

# ESSE Einführung in Security – VO 14: Usable Security und Trust

Rafael Vrecar, Florian Fankhauser, Christian Schanes

24W



ESSE (Establishing Security) – IT Security Research Team  
Research Group for Industrial Software (INSO)

<https://establishing-security.at/>

# Agenda

- Definition von „Trust“ (dt. Vertrauen)
- Rolle von Vertrauen in der IT-Sicherheit
- Misstrauen (Mistrust vs. Distrust)
- Perspektiven auf Security und Usability
- Definition bzw. Motivation von Usable Security
- Prinzipien und Lektionen zu Usable Security
- Ausblick: User-Centered Design
- Literatur und Quellen
- Zusammenfassung

Was bedeutet  
*für Sie*  
„Trust“ (dt. Vertrauen)?

# (Eine) Definition: „Vertrauen“



(Bild generiert mit ChatGPT)

„Wir definieren *Vertrauen* (*en. Trust*) als die Bereitschaft einer Entität (i.e., *Treugeber:in* (*en. Trustor*)), sich gegenüber einer anderen Entität (i.e. *Treuhänder:in* (*en. Trustee*)) verwundbar zu machen.

Wenn der:die *Treugeber:in* dieses *Risiko* eingeht, geht er:sie davon aus, dass der:die *Treuhänder:in* in einer Weise handeln wird, die dem Wohlergehen des:der *Treugeber:in* förderlich ist, obwohl die Handlungen des:der *Treuhänder:in* außerhalb der Kontrolle des:der *Treugeber:in* liegen.“

(Vergleiche Schilke et al. 2021.)

# (Wie) Kann man „Vertrauen“ modellieren und messen?

(Vergleiche Li et al. 2008.)

# Vertrauen zu quantifizieren, ist kompliziert

(Vergleiche Li et al. 2008.)

# Ausblick: Ein Ansatz, Vertrauen zu quantifizieren

(Vergleiche Li et al. 2008.)

# Welche Rolle spielt Vertrauen in der IT-Sicherheit?

# Vertrauen in der IT-Sicherheit

- User:innen vertrauen Dienstleister:innen. (?)
- Entwickler:innen vertrauen Libraries etc. (?)
- Firmen vertrauen anderen Firmen. (?)
- Studierende vertrauen Lehrenden. ;) (?)
- Lehrende vertrauen Studierenden. (?)
- Menschen vertrauen öffentlichen Organisationen/Entitäten. (?)
- E-Mail-Empfänger:innen vertrauen CAs. (?)
- ...
  
- *(Reminder)* vergangene Vorlesung: „Chain of Trust“

# Misstrauen

- en. „Mistrust“  $\neq$  „Distrust“
- **Übersetzung von DeepL:** „Es gibt kaum einen Unterschied zwischen diesen beiden Wörtern, aber *Misstrauen (distrust)* ist *gebräuchlicher* und *vielleicht etwas stärker*. Wenn Sie **sicher** sind, dass jemand unehrlich handelt oder man sich nicht auf ihn verlassen kann, werden Sie eher sagen, dass Sie ihm misstrauen (distrust). Wenn Sie dagegen **Zweifel und Verdächtigungen** äußern, würden Sie wahrscheinlich Misstrauen (mistrust) verwenden.“
- konzeptuell *beide* Begriffe relevant
- verschiedene Vertrauens-, aber auch Misstrauensgrade

(Vergleiche

[https://www.oxfordlearnersdictionaries.com/definition/english/mistrust\\_1.](https://www.oxfordlearnersdictionaries.com/definition/english/mistrust_1.))

# 100%ige Sicherheit == 100%iges Misstrauen?

- Nur Open Source Programme?
- Jede Zeile Code verstehen?
- Compiler auch Open Source?
- Betriebssystem auch Open Source?
- Hardware-Spezifikation Open Source?
- Hardware-Fertigung?
- ...

⇒ *Trade-off*: Technologie nicht verwenden vs. trotz Misstrauen verwenden ...

# Vertrauen ist auch wirtschaftlich wichtig

(Vergleiche <https://hbr.org/2023/07/companies-need-to-prove-they-can-be-trusted-with-technology>.)

Was sind Probleme, die durch  
„unangebrachtes“ Vertrauen  
– aber auch Misstrauen –  
auftreten (können)?

# User:innen haben unangebrachtes Vertrauen ...

- ... geben sensible Daten preis.
- ... verlieren Geld.
- ... unterstützen Entitäten, die ihren eigenen Werten widersprechen.
- ... gefährden ihre eigene „digitale“ oder physische Sicherheit!
- ... gefährden andere!
- ...

# User:innen haben unangebrachtes (?) Misstrauen ...

- ... verwenden keine Passwortmanager, biometrische Auth. etc.  
⇒ *potenziell unsicherere Methoden, z.B. Passwörter auf Zettel, überall dasselbe Passwort.*
- ... verwenden überhaupt keine Computer/Smartphones.  
⇒ *in Berufswahl etc. eingeschränkt. Akzeptabler Trade-off?*
- ... misstrauen der Wissenschaft.  
⇒ *potenzielle Selbst-/Fremdgefährdung, z.B. die Eibe hat so schöne Beeren, die können gar nicht giftig sein ...*
- ... misstrauen uns als Techniker:innen.  
⇒ *potenzielle Selbst-/Fremdgefährdung, z.B. ich repariere mein Auto selbst, obwohl ich mich nicht auskenne ...*

# Kann **Misstrauen** überhaupt unangebracht sein?

⇒ (bzw.) Kann man „beweisen“, dass es unangebracht ist?

- ... verwenden keine Passwortmanager, biometrische Auth. etc.

⇒ *Es gibt immer wieder Security-Incidents!*

*Alternative: z.B. Passwörter selbst verschlüsseln ....*

- ... verwenden überhaupt keine Computer/Smartphones.

⇒ *Überwiegen die Nachteile wirklich die Vorteile?*

- ... misstrauen der Wissenschaft.

⇒ *Auch Wissenschaftler:innen können irren, unethisch handeln, ...*

- ... misstrauen uns als Techniker:innen.

⇒ *Auch Mechaniker:innen können irren, unethisch handeln, ...*

# Welche Faktoren beeinflussen *Vertrauen?*

# Faktoren für Vertrauen – eine unvollständige Auswahl ...

- Vertrauenshaltung
- Reputation
- Kosten/Nutzen-Rechnung
- Technologische situative Normalität
- Technologische Struktursicherheit
- Organisatorische situative Normalität
- Organisatorische Struktursicherheit
- Subjektive Norm
- ...
- **Usability**

(Vergleiche Li et al. 2008 & Ziegler Acemyan und Kortum 2012.)

# Security vs. Usability/HCI vs. Usable Security

Drei Perspektiven:

- **Sicherheitszentriert:** Security hat Vorrang, Usability hat Nachrang.
- **Usability-/HCI-zentriert:** Der Mensch, i.e. Usability, steht im Zentrum, Security hat Nachrang.
- **Usable Security:** Mensch und Security sind *beide* gleichrangig!

⇒ Können Sicherheit und Usability *gleichzeitig* maximiert werden?

(Vergleiche Mathiasen und Bødker 2008.)

# xkcd: UI Change (no. 1770)

(Vergleiche [https://xkcd.com/1770/.](https://xkcd.com/1770/))

# Usability – eine Definition



(Bild generiert mit ChatGPT)

*„Usability (dt. Benutzer:innenfreundlichkeit/Benutzbarkeit) ist das Ausmaß, zu welchem ein Produkt von bestimmten Nutzer:innen verwendet werden kann, um bestimmte Ziele mit Wirksamkeit, Effizienz und Zufriedenheit in einem bestimmten Nutzungskontext zu erreichen.“*

(Vergleiche ISO – International Organization for Standardization.)

# Sicherheit – eine Definition

(Wiederholung aus der ersten Vorlesungseinheit)

- Definition nach DIN VDE 31000

- „Sicherheit ist eine Sachlage, bei der das [Rest-]Risiko nicht größer als das Grenzkrisiko ist.“
- „Das Grenzkrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes.“
- „Eine absolute Sicherheit ohne jegliches Risiko gibt es weder in der Technik noch in der Natur.“

- Risiko = Schaden \* Eintrittswahrscheinlichkeit



(Bild generiert mit ChatGPT)

Wie lautet – basierend darauf –  
eine Definition von  
*Usable Security*?

# Usable Security – eine Definition?

- keine formale Definition von *Usable Security*
- Fokus auf praktische Probleme (i.e. im Anwendungskontext)
- beschäftigt sich mit dem Zusammenspiel von Sicherheit und Usability.
- zentrale „Probleme“:
  - Authentifizierung
  - Verschlüsselung
  - Security Dialoge
  - Social Engineering (nächste Vorlesungseinheit!)
  - Privacy

# 10 Prinzipien von Usable Security (1-3)

1. **Der Weg des geringsten Widerstands:** Die einfachste Art, eine Aufgabe zu erledigen, sollte gleichzeitig die „sicherste“ sein.
2. **Aktive Autorisierung:** Nutzer:innen erteilen Berechtigungen durch bewusste Handlungen, die ihre Zustimmung signalisieren.
3. **Widerrufbarkeit:** Nutzer:innen sollte es leicht gemacht werden, einmal erteilte Berechtigungen zu widerrufen.

(Vergleiche Payne und Edwards 2008,  
basierend auf Yee 2002.)

# 10 Prinzipien von Usable Security (4-7)

4. **Sichtbarkeit:** Nutzer:innen sollen genau wissen, wer Zugriff auf ihre Ressourcen hat und welche Befugnisse diese Personen haben.
5. **Selbstwahrnehmung:** Nutzer:innen sollen ihr eigenes Autoritätsniveau im System verstehen.
6. **Vertrauenswürdiger Pfad:** Jene „Wege“, über die Nutzer:innen ihre Sicherheitseinstellungen verwalten, sollten geschützt sein.
7. **Ausdrucksfähigkeit:** Nutzer:innen sollten in der Lage sein, ihre Sicherheitspräferenzen in einer Weise auszudrücken, die ihren Aufgaben und ihrem Verständnis entspricht.

(Vergleiche Payne und Edwards 2008,  
basierend auf Yee 2002.)

# 10 Prinzipien von Usable Security (8-10)

8. **Relevante Grenzen:** Das System sollte klare Unterschiede zwischen verschiedenen Objekten und Aktionen machen, insbesondere in für die Aufgaben der Nutzer:innen relevanten Kontexten.
9. **Identifizierbarkeit:** Objekte und Aktionen im System sollten leicht unterscheidbar und „ehrlich“ präsentiert werden.
10. **Voraussicht:** Die Folgen von Entscheidungen, die Nutzer:innen treffen sollen, müssen für sie klar ersichtlich sein.

(Vergleiche Payne und Edwards 2008,  
basierend auf Yee 2002.)

*„Der Unterschied zwischen einem schlechten und einem guten Interface kann die Fähigkeit der Nutzer:innen beeinflussen, Aufgaben sicher auszuführen.“*

– Payne und Edwards, 2008.

# Alles OK?!



(Bild generiert mit ChatGPT)

# ERROR?!



(Bild generiert mit ChatGPT)

# Fünf Lektionen zu Usable Security (1-3)

1. **(Usable) Security kann nicht nachträglich eingeführt werden.** Sicherheit und Benutzer:innenfreundlichkeit/Benutzbarkeit (en. Usability) von Anfang an in Systeme integrieren  $\Rightarrow$  auch *Usable Security* von Beginn an mitdenken.
2. **Werkzeuge sind keine (fertigen) Lösungen.** SSL, IPsec etc. sind wertvoll, da sichere Basis für Anwendung. Anwendung trotzdem unsicher, wenn User:innen dazu verleitet, sie falsch zu nutzen.
3. **Die „oberen Ebenen“ müssen beachtet werden.** z.B. Sicherheit nur auf Netzwerkebene „denken“  $\Rightarrow$  User:innen agieren bei Problemen auch auf dieser Ebene  $\Rightarrow$  Probleme treten unweigerlich auf.

(Vergleiche Balfanz et al. 2004.)

# Fünf Lektionen zu Usable Security (4-5)

4. **Kund:innen/Nutzer:innen müssen zufrieden gehalten werden.** Nur, weil Sicherheit für Expert:innen wichtig, heißt nicht, dass Nutzer:innen genauso sehen.
5. **Lokal denken, lokal handeln.** *Beispiel:* Zertifikat hat außerhalb der E-Mail-Anwendung Bedeutung/Verwendung ⇒ Konzept/Anwendungsbereich für User:innen schwerer überblickbar.

(Vergleiche Balfanz et al. 2004.)

*„Sicherheit ist nicht etwas, das nur in den unteren Schichten des Network-Stacks oder in den Tiefen des Betriebssystems zu behandeln ist.“*

– Balfanz et al. 2004.

*„Wir müssen Systeme entwickeln, die gleichzeitig  
(be)nutzbar und sicher sind.“*

– Balfanz et al. 2004.

# Wie können wir derartige Systeme entwickeln?

# Ausblick: User-Centered Design (UCD)

- dt. „Nutzer:innen-orientierte Gestaltung“
- ganzheitlicher Ansatz
- *Ziel*: optimale User Experience
- vier Bausteine:
  - Verstehen ⇒ *User Research*
  - Explorieren ⇒ *Explorative Design, Speculative Design, ...*
  - Entwerfen ⇒ Design Methoden
  - Testen ⇒ *User Testing*, Testen nicht nur auf Code-Ebene!

(Vergleiche <https://www.usability.de/leistungen/ux-design.html> & <https://www.interaction-design.org/literature/topics/user-centered-design>.)

# Quellen und Literatur 1/5

- Oliver Schilke, Martin Reimann, und Karen S Cook. **Trust in social relations.** *Annual Review of Sociology*, 47:239–259, 2021.  
doi: [10.1146/annurev-soc-082120-082850](https://doi.org/10.1146/annurev-soc-082120-082850)
- Bryan D Payne und W Keith Edwards. **A brief introduction to usable security.** *IEEE Internet Computing*, 12(3):13–21, 2008.  
doi: [10.1109/MIC.2008.50](https://doi.org/10.1109/MIC.2008.50)
- Mary Theofanos. **Is Usable Security an Oxymoron?** *Computer*, 53(2):71–74, 2020.  
doi: [10.1109/MC.2019.2954075](https://doi.org/10.1109/MC.2019.2954075)

## Quellen und Literatur 2/5

- Claudia Ziegler Acemyan und Philip Kortum. *The relationship between trust and usability in systems.*

In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Band 56, Seiten 1842–1846. SAGE Publications Sage CA: Los Angeles, CA, 2012.

doi: [10.1177/1071181312561371](https://doi.org/10.1177/1071181312561371)

- Dirk Balfanz, Glenn Durfee, Diana K Smetters, und Rebecca E Grinter. *In Search of Usable Security: Five Lessons from the Field.*

*IEEE Security & Privacy*, 2(5):19–24, 2004.

doi: [10.1109/MSP.2004.71](https://doi.org/10.1109/MSP.2004.71)

## Quellen und Literatur 3/5

- Markus Lennartsson, Joakim Kävrestad, und Marcus Nohlberg. [Exploring the meaning of usable security—a literature review.](#)  
*Information & Computer Security*, 29(4):647–663, 2021.  
[doi: 10.1108/ICS-10-2020-0167](#)
- Harshul Garg, Tanupriya Choudhury, Praveen Kumar, und Sai Sabitha. [Comparison between significance of usability and security in HCI.](#)  
In *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, Seiten 1–4, 2017.  
[doi: 10.1109/CIACT.2017.7977269](#)

# Quellen und Literatur 4/5

- Xin Li, Traci J Hess, und Joseph S Valacich. [Why do we trust new technology? A study of initial trust formation with organizational information systems.](#) *The Journal of Strategic Information Systems*, 17(1):39–71, 2008.  
doi: [10.1016/j.jsis.2008.01.001](https://doi.org/10.1016/j.jsis.2008.01.001)
- Ronald Kainda, Ivan Fléchais, und Andrew William Roscoe. [Security and Usability: Analysis and Evaluation.](#)  
In *2010 International Conference on Availability, Reliability and Security*,  
Seiten 275–282, 2010.  
doi: [10.1109/ARES.2010.77](https://doi.org/10.1109/ARES.2010.77)

# Quellen und Literatur 5/5

- Niels Raabjerg Mathiasen und Susanne Bødker. [Threats or Threads: From Usable Security to Secure Experience?](#)

NordiCHI '08, Seiten 283–289, New York, NY, USA, 2008. Association for Computing Machinery.

[ISBN 9781595937049.](#)

[doi: 10.1145/1463160.1463191](#)

# Zusammenfassung: Vertrauen

- Vertrauen ist ein schwer „greifbares“ Konstrukt, aber von hoher Wichtigkeit bei der Verwendung/Gestaltung von Technologien.
- Sowohl Vertrauen als auch Misstrauen können bei Fehleinschätzung schwerwiegende Folgen haben.
- Da Vertrauen ein komplexes Konzept ist, ist es schwer zu quantifizieren, welche Faktoren wie viel Einfluss auf das erteilte Vertrauen nehmen.
- Vertrauen scheint unweigerlich mit IT-Sicherheit und Usability verknüpft.

# Zusammenfassung: Usable Security

- Es gibt verschiedene Perspektiven auf Usability und IT-Sicherheit, zwei (nicht zwangsläufig?) gegensätzliche Konzepte.
- Usable Security beschreibt den Versuch, IT-Sicherheit und Usability gleichzeitig zu optimieren.
- User-Centred Design ist eine zielführende Perspektive, um Usable Security zu erreichen.

**Vielen Dank!**

<https://establishing-security.at/>