CSE227 – Graduate Computer Security

Usable Security

UC San Diego

Housekeeping

General course things to know

- Grades for midpoint should be released today (but everyone can expect to do well)
- Final presentations will be final week of class — schedule released next week
- Presentation Details
  - 10 minutes for presentation, 2 mins for questions (I will cut you off!)
  - Talk should include introduction to the problem, your research questions, your methodology (including data collection), and your results
  - All team members must speak approximately an even amount
  - **Number 1 Rule: Not boring!**

Housekeeping

General course things to know

- Comprehensive exam details
  - Write-up, same template / formatting as final write up
  - 3 pages, **must be your individual work on the project**
  - Contextualize your broader project, then discuss exactly what you contributed
    - What challenges did you run into? How did you evaluate your own progress?
  - **All the text must be your own**

This week’s goal

Research milestones

- Do what you said you would!

Today's lecture

Learning Objectives

- Learn about usable security, what it is and why we should care, and how research is done in this space
- Discuss the Johnny paper
- Discuss the Alice paper

Preliminaries

What are some reasonable restrictions for a password?

What are some reasonable restrictions for a password?

- Require long passwords
- Require numbers/symbols
- Change passwords regularly

What are some reasonable restrictions for a password?

- Require long passwords
  - How would you get around this restriction?
- Require numbers/symbols
- Change passwords regularly

What are some reasonable restrictions for a password?

- Require long passwords
  - Add some padding (e.g., “aaaaaaaaa”)
- Require numbers/symbols
- Change passwords regularly

What are some reasonable restrictions for a password?

- Require long passwords
  - Add some padding (e.g., “aaaaaaaaa”)
- Require numbers/symbols
  - How would you get around this restriction?
- Change passwords regularly

What are some reasonable restrictions for a password?

- Require long passwords
  - Add some padding (e.g., “aaaaaaaaa”)
- Require numbers/symbols
  - 123456 (also works for step 1!)
- Change passwords regularly

What are some reasonable restrictions for a password?

- Require long passwords
  - Add some padding (e.g., “aaaaaaaaa”)
- Require numbers/symbols
  - 123456 (also works for step 1!)
- Change passwords regularly
  - How would you get around this restriction?

What are some reasonable restrictions for a password?

- Require long passwords
  - Add some padding (e.g., “aaaaaaaaa”)
- Require numbers/symbols
  - 123456 (also works for step 1!)
- Change passwords regularly
  - Add the month to your password (e.g., BatmanSpring, BatmanFall, BatmanSummer, etc.)

What is usable security?

What is usable security?

A subfield of computer security concerned with the *user design* of cybersecurity systems

Defining Usability for Security

- Definition: Security software is usable if the people who are expected to use it:
  - Are reliably made aware of the security tasks they need to perform
  - Are able to figure out how to successfully perform those tasks
  - Don’t make dangerous errors
  - Are sufficiently comfortable with the interface to *continue* using it

Usable Security is a highly focused subfield of security

- They have their own conferences
  - SOUPS: Symposium on Usable Privacy & Security
  - USEC: Symposium on Usable Security (happened on Monday, usually in San Diego!)
- But also have a presence at major conferences
  - USENIX Security, CHI, PETS, etc.
- Researchers carve out usability as their main thing
  - E.g., See Imani Munyaka's Usable Security & Privacy courses

Why is usability hard?

- What is the unmotivated user property?
- What is the abstraction property?
- What is the lack of feedback property?
- What is the barn door property?
- What is the weakest link property?

Discussion: Why is usability important?

- Adams and Sasse, “Users are not the enemy,” CACM December 1999
- In it, they describe a vicious cycle
  - Users lack security knowledge
  - Users will circumvent restrictions that get in their way because security is not the point
  - Doing this lowers respect for security mechanisms, and repeat
- Their takeaway: **security needs user-centered designed, or it’s doomed to fail**

USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

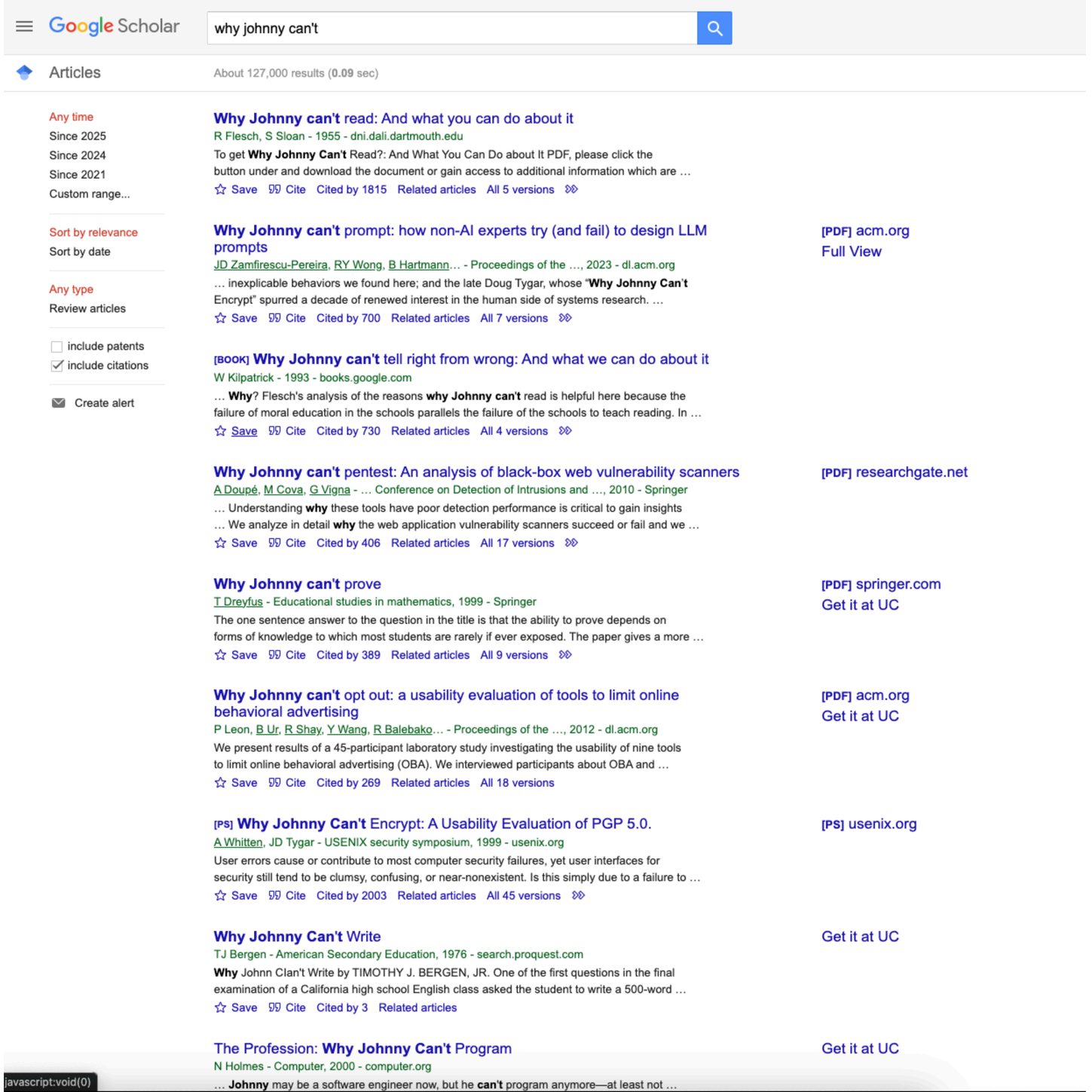
The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary’s ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password lifetime*—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

ANNE ADAMS AND MARTINA ANGELA SASSE

QUENTIN WEBB

Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0


Google Scholar
why johnny can't
Articles
About 127,000 results (0.09 sec)
Any time
Since 2025
Since 2024
Since 2021
Custom range...
Sort by relevance
Sort by date
Any type
Review articles
include patents
include citations
Create alert
Why Johnny can't read: And what you can do about it
R Flesch, S Sloan - 1955 - dni.dali.dartmouth.edu
To get Why Johnny Can't Read?: And What You Can Do about It PDF, please click the button under and download the document or gain access to additional information which are …
Save Cite Cited by 1815 Related articles All 5 versions
Why Johnny can't prompt: how non-AI experts try (and fail) to design LLM prompts
JD Zamfirescu-Pereira, RY Wong, B Hartmann… - Proceedings of the …, 2023 - dl.acm.org
… inexplicable behaviors we found here; and the late Doug Tygar, whose "Why Johnny Can't Encrypt" spurred a decade of renewed interest in the human side of systems research. …
Save Cite Cited by 700 Related articles All 7 versions
[PDF] acm.org
Full View
[BOOK] Why Johnny can't tell right from wrong: And what we can do about it
W Kilpatrick - 1993 - books.google.com
… Why? Flesch's analysis of the reasons why Johnny can't read is helpful here because the failure of moral education in the schools parallels the failure of the schools to teach reading. In …
Save Cite Cited by 730 Related articles All 4 versions
Why Johnny can't pentest: An analysis of black-box web vulnerability scanners
A Doupé, M Cova, G Vigna - … Conference on Detection of Intrusions and …, 2010 - Springer
… Understanding why these tools have poor detection performance is critical to gain insights
… We analyze in detail why the web application vulnerability scanners succeed or fail and we …
Save Cite Cited by 406 Related articles All 17 versions
[PDF] researchgate.net
Why Johnny can't prove
T Dreyfus - Educational studies in mathematics, 1999 - Springer
The one sentence answer to the question in the title is that the ability to prove depends on forms of knowledge to which most students are rarely if ever exposed. The paper gives a more …
Save Cite Cited by 389 Related articles All 9 versions
[PDF] springer.com
Get it at UC
Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising
P Leon, B Ur, R Shay, Y Wang, R Balebako… - Proceedings of the …, 2012 - dl.acm.org
We present results of a 45-participant laboratory study investigating the usability of nine tools to limit online behavioral advertising (OBA). We interviewed participants about OBA and …
Save Cite Cited by 269 Related articles All 18 versions
[PDF] acm.org
Get it at UC
[PS] Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.
A Whitten, JD Tygar - USENIX security symposium, 1999 - usenix.org
User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to …
Save Cite Cited by 2003 Related articles All 45 versions
[PS] usenix.org
Why Johnny Can't Write
TJ Bergen - American Secondary Education, 1976 - search.proquest.com
Why Johnn Clan't Write by TIMOTHY J. BERGEN, JR. One of the first questions in the final examination of a California high school English class asked the student to write a 500-word …
Save Cite Cited by 3 Related articles
Get it at UC
The Profession: Why Johnny Can't Program
N Holmes - Computer, 2000 - computer.org
… Johnny may be a software engineer now, but he can't program anymore—at least not …
Get it at UC
javascript:void(0)

What’s the goal of this paper?

What's the goal of this paper?

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, **will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?**

What is PGP?

What is PGP?

Pretty Good Privacy: An encryption and authentication mechanism for email.
Built using a PKI (e.g., RSA) with different keys for signing and encryption.

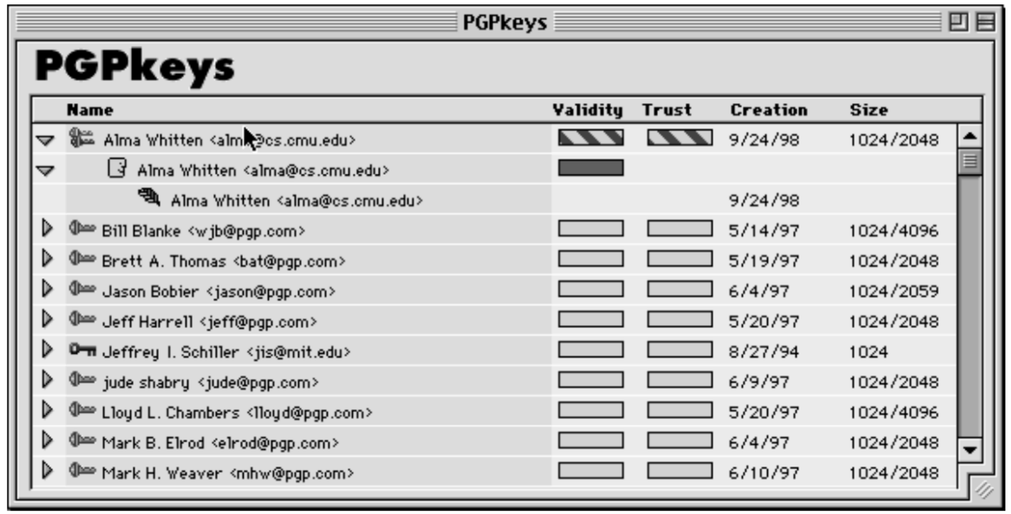
How did the authors evaluate the usability goodness of PGP?

How did the authors evaluate the usability goodness of PGP?

- Two distinct evaluation methods
  - Cognitive walkthrough w/ heuristic evaluation
  - User study
- Discussion point: What do you think the pros / cons of each method are?

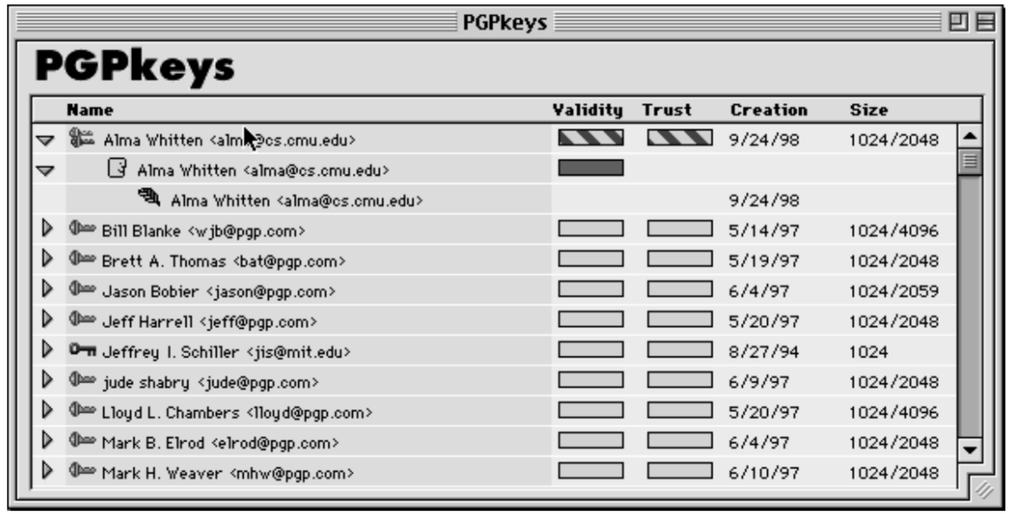
Visual Metaphors

- Icons you choose can shape how people use your product
  - Do all the icons seem to make sense? Why or why not?



Visual Metaphors

- Icons you choose can shape how people use your product
  - Do all the icons seem to make sense? Why or why not?
- Keys seem to be people?
- WTF is validity and trust? Are these progress bars?



Irreversible Actions

- One aspect of usability is that it should not be so easy to operate a foot-gun, that is, to be able to “shoot yourself in the foot.”
- Some things that have bad outcomes…
  - Accidentally deleting the private key – why is this bad?
  - Accidentally publicizing a key – why is this bad?
  - Accidentally revoking a key – why is this bad?

Overall takeaways

- Public-key crypto makes no sense to users
  - We don’t usually think about other people’s keys
  - We don’t use keys in this way
- Very hard for users to construct mental model
- Way too much information is being presented to make sense of what’s going on
- Way too easy to shoot yourself in the foot

User Study

- How did the authors set up their user study to test the usability of PGP?

User Study

- How did the authors set up their user study to test the usability of PGP?
  - Participant volunteered w/ a political campaign – needed to send email via PGP in order to run the group
- 12 users
  - Five members of a the campaign team
  - 90 minutes to complete task
    - Send secure/verifiable campaign update to all members of the team
    - Receive an validate instructions from members in response and respond

Results: bad

- Encryption
  - Three participants emailed secret to team members without encryption
  - One forgot passphrase and had to start over
  - P4 believed security was just “happening”
  - One couldn’t encrypt with any key
  - One generated new public keys for each recipient
- Decryption
  - Only two were able to do it easily

Exercise: Come up with better metaphors

- With folks around you, can you brainstorm better metaphors or language to help people understand encryption / decryption?

Meta Thoughts on this Paper

- What did we think about this paper? Is this kind of analysis useful, why or why not?
- What surprised you about this paper?

Break Time + Attendance

https://tinyurl.com/cse227-attend

Codeword:
SadUsers

Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness

What’s the goal of this paper?

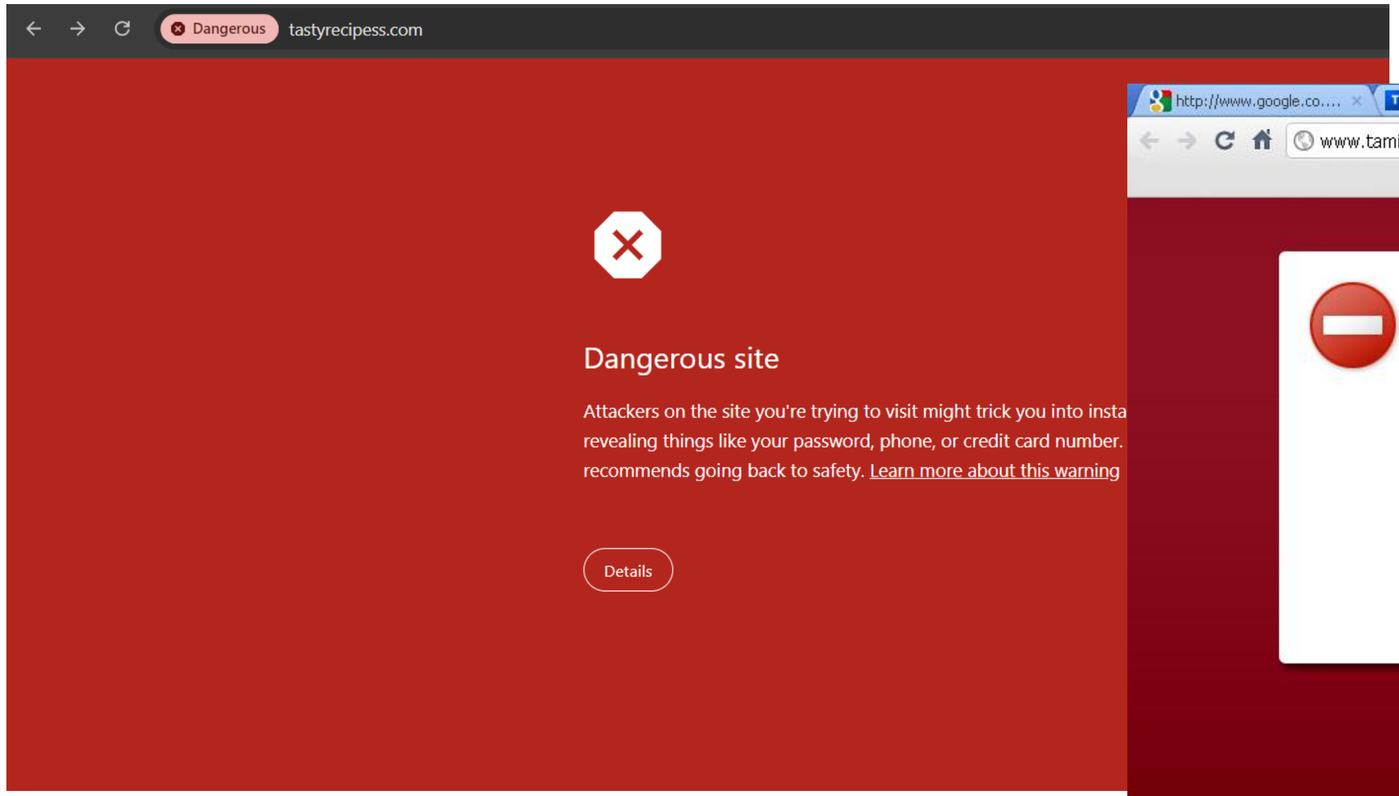
What's the goal of this paper?

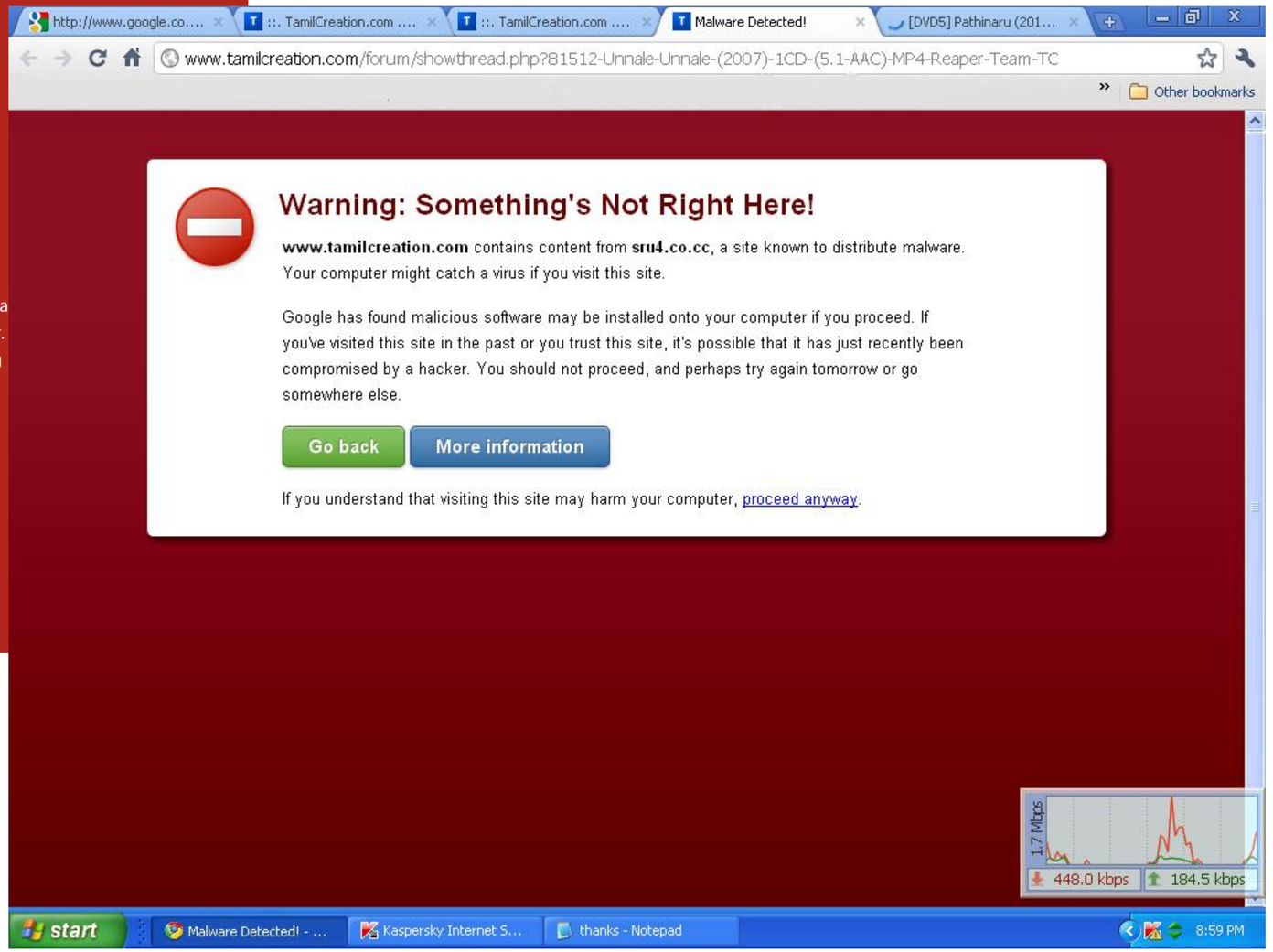
The security community's perception of the "oblivious" user evolved from the results of a number of laboratory studies on browser security indicators. However, these studies are not necessarily representative of the current state of browser warnings in 2013. Most of the studies evaluated warnings that have since been deprecated or significantly modified, often in response to criticisms in the aforementioned studies. **Our goal is to investigate whether modern browser security warnings protect users in practice.**

Background on this paper

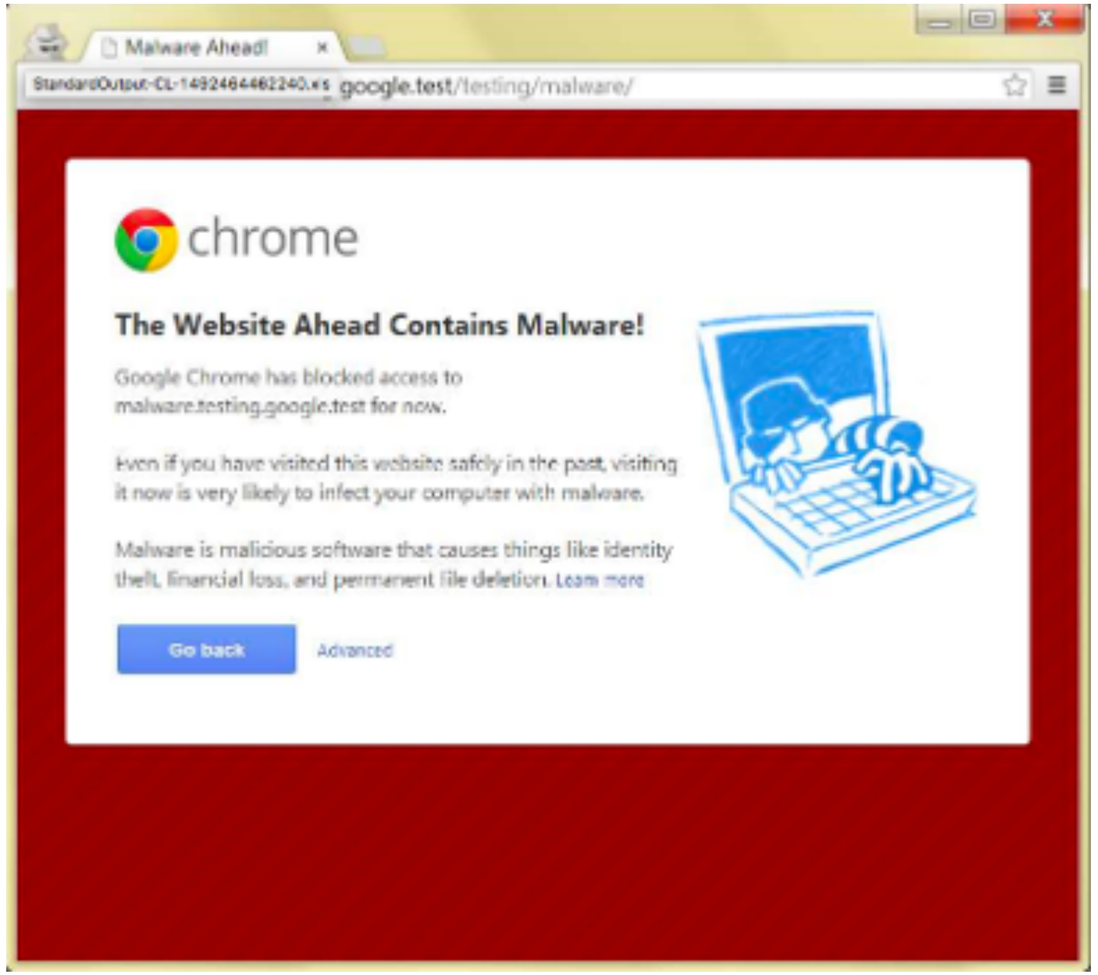
- Users are often chided for not taking security seriously
  - “Given the choice between dancing pigs and security, users will choose dancing pigs every time” – some famous security researchers
- Obliviousness is often cited as a main reason for this
  - **Are users actually oblivious to browser warnings?**

Browser warnings are abundant

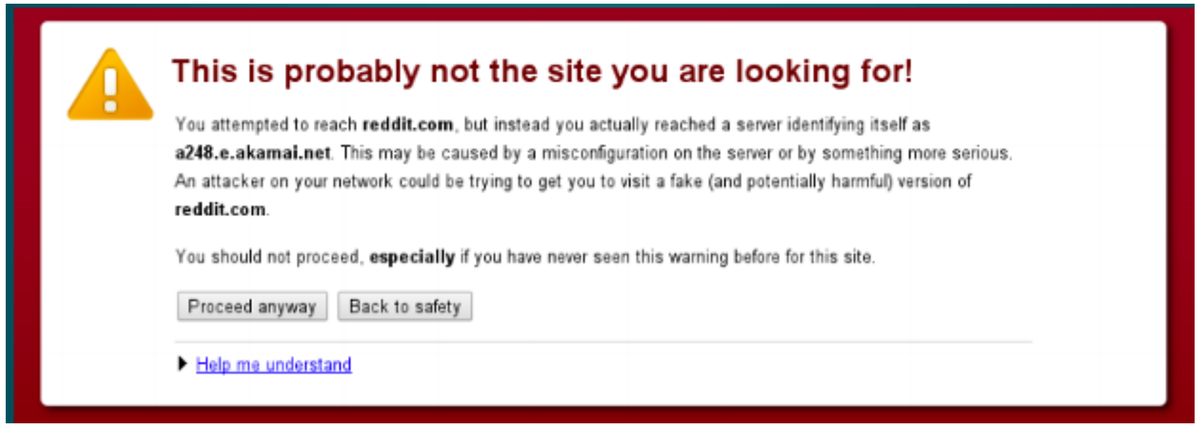


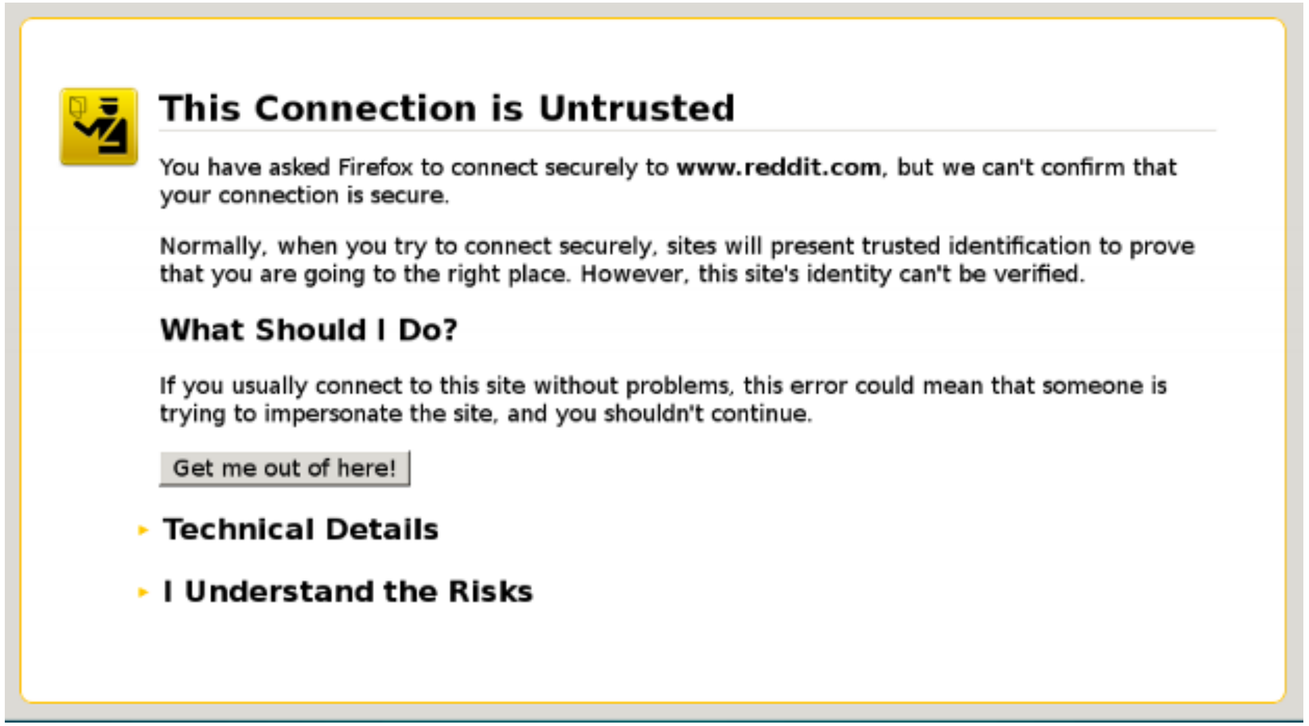


Malware Warnings

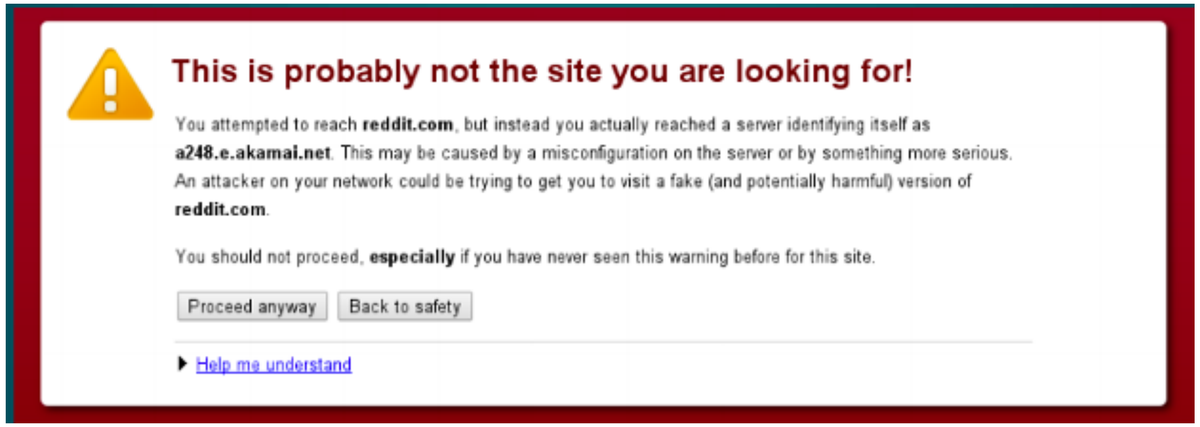


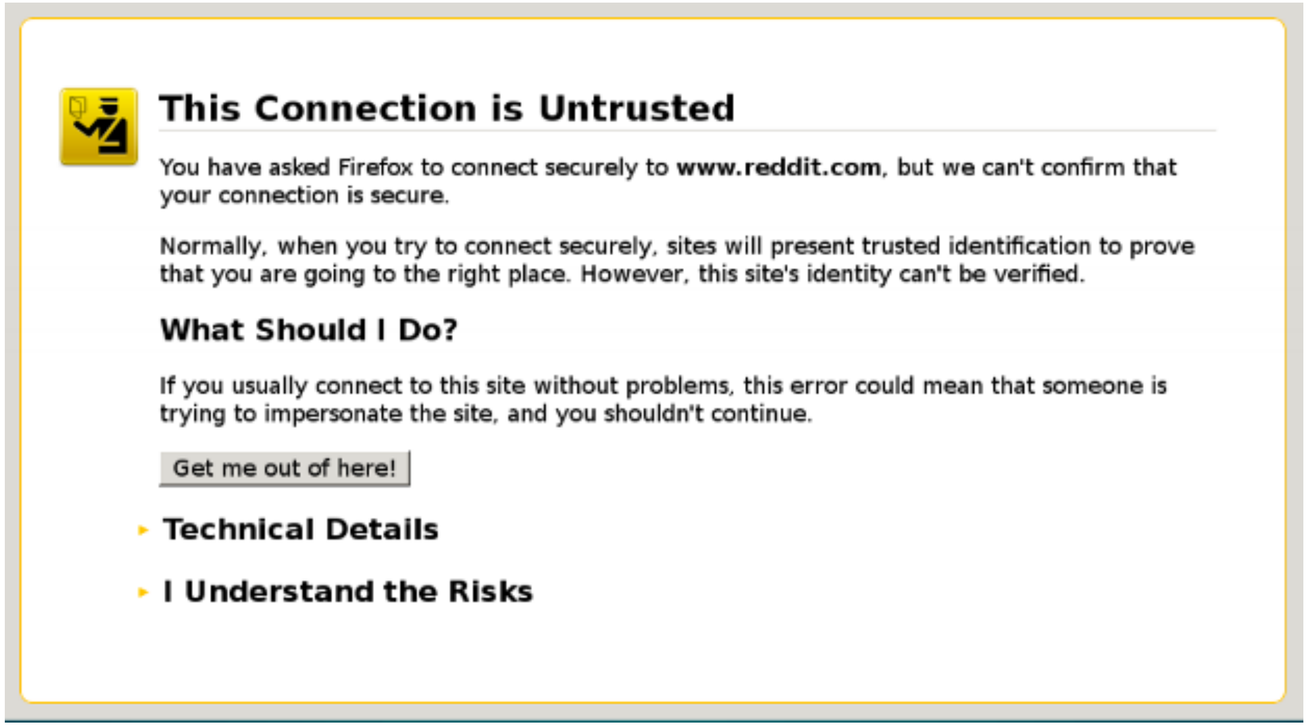
SSL Warnings





SSL Warnings





Notice any differences between malware and SSL?

Methods

- What metrics did the authors use to measure effectiveness of warnings?

Methods

- What metrics did the authors use to measure effectiveness of warnings?
  - Click through rates and time spent on warnings

Methods

- What metrics did the authors use to measure effectiveness of warnings?
  - Click through rates and time spent on warnings
- How did the authors collect the data they were looking for?

Methods

- What metrics did the authors use to measure effectiveness of warnings?
  - Click through rates and time spent on warnings
- How did the authors collect the data they were looking for?
  - Instrumented both Chrome and Firefox to log clickthrough rates at scale

Methods

- What metrics did the authors use to measure effectiveness of warnings?
  - Click through rates and time spent on warnings
- How did the authors collect the data they were looking for?
  - Instrumented both Chrome and Firefox to log clickthrough rates at scale
- *Meta-note: This was only possible because both authors worked at respective browser companies!*

Malware / Phishing Results

- Malware: Chrome 23.2%, Firefox 7.2%
- Phishing: Chrome 18%, Firefox 9.1%
- Some reasons for this…
  - Temporality – Chrome wildly unstable, Firefox fairly stable
  - Warning scariness?
  - Demographics of users?
- Any theories?

SSL Results

- Firefox, 33%, Chrome: 70.2%!
- Number of buttons
  - Chrome requires one click, Firefox requires *three*
- Visual metaphors
  - Firefox has a policeman, Chrome doesn’t show any images
- Remembering exceptions
  - Firefox lets people shoot themselves in the foot permanently, possibly hiding potential bypasses

So… what do we do with this study?

- Experiment! APF went onto publish lots in this space and *actually* change things in Google Chrome for the better

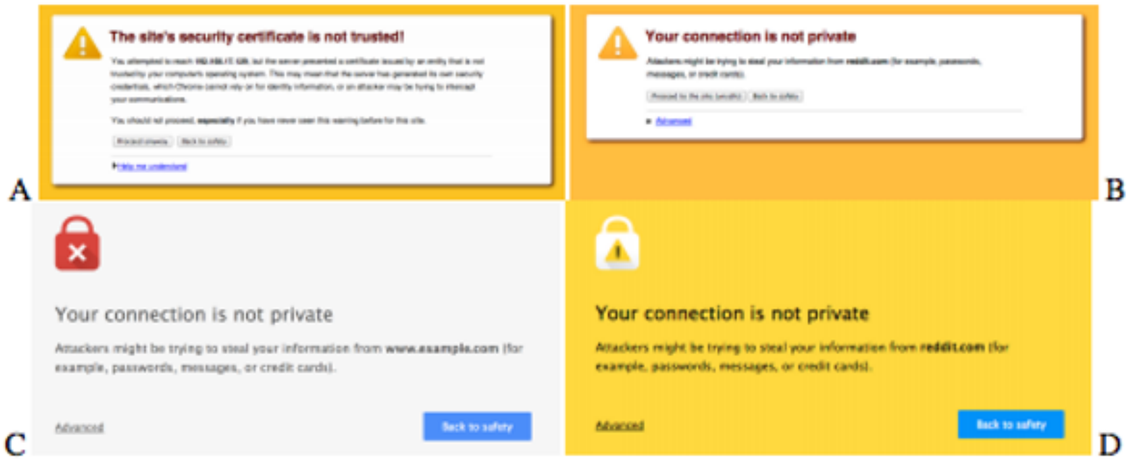
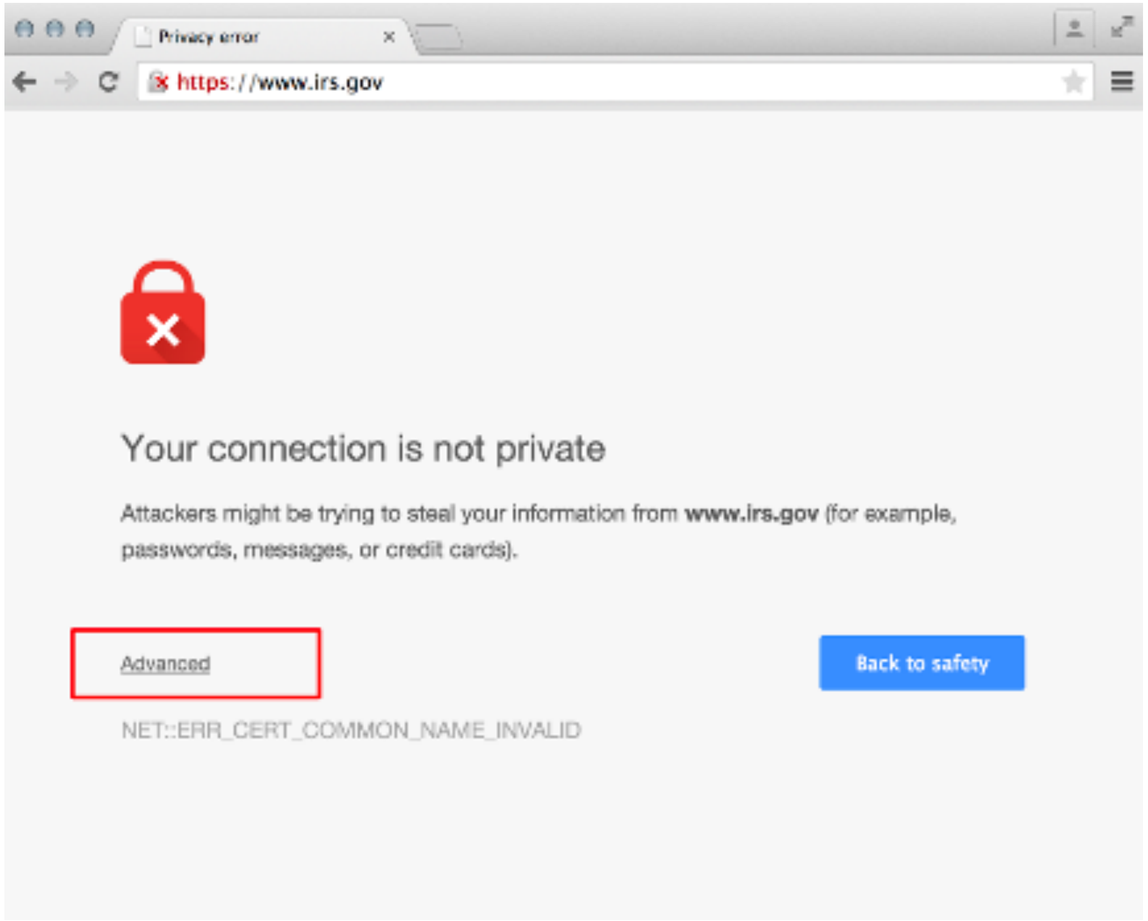


Figure 4. Conditions for our field experiment. *A* is the Chrome 36 warning, and *C* is the Chrome 37 warning.



Meta Thoughts on this Paper

- What is the role of context in improving usability?
- Do we like this work? Why or why not?

Next time…

- AI, Society, Doom
- Work on your projects :)