Augmenting the MetaMask-Wallet with Domain Name based Authentication of Ethereum Accounts

Jonas Ebel, 16.11.2020, Master Thesis Kick-off Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technical University Munich
wwwmatthes.in.tum.de

Outline

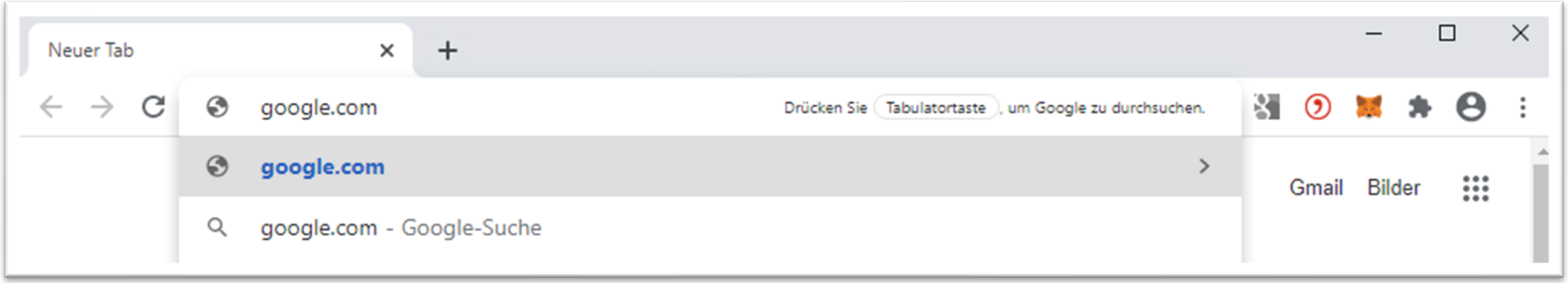
- Introduction and Motivation
- Research Questions
- Research Methods and current Results
- Next Steps

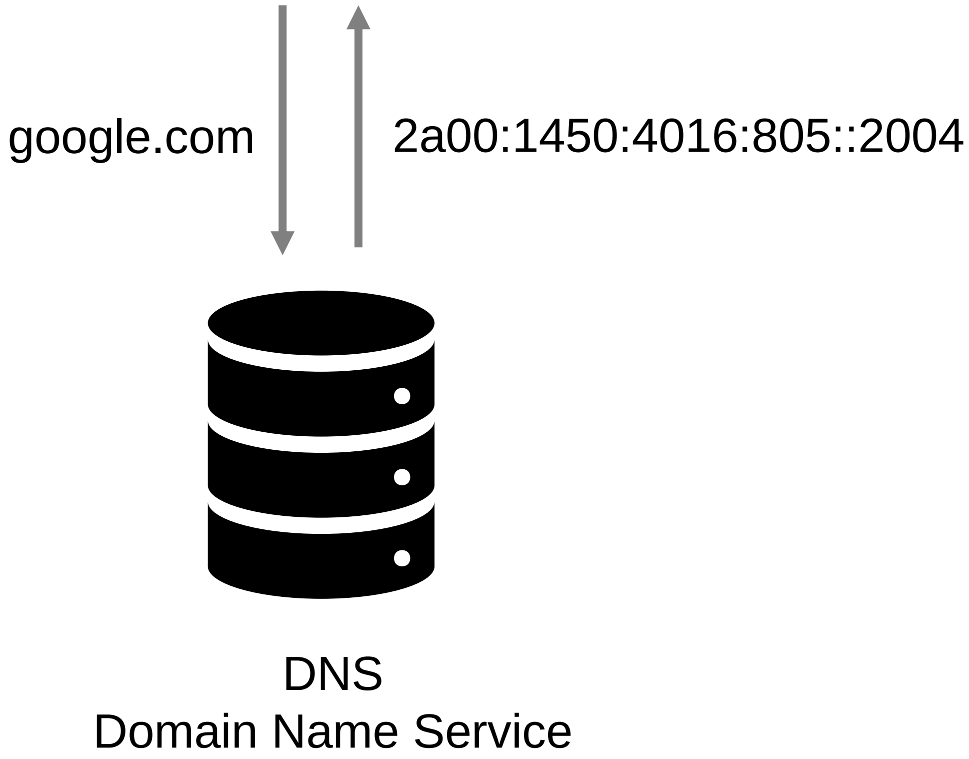
Motivation

INTERNET OF TODAY

HOW DO PEOPLE SURF SECURELY?

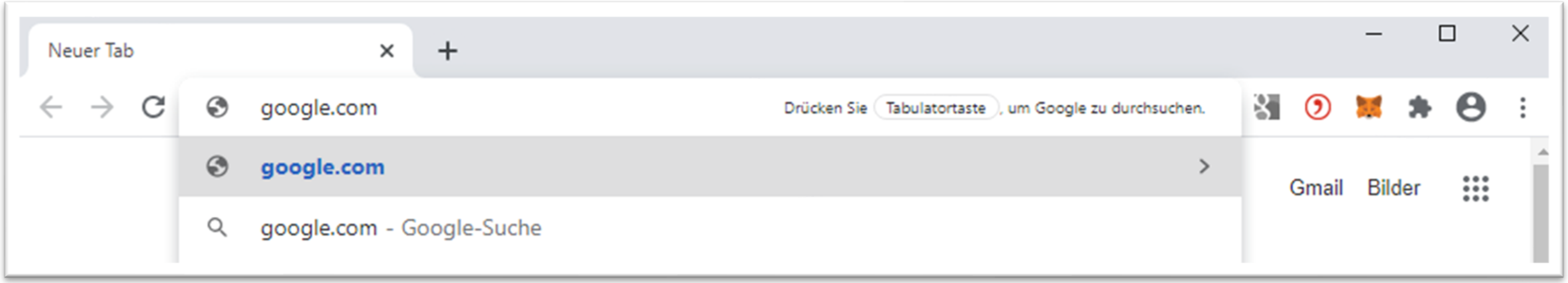
Motivation: DNS


Neuer Tab
google.com
Drücken Sie Tabulatortaste , um Google zu durchsuchen.
google.com
google.com - Google-Suche
Gmail
Bilder



- User enters domain name
- Browser resolves to Hostname

Motivation: Host name Verification

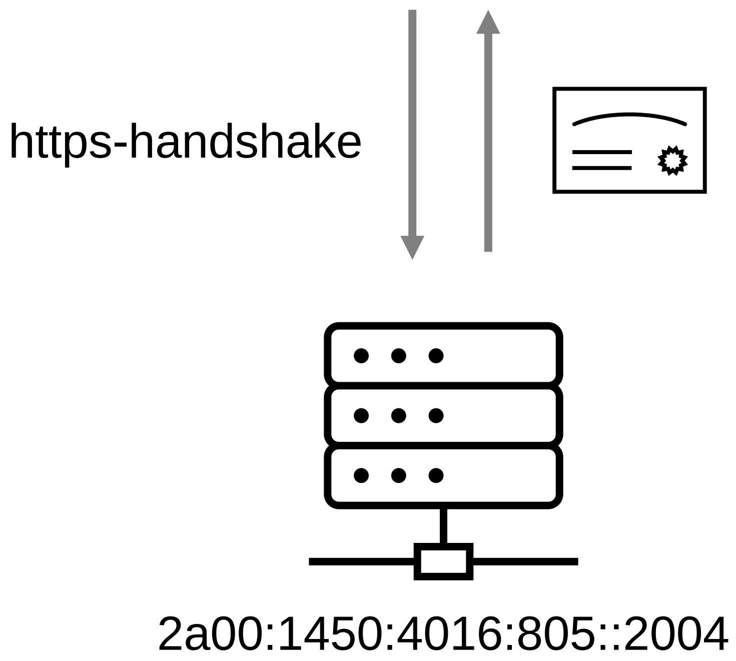


google.com

Drücken Sie Tabulatortaste , um Google zu durchsuchen.

google.com

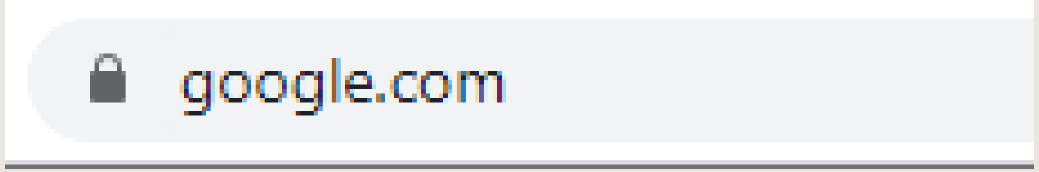
google.com - Google-Suche



- Browser initiates HTTPS-handshake with host
- Part of this protocol is to exchange identity certificates
- Browser evaluates host‘s identity

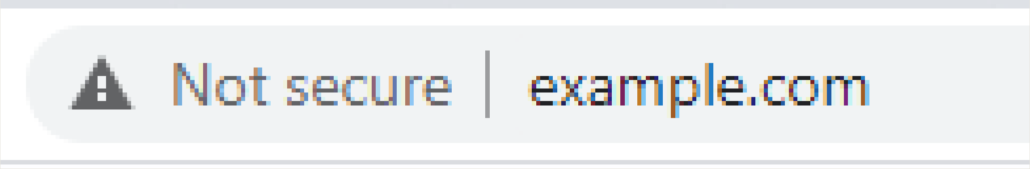
Motivation: Google‘s error pages

Secure & Trusted HTTPS Page



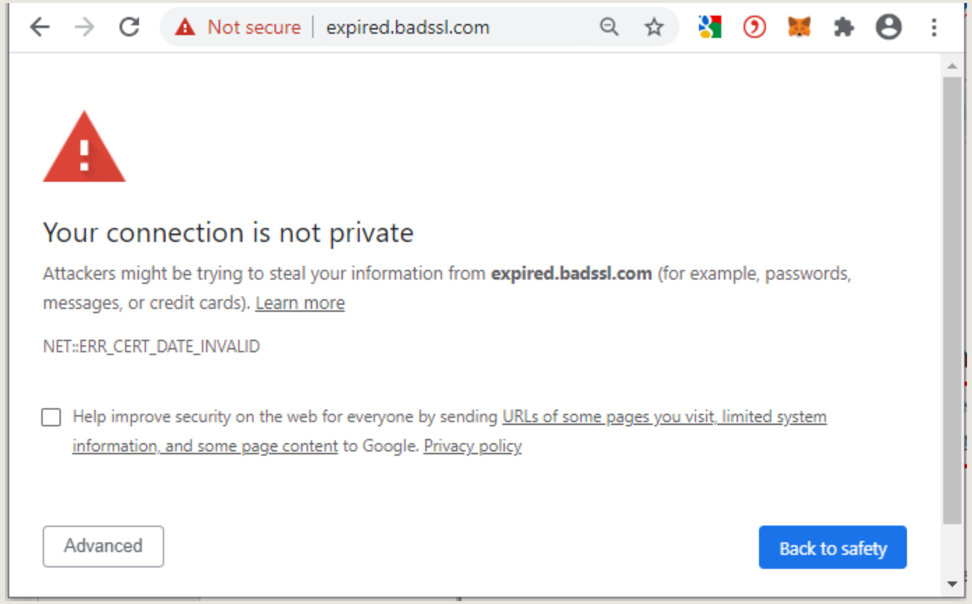
google.com

Untrusted HTTP Page



Not secure | example.com

Certificate Error



Not secure | expired.badssl.com

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

□ Help improve security on the web for everyone by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Motivation

BLOCKCHAIN:
ETHEREUM

HOW DO PEOPLE
INTERACT?

Motivation: Ethereum

Ethereum Blockchain

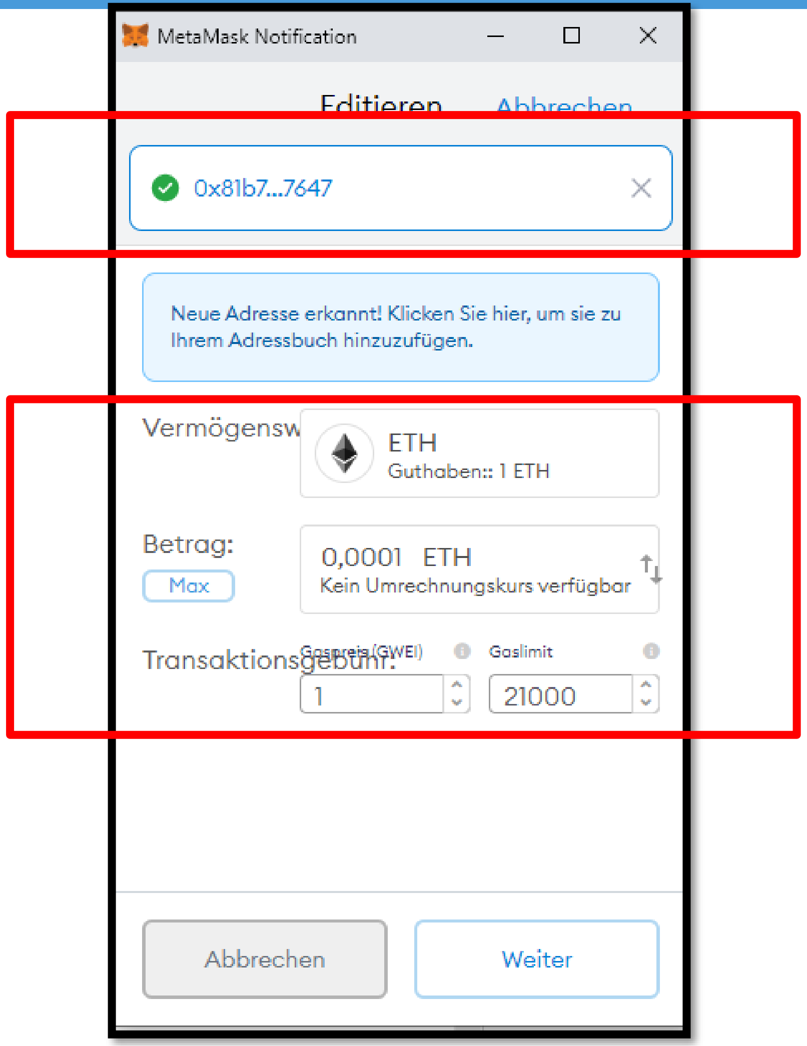
- Introduced 2015
- Public Permissionless Blockchain
- Smart Contract describes business logic
- Associated Currency Ether has highest market capitalization

MetaMask

- Wallet for Ethereum
- Manages the user‘s access to its accounts
- Browser Extension

Motivation: MetaMask

Use Case: Sending Ether to another Entity



0x81b7...7647

Neue Adresse erkannt! Klicken Sie hier, um sie zu Ihrem Adressbuch hinzuzufügen.

Vermögensw: ETH Guthaben:: 1 ETH

Betrag: 0,0001 ETH Kein Umrechnungskurs verfügbar

Transaktionsgebühr: Gaspreis (GWEI) 1 Gaslimit 21000

Possible Error Scenarios

Spelling Error

- No confirmation, whether it’s the correct account
- 40 Characters
- Not readable
- Ex.:

0xdc51Bac25e1c22E2F04bAAc20396D99fe56f7359

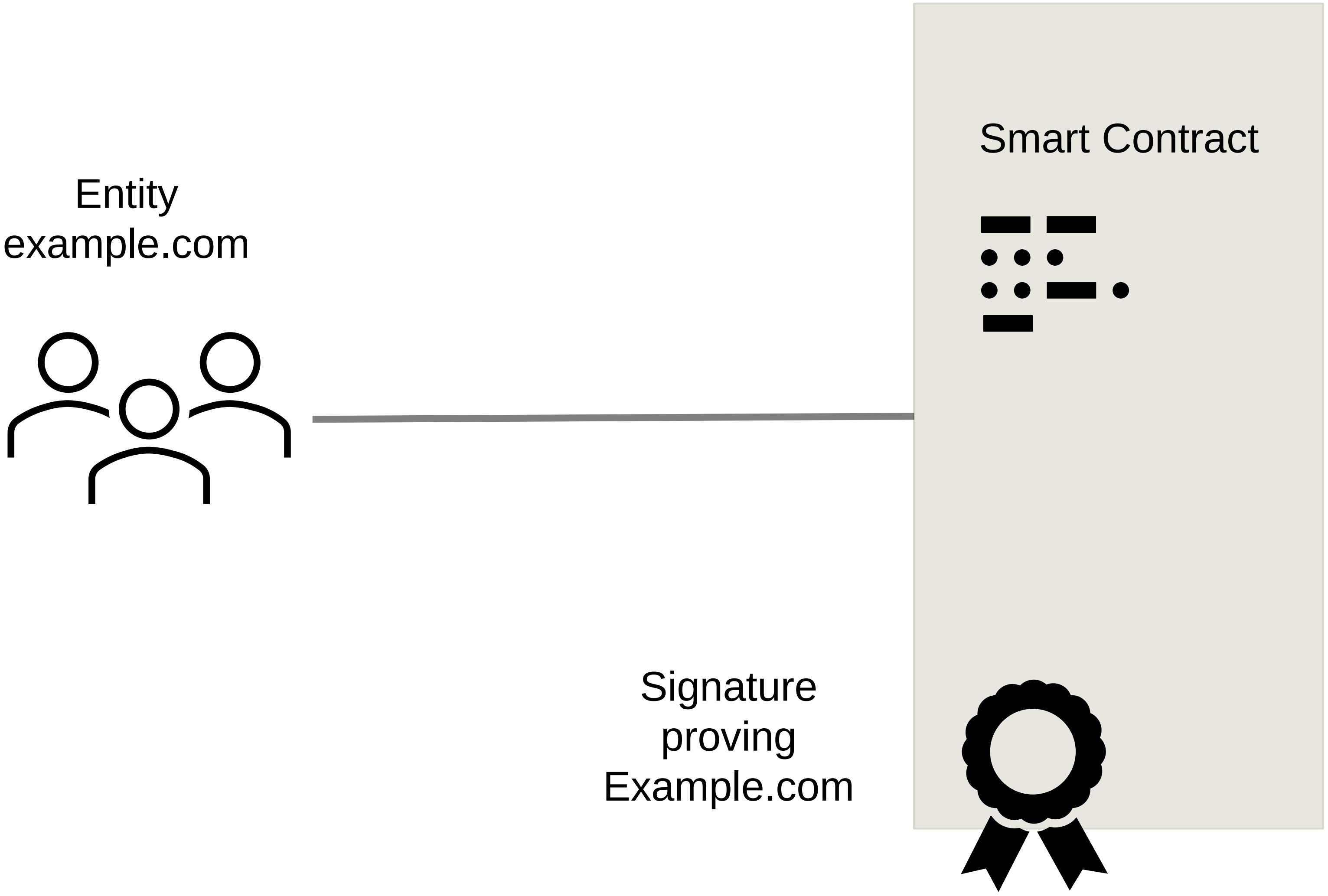
Phishing

- Source of the Addresses: WebPages
- If they are hacked…

Application of similar concept as HTTPS Host Name Verification

TeSC: TLS/SSL-certificate endorsed Smart Contracts

TeSC (TLS/SSL-certificate endorsed Smart Contracts)



U. Gallersdörfer and F. Matthes. AuthSC: Mind the Gap between Web and Smart Contracts. 2020.

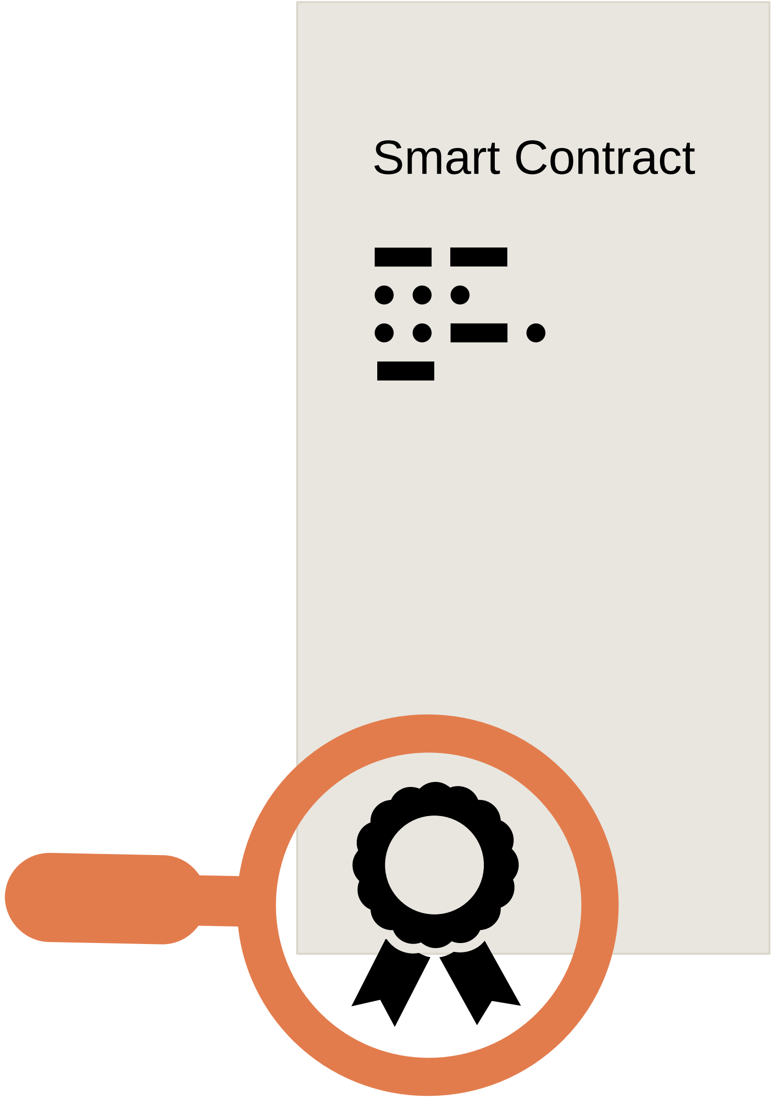
TeSC (TLS/SSL-certificate endorsed Smart Contracts)

Protocol

- Interface for Smart Contract
- Smart contract for on-chain registry like DNS

What is missing?

- A verifier that can be used by end users
- A design concept to communicate verification to user



U. Gallersdörfer and F. Matthes. AuthSC: Mind the Gap between Web and Smart Contracts. 2020.

Research Topic

How To Augment MetaMask with Domain Name based Authentication of Ethereum Addresses

Research Questions

1. How can DNS-based authentication indication in MetaMask be designed?

2. What is a feasible architecture concept of an Off-Chain Verifier for MetaMask?

3. Does the application of TeSC improve the user‘s security interacting with Ethereum?

UI-Design Method

Orientation on Browser and Others

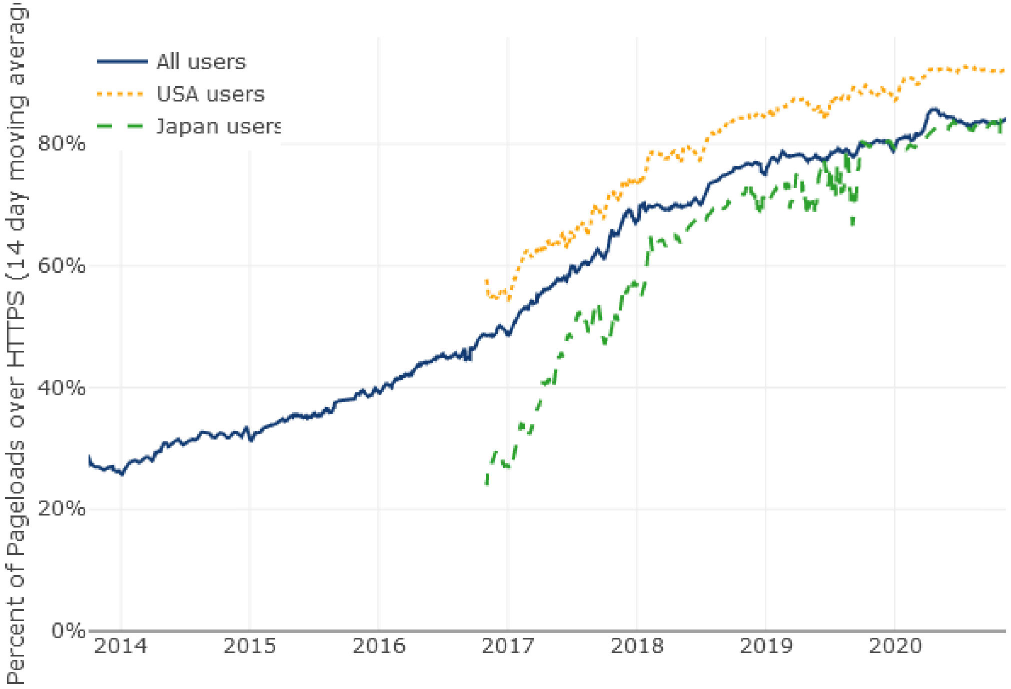
How to design the UI?

HTTPS Indicator Research

- First laboratory experiments in 2006
- Since then adoption is rising
- Results are getting better, but not perfect

Key take aways

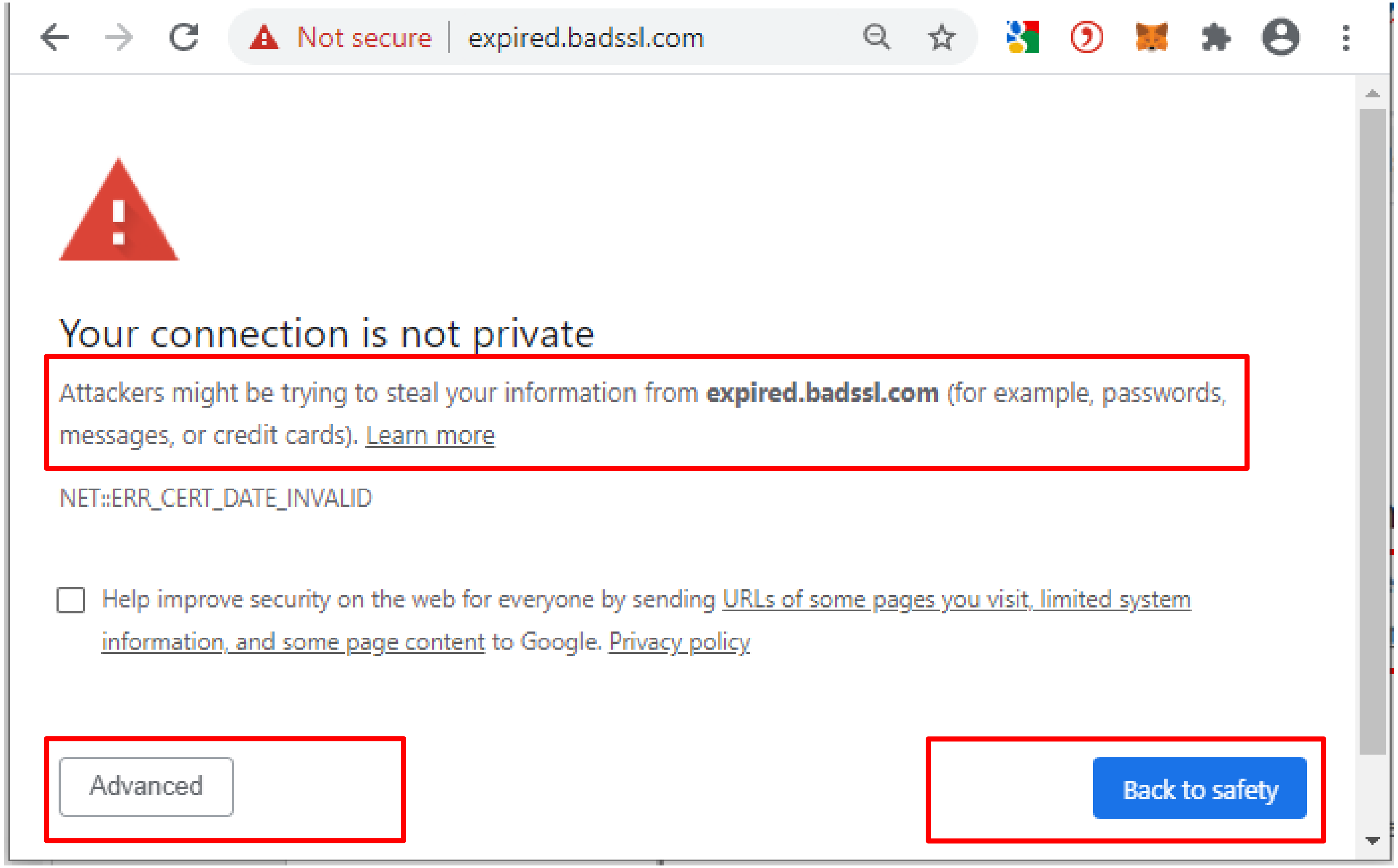
- Avoid Habituation
  [5,6,4]
- Passive Warnings are ignored &
  Absence of Passive indicators are ignored
  [2,6,7,10]
- Only educated user make informed decision
  [1,2,3,4,6,8,9,10]



HTTPS Pageloads in Firefox 2014 – 2020
HTTPS exists since 1994 for Netscape

https://letsencrypt.org/stats/, Zugriff:12.11.2020

Inspection Example: Expired SSL Certificate Warning in Google Chrome



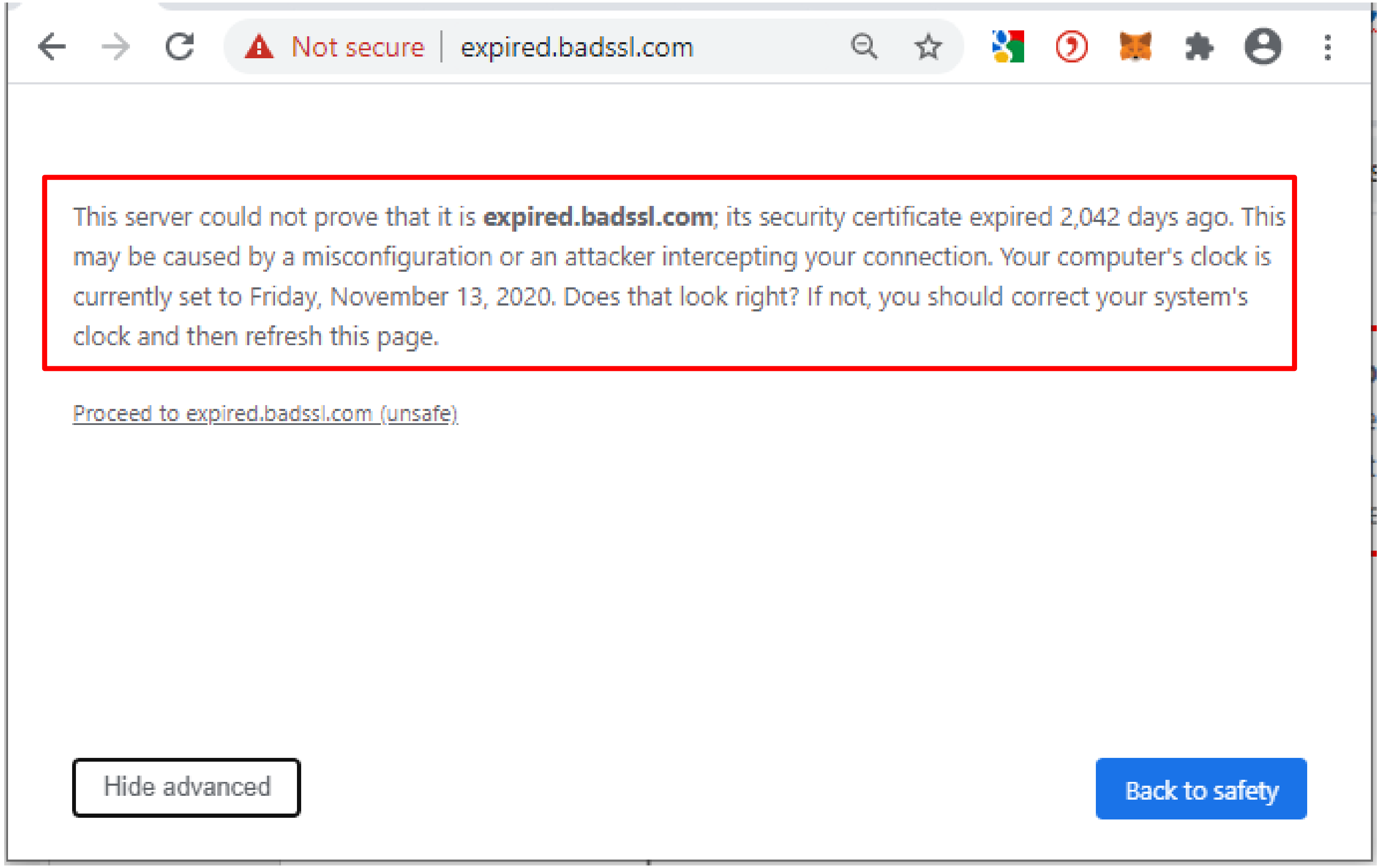
Your connection is not private

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

□ Help improve security on the web for everyone by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Inspection Example: Expired SSL Certificate Warning in Google Chrome



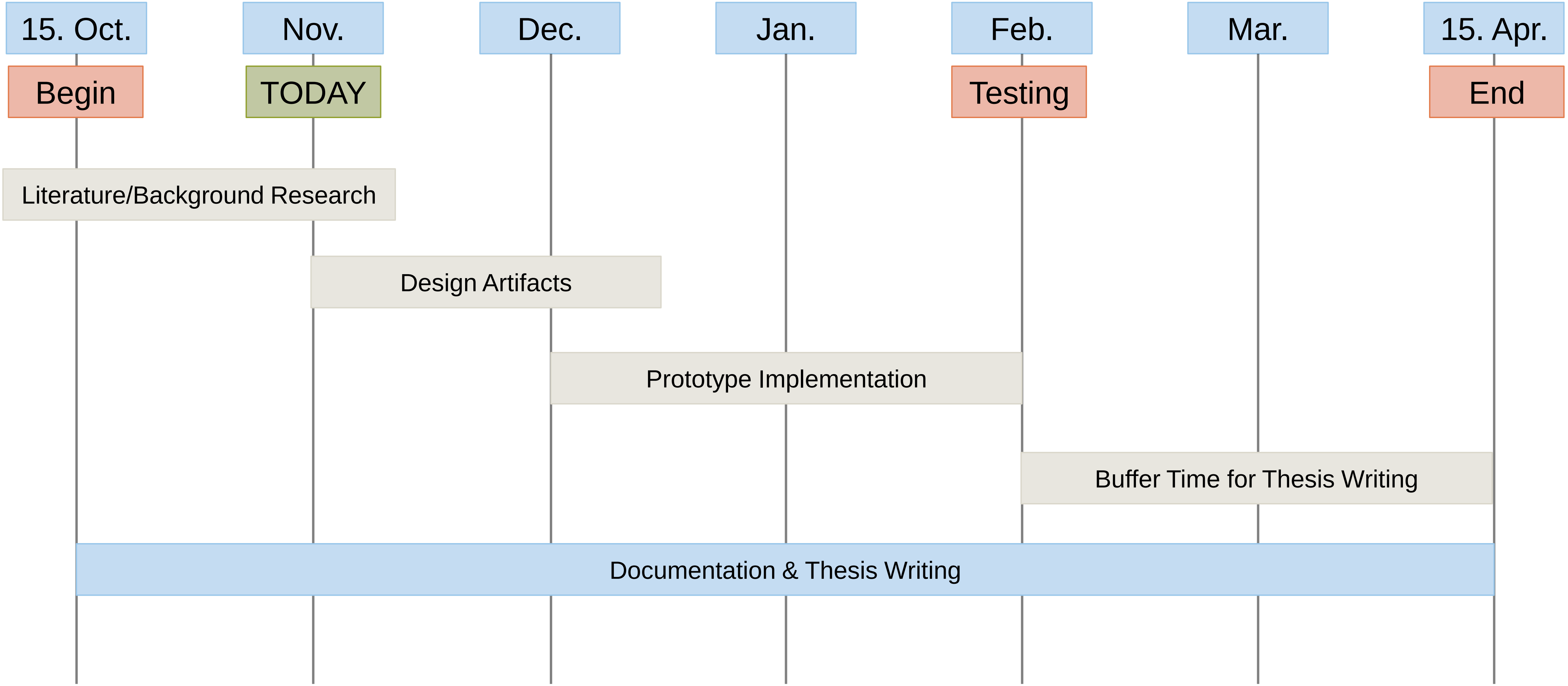
This server could not prove that it is **expired.badssl.com**; its security certificate expired 2,042 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Friday, November 13, 2020. Does that look right? If not, you should correct your system's clock and then refresh this page.

Proceed to expired.badssl.com (unsafe)

Next Steps

Timetable

Timetable



15. Oct. – Begin

Nov. – TODAY

Dec.

Jan.

Feb. – Testing

Mar.

15. Apr. – End

Literature/Background Research

Design Artifacts

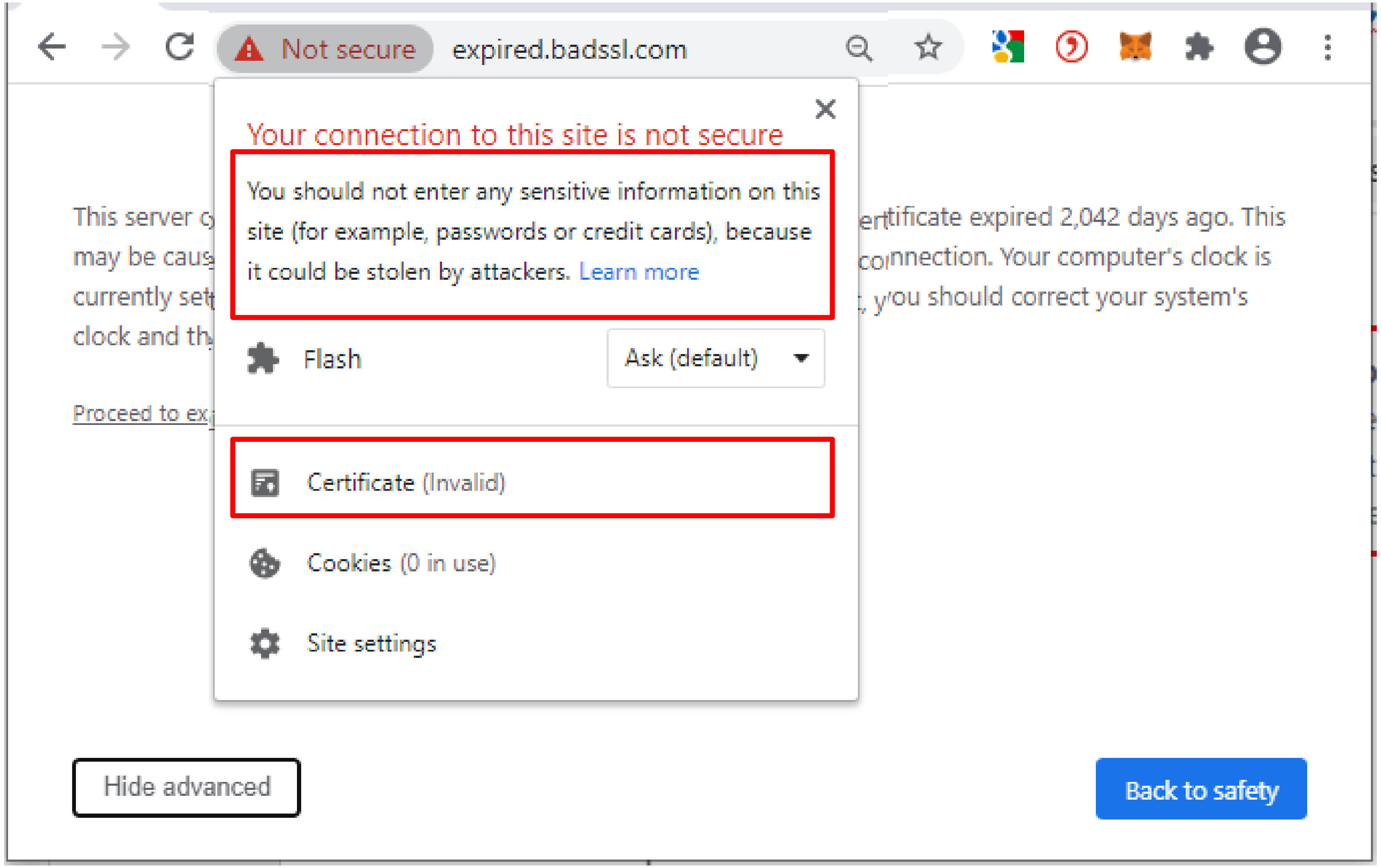
Prototype Implementation

Buffer Time for Thesis Writing

Documentation & Thesis Writing

B.Sc.
Jonas Ebel
Student
jonas.ebel@tum.de

Inspection Example: Expired SSL Certificate Warning in Google Chrome



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Flash: Ask (default)

This server c… ertificate expired 2,042 days ago. This may be caus… connection. Your computer's clock is currently set… , you should correct your system's clock and th…

Proceed to ex…

Open Tasks – Sorted after Design Science Cycle

Environment Analysis

- MetaMask UI Inspection ✓
- Ethereum/MetaMask Interface Review ✓
- Similar Solutions ✗

Knowledge Base Analysis

- Literature search: Browser inspection ✓
- Browser UI Inspection ⏳
- Review SSL/TLS Certificate RFC ✗

Build & Design

- Use Case Definition ⏳
- Error Scenarios ✗
- MetaMask Design Concept ✗
- Architecture Design ✗
- Implementation ✗

Evaluation

- Testing Concept ✓
- Concrete Test Implementation ✗
- Tests in beginning of February ✗

Hevner, Alan R. (2007) "A Three Cycle View of Design Science Research," *Scandinavian Journal of Information Systems*: Vol. 19: Iss. 2, Article 4.

Validating the Contribution

User Study Concept

User Study Concept

Orientate on Browser research

- Laboratory Experiment
- Between subject study
- Exit-survey for design evaluation / feedback

Concept

- User transact on test network with fraudulent cases
- Group A works with „normal“ MetaMask plugin
- Group B works with the TeSC enabled prototype

Hypothesis

Group B outperforms Group A in detected errors and attacks

Literature

[1] Bravo-Lillo, Cristian; et al. (2011): Bridging the Gap in Computer Security Warnings: A Mental Model Approach. In: *IEEE Secur. Privacy Mag.* 9 (2), S. 18–26. DOI: 10.1109/MSP.2010.198.

[2] Thompson, Christopher; et al. (2019): The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators. In: Proceedings of 28th USENIX. Security Symposium. Santa Clara, USA, p. 1715–1732.

[3] Felt, Adrienne Porter; et al. (2015): Improving SSL Warnings. In: Jinwoo Kim (Ed.): Proceedings of the 33rd Annual CHI Conference on Human Factors in Computing Systems. Seoul, Republic of Korea. New York, NY: ACM, p. 2893–2902.

[4] Desolda, Giuseppe; et al. (2019): Alerting Users About Phishing Attacks. In:. International Conference on Human-Computer Interaction: Springer, Cham, S. 134–148.

[5] Jelovčan, L.; Vrhovec, S.L.R.; Mihelič, A. (2020): A literature survey of security indicators in web browsers. In: *Elektrotehniški vestnik* 87 (1-2), p. 31–38.

[6] Reeder, Robert W.; et al. (2018): An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In: Regan Mandryk und Mark Hancock (Ed.): Engage with CHI. The 2018 CHI Conference. Montreal QC, Canada. New York, New York: The Association for Computing Machinery, p. 1–13.

[7] Sobey, Jennifer; Biddle, Robert; van Oorschot, P. C.; Patrick, Andrew S. (2008): Exploring User Reactions to New Browser Cues for Extended Validation Certificates. In: Sushil Jajodia und Javier Lopez (Ed.): Computer Security - ESORICS 2008. Berlin, Heidelberg, 2008. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 411–427.

[8] Stojmenoviæ, Milica; Biddle, Robert (2018): Hide-and-Seek with Website Identity Information. In: Kieran McLaughlin, et al.(Ed.): 2018 16th Annual Conference on Privacy, Security and Trust (PST). Belfast, 8/28/2018 - 8/30/2018. Annual Conference on Privacy, Security and Trust; Institute of Electrical and Electronics Engineers; International Conference on Privacy, Security and Trust; PST. Piscataway, NJ: IEEE, S. 1–6.

[9] Yi, Christine Lim Xin; et al. (2020): Appraisal on User’s Comprehension in Security Warning Dialogs: Browsers Usability Perspective. In: Mohammed Anbar, et al. (Ed.): Advances in Cyber Security. Singapore, 2020. 1st ed. 2020. Singapore: Springer Singapore (Communications in Computer and Information Science), p. 320–334.

[10] Xiong, Aiping; et al. (2017): Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages? In: *Human factors* 59 (4), p. 640–660.