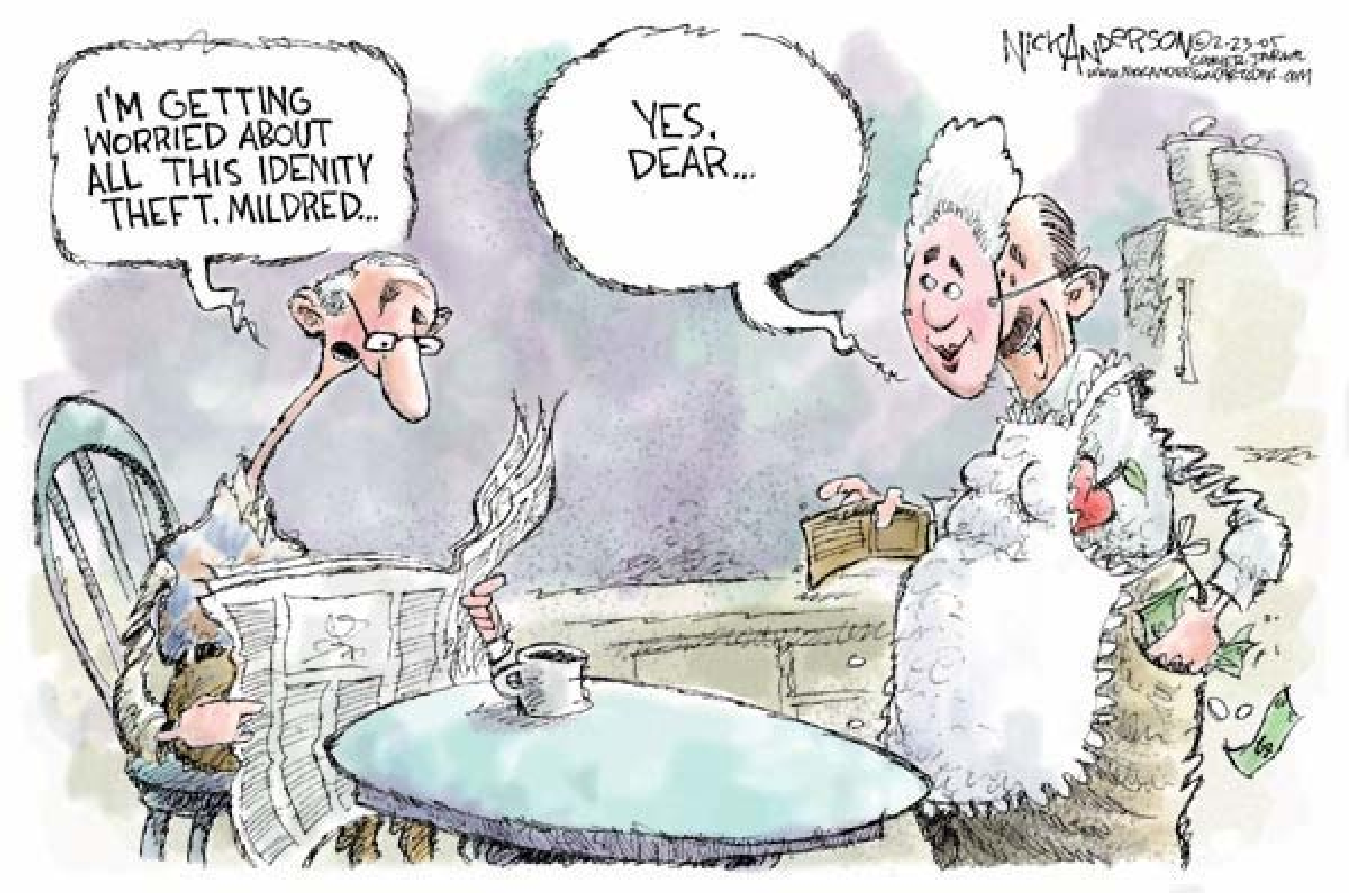
Client Authentication in a Federation Using a Security Mode

Sebastian Gajek and Ahmad-Reza Sadeghi

Horst-Görtz Institute for IT-Security

Ruhr-University Bochum, Germany

Problem


I'M GETTING WORRIED ABOUT ALL THIS IDENITY THEFT, MILDRED...
YES, DEAR...
NICK ANDERSON ©2-23-05
COURIER-JOURNAL
www.nickandersoncartoons.com

Terms

Phishing: stealing credentials or any other valuable information by *actively* or *passively* creating a fake environment to deceive victims

- mounting attacks (e.g., DNS-based)
- spoofing attacks (e.g., Web Spoofing, Picture-in-Picture)

Malwared Phishing: *additionally* compromises the local system

- Host-file alternation
- Keylogger
- Trojan Horses

What is a Security Mode?

Security Mode

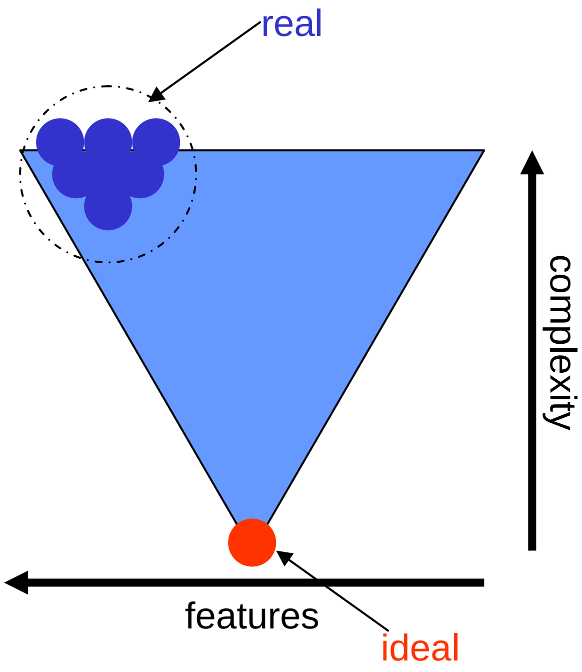
- Tame browser to ideal behavior

Predication

- Web Browsers are full of (potentially) malicious features
- Verifying security not manageable by ordinary user

Objectives

- Reduce Tampering
- User-Transparency
- Proving Security Requirements



What is a Security Mode?

Security Mode

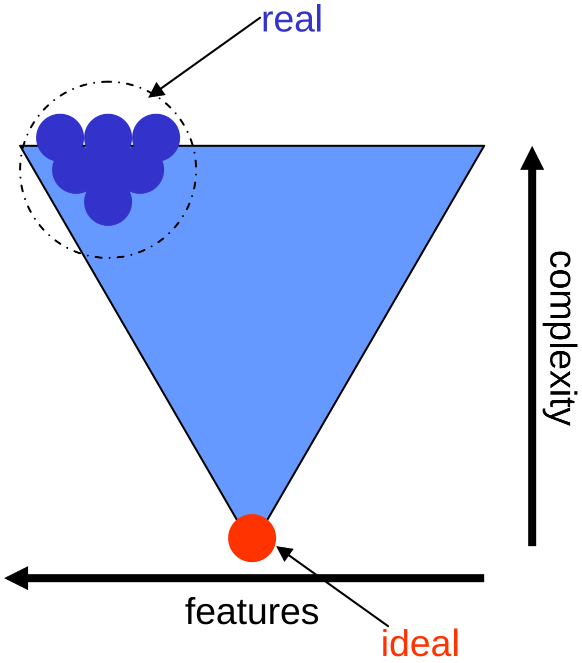
- Tame browser to ideal behavior

Predication

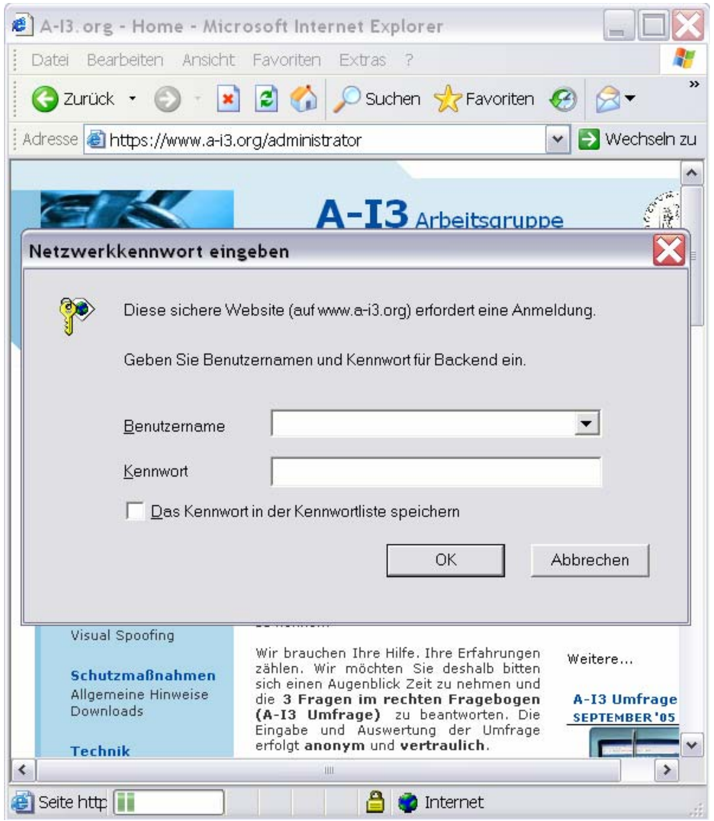
- Web Browsers are full of (potentially) malicious features
- Verifying security not manageable by ordinary user

Objectives

- Reduce Tampering
- User-Transparency
- Proving Security Requirements



Case Study: Tampering


A-I3.org - Home - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
Wechseln zu
A-I3 Arbeitsgruppe
Seite http
Internet

https://www.a-i3.org/administrator

Netzwerkkennwort eingeben

Diese sichere Website (auf www.a-i3.org) erfordert eine Anmeldung.

Geben Sie Benutzernamen und Kennwort für Backend ein.

Benutzername

Kennwort

□ Das Kennwort in der Kennwortliste speichern

OK Abbrechen

Visual Spoofing

Schutzmaßnahmen
Allgemeine Hinweise
Downloads

Technik

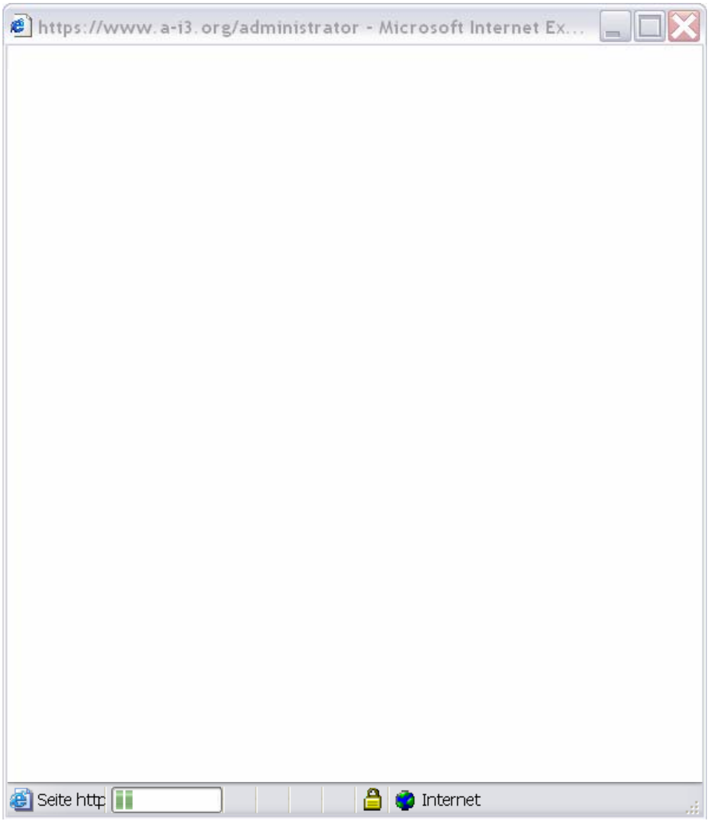
Wir brauchen Ihre Hilfe. Ihre Erfahrungen zählen. Wir möchten Sie deshalb bitten sich einen Augenblick Zeit zu nehmen und die **3 Fragen im rechten Fragebogen (A-I3 Umfrage)** zu beantworten. Die Eingabe und Auswertung der Umfrage erfolgt **anonym** und **vertraulich**.

Weitere...

A-I3 Umfrage SEPTEMBER'05

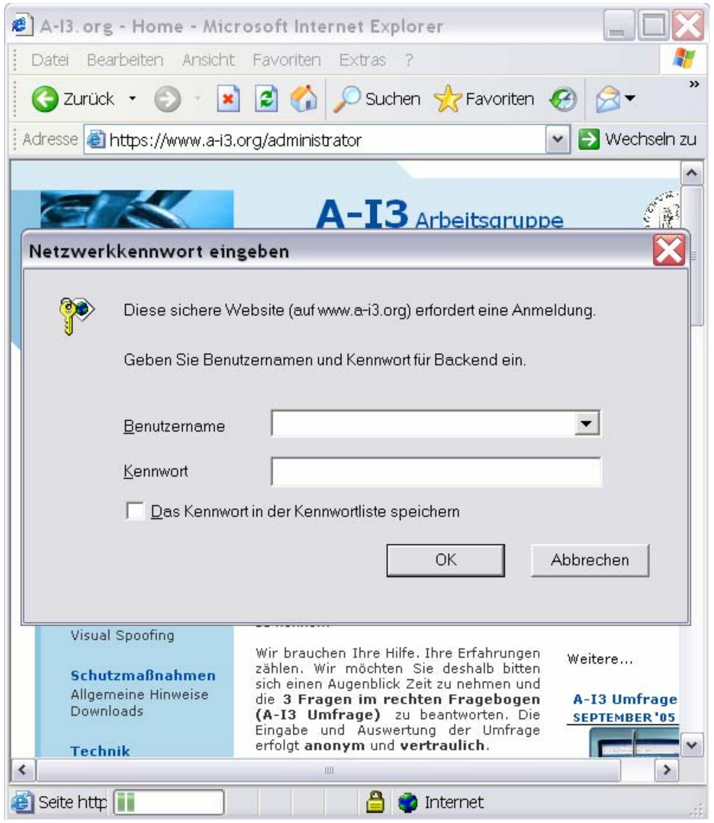
original

=


https://www.a-i3.org/administrator - Microsoft Internet Ex...
Seite http
Internet

fake

Case Study: Tampering



https://www.a-i3.org/administrator

Netzwerkkennwort eingeben

Diese sichere Website (auf www.a-i3.org) erfordert eine Anmeldung.

Geben Sie Benutzernamen und Kennwort für Backend ein.

Benutzername

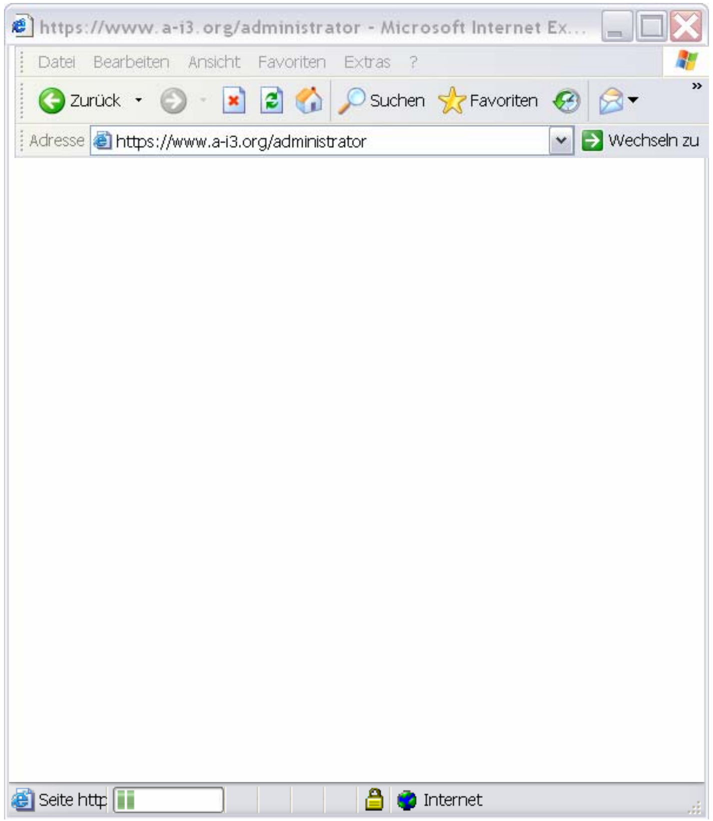
Kennwort

□ Das Kennwort in der Kennwortliste speichern

Wir brauchen Ihre Hilfe. Ihre Erfahrungen zählen. Wir möchten Sie deshalb bitten sich einen Augenblick Zeit zu nehmen und die **3 Fragen im rechten Fragebogen (A-I3 Umfrage)** zu beantworten. Die Eingabe und Auswertung der Umfrage erfolgt **anonym** und **vertraulich**.

original

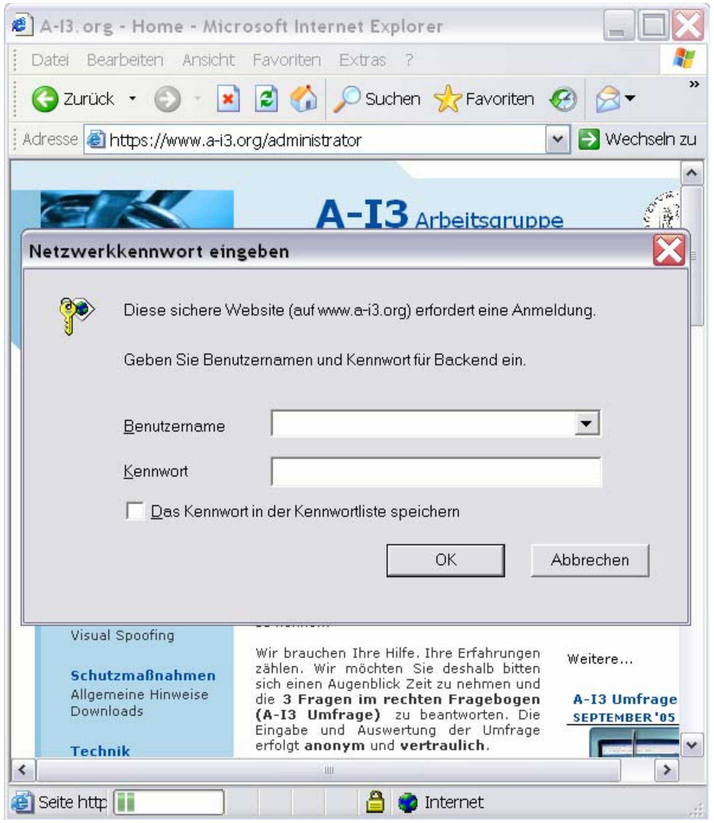
=


https://www.a-i3.org/administrator - Microsoft Internet Ex...
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Favoriten
Adresse
Wechseln zu
Seite http
Internet

https://www.a-i3.org/administrator

fake

Case Study: Tampering



A-I3.org - Home - Microsoft Internet Explorer

https://www.a-i3.org/administrator

A-I3 Arbeitsgruppe

Netzwerkkennwort eingeben

Diese sichere Website (auf www.a-i3.org) erfordert eine Anmeldung.

Geben Sie Benutzernamen und Kennwort für Backend ein.

Benutzername

Kennwort

□ Das Kennwort in der Kennwortliste speichern

OK Abbrechen

Visual Spoofing

Schutzmaßnahmen
Allgemeine Hinweise
Downloads

Technik

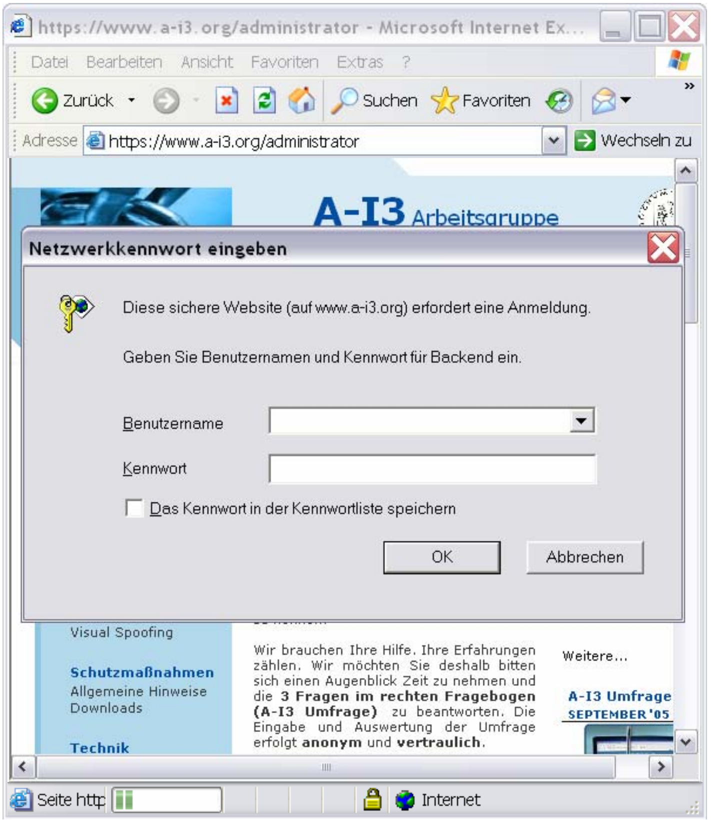
Wir brauchen Ihre Hilfe. Ihre Erfahrungen zählen. Wir möchten Sie deshalb bitten sich einen Augenblick Zeit zu nehmen und die **3 Fragen im rechten Fragebogen (A-I3 Umfrage)** zu beantworten. Die Eingabe und Auswertung der Umfrage erfolgt **anonym** und **vertraulich**.

Weitere...

A-I3 Umfrage
SEPTEMBER'05

original

=



https://www.a-i3.org/administrator - Microsoft Internet Ex...

https://www.a-i3.org/administrator

A-I3 Arbeitsgruppe

Netzwerkkennwort eingeben

Diese sichere Website (auf www.a-i3.org) erfordert eine Anmeldung.

Geben Sie Benutzernamen und Kennwort für Backend ein.

Benutzername

Kennwort

□ Das Kennwort in der Kennwortliste speichern

OK Abbrechen

Visual Spoofing

Schutzmaßnahmen
Allgemeine Hinweise
Downloads

Technik

Wir brauchen Ihre Hilfe. Ihre Erfahrungen zählen. Wir möchten Sie deshalb bitten sich einen Augenblick Zeit zu nehmen und die **3 Fragen im rechten Fragebogen (A-I3 Umfrage)** zu beantworten. Die Eingabe und Auswertung der Umfrage erfolgt **anonym** und **vertraulich**.

Weitere...

A-I3 Umfrage
SEPTEMBER'05

fake

What is Security Mode?

Security Mode

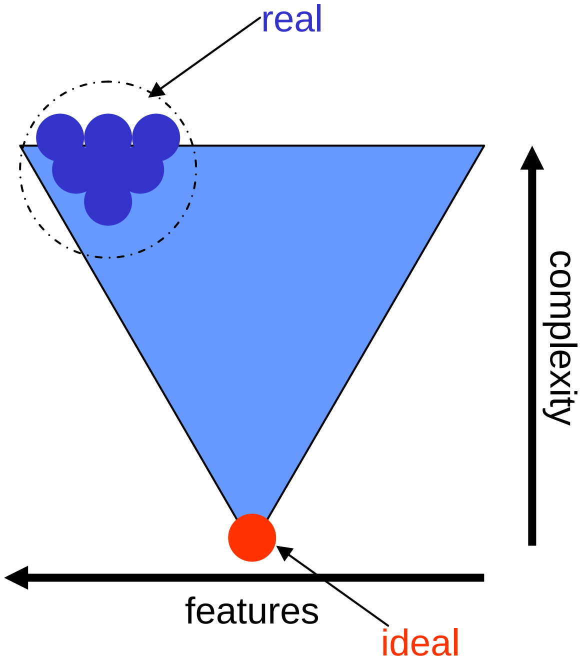
- Tame browser to ideal behavior

Predication

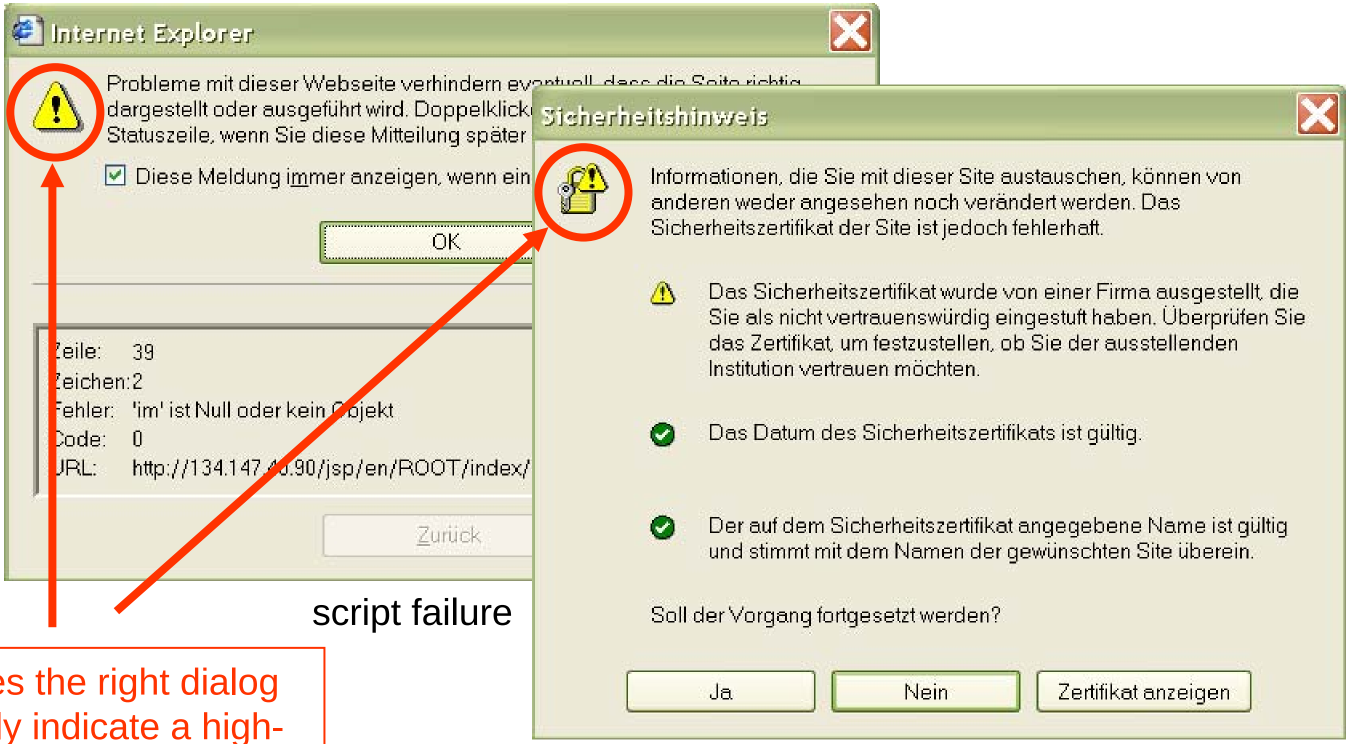
- Web Browsers are full of (potentially) malicious features
- Verifying security not manageable by ordinary user

Objectives

- Reduce Tampering
- User-Transparency
- Proving Security Requirements



Case Study: Transparency



Internet Explorer

Probleme mit dieser Webseite verhindern eventuell, dass die Seite richtig dargestellt oder ausgeführt wird. Doppelklick Statuszeile, wenn Sie diese Mitteilung später

☑ Diese Meldung immer anzeigen, wenn ein

OK

Zeile: 39
Zeichen: 2
Fehler: 'im' ist Null oder kein Objekt
Code: 0
URL: http://134.147.40.90/jsp/en/ROOT/index/

Zurück

Sicherheitshinweis

Informationen, die Sie mit dieser Site austauschen, können von anderen weder angesehen noch verändert werden. Das Sicherheitszertifikat der Site ist jedoch fehlerhaft.

⚠ Das Sicherheitszertifikat wurde von einer Firma ausgestellt, die Sie als nicht vertrauenswürdig eingestuft haben. Überprüfen Sie das Zertifikat, um festzustellen, ob Sie der ausstellenden Institution vertrauen möchten.

✓ Das Datum des Sicherheitszertifikats ist gültig.

✓ Der auf dem Sicherheitszertifikat angegebene Name ist gültig und stimmt mit dem Namen der gewünschten Site überein.

Soll der Vorgang fortgesetzt werden?

Ja | Nein | Zertifikat anzeigen

script failure

SSL alert

Does the right dialog really indicate a high-security failure?

What is a Security Mode?

Security Mode

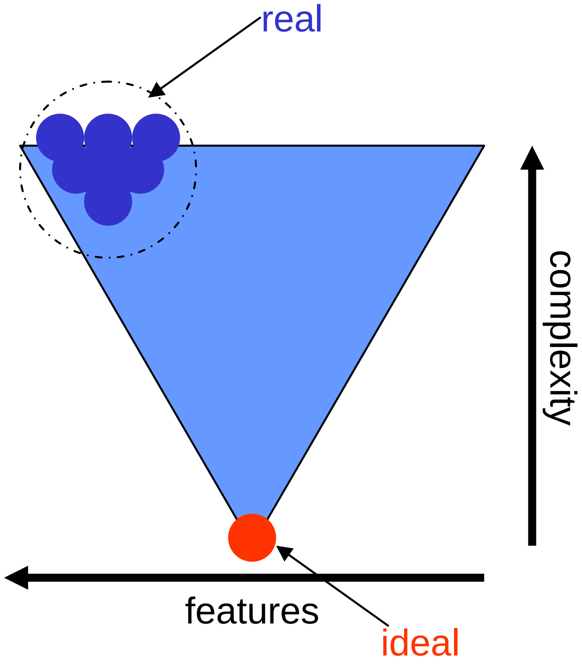
- Tame browser to ideal behavior

Predication

- Web Browsers are full of (potentially) malicious features
- Verifying security not manageable by ordinary user

Objectives

- Reduce Tampering
- User-Transparency
- Proving Security Requirements



Proving Security Requirements in Browser Model

De-facto-Standard in Web authentication:

- Unilateral SSL authentication with username/password
- Related Work (e.g. [WS96,MSS98]) analyzed SSL in 2-Party-Scenario
- 3-Party-Protocol
  - User U (security-unaware)
  - Browser B (protocol-unaware)
  - Server S (crypto-expert)
- Recent Work [GPS05a] attempts to formally analyze browser-based protocols based on “ideal/real world” paradigm (here by [PSW00])
  - Principals are finite state machines
  - Behavior idealized
- Proved WS-Federation Passive Requestor Profile [GPS05b]

Proving Security Requirements in Browser Model

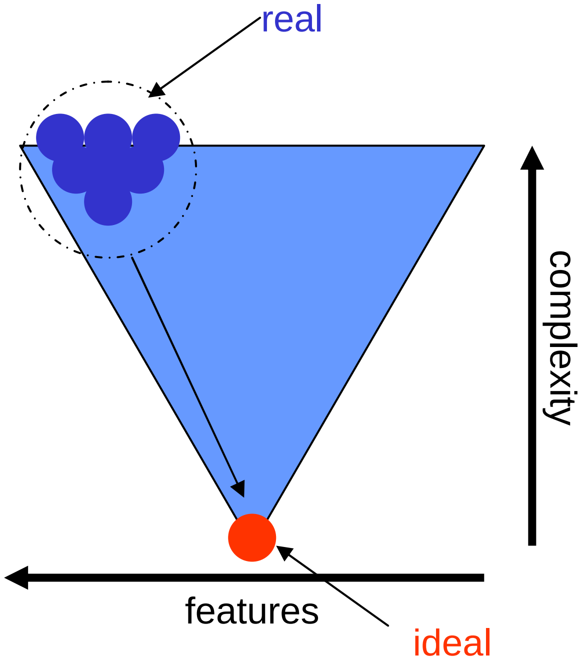
Problem

- Idealized model very complex
- Real model contains many features, not regarded

Conclusion

- If browser can be tamed to ideal behavior then one better reason about security properties
- If sender knows Browser behaves ideally and the authentication protocol is sound then sender can imply that user has been correctly authenticated

ideal browser → security mode

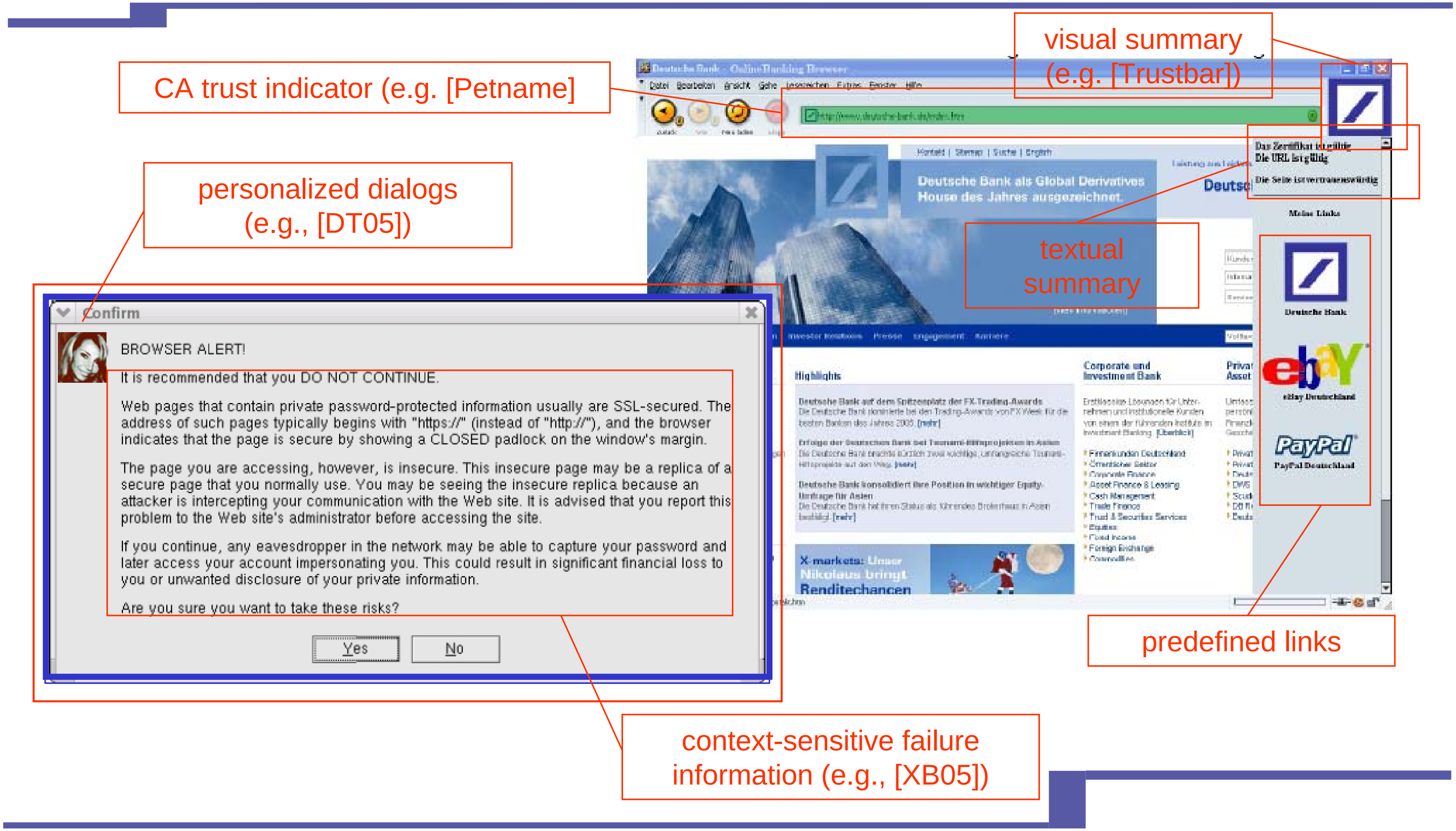


Candidate Solution I: Secure Mode Browser

Security Mode

- Limit the functionality → “zero-footprint”
  - User should always be aware of “what he sees is what he gets”
  - Does not solve completely phishing problem
  - Domesticates the “tools” of illusion attacks
- Non-cryptographic presentation of SSL
  - Laymen should understand SSL (e.g., [Trustbar], [Petname])
- Context-sensitive presentation of security indicators
  - Clearly highlight security alerts
  - Reduce amount of failure alerts
  - Deploy empirical results of, e.g., [XB05]
- Highlight the trustworthiness of certificate authorities
  - Today more than 70 root certificates are installed in a standard browser
  - Equally treated, but issue polices different

Example of "Online-Banking Browser"



CA trust indicator (e.g. [Petname])

visual summary (e.g. [Trustbar])

personalized dialogs (e.g., [DT05])

textual summary

predefined links

context-sensitive failure information (e.g., [XB05])

Confirm

BROWSER ALERT!

It is recommended that you DO NOT CONTINUE.

Web pages that contain private password-protected information usually are SSL-secured. The address of such pages typically begins with "https://" (instead of "http://"), and the browser indicates that the page is secure by showing a CLOSED padlock on the window's margin.

The page you are accessing, however, is insecure. This insecure page may be a replica of a secure page that you normally use. You may be seeing the insecure replica because an attacker is intercepting your communication with the Web site. It is advised that you report this problem to the Web site's administrator before accessing the site.

If you continue, any eavesdropper in the network may be able to capture your password and later access your account impersonating you. This could result in significant financial loss to you or unwanted disclosure of your private information.

Are you sure you want to take these risks?

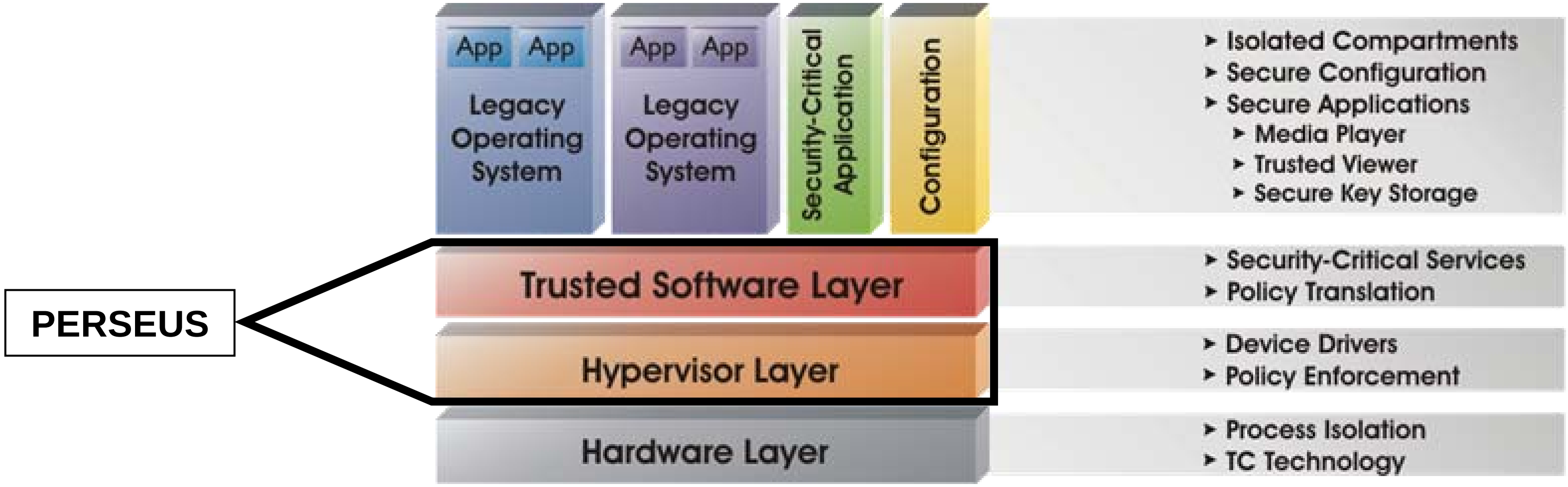
Yes | No

Deutsche Bank - Online-Banking Browser
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Fenster Hilfe
http://www.deutsche-bank.de/index.htm
Das Zertifikat ist gültig
Die URL ist gültig
Die Seite ist vertrauenswürdig
Meine Links
Deutsche Bank
eBay Deutschland
PayPal Deutschland
Deutsche Bank als Global Derivatives House des Jahres ausgezeichnet.
Highlights
Corporate und Investment Bank
X-markets: Unser Nikolaus bringt Renditechancen

Candidate Solution II: PERSEUS

Security Architecture against Malwared Phishing

- Software-based security kernel (secure operating system)
- Trusted Computing (TC) functionalities
  - More and more vendors integrate a Trusted Platform Module (TPM)
- Provides elementary security properties (e.g., trusted channels, process isolation)
- PERSEUS: A generic security architecture

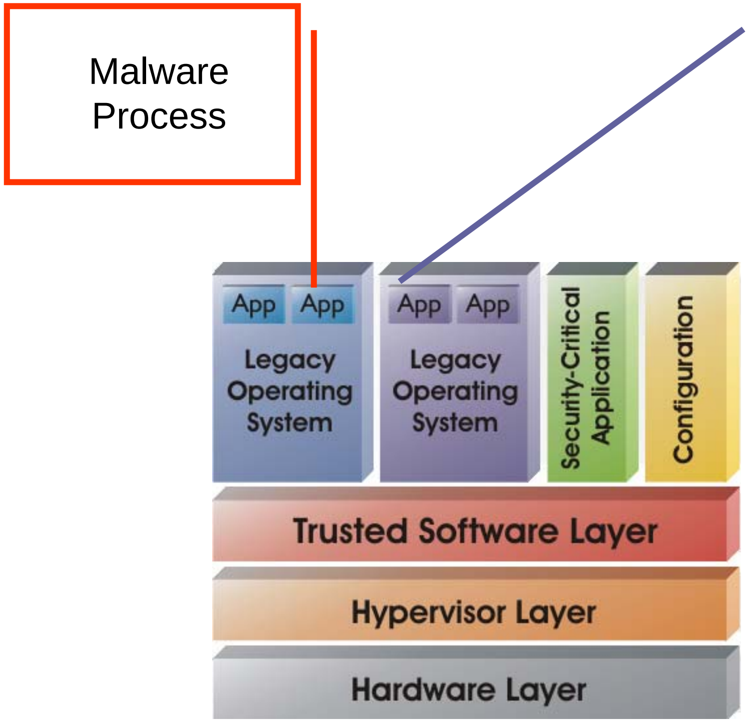


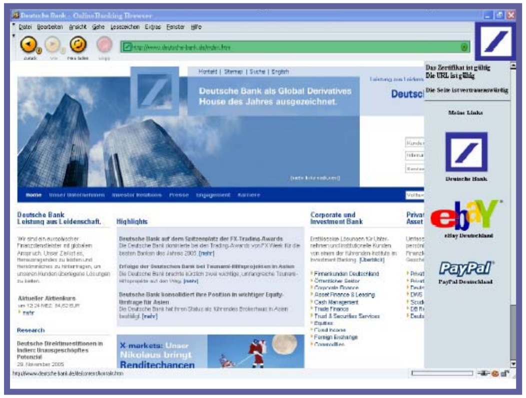
Candidate Solution II: PERSEUS

- Hypervisor Layer
  - Abstraction of underlying hardware (e.g., CPU, interrupts)
  - Offer an appropriate management interface
  - Enforce resource-based access control policy
- Trusted Software Layer
  - **Trusted GUI** secure path to applications (identify applications and thus protects against Trojan horse attacks like faked dialogs)
  - **Application Manager** enforces a security policy defining the applications that are allowed to be executed, measures the application’s integrity
  - **Trust Manager** creates and certifies keys bounded to applications
  - **Storage Manager** enables other applications to persistent store their states and data

Candidate Solution I+II

PERSEUS instantiations can be used to run (para-) virtualized legacy operating system (currently Linux)




Deutsche Bank - OnlineBanking Browser
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Fenster Hilfe
http://www.deutsche-bank.de/index.htm
Kontakt | Sitemap | Suche | English
Home Unser Unternehmen Investor Relations Presse Engagement Karriere
Meine Links
Deutsche Bank
eBay Deutschland
PayPal Deutschland

Das Zertifikat ist gültig
Die URL ist gültig
Die Seite ist vertrauenswürdig

Deutsche Bank als Global Derivatives House des Jahres ausgezeichnet.

Deutsche Bank
Leistung aus Leidenschaft.

Highlights

Deutsche Bank auf dem Spitzenplatz der FX-Trading-Awards

Erfolge der Deutschen Bank bei Tsunami-Hilfsprojekten in Asien

Deutsche Bank konsolidiert ihre Position in wichtiger Equity-Umfrage für Asien

Corporate und Investment Bank

Research

X-markets: Unser Nikolaus bringt Renditechancen

run web browser in an isolated environment (compartment)!!!

Summary

Proof-of-Concept for Online-Banking on-going

Challenges we face

- User-friendly presentation of a trusted compartment
- Policies how to automatically activate a new compartment
- Secure and efficient migration of compartments

For more information see www.prosec.rub.de

Thank you!

Candidate Solution I

Sebastian Gajek

sebastian.gajek@nds.rub.de

Candidate Solution II

Ahmad-Reza Sadeghi

sadeghi@crypto.rub.de

References

[DT05] Rachna Dhamija and J.D. Tygar: *The Battle Against Phishing: Dynamic Security Skins*.In: ACM Symposium on Usable Security and Privacy, 2005.

[GPS05a] Thomas Groß, Birgit Pfitzmann, and Ahmad-Reza Sadeghi. *Browser model for security analysis of browser-based protocols*. In: European Symposium on Research in Computer Security, 2005.

[GPS05b] T. Groß, B. Pfitzmann, and A.-R. Sadeghi. *Proving a WS-Federation requestor profile with a browser model*. In: ACM Workshop on Services (SWS), 2005.

[MSS98] John C. Mitchell, Vitaly Shmatikov und Ulrich Stern:. *Finite-State Analysis of SSL 3.0*. In: 7th USENIX Security Symposium, 1998.

[Perseus] PERSEUS Project Page: http://www.perseus-os.org/

[Petname] Ka-Ping Yee: *Designing and Evaluating a Petname Anti-Phishing Tool*. 2005

[PSW00] Birgitt Pfitzmann, Matthias Schunter and Michael Waidner: *Secure Reactive Systems*. IBM Technical Report RZ 3206, May 2000.

[Trustbar] A. Herzberg and A. Gbara. TrustBar: *Protecting (even Naive) Web Users from Spoofing and Phishing Attacks*. IACR Cryptology ePrint Archive, 2004.

[WS96] David Wagner und Bruce Schneier. *Analysis of the SSL 3.0 Protocol*. In: 2nd USENIX Workshop on Electronic Commerce Proceedings, 1996.

[XB05] Haidong Xia and Jose Carlos Brustoloni: *Hardening Web Browsers Against Man in the Middle and Eavesdropping Attacks*. In: International World Wide Web Conference Committee, 2005