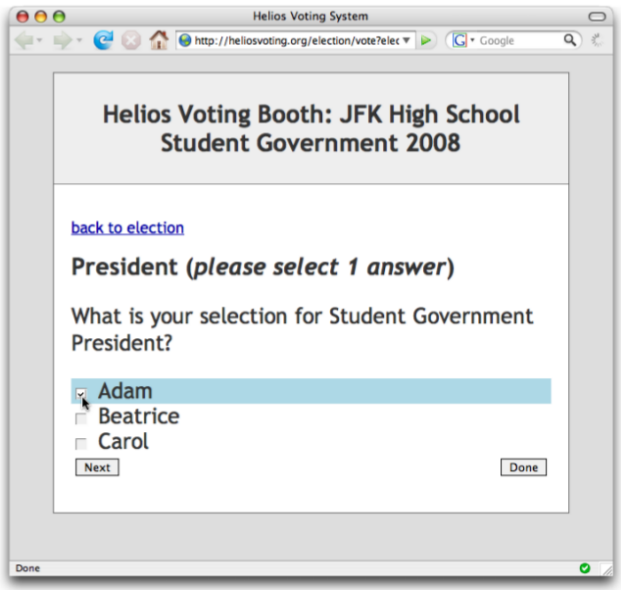
(2) $\forall$ traces: if S sends message m to R then m is not known to adversary.

Condition (1) eliminates trivial protocols. E.g., confidentiality of messages that are never communicated.

Security Properties (2/2)

We distinguish between restricted and unrestricted communication.

Example:

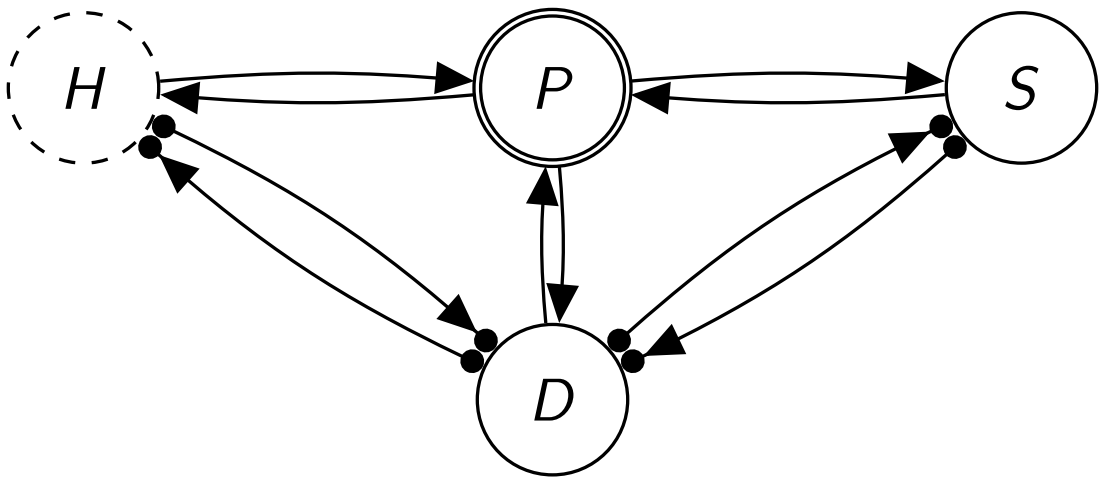


sending a yes/no vote to server
(e.g., secure channel)

sending an (e-)mail
(e.g., originating secure channel)

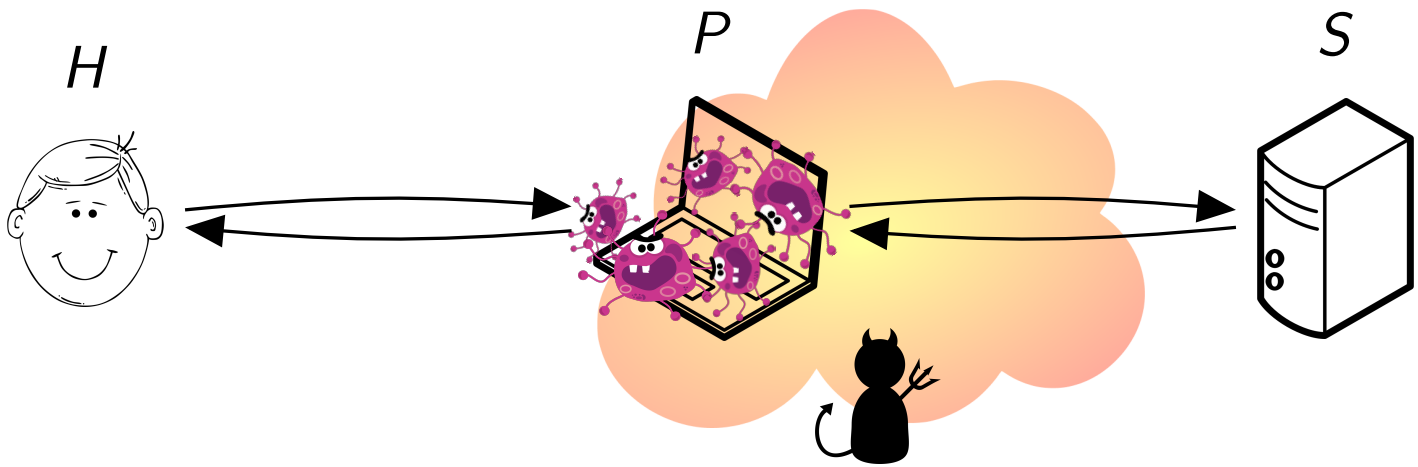
Characterization of Secure Human-Server Communication

In which subgraphs is secure communication from H to S possible?



Obvious, necessary condition: Need a path from H to S.

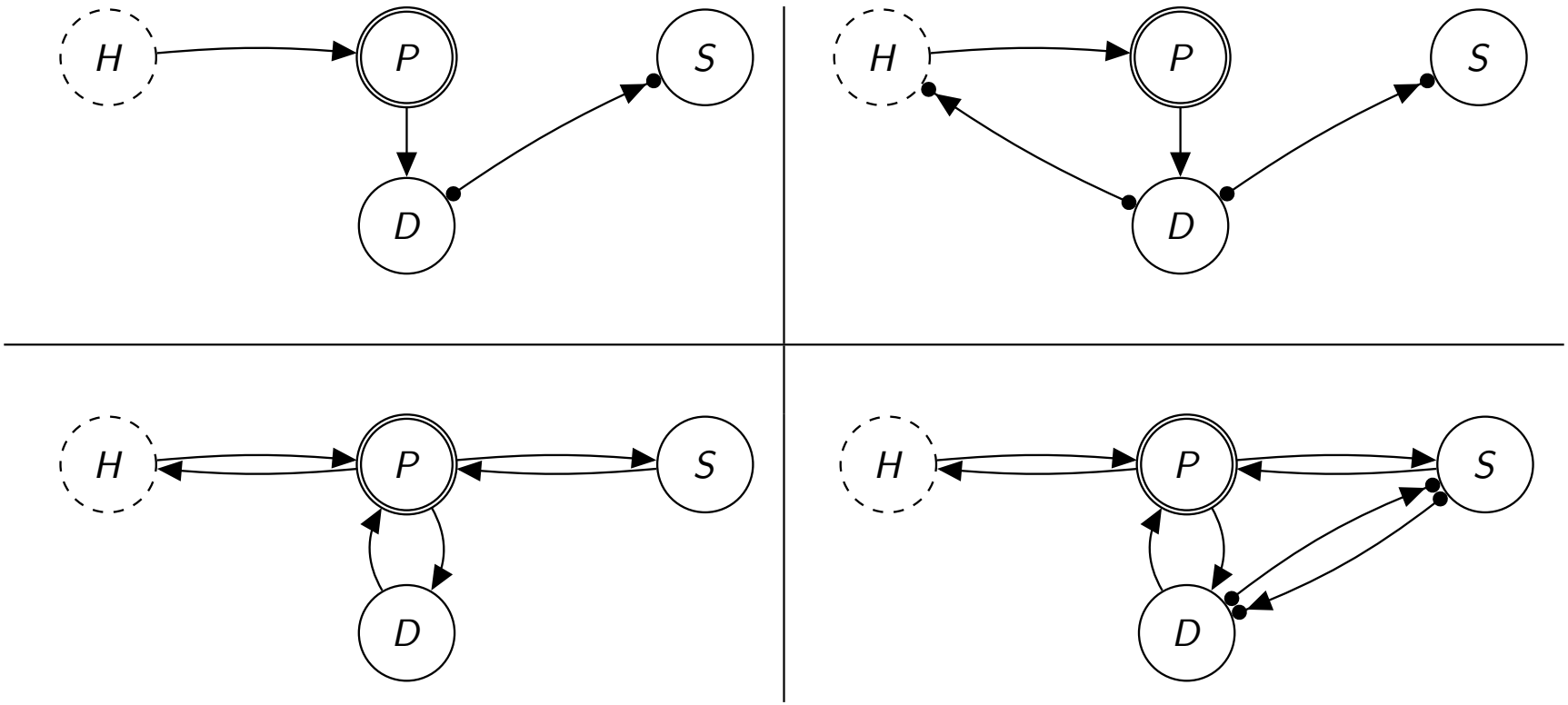
Impossibility Results: Paper & Pencil Proofs



Lemma: If H has no initial knowledge, secure communication between H and S over insecure channels is impossible.

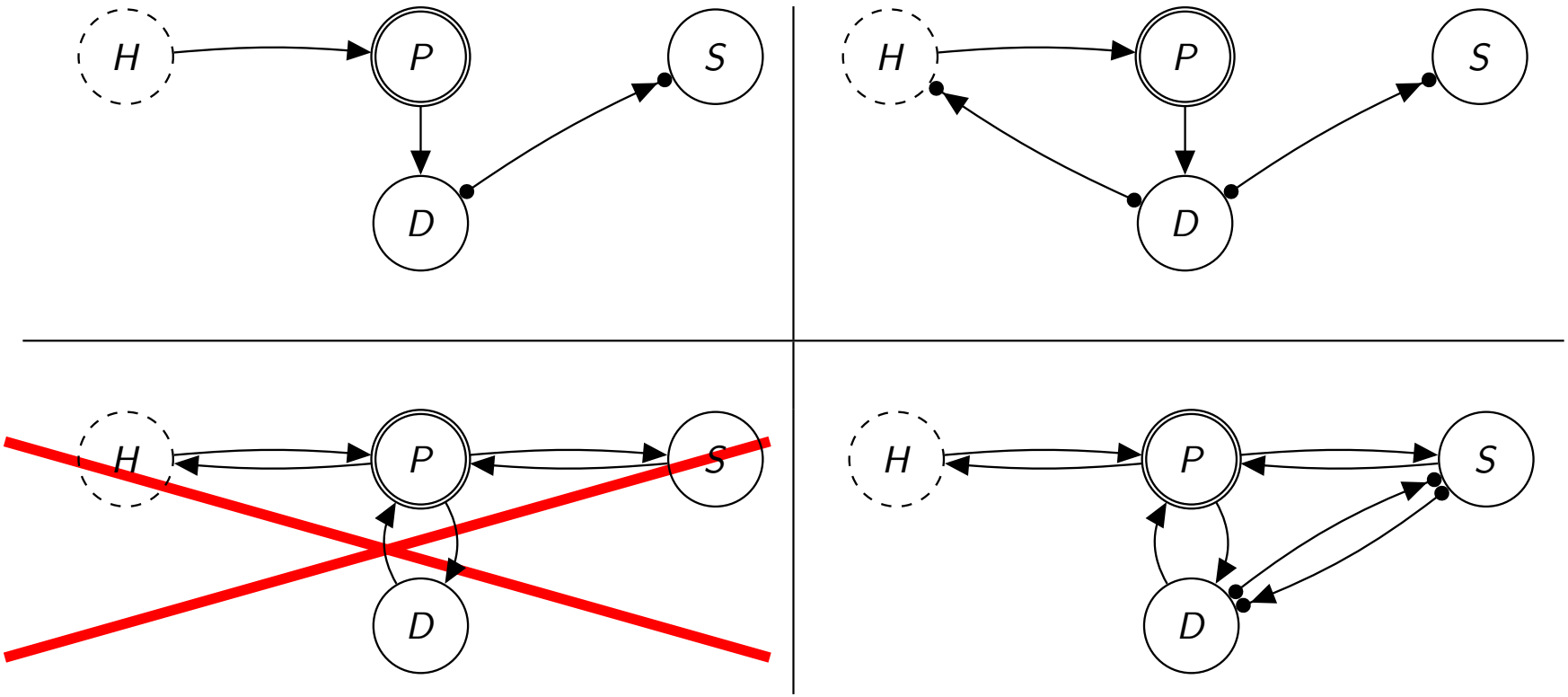
Example

Assume H has no initial knowledge. Which of these topologies allow for secure communication from H to S?



Example

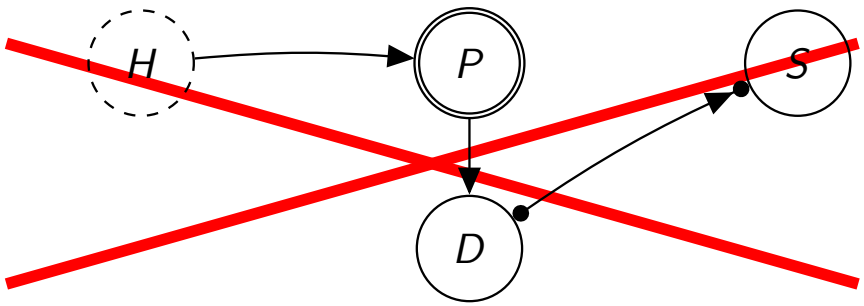
Assume H has no initial knowledge. Which of these topologies allow for secure communication from H to S?



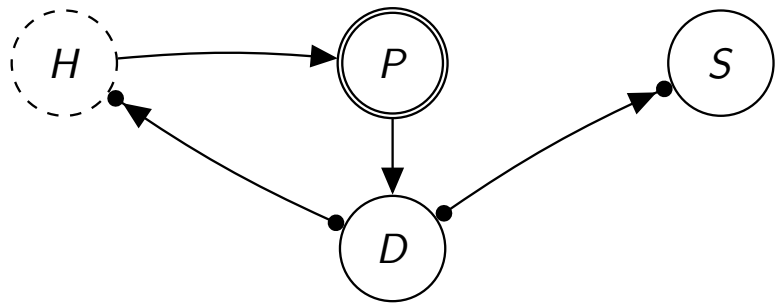
By Lemma

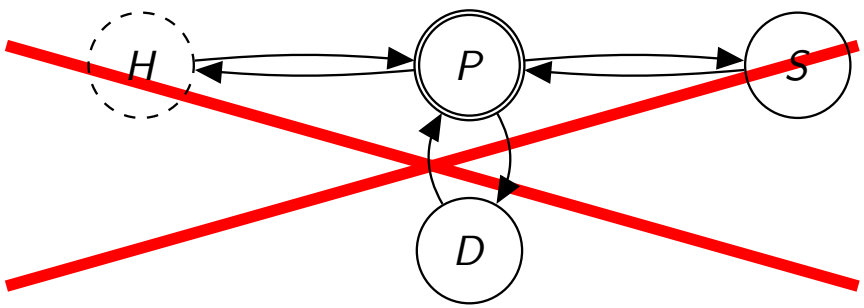
Example

Assume H has no initial knowledge. Which of these topologies allow for secure communication from H to S?

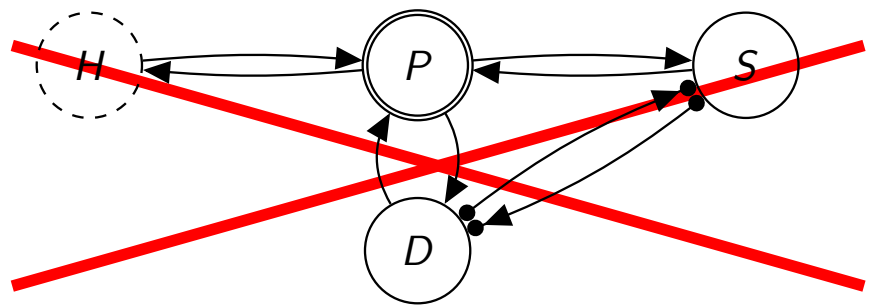


By Lemma + contraction argument



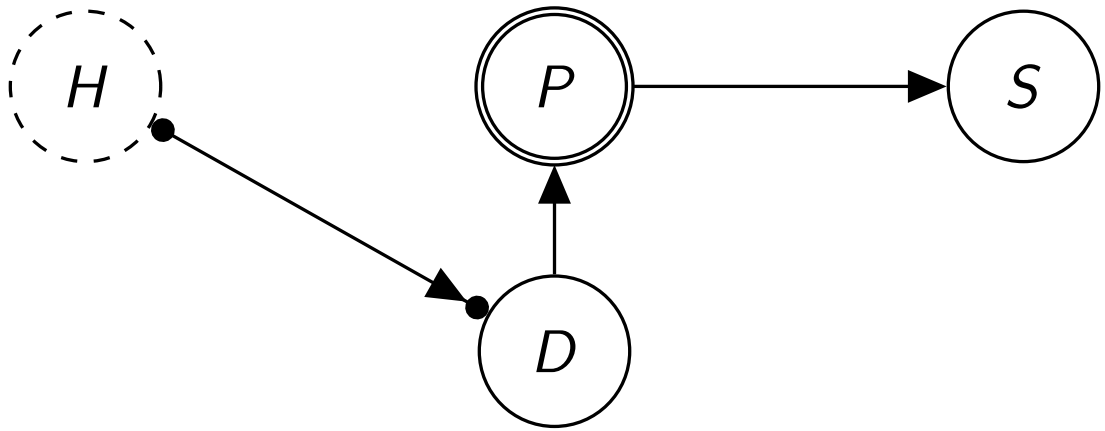


By Lemma



By Lemma + contraction argument

Possibility Results: Explicit Constructions

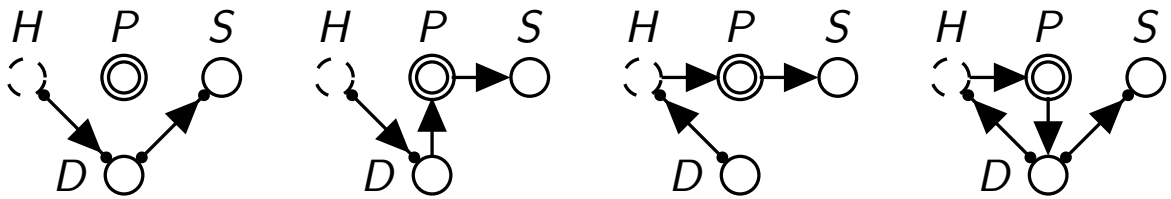


0.	D:	$\mathsf{knows}(S, k)$
0.	S:	$\mathsf{knows}(D, k)$
1.	$H \bullet\!\!\rightarrow\!\!\bullet\ D$:	$\mathsf{fresh}(m).\ \langle S, m\rangle$
2.	$D \rightarrow P$:	$\{\langle H, m\rangle\}_k$
3.	$P \rightarrow S$:	$\{\langle H, m\rangle\}_k$

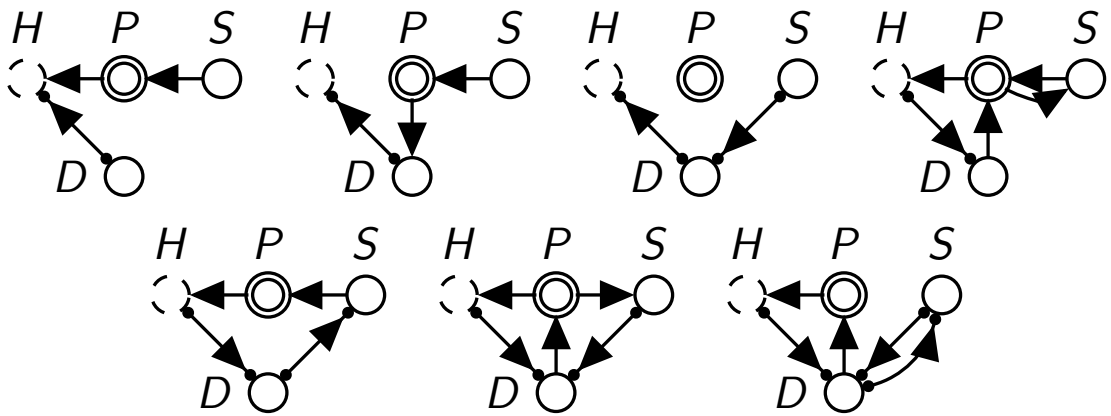
Security properties of all constructions are verified with Tamarin prover.

Minimal HISP Topologies for Secure Communication*

Secure Channel from Human to Server:



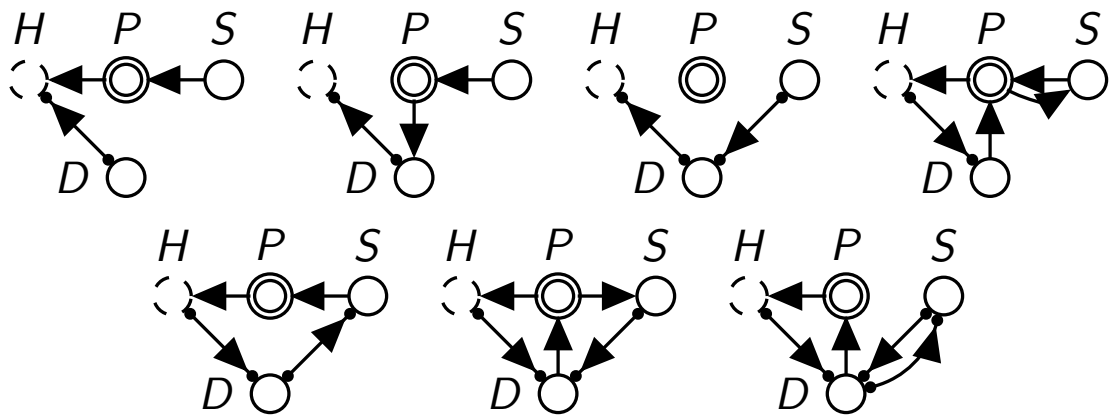
Secure Channel from Server to Human:



*H has no initial knowledge.

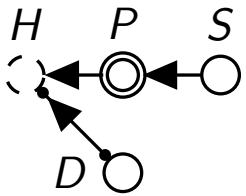
Example: Guided Design of Secure Protocols

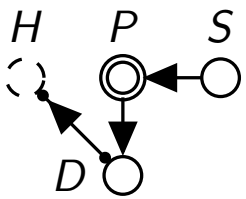
Problem: Communicate medical test results from S to H.
P must not learn the test results.

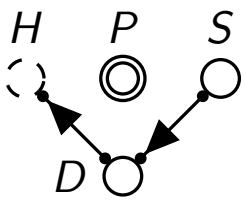


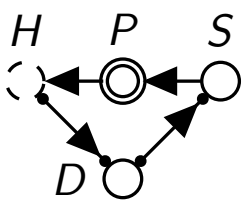
Example: Guided Design of Secure Protocols

Problem: Communicate medical test result from S to H.



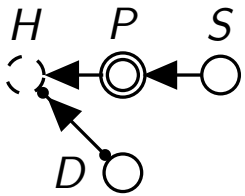


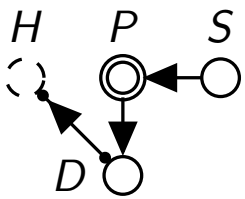


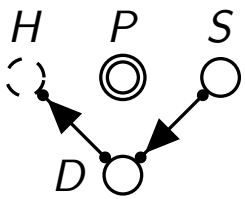


Example: Guided Design of Secure Protocols

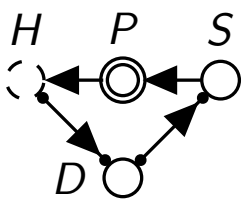
Problem: Communicate medical test result from S to H.





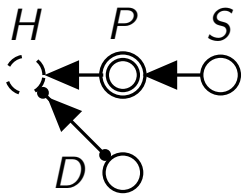


Results sent to H by postal mail.

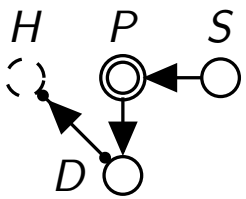


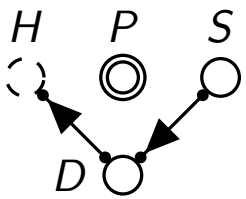
Example: Guided Design of Secure Protocols

Problem: Communicate medical test result from S to H.

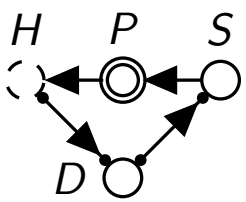


Code sheet D generated and given to H in testing facility.



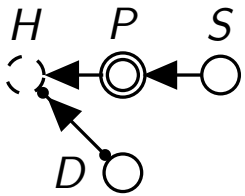


Results sent to H by postal mail.

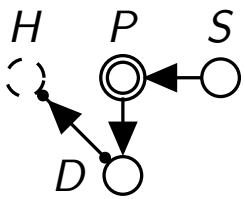


Example: Guided Design of Secure Protocols

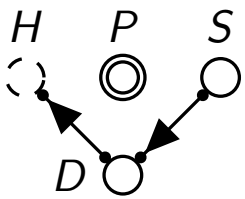
Problem: Communicate medical test result from S to H.



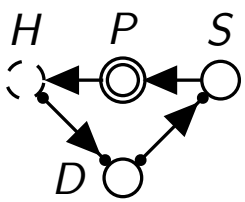
Code sheet D generated and given to H in testing facility.



As above, with visual cryptography transparencies.

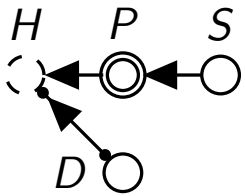


Results sent to H by postal mail.

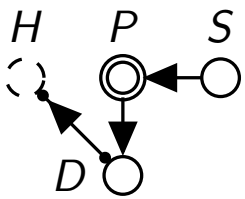


Example: Guided Design of Secure Protocols

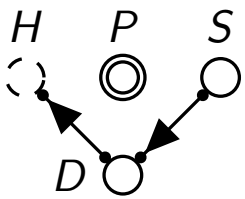
Problem: Communicate medical test result from S to H.



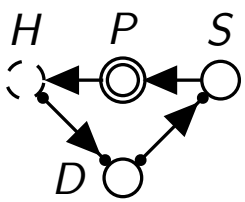
Code sheet D generated and given to H in testing facility.



As above, with visual cryptography transparencies.



Results sent to H by postal mail.



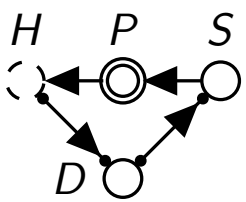
Mail-in testing kit, returned with code words supplied by H on a form.

Future Work

- Guided protocol design:
  1. What is the "most secure" channel achievable for a given arbitrary communication topology?
  2. How to construct such a protocol automatically?

Future Work

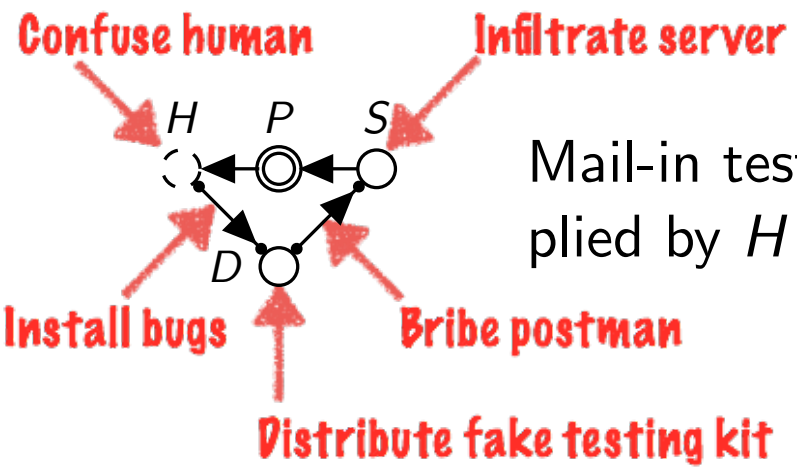
- Guided protocol design:
  1. What is the "most secure" channel achievable for a given arbitrary communication topology?
  2. How to construct such a protocol automatically?
- Attack-surface analysis:
  E.g.:



Mail-in testing kit, returned with code words supplied by H on a form.

Future Work

- Guided protocol design:
  1. What is the "most secure" channel achievable for a given arbitrary communication topology?
  2. How to construct such a protocol automatically?
- Attack-surface analysis:
  E.g.:

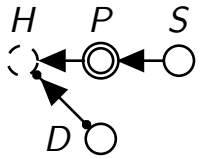


Mail-in testing kit, returned with code words supplied by H on a form.

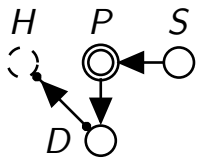
Conclusion

- HISP communication topology models human, dishonest computing platform, trusted device, and remote server.
- Our complete characterization of HISP topologies provides necessary and sufficient conditions for secure human-server communication.
- Characterization is relevant for practical applications such as online banking and Internet voting.
- Allows quick plausible security assessment of protocol designs.
- Can be used to guide the design of novel protocols.

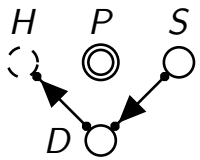
Guided Design Example



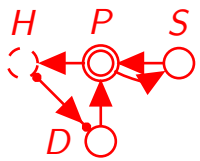
Code sheet D generated and given to H in testing facility.



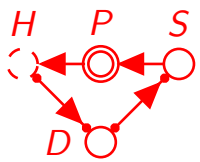
As above, with visual cryptography transparencies.



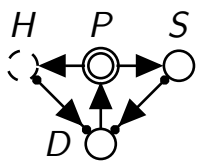
Results sent to H by postal mail.



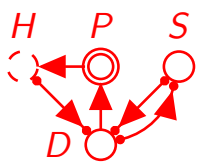
Use code words supplied by H, signed and encrypted by D.



Mail-in testing kit, returned with code words supplied by H on a form.

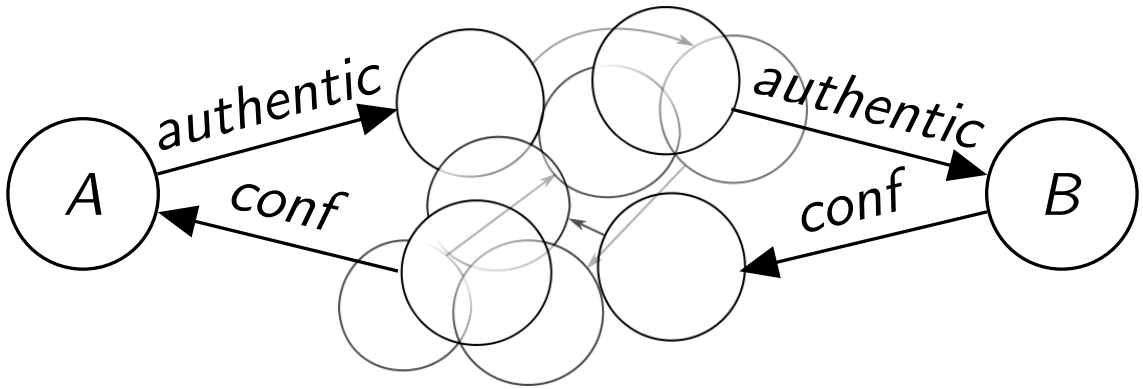


Signed and encrypted code words, results on USB stick or paper with QR code.



Mail-in testing kit, results on USB stick or paper with QR code.

Example of an Impossibility Result



Lemma

There is no protocol providing a confidential channel from A to B in any communication topology where $A \neq B$ and

- *A or B has empty initial knowledge,*
- *A's outgoing links are authentic, incoming links are confidential,*
- *B's incoming links are authentic, outgoing links are confidential.*

Related Work

- Ellison, Security Ceremonies, 2003.
- Bella and Coles-Kemp extend security ceremonies with socio-technical elements such as a human agent's belief system and cultural values. Focus on methodology to represent protocol's environment and context.
- Meadows and Pavlovic propose a "logic of moves" and analyze physical airport security procedures.
- Carlos, Martina, Price, and Custódio have studied Bluetooth pairing ceremony under different adversary models.
- Mödersheim and Viganò have formalized authentic, confidential, secure channels in an "ideal channel model", implemented using asymmetric cryptography.