

Security and Usability: Analysis and Evaluation

Ronald Kainda, Ivan Flechais, and A.W. Roscoe

Oxford University Computing Laboratory

Availability, Reliability and Security (ARES) Conference
Krakow, Poland

18 February, 2010

Outline

- 1 Introduction
- 2 Security-usability threat model
- 3 Security and usability evaluation
- 4 Summary

Human-Computer Interaction (HCI)

Human-Computer Interaction (HCI)

- ...discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them (Source: SIGCHI, 1992)

Human-Computer Interaction (HCI)

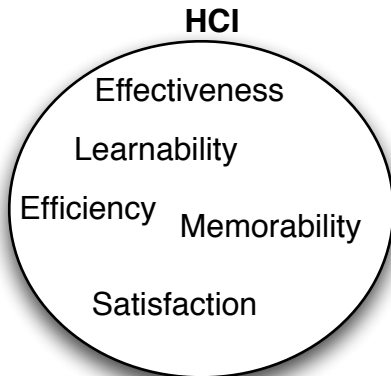
Human-Computer Interaction (HCI)

- ...discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them (Source: SIGCHI, 1992)

Usability

- The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (ISO 9241-11)

Human-Computer Interaction (HCI)



Human-Computer Interaction Security (HCISec)

Technical security

- Formal proofs
- Focus on malicious attacks
- Technical solutions typical

Human-Computer Interaction Security (HCISec)

Technical security

- Formal proofs
- Focus on malicious attacks
- Technical solutions typical

Effective security

- Secure systems are socio-technical (Sasse et al.)
- Humans forget, make mistakes
- Human failures are not covered by formal proofs

Human-Computer Interaction Security (HCISec)

Technical security

- Formal proofs
- Focus on malicious attacks
- Technical solutions typical

Effective security

- Secure systems are socio-technical (Sasse et al.)
- Humans forget, make mistakes
- Human failures are not covered by formal proofs

Human-Computer Interaction Security (HCISec)

- Focusses on the design, evaluation, and implementation of interactive secure systems.

Human-Computer Interaction Security (HCISec)

Security software properties (Whitten, '99)

- Secondary goal property

Human-Computer Interaction Security (HCISec)

Security software properties (Whitten, '99)

- Secondary goal property
- Hidden failure property

Human-Computer Interaction Security (HCISec)

Security software properties (Whitten, '99)

- Secondary goal property
- Hidden failure property
- Barn door property

Human-Computer Interaction Security (HCISec)

Security software properties (Whitten, '99)

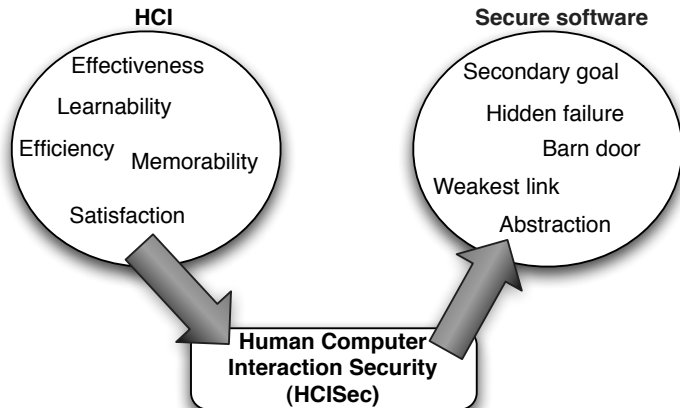
- Secondary goal property
- Hidden failure property
- Barn door property
- Weakest link property

Human-Computer Interaction Security (HCISec)

Security software properties (Whitten, '99)

- Secondary goal property
- Hidden failure property
- Barn door property
- Weakest link property
- Abstraction property

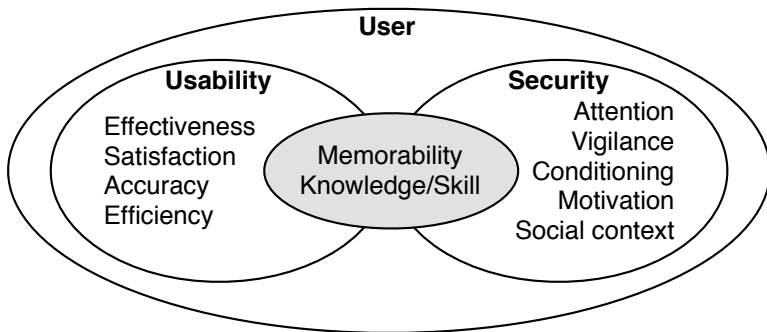
Human Computer Interaction Security (HCISec)



Analysis and evaluation of secure software

- What factors are crucial to usability analysis?
- What factors are crucial to security analysis?
- How do we use these factors for evaluating security and usability of secure systems?

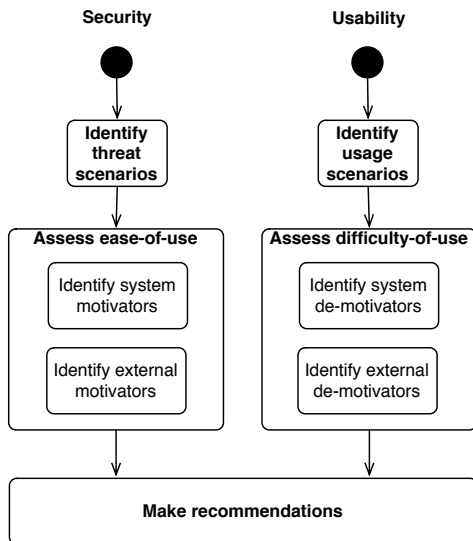
Security-usability threat model



Security measurable metrics

Factor	Metrics
Attention	Failures
Vigilance	Failures
Conditioning	Failures
Motivation	Perceived benefits, susceptibility, barriers, severity
Memorability	Recall
Knowledge/skill	Failures, mental models
Context	Impact of context

Process for security and usability evaluation



Make recommendations

- Usability factors
- Security factors
- Conflicting factors

Make recommendations

- Usability factors
- Security factors
- Conflicting factors

- NIST Risk-Level Matrix

Likelihood	Impact		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Summary and future work

Conclusion

- Secure systems have properties that differentiate them from other systems
- We propose a security-usability threat model
- A process for evaluating security and usability is also proposed
 - Threat scenarios
 - Usage scenarios
- Both internal and external factors may cause users to engage in insecure behaviours

Summary and future work

Conclusion

- Secure systems have properties that differentiate them from other systems
- We propose a security-usability threat model
- A process for evaluating security and usability is also proposed
 - Threat scenarios
 - Usage scenarios
- Both internal and external factors may cause users to engage in insecure behaviours

Future work

- Empirical validation
- Extend to malicious users
- Developing metrics for comparing different elements of a system

THANK YOU

ANY QUESTIONS?