How Does Usable Security (Not) End Up in Software Products?

Results From a Qualitative Interview Study

Marco Gutfleisch
Ruhr University Bochum
marco.gutfleisch@ruhr-uni-bochum.de

Jan H. Klemmer
Leibniz University Hannover
klemmer@sec.uni-hannover.de

Niklas Busch
CISPA Helmholtz Center
for Information Security
niklas.busch@cispa.de

Yasemin Acar
Paderborn University,
George Washington University,
yasemin.acar@uni-paderborn.de

M. Angela Sasse
Ruhr University Bochum
martina.sasse@ruhr-uni-bochum.de

Sascha Fahl
CISPA Helmholtz Center
for Information Security
sascha.fahl@cispa.de

RUHR UNIVERSITÄT BOCHUM RUB

Leibniz Universität Hannover

PADERBORN UNIVERSITY

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Funded by DFG Deutsche Forschungsgemeinschaft
German Research Foundation

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

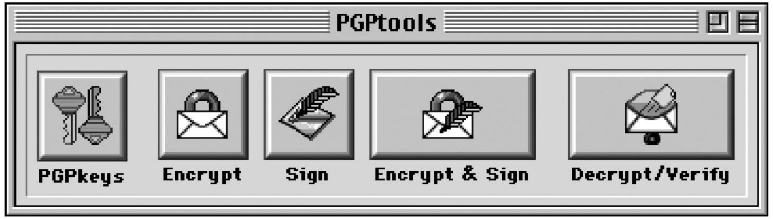
MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

CISPA

Motivation – Cryptography is Hard to Use

For more than 20 years:

Usable security problems with PGP [1]



Source: Whitten and Tygar [1]

And today?

0.06% encrypted emails [2]

→ Hard to use, low adoption!

[1] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in Proceedings of the 8th USENIX Security Symposium, Washington, D.C., 1999.
[2] C. Stransky, O. Wiese, V. Roth, Y. Acar and S. Fahl, "27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University," in Proceedings of the 43rd IEEE Symposium on Security and Privacy (SP'22), San Francisco, CA, US, 2022.

Motivation – Passwords and their Challenges

One of the oldest usable security fields and problems [3]

- Password re-use
- Written on post-its
- Too short
- Easily guessable
- …

→ Human factors impact security.

[3] A. Adams and M. A. Sasse, "Users Are Not the Enemy," Commun. ACM, vol. 42, no. 12, Art. no. 12, Dec. 1999.

Previous research showed…

To achieve effective security, security features need to be both *usable and secure.*

Lack of Usable Security Knowledge in Industry

Lots of research on usable security

Many insights, especially on end-user usable security

→ But: software still often has usable security issues!

What we did

Problem & Research Questions

It is unclear…

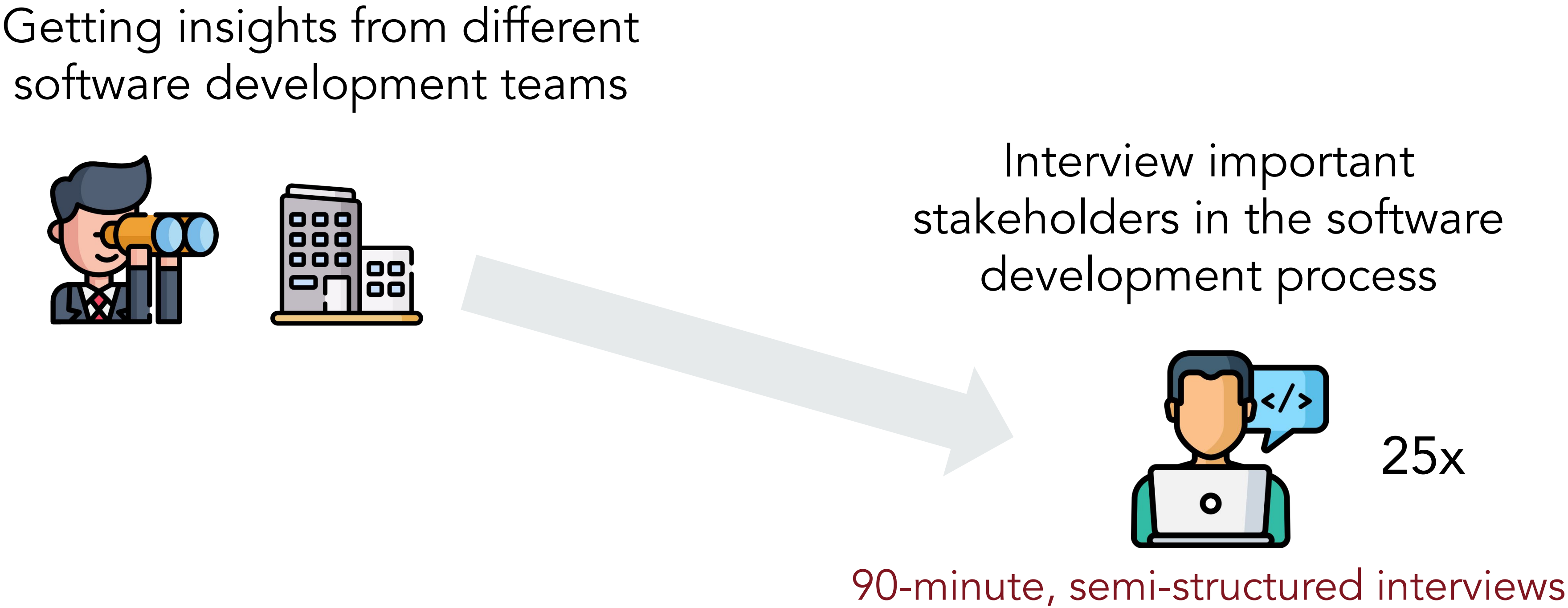
…whether companies/software teams take care of usable security.

…how processes for usable security look in the wild.

RQs:

1) Which factors in the software development process (SDP) and in companies influence usable security?
2) What are contributors and blockers for usable security in software development?
3) When and where in the SDP are important decisions made that influence usable security?

25 Interviews with Stakeholders



Getting insights from different software development teams

Interview important stakeholders in the software development process

25x

90-minute, semi-structured interviews

Marco Gutfleisch, Jan H. Klemmer, et al.

Interview Structure

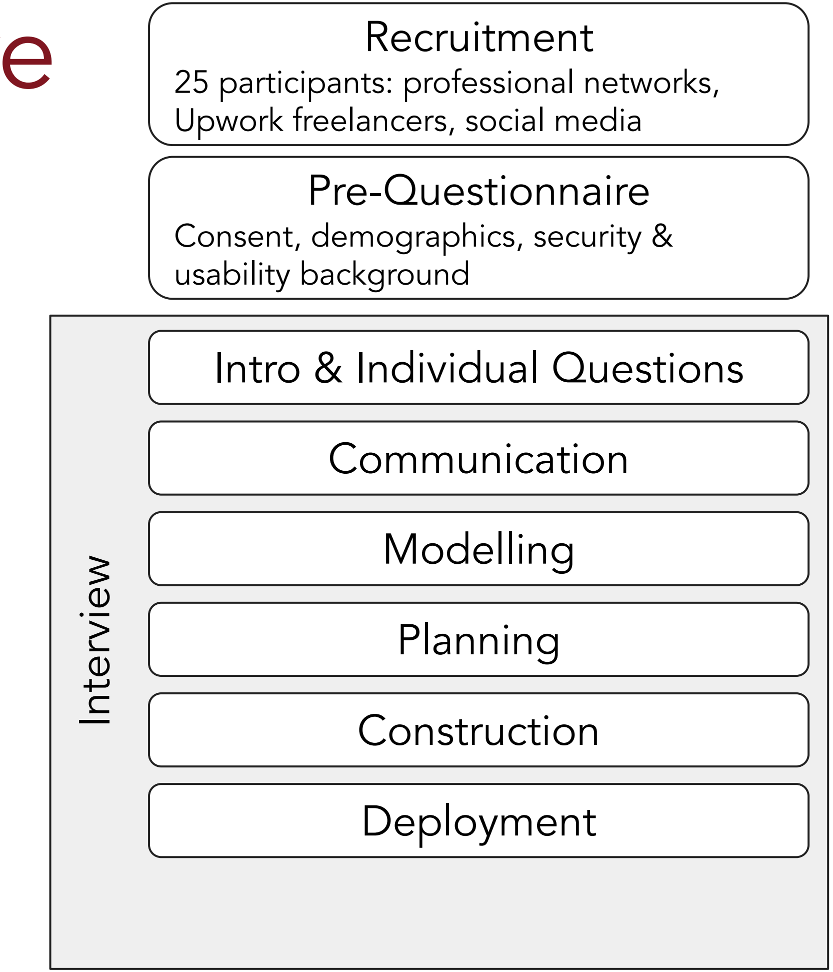
Recruitment

25 participants: professional networks, Upwork freelancers, social media

Pre-Questionnaire

Consent, demographics, security & usability background

Interview Structure



Recruitment

25 participants: professional networks, Upwork freelancers, social media

Pre-Questionnaire

Consent, demographics, security & usability background

Interview

Intro & Individual Questions

Communication

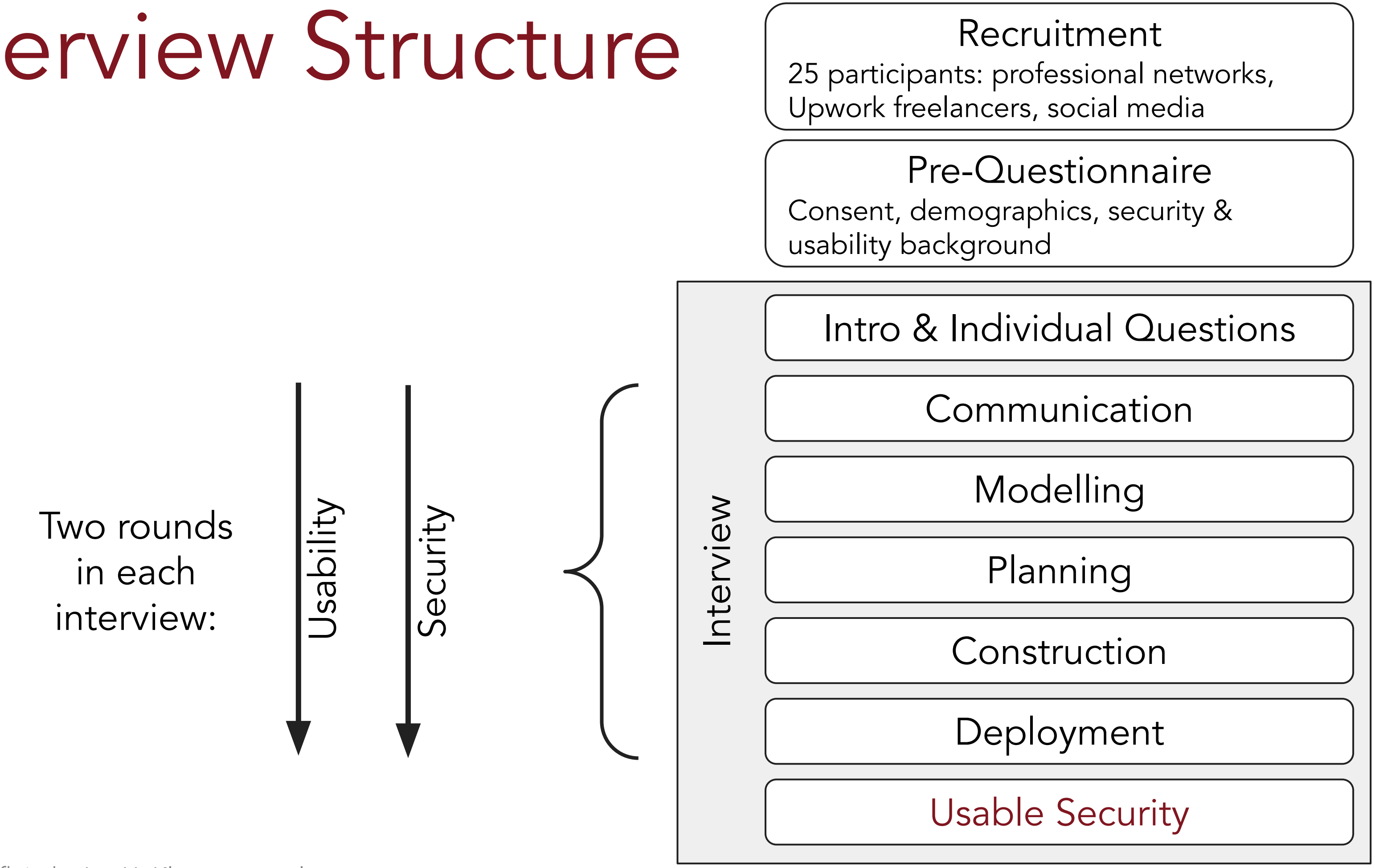
Modelling

Planning

Construction

Deployment

Interview Structure



Recruitment

25 participants: professional networks, Upwork freelancers, social media

Pre-Questionnaire

Consent, demographics, security & usability background

Interview

Intro & Individual Questions

Communication

Modelling

Planning

Construction

Deployment

Usable Security

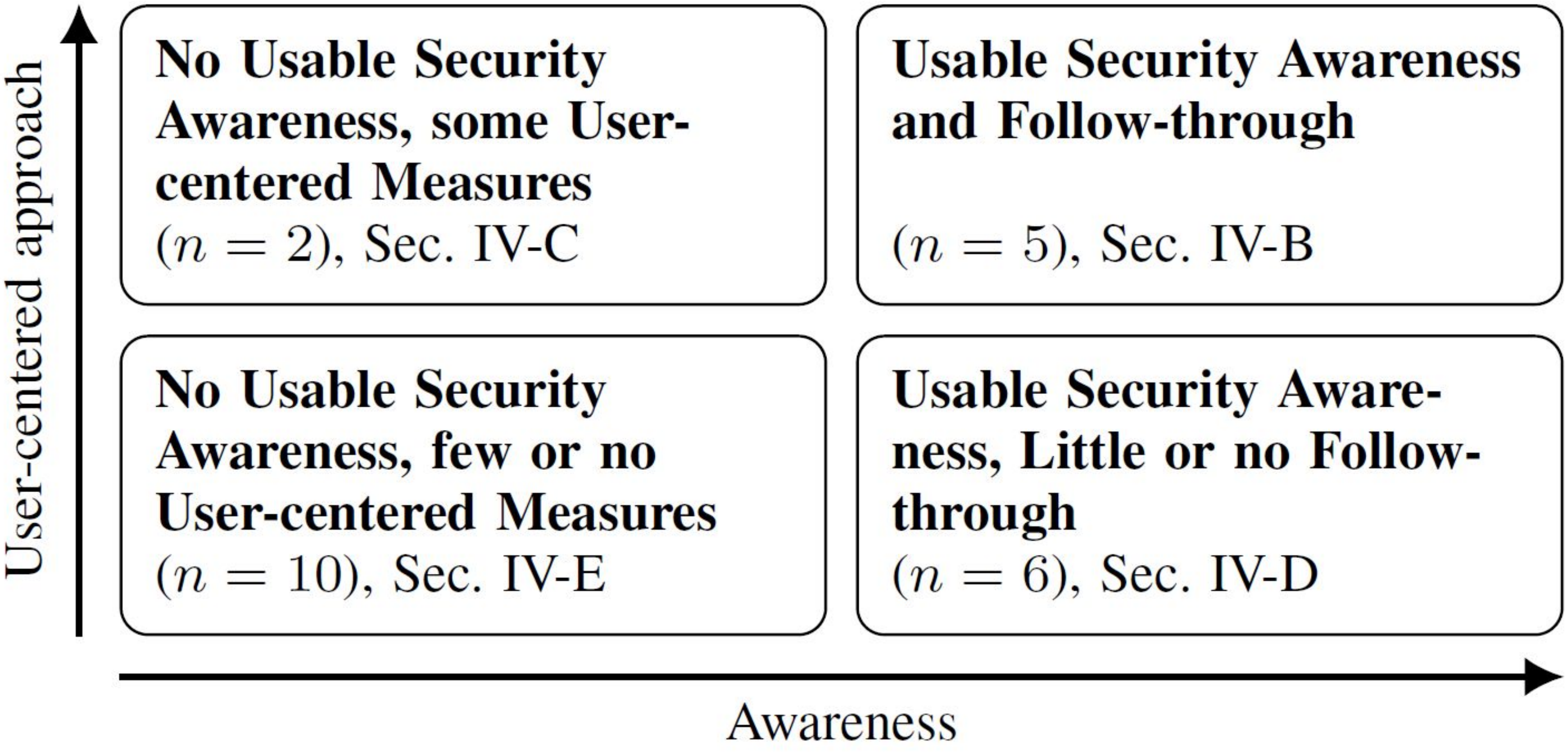
Two rounds in each interview:

Usability

Security

What we found

Key Findings



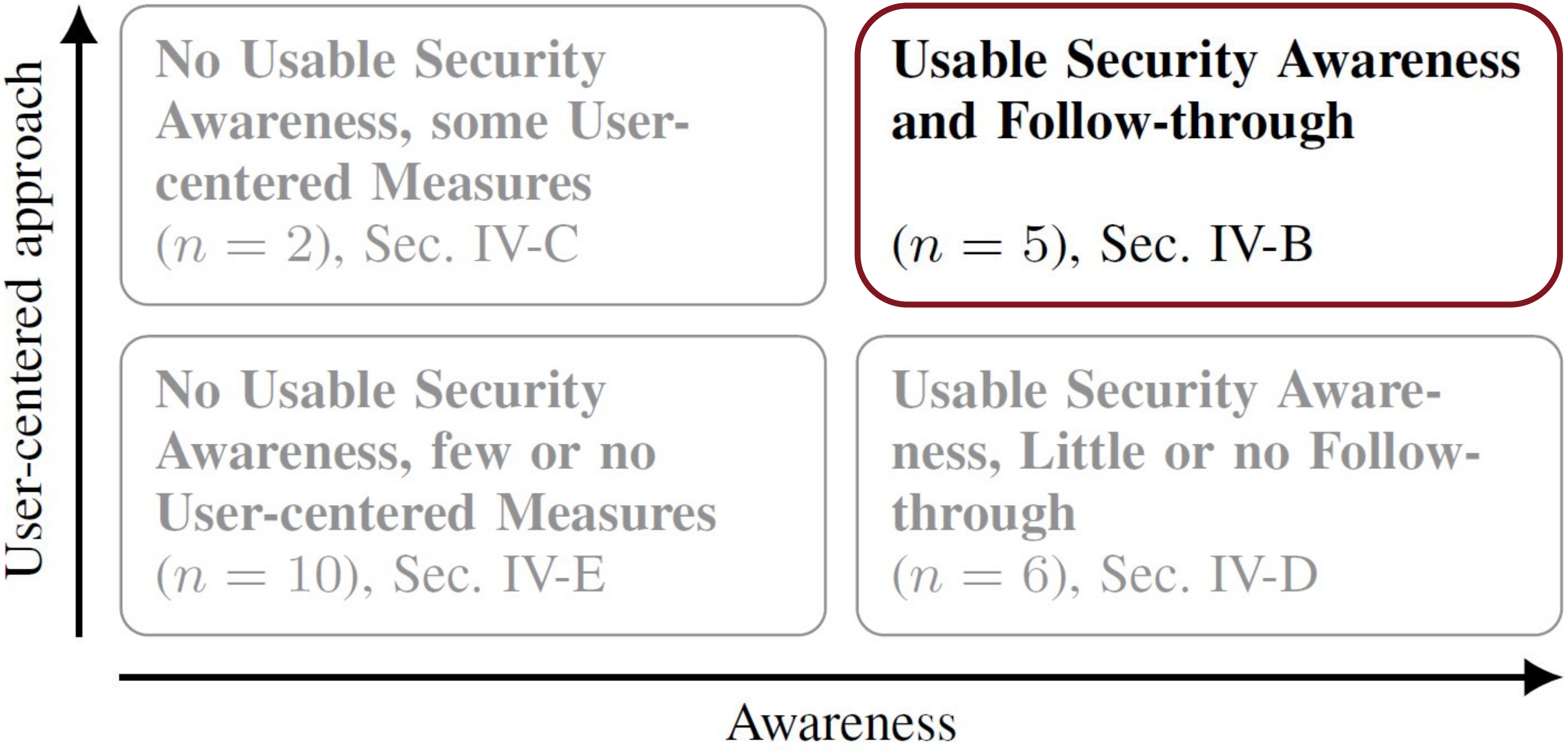
No Usable Security Awareness, some User-centered Measures
($n = 2$), Sec. IV-C

Usable Security Awareness and Follow-through
($n = 5$), Sec. IV-B

No Usable Security Awareness, few or no User-centered Measures
($n = 10$), Sec. IV-E

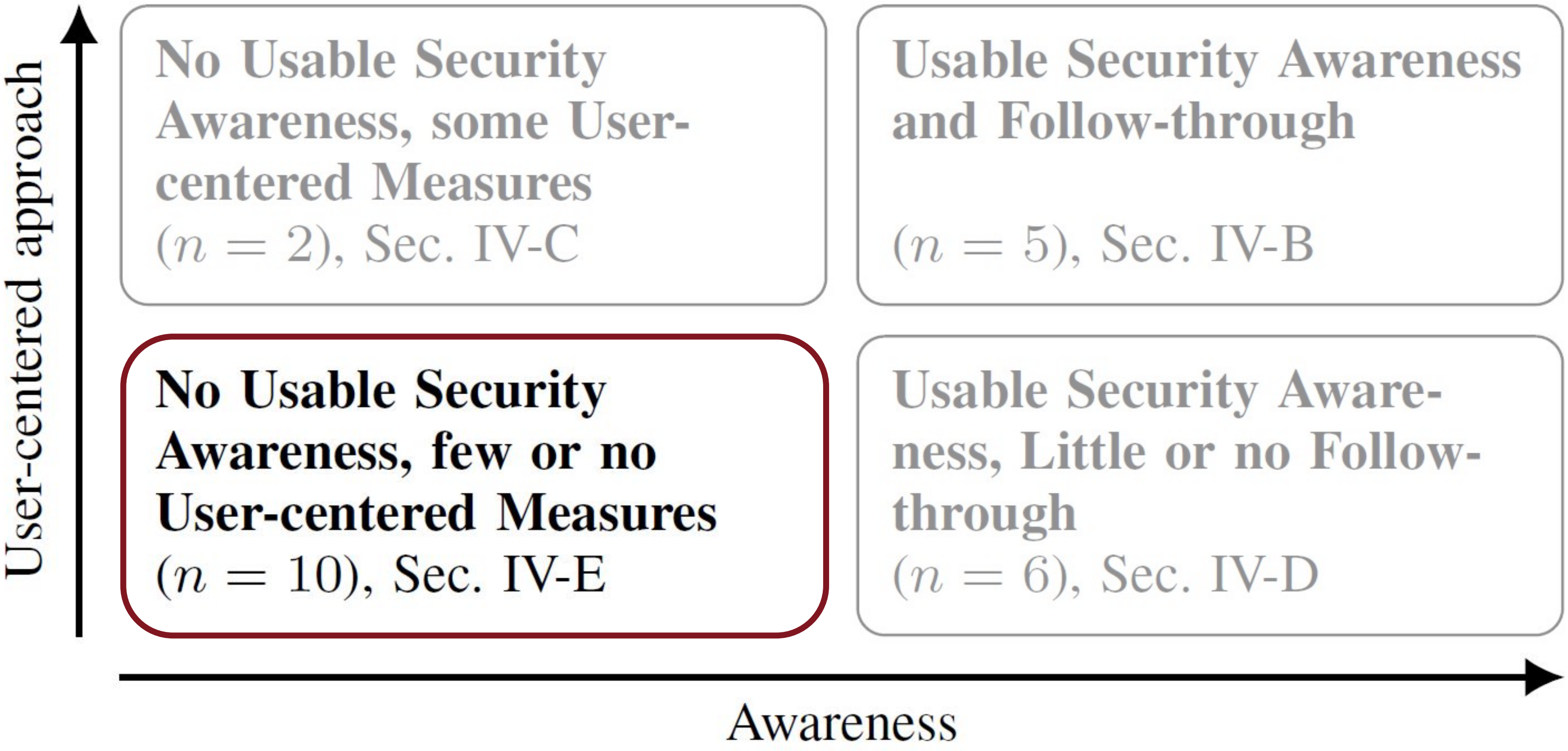
Usable Security Awareness, Little or no Follow-through
($n = 6$), Sec. IV-D

Key Findings



User-centered approach	**No Usable Security Awareness, some User-centered Measures** ($n = 2$), Sec. IV-C	**Usable Security Awareness and Follow-through** ($n = 5$), Sec. IV-B
	No Usable Security Awareness, few or no User-centered Measures ($n = 10$), Sec. IV-E	**Usable Security Awareness, Little or no Follow-through** ($n = 6$), Sec. IV-D
	Awareness	

Key Findings



No Usable Security Awareness, some User-centered Measures
($n = 2$), Sec. IV-C

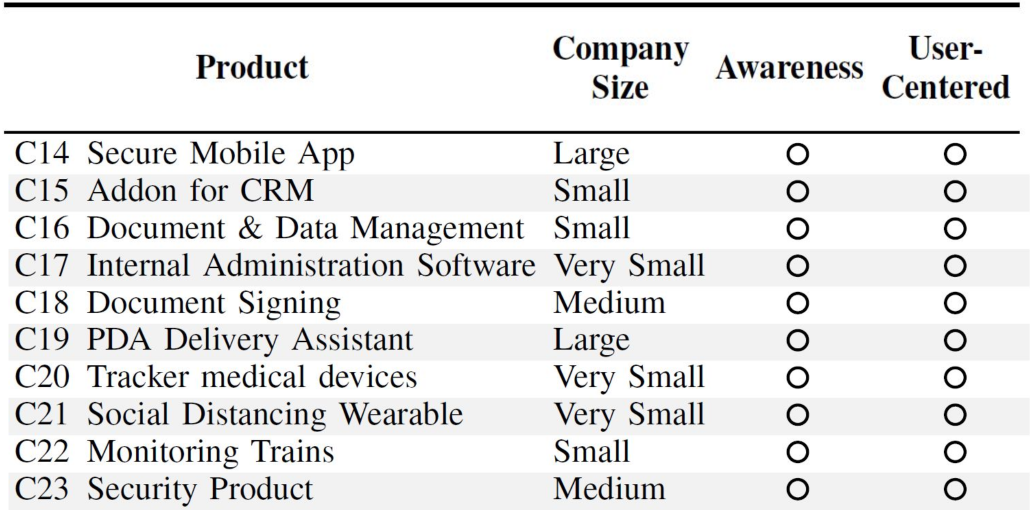
Usable Security Awareness and Follow-through
($n = 5$), Sec. IV-B

No Usable Security Awareness, few or no User-centered Measures
($n = 10$), Sec. IV-E

Usable Security Awareness, Little or no Follow-through
($n = 6$), Sec. IV-D

No Usable Security Awareness, few or no User-Centered Measures

- Misconceptions & Misunderstandings of usable security
- Rare availability of usability or UX experts or less involvement of those

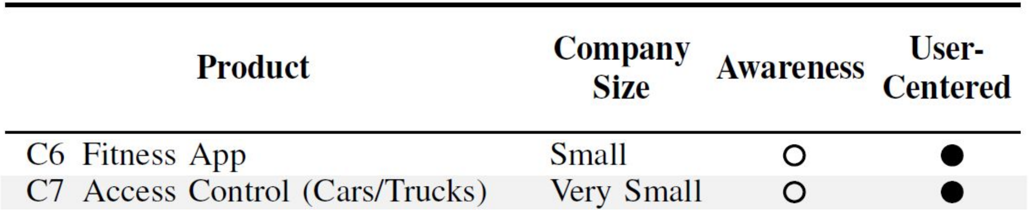


	Product	Company Size	Awareness	User-Centered
C14	Secure Mobile App	Large	○	○
C15	Addon for CRM	Small	○	○
C16	Document & Data Management	Small	○	○
C17	Internal Administration Software	Very Small	○	○
C18	Document Signing	Medium	○	○
C19	PDA Delivery Assistant	Large	○	○
C20	Tracker medical devices	Very Small	○	○
C21	Social Distancing Wearable	Very Small	○	○
C22	Monitoring Trains	Small	○	○
C23	Security Product	Medium	○	○

"I don't think there was a designer involved. [laughs] That's how it developed over time – like a plant grows [...]." (C18)

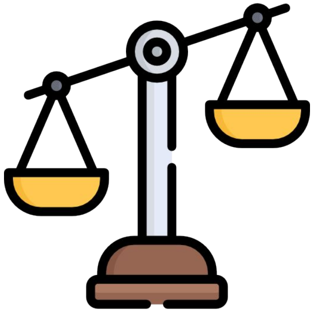
No Usable Security Awareness, some User-Centered Measures

- Focus on usability – security of lower priority
- "Usability-Security tradeoff"



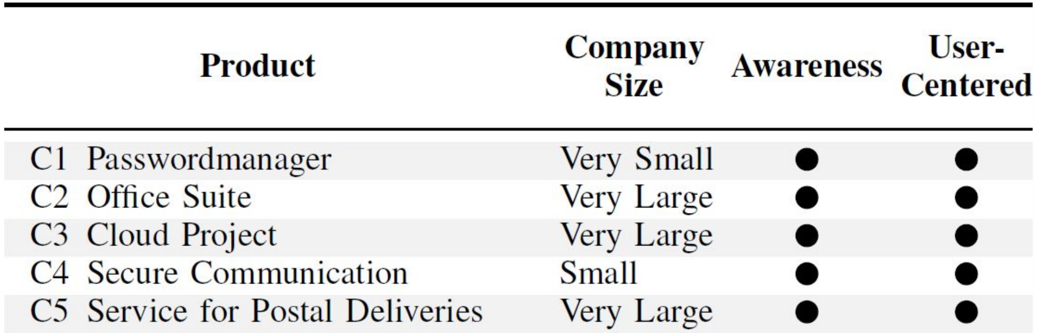
Product		Company Size	Awareness	User-Centered
C6	Fitness App	Small	○	●
C7	Access Control (Cars/Trucks)	Very Small	○	●

"They were more concerned about usability. Like I said, they even made decisions which sort of decreases security, develop the product just so that it is more usable." (C6)



Usable Security Awareness & Follow-through

- Often usable security was part of the business goals
- Active user feedback gathering
- All had subject-matter experts
- At least one person actively strengthened the communication about usable security

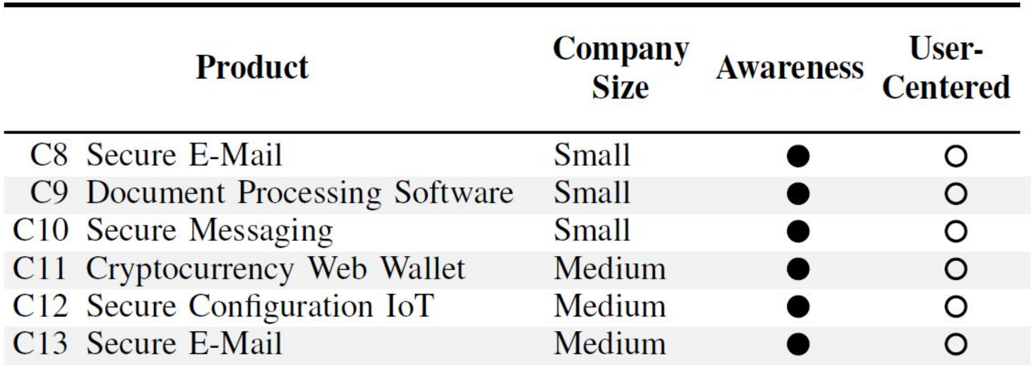


	Product	Company Size	Awareness	User-Centered
C1	Passwordmanager	Very Small	●	●
C2	Office Suite	Very Large	●	●
C3	Cloud Project	Very Large	●	●
C4	Secure Communication	Small	●	●
C5	Service for Postal Deliveries	Very Large	●	●

"Actually, I think that the security issues should be solved as much as possible technically and should not bother the user. Most of the time, the user is not an expert [...] That is, all the decisions that can be made for him, should be made in advance." *(C1)*

Usable Security Awareness, Little or no Follow-through

- Five companies had a strong focus on security and had dedicated security experts
- Only one company had a designer actively involved
- No specific measures for usability testing or user research



	Product	Company Size	Awareness	User-Centered
C8	Secure E-Mail	Small	●	○
C9	Document Processing Software	Small	●	○
C10	Secure Messaging	Small	●	○
C11	Cryptocurrency Web Wallet	Medium	●	○
C12	Secure Configuration IoT	Medium	●	○
C13	Secure E-Mail	Medium	●	○

"No, actually, we had for a very long time an open position for a UI/UX designer... but if you are looking for a UI/UX designer with additional qualification in the security environment… then, yes, you have to make one yourself." (C13)

Blockers

Limited Resources

- Lack of budget (n=8):
  "If the customer doesn't have enough budget for development, you can't set up that kind of security. [...] They have budget for main functionality but not for security or usability." (P18)

- Lack of time (n=10)

- "Functionality first" attitude (n=8)

Blockers

Limited Resources

Misconceptions

- Blaming users:

  “[This problem is] not related to usability, mostly it’s related to lack of technology skills. […] we can’t do anything about [authentication].” (P21)

- Misunderstanding usable security

- Usability is not taken seriously

Blockers

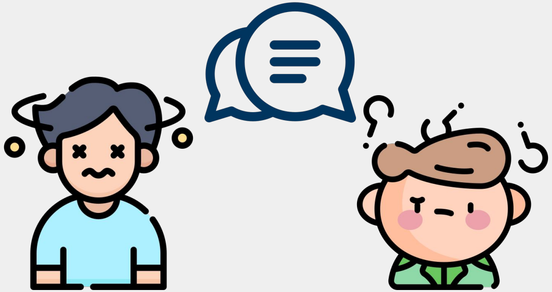
Limited Resources

Misconceptions

Communication Barriers

- Communication problems or even no communication at all

"But what you wonder is if the designer was even able to grasp the front-end developer." (P10)



Designers & UX Experts

Developers & Security Experts

Enablers

Communication Pivot

- Strong and efficient communication among subject-matter experts (security & UI/UX)
- Not necessarily a "usable security champion"

One team involved designers/UX experts in threat modeling activities

Enablers

Communication Pivot

Usability Commitment

- Usability was accepted and demanded by companies or customers

- Often it was part of the business goals:

"The main and the most important request from the management was: they need an easy-to-use software or app or interface to compete with other competitors" (P21)

Enablers

Communication Pivot

Usability Commitment

Usable Security Knowledge & Awareness

- Need to think about interplay of human factors, usability, and security
- At least a basic understanding of user-centered methods is needed
- Processes need to be adapted

Takeaways

Key Takeaways

Several factors impact usable security (e.g., limited resources, different decision makers, organizational commitment towards usability).

Usable security decisions are made by stakeholders in different stages of the SDP.

Usable security is interdisciplinary → need to combine usability, human factors, and security.

Implications for Industry

- Create awareness for usable security
- Improve communication among experts

- Shift usable security left in the SDP
- Measure & track usable security
  - Use practices from human-computer interaction
- "Usable security champions" may be helpful but rare

Implications for Research

Knowledge gap between industry and academia

Holistic view on SDPs needed, considering circumstances

→ *"It's not only about developers"*
→ Decisions are made at many stages

Need for lightweight usable security measures

How Does Usable Security (Not) End Up in Software Products?

Results From a Qualitative Interview Study

Marco Gutfleisch
Ruhr University Bochum
marco.gutfleisch@ruhr-uni-bochum.de

Jan H. Klemmer
Leibniz University Hannover
klemmer@sec.uni-hannover.de

Niklas Busch
CISPA Helmholtz Center for Information Security
niklas.busch@cispa.de

Yasemin Acar
Paderborn University,
George Washington University,
yasemin.acar@uni-paderborn.de

M. Angela Sasse
Ruhr University Bochum
martina.sasse@ruhr-uni-bochum.de

Sascha Fahl
CISPA Helmholtz Center for Information Security
sascha.fahl@cispa.de

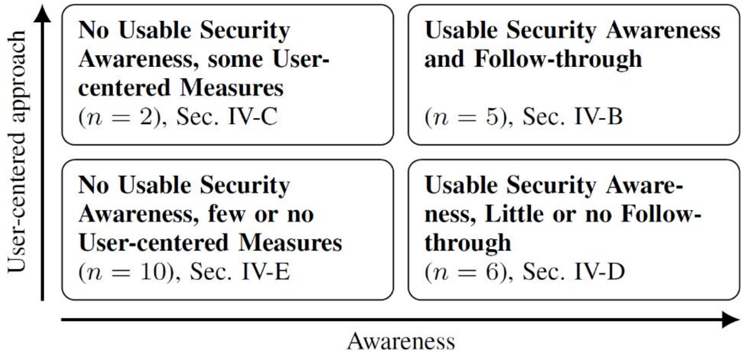
Blockers

- Limited Resources
- Misconceptions
- Communication Barriers

Enablers

- Communication Pivot
- Usability Commitment
- Usable Security Knowledge & Awareness

Key Findings



No Usable Security Awareness, some User-centered Measures ($n = 2$), Sec. IV-C

Usable Security Awareness and Follow-through ($n = 5$), Sec. IV-B

No Usable Security Awareness, few or no User-centered Measures ($n = 10$), Sec. IV-E

Usable Security Awareness, Little or no Follow-through ($n = 6$), Sec. IV-D

Key Takeaways

Several factors impact usable security (e.g., limited resources, different decision makers, organizational commitment towards usability).

Usable security decisions are made by stakeholders in different stages of the SDP

Usable security is interdisciplinary → need to combine usability, human factors, and security.

Published @ IEEE S&P'22 — https://publications.teamusec.de/2022-oakland-usec-in-sdps/