Usability of TLS/PKI

Mainack Mondal

CS 60081
Autumn 2022

Roadmap

- Trust on the web
  - SSL notifications

SSL/ TLS

- Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS)
  - Enable secure communication

- Frequently encountered with web browsing (HTTPS) and more behind the scenes protocols
  - VOIP, etc

Attacker Model

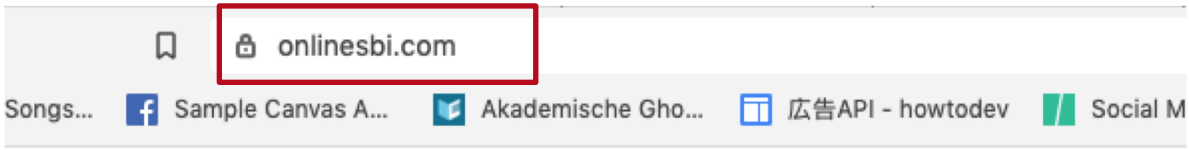
- Passive: People eavesdropping
  - Goal: content of what we are sending
  - Goal: getting session cookies

- Active: Man in the middle attack
  - Goal: intercept all communication
  - Solution: authenticate that we are talking to the right site, not an imposter
  - Solution: Use certificates inside a public-key infrastructure (PKI)

Certificates → Trust

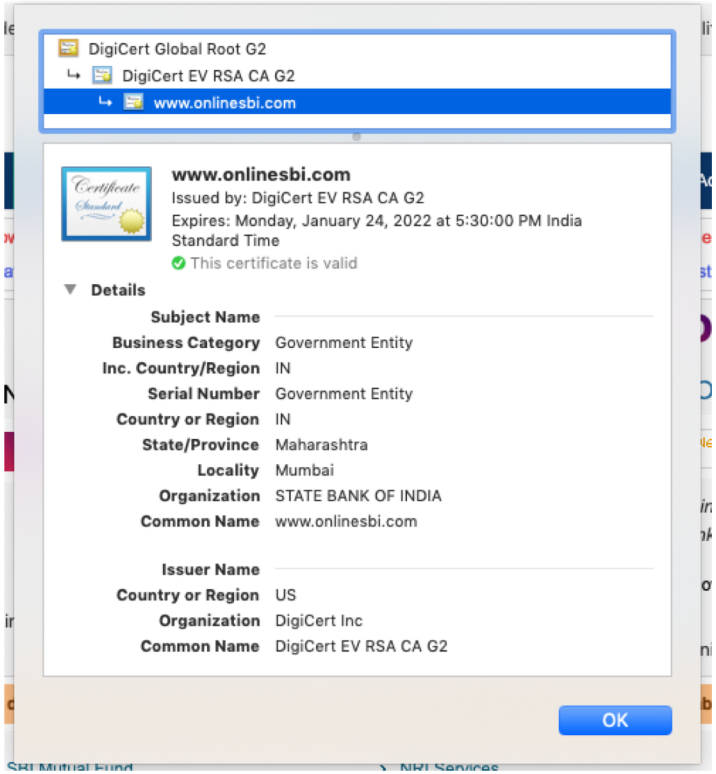
- Public-Key Infrastructure (PKI)
  - Certificates are issued by certificate authorities that bind cryptographic keys to identities
  - In https:
    - Identifies == web site owners (google.com)
    - By Certificate Authority (CA) == GlobalSign
    - Using Certificates: proving authenticity of google.com which is verified by Globabsign

Certificate: point of view of users



SBI

Different for different browsers



Usability: The look of SSL is non-uniform across browsers

Browser	HTTPS	HTTPS minor error	HTTPS major error	HTTP	EV	Malware
Chrome 48 Win	https://ww	https://mix	~~https~~://wro	www.exam	Symantec Co	https://dow
Edge 20 Win	example.	https://mix	wrong.host.bads	example.com	Symantec Co	Unsafe website
Firefox 44 Win	https://www.e	https://mixec	https://expire	www.example	Symantec Corpo	https://spacet
Safari 9 Mac	example.com	mixed.badssl.c	*URL hidden*	example.com	Symantec Cor	downloadgam
Chrome 48 And	https://v	https://mixe	~~https~~://v	www.examp	https://v	https://spac
Opera Mini 14 And	www.exam	mixed.badssl.(	wrong.host.ba	www.example	www.syma	*Unavailable*
UC Mini 10 And	Example D	mixed.bads	*Blocked*	Example D	Endpoint, C	*Blocked*
UC Browser 2 iOS	Example Do.	mixed.bads..	wrong.host..	Example Do.	Endpoint, C.	*Unavailable*
Safari 9 iOS	example.c	mixed.badss	wrong.host	example.com	Symantec	*Unavailable*

Figure 2: Security indicators for major browsers on Windows (Win), Mac, Android (And), and iOS. For categories that trigger warnings (e.g., malware), we include the security indicator state during the warning.

Felt et al., SOUPS 2016, required reading

PKI: Point of view of browser software

- Couple of hundreds of trusted Ca
  - Hardcoded into browsers
  - They issue certificates → Certificate authorities (CAs) sign the certificates binding identities (domain name) to keys
  - These keys are used for proving identity + secure communication

PKI: Point of view of domain owners

- Apply for a certificate to a CA
  - Validation process + payment
  - Give you a certificate file
  - You put that file in your server

Security/Usability issues

- Implementation issues
- Compromised CA
- Man-in-the-middle attacks
  - Downgrade/dumbing-down attacks
  - Addition of “rogue” certificates
- Revocation of certificates
- Timing attacks and other side channels
- Communicating to users the underlying mechanism / issues

Example of implementation issue

- Heartbleed: OpenSSL bug
  - CVE-2014-0160
  - TLS heartbeat extension misses a bounds check and thus lets an attacker “read” memory

Compromised CAs (yes it happens)

- Comodo and Diginotar suffered breaches in 2011 that let attackers issue rogue certificates which the attackers know
- Untrustworthy CAs
  - Compelled certificate creation attacks
  - https://crypto.stanford.edu/cs155old/cs155-spring11/papers/ssl-mitm.pdf
  - “This paper introduces the compelled certificate creation attack, in which government agencies may compel a certificate authority to issue false SSL certificates that can be used by intelligence agencies to covertly intercept and hijack individuals’ secure Web-based communications”

Man-in-the-middle attacks (MITM)

- many corporations perform MITM attacks by adding certificates to users' computers
  - Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections: https://arstechnica.com/?post_type=post&p=615263

- A man in the middle can also tell you a site doesn't support SSL/TLS (downgrade) or any strong ciphers (dumbing down)

Validity of a certificate

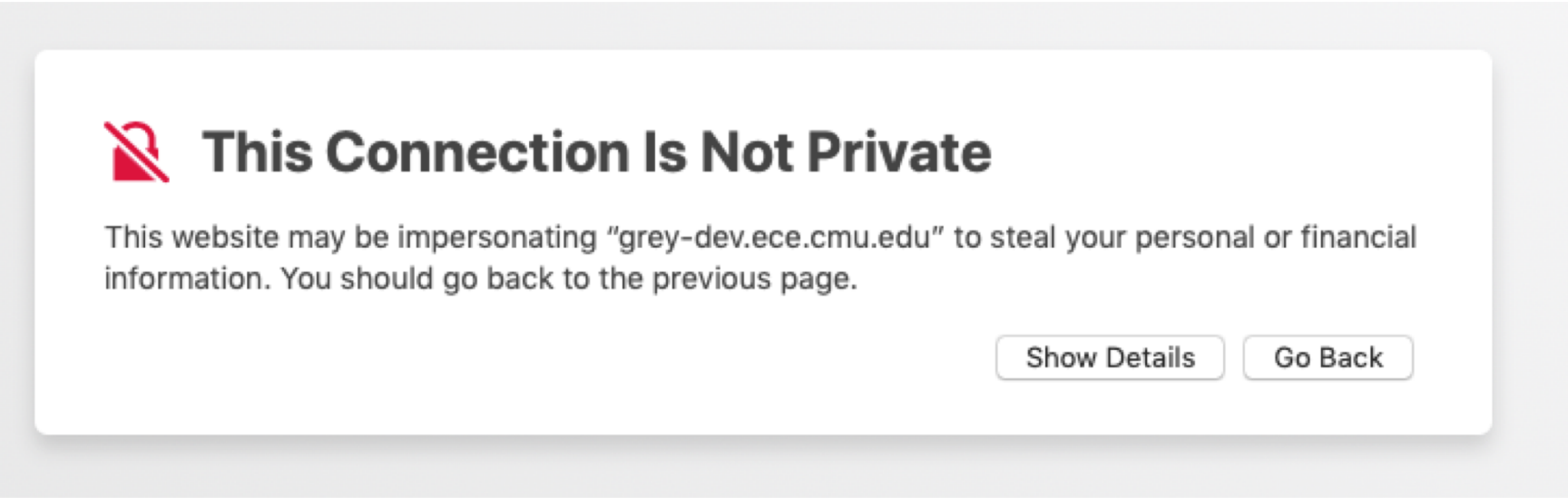
- Certificates can be revoked in case of a compromise
- Certificate Revocation Lists (CRLs) were used, but they got really large – Incremental updates were better
- Online Certificate Status Protocol (OCSP)

Self signed certificates

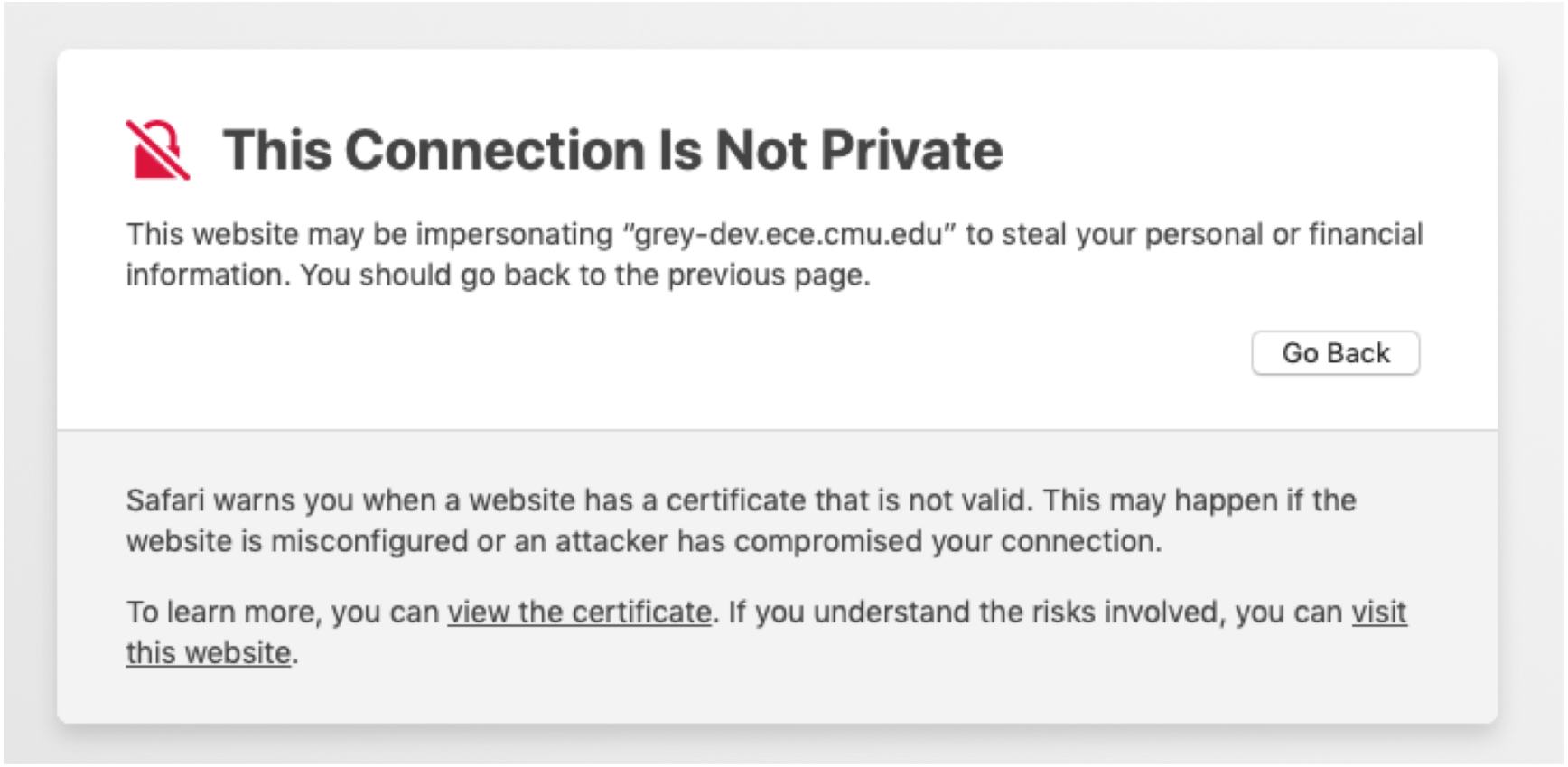
- You can create a certificate yourself
  - A good certificate: CA signs the certificate
  - A bad certificate: you sign it yourself OR use certificate meant for someone else

- Naturally the browser complains
  - You get a warning
  - Example: https://grey-dev.ece.cmu.edu/

Safari


This Connection Is Not Private
This website may be impersonating "grey-dev.ece.cmu.edu" to steal your personal or financial information. You should go back to the previous page.
Show Details
Go Back

Safari


This Connection Is Not Private
This website may be impersonating "grey-dev.ece.cmu.edu" to steal your personal or financial information. You should go back to the previous page.
Go Back
Safari warns you when a website has a certificate that is not valid. This may happen if the website is misconfigured or an attacker has compromised your connection.
To learn more, you can view the certificate. If you understand the risks involved, you can visit this website.

Chrome

Your connection is not private

Attackers might be trying to steal your information from **grey-dev.ece.cmu.edu** (for example, passwords, messages, or credit cards). Learn more

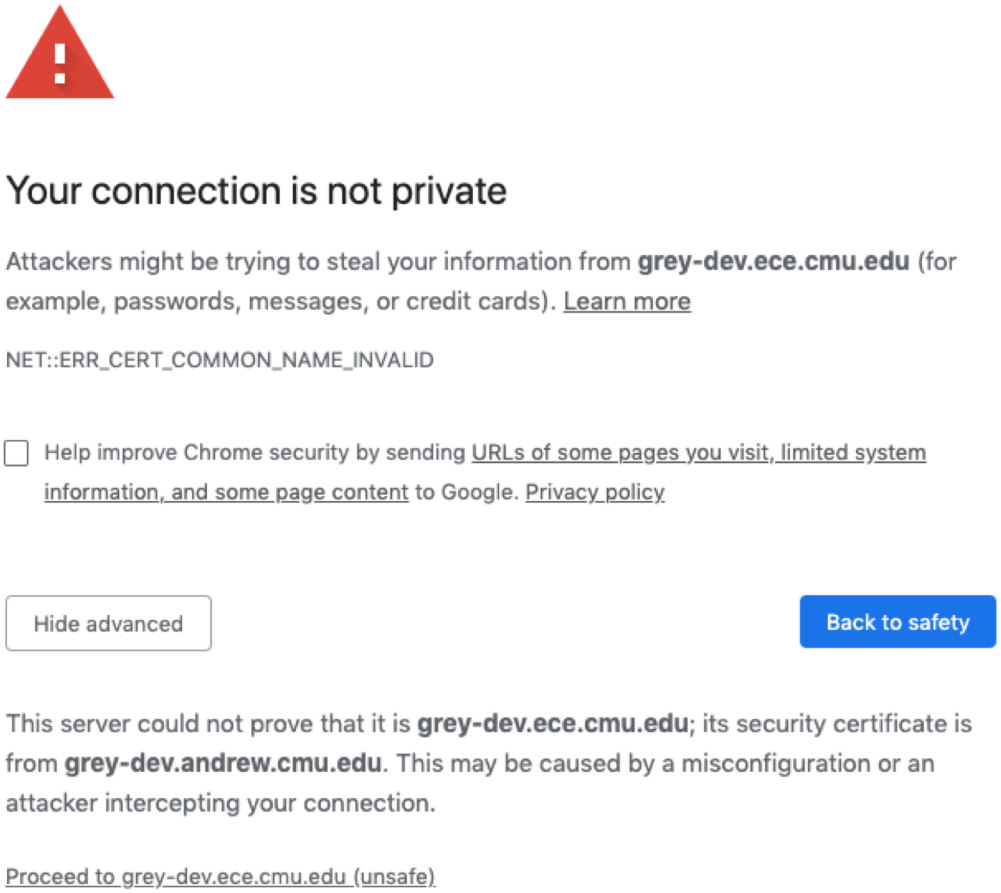
NET::ERR_CERT_COMMON_NAME_INVALID

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

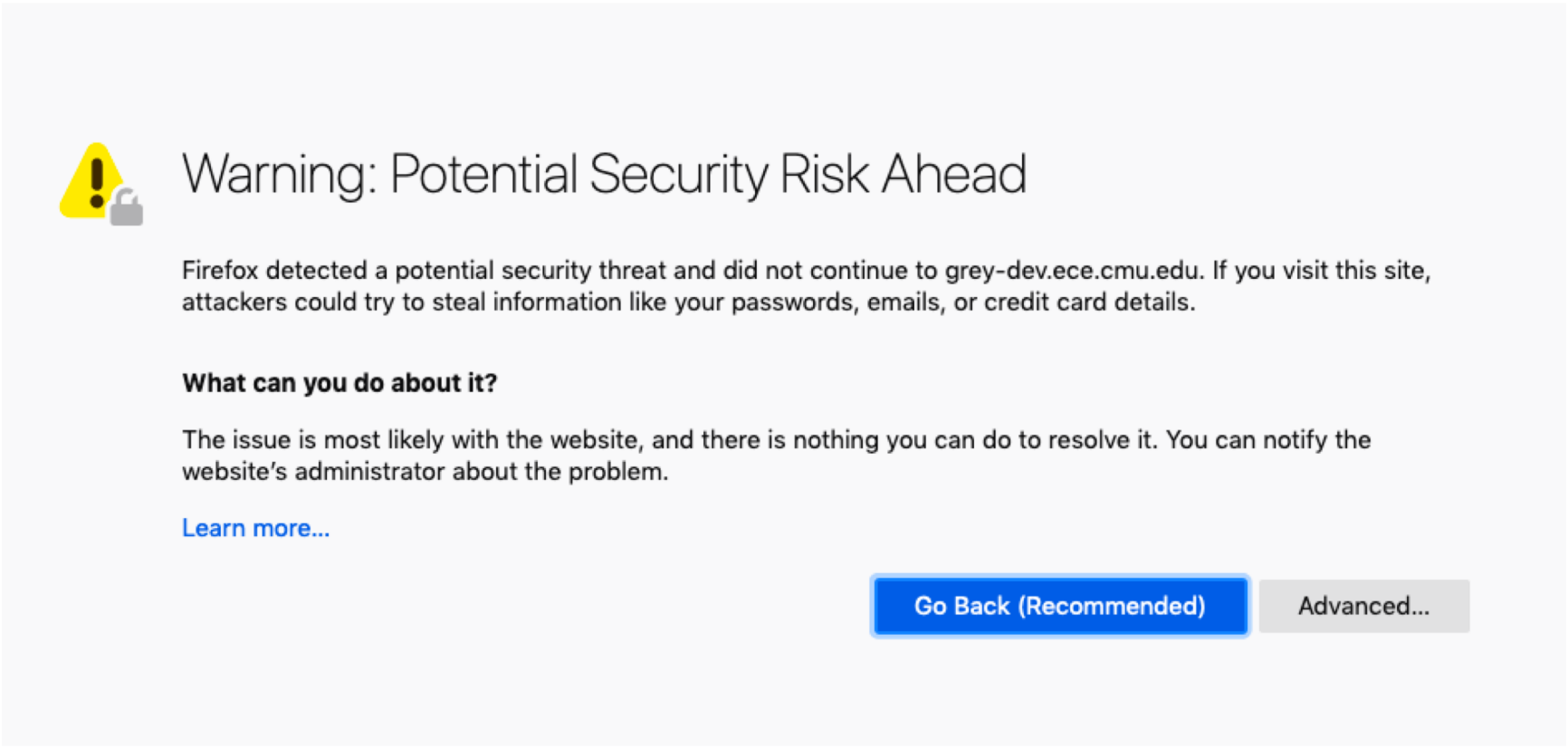
Advanced

Back to safety

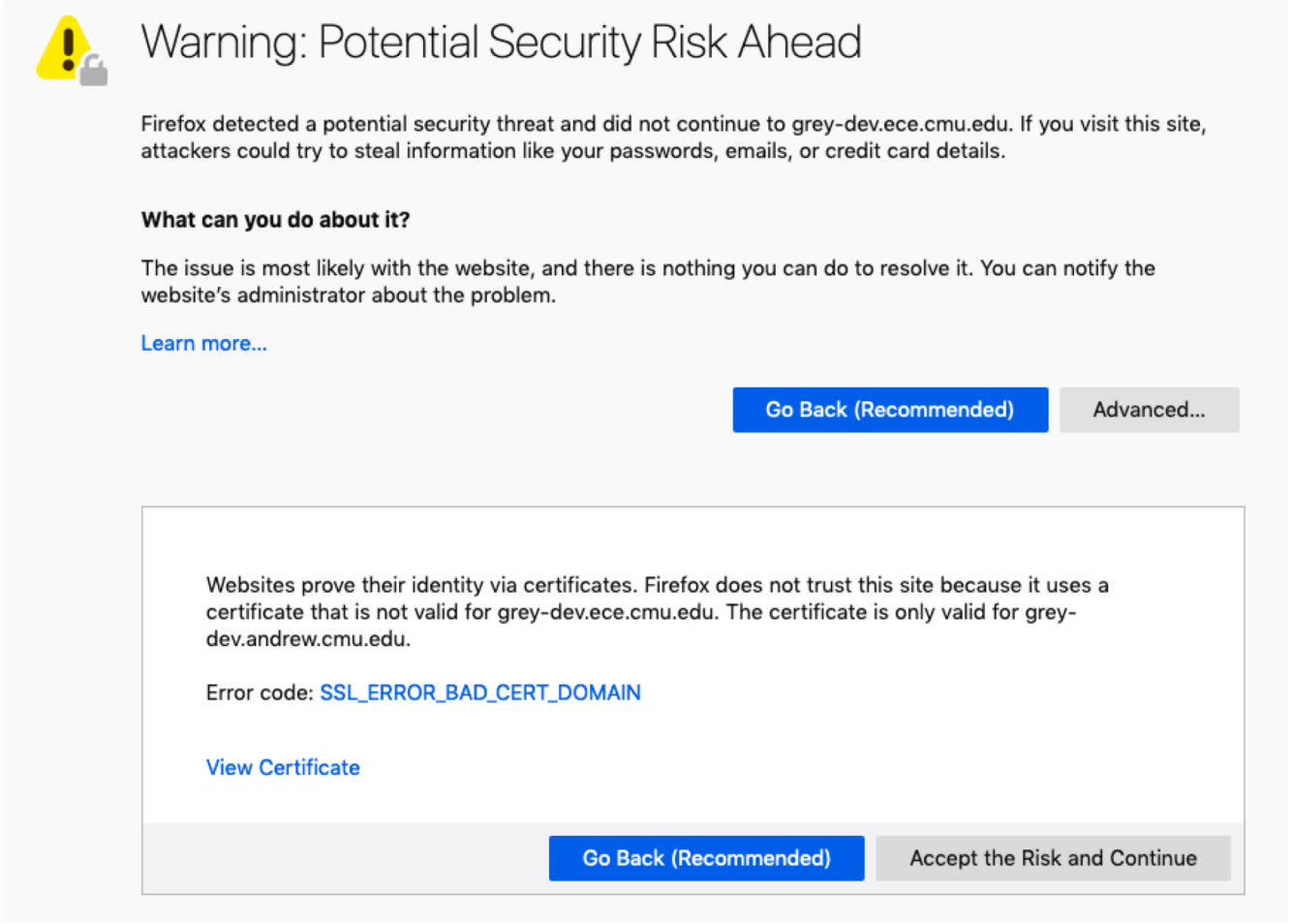
Chrome


Your connection is not private
Attackers might be trying to steal your information from grey-dev.ece.cmu.edu (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_COMMON_NAME_INVALID
Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy
Hide advanced
Back to safety
This server could not prove that it is grey-dev.ece.cmu.edu; its security certificate is from grey-dev.andrew.cmu.edu. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to grey-dev.ece.cmu.edu (unsafe)

Firefox


Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to grey-dev.ece.cmu.edu. 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. You can notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...

Firefox


Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to grey-dev.ece.cmu.edu. 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. You can notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...
Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for grey-dev.ece.cmu.edu. The certificate is only valid for grey-dev.andrew.cmu.edu.
Error code: SSL_ERROR_BAD_CERT_DOMAIN
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

Which warning prompt ensures security of the user?

Rethinking Connection Security Indicators

Adrienne Porter Felt[1], Robert W. Reeder[1], Alex Ainslie[1], Helen Harris[1], Max Walker[1], Christopher Thompson[2], Mustafa Emre Acer[1], Elisabeth Morant[1], Sunny Consolvo[1]
Google[1], UC Berkeley[2]
security-enamel@chromium.org[1], cthompson@cs.berkeley.edu[2]

ABSTRACT

We propose a new set of browser security indicators, based on user research and an understanding of the design challenges faced by browsers. To motivate the need for new security indicators, we critique existing browser security indicators and survey 1,329 people about Google Chrome's indicators. We then evaluate forty icons and seven complementary strings by surveying thousands of respondents about their perceptions of the candidates. Ultimately, we select and propose three indicators. Our proposed indicators have been adopted by Google Chrome, and we hope to motivate others to update their security indicators as well.

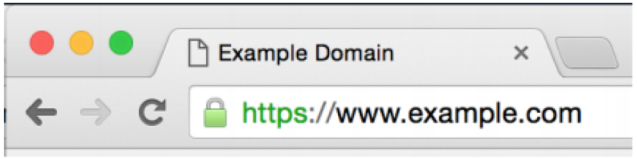


Figure 1: The green lock is a security indicator.

We then began the task of creating and testing new security indicators, working within the additional constraints posed by modern browser needs. Browsers are used by diverse audiences on diverse devices. Security indicators therefore face several design constraints:

Felt et al. (Required reading)

- survey 1,329 people about Google Chrome's indicators using a Google chrome extension
- screenshot of Chrome's URL bar with a red circle around the lock icon
  - *What does the green symbol to the left of the URL mean to you?*
- Coding (codebook development)
  - One codemaster used open coding for an initial codebook
  - Two partial coding rounds: each time giving feedback to the codemaster about shortcomings in the codebook