

# Usable Security: Was ist das und wozu in aller Welt braucht man das?

Karoline Busse - USECAP Uni Bonn

Usability + Security

# Usability



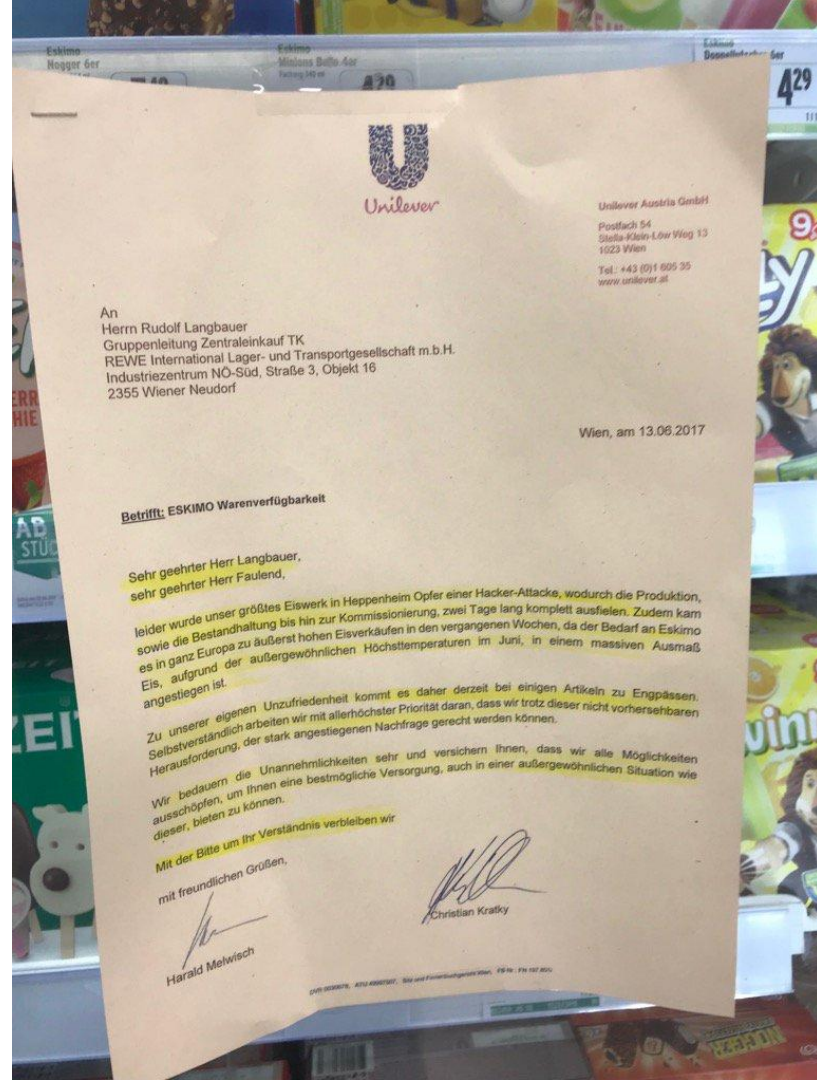
# Security

“leider wurde unser größtes Eiswerk in Hoppenheim Opfer einer Hacker-Attacke, wodurch die Produktion [...] zwei Tage lang komplett ausfielen.

[...]

Zu unserer eigenen Unzufriedenheit kommt es daher derzeit bei einigen Artikeln zu Engpässen.”

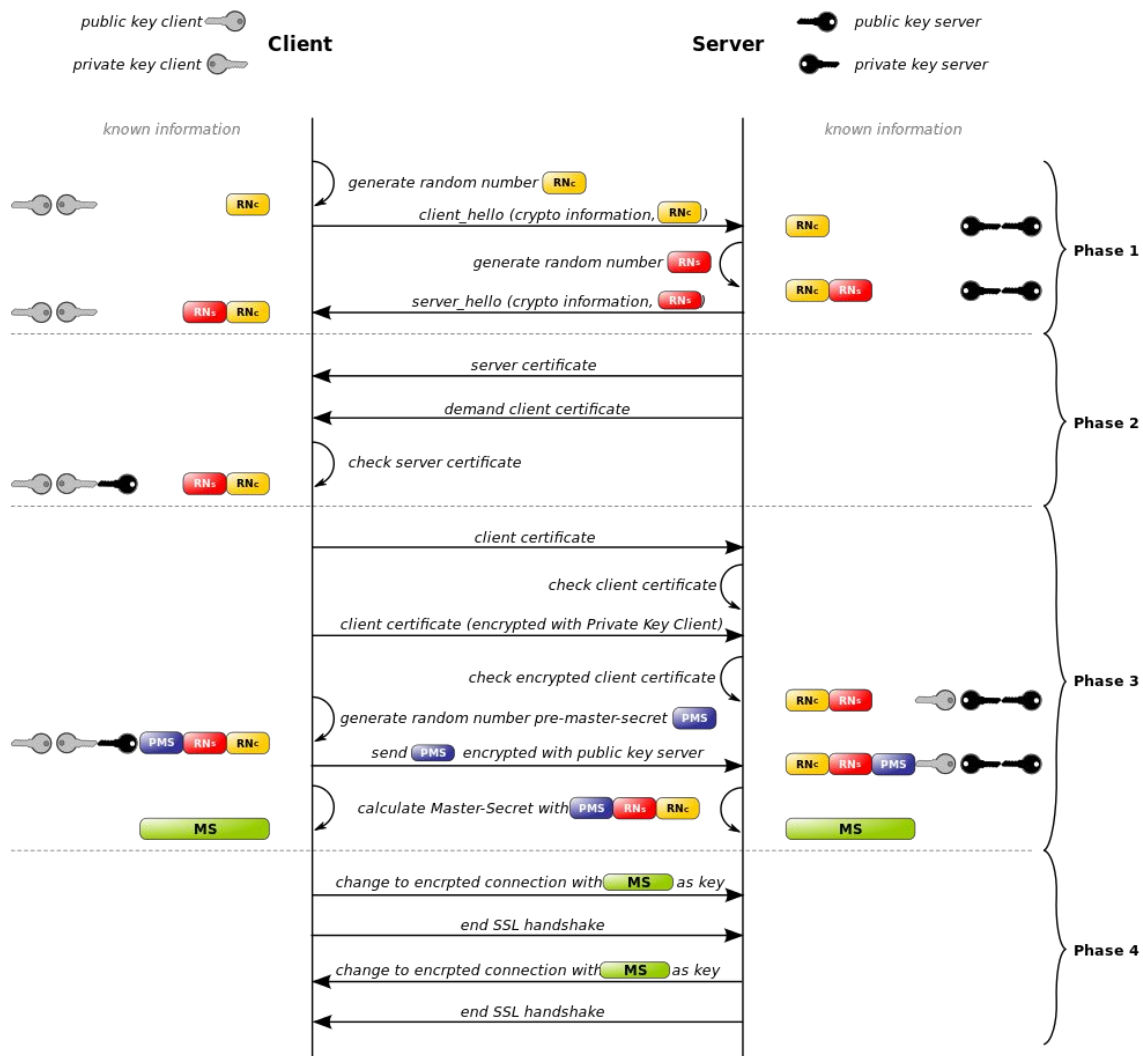
Bild: @skoops/Twitter



... but how?

# Fallbeispiel: SSL/TLS

# SSL Handshake



# Indicators






# Warnings

Privacy error - Chromium

Privacy error

Not secure | ~~https://~~pads.ccc.de



## Your connection is not private

Attackers might be trying to steal your information from **pads.ccc.de** (for example, passwords, messages, or credit cards). NET::ERR\_CERT\_AUTHORITY\_INVALID

ADVANCED

Back to safety



Something happened and you need to click OK to get on with things.

Certificate mismatch security identification  
administration communication intercept liliputian  
snotweasel foxtrot omegaforce.

Technical Crap ...

- More technical crap
- Hoyvin-Glayvin!
- Launch photon torpedos

OK

Cancel

Was hat die Forschung gemacht?

# Ressourcen zum Thema HTTPS und Usability

Sunshine et al., “Crying Wolf: An Empirical Study of SSL Warning Effectiveness”, 18th Usenix Security Symposium, 2009

Porter Felt et al., “Experimenting at Scale with Google Chrome’s SSL Warning”, CHI 2014

Akhav and Porter Felt: “Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness”, 22nd Usenix Security Symposium, 2014

Porter Felt et al., “Improving SSL Warnings: Comprehension and Adherence”, CHI 2015

Adrienne Porter Felt auf Twitter: @\_\_apf\_\_

# Fallbeispiel PGP (Der Klassiker)

COMODO...

WTF

Public Key

00110011101010  
3337869439000  
00110011101010  
123456789012345  
3337869439000



Private Key

123456789012345  
00110011101010  
3337869439000  
3337869439000  
00110011101010



# Public Key & Private Key

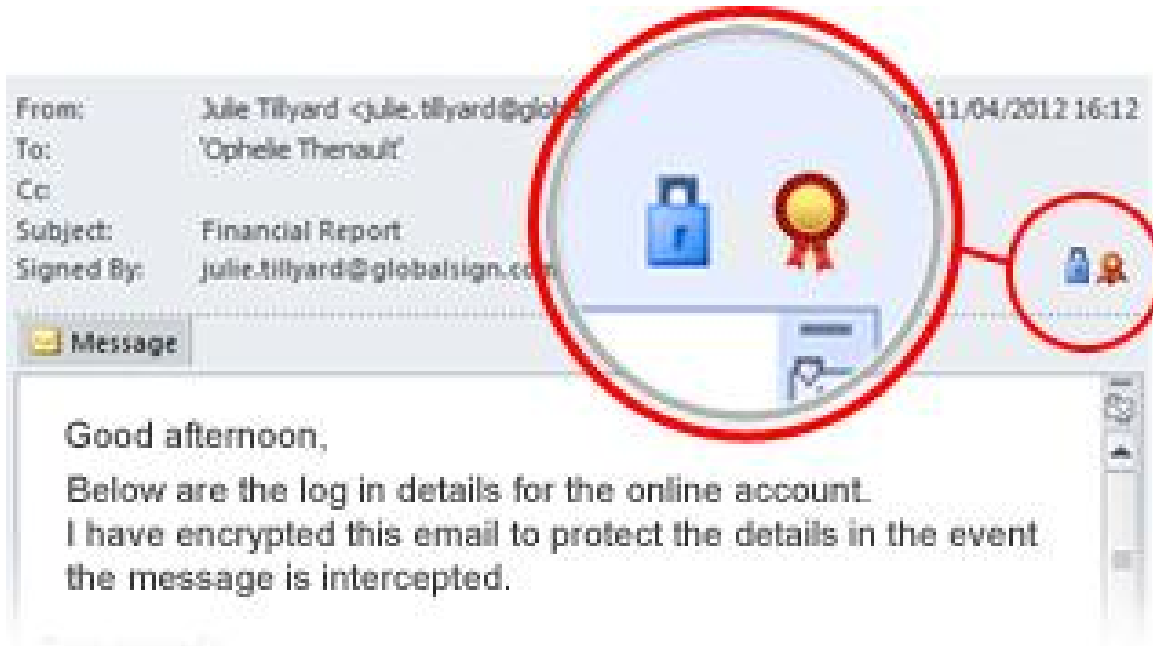
Public Key



Private Key



# Encryption & Digital Signature







Most prominent USec paper: Why  
Johnny can't Encrypt

# Even the pros are quitting

“Trust me when I tried [...] But it just didn't work. [...] First, there's the adoption issue [...]. Then, there's the UX problem. Easy crippling mistakes. [...] And all this for what gain?”

“I'm not dropping to plaintext. [...] Mostly I'll use Signal or WhatsApp, which offer vastly better endpoint security on iOS, ephemerality, and smoother key rotation.”

What next?  
(Google seems to give up, too)

# Ressourcen zum Thema PGP Usability

Whitten und Tygar, “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0”, Usenix Security Symposium 1999

Sheng et al, “Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software”, SOUPS 2006

Ruoti et al., “ "We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users”, CHI 2016

Okay, aber wie geht das jetzt mit Usable  
Security?