

Introduction to Information Security

14-741/18-631 Fall 2021

Unit 6, Lecture 3: Usable Security

Hanan Hibshi

hhibshi@andrew

Motivation



- Security breaches start with human error
- Phishing is one of the best examples
 - ▼ Common compromise, very dangerous (id theft)
 - ▼ Not an attack on crypto
 - ▼ No complicated break-in of a security protocol
 - ▼ Scam based on HCI

This Lecture's Agenda

■ Outline

- ▼ Why secure systems are at odds with human factors
- ▼ The Human-in-the-loop Framework
- ▼ Case Studies where security failed because of usability
 - ▼ Phishing
 - ▼ Why Johnny can't encrypt by Whitten and Tygar
 - ▼ Proposals for making SSL warning more effective
- ▼ Usable Security Core Guidelines

■ Objective

- ▼ Make you think about human factors when designing/evaluating secure systems
- ▼ Understand effect of human factors on threat modelling

Understanding Humans

- **The field of Human Computer Interaction studies human interactions with systems and technology**
- **In Security, understanding humans is essential**
 - ▼ Security is a secondary task
 - ▼ How to get humans attention?
 - ▼ Security can become complicated
 - ▼ Do we need the human? (automation, default settings)
 - ▼ If human is needed, how to inform the human to make an informed decision ?
 - ▼ There are malicious users, but most could be
 - ▼ Tired, distracted
 - ▼ Unmotivated
 - ▼ Confused, lack technical background

The Principle of Psychological Acceptability

- **Make it easier for users to use system properly, otherwise they are likely to incorrectly use the protection mechanisms**
- **Remember that “users are not the enemy”**

Examples of Security Tasks in Everyday Life

■ Passwords

- ▼ Remember: passwords are overheads to people
- ▼ Poorly selected passwords
 - ▼ Guessability: Iloveyou vs. leatKale [1]
 - ▼ Default Passwords

■ Patching

- ▼ Important for fixing security problems
- ▼ Another overhead to users, and network administrators
 - ▼ Different systems on the network require different patches
- ▼ Trustworthiness of the source

■ Configuration

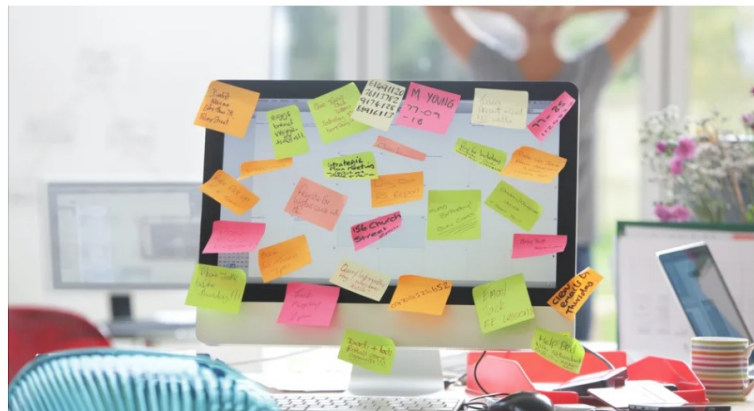
- ▼ Configuration can increase or decrease security of default settings

[1] Blase Ur et al. 2016. Do Users' Perceptions of Password Security Match Reality? (CHI '16). ACM.

Remembering Passwords

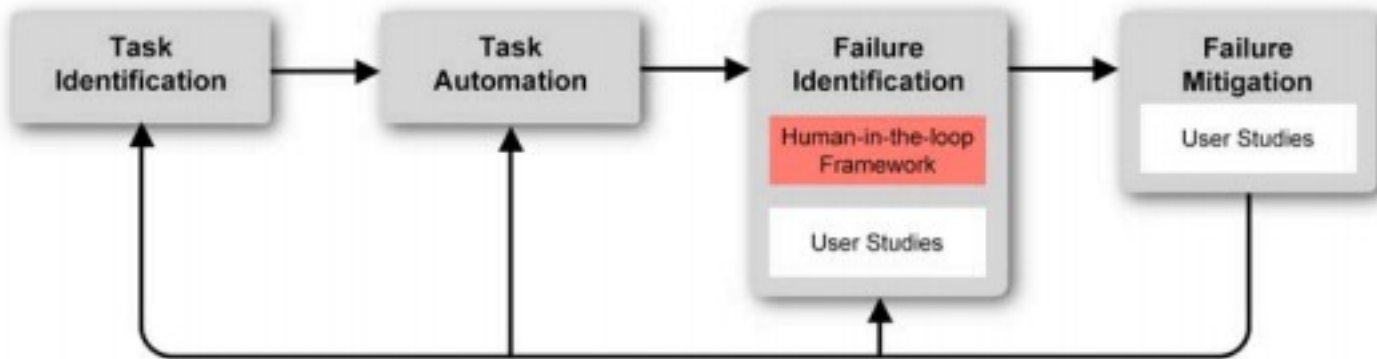
- A 2018 study showed that almost half of U.S. consumers use 1-5 passwords to access all their online applications
- Users prefer sticky notes over password management apps

Working from home? Think twice about posting that desk pic.



<https://www.securitymagazine.com/articles/88963-americans-keep-passwords-on-sticky-notes-recipe-cards-and-slips-of-paper>

The Human-in-the-Loop Framework



- **Try to get the human out-of-loop**
 - ▼ Automated functions
 - ▼ Default configuration settings
- **Build intuitive systems**
 - ▼ Easy to use
- **Teach humans about security tasks**



Usability (General Definition)

■ Learnability

- ▼ How easy to accomplish basic tasks from the first time?

■ Efficiency

- ▼ How quickly can users perform tasks?

■ Memorability

- ▼ Can the interface still be used efficiently after a period of time?

■ Accuracy

- ▼ How many *errors*; How severe? How easy to recover?

■ Satisfaction

- ▼ How pleasant is it to use the design?

Usable Security Heuristics

(Adapted from S. Garfinkel usable security principles)

- **Consistency**
 - with controls and Placement ; with Vocabulary
- **“Least Surprise”**
 - ▼ Users might expect computers are behaving securely
- **Completion**
 - ▼ If deleted, do not store somewhere else
- **Observe existing work practices**
- **Employ iterative design**
- **Expose necessary information, not junk data**
- **Zero-click**
 - ▼ Avoid confirmations, use undo instead
- **Design for responsiveness**

Usable Security

■ Security traditionally focused on:

- ▼ Software bugs
- ▼ Networking protocols
- ▼ Cryptography algorithms

■ Usable security:

- ▼ People make mistakes
- ▼ People are something that can go wrong
- ▼ Usable security: designing systems to minimize human errors that lead to security problems

Usability for Security

■ Reliability

- ▼ Users are reliably made aware of the tasks they need to perform
 - ▼ E.g., use their private key for signing, the correspondent's public key for encryption

■ Intuitiveness

- ▼ Users are able to figure out how to successfully perform these tasks

■ Safety

- ▼ Users don't/can't make dangerous errors

■ Comfort

- ▼ Users are sufficiently comfortable with the interface to continue using it

Why is Usable Security Difficult?

■ Unmotivated user property

- ▼ Security is not a primary goal
 - ▼ It should “just work”
- ▼ Users won’t read (lengthy) manuals

■ Abstraction property

- ▼ Security rules and policies are complex
- ▼ Unintuitive for users

■ Lack of feedback property

- ▼ The “correct” security configuration is “what the user wants”
 - ▼ Error checking is difficult

Why is Usable Security Difficult?

■ Barn door property

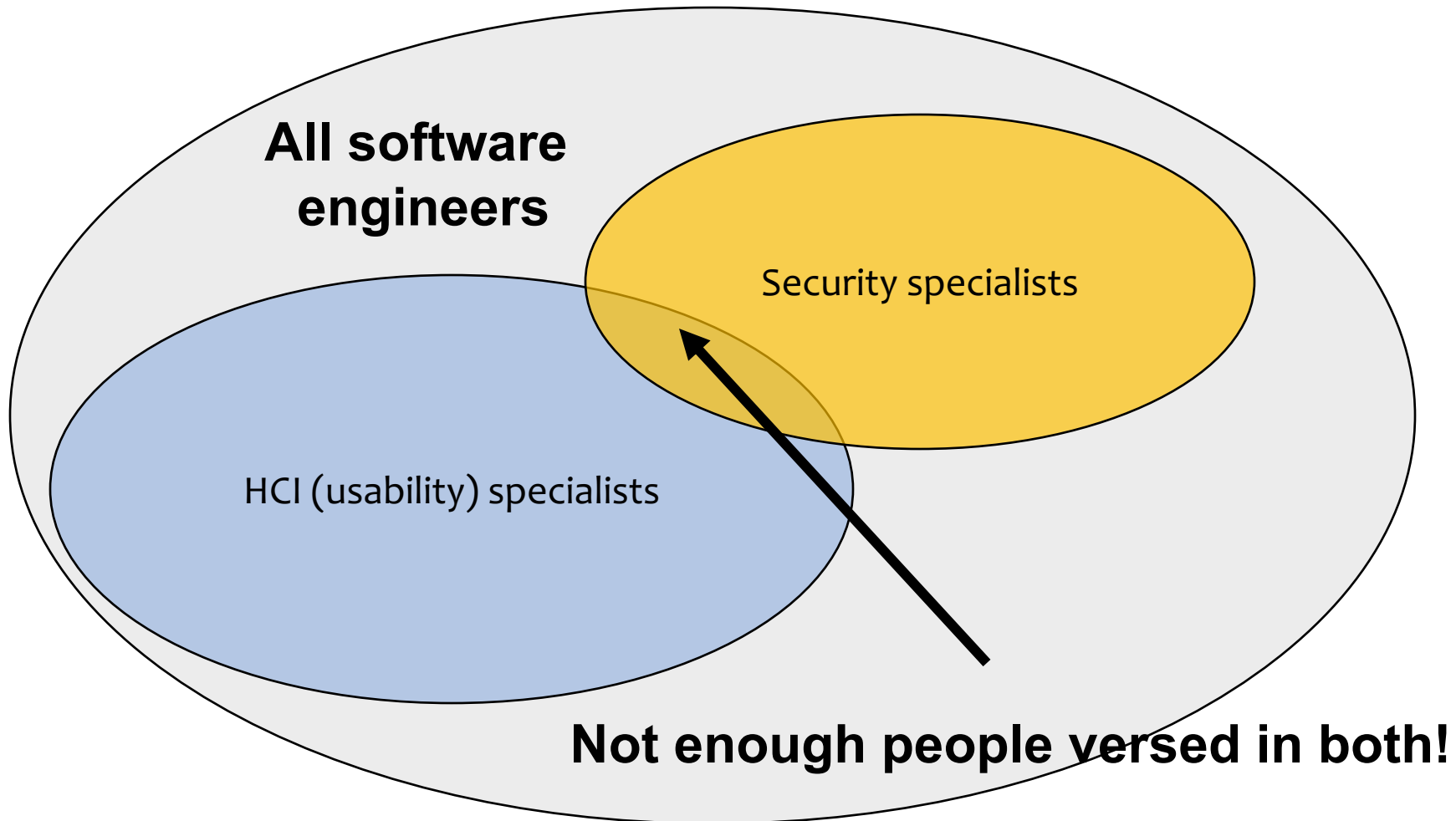
- ▼ Once a secret has been exposed/left unprotected, security can't be guaranteed anymore
 - ▼ If you ever expose your private key, you have to
 - Revoke the key
 - Regenerate the key pair

■ Weakest link property

- ▼ A single error can compromise the whole system/network
- ▼ Users can't explore/discover things by themselves

More Difficulties...

(Adapted from S. Garfinkel)



Other Causes

(Adapted from S. Garfinkel)

- **Emphasis on bug fixing, rather than correct design**
- **Emphasis on cryptography**
- **Researcher disinterest**
 - ▼ HCI/psychology on the one hand
 - ▼ Math/crypto on the other hand
- **Difficulty of performing user tests**

Phishing and Digital Signatures

- Possible solution against phishing: require all banks to use PGP or similar digital signature scheme
- Imposters easily defeated
- ... except that most users have no clue how to verify a digital signature...
- ... or even know (or care) about what it is!

Digitally Signed Email

- **Focus of Whitten & Tygar's paper**
- **Representative security primitive**
 - ▼ Useful, could be adopted by most people
- **Good user interface in PGP 5.0 by traditional usability/HCI standards**
- **Is PGP 5.0 usable?**

Usability Evaluation of PGP 5.0

- **Two-pronged approach**
- **Cognitive walkthrough**
 - ▼ Look at every function of the program through the eyes of a complete novice
 - ▼ Similar to code walkthrough
- **User study**
 - ▼ Put people in a room, have them use software

Cognitive Walkthrough of PGP 5.0

■ **Single key metaphor (icon)**

- ▼ User incorrectly assume that encryption/decryption work with a single key
- ▼ Can be very dangerous
 - ▼ exposure of private key

■ **Quill pen object for denoting signatures**

- ▼ Completely disconnected from underlying crypto machinery

■ **Decrypt/Verify a single button**

- ▼ Leads to more confusion between encryption and signatures

Cognitive Walkthrough of PGP 5.0

- **Confusion between different (incompatible) types of keys**
- **Key server hidden in a menu**
 - ▼ Users may have a hard time distinguishing between remote and local operations
- **Key management policy**
 - ▼ Unclear that PGP automatically sets ratings for keys

Cognitive Walkthrough of PGP 5.0

- **Not enough warnings of the consequences of deleting private keys**
- **Relatively easy to accidentally publish a key**
 - ▼ Can't remove a publicized key from the server (write-only)
- **Revocation operations don't provide enough information**
 - ▼ User may assume revocation is also distributed
 - ▼ Undo difficult - but the user is not made aware of that

Does PGP Provide Usable Security?

- **Cognitive walkthrough seems to indicate several problems**
- **User study**
 - ▼ 12 people
 - ▼ Experienced with email, not with security
 - ▼ Play the role of a political campaign worker
 - ▼ Have to exchange secret messages (e.g., the politician's itinerary) with other members

Does PGP Provide Usable Security?

■ Reliability

- ▼ Users are reliably made aware of the tasks they need to perform

■ Intuitiveness

- ▼ Users are able to figure out how to successfully perform these tasks

■ Safety

- ▼ Users don't/can't make dangerous errors

■ Comfort

- ▼ Users are sufficiently comfortable with the interface to continue using it

Does PGP Provide Usable Security?

■ Reliability

- ▼ Users are reliably made aware of the tasks they need to perform
- ⇒ **No obvious distinction between encryption and signatures**

■ Intuitiveness

- ▼ Users are able to figure out how to successfully perform these tasks
- ⇒ **A number of users encrypted using the wrong key**

■ Safety

- ▼ Users don't/can't make dangerous errors
- ⇒ **Some users emailed message to be encrypted in plaintext**

■ Comfort

- ▼ Users are sufficiently comfortable with the interface to continue using it
- ⇒ **User survey indicates most of them wouldn't use PGP anymore**

Conclusion on PGP Study

- **Usability for security is hard**

- ▼ A program can have good usability from a GUI perspective, and still completely fail at providing usable security

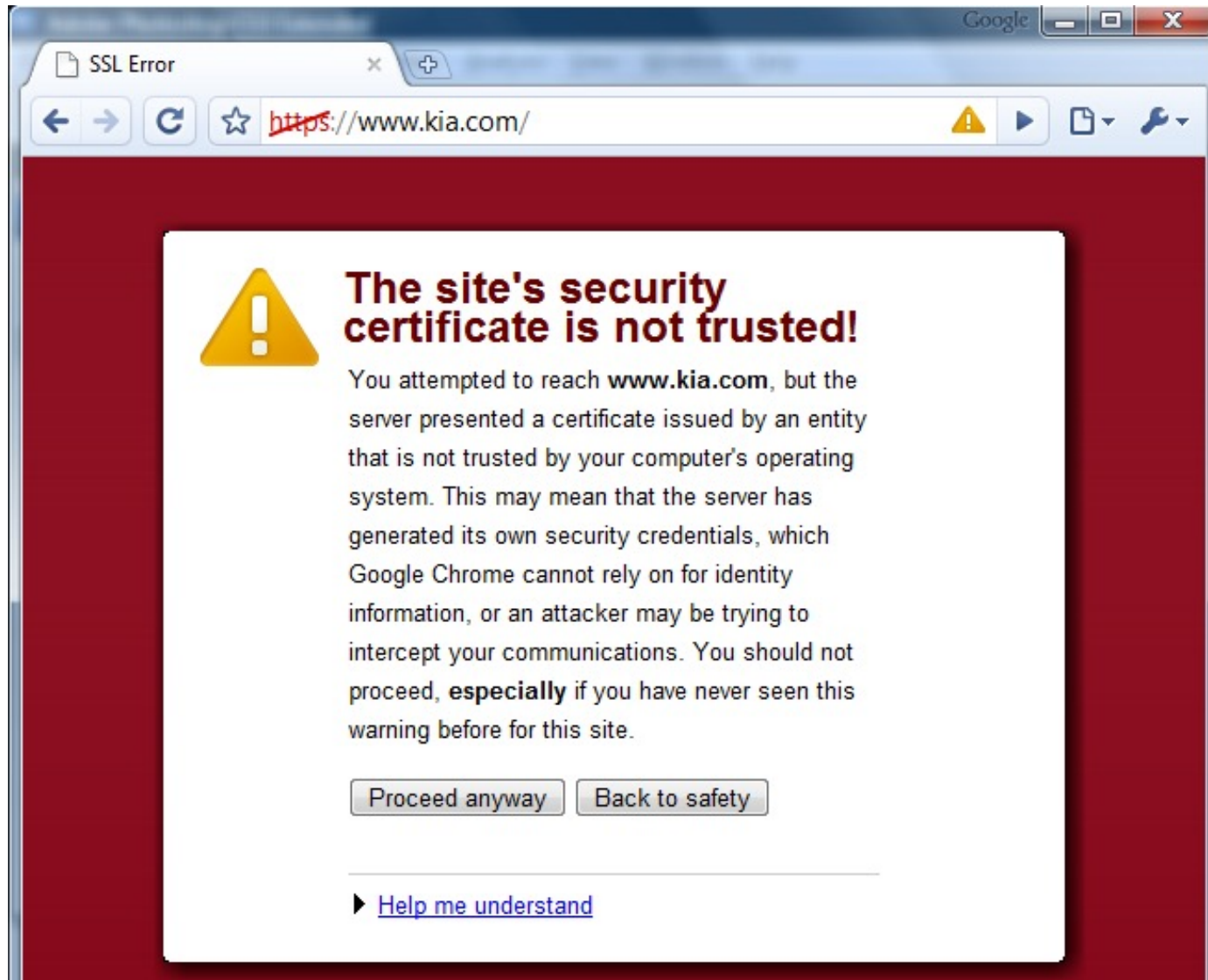
- **How do we go about making security usable?**

- **Is it even possible?**

Usable Security Problems

- Currently a “hot” research area
- Phishing
- Authentication
- SSL/TLS indicators
- Security warnings
- Access control settings
- Privacy settings

Case Study of SSL Warnings



Case Study of SSL Warnings

- **Warnings are meant to help users steer away from danger**
- **Why SSL warnings are displayed by browsers?**
 - ▼ Expired certificate
 - ▼ Certificate signed by a CA not in the trusted CA list
 - ▼ Mismatch of domain name
 - ▼ Invalid certificate
- **What security problems are the warnings indicate?**
 - ▼ Man-In-The-Middle attack
 - ▼ DNS spoofing
 - ▼ Server misconfiguration

Are SSL Warnings Effective?

- Do SSL warnings effectively communicate the risks?
- Do SSL warnings effectively provide instructions for avoiding the hazard?
- How to design better SSL warnings?
- Many papers on this topic
 - ▼ Sunshine et al. USENIX Security 2009
 - ▼ Felt et al. CHI 2015

- **Present screenshots of SSL warnings from different browsers to participants**
 - ▼ From craigslist.org (no private info)
 - ▼ From amazon.com (lots of private info)
- **Ask a series of questions**
- **Classify them as ordinary user vs. computer experts**

Warnings

You are being redirected to Cameo.

Please [click here](#) if

Website Certified by an Unknown Authority



Unable to verify the identity of cameo.library.cmu.edu as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be cameo.library.cmu.edu, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to accept this certificate for the purpose of identifying the Web site cameo.library.cmu.edu?

[Examine Certificate...](#)


- ☐ Accept this certificate permanently
- ☒ Accept this certificate temporarily for this session
- ☐ Do not accept this certificate and do not connect to this Web site

OK

Cancel

(a) Firefox 2

Warnings – IE 7





There is a problem with this website's security certificate.


The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

 [Click here to close this webpage.](#)

 [Continue to this website \(not recommended\).](#)

 [More information](#)

(b) Internet Explorer 7

Warnings – FF3



Figure 3: Screenshot of the initial FF3 warning.

Survey Results

- No significant difference based on the type of websites
- Risk perception is key to respondents' decision as to proceed or not
 - ▼ users who understood the warnings tended to behave differently than those who did not

Comprehension

- **Asked to list the possible consequences of ignoring each of the warnings**
 - ▼ fraud, identity theft, stolen credentials, phishing, or eavesdropping
 - ▼ 39% of responses for FF2 warnings
 - ▼ 44% of responses for FF3 warnings
 - ▼ 37% of responses for IE7 warnings
- **Wrong answers**
 - ▼ No clue
 - ▼ Wrong attacks: viruses and worm
 - ▼ Others:
 - ▼ “I use a Mac so nothing bad would happen.” “Since I use FreeBSD, rather than Windows, not much [risk].
 - ▼ “On my Linux box, nothing significantly bad would happen.”

How to Design Better SSL Warning? [Felt et al. 2015]

- In 2014, Firefox seems to be doing a lot better than Chrome in SSL warning adherence rate (70% vs 30%)
- Why the difference?
 - ▼ Firefox has removed tech jargons from the warning (e.g., certificates)
- How to make Chrome's SSL warning better?

Aspects for improvement

- **Comprehension:** The user should be able to make an informed decision after seeing an SSL warning.
 - ▼ Threat source
 - ▼ Data risk
 - ▼ False positives
- **Adherence:** The warning should encourage users to act in a conservatively safe manner by not proceeding.

Comprehension

■ Avoid technical jargons

- ▼ Using simple, non-technical language
- ▼ Brevity
- ▼ Specific Risk Description (use concrete relatable examples)
- ▼ Illustration

■ ***Chrome 36: “...the server presented a certificate issued by an entity that is not trusted by your computer’s operating system.”***

■ ***IE: “The security certificate presented by this website was not issued by a trusted certificate authority.”***

Adherence

■ Opinionated design

- ▼ promote the safe choice as the preferred option
- ▼ adherence to be a more visually attractive choice than non-adherence
 - ▼ the safe button is a bright blue color that stands out against the background
 - ▼ the unsafe choice is a dark gray text link.

Chrome New Warning

illustration

More info

Advanced

Specific risk

Safe choice in bright blue

Back to safety

This server could not prove that it is **www.pcwebshop.co.uk**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to **www.pcwebshop.co.uk (unsafe)**

unsafe choice in grey and hidden

NET::ERR_CERT_AUTHORITY_INVALID

More Examples

■ Whatsapp users without two-step verification

- ▼ Whatsapp account can easily get hacked from another phone using the victim's number
- ▼ Verification code is sent to voicemail instead
- ▼ Users did not change default voicemail password (e.g.1234)
- ▼ Hackers might set-up the two step-verification
 - ▼ Makes it harder for a user to retrieve their account
- ▼ Users did not add the two-step verification for better satisfaction!

■ Enabling insecure components

- ▼ Users are not well-informed about insecure components
- ▼ Examples: WordPress, Flash ...

Take Away Slide

- **Security starts (and often ends, unfortunately) with humans**
 - ▼ See success of phishing attacks
 - ▼ We need to take into account human factors
- **Security and usability are at odds**
 - ▼ Even interfaces that seem ok (e.g., PGP 5.0) appear to be inadequate
- **Required design goals for usable security**
 - ▼ Reliability, Intuitiveness, Safety and Comfort
- **Security warning (SSL)**
 - ▼ Comprehension and adherence
- **Usable security promising field**