Understanding the weaknesses of human-protocol interaction

Marcelo C. Carlos
Geraint Price
{*marcelo.carlos.2009, geraint.price*}*@rhul.ac.uk*

Information Security Group
Royal Holloway University of London

2 March 2012

Royal Holloway University of London

Information Security Group

Contents

Motivation

Motivation

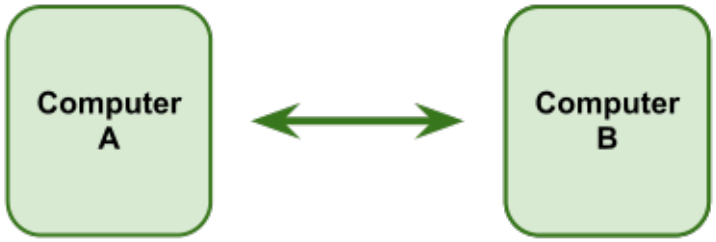
- Protocol design and analysis is a well developed research area
- When protocols are implemented, some of them fail to provide the expected security properties

Motivation

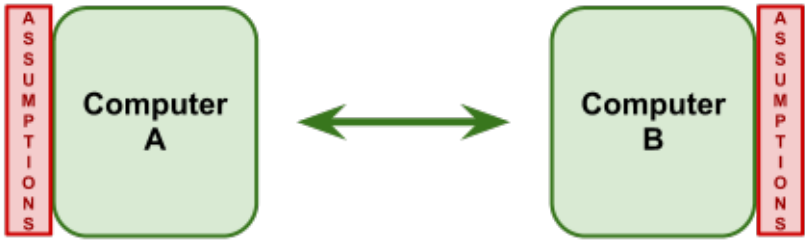
- Protocol design and analysis is a well developed research area
- When protocols are implemented, some of them fail to provide the expected security properties

Why?

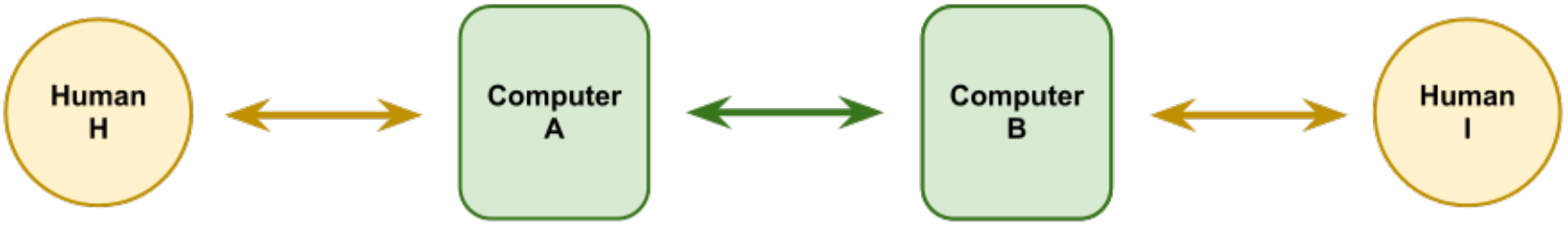
Security Protocols / Ceremonies



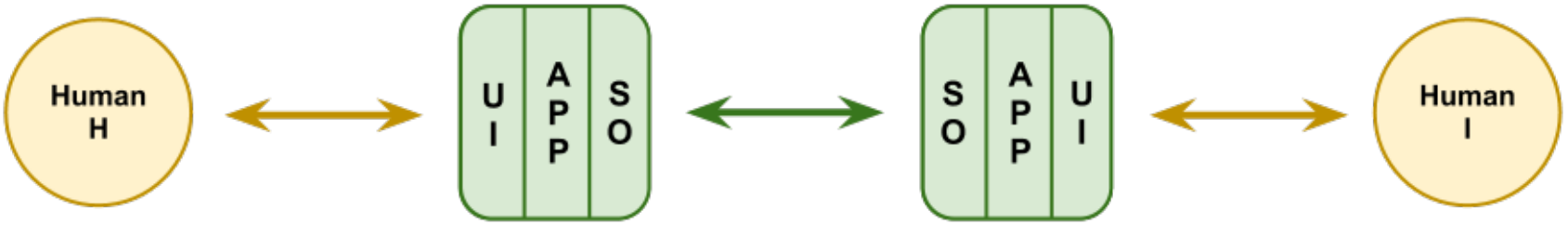
Security Protocols / Ceremonies



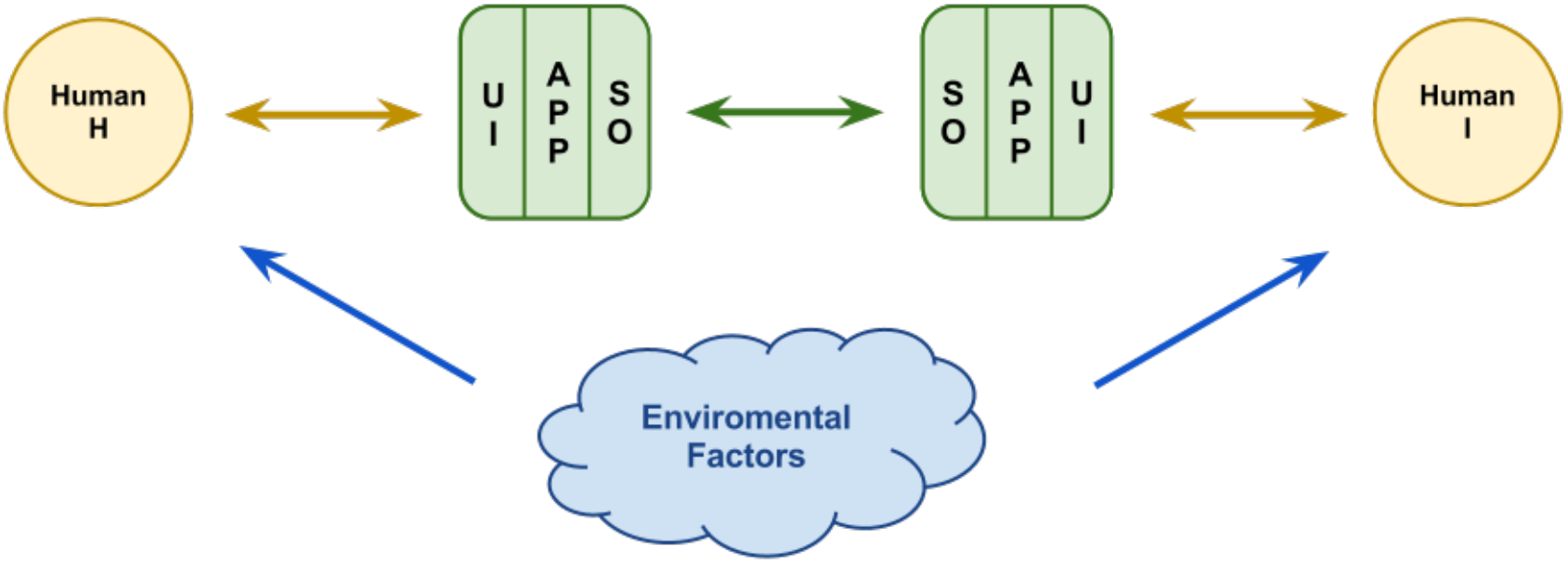
Security Protocols / Ceremonies



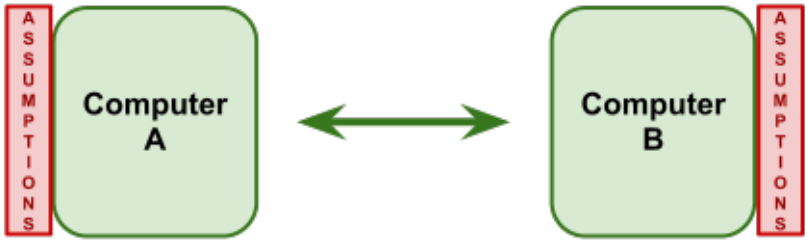
Security Protocols / Ceremonies



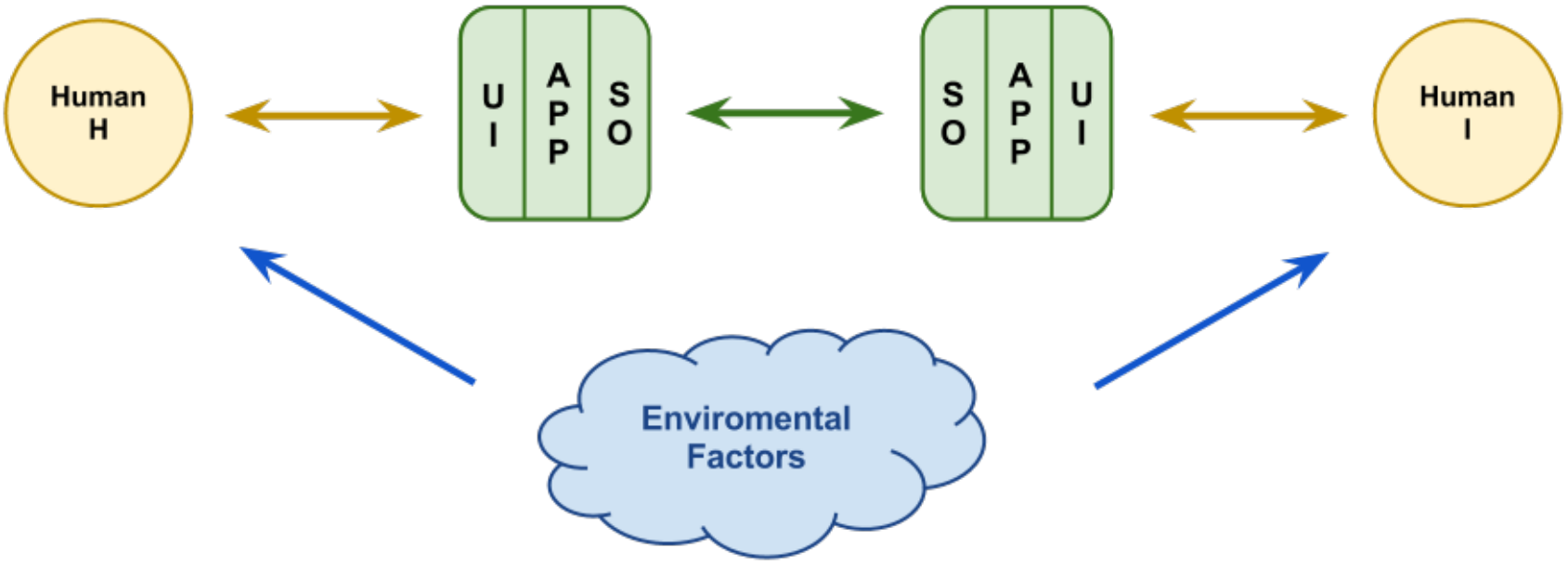
Security Protocols / Ceremonies



Security Protocols / Ceremonies



Security Protocols / Ceremonies



We need to understand why protocols fail when put in practice!

Taxonomy of overlooked components of human-protocol interaction

Taxonomy of overlooked components of human-protocol interaction

- Thorough review of existing research
  - Theoretical research
  - Experiments
  - Empirical research
- We found 5 main components that could be exploited by attackers in implemented protocols

Taxonomy of overlooked components of human-protocol interaction

- 5 components:
  - User Knowledge
  - Authentication Capabilities
  - Decision making influencing factors
  - Bounded Attention
  - Inherent Characteristics

Taxonomy of overlooked components of human-protocol interaction

- User Knowledge:
  - Lack of knowledge of computing
  - Lack of knowledge of security
  - Lack of knowledge of security threats
  - Inaccurate mental models

Taxonomy of overlooked components of human-protocol interaction

- Authentication capabilities:
  - Users are good at authenticating people they know
  - Users are not good at authenticating objects
  - Users are not good at authenticating strangers
  - Users are not good at authenticating digital objects

Taxonomy of overlooked components of human-protocol interaction

- Factors influencing decision making:
  - Social conditioning
  - User's principles
  - Time constraints
  - Shared risk
  - Fear

Taxonomy of overlooked components of human-protocol interaction

- Bounded Attention:
  - Lack of attention to security
  - Lack of attention to the absence of security
  - Security in a secondary workflow
  - Conditioning

Taxonomy of overlooked components of human-protocol interaction

- Inherent human characteristics:
  - Memory limitations
  - Lapses and Slips
  - Problem solving limitations
  - Task termination
  - Non-deterministic behaviour

Design Recommendations

Design Recommendations

- From the taxonomy of overlooked components, we built a set of design recommendations
- It is not a direct mapping (one component to one recommendation)
- Some factors, even belonging to the same category in the taxonomy, have to be treated in different ways
  - The opposite situation was also found, when factors from different weaknesses could be handled in a similar manner
- In fact, almost all of components are linked to two or more recommendations.
  - This happens due to the internal subdivision of each component
  - In many cases, sub-components of the same taxonomy item had to be treated differently

Design Recommendations

- 5 design recommendations:
  - Do not give users an unfeasible task
  - Do not rely on users' authentication capabilities
  - Integrate security into the main workflow
  - Consider that the expected behaviour might change under different circumstances
  - Design should prevent a user from performing an inappropriate interaction

Design Recommendations

- Do not give users an unfeasible task:
  - Consider users' skills and knowledge when designing an interaction
  - The more generic the target users are, the lower the level of understanding and skills should be required
  - Whenever possible, avoid using user input as a main component of the establishment of security properties of a protocol

Design Recommendations

- Do not rely on users' authentication capabilities:
  - Do not ask users to authenticate objects
  - Do not ask users to authenticate unknown people
  - Verify if the authentication task requires specific knowledge. If so, check whether the target audience is sufficiently capable to perform this task

Design Recommendations

- Integrate security into the main workflow:
  - Integrate security concerns into the main path of the users' tasks
  - Use active and interactive interruptions other than passive warnings
  - Whenever possible, infer authorisation from users' acts
  - Respect users' intentions

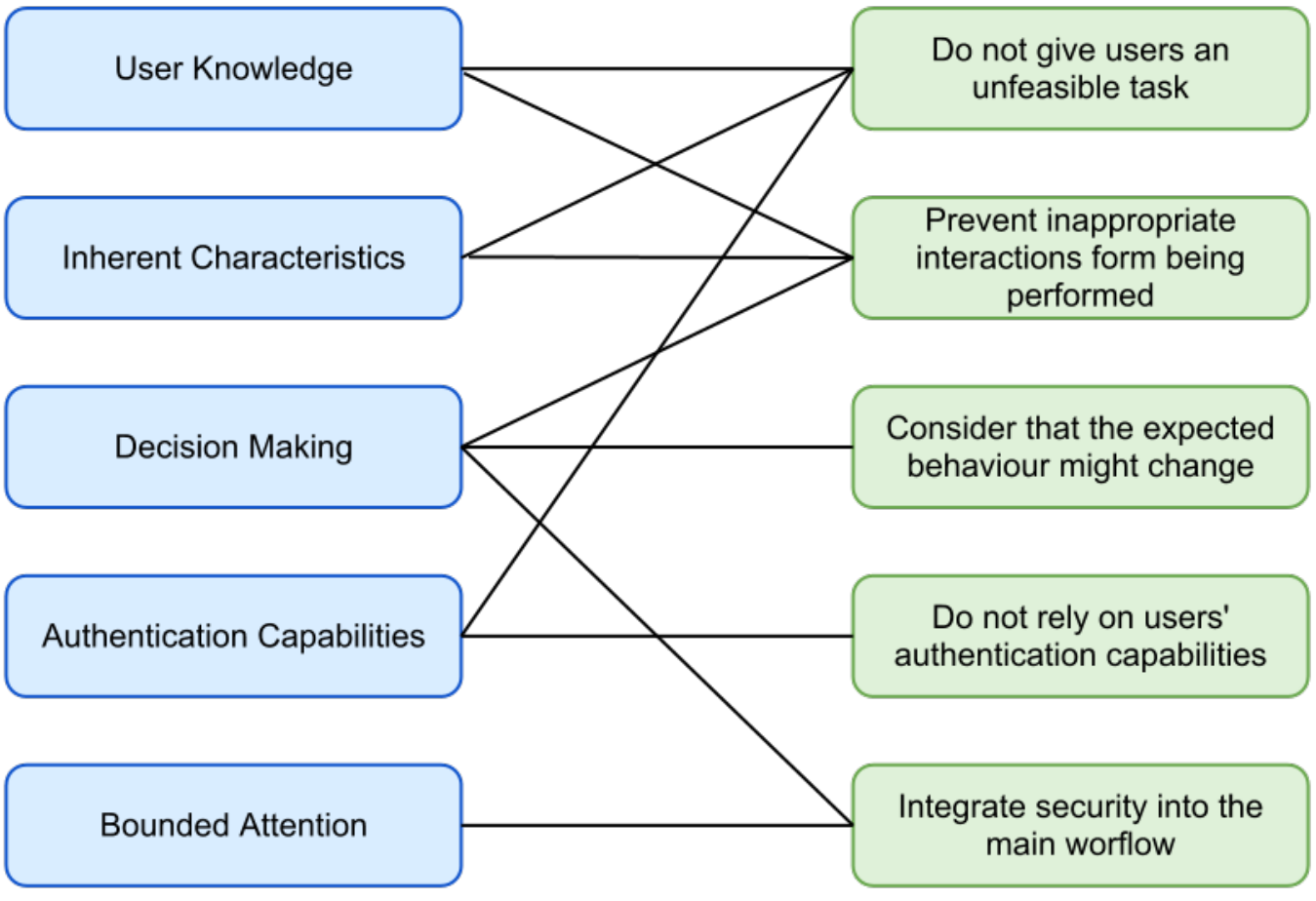
Design Recommendations

- Consider that the expected behaviour might change under different circumstances:
  - Do not assume that a user will always behave in the same (predictable) manner
  - Check whether a given decision might be taken differently under different conditions (e.g. time pressure)
  - Avoid asking users for decisions in situations where they might under influence of external factors
  - Whenever possible, make use of mechanisms that are immune or less likely to be affected by users' unexpected behaviour.

Design Recommendations

- Design should prevent a user from performing an inappropriate interaction
  - Always attempt to provide/enable only the safe options to users
  - Whenever possible, make use of forcing functions
    - Avoid drastic changes in the usability due to the use of forcing functions

Associations between the taxonomy and the design recommendations



Concluding remarks

Future work

- Further validation of the human-protocol interaction weaknesses and design recommendations against real world systems
- Detect how the taxonomy items affect each ceremony node
- Extend existing formal models for protocols to support the recommendations presented

Concluding remarks

- Many factors have to be taken into account when considering human-protocol interaction
- There is a wealth of research involving human behaviour analysis, but there is a lack of harmonisation regarding the definitions
- We propose a taxonomy of human-protocol interaction components, often overlooked, that merges different research findings into a well defined set
- From the taxonomy, we define a set of design recommendations to mitigate or reduce the security problems discussed

Thank you for your attention!