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
www.matthes.in.tum.de
Outline

• Introduction and Motivation

• Research Questions

• Research Methods and current Results

• Next Steps
INTERNET OF TODAY

HOW DO PEOPLE SURF SECURELY?
Motivation: DNS

- User enters domain name
- Browser resolves to Hostname

google.com

2a00:1450:4016:805::2004

DNS
Domain Name Service
Motivation: Host name Verification

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

https-handshake

2a00:1450:4016:805::2004
Motivation: Google's error pages

Secure & Trusted HTTPS Page

Untrusted HTTP Page

Certificate Error
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

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)

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

Research Topic
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

Advanced

Back to safety
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
15. Oct.  Begin  Literature/Background Research

Nov.  TODAY  Design Artifacts

Dec.  Prototype Implementation

Jan.  Testing

Feb.  Buffer Time for Thesis Writing

Mar.  End

15. Apr.
Inspection Example: Expired SSL Certificate Warning in Google Chrome
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

---

Validating the Contribution

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


