

CS558 Network Security

Lecture 3: (Un)usable Security



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

← → ↺ 🔒 [REDACTED] 8080/job/ComplyService/ws/ComplyServices/ ☰

```
amazon.dynamodb.endpoint=dynamodb.us-east-1.amazonaws.com
amazon.s3.endpoint=https://s3.us-east-1.amazonaws.com
amazon.dynamodb.region=com.amazonaws.regions.Regions.US_EAST_1

#UAT SERVER
#amazon.aws.accesskey=AKIA[REDACTED]
#amazon.aws.secretkey=[REDACTED]

#PROD SERVER
amazon.aws.accesskey=AKIA[REDACTED]
amazon.aws.secretkey=[REDACTED]

bucketName=uat-fltplan-outbound-pdf-store
downloadFilePath=C:/C5_SERVICES_TEMP/ComplyService/
flightDetailsTable=C5_FlightDetails

#UAT
#complyUploadUrl=https://commutair-test-api.comply365.net/api/SYS/v1/Files/UploadFile?uid=
#categoryUid=[REDACTED]

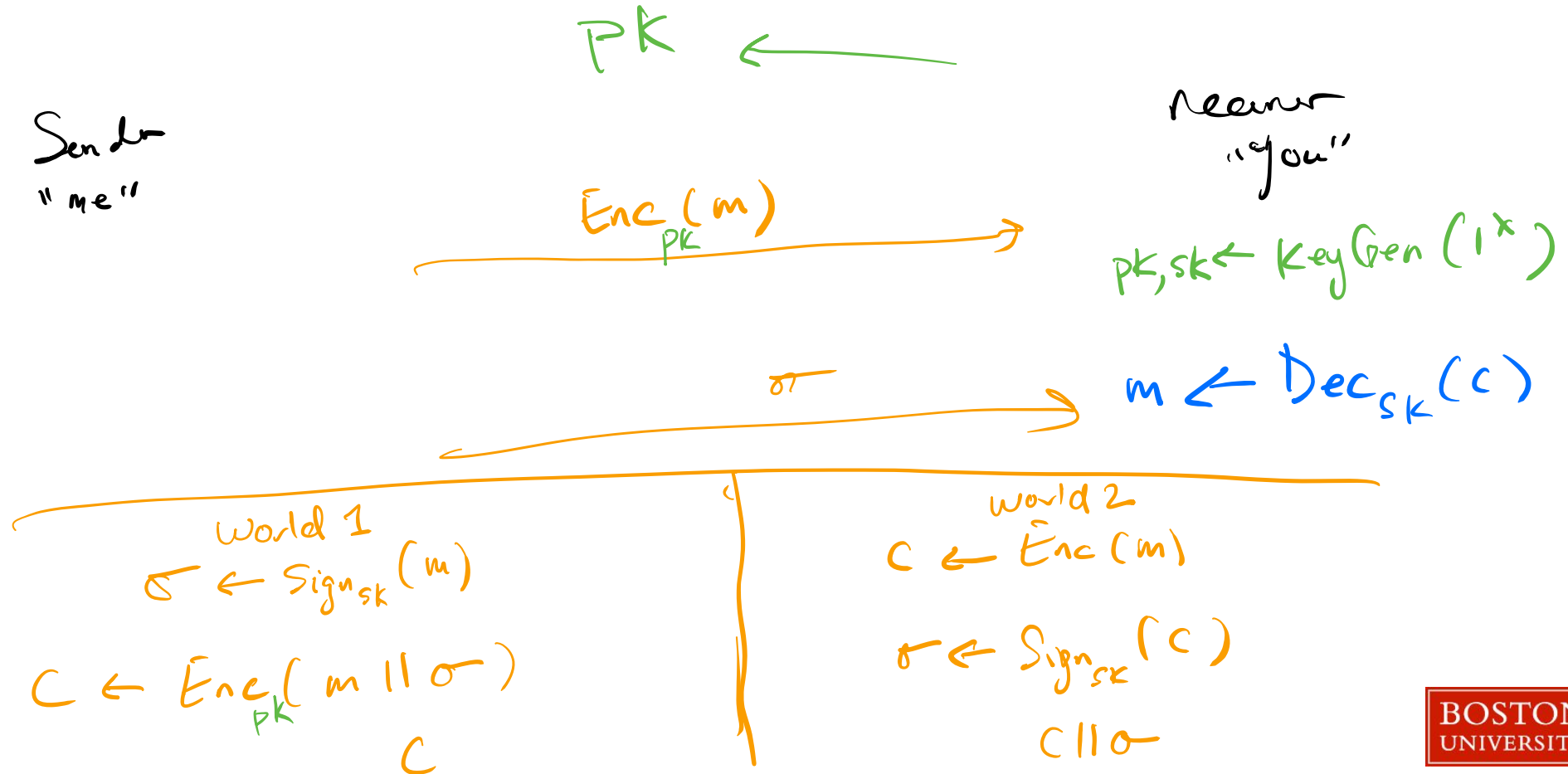
#PROD
complyUploadUrl=https://commutair-api.comply365.net/api/SYS/v1/Files/UploadFile?uid=
categoryUid=[REDACTED]

toMailList=[REDACTED]
```

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?

World 1
Sign then Encrypt

$$\sigma \leftarrow \text{Sign}_{\text{sk}_{\text{Joe}}}(\text{"I Quit"})$$

$$c \leftarrow \text{Enc}_{\text{pk}_{\text{Gabe}}}(\text{"I Quit"} \parallel \sigma)$$

No Receiver Bindings

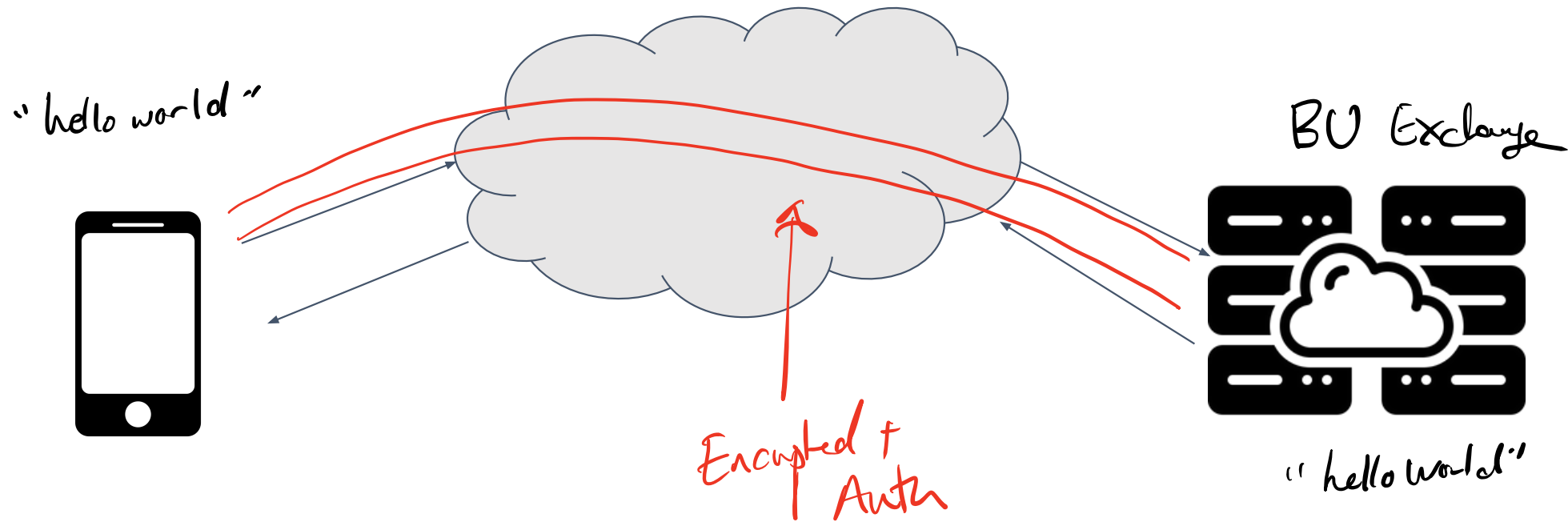
World 2
Enc then Sign

$$c \parallel \sigma \quad \text{X}$$

$$c \parallel \sigma \quad \text{O}$$

No Sender Bindings

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}

¹School of Electrical Engineering and Computer Science

²School of Public Policy

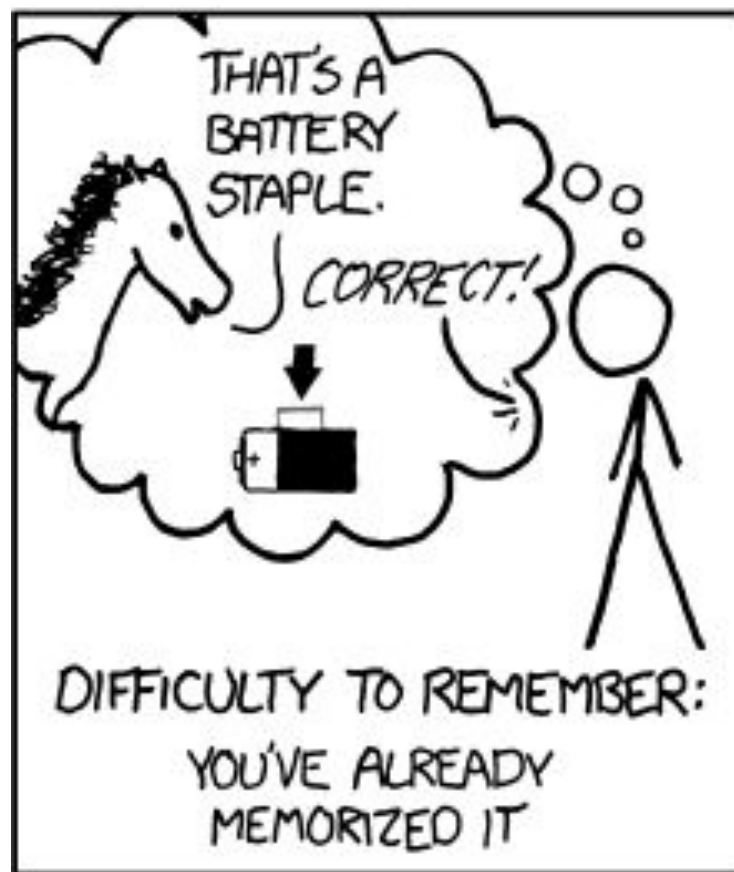
Oregon State University

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 took place prior

Passwords



';--have i been pwned?

Check if your email address is in a data breach

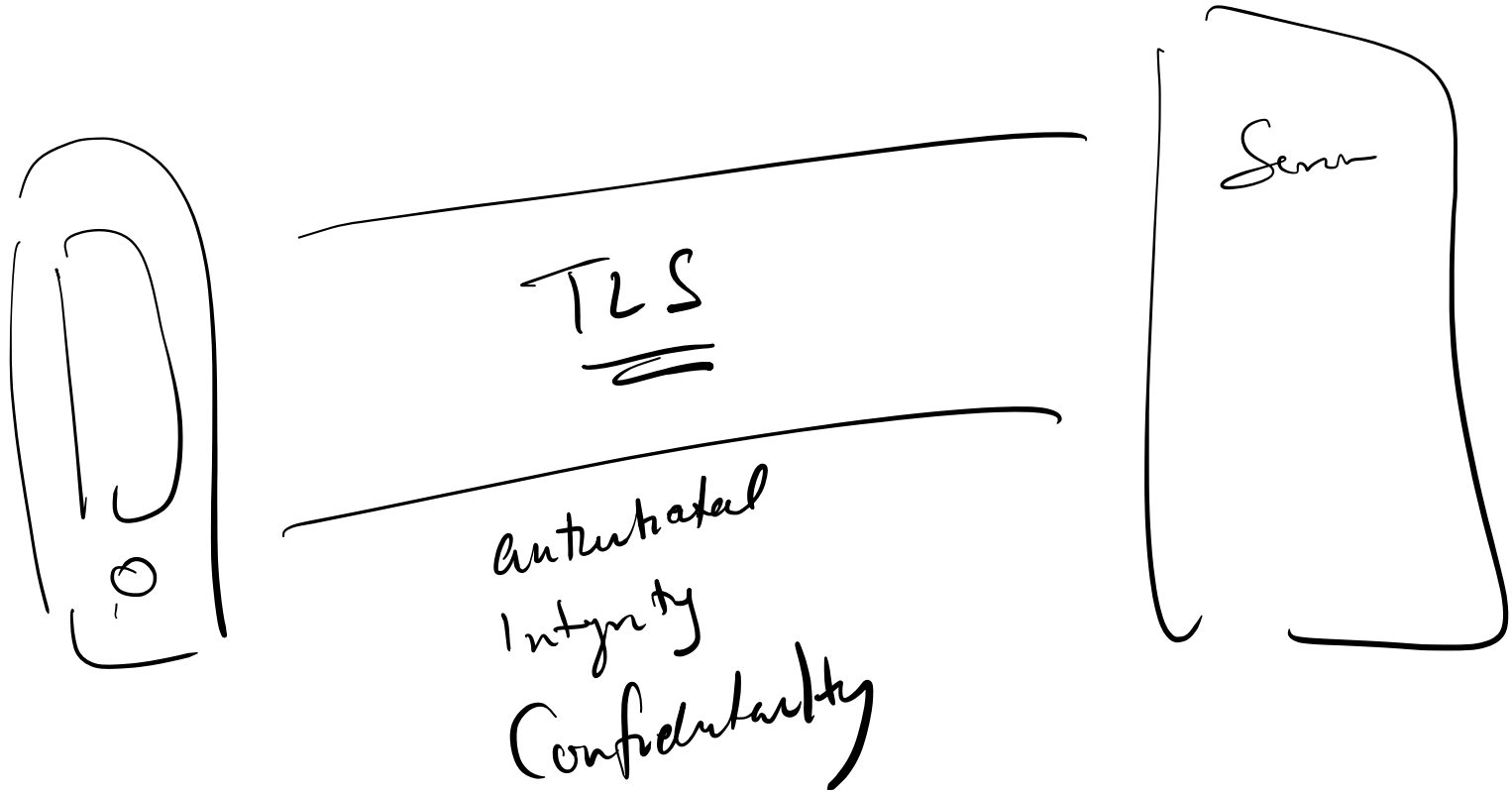
kaptchuk@bu.edu

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

TLS



IE6
mid 2000s



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

2006



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

	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 Almuhiemedi, Neha Atri, and Lorrie Faith Cranor, Usenix 2009



This Connection is Untrusted

You have asked Firefox to connect securely to **www.reddit.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Figure 4: SSL warning for Mozilla Firefox



This is probably not the site you are looking for!

You attempted to reach **reddit.com**, but instead you actually reached a server identifying itself as **a248.e.akamai.net**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **reddit.com**.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway

Back to safety

► [Help me understand](#)

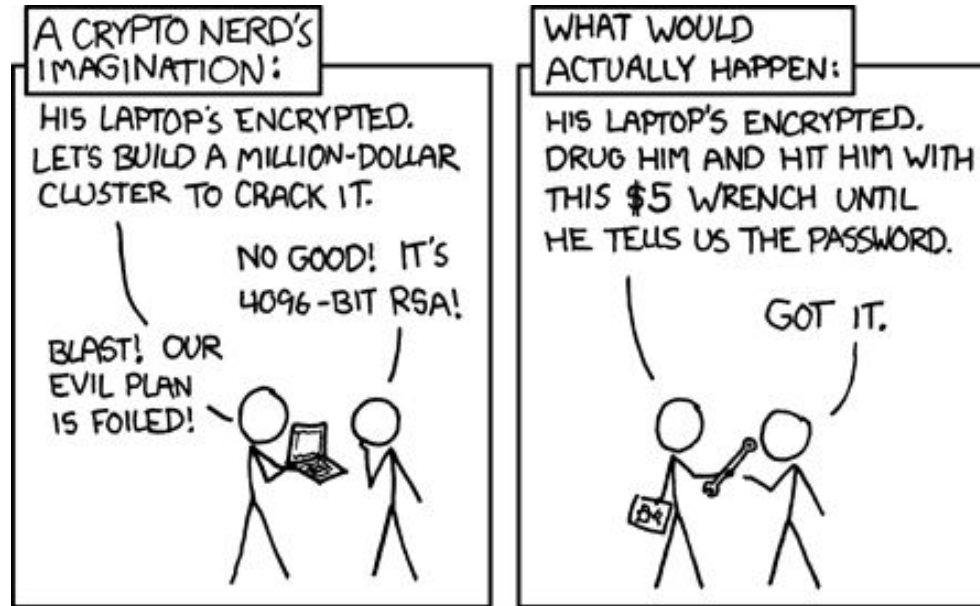
Figure 3: SSL warning for Google Chrome. The first paragraph changes depending on the specific SSL error.

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...?

PK
← "internet"

(1) Everyone picks someone to trust

(2) Web of trust

