

## HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:

LOOK FOR THIS  
TEXT AT THE TOP:



# Gründe für die geringe Verbreitung von Emailkryptographie

## Studienauswertung

Ulrich Dorsch, Tim Grocki, Leonhard Hösch  
[ulrichdorsch@gmail.com](mailto:ulrichdorsch@gmail.com), [tgrocki@lavabit.com](mailto:tgrocki@lavabit.com), [lh@dancingwolf.de](mailto:lh@dancingwolf.de)

Friedrich-Alexander-Universität Erlangen  
Department Informatik  
Lehrstuhl 1 - Human Factors in IT Security

July 10, 2013

# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion

# Motivation

- E-Mail-Kryptographie ist nicht weit verbreitet, obwohl es viele Gründe für deren Einsatz gibt.
- Es wird oft vermutet, dass schlechte Benutzerfreundlichkeit der Grund für die geringe Verbreitung ist.
- Wir haben dies mit unserer Studie überprüft.

# Forschungsfrage

Sind Usability-Probleme tatsächlich die Hauptgründe für die geringe Verbreitung von E-Mail-Kryptographie?

# Forschungsfrage

Sind Usability-Probleme tatsächlich die Hauptgründe für die geringe Verbreitung von E-Mail-Kryptographie?

Welche anderen Ursachen spielen eine (wie große) Rolle?

# Hypothese

Usability-Probleme im Zusammenhang mit Kryptographie-Software sind nicht die primäre Ursache für die geringe Verbreitung von E-Mail-Kryptographie, da mehr als 50% der potenziellen Nutzer durch andere Ursachen davon abgehalten werden, E-Mail-Kryptographie zu nutzen.

# Hypothese

Usability-Probleme im Zusammenhang mit Kryptographie-Software sind nicht die primäre Ursache für die geringe Verbreitung von E-Mail-Kryptographie, da mehr als 50% der potenziellen Nutzer durch andere Ursachen davon abgehalten werden, E-Mail-Kryptographie zu nutzen.

## Usability-Problem – Definition

In unserem Kontext betrachten wir ein Usability-Problem als eine technische Hürde, die die Benutzung von E-Mail-Kryptographie verhindert oder deutlich erschwert.




# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion

# NSA-Skandal

- Der NSA-Skandal ging im Zeitraum unserer Umfrage durch alle Medien <sup>2</sup>
- Überwachung des Internets, insbesondere von E-Mails
- Überwachung auch in Deutschland
- ⇒ Erhöhtes Bewusstsein für IT-Sicherheit und die Existenz von Eingriffen in die Privatsphäre

---

<sup>2</sup><http://www.tagesschau.de/ausland/spionageaffaere100.html> 

# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion

# Zielgruppe

Studierende (an der technischen Fakultät der Universität Erlangen)

# Zielgruppe

Studierende (an der technischen Fakultät der Universität Erlangen)

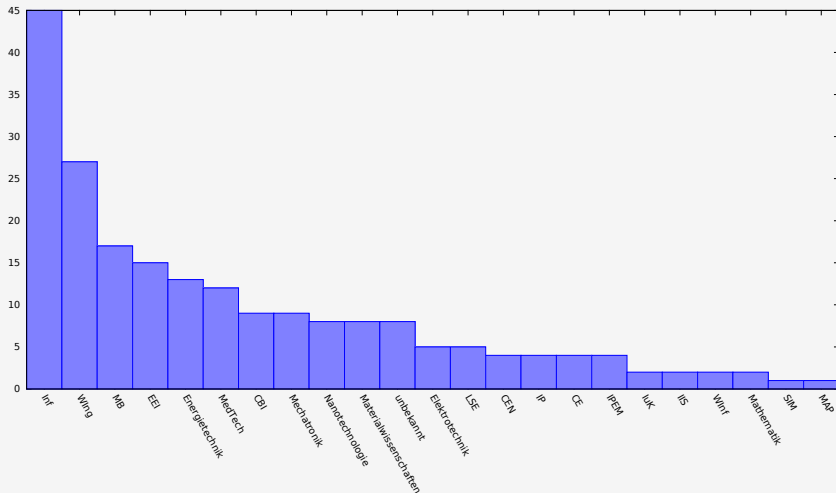
- einfach zu erreichen
- höchstwahrscheinlich aktive Nutzer von E-Mail-Kommunikation
- ca. 9000 Personen

# Rücklauf

- 207 vollständige und verwertbare Rückläufer
- ca. 2,3% der vorhandenen Zielgruppe
- Rückläufer aus diversen Studienfächern

# Demographische Daten

## Studienfächer



# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion



# Interesse an E-Mail-Kryptographie

Halten Sie das Verschlüsseln von E-Mails für sich persönlich für sinnvoll?

Ja	51%
Nein	41%
keine Antwort	8%

# Interesse an E-Mail-Kryptographie

Halten Sie das Verschlüsseln von E-Mail im Allgemeinen für sinnvoll?

Ja	87%
Nein	6%
keine Antwort	7%

# Interesse an E-Mail-Kryptographie

Hätten Sie gerne die Möglichkeit, mit Banken oder ähnlichen Institutionen/Unternehmen verschlüsselt zu kommunizieren?

Ja	83%
Nein	7%
keine Antwort	10%

# Interesse an E-Mail-Kryptographie

Würden Sie sich wünschen, dass Unternehmen wie z.B. Banken intern verschlüsselt kommunizieren?

Ja	85%
Nein	6%
keine Antwort	9%

# Bekanntheit von Gefahren

Eine unverschlüsselte E-Mail, die Sie versenden, kann auf dem Zustellweg von einem Angreifer mitgelesen und verändert werden.

Wussten Sie das?

Ja	82%
Nein	15%
keine Antwort	2%

# Bekanntheit von Gefahren

E-Mails können mit sehr geringem Aufwand unter falschem Absender versendet werden, wenn diese nicht kryptographisch signiert sind.

Wussten Sie das?

Ja	68%
Nein	29%
keine Antwort	3%

# Bekanntheit von Gefahren

Sollte ein Angreifer (Hacker) administrative Zugriffsrechte auf den Server einer Firma erlangen kann dieser alle unverschlüsselten E-Mails der Firma lesen oder sogar verändern.

Wussten Sie das?

Ja	84%
Nein	14%
keine Antwort	3%

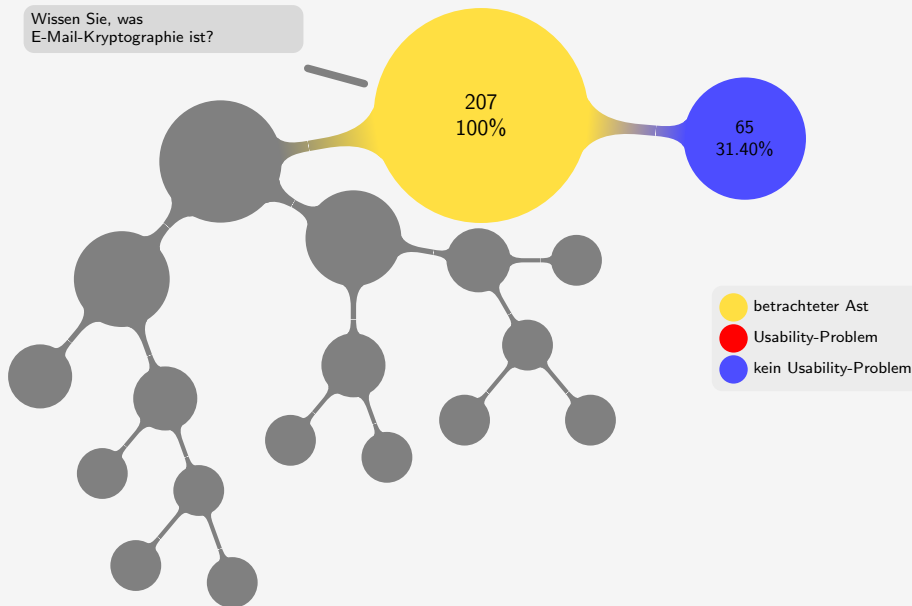
# Fragebogenverlauf

Der Rest des Fragebogens ist baumartig strukturiert, sodass eine Einteilung in verschiedene Kategorien leichtfällt.

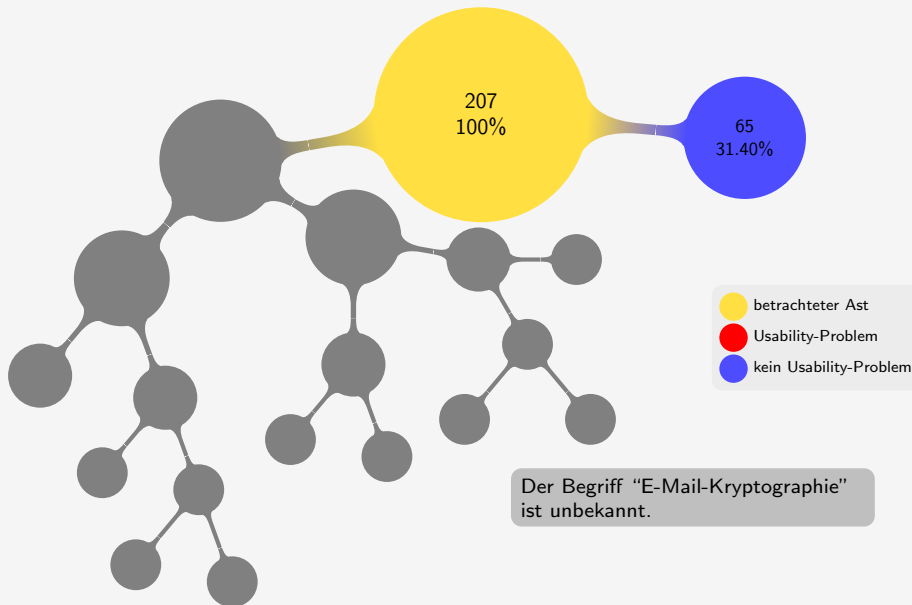


# Fragebogenverlauf

Wissen Sie, was  
E-Mail-Kryptographie ist?

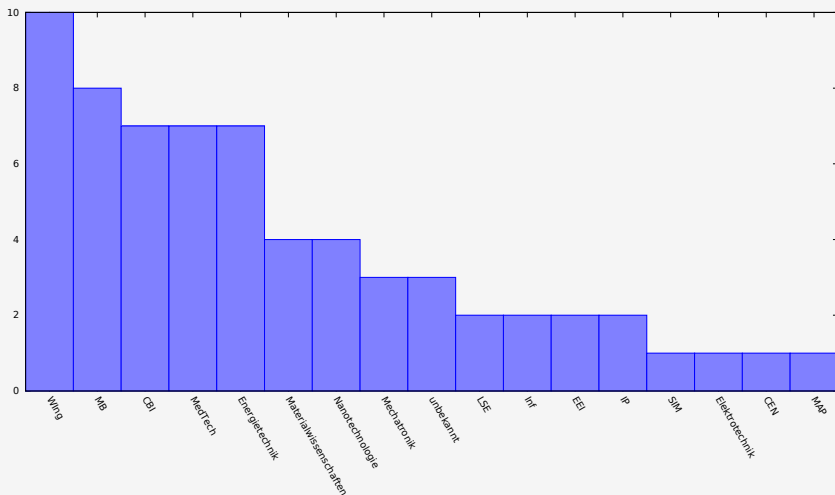


# Fragebogenverlauf



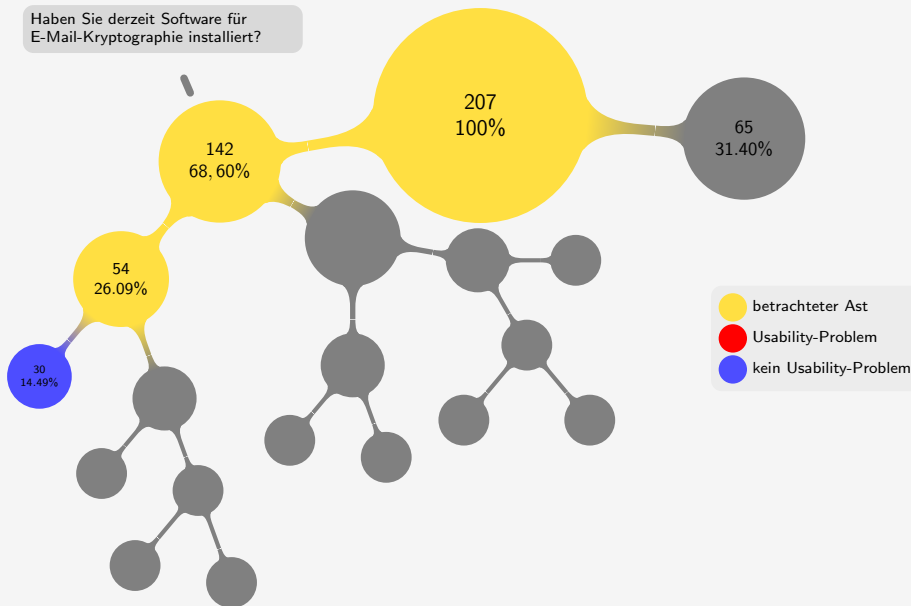
# Details

## Studienfächer



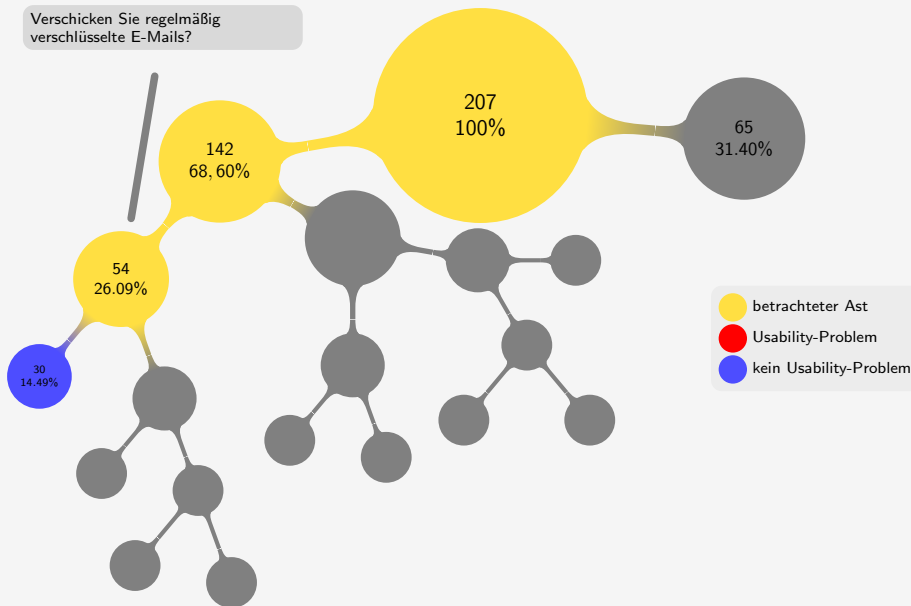
# Fragebogenverlauf

Haben Sie derzeit Software für  
E-Mail-Kryptographie installiert?

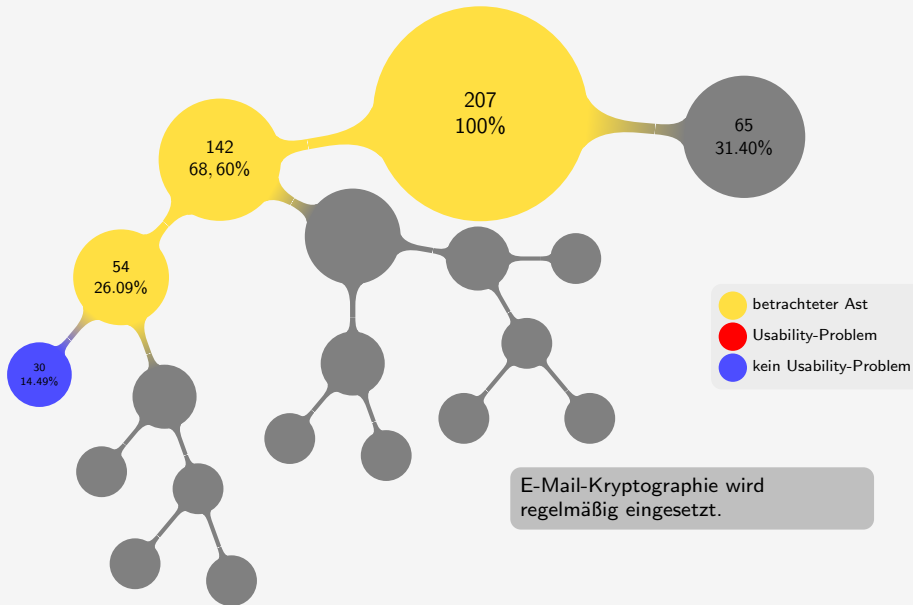


# Fragebogenverlauf

Verschicken Sie regelmäßig  
verschlüsselte E-Mails?

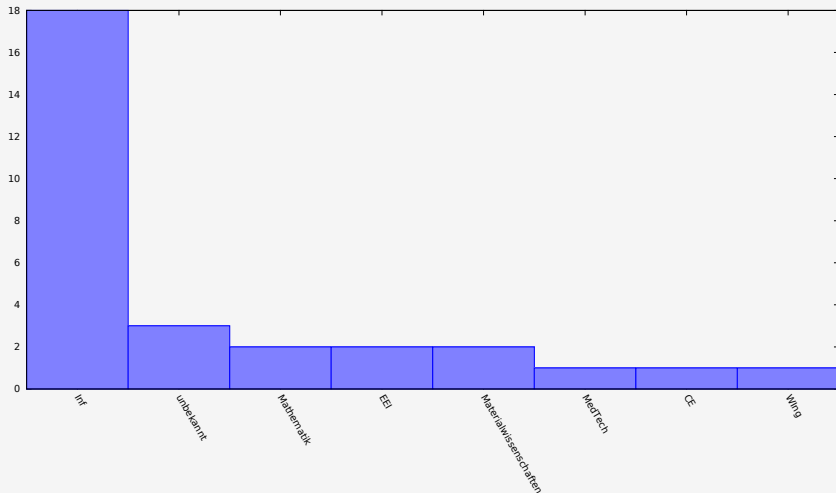


## Fragebogenverlauf



# Details

## Studienfächer



## Details

30 Befragte, die E-Mail-Kryptographie regelmäßig einsetzen:



# Details

30 Befragte, die E-Mail-Kryptographie regelmäßig einsetzen:

- 29 finden, dass ihre Software einfach zu bedienen ist
- 1 Informatiker (12. Semester, E-Mail-Client: Thunderbird, OS: Linux) findet seine Software schwer zu bedienen

## Details

30 Befragte, die E-Mail-Kryptographie regelmäßig einsetzen:

- 29 finden, dass ihre Software einfach zu bedienen ist
- 1 Informatiker (12. Semester, E-Mail-Client: Thunderbird, OS: Linux) findet seine Software schwer zu bedienen
- Die Studierenden verschicken im Durchschnitt 8.5 verschlüsselte Mails im Monat (Standardabw.: 8.3, Maximum: 30)

## Details

30 Befragte, die E-Mail-Kryptographie regelmäßig einsetzen:

- 29 finden, dass ihre Software einfach zu bedienen ist
- 1 Informatiker (12. Semester, E-Mail-Client: Thunderbird, OS: Linux) findet seine Software schwer zu bedienen
- Die Studierenden verschicken im Durchschnitt 8.5 verschlüsselte Mails im Monat (Standardabw.: 8.3, Maximum: 30)
- Die Studierenden haben im Durchschnitt 4.1 Kontakte, mit denen sie verschlüsselt kommunizieren können (Standardabw.: 5.2, Maximum: 25)

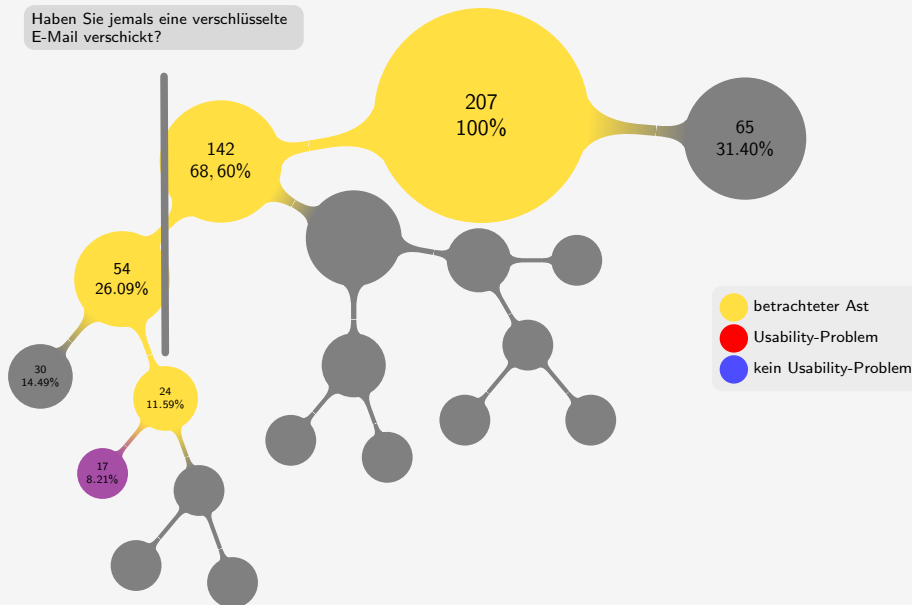
## Details

30 Befragte, die E-Mail-Kryptographie regelmäßig einsetzen:

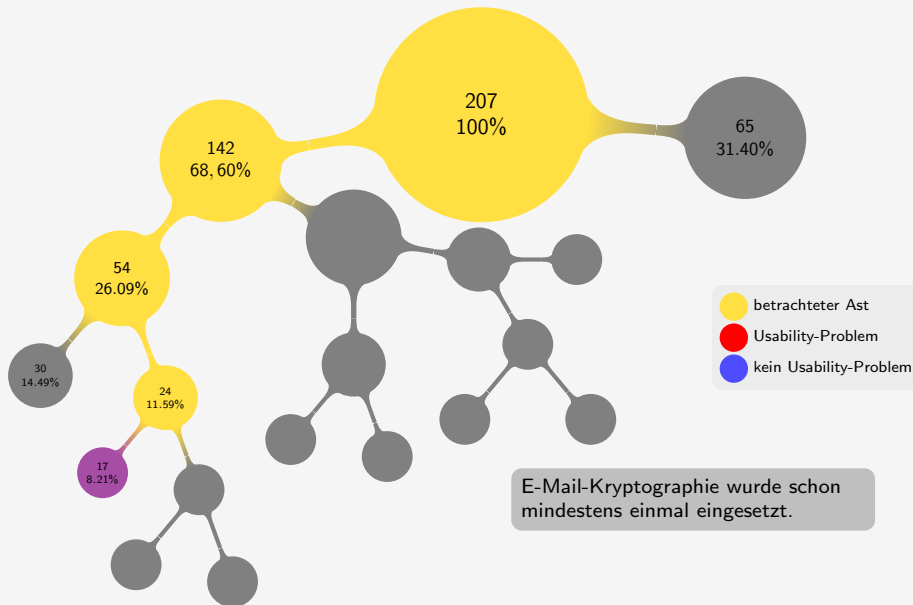
- 29 finden, dass ihre Software einfach zu bedienen ist
- 1 Informatiker (12. Semester, E-Mail-Client: Thunderbird, OS: Linux) findet seine Software schwer zu bedienen
- Die Studierenden verschicken im Durchschnitt 8.5 verschlüsselte Mails im Monat (Standardabw.: 8.3, Maximum: 30)
- Die Studierenden haben im Durchschnitt 4.1 Kontakte, mit denen sie verschlüsselt kommuniziert können (Standardabw.: 5.2, Maximum: 25)
- 17 Studierenden nutzen Thunderbird, 8 OS X Mail, oft in Kombination mit Webclient und Smartphone

# Fragebogenverlauf

Haben Sie jemals eine verschlüsselte E-Mail verschickt?

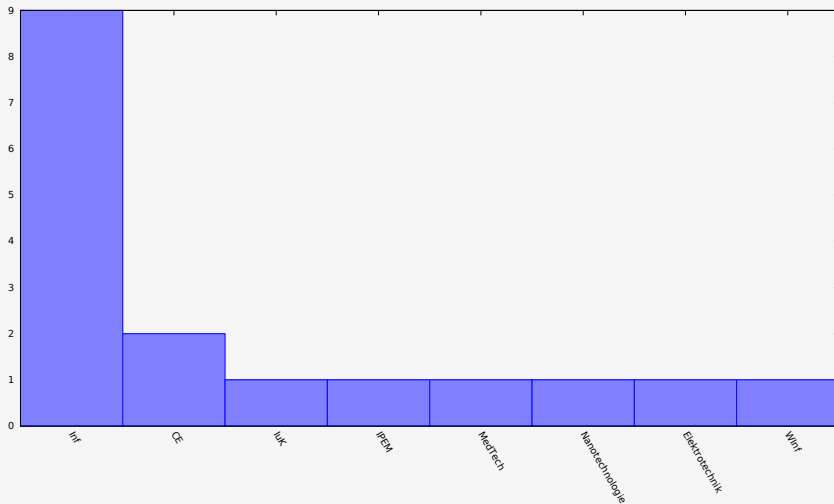


# Fragebogenverlauf



# Details

## Studienfächer



# Details

Usability-Probleme, aufgrund deren E-Mailverschlüsselung nicht (regelmäßig) eingesetzt wird:

- Empfänger können trotz des Besitzes eines PGP-Keys nicht entschlüsseln (z.B. wegen fehlender Software)



# Details

Usability-Probleme, aufgrund deren E-Mailverschlüsselung nicht (regelmäßig) eingesetzt wird:

- Empfänger können trotz des Besitzes eines PGP-Keys nicht entschlüsseln (z.B. wegen fehlender Software)
- Etliche E-Mail-Clients (insb. Webclients) unterstützen keine Verschlüsselung

## Details

Usability-Probleme, aufgrund deren E-Mailverschlüsselung nicht (regelmäßig) eingesetzt wird:

- Empfänger können trotz des Besitzes eines PGP-Keys nicht entschlüsseln (z.B. wegen fehlender Software)
- Etliche E-Mail-Clients (insb. Webclients) unterstützen keine Verschlüsselung
- Absprache mit Kommunikationspartner und Schlüsseltransfer aufwändig

# Details

Usability-Probleme, aufgrund deren E-Mailverschlüsselung nicht (regelmäßig) eingesetzt wird:

- Empfänger können trotz des Besitzes eines PGP-Keys nicht entschlüsseln (z.B. wegen fehlender Software)
- Etliche E-Mail-Clients (insb. Webclients) unterstützen keine Verschlüsselung
- Absprache mit Kommunikationspartner und Schlüsseltransfer aufwändig
- Public-Keys selten veröffentlicht, kein praktikables System für Schlüsselweitergabe vorhanden

## Details

Andere Ursachen, weshalb E-Mail-Verschlüsselung nicht (regelmäßig) eingesetzt wird:

- Kommunikationspartner halten es für unnötig

# Details

Andere Ursachen, weshalb E-Mail-Verschlüsselung nicht (regelmäßig) eingesetzt wird:

- Kommunikationspartner halten es für unnötig
- Meistens sei es wichtiger, dass eine E-Mail ankommt, als dass sie verschlüsselt ist

# Details

Andere Ursachen, weshalb E-Mail-Verschlüsselung nicht (regelmäßig) eingesetzt wird:

- Kommunikationspartner halten es für unnötig
- Meistens sei es wichtiger, dass eine E-Mail ankommt, als dass sie verschlüsselt ist
- Im privaten Umfeld wenig verbreitet

# Details

Andere Ursachen, weshalb E-Mail-Verschlüsselung nicht (regelmäßig) eingesetzt wird:

- Kommunikationspartner halten es für unnötig
- Meistens sei es wichtiger, dass eine E-Mail ankommt, als dass sie verschlüsselt ist
- Im privaten Umfeld wenig verbreitet
- In vielen E-Mails werden keine wichtigen (schützenswerten) Informationen versendet

## Details

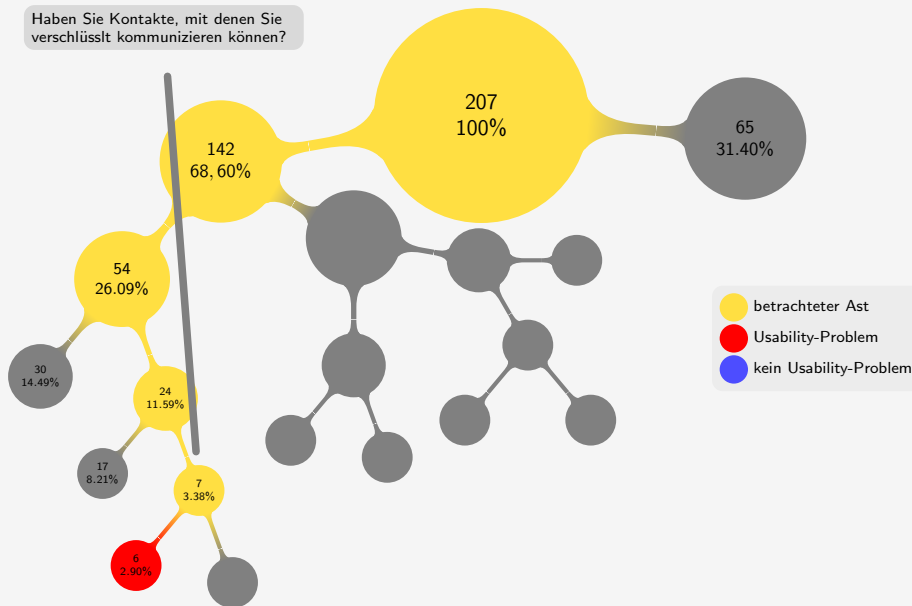
Andere Ursachen, weshalb E-Mail-Verschlüsselung nicht (regelmäßig) eingesetzt wird:

- Kommunikationspartner halten es für unnötig
- Meistens sei es wichtiger, dass eine E-Mail ankommt, als dass sie verschlüsselt ist
- Im privaten Umfeld wenig verbreitet
- In vielen E-Mails werden keine wichtigen (schützenswerten) Informationen versendet
- sensible Daten werden nur persönlich an Vertraute weitergegeben

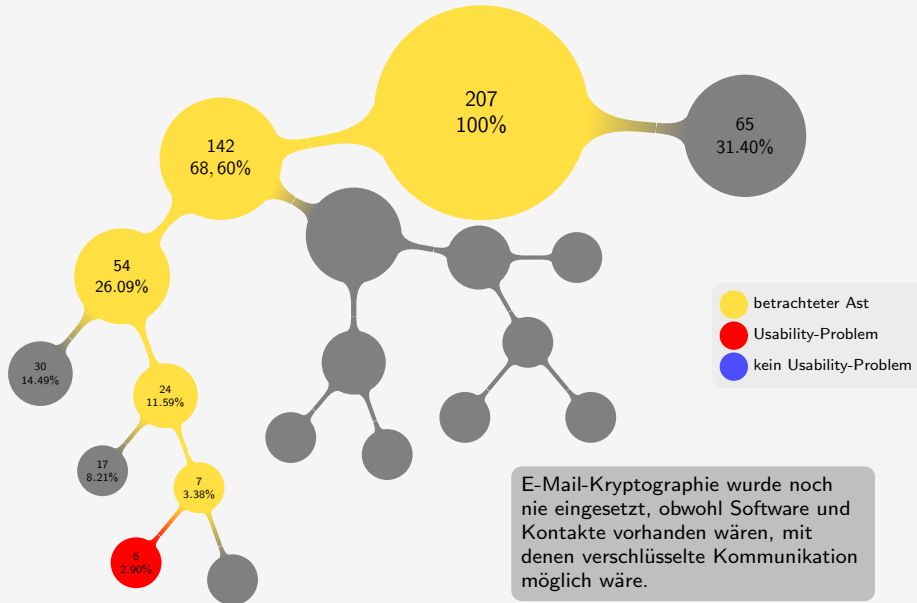


# Fragebogenverlauf

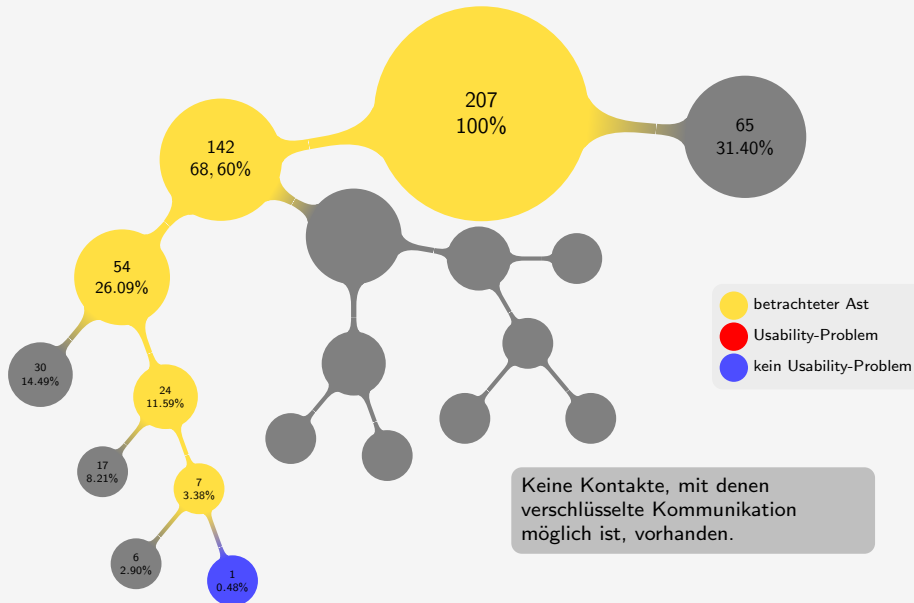
Haben Sie Kontakte, mit denen Sie verschlüsselt kommunizieren können?



# Fragebogenverlauf

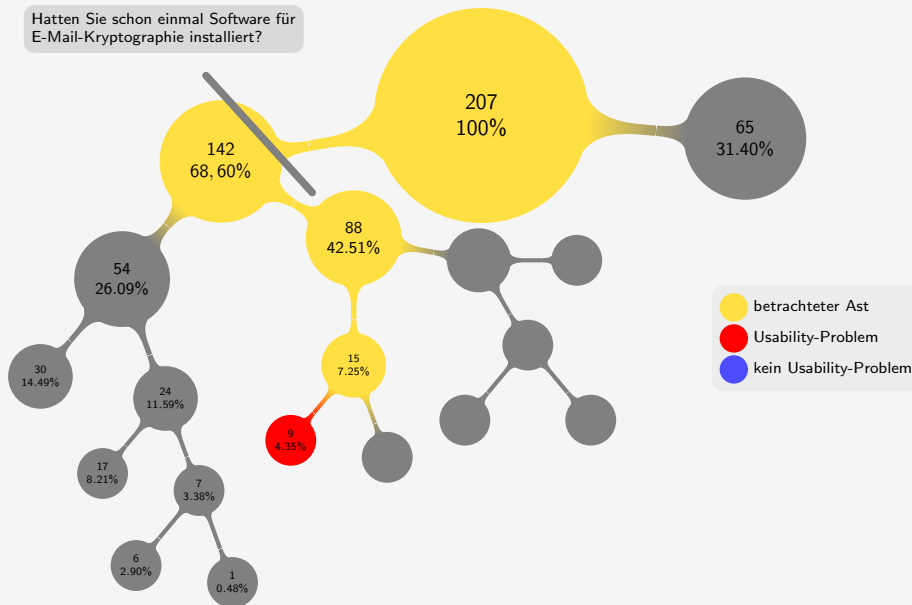


# Fragebogenverlauf



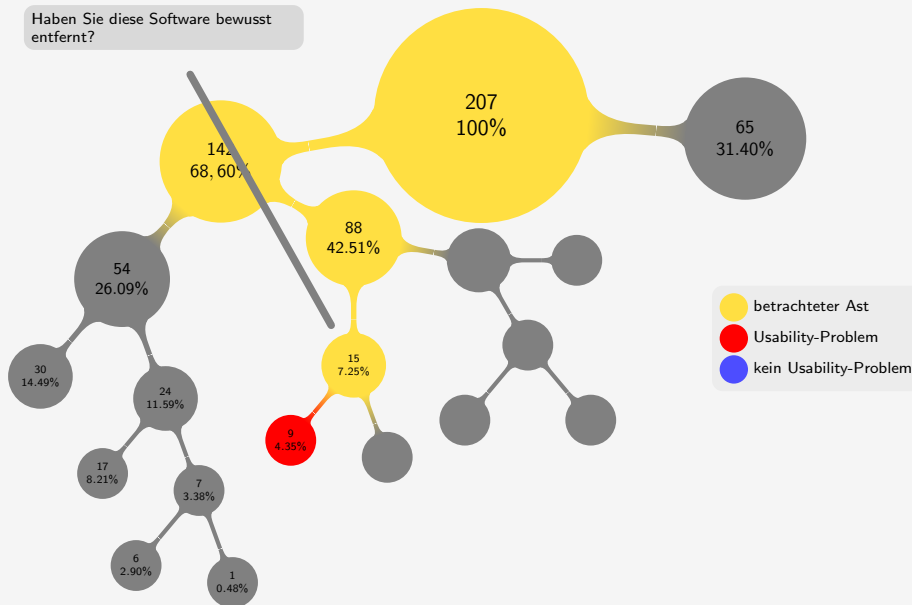
# Fragebogenverlauf

Hatten Sie schon einmal Software für E-Mail-Kryptographie installiert?

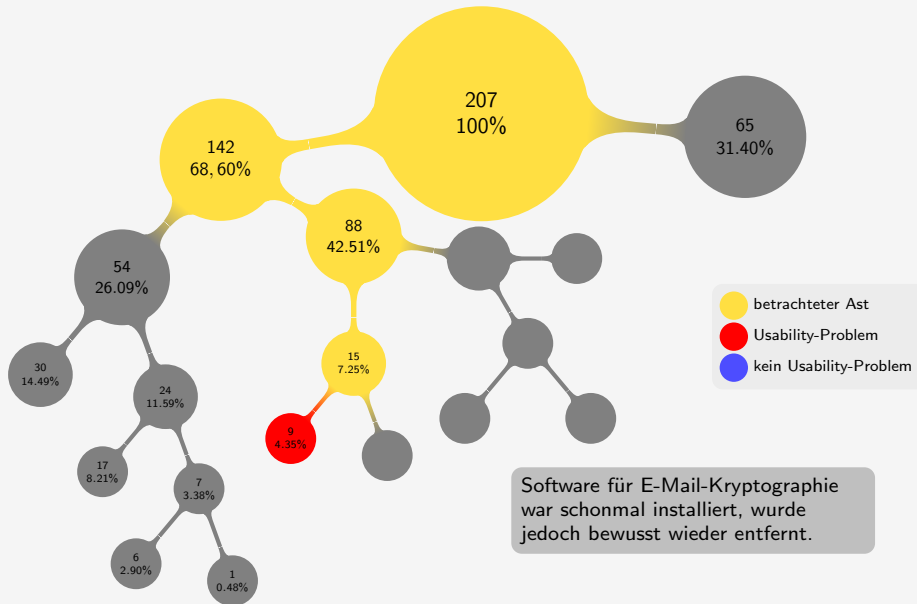


# Fragebogenverlauf

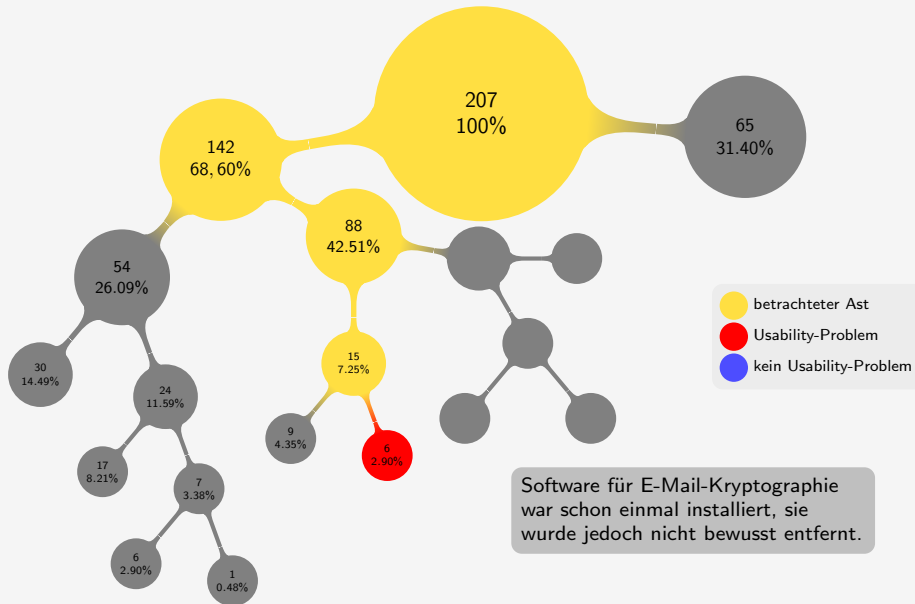
Haben Sie diese Software bewusst entfernt?



# Fragebogenverlauf



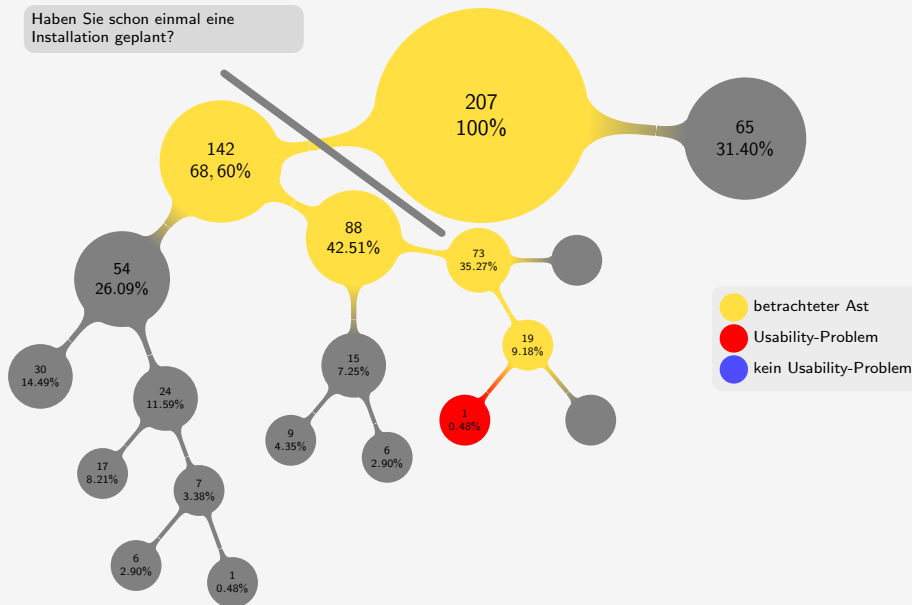
# Fragebogenverlauf



Software für E-Mail-Kryptographie war schon einmal installiert, sie wurde jedoch nicht bewusst entfernt.

# Fragebogenverlauf

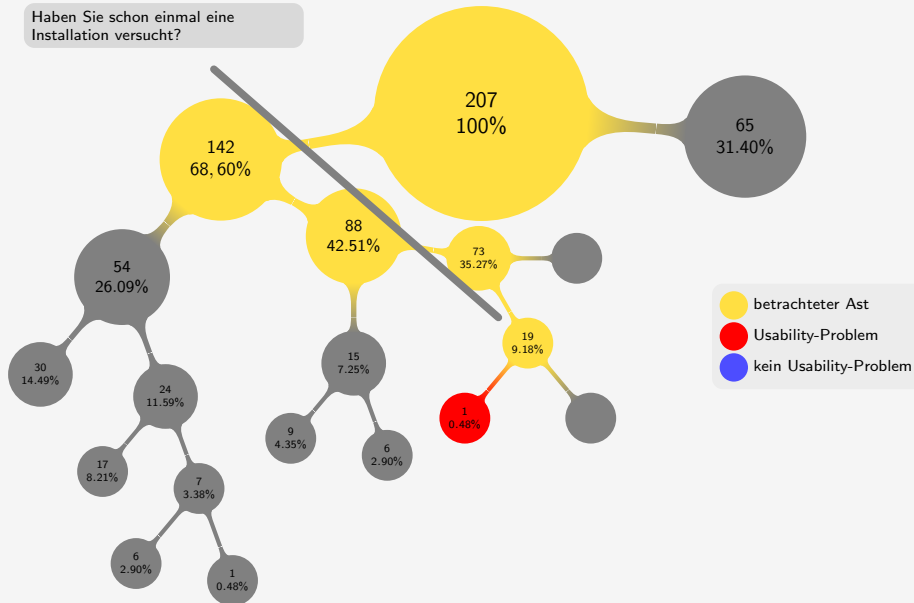
Haben Sie schon einmal eine Installation geplant?



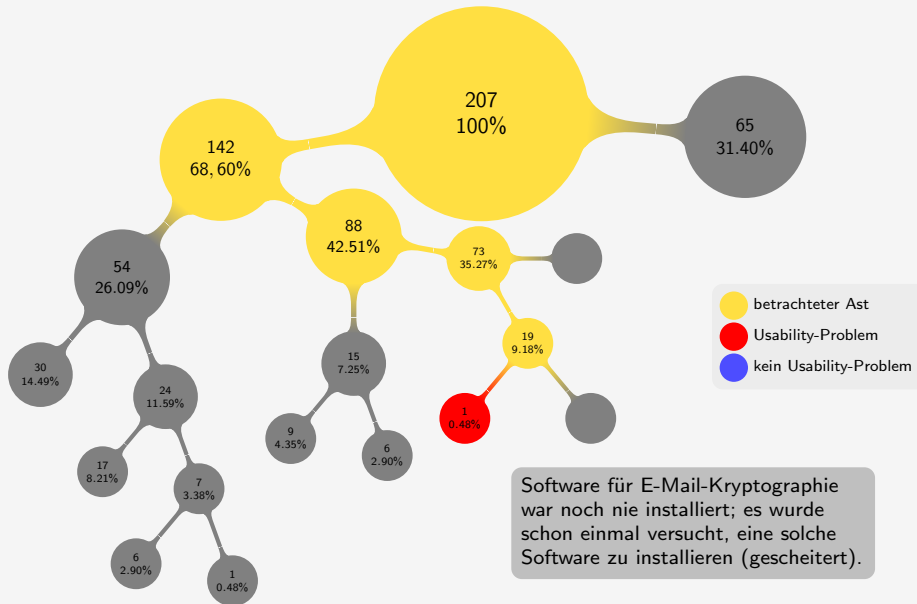


# Fragebogenverlauf

Haben Sie schon einmal eine Installation versucht?



# Fragebogenverlauf

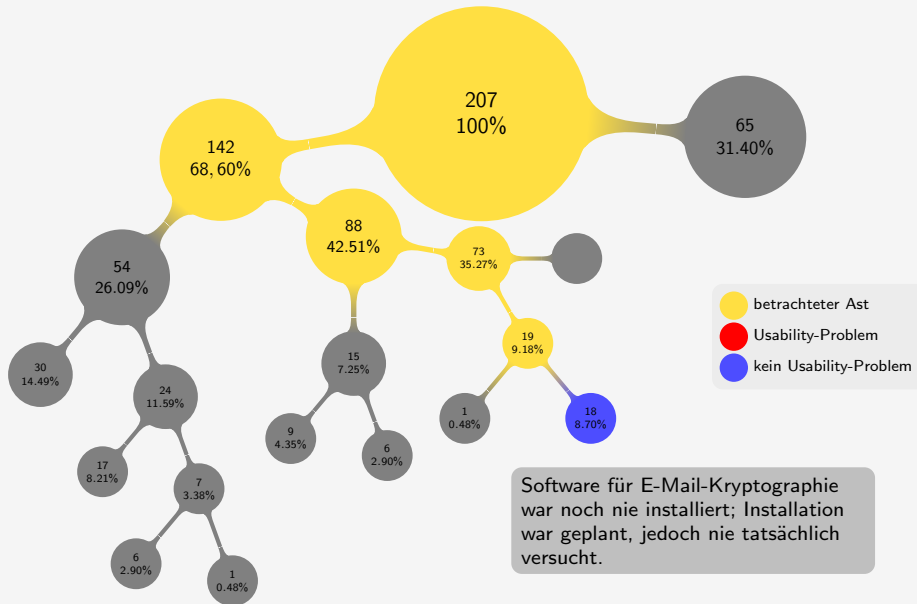


# Details

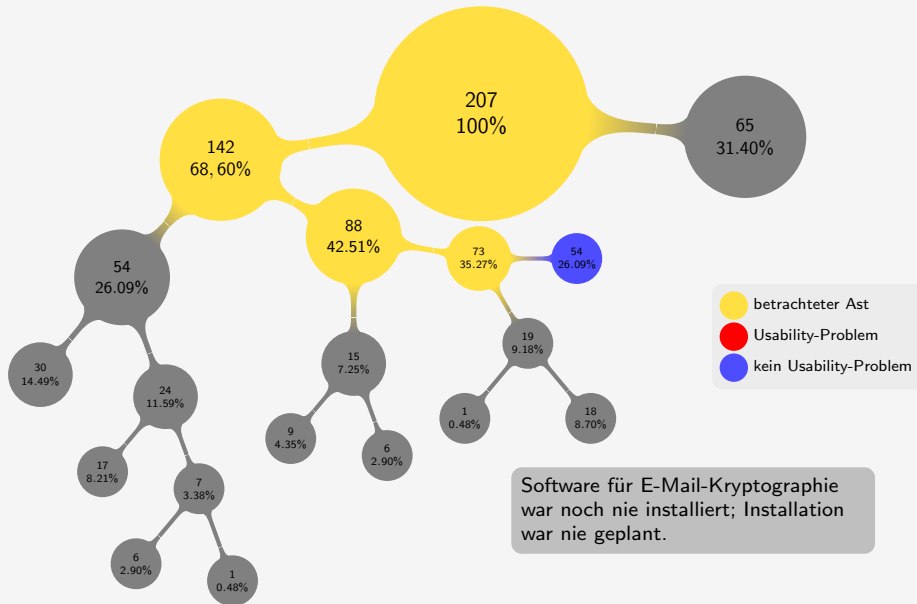
1 Wirtschaftsingenieur (6. Semester, OS: Windows, Client: Thunderbird) hat schon einmal versucht, Software für E-Mail-Kryptographie zu installieren.

Kommentar: "Fehler Meldung! Danach hab ichs deinstalliert, weil eh keiner 'mitmacht' und sich den Aufwand macht. Wenn keiner Verschlüsselung nutzt lohnt der Aufwand (auch wenns eigentlich keiner ist) nicht es ein zweites Mal zu probieren!"

# Fragebogenverlauf

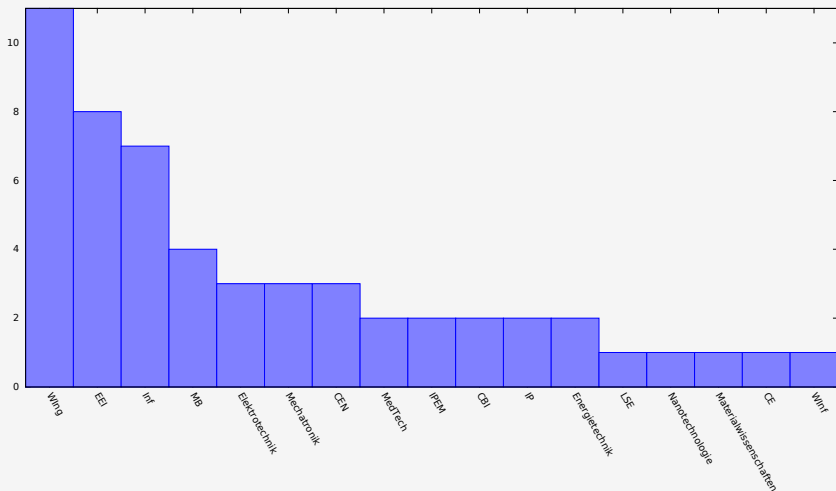


# Fragebogenverlauf



# Details

## Studienfächer



# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion

# Forschungsergebnis

- Von 207 befragten setzen 30 E-Mail-Kryptographie regelmäßig ein
- Von den restlichen 177 werden (konservativ betrachtet) 39 durch Usability-Probleme vom Einsatz von E-Mail-Kryptographie abgehalten; dies entspricht 22.03%
- 77.97% werden also aus anderen Gründen vom Einsatz von E-Mail-Kryptographie abgehalten



# Forschungsergebnis

- Von 207 befragten setzen 30 E-Mail-Kryptographie regelmäßig ein
- Von den restlichen 177 werden (konservativ betrachtet) 39 durch Usability-Probleme vom Einsatz von E-Mail-Kryptographie abgehalten; dies entspricht 22.03%
- 77.97% werden also aus anderen Gründen vom Einsatz von E-Mail-Kryptographie abgehalten
- die Hypothese ist somit bestätigt

## Hypothese

Usability-Probleme von Kryptographie-Software sind nicht die primäre Ursache für die geringe Verbreitung von E-Mail-Kryptographie, da mehr als 50% der potenziellen Nutzer durch andere Ursachen davon abgehalten werden, E-Mail-Kryptographie zu nutzen.

# Forschungsergebnis

- Von 207 befragten setzen 30 E-Mail-Kryptographie regelmäßig ein
- Von den restlichen 177 werden (konservativ betrachtet) 39 durch Usability-Probleme vom Einsatz von E-Mail-Kryptographie abgehalten; dies entspricht 22.03%
- 77.97% werden also aus anderen Gründen vom Einsatz von E-Mail-Kryptographie abgehalten

## andere Probleme

Unwissen (31.40%)

Desinteresse (26.09%)

mangelnde Motivation (8.70%)

mangelnde Verbreitung von E-Mail-Kryptographie (ca. 4.8%)

# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion

# Einschränkungen

- indirekte Effekte schlechter Usability werden nicht betrachtet
- Frage nach dem Begriff “E-Mail-Kryptographie” problematisch
- nur Studierende aus technischen Fächern befragt
- technische Probleme

# Inhalt

- 1 Zielsetzungen der Studie
  - Motivation
  - Forschungsfrage
  - Hypothese
- 2 Umfrageumstände
- 3 Demographische Daten
- 4 Auswertung der Antworten
  - Interesse an E-Mail-Kryptographie
  - Bekanntheit von Gefahren
  - Schema des Fragebogens
- 5 Forschungsergebnis
- 6 Einschränkungen
- 7 Diskussion

# Diskussion

Was könnte man verbessern? Was könnte man in Folgestudien untersuchen?

- Andere Zielgruppen (alle Studierenden an der Universität, Beschäftigte in der Industrie, verschiedene Altersgruppen)

# Diskussion

Was könnte man verbessern? Was könnte man in Folgestudien untersuchen?

- Andere Zielgruppen (alle Studierenden an der Universität, Beschäftigte in der Industrie, verschiedene Altersgruppen)
- Ergänzung durch detailliertere Fragen

# Diskussion

Was könnte man verbessern? Was könnte man in Folgestudien untersuchen?

- Andere Zielgruppen (alle Studierenden an der Universität, Beschäftigte in der Industrie, verschiedene Altersgruppen)
- Ergänzung durch detailliertere Fragen
- Auswertung von Zusammenhängen zwischen Angaben im “Baum” und Interessen- und Wissensfragen



# Diskussion

Was könnte man verbessern? Was könnte man in Folgestudien untersuchen?

- Andere Zielgruppen (alle Studierenden an der Universität, Beschäftigte in der Industrie, verschiedene Altersgruppen)
- Ergänzung durch detailliertere Fragen
- Auswertung von Zusammenhängen zwischen Angaben im “Baum” und Interessen- und Wissensfragen
- Untersuchung einzelner Phänomene (Einfluss des Rufes von E-Mail-Kryptographie auf die Ergebnisse, o.Ä.)

# Diskussion

Was könnte man verbessern? Was könnte man in Folgestudien untersuchen?

- Andere Zielgruppen (alle Studierenden an der Universität, Beschäftigte in der Industrie, verschiedene Altersgruppen)
- Ergänzung durch detailliertere Fragen
- Auswertung von Zusammenhängen zwischen Angaben im “Baum” und Interessen- und Wissensfragen
- Untersuchung einzelner Phänomene (Einfluss des Rufes von E-Mail-Kryptographie auf die Ergebnisse, o.Ä.)
- Wieviele Studierende wissen nicht, was sie studieren? (Studienfach: “Masters”, “Lehramt”)  
Wieviele Studierende können ihr Studienfach nicht richtig schreiben?

# Diskussion

Fragen?  
Anmerkungen?  
Kritik?  
Diskussion!

# Inhalt

## 8 Appendix

## Details

65 Studierende, die den Begriff “E-Mail-Kryptographie” nicht kennen:

- Die Studierenden sind im Durchschnitt im 5.1-ten Semester (Standardabw.: 2.9, Maximum: 12)
- OS: 53 nutzen Microsoft Windows, 9 nutzen Mac OS
- E-Mail-Clients: 37 nutzen Seamonkey, 11 OS X Mail, 8 Thunderbird, häufig zusätzliche Nutzung von Webclients, Smartphones

## Details

17 Befragte, die schon mindestens einmal eine verschlüsselte E-Mail versendet haben:

- 9 Informatiker
- 11 setzen Linux, 3 Windows, 2 Mac OS als Betriebssystem ein
- 10 benutzen Thunderbird, 7 Webclients (oft in Kombination)
- Die Befragten sind im Durchschnitt im 6.1-ten Semester (Standardabw.: 2.4, Maximum: 10)

# Details

6 Befragte, die trotz vorhandener Kontakte keine verschlüsselten Mails versenden:

- Studienfächer: Informatik (2), Nanotechnologie, Maschinenbau, Mechatronik, Materialwissenschaften
- Semester: im Durchschnitt 9.0 (Standardabw.: 3.6, Maximum: 16)
- Betriebssystem: 4 Windows, 2 Linux
- E-Mail-Client: Thunderbird, Outlook, Webclient, u.a.

# Details

1 Befragter, der keine Kontakte hat, mit denen er verschlüsselt kommunizieren kann:

- Wirtschaftsingenieur
- 6. Semester
- OS: Linux
- E-Mail-Client: Thunderbird



# Details

9 Befragte, die E-Mail-Kryptographie-Software bewusst entfernt haben:

- Studienfach: Informatik (4), EEI (2), WIng (2), Maschinenbau
- Semester: 7.1 im Durchschnitt (Standardabw.: 3.6, Maximum: 13)
- OS: Windows (6), Linux (2), Mac OS
- E-Mail-Client: Webclient, Thunderbird, u.a.

# Details

6 Befragte, die ihre E-Mail-Kryptographie-Software nicht bewusst entfernt haben:

- Studienfach: Informatik (2), LSE, Energietechnik, Nanotechnologie
- Semester: 5.7 im Durchschnitt (Standardabw.: 1.8, Maximum: 8)
- OS: Windows (4), Linux
- E-Mail-Clients: Webclient, Thunderbird und andere

# Details

18 Befragte hatten zwar schon einmal geplant E-Mail-Kryptographie-Software zu installieren, es jedoch nie tatsächlich versucht:

- Studienfächer: Energietechnik (3), Maschinenbau (3), Mechatronik (2), IIS (2), u.a.
- Semester: 5.2 (Standardabw.: 2.6, Maximum: 12)
- OS: Windows (16), Linux (2)
- E-Mail-Client: Webclient, Thunderbird, u.a.

# Details

54 Befragte, die Software für E-Mail-Kryptographie noch nie installiert hatten und dies auch noch nie geplant haben:

- Semester: 6.6 (Standardabw.: 3.4, Maximum: 14)
- OS: Windows (43), Mac OS (8), Linux (2)
- E-Mail-Clients: Webclient (30), Outlook (17), Thunderbird (11), u.a. (OS X Mail, Smartphone-Clients, Mutt, ...)