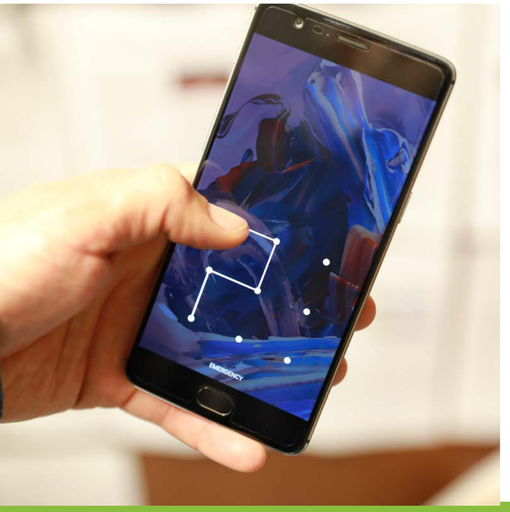
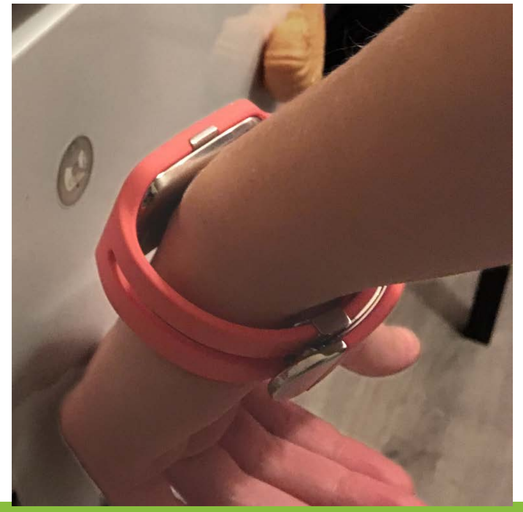
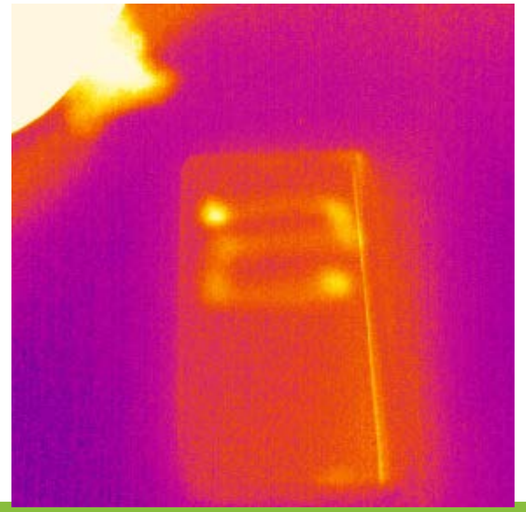
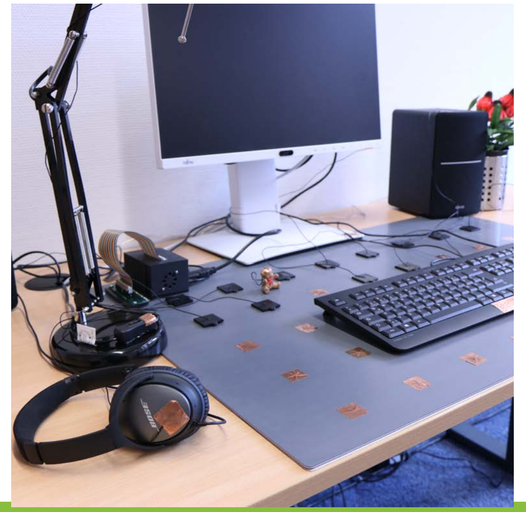






Intelligent Usable Security

Florian Alt

Short Bio

INDUSTRY EXPERIENCE

- **Pinnacle Systems** (2005)
- **Fraunhofer IAIS** (2007)
- **Schreiner MediPharm** (2007–2008)
- **Telekom Labs** (2011)

SCIENTIFIC EDUCATION

- **LMU Munich** (2001–2007)
- **Universität Essen** (2008–2011)
- **Universität Stuttgart** (2011–2013)
- **LMU Munich | HAW Munich** (2013–2018)
- **UniBW Munich** (from 2018)

florian.alt@unibw.de | https://go.unibw.de/usec

Learning Goals

- Know about important terms and definitions.
- Gain an appreciation for the importance of usability within security and privacy.
- Understand opportunities and challenges of designing user interfaces for intelligent security mechanisms.

Categorisation of Authentication Concepts

Terms & Definitions

knowledge-based	token-based	biometric
alphanumeric	hardware	physical
graphical	software	behavior
gestures		

Goals of the User

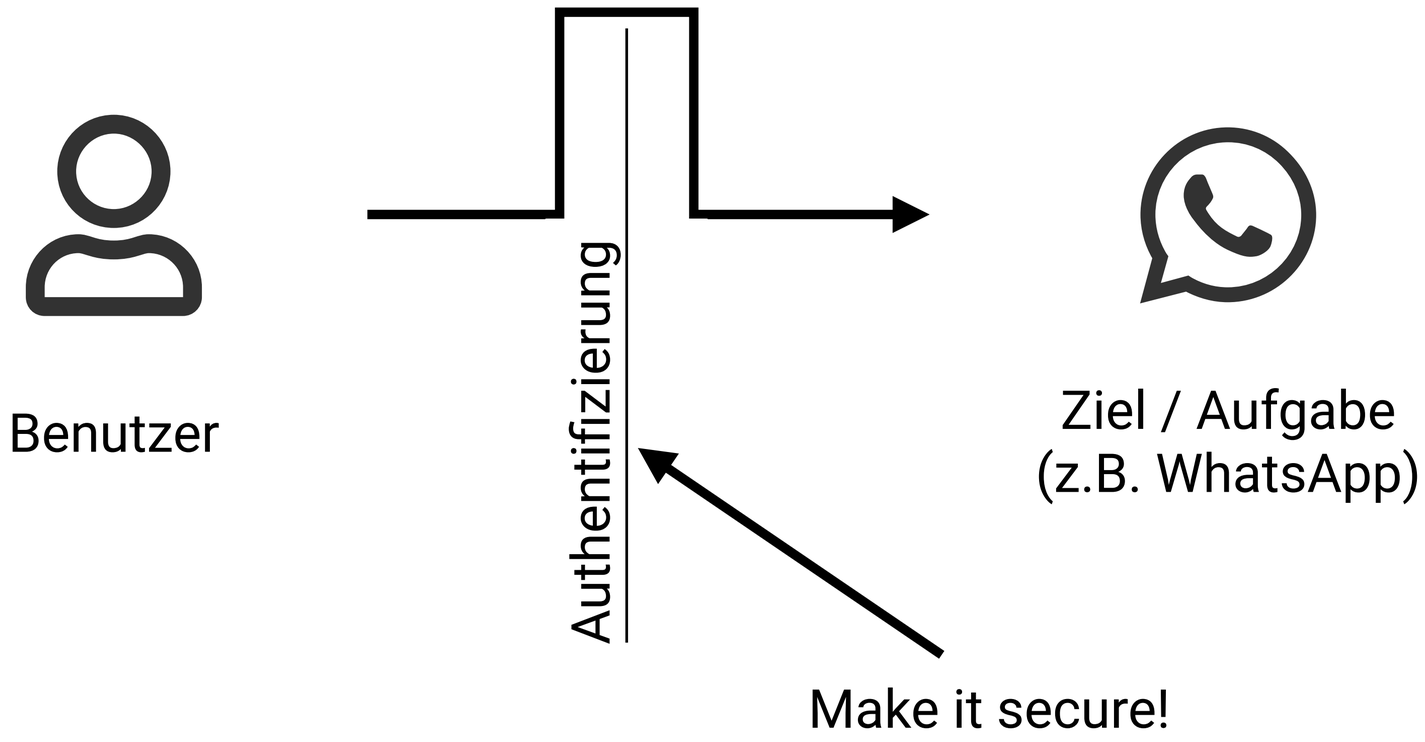
Adams et al., 1999

Benutzer

Ziel / Aufgabe
(z.B. WhatsApp)

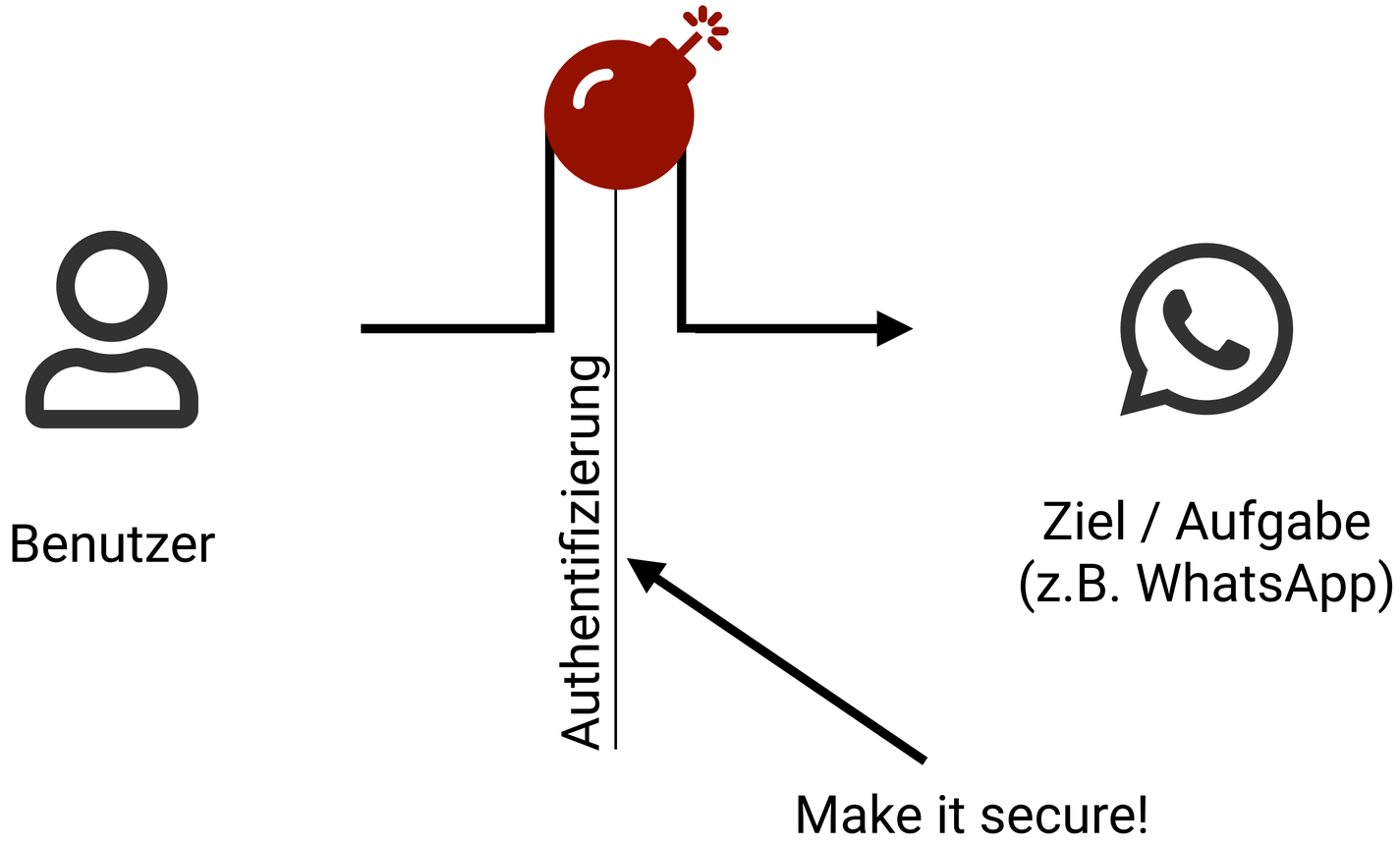
Goals of a Security Expert

Adams et al., 1999



Goals of a Security Expert

Adams et al., 1999



Most Frequent PINs and Passwords

The 25 most frequent PINs

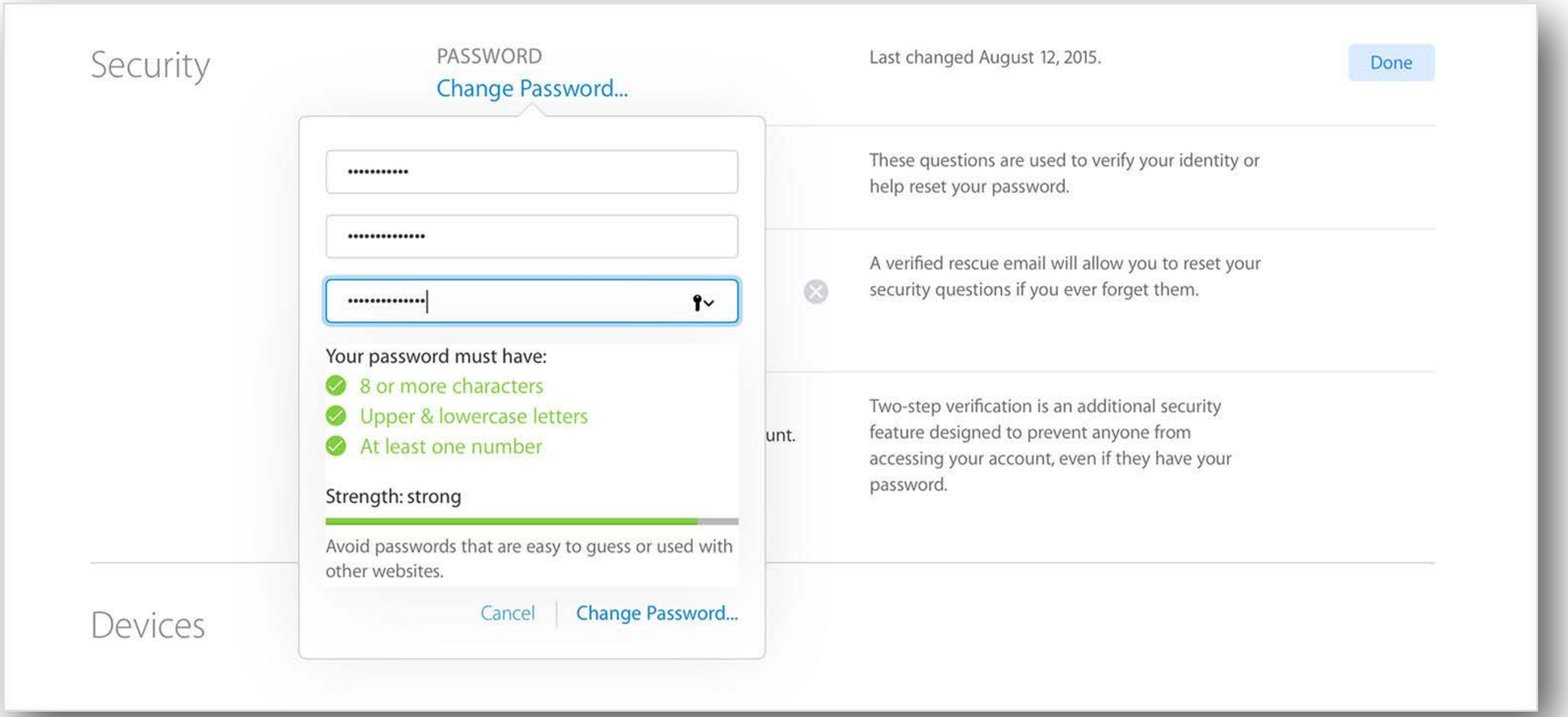
1. 1234
2. 0000
3. 2580
4. 1111
5. 5555
6. 5683
7. 0852
8. 2222
9. 1212
10. 1998
11. 6969
12. 1379
13. 1997
14. 2468
15. 9999
16. 7777
17. 1996
18. 2011
19. 3333
20. 1999
21. 8888
22. 1995
23. 2525
24. 1590
25. 1235

The 25 most frequent passwords

1. password
2. 123456
3. 12345678
4. 1234
5. qwerty
6. 12345
7. dragon
8. pussy
9. baseball
10. football
11. letmein
12. monkey
13. 696969
14. abc123
15. mustang
16. michael
17. shadow
18. master
19. jennifer
20. 111111
21. 2000
22. jordan
23. superman
24. harley
25. 1234567

http://www.netzpiloten.de/die-25-haufigsten-passworter-und-pins/

Password Policies

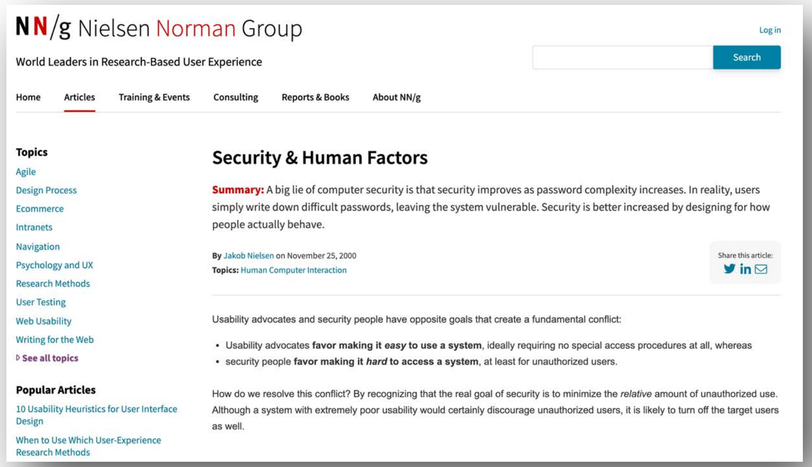


https://support.apple.com/en-us/HT201303

Security and Human Factors

A definition by Jakob Nielson

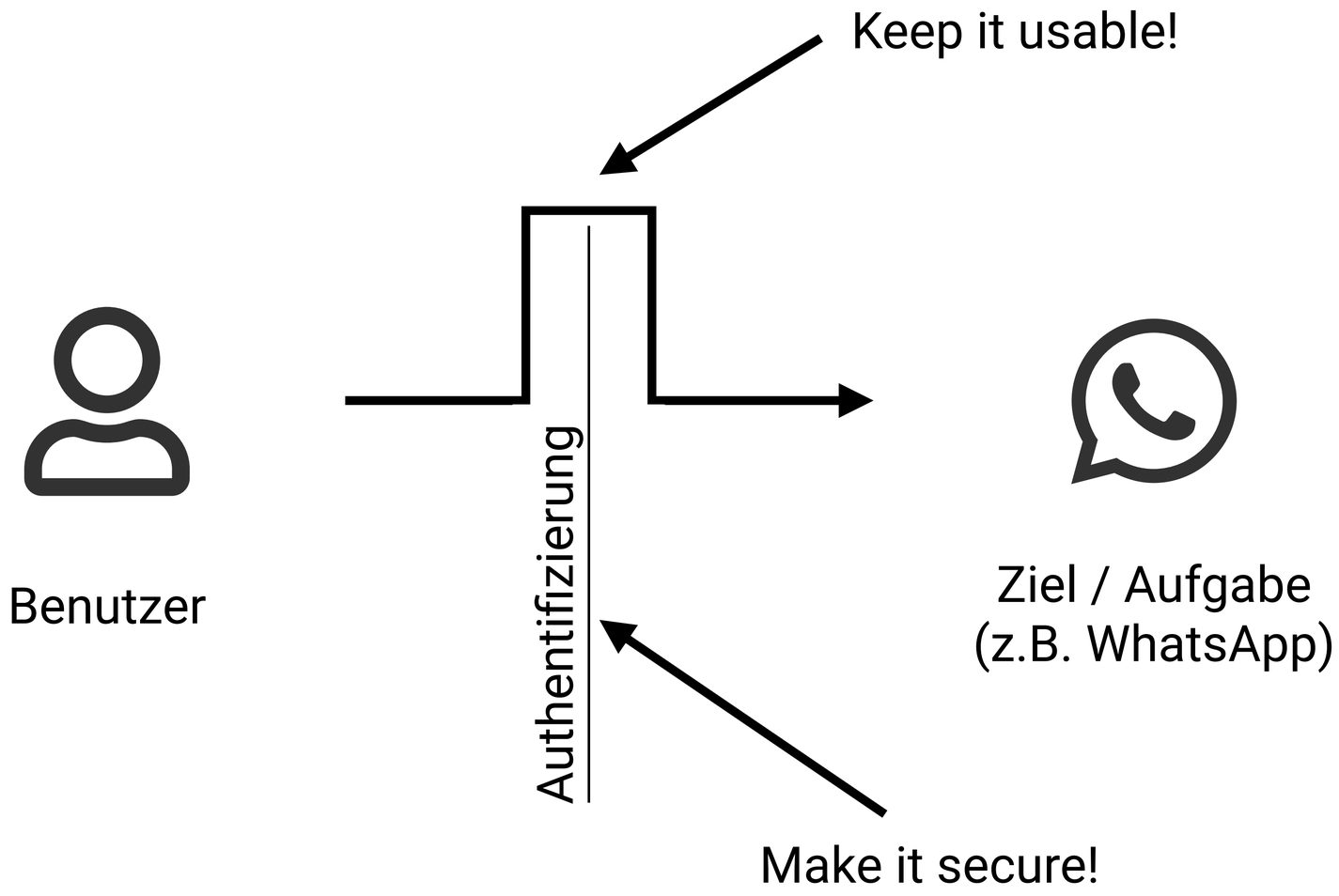
- “A big lie of computer security is that security improves as password complexity increases. In reality, users simply write down difficult passwords, leaving the system vulnerable. Security is better increased by **designing for how people actually behave**.”



Jakob Nielsen. Security and Human Factors. https://www.nngroup.com/articles/security-and-human-factors/

Goals of a Usable Security Expert

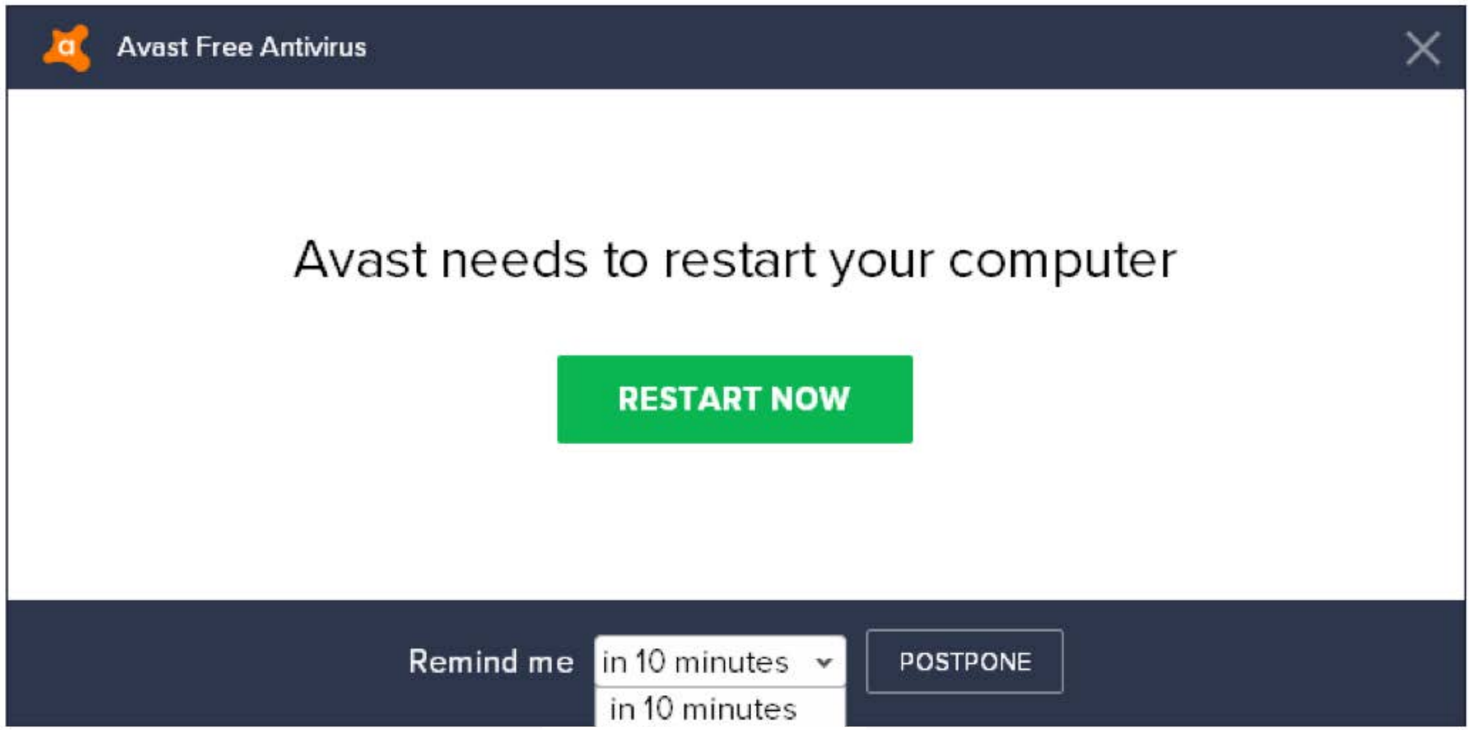
Adams et al., 1999



Usable Security and Privacy

Aim of Usable Security and Privacy:
To make privacy and security and integrated, natural, unburdened part of Human-Computer Interaction.

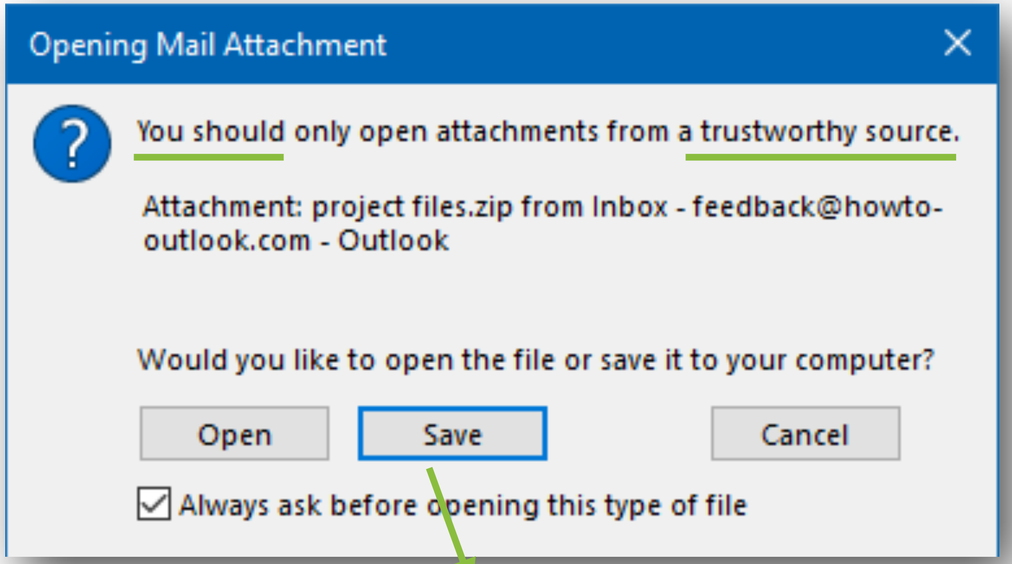
Security is a Secondary Task



Misligned Priorities

Complicated Security Concepts

What if I don’t?

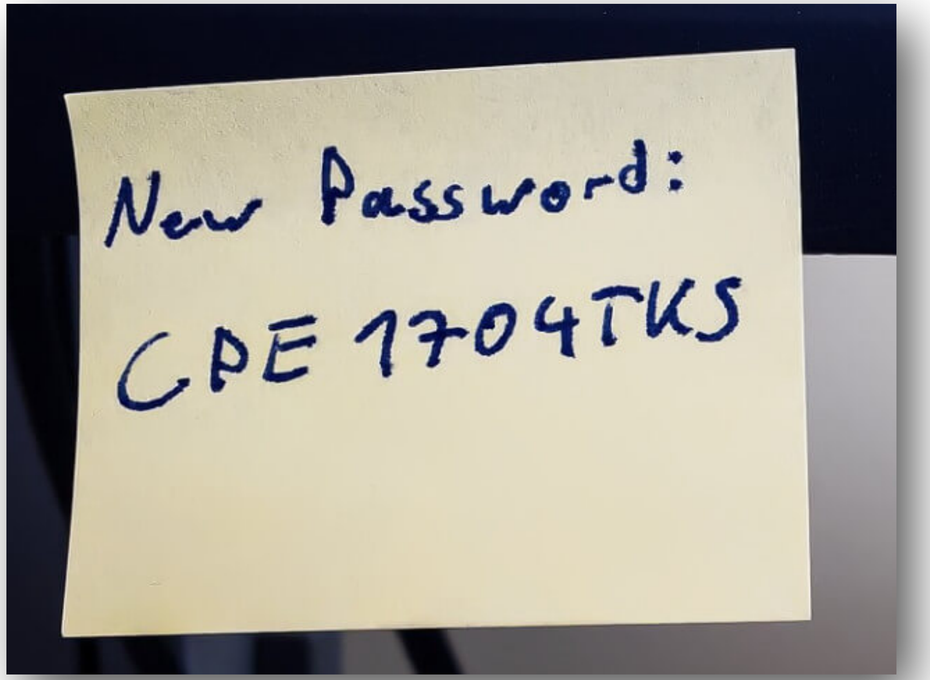


What makes a source trustworthy?

Opening is not okay? I guess this means saving is fine?

https://social.technet.microsoft.com/Forums/en-US/f9912914-ad11-4d5c-8b13-756dbca46533/only-open-attachments-from-trustworthy-sources-prompt-popping-up-on-emails-from-people-in-same?forum=outlook

Limited Capacity of Users



https://techsolvers.com.au/blog/how-to/choose-manage-strong-passwords/

https://me.me/i/changed-all-my-passwords-to-incorrect-so-whenever-i-forget-3419912

Habituation

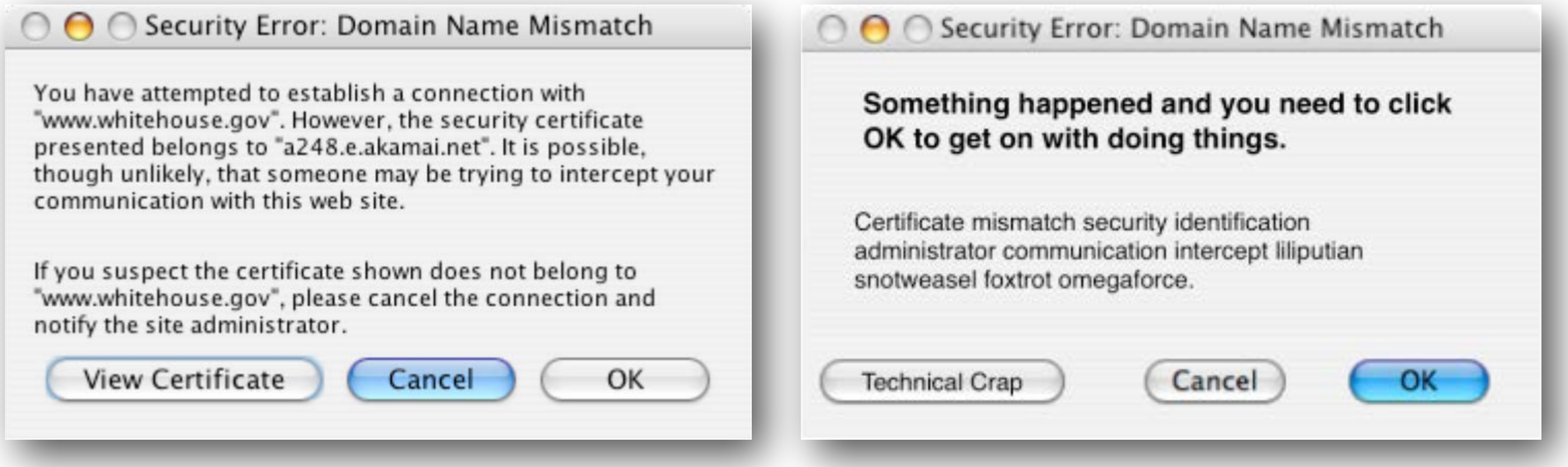
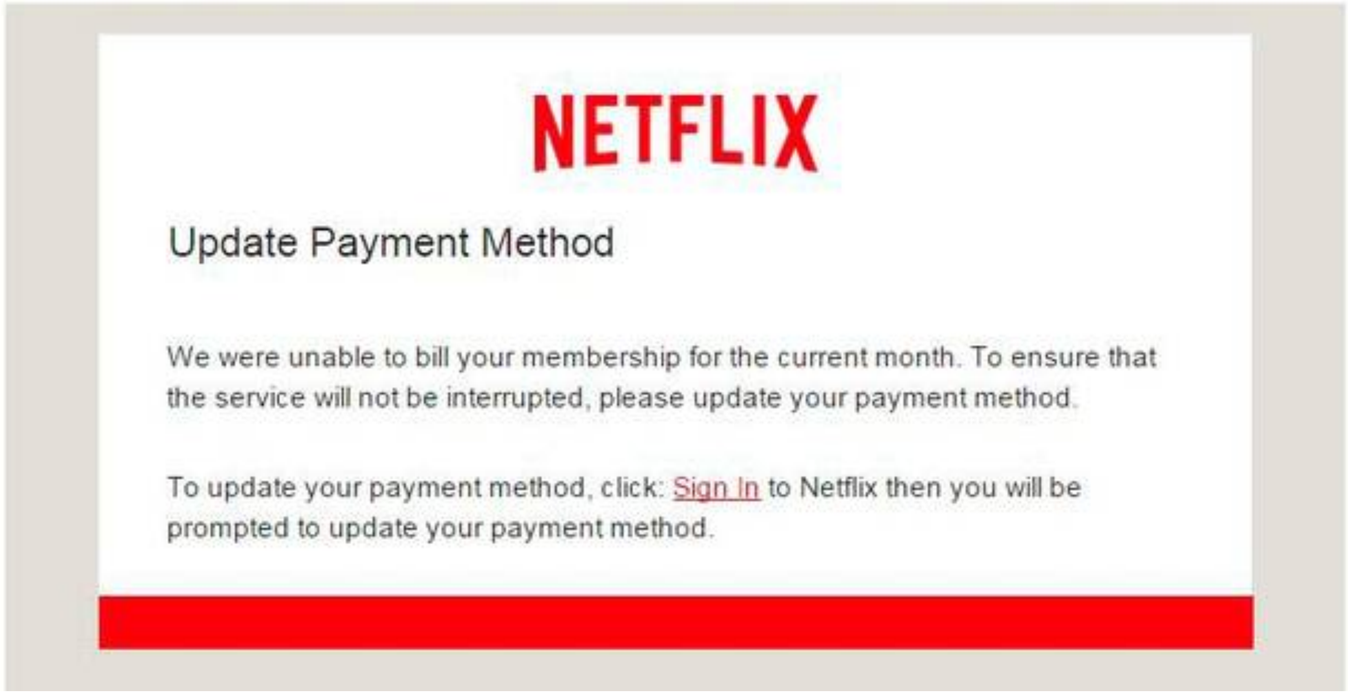


Image courtesy of Johnathan Nightingale

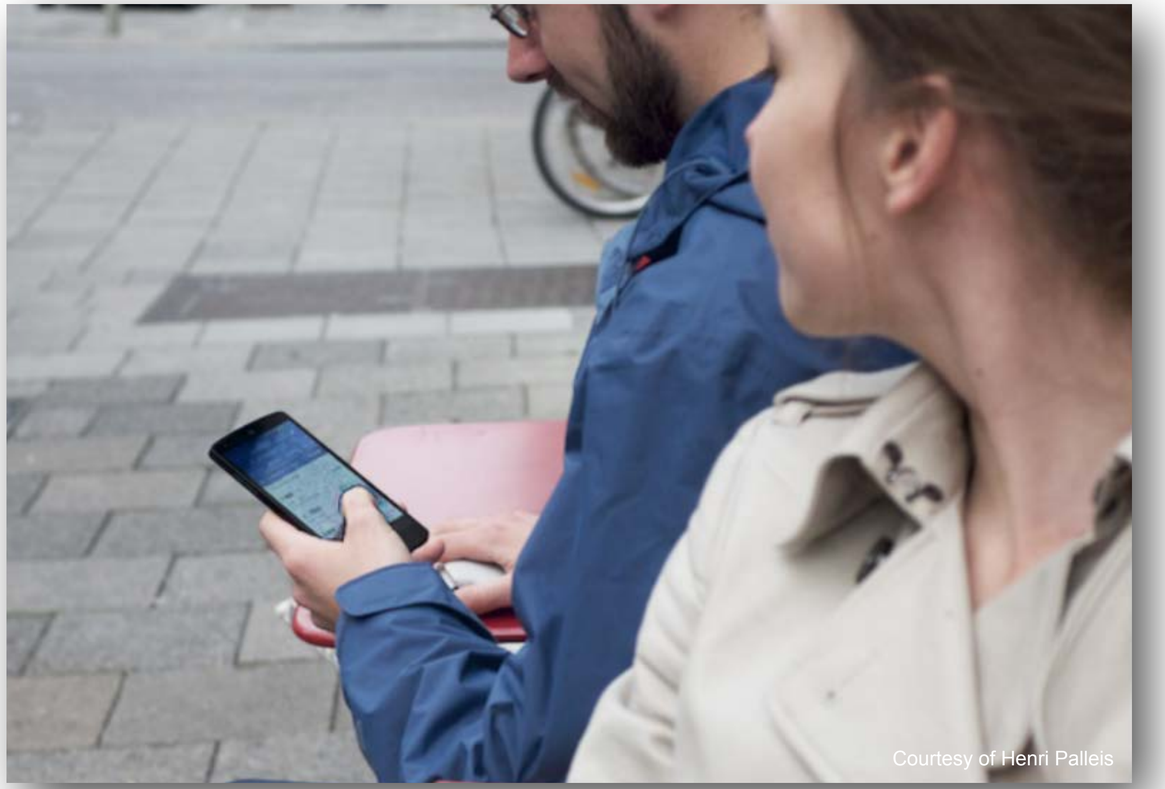
Humans are Prone to Social Engineering

From: Netflix <noreply@netl.com>
Sent: 03 March 2016 14:12
Subject: You need to update your payment method



Humans are Prone to Side-Channel Attacks

Shoulder Surfing



Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). ACM, New York, NY, USA, 4254-4265.

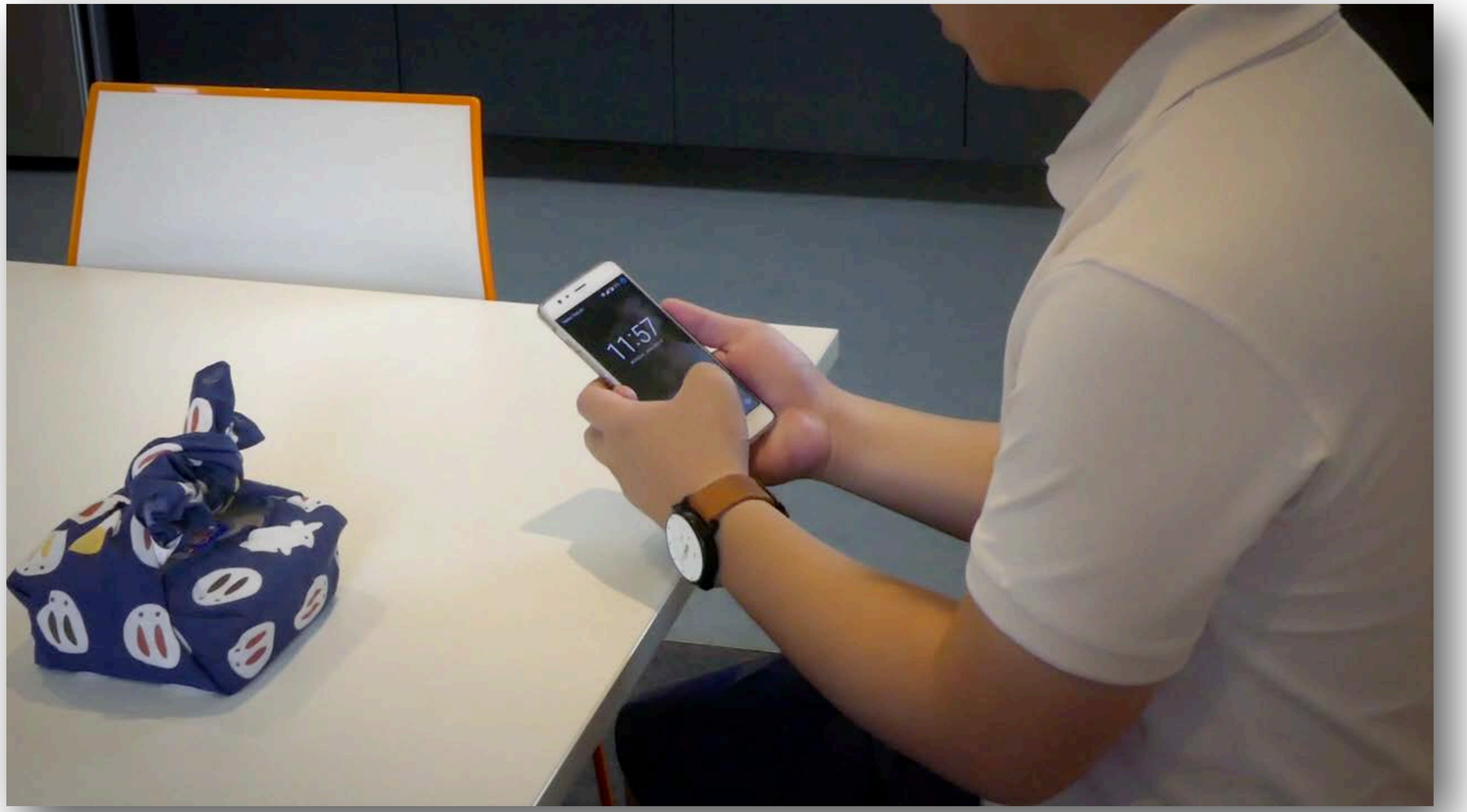
Humans are Prone to Side-Channel Attacks

Smudge Attacks

Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX conference on Offensive technologies (WOOT'10). USENIX Association, Berkeley, CA, USA, 1-7.

Humans are Prone to Side-Channel Attacks

Thermal Attacks

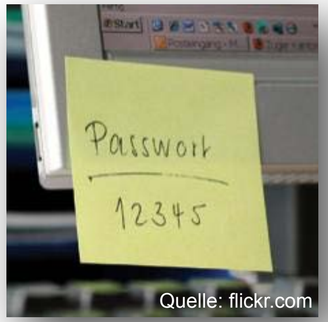


Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. (CHI '17). ACM, New York, NY, USA, 3751-3763.

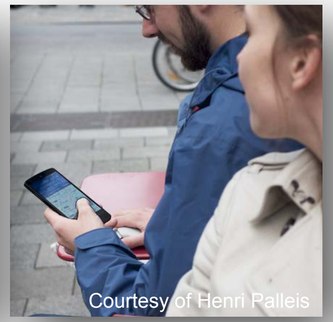
Selected Threats in Authentication

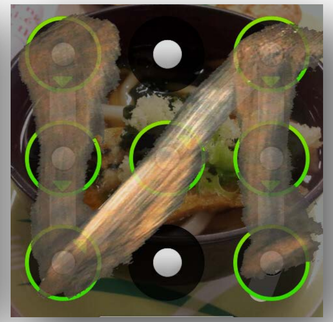
Terms & Definitions

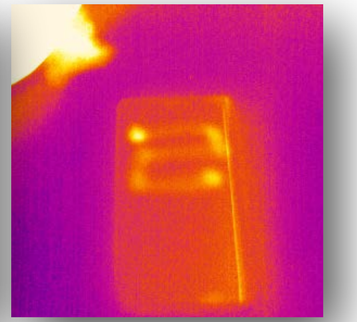
- Guessing Attack
- Observation Attack, e.g.,
  - Shoulder Surfing
- Reconstruction Attacks, e.g.
  - Smudge Attack
  - Thermal Attack
- Mimicry Attacks



Quelle: flickr.com


Courtesy of Henri Palleis





Personas & Task Frequency Analysis

Recap from Human-Computer Interaction

- Who are your users?
- What is the user trying to do?
  - What is their goals?
  - What is their needs?
  - Which tasks result from this?

Task / Persona	Group reservation	Change of itinerary	Booking child care	Comparing sales agent performance
Sales agent	0.2	0.1	0.1	0
Manager	0	0	0	0.3
Traveler	0.01	0.2	0.01	0

Threat Modeling

- Can’t protect against everything
  - Too expensive
  - Too inconvenient
  - Not worth the effort
- **Approach**
  - Identify likely attackers and their resources
    — Dumpster diving or rogue nation?
  - Identify most likely ways system will be attacked
    — e.g., user-centred attack
  - Identify consequences of possible attacks
    — Mild embarrassment or bankruptcy?
  - Design security measures accordingly
    — Accept that they will not defend against all attacks

} part of your threat model

Modeling the Attacker

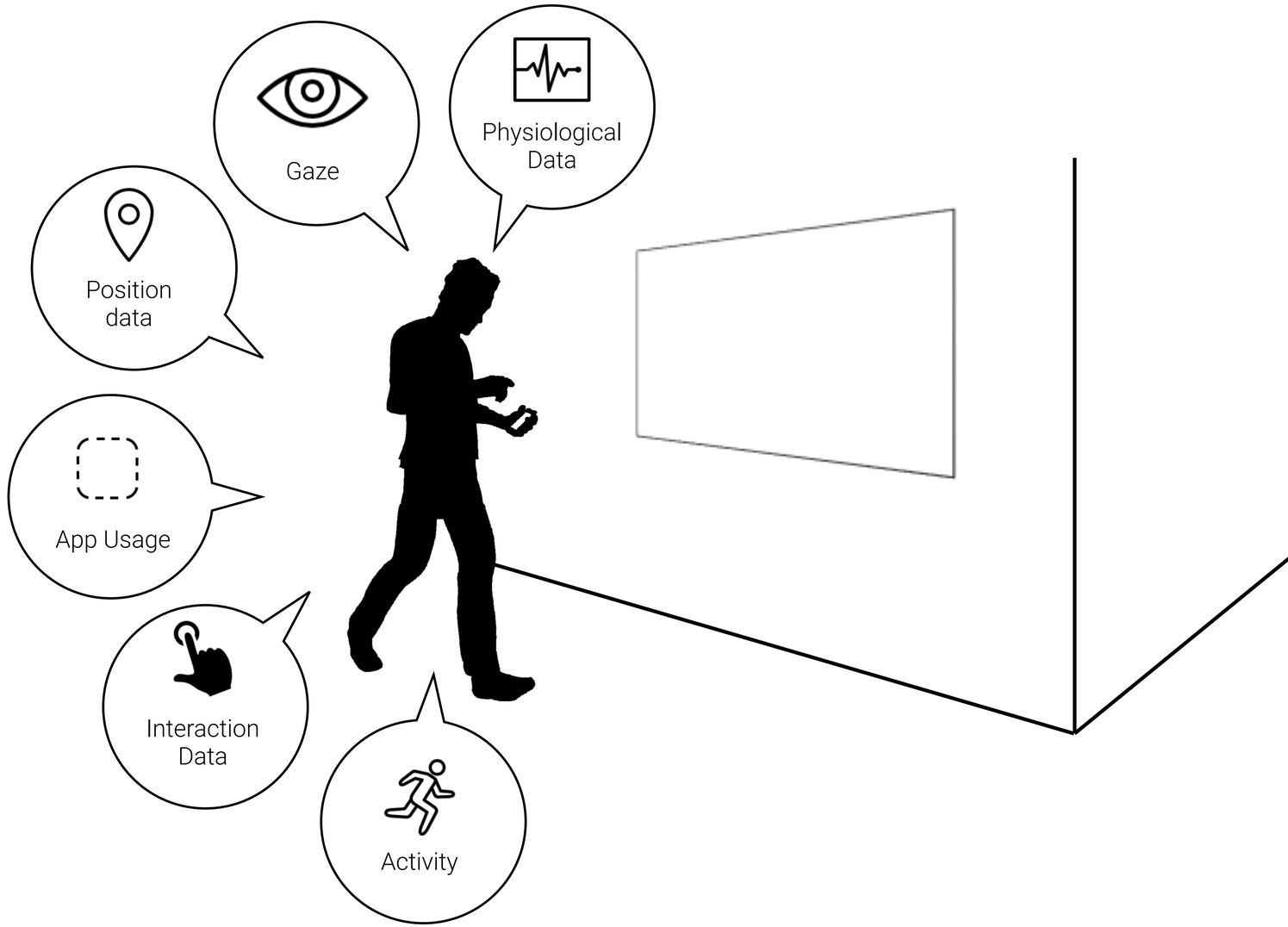
- What type of **action** will they take?
  - Passive (look, but don’t touch)
  - Active (look and inject messages)
- How **sophisticated** are they?
- How much do they **care**?
- What **resources** do they have?
  - How much time/money will they spend?
- How much do they already **know**?
  - External / internal attacker?

Modeling the Attack

- Identify possible attacks
  - From the literature
  - From brainstorming (e.g., scenario analysis)
- **Attack Description:**
  We assume an attacker who is already in possession of a user's password pattern for a mobile device. That is, the first security barrier has already been breached. How the attacker got this information is of no concern here. In addition, the attacker managed to retrieve the mobile device (e.g. using pickpocketing) and wants to gain access to valuable information on it. For this, as for other commercial systems, the attacker has three tries until the device will be blocked.

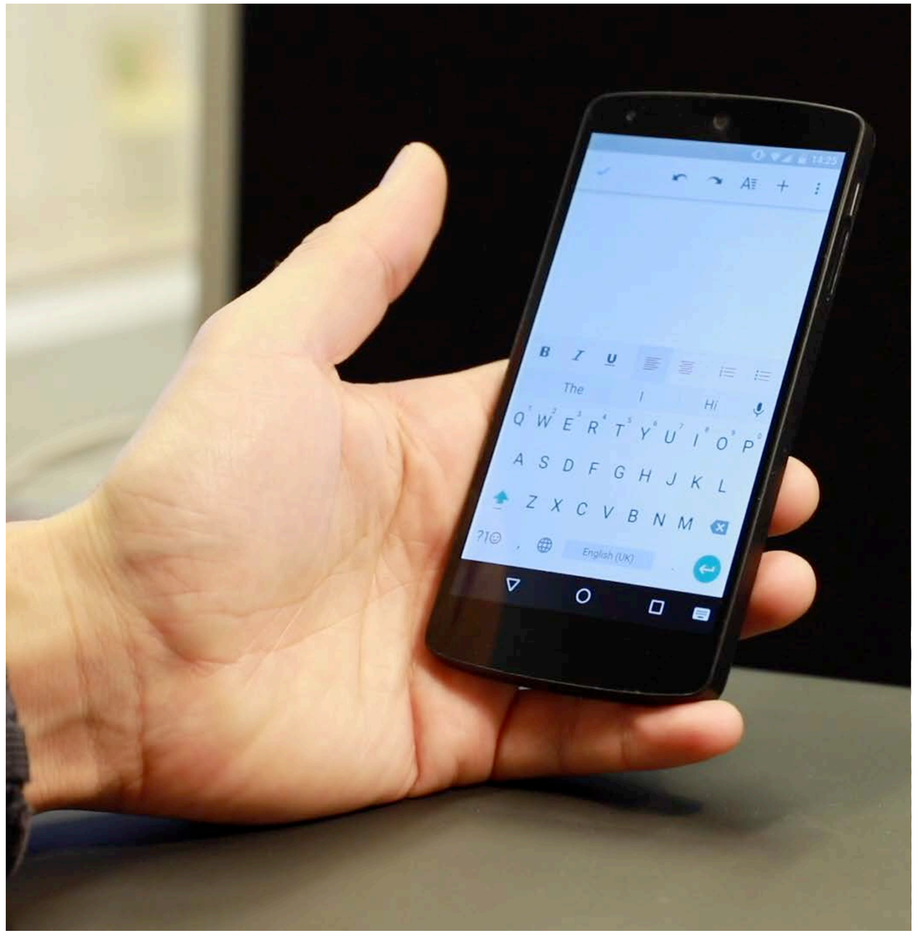
Adapted from "De Luca et al. 2012. Touch me once and i know it's you! Implicit authentication based on touch screen patterns. In Proc. of CHI '12".

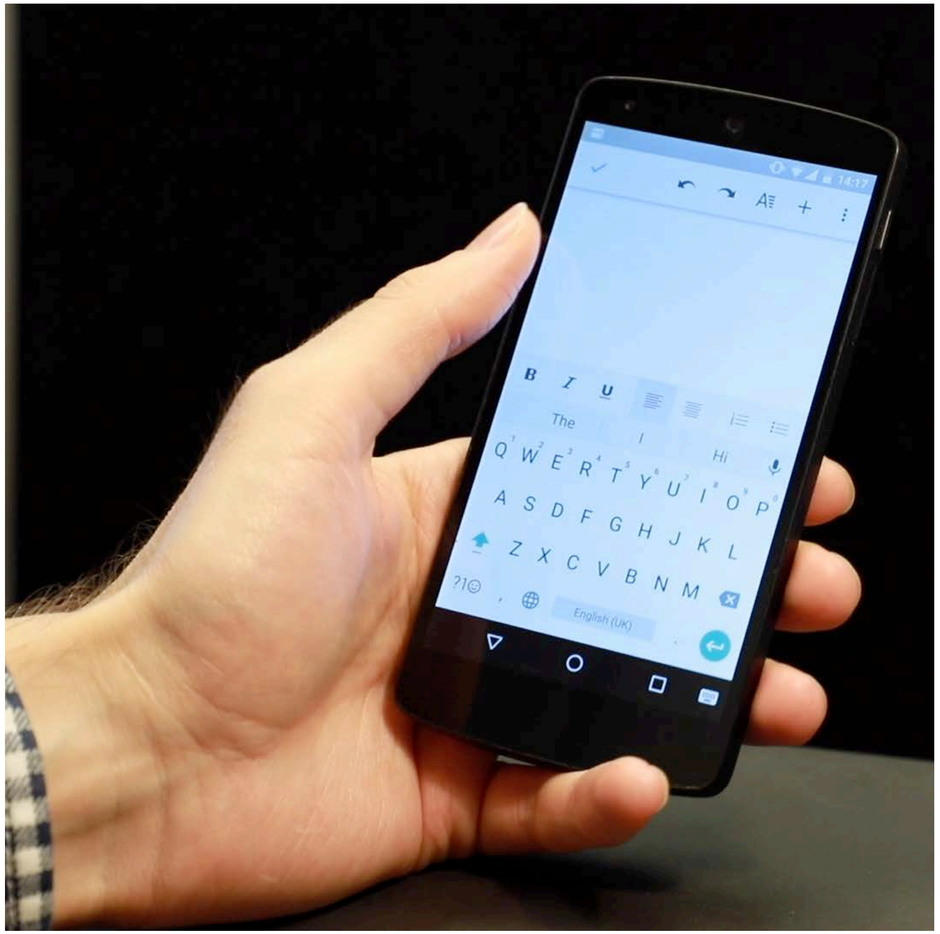
Towards Intelligent Usable Security



Identifying Users from Behavior

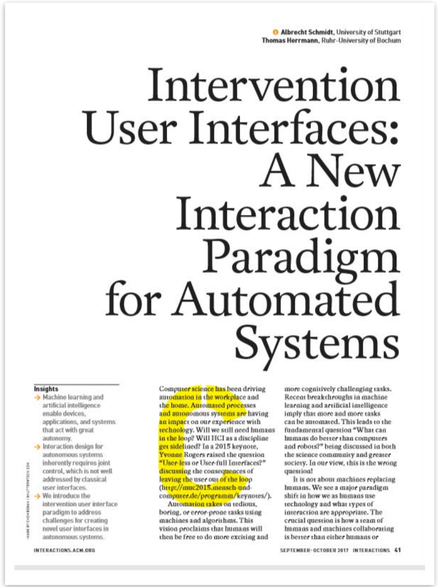
Typing





Challenges

- Enrollment
- Fallback Authentication
- Re-Authentication
- User View / Privacy
- …



Albrecht Schmidt, University of Stuttgart
Thomas Herrmann, Ruhr-University of Bochum

Intervention User Interfaces: A New Interaction Paradigm for Automated Systems

Insights

Machine learning and artificial intelligence enable devices, applications, and systems that act with great autonomy.

Interaction design for autonomous systems inherently requires joint control, which is not well addressed by classical user interfaces.

We introduce the intervention user interface paradigm to address challenges for creating novel user interfaces in autonomous systems.

Computer science has been driving automation in the workplace and the home. Automated processes and autonomous systems are having an impact on our experience with technology. Will we still need humans in the loop? Will HCI as a discipline get sidelined? In a 2015 keynote, Yvonne Rogers raised the question "User less or User full Interfaces?" discussing the consequences of leaving the user out of the loop (http://mmc2015.mensch-und-computer.de/programm/keynotes/).

Automation takes on tedious, boring, or error-prone tasks using machines and algorithms. This vision proclaims that humans will then be free to do more exciting and more cognitively challenging tasks. Recent breakthroughs in machine learning and artificial intelligence imply that more and more tasks can be automated. This leads to the fundamental question "What can human do better than computers and robots?" being discussed in both the science community and greater society. In our view, this is the wrong question!

It is not about machines replacing humans. We see a major paradigm shift in how we as human use technology and what types of interaction are appropriate. The crucial question is how a team of humans and machines collaborating is better than either humans or

INTERACTIONS.ACM.ORG

SEPTEMBER+OCTOBER 2017 INTERACTIONS 41

Which design principles hold for "intervention security interfaces"?

- Ensure expectability and predictability.
- Communicate options for interventions.
- Allow easy exploration of interventions.
- Easy reversal of automated and intervention actions.
- Minimize required attention.
- Communicate how control is shared.

Albrecht Schmidt and Thomas Herrmann. 2017. Intervention user interfaces: a new interaction paradigm for automated systems. interactions 24, 5 (September - October 2017), 40–45. DOI:https://doi.org/10.1145/3121357

Mini Exercise

Towards Intelligent Authentication

- **Available information**
  - User Location / Time
  - Activity
  - People in the Vicinity
  - User's Emotional State
  - User's Stress Level
  - Current Cognitive Load
  - App Usage History
- **Authentication Contexts**
  - Smartphone
  - Smart Home Appliance (TV, fridge, vacuum cleaner)
  - Chose your own

- **Task**: 5 minutes | teams of 3
  Discuss, how context information could be used to (a) **enhance** current authentication mechanisms or to (b) build a **new** authentication mechanism?

Mini Exercise

Towards Intelligent Authentication

- **Guiding Questions**
  - How can your approach reduce the time required for authentication?
  - How can your approach reduce interruption costs?
  - How well does your approach protect against different types of user-centred attacks?
  - How easy is your approach to implement?

- **Task**: 5 minutes | teams of 3
  Discuss, how context information could be used to (a) **enhance** current authentication mechanisms or to (b) build a **new** authentication mechanism?

Usable Security Origins

- Three seminal papers are seen as the origin of Usable Security and Privacy research:
  - 1996 Zurko and Simon's: "User-Centered Security"
  - 1999 Adams and Sasse's: "Users Are Not the Enemy"
  - 1999 Whitten and Tygar's "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0"
  - USENIX Security Test of Time Award 2015
- All argued that users should not be seen as the problem to be dealt with, but that **security experts need** to communicate more with users, and **adopt user-centered design approaches**.

User-Centered Security:
Stepping Up to the Grand Challenge

Mary Ellen Zurko
IBM Software Group
mzurko@ibm.us.com

Abstract

User-centered security has been identified as a grand challenge in information security and assurance. It is on the brink of becoming an established subdomain of both security and human/computer interface (HCI) research, and an influence on the product development lifecycle. Both security and HCI rely on the reality of interactions with users to prove the utility and validity of their work.

As practitioners and researchers in those areas, we still face major issues when applying even the most foundational tools used in either of these fields across both of them. This essay discusses the systemic roadblocks at the social, technical, and pragmatic levels that user-centered security must overcome to make substantial breakthroughs. Expert evaluation and user testing are producing effective usable security today. Principles such as safe staging, enumerating usability failure risks, integrated security, transparent security and reliance on trustworthy authorities can also form the basis of improved systems.

1. The Problem of User-Centered Security

The importance and challenge of the relationship between human users and security mechanisms has been recognized since the dawn of time in the systems security field. Saltzer and Schroeder [43] defined the principle of psychological acceptability in their seminal 1975 paper on the protection of information in computer systems.

> "It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors."

The mode of interaction with security mechanisms was users applying them consciously and directly as standalone tools in a context they understood. The challenge was to make the security model of the tools consistent with the user's mental model of security, so that undesirable errors would be minimized.

By 1996, humans' relationships to computers had changed dramatically. The World Wide Web, invented in 1989, was popularized with a GUI in 1992, and began its steady rise to ubiquity. The more diverse, distributed, and popular uses of the web, the network, and computers became, the more obvious it became that problems with the usability of existing security mechanisms would compromise their effectiveness. Simon and I [58] defined the term **user-centered security** to refer to "security models, mechanisms, systems, and software that have usability as a primary motivation or goal." We foresaw the following three categories of solutions: (1) applying human-computer interaction (HCI) design and testing techniques to secure systems, (2) providing security mechanisms and models for human collaboration software, and (3) designing security features directly desired by users for their immediate and obvious assurances (for example, signatures). Security researchers pursued the usability in some of the most important and intractable areas, including trust models, encryption and signing, and authentication. HCI researchers began to attack the same problems. Sometimes these even talked to each other.

Two years ago, in November 2003, Computing Research Association held a conference on "Grand Challenges in Information Security & Assurance" [10]. One of the four resulting grand challenges was:

> "Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future."

In the 28 years since psychological acceptability was defined, the problem has increased in urgency.

While there has been substantial work in usable security in the last nine years, the CRA's grand challenge indicates that the problem is not only

References

- Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. (CHI '17). ACM, New York, NY, USA, 3751-3763.
- Adams, Anne, and Martina Angela Sasse. "Users are not the enemy." Communications of the ACM 42.12 (1999): 40-46.
- Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX conference on Offensive technologies (WOOT'10). USENIX Association, Berkeley, CA, USA, 1-7.
- De Luca, A., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012, May). Touch me once and i know it's you! implicit authentication based on touch screen patterns. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 987-996).
- Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). ACM, New York, NY, USA, 4254-4265.
- C. Kaufman, R. Perlman, and M. Speciner. Network Security: PRIVATE Communication in a PUBLIC World. 2nd edition. Prentice Hall, page 237, 2002.
- Jakob Nielsen. Security and Human Factors. https://www.nngroup.com/articles/security-and-human-factors/
- Albrecht Schmidt and Thomas Herrmann. 2017. Intervention user interfaces: a new interaction paradigm for automated systems. interactions 24, 5 (September - October 2017), 40–45. DOI:https://doi.org/10.1145/3121357
- Whitten, Alma, and J. Doug Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." USENIX Security Symposium. Vol. 348. 1999.
- Zurko, Mary Ellen, and Richard T. Simon. "User-centered security." Proceedings of the 1996 workshop on New security paradigms. 1996.