CSEP 564 : Computer Security and Privacy

Designing Systems

Fall 2022

David Kohlbrenner

dkohlbre@cs.washington.edu

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Logistics

- Lab 3a due tonight
- Lab 3b due in a week
  - Patch testing descriptions will go up tomorrow

- If you need a grade-attestation letter (e.g. for Microsoft) and haven't filled out the form linked on ed, you need to do that ASAP.

Course Eval

6:42

- https://uw.iasystem.org/survey/266239

- Please fill it out, I genuinely read every comment
  - Those comments directly affect the material, presentation of material, and types of assignments we do.

A quick lesson in why you do code review

A quick lesson in why you do code review

then pushing live

michael flanders

there is a command injection in test-patch.c

```
$ touch ';echo $(whoami)' && /lab3/test-patch ';echo $(whoami)'
The name of your patch should be formatted as 'sploitN-patch.diff' where N is the sploit number.
root
```

David Kohlbrenner

oh lol

yes

David Kohlbrenner

probably fixed

Usability and Security

Importance of Usability in Security

- Why is usability important?
  - People are the critical element of any computer system
    - People are the reason computers exist in the first place
  - Even if it is **possible** for a system to protect against an adversary, people may use the system in other, **less secure** ways

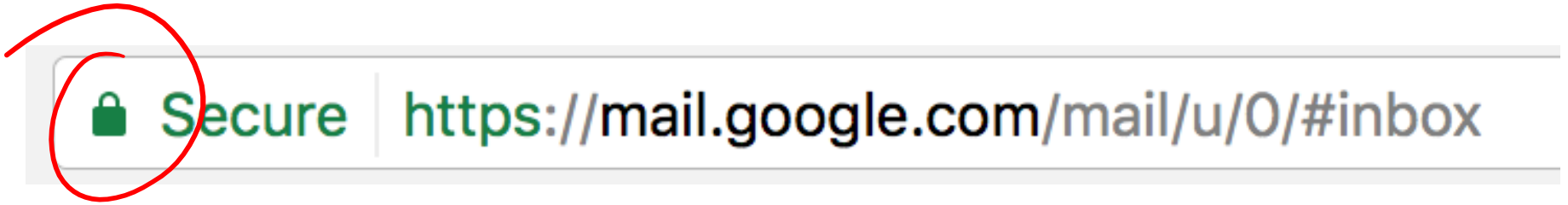
Usable Security Roadmap

- 3 case studies
  - HTTPS indicators + SSL warnings
  - Phishing
  - Password managers
- Step back: root causes of usability problems, and how to address

Case Study #1: Browser HTTPS Indicators

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site's SSL certificate is untrusted?
  - You discussed this in section a couple weeks ago

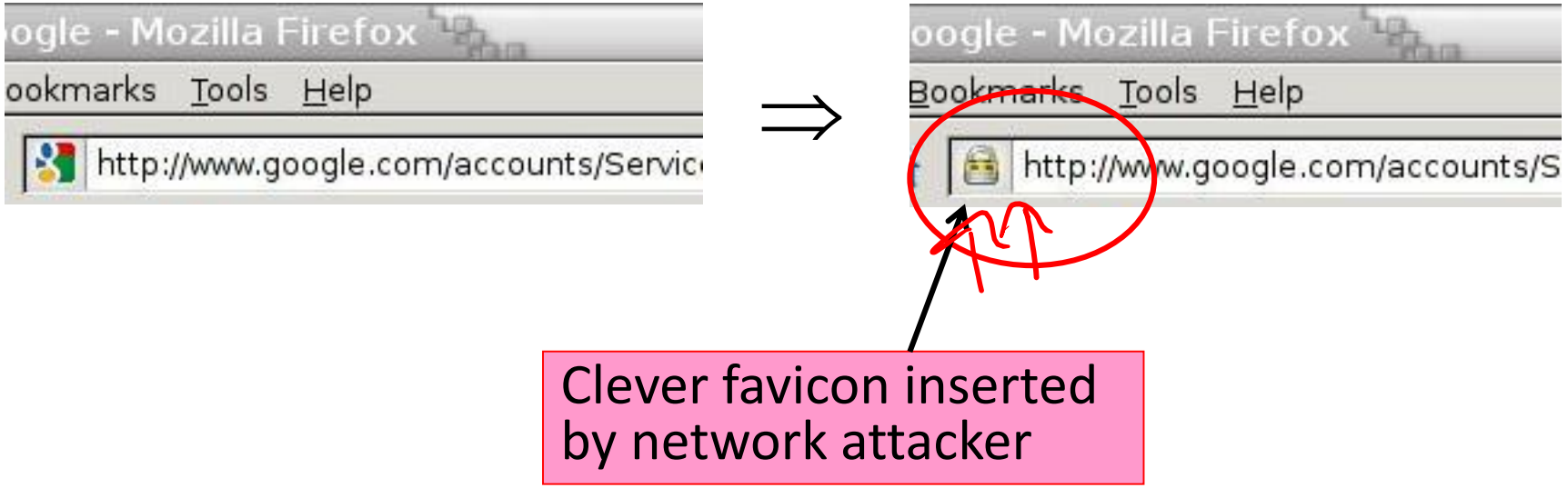
The Lock Icon



- Goal: identify secure connection
  - SSL/TLS is being used between client and server to protect against active network attacker
- Lock icon should only be shown when the page is secure against network attacker
  - Semantics subtle and not widely understood by users
  - Whose certificate is it??
  - Problem in user interface design

[Moxie Marlinspike]

Will You Notice?



Do These Indicators Help? (2007)

- "The Emperor's New Security Indicators"
  - http://www.usablesecurity.org/emperor/emperor.pdf

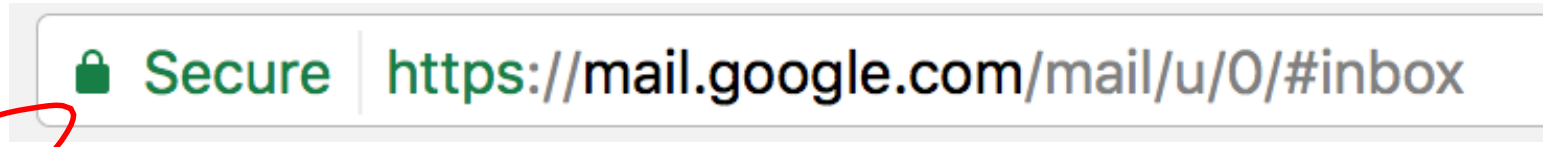
		Group				
Score	*First chose not to enter password...*	*1*	*2*	*3*	*1 ∪ 2*	*Total*
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%	8 36%	22 63%	30 53%
	Total	18	17	22	35	57

Lesson:

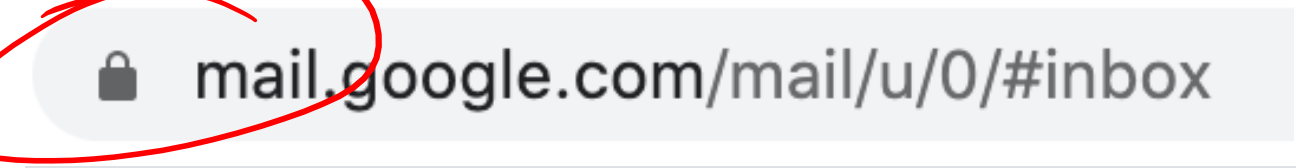
Users don't notice the **absence** of indicators!

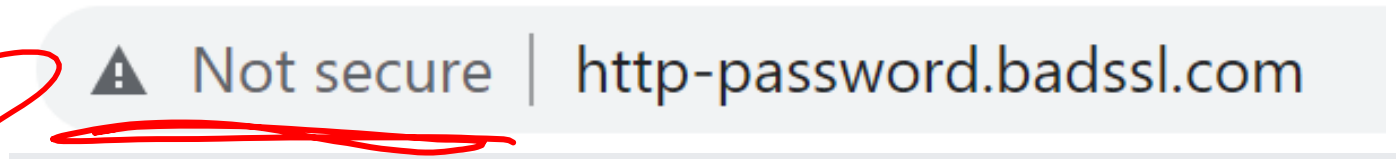
Newer Versions of Chrome

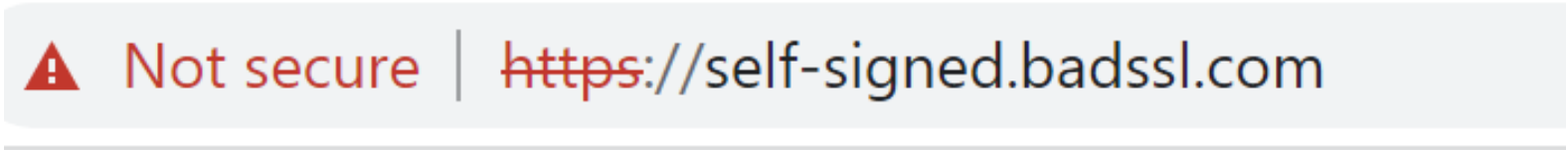
c. 2017



2022

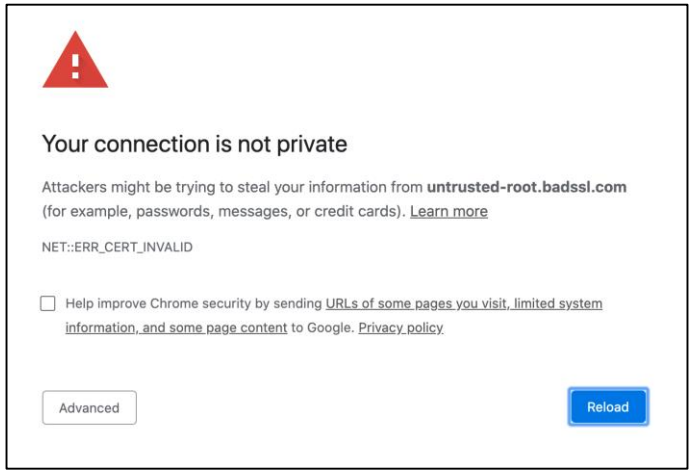






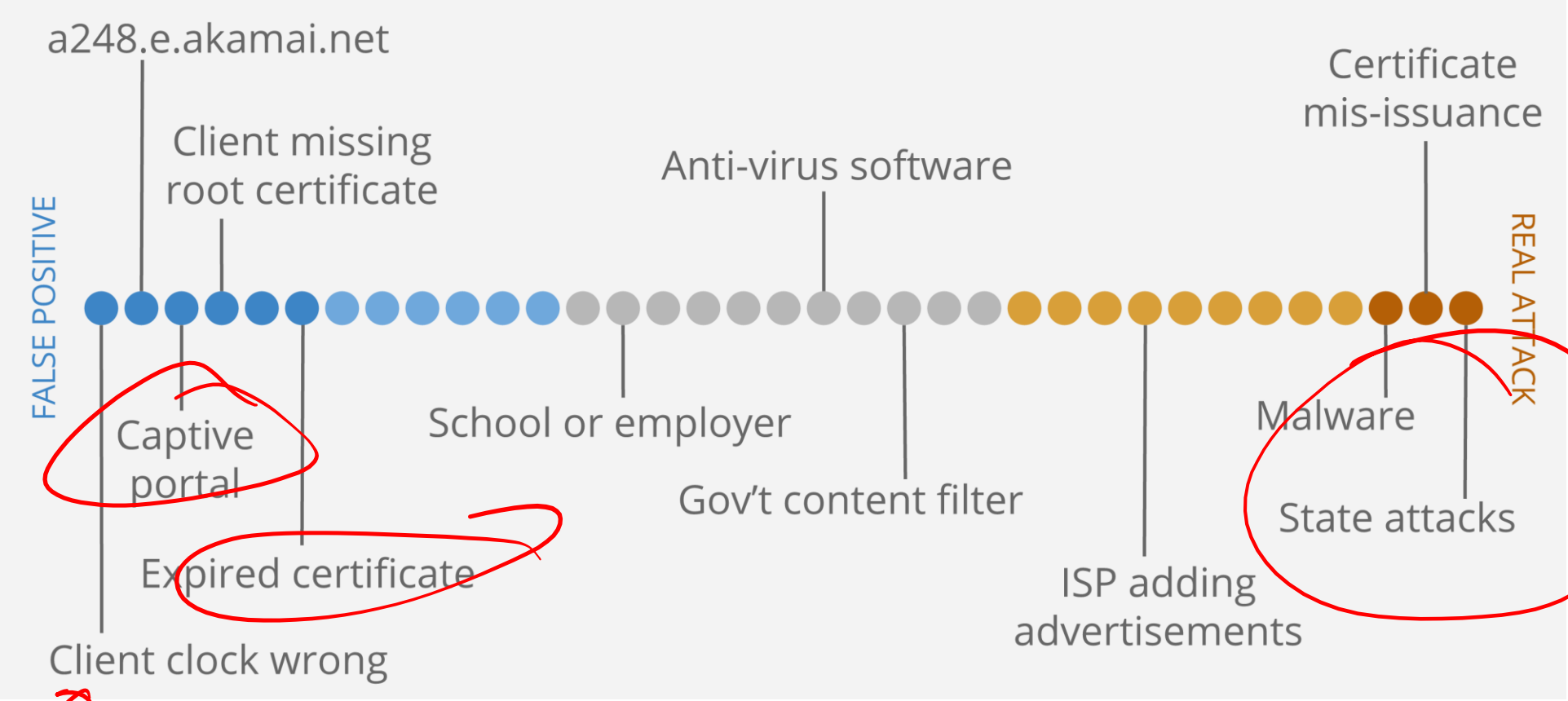
Case Study #1: Browser HTTPS Indicators

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site's SSL certificate is untrusted?



[Felt et al.]

Challenge: Meaningful Warnings

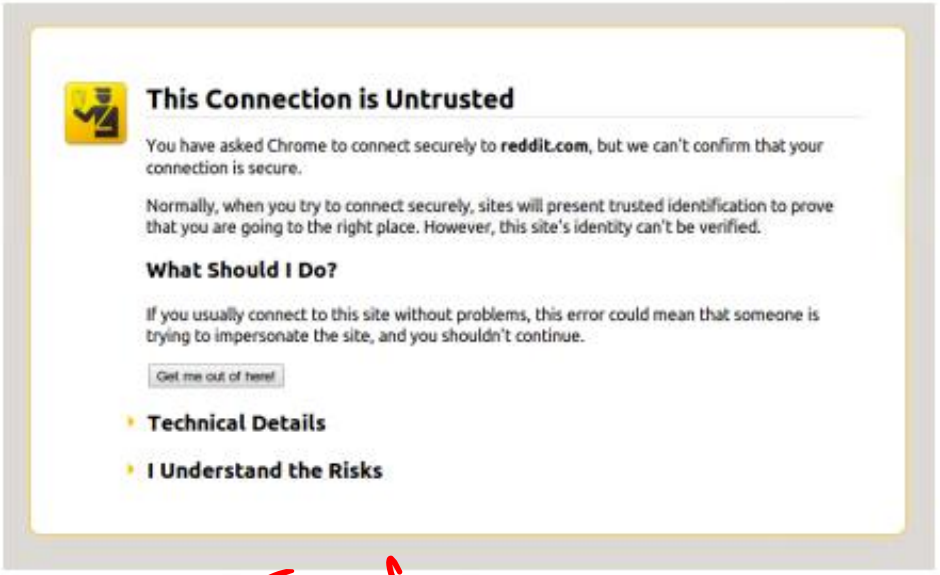


See current designs for different conditions at https://badssl.com/.

[Felt et al.]

Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate



Firefox

Chrome

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)		
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

Figure 1. The default Chrome SSL warning (Condition 1).

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

Figure 1. The default Chrome SSL warning (Condition 1).

Figure 4. The three images used in Conditions 2-4.

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19.297
7	Mock Firefox with corporate styling		

Table 1. Click-through rates and sample size for conditions.

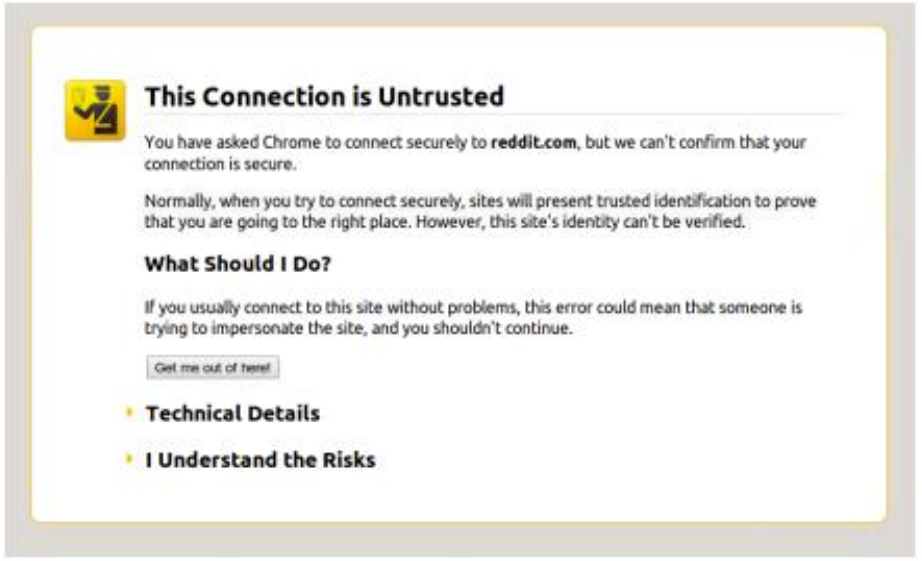


Figure 2. The mock Firefox SSL warning (Condition 5).

[Felt et al.]

Experimenting w/ Warning Design

#	Condition	CTR	N
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19,297
7	Mock Firefox with corporate styling	55.8%	19,845

Table 1. Click-through rates and sample size for conditions.

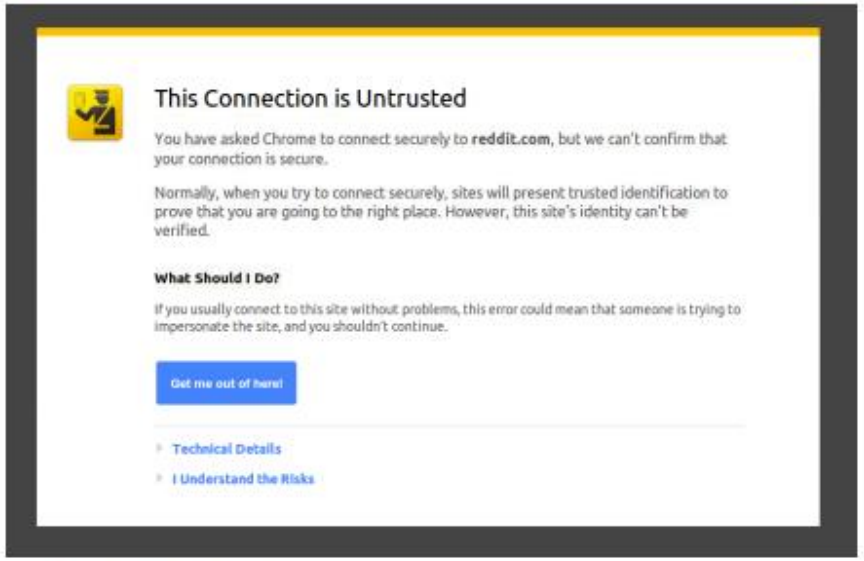
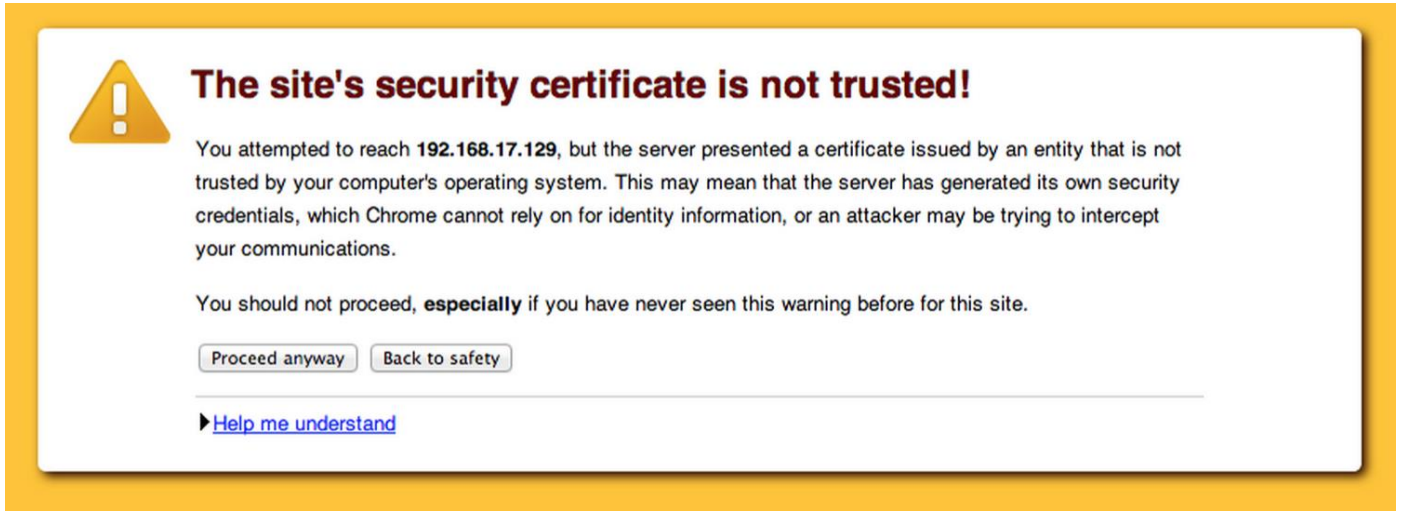


Figure 3. The Firefox SSL warning with Google styling (Condition 7).

[Felt et al.]

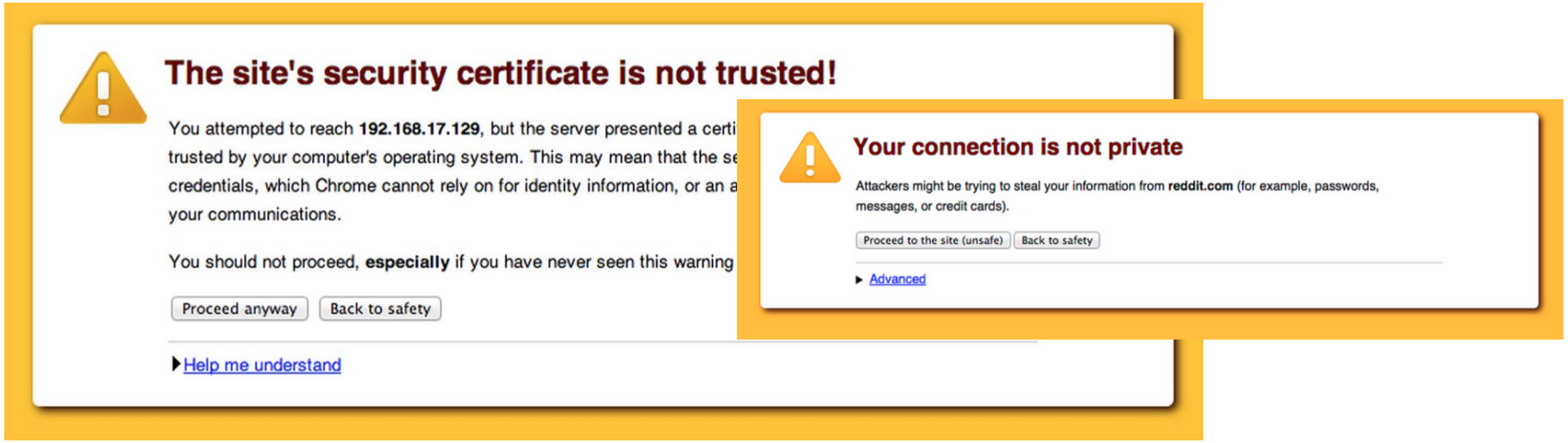
Opinionated Design Helps!

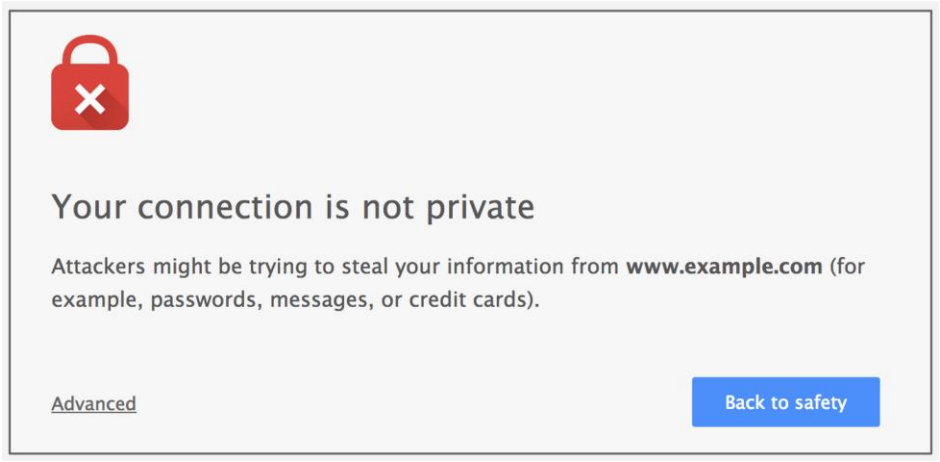


Adherence	N
30.9%	4,551

[Felt et al.]

Opinionated Design Helps!





Adherence	N
30.9%	4,551
32.1%	4,075
58.3%	**4,644**

Today’s warnings

Deprecated encryption schemes

This site can't provide a secure connection

rc4.badssl.com uses an unsupported protocol.

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Details

Secure Connection Failed

An error occurred during a connection to rc4.badssl.com. Cannot communicate securely with peer: no common encryption algorithm(s).

Error code: SSL_ERROR_NO_CYPHER_OVERLAP

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...

Try Again

Expired certificates

Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Advanced

Back to safety

Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to expired.badssl.com. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

Your computer clock is set to 12/7/2022. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh expired.badssl.com.

If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the problem.

Learn more...

Go Back (Recommended)

Advanced...

Self-signed certificates

Your connection is not private

Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Advanced

Back to safety

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to self-signed.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...

Go Back (Recommended)

Advanced...

Untrusted Root certificate

Your connection is not private

Attackers might be trying to steal your information from **untrusted-root.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Advanced

Back to safety

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to untrusted-root.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

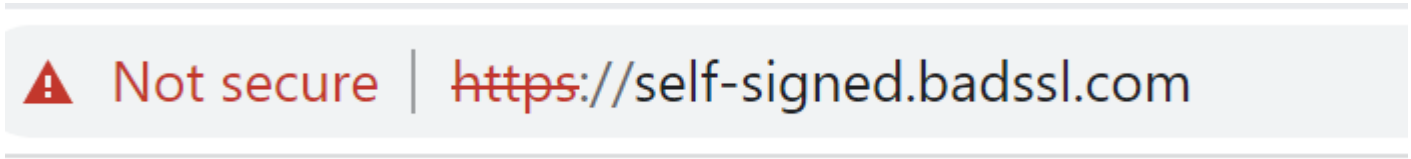
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

Go Back (Recommended)

Advanced...

Address Bar behaviors



Does anything stand out?

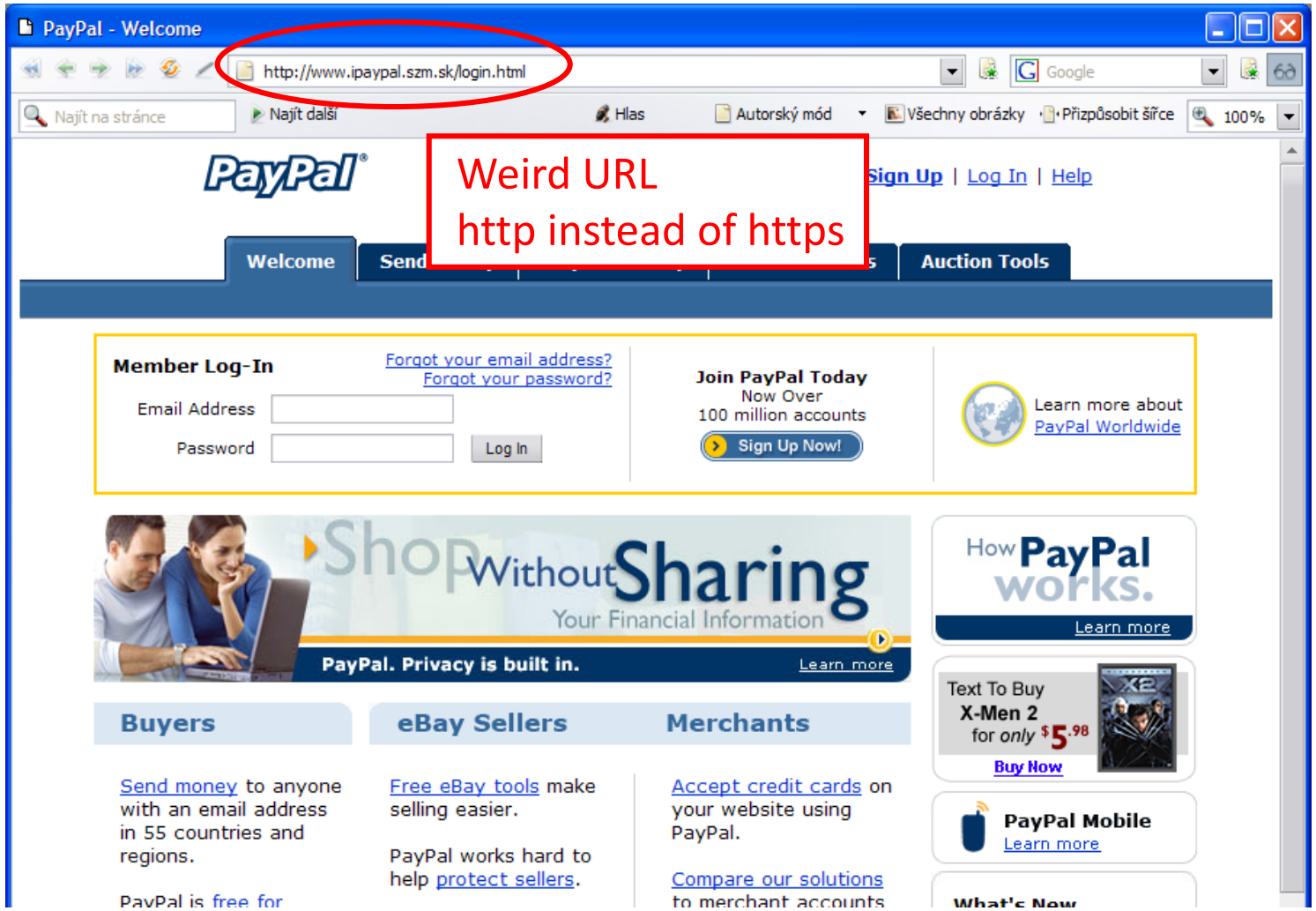
7:10

- Pollev
- What makes warnings hard, especially over time?
- Why do Firefox and Chrome make different warning designs?

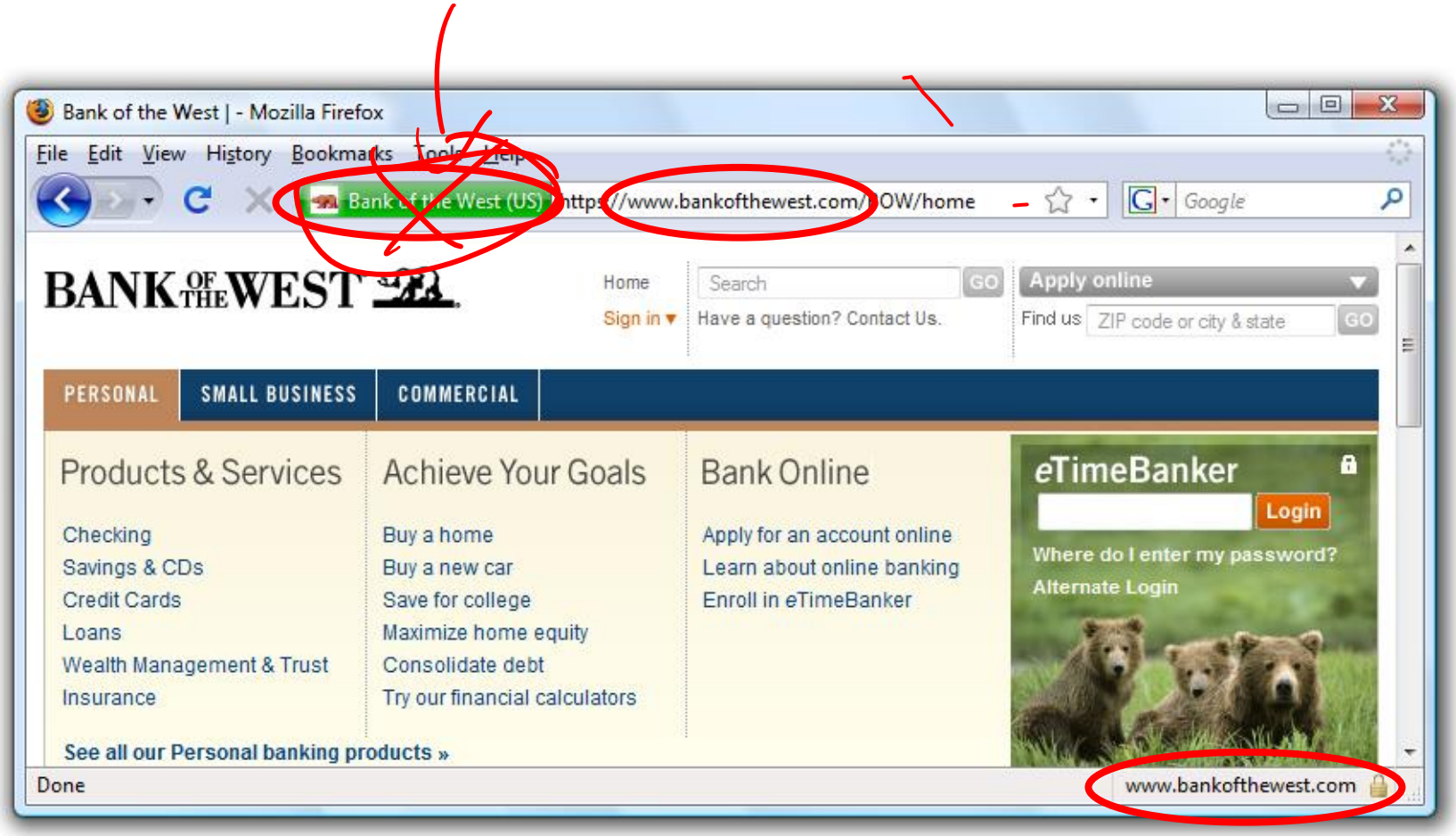
Case Study #2: Phishing

- **Design question:** How do you help users avoid falling for phishing sites?

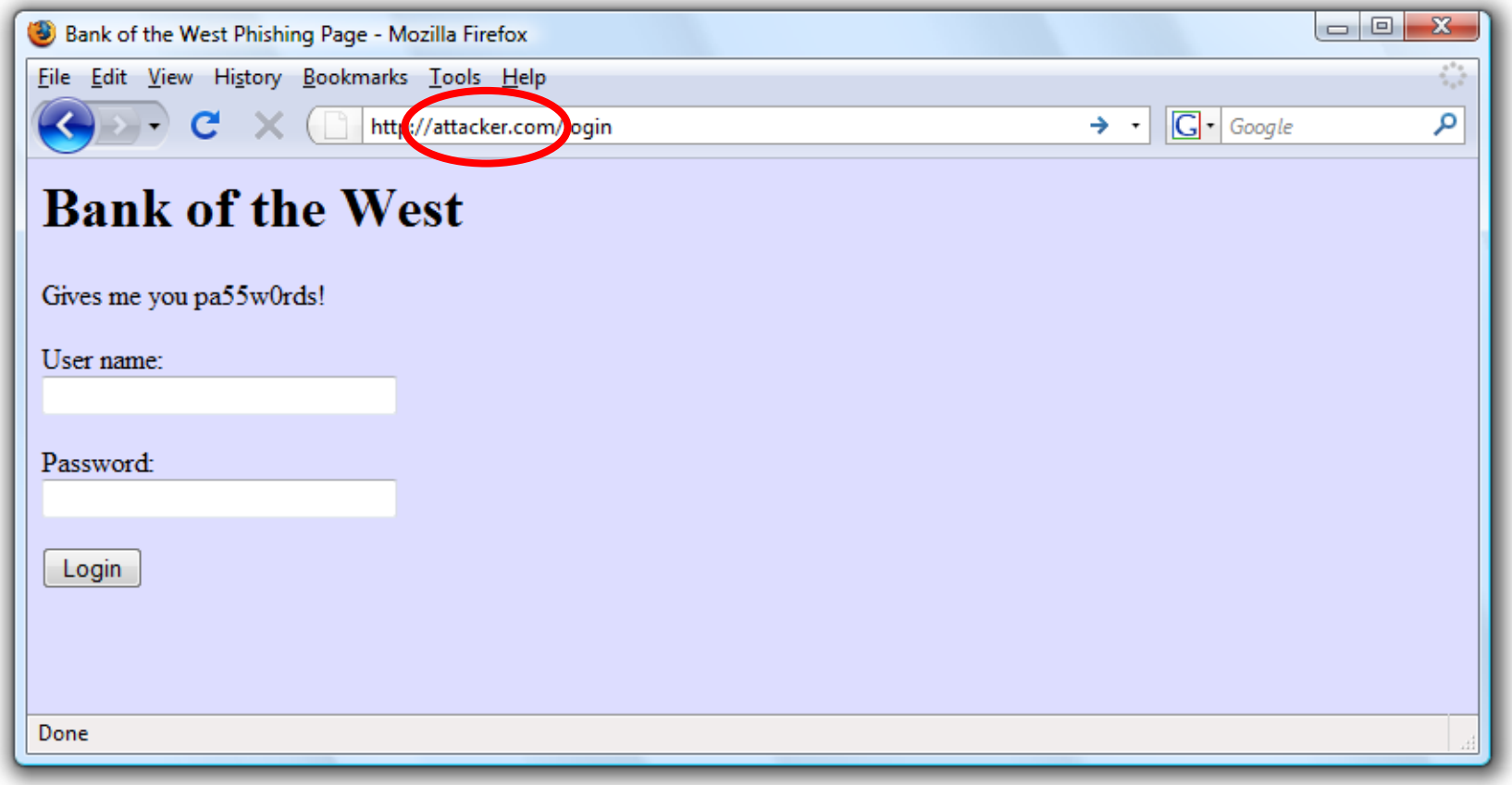
A Typical Phishing Page



Safe to Type Your Password?

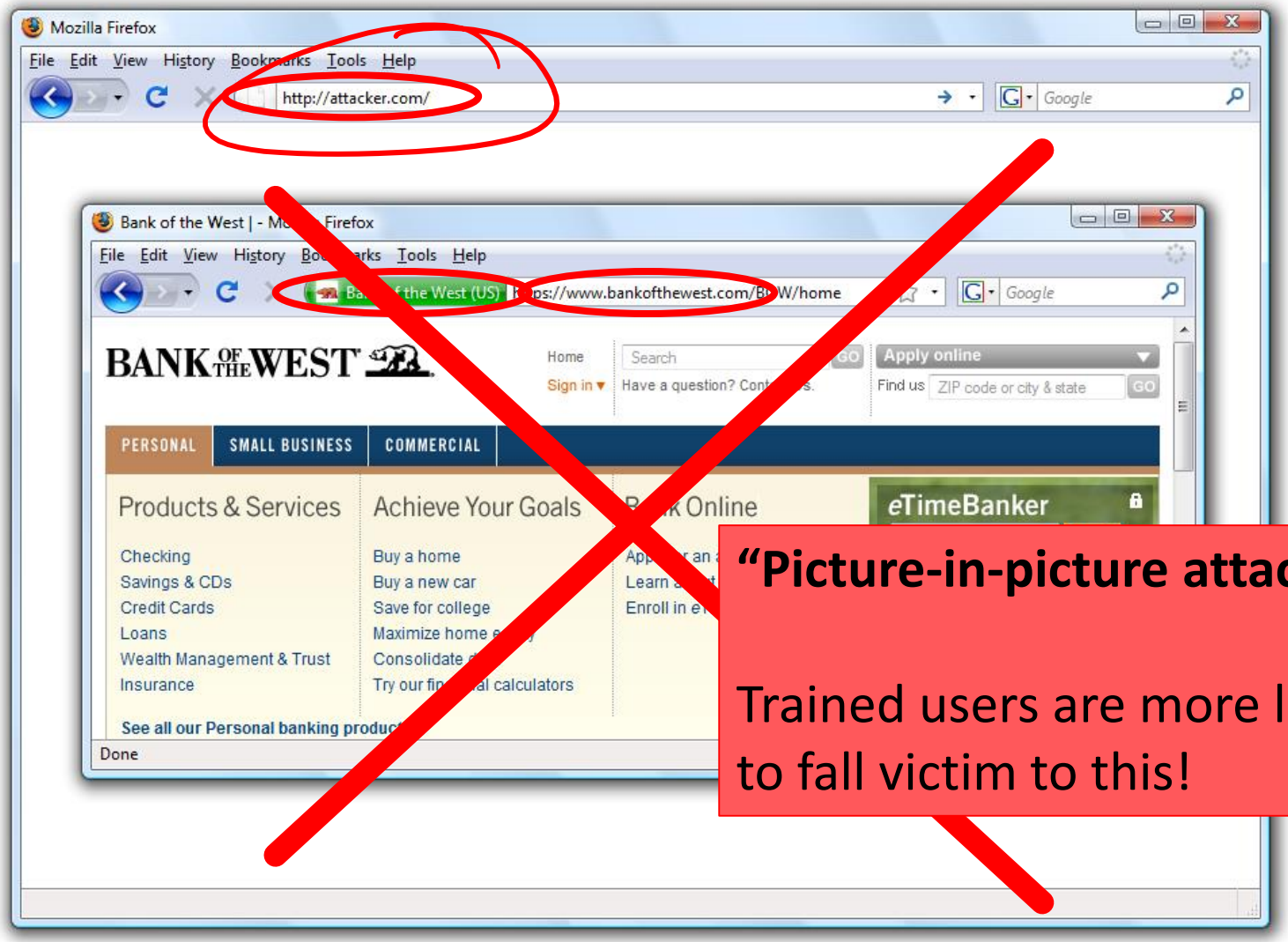


Safe to Type Your Password?



Safe to Type Your Password?

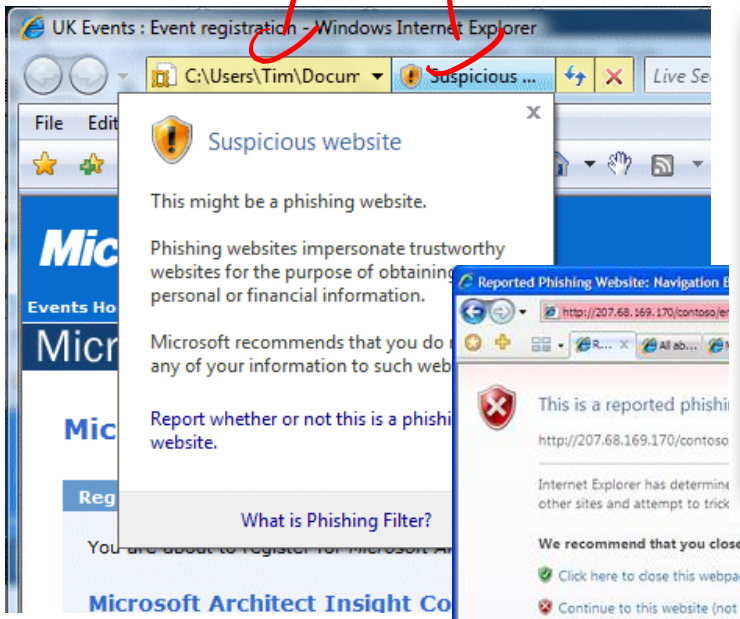
Safe to Type Your Password?



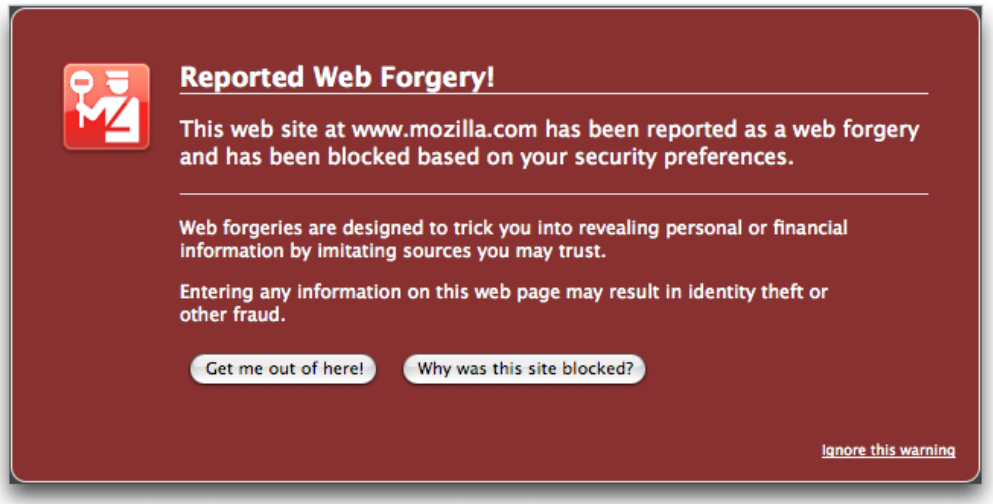
"Picture-in-picture attacks"

Trained users are more likely to fall victim to this!

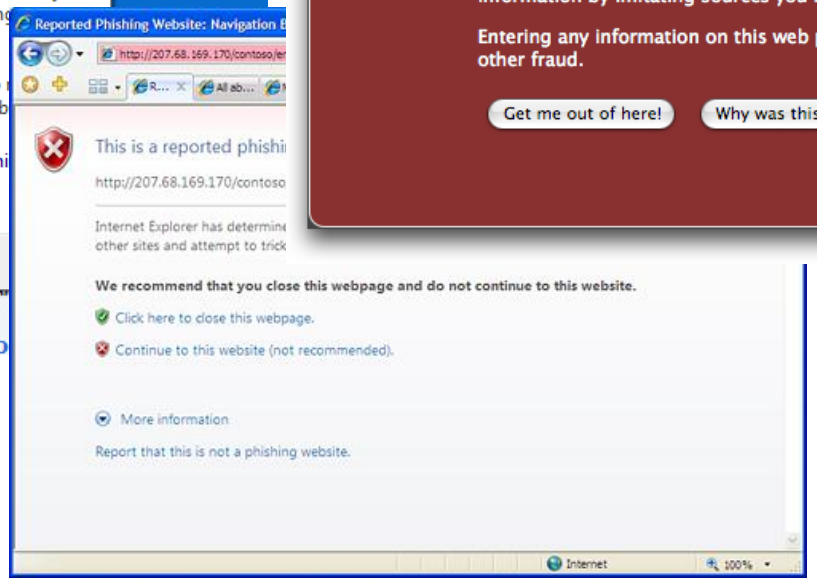
Phishing Warnings (2008)



Passive (IE)



Active (Firefox)

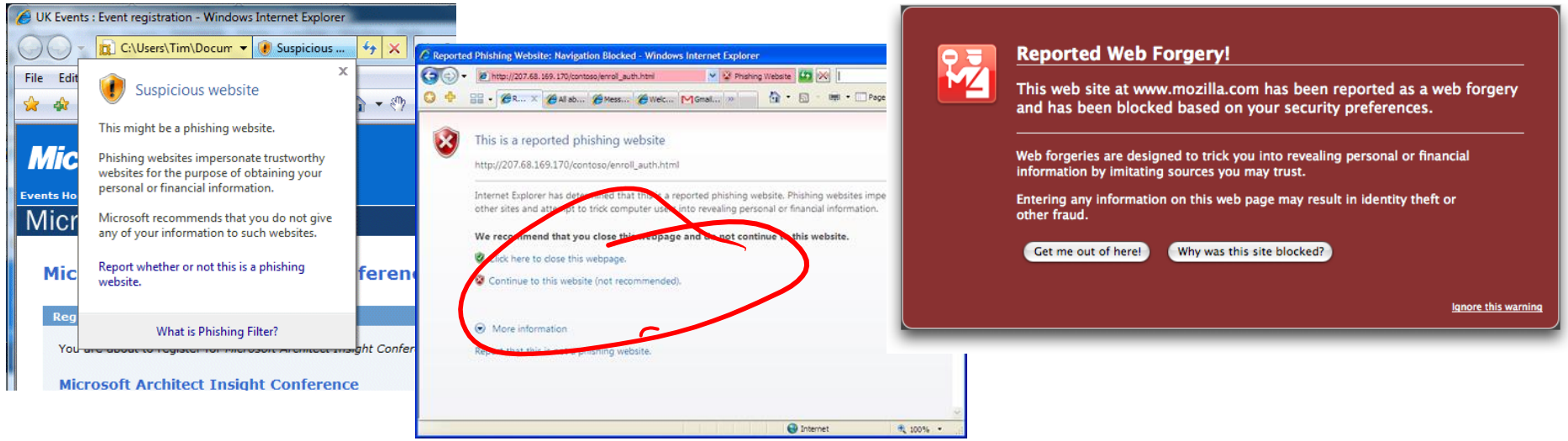


Active (IE)

[Egelman et al.]

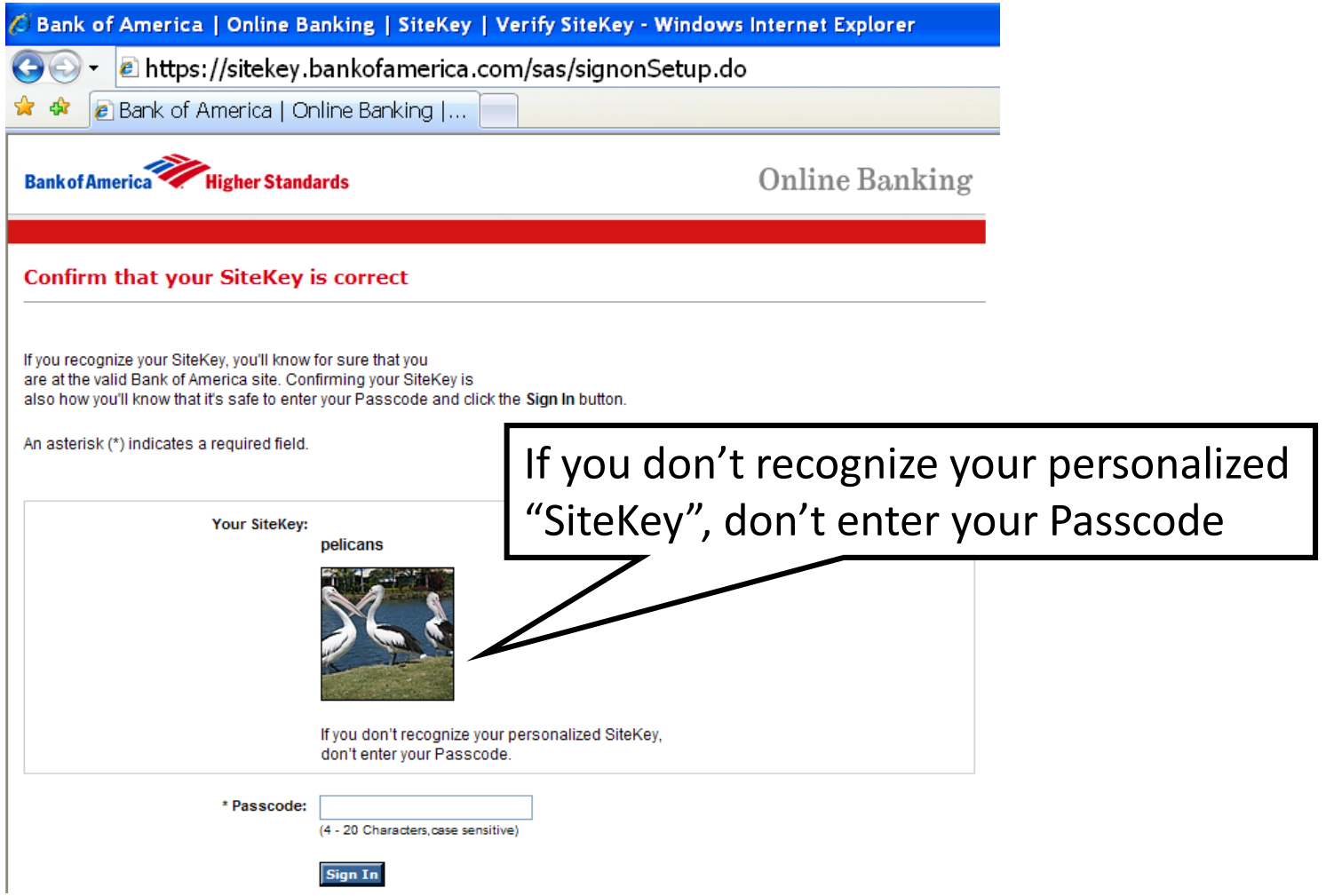
Active vs. Passive Warnings

- Active warnings significantly more effective
  - Passive (IE): 100% clicked, 90% phished
  - Active (IE): 95% clicked, 45% phished
  - Active (Firefox): 100% clicked, 0% phished



Passive (IE) Active (IE) Active (Firefox)

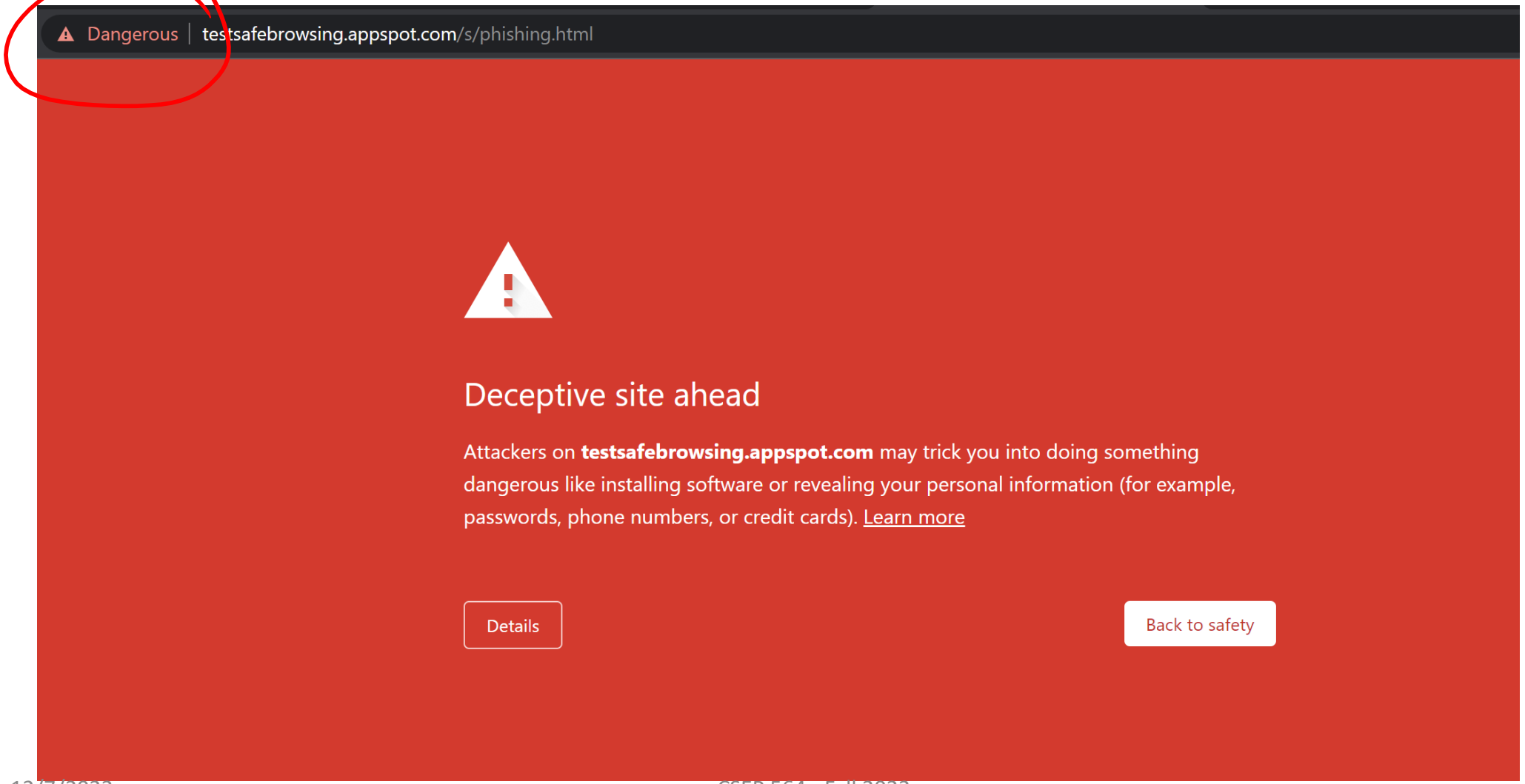
FYI: Site Authentication Image

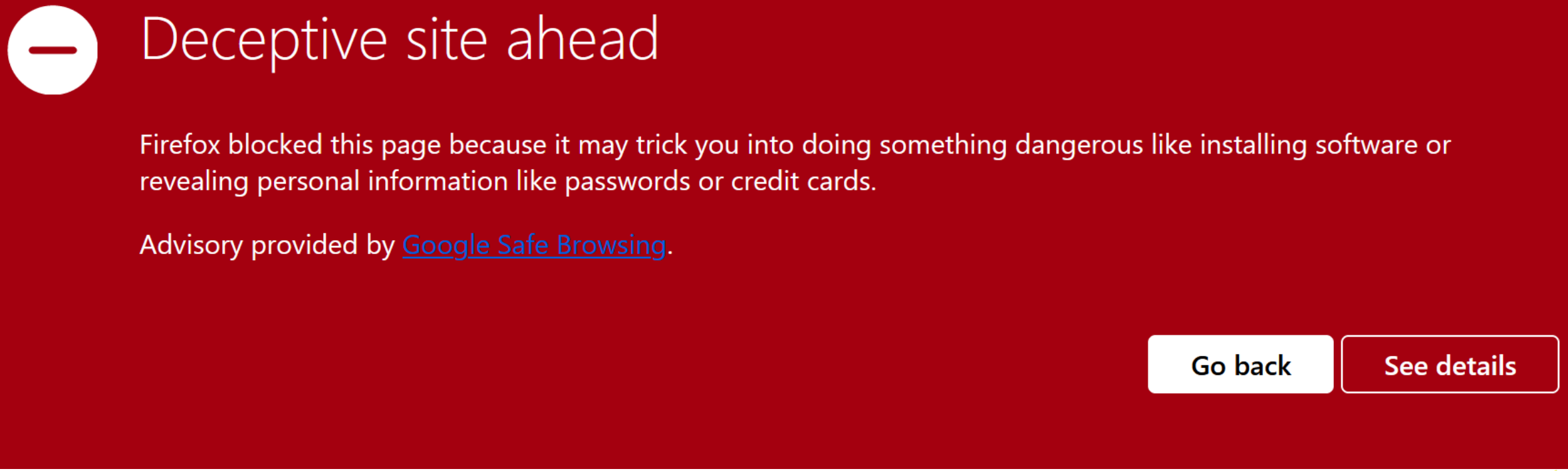


Modern anti-phishing

- Largely driven by Google Safe Browsing
  - Browser sends 32-bit prefix of hash(url)
  - API says: good or bad

Modern warnings



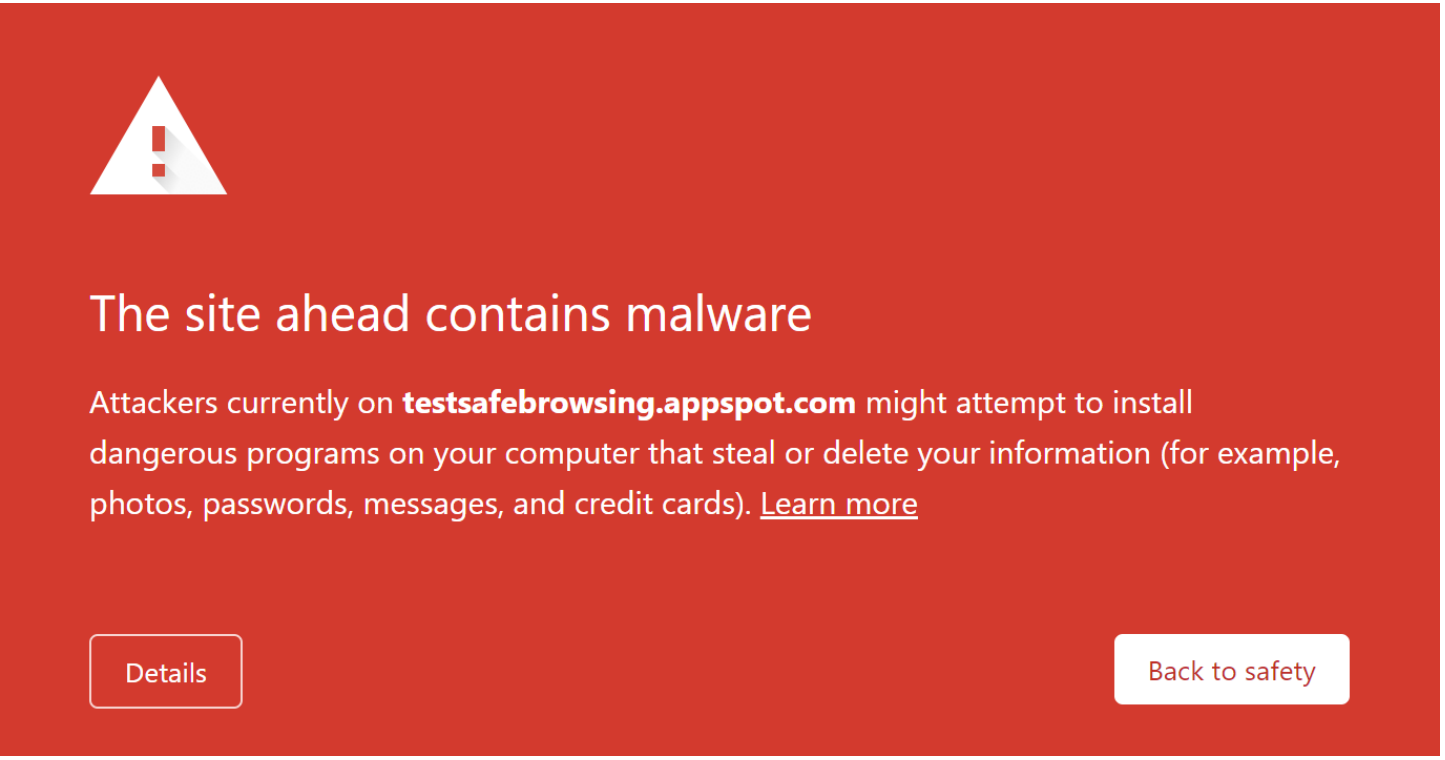

Deceptive site ahead
Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.
Advisory provided by Google Safe Browsing.
Go back
See details

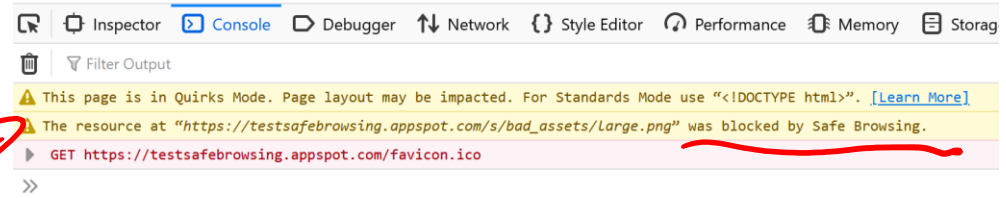
The page ahead may try to charge you money

These charges could be one-time or recurring and may not be obvious.

Proceed

Go back


The site ahead contains malware
Attackers currently on **testsafebrowsing.appspot.com** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards). Learn more
Details
Back to safety

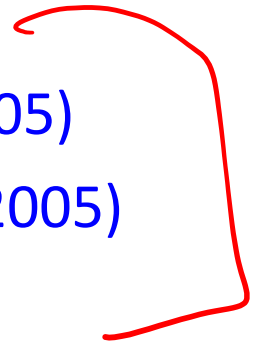

Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storag
Filter Output
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use "<!DOCTYPE html>". [Learn More]
The resource at "https://testsafebrowsing.appspot.com/s/bad_assets/Large.png" was blocked by Safe Browsing.
GET https://testsafebrowsing.appspot.com/favicon.ico

Which warning is ‘better’?

- For user security?
- For user agency?
- For user understanding?
- For… what?

Case Study #3: Password Managers

- Password managers handle creating and “remembering” strong passwords
- Potentially:
  - **Easier** for users
  - More **secure**
- Early examples:
  - PwdHash (Usenix Security 2005)
  - Password Multiplier (WWW 2005)



PwdHash

@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

Password Multiplier

Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

Both solutions target simplicity and transparency.

[Chiasson, van Oorschot, Biddle]

Usability Testing

- Are these programs usable? If not, what are the problems?
- Approaches for evaluating usability:
  - Usability inspection (no users)
    - Cognitive walkthroughs
    - Heuristic evaluation
  - User study
    - Controlled experiments
    - Real usage

[Chiasson, van Oorschot, Biddle]

Task Completion Results

	Success	Potentially Causing Security Exposures			
		Dangerous Success	Failures		
			Failure	False Completion	Failed due to Previous
PwdHash					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	42%	35%	11%	11%	N/A
Remote Login	27%	42%	31%	0%	N/A
Update Pwd	19%	65%	8%	8%	N/A
Second Login	52%	28%	4%	0%	16%
Password Multiplier					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	16%	32%	28%	20%	N/A
Remote Login	N/A	N/A	N/A	N/A	N/A
Update Pwd	16%	4%	44%	28%	N/A
Second Login	16%	4%	16%	0%	16%

[Chiasson, van Oorschot, Biddle]

Problem: Mental Model

- Users seemed to have misaligned mental models
  - Not understand that one needs to put "@@" before *each* password to be protected.
  - Think different passwords generated for each session.
  - Think successful when were not.
  - Not know to click in field before Alt-P.
  - Don't understand what's happening: "Really, I don't see how my password is safer because of two @'s in front"

[Chiasson, van Oorschot, Biddle]

Problem: Transparency

- Unclear to users whether actions successful or not.
  - Should be obvious when plugin activated.
  - Should be obvious when password protected.
- Users feel that they should be able to know their own password.

[Chiasson, van Oorschot, Biddle]

Problem: Dangerous Errors

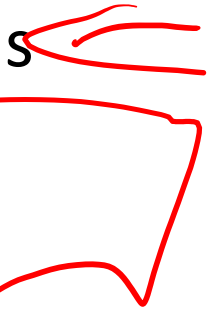
- Tendency to try all passwords
  - A poor security choice – phishing site could collect many passwords!
  - May make the use of PwdHash or Password Multiplier *worse* than not using any password manager.
- Usability problem leads to security vulnerabilities.
  - Theme in course: sometimes things designed to increase security can also increase other risks

Stepping Back: Root Causes?

- Computer systems are complex; users lack intuition
- Users in charge of managing own devices
  - Unlike other complex systems, like healthcare or cars.
- Hard to gauge risks
  - “It won’t happen to me!”
- Annoying, awkward, difficult
- Social issues
  - Send encrypted emails about lunch?...

How to Improve?

- Security education and training
- Help users build accurate mental models
- Make security invisible
- Make security the least-resistance path
- …?



Beyond Specific Tools: Different User Groups

- Not all users are the same!

- Designing for one group of users, or “generic” users, may leads to dangerous failures or reasons that people will not use security tools

- Examples from (qualitative) research at UW:
  - Journalists (most sources are not security educated!)
  - Refugees in US (security measures may embed US cultural assumptions!)

Security Research

Its an odd field to work in!

- Covers everything:
  - How different groups of people use their smartphones
  - The effectiveness of airport bodyscanners at detecting firearms
  - Electromagnetic emanations from electronics
  - XSS on webpages
  - The spread of misinformation online
  - Adversarial attacks on computer vision

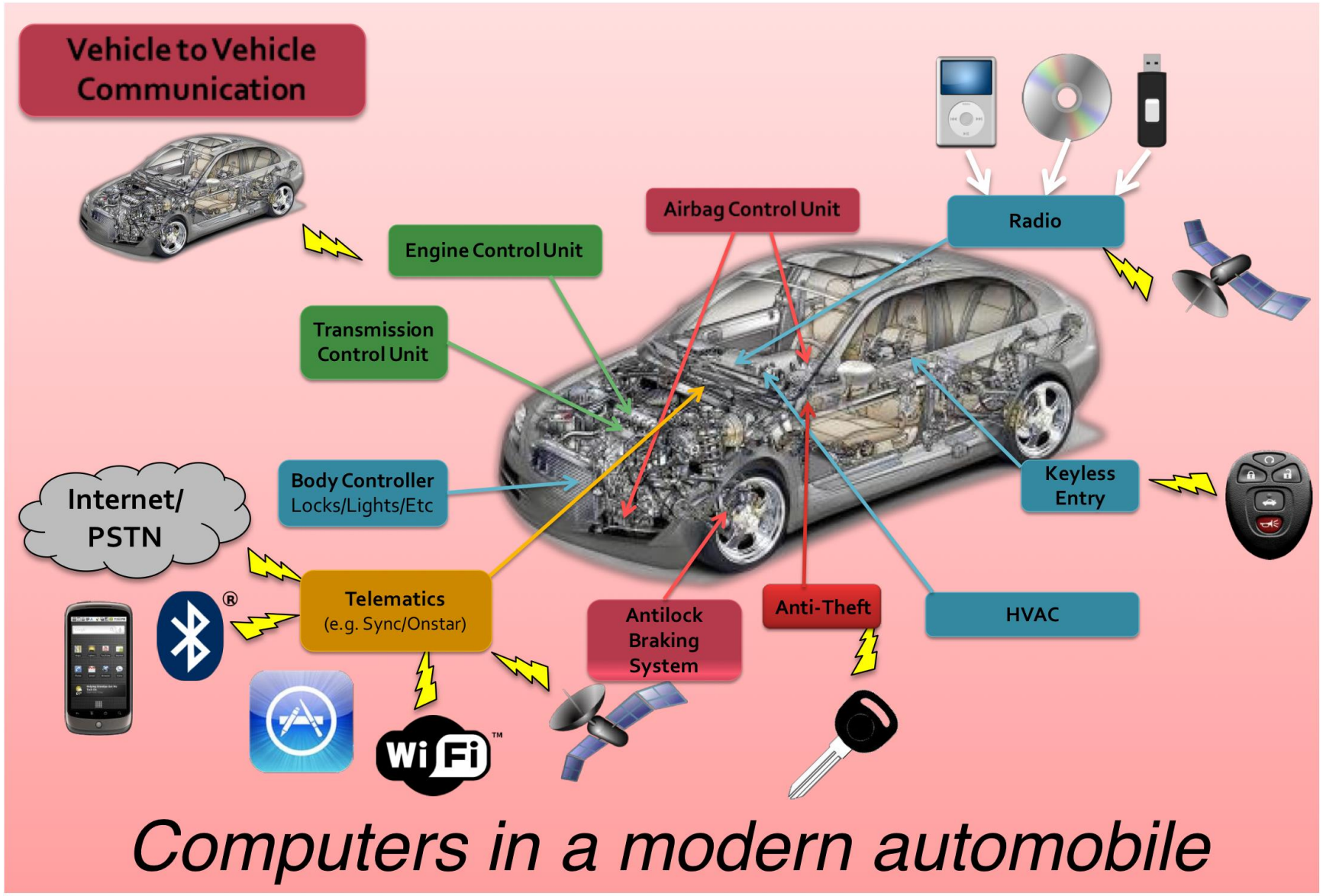
Security and Privacy For Emerging Technologies

(1) Connected Automobiles

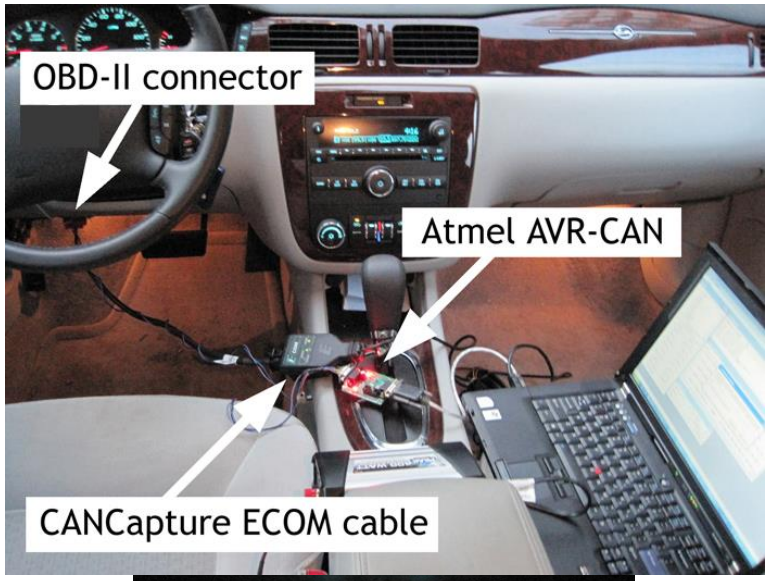
- Already emerged by now, but a fun story ☺

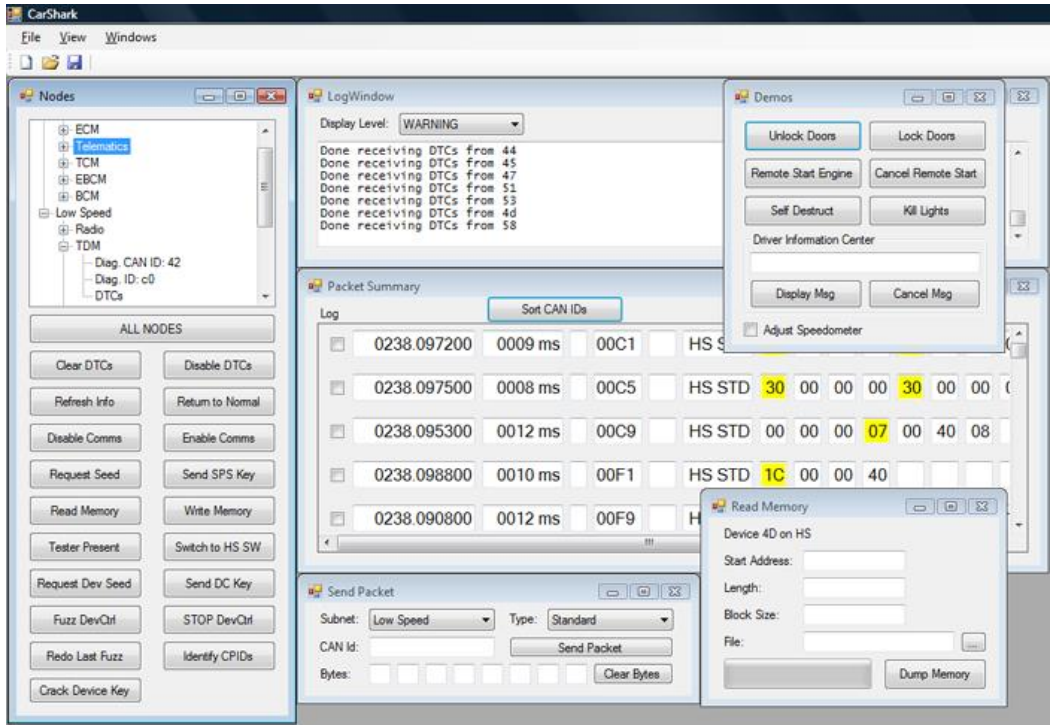
- Automobiles were only just being connected to the internet when UW+UCSD studied them (~2009)
  - Had not faced significant adversarial pressure
  - Won a "Test of Time" Award recently

www.autosec.org

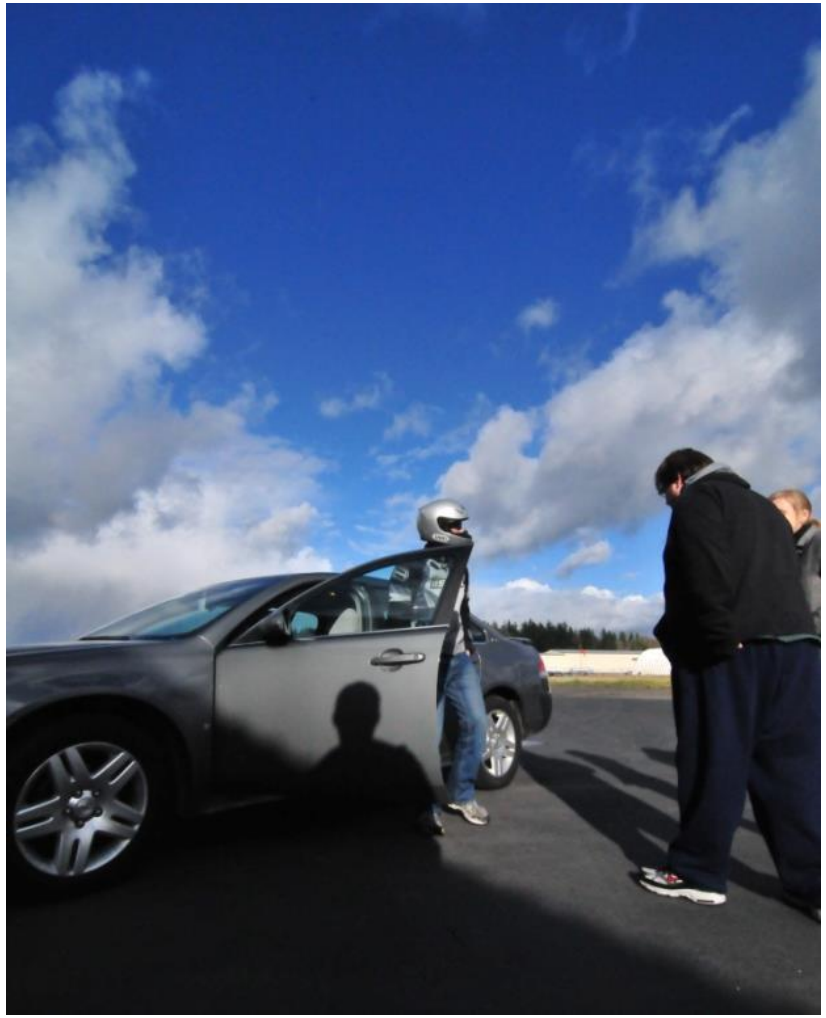

Vehicle to Vehicle Communication
Engine Control Unit
Airbag Control Unit
Radio
Transmission Control Unit
Body Controller Locks/Lights/Etc
Keyless Entry
Internet/ PSTN
Telematics (e.g. Sync/Onstar)
Antilock Braking System
Anti-Theft
HVAC
Wi Fi
Computers in a modern automobile

Experiments with a Real Car





Experiments with a Real Car



Example: Force Brakes On/Off

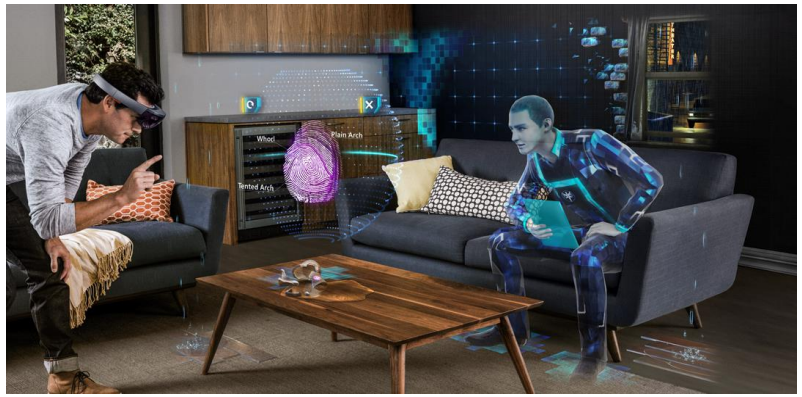
https://www.youtube.com/watch?v=H6o0zuid1K4

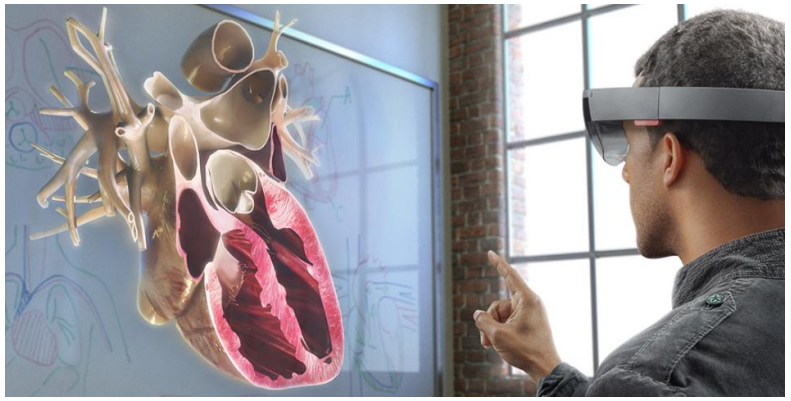
https://www.youtube.com/watch?v=917VOx6tBKA

Impacts

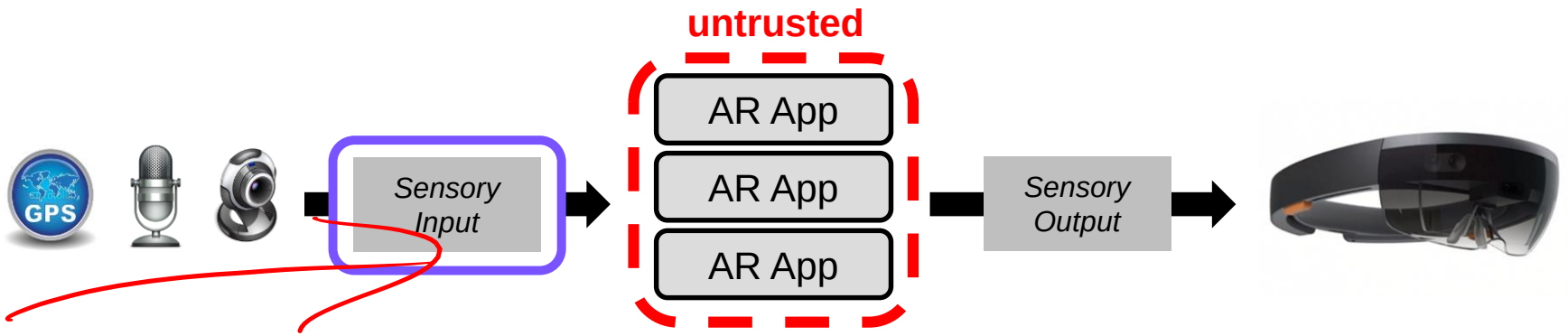
- Impact on automotive industry
  - Significant investment by automotive companies
  - Spurred vendor industry around automotive security
- Impact on standards, regulation, and legislation
  - SAE International (de facto standards body for the U.S. automotive industry) created committee and standards
  - Resources committed by NHTSA
  - U.S. bills on automotive cybersecurity
- Impact on research
  - New subfield of automotive security and significant DARPA and other funding efforts

(2) Security and Privacy for Augmented Reality





AR Input Privacy

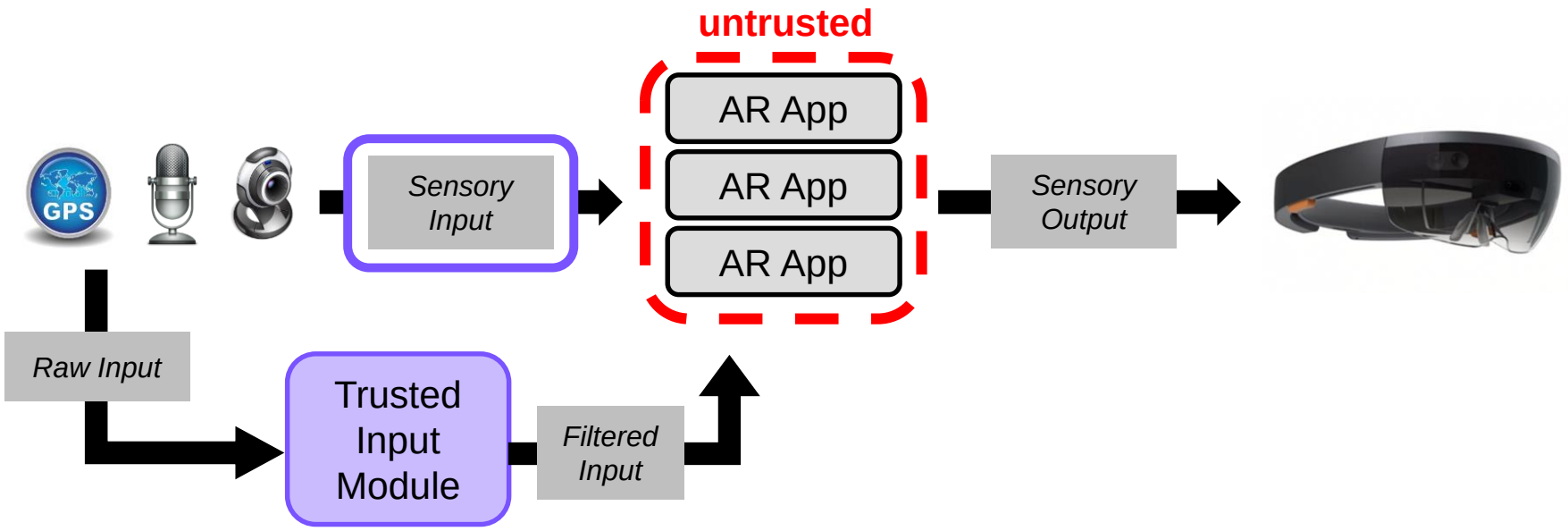


Seattle dive bar becomes first to ban Google Glasses over privacy fears

By NINA GOLGOWSKI

PUBLISHED: 00:43 EST, 10 March 2013 | **UPDATED:** 02:16 EST, 10 March 2013

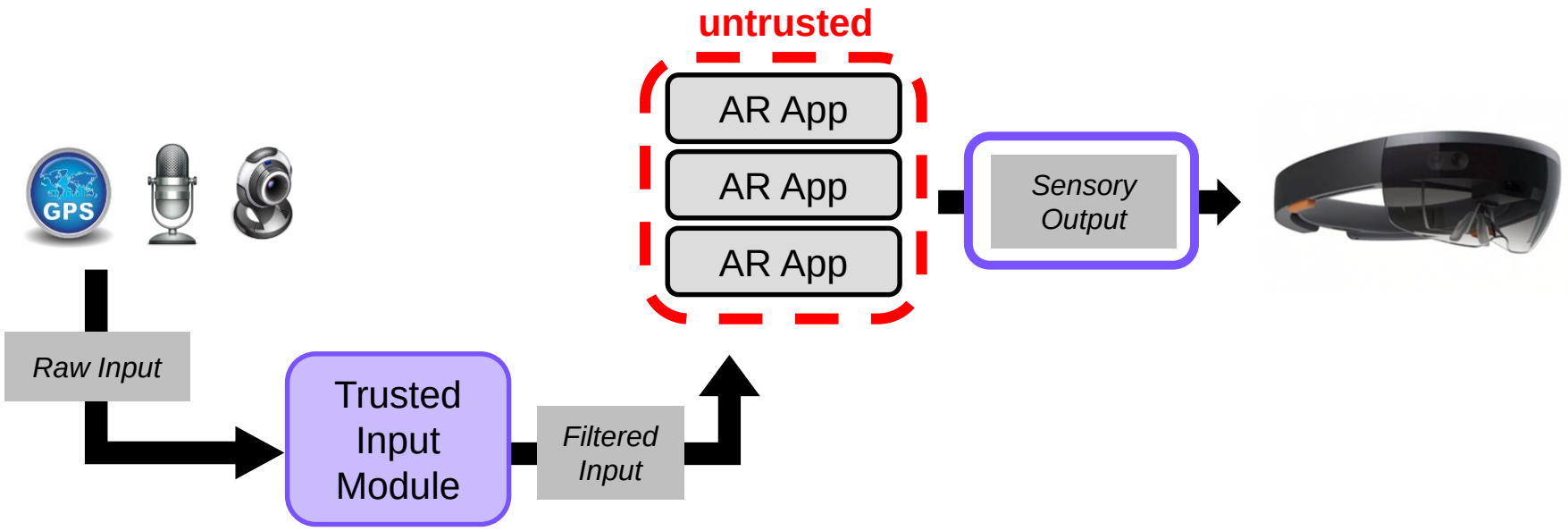
AR Input Privacy



Input Privacy

- Jana et al., USENIX Security ’13
- **Roesner et al., CCS ’14**
- Templeman et al., NDSS ’14
- Raval et al., MobiSys ’16

AR Output Security



Hyper Reality (https://www.youtube.com/watch?v=YJg02ivYzSs)

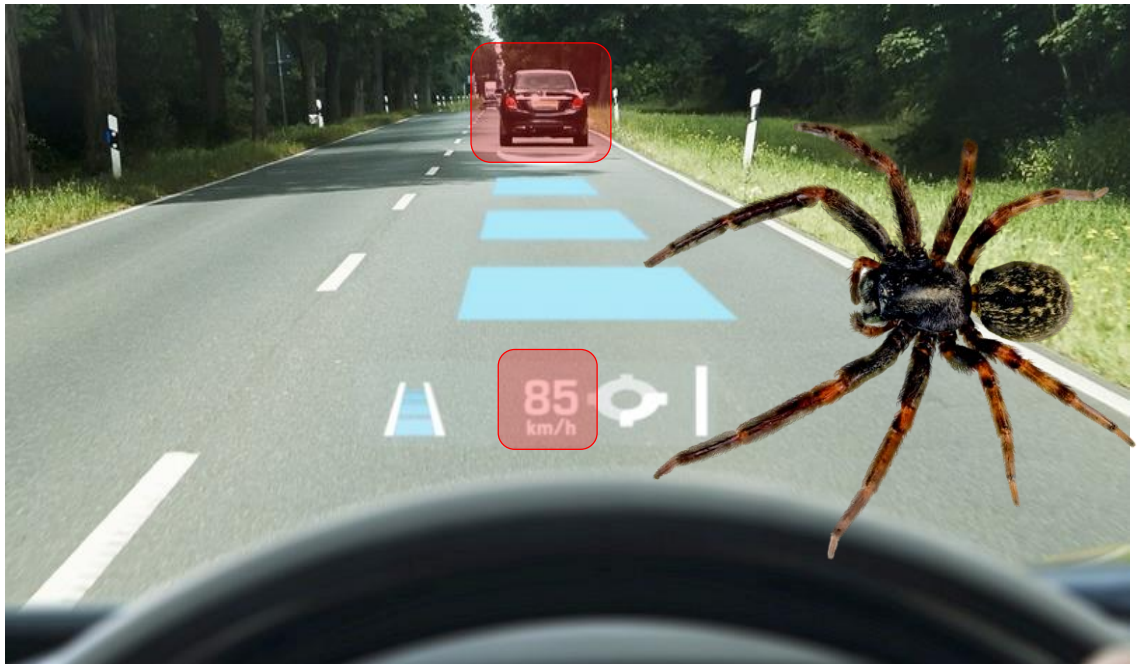
AR Output Security

A buggy or malicious app might…

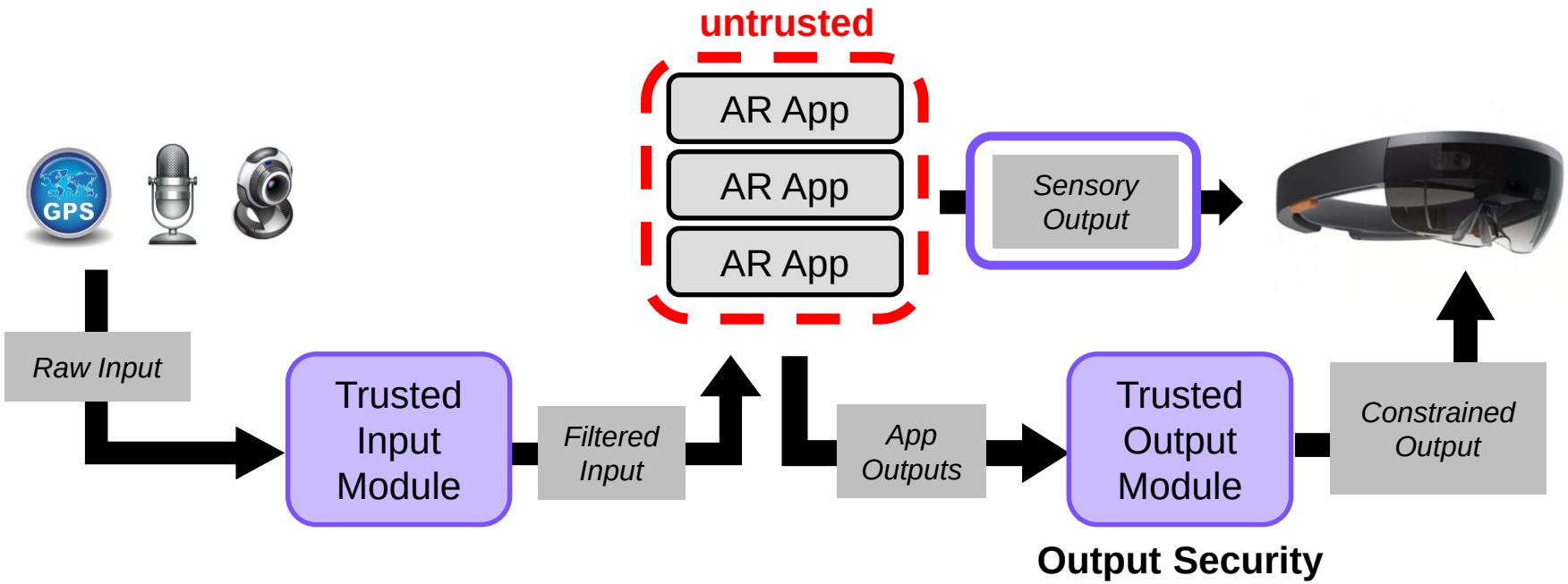
Obscure another app's virtual content to hide or modify its meaning

Obscure important real-world content, such as traffic signs or cars

Disrupt the user physiologically, such as by startling them



AR Output Security



Output Security

- **Lebeck et al., HotMobile '16**
- **Lebeck et al., IEEE S&P '17**
- **Lebeck et al., HotMobile '19**

Many Other Questions

- How to handle multiple apps augmenting reality at the same time?
  - **Lebeck et al., HotMobile '19**
- How to handle interactions between multiple users who may see different realities?
  - **Ruth et al., USENIX Security '19**

https://ar-sec.cs.washington.edu

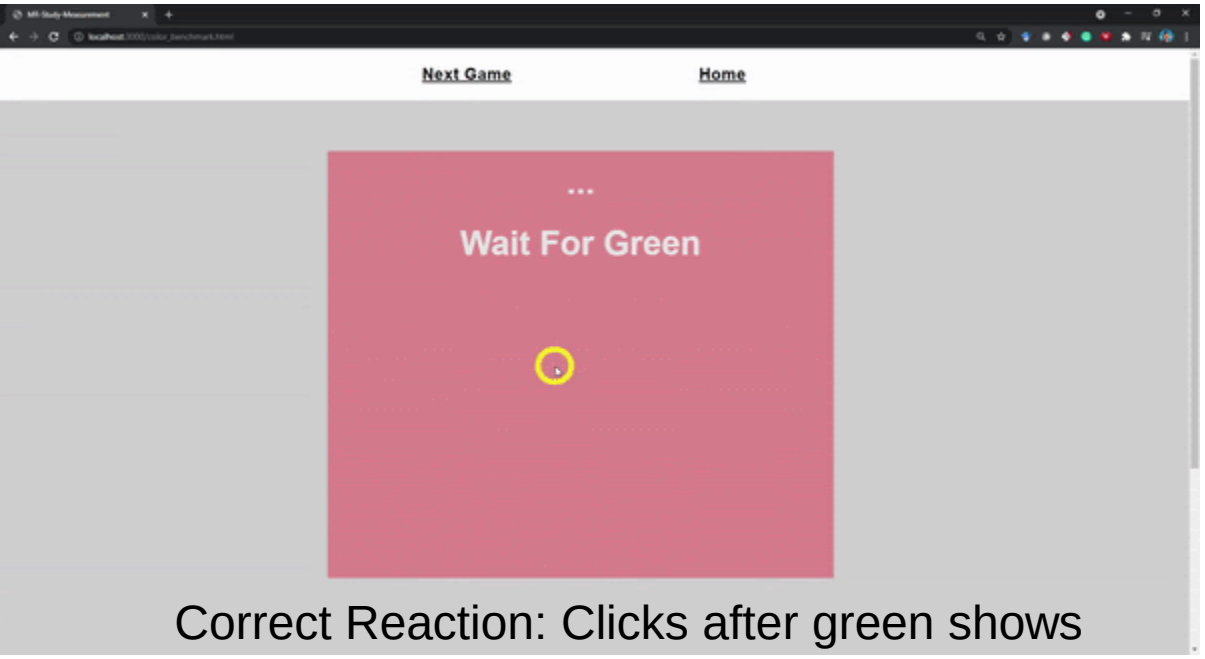
Recent developments in MR Security:

Researchers presented the microbenchmarks **(real-world stimuli)** on a computer monitor.

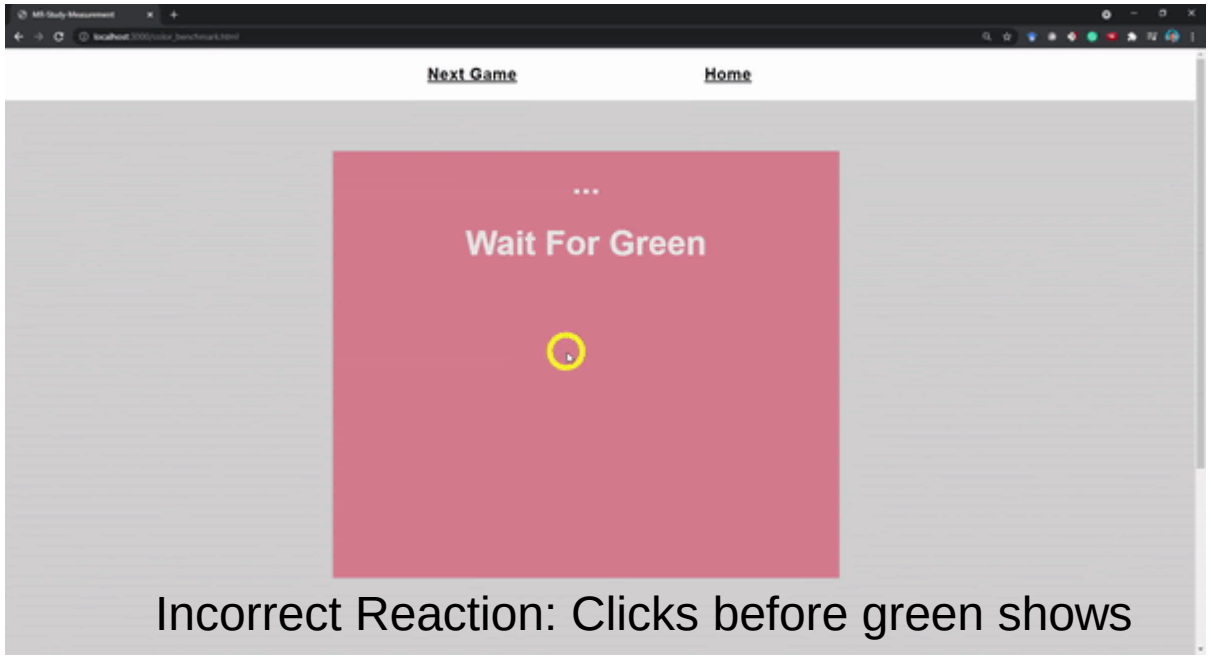
To allow for safe & controllable experiments where things were the same between all participants

Slides from Kaiming Chen (UW S&P Lab)

Reaction Time Task & MR Attacks



Correct Reaction: Clicks after green shows



Incorrect Reaction: Clicks before green shows

Goals for MR Attack:

Delay a correct reaction significantly or *induce an incorrect reaction*

Slides from Kaiming Chen (UW S&P Lab)

Key Lessons

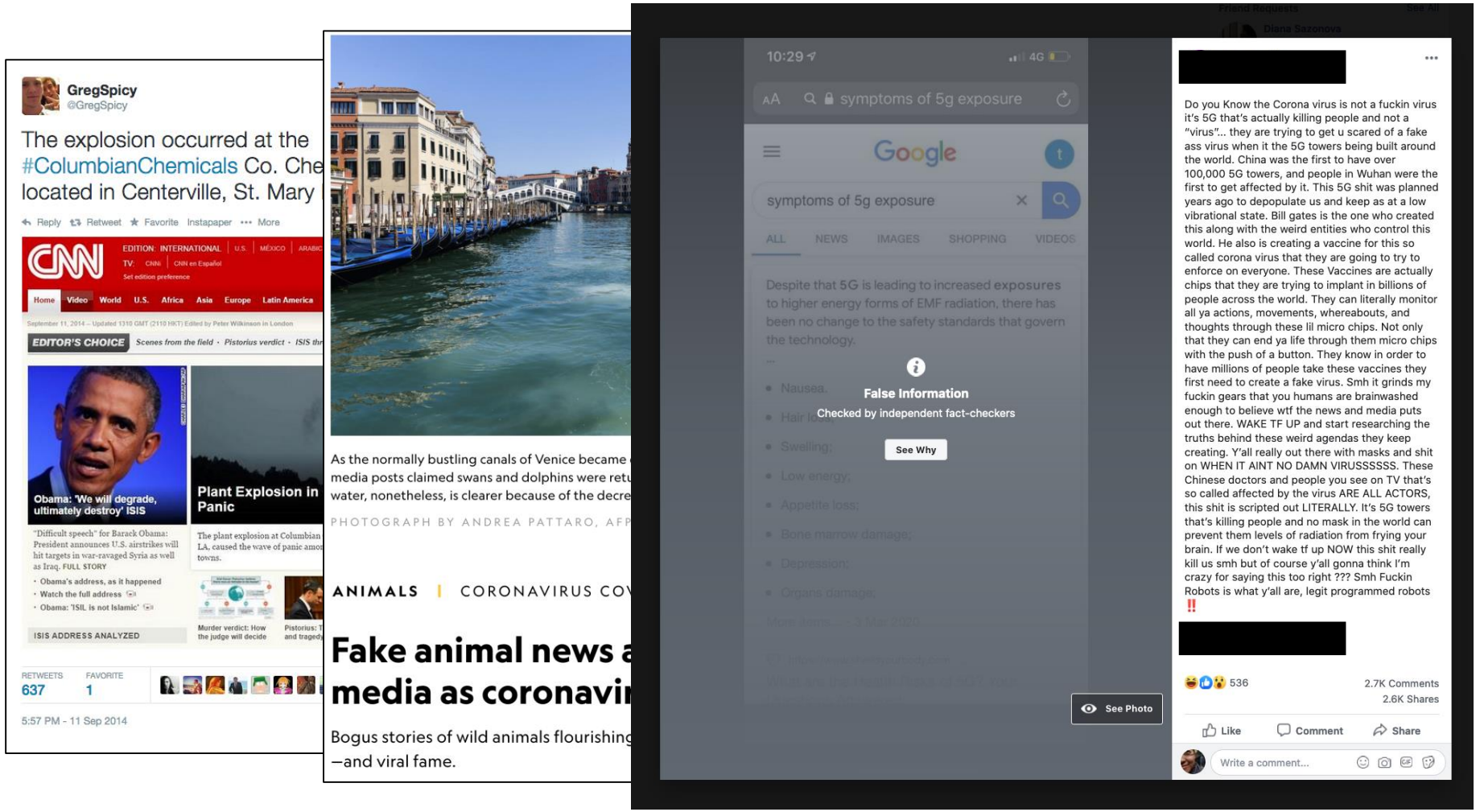
1. MR output attacks **can** have significant impacts on users.

2. In addition to **direct impacts** from attacks (e.g., inducing incorrect reactions on a task), we also documented **secondary impacts** from attacks that manifested on subsequent tasks.

3. **Dynamic**: Examples of participants' defensive strategies succeeding or backfiring

Slides from Kaiming Chen (UW S&P Lab)

(3) Technology-Enabled Disinformation



Serious Potential Consequences

Facebook uncovers disinformation campaign to influence US midterms

Social network removes 32 pages and accounts for 'co-ordinated inauthentic behaviour'

Hannah Kuchler in San Francisco and **Demetri Sevastopulo** in Washington JULY 31, 2018

How WhatsApp Destroyed A Village

In July, residents of a rural Indian town saw rumors of child kidnappers on WhatsApp. Then they beat five strangers to death.

Pranav Dixit
BuzzFeed News Reporter

Ryan Mac
BuzzFeed News Reporter

Reporting From
New Delhi

Posted on September 9, 2018, at 9:00 p.m. ET

Many Types of “False News”

	Satire	False Connection	Misleading Content	False Context	Imposter Content	Manipulated Content	Fabricated Content
Poor journalism		✔	✔	✔			
To Parody	✔				✔		✔
To Provoke or to ‘punk’					✔	✔	✔
Passion				✔			
Partisanship			✔	✔			
Profit		✔			✔		✔
Political Influence			✔	✔		✔	✔
Propaganda			✔	✔	✔	✔	✔

From Claire Wardle, https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79

What's New?

The Technology, Not the Incentives

- How content is created
  - Scale and democratization
  - Automated fake content creation
    - Video: https://grail.cs.washington.edu/projects/AudioToObama/
    - Text: https://rowanzellers.com/grover/
- How content is disseminated
  - Scale and democratization
  - Tracking and targeting
  - Algorithmic curation
  - Anonymity and bots
  - Immediate reach and feedback
- How content is consumed
  - Attention economy
  - Filter bubbles

Not Just a Technical Problem: Human Cognitive Vulnerabilities

8:42

(e.g., confirmation bias, backfire effect)

Exceptional Access

Last section, run different:

- Repeated use of short discussion, ~~no in-class assignment~~
- There aren't given answers
- Pollev will be used to remind what the question is
  - You can type interesting answers in, but aren't required to, since they are tied to your name

A brief aside, useful for consideration

- DES S-boxes
- Dual_EC_DRBG

History: Dual-use

- Technologies under restriction regimes may be *dual-use*
- A missile is *not* dual-use
  - Hunting firearms *are* dual-use
- That is, military and civilian applications

Discuss

History: Cryptography

- Post WWII all cryptography was a ‘munition’
  - Subject to export restrictions
  - Fundamentally a military technology
- This was (mostly) reasonable
- It stopped being (as) reasonable once electronic communications became a thing
  - Really clearly dual-use at this point

History: The crypto wars (1st)

- Cold war ends in 1991
- Some export restrictions are lifted in 1992
  - <40bits of key systems allowed
  - 40 bits is crackable in days at the time
- PGP (Pretty Good Privacy) written in 1992
  - >>>40 bits
- "Crypto wars" kick off as a reaction to restrictions

History: SSL in the 90s

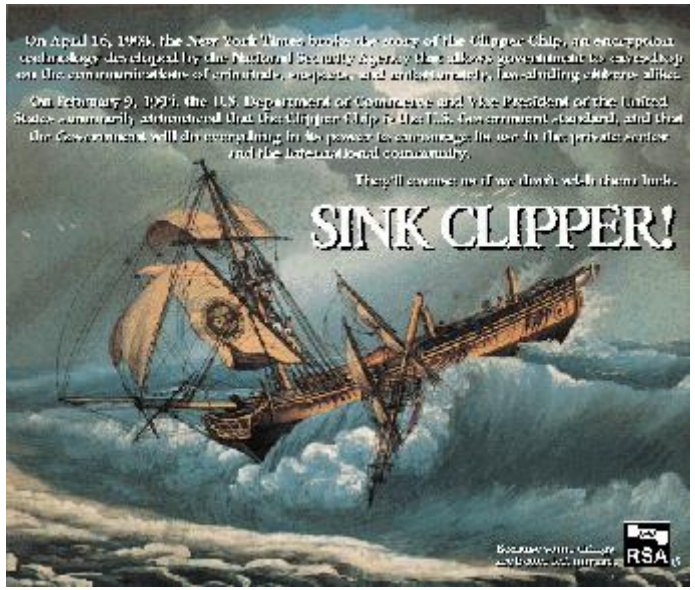
- Netscape had SSL (HTTPS) for e-commerce
- Problem: SSL was 128bits of key
- Solution: Two versions of the browser
  - US Version: 128bits
  - International Version: 40bits (reveals 88bits)

History: The Clipper Chip

- 1994 a new system is proposed: Skipjack
- 80-bits of security
- “Trap-door” built in to allow government recovery of messages
  - This was public
- Proposal was to put the “clipper chip” into everything

History: The Clipper Chip

- Argument was that ‘terrorists’ would be caught
- This was… not well received
- It also had a number of serious technical flaws
- It died reasonably fast



By Source (WP:NFCC#4), Fair use, https://en.wikipedia.org/w/index.php?curid=48926067

History: Crypto wars end

- In 2000 restrictions are eased
  - (Per 1996 order that made this possible)
- AES is standardized
- Cryptography ‘golden age’ starts

Today: Continuation

- Cryptography is back in the headlines

- It is trivial to have encrypted data
  - Mobile phones
  - Backup systems
  - Messaging platforms

- Governments want access to encrypted data

Good starting points

- Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion - Stefan Savage
  - http://cseweb.ucsd.edu/~savage/papers/lawful.pdf
- The Export of Cryptography in the 20th Century and the 21st - Whitfield Diffie and Susan Landau
  - https://privacyink.org/pdf/export_control.pdf