CS558 Network Security

Lecture 3: (Un)usable Security

BOSTON UNIVERSITY

maia blog

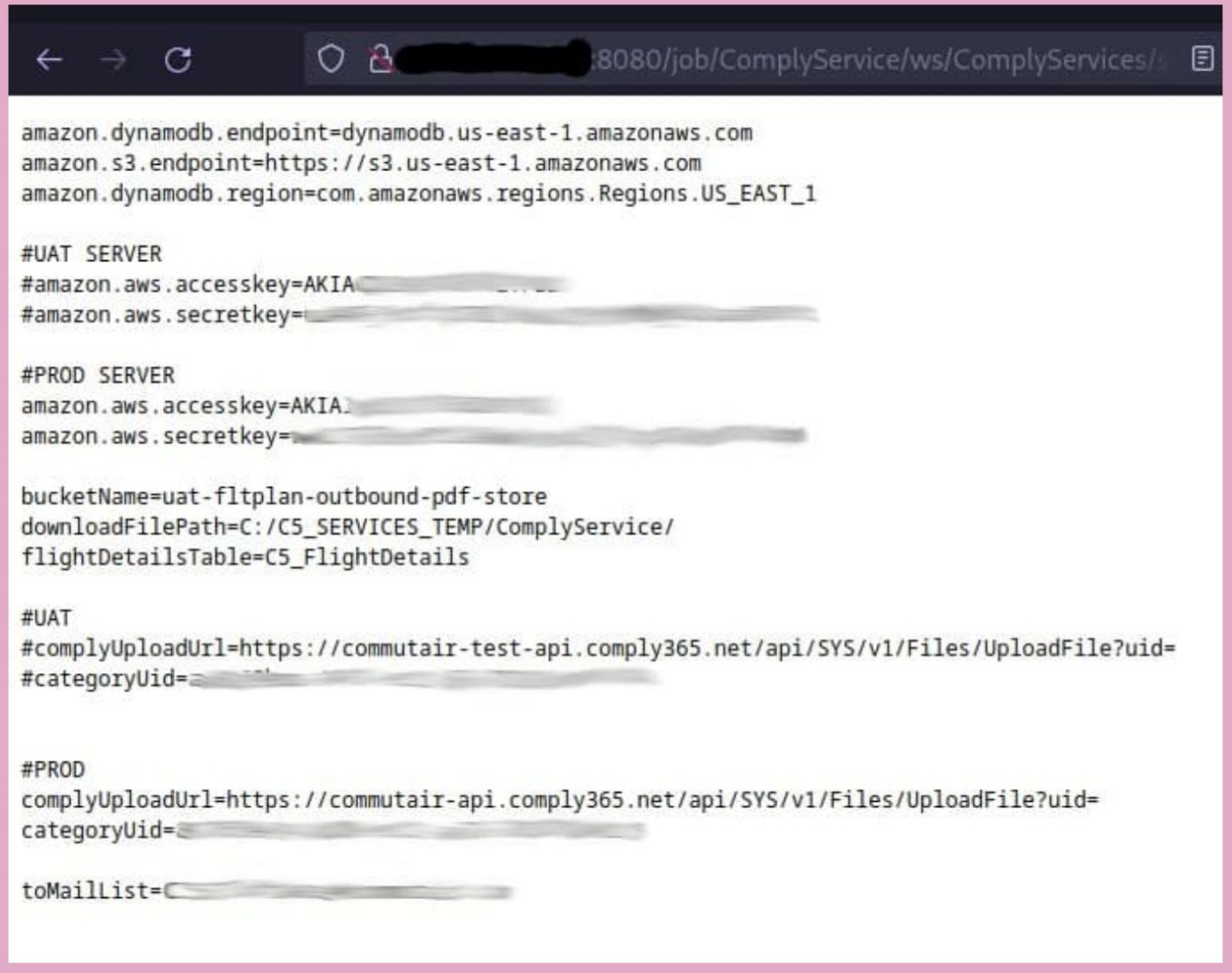
Jan 19, 2023 by **maia arson crimew** in security, infosec, jenkins, aviation, nofly

how to completely own an airline in 3 easy steps

and grab the TSA nofly list along the way

note: this is a slightly more technical* and comedic write up of the story covered by my friends over at dailydot, which you can read here

*i say slightly since there isnt a whole lot of complicated technical stuff going on here in the first place

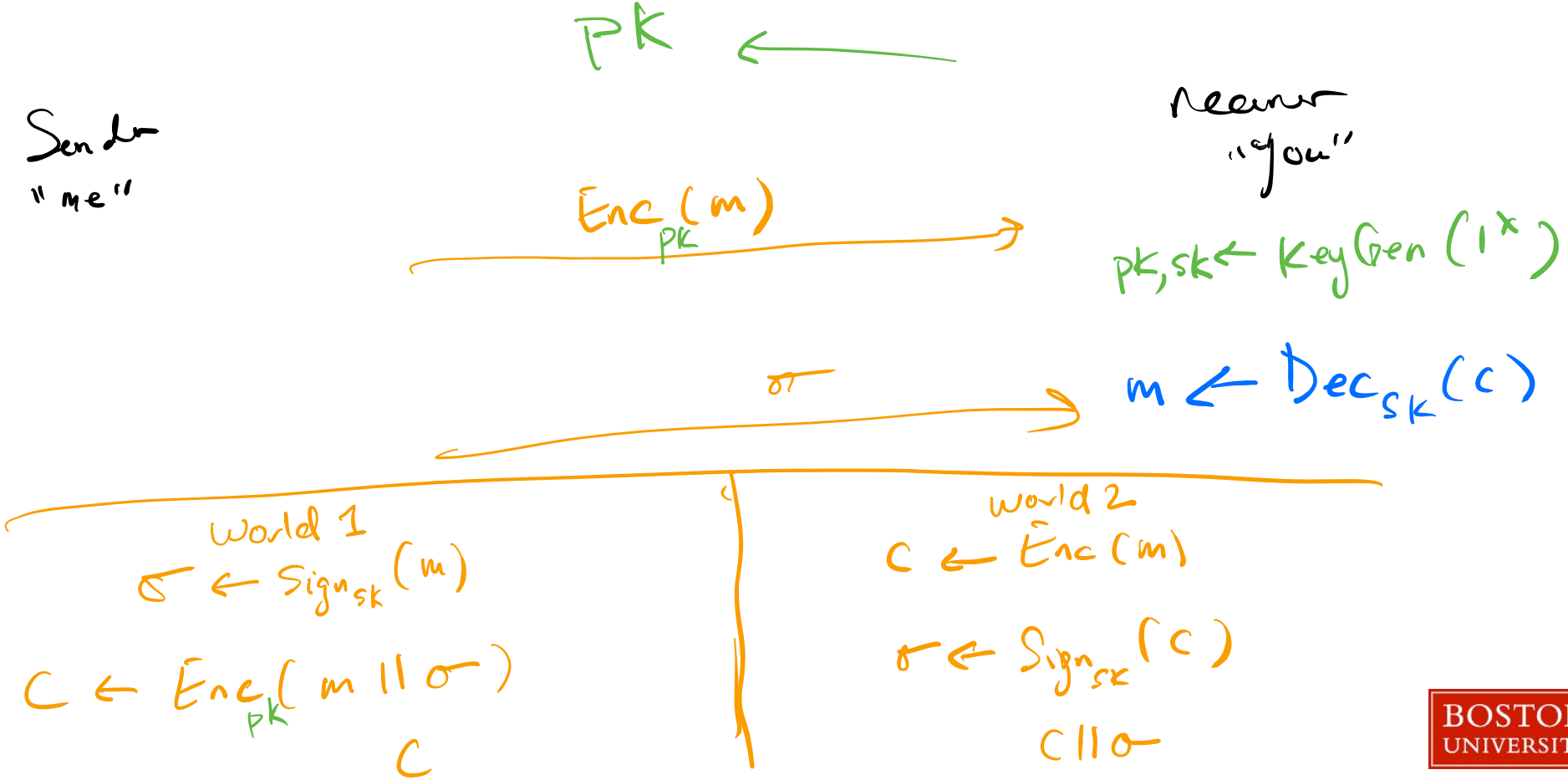


BOSTON UNIVERSITY

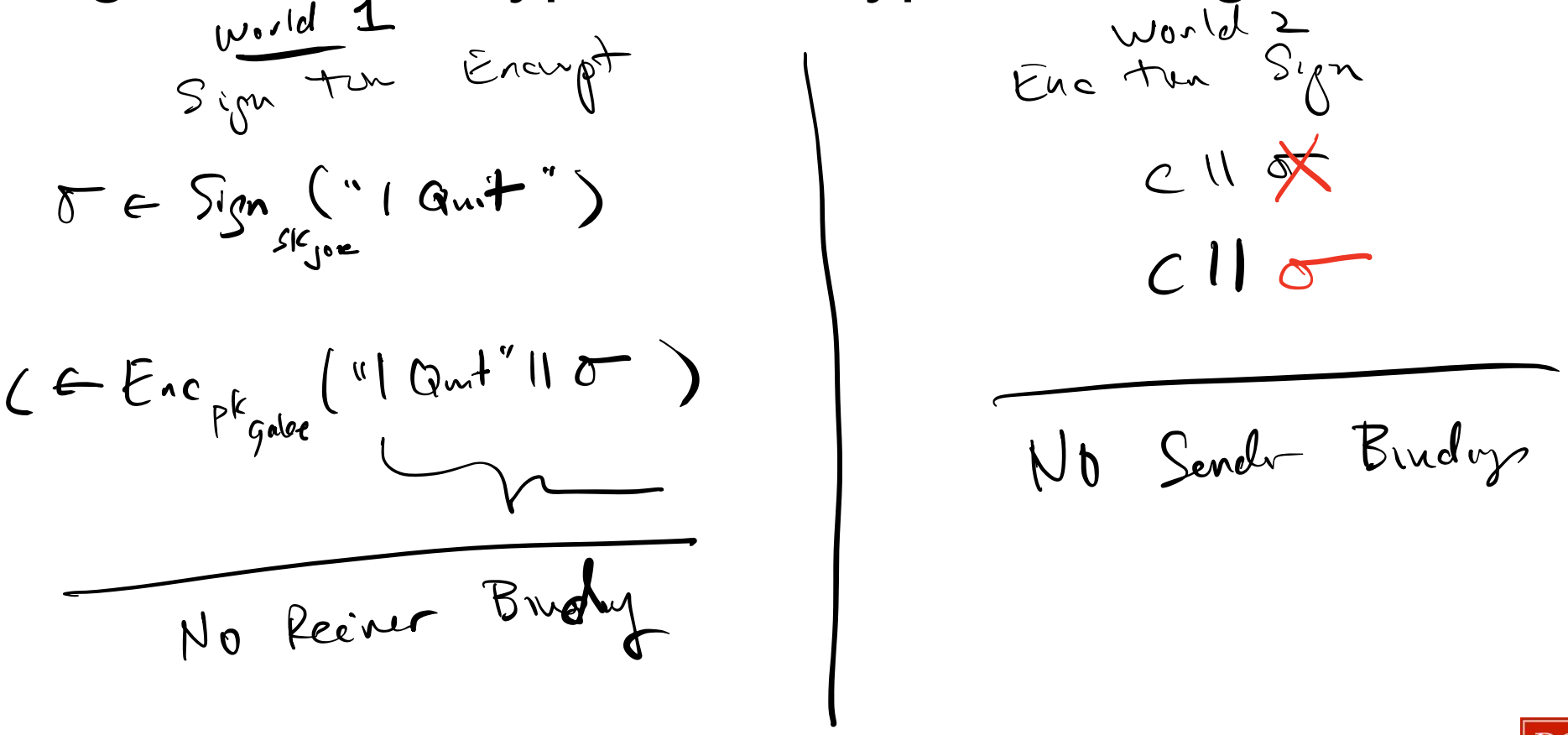
Things to learn in class:

- Just building a security tool isn't enough if no one uses it or can figure out how to use it
- Security by default is really important
- People are very lazy when it comes to security and privacy
- Sign then Encrypt vs Encrypt then Sign

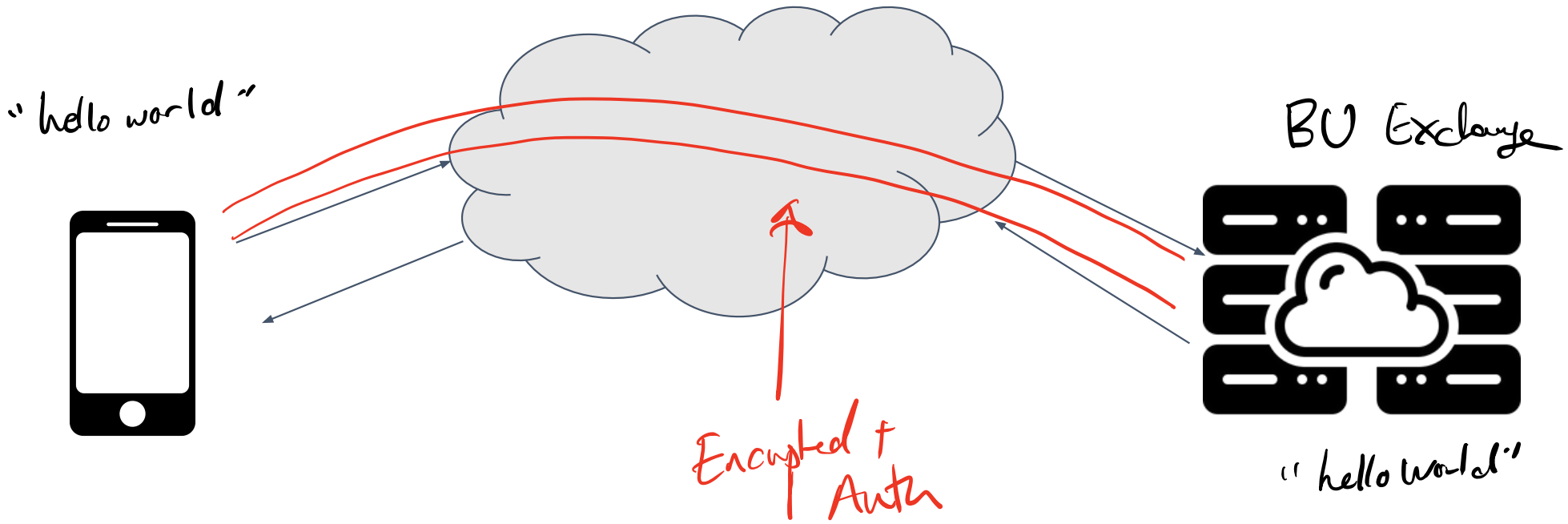
Encrypted Email, PGP (Technical Overview)



Sign then Encrypt or Encrypt then Sign?



Considering the Full Stack



“Given a choice between dancing pigs and security, users will pick dancing pigs every time”

- Gary McGraw and Edward Felten: *Securing Java*, 1999

Encrypted Email (The 2005 Experience)

"Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the Encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world readable."

- "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", Alma Whitten and J. D. Tygar, 2005

Why Johnny Can’t Encrypt

“Three of the twelve test participants (P4, P9, and P11) accidentally emailed the secret to the team members without encryption.”

“He kept attempting to find a way to “turn on” encryption, and at one point believed that he had done so by modifying the settings in the Preferences dialog in PGPkeys. Another of the 12 (P2) took more than 30 minutes to figure out how to encrypt”

“Seven participants (P1, P2, P7, P8, P9, P10, and P11) used only their own public keys to encrypt email to the team members. Of those seven, only P8 and P10 eventually succeeded in sending correctly encrypted email to the team members before the end of the 90-minute test session”

“Another of the 11 (P5) so completely misunderstood the model that he generated key pairs for each team member rather than for himself, and then attempted to send the secret in an email encrypted with the five public keys he had generated”

The Motivated Can Encrypt (Even with PGP)

Glencora Borradaile*[1], Kelsy Kretschmer†[2], Michele Gretes‡[1], and Alexandria LeClerc§[1]

[1]School of Electrical Engineering and Computer Science
[2]School of Public Policy
Oregon State University

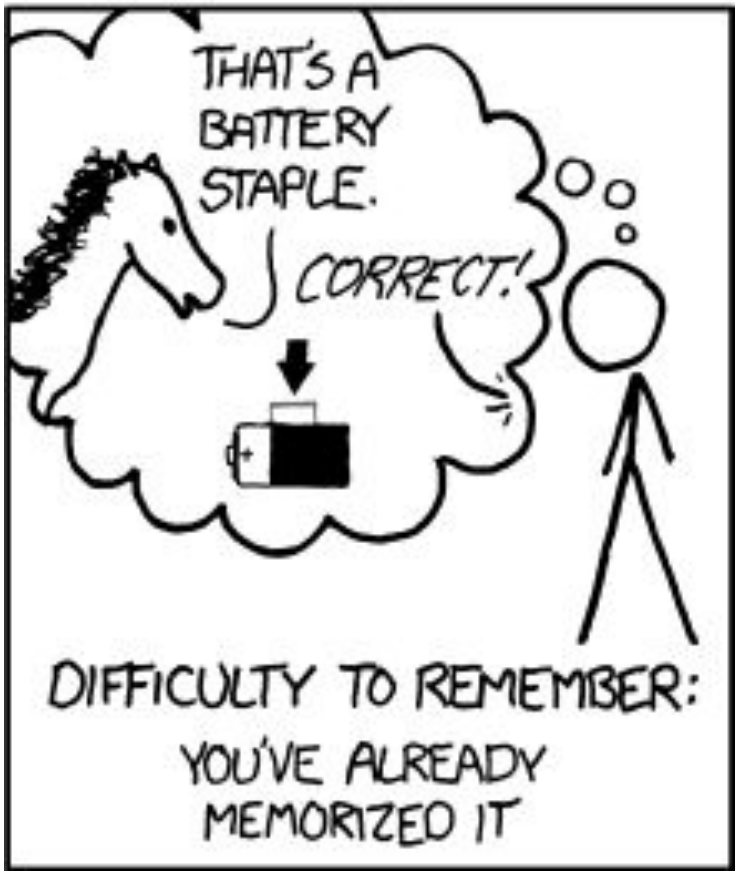
2021

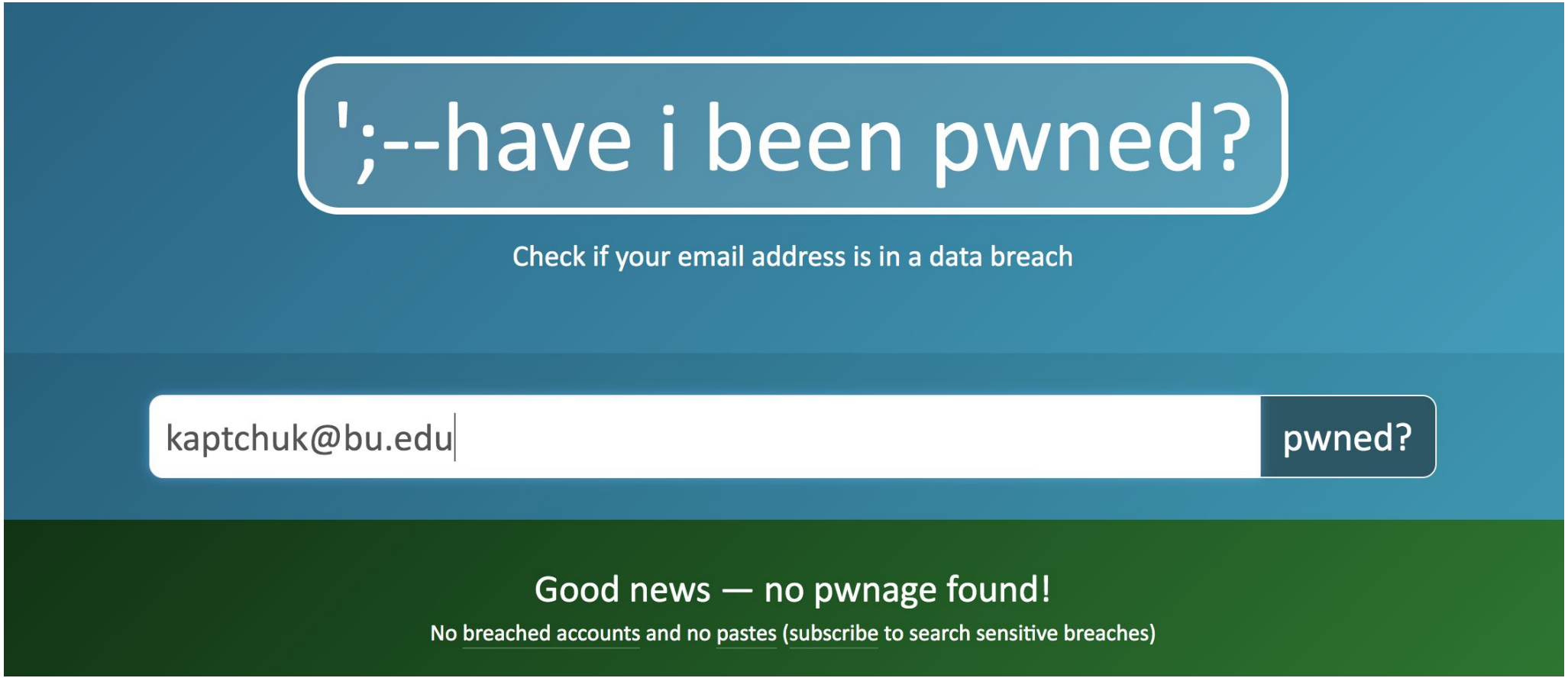
Abstract

Existing end-to-end-encrypted (E2EE) email systems, mainly PGP, have long been evaluated in controlled lab settings. While these studies have exposed usability obstacles for the average user and offer design improvements, there exist users with an immediate need for private communication, who must cope with existing software and its limitations. We seek to understand whether individuals motivated by concrete privacy threats, such as those vulnerable to state surveillance, can overcome usability issues to adopt complex E2EE tools for long-term use. We surveyed regional activists, as surveillance of social movements is well-documented. Our study group includes individuals from 9 social movement groups in the US who had elected to participate in a workshop on using Thunderbird+Enigmail for email encryption. These workshops tool place prior

BOSTON UNIVERSITY

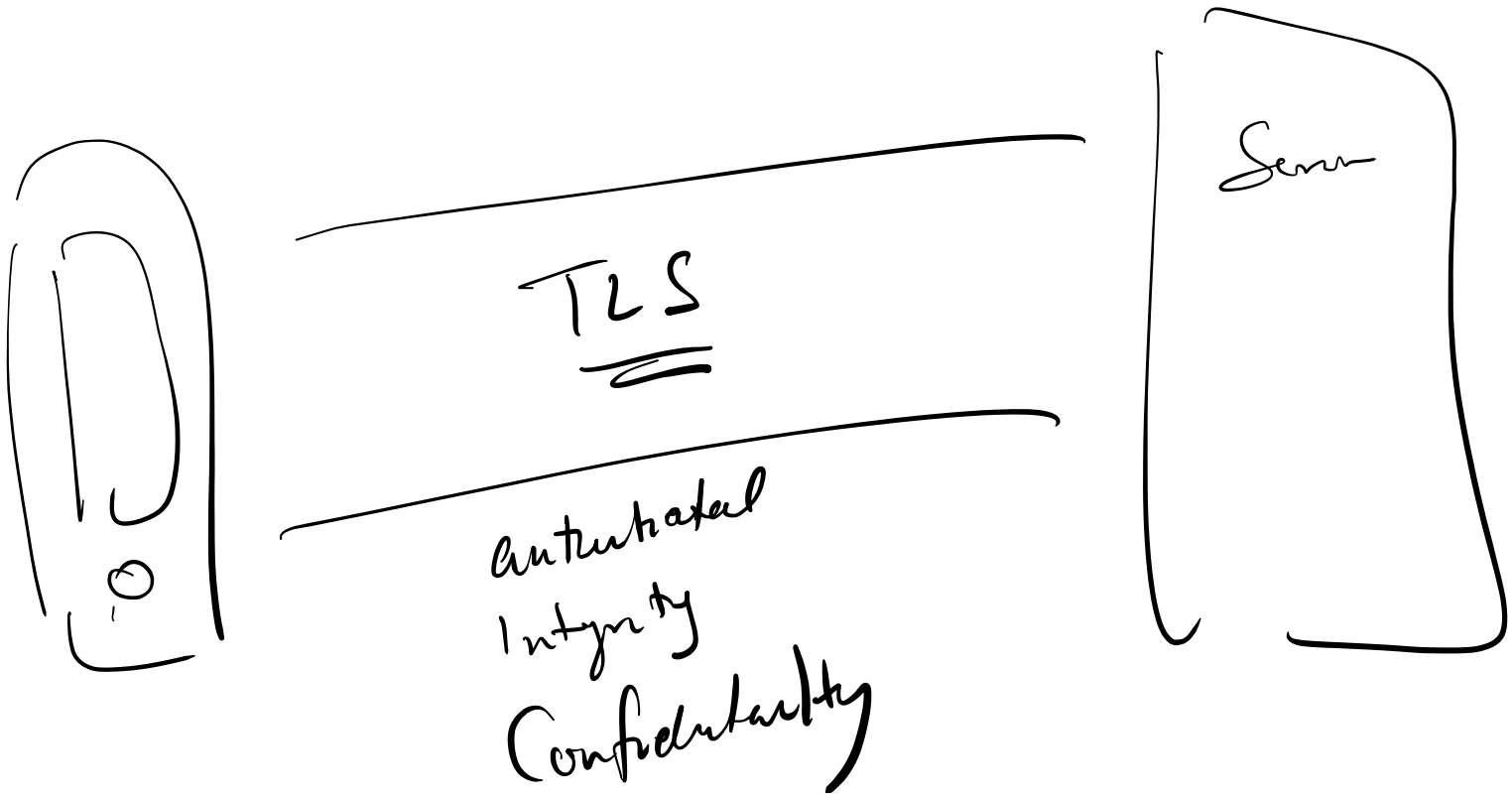
Passwords


THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

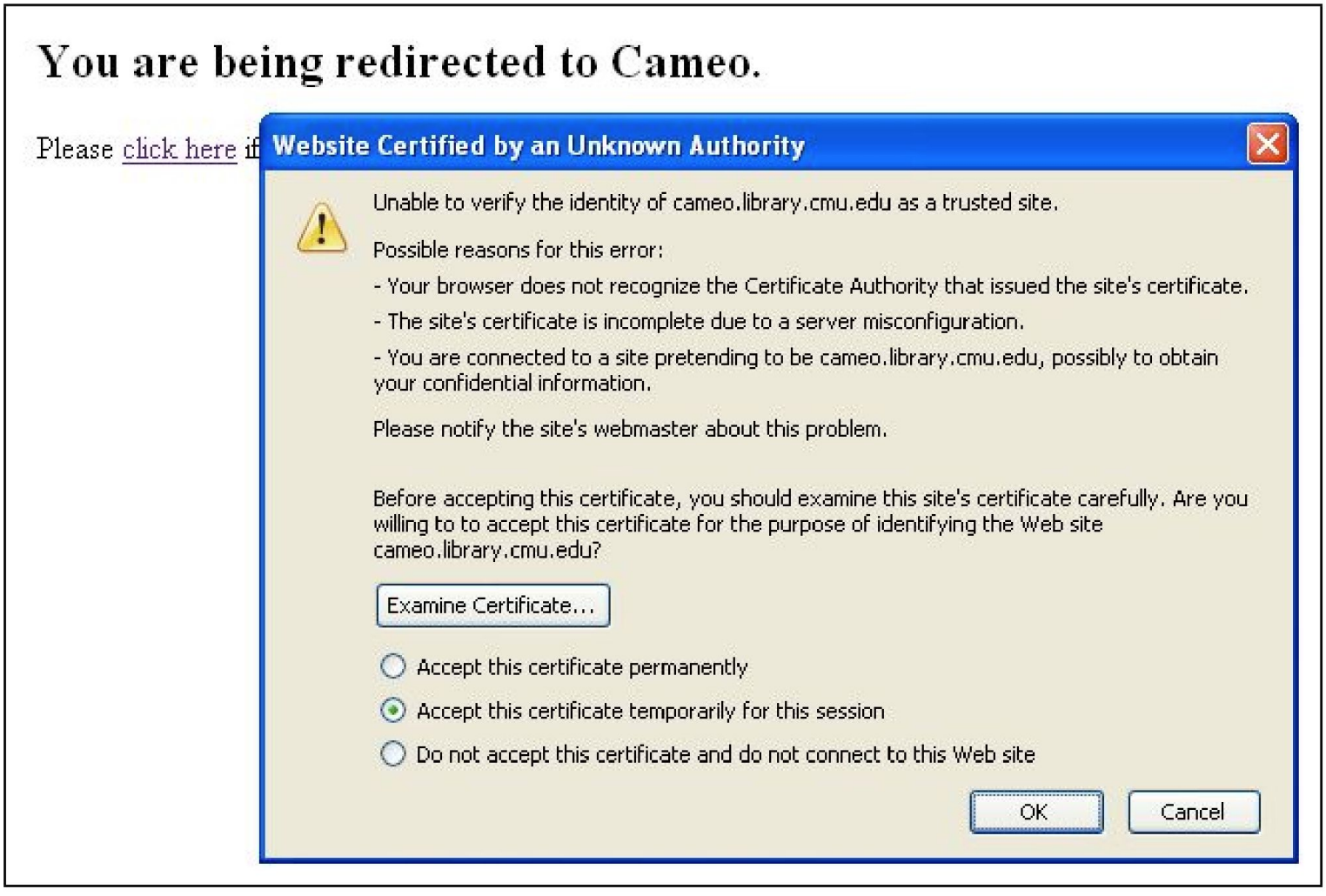


BOSTON UNIVERSITY

TLS

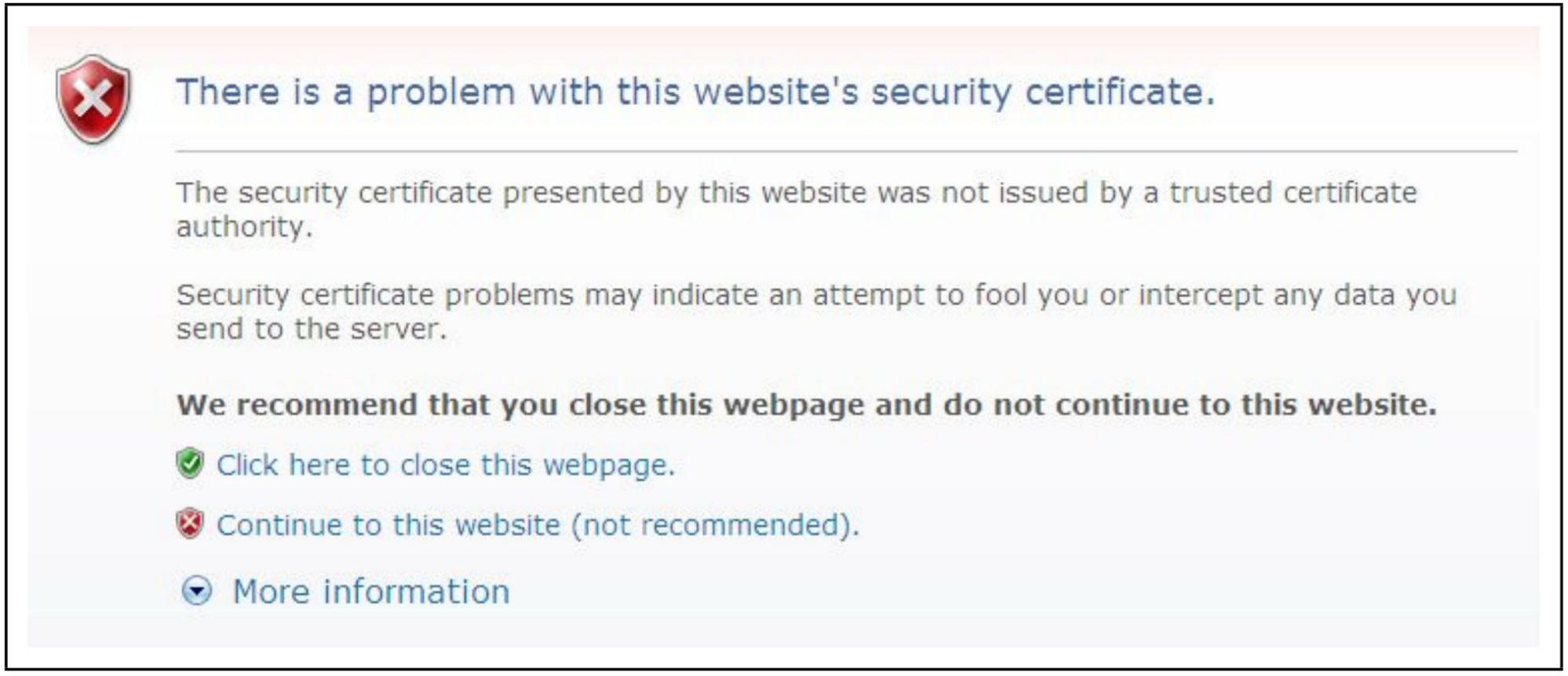


IE6
mid 2000s



(a) Firefox 2

2006



(b) Internet Explorer 7

	FF2		FF3		IE7		Single-Page		Multi-Page	
Bank	18	(90%)	11	(55%)	18	(90%)	9	(45%)	12	(60%)
Library	19	(95%)	12	(60%)	20	(100%)	16	(80%)	19	(95%)

Table 5: Number (and percentage) of participants in each condition who ignored the warning and used the website to complete the library and bank tasks.

"Crying Wolf: An Empirical Study of SSL Warning Effectiveness", Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor, Usenix 2009

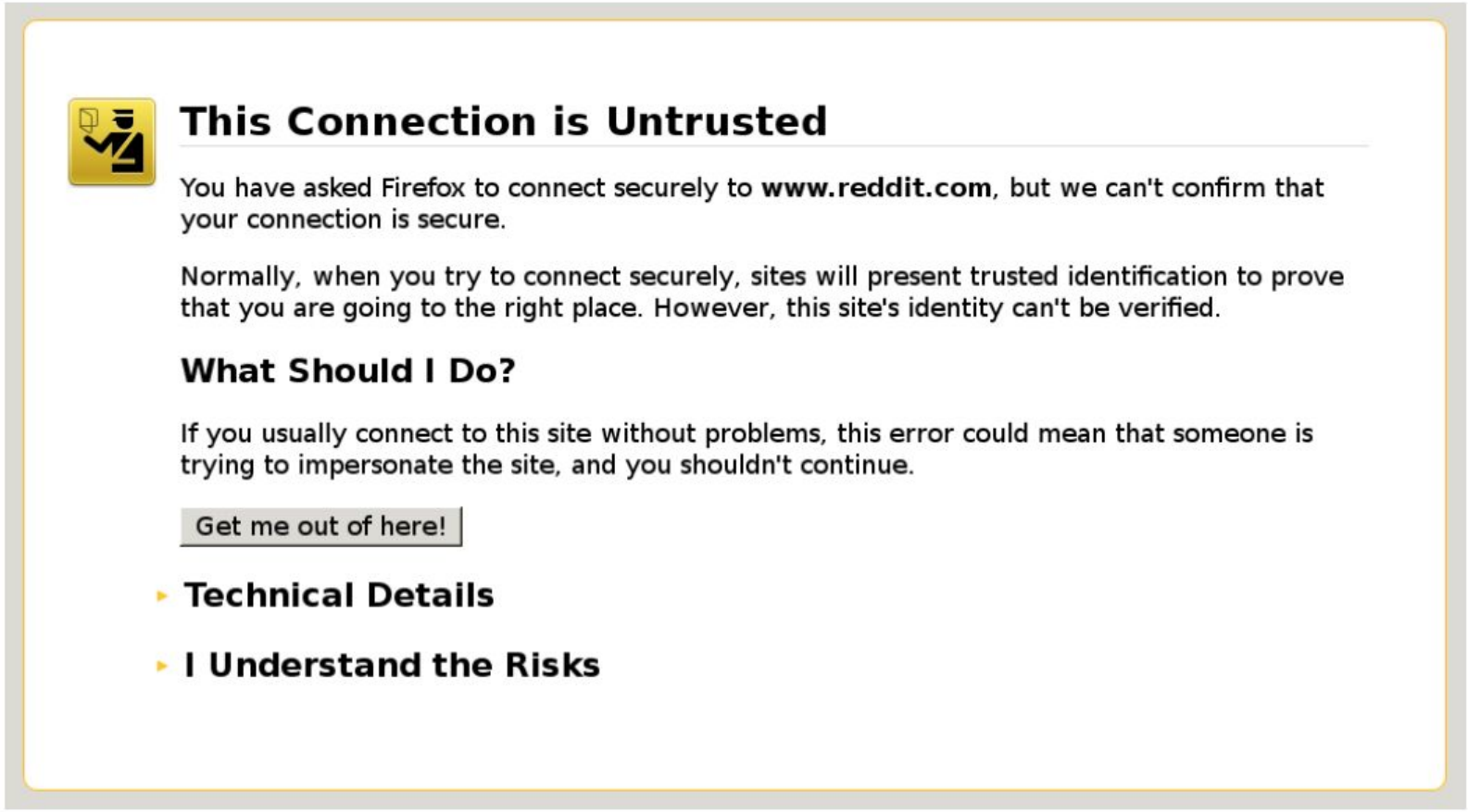


Figure 4: SSL warning for Mozilla Firefox

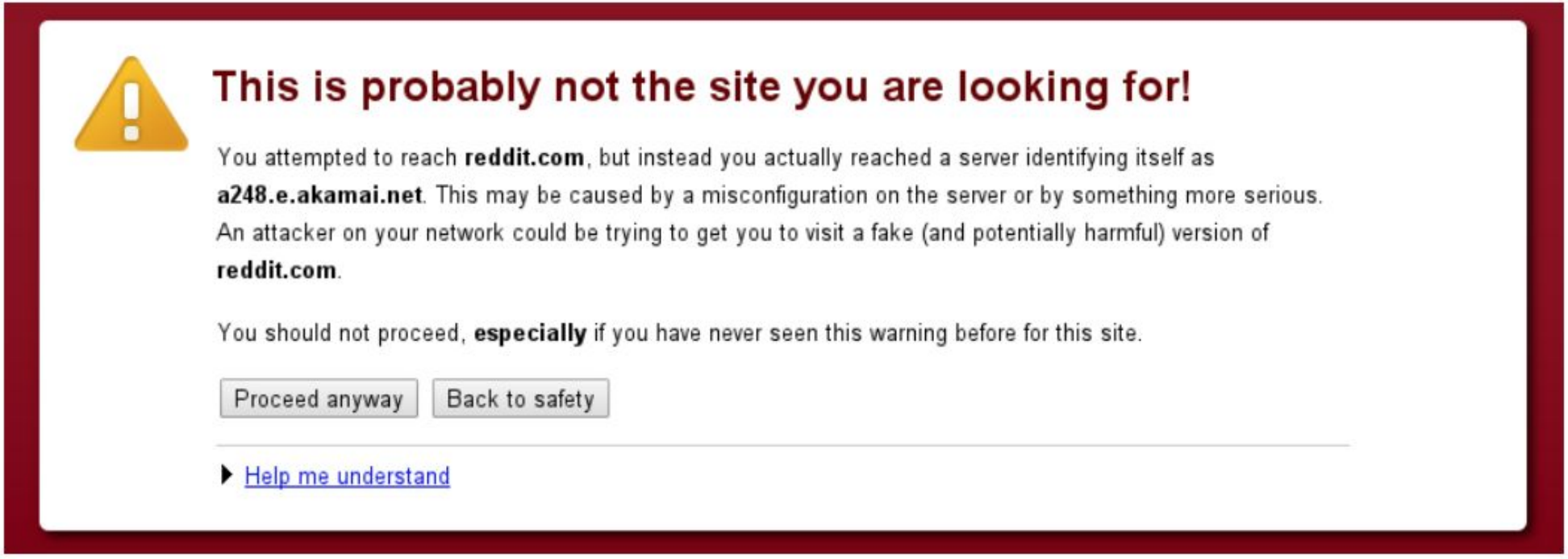


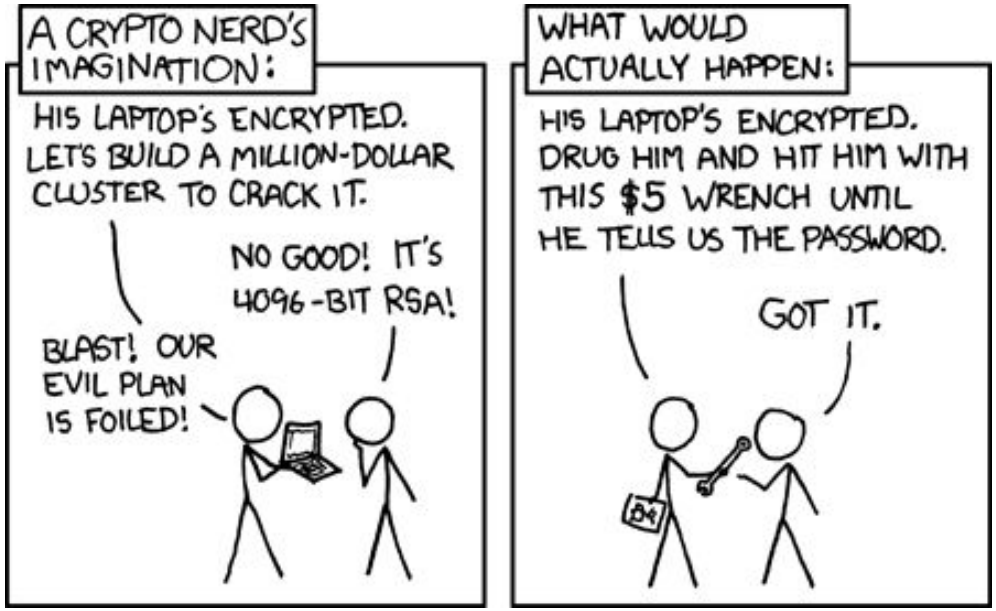
Figure 3: SSL warning for Google Chrome. The first paragraph changes depending on the specific SSL error.

Operating System	SSL Warnings	
	Firefox	Chrome
Windows	32.5%	71.1%
MacOS	39.3%	68.8%
Linux	58.7%	64.2%
Android	NC	64.6%

Table 3: User operating system vs. clickthrough rates for SSL warnings. The Google Chrome data is from the stable channel, and the Mozilla Firefox data is from the beta channel.

"Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness", Devdatta Akhawe and Adrienne Porter Felt, Usenix 2013

Human Factors broadly



But how to I get the keys…?

(1) Everyone picks someone to trust

(2) Web of trust