Web-Authentifizierung
mit
OpenID

Seminar KvBK
Sommersemester 2010

Martin Russer
martin.russer@informatik.stud.uni-erlangen.de

14.Juli 2010

Motivation


ebay
myspace.com
(16)
WEB.DE
Jabber
(6)
YouTube
WordPress
studiVZ
DAS STUDIVERZEICHNIS
(17)
(10)
(12)
skype
OpenID
(18)
Google
Mail
(9)
MyVideo
(13)
twitter
msn
(7)
facebook
(14)
amazon.de
(3)
Blogger
(11)
(15)

Motivation (2)

- Problem:
  - unzählige Logins
  - unterschiedliche Passwörter

- Wunsch:
  Ein Login für viele Webseiten bzw. Webdienste
  → sog. „Single-Sign-On“

- Lösungsansatz:
  z.B. mit OpenID

(18)

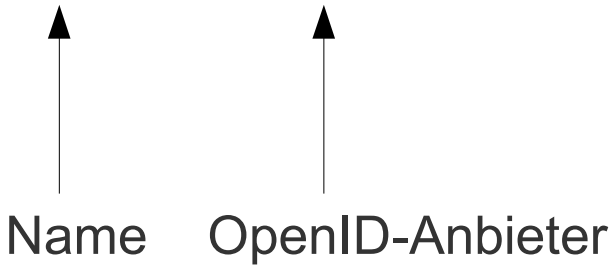
Gliederung

- Motivation
- OpenID
  - „Was ist OpenID?“
  - Komponenten
  - Funktionsweise
  - Integration bei einer Registrierung
  - Spezifikationen
  - Sicherheit & Kritik
- Vergleich: OpenID und OAuth
- Zusammenfassung
- Quellen

„Was ist OpenID?“

- Dezentrales Authentifizierungssystem
- URL-basierte Identität („Identifier“)
  - Beispiel:

    `https://mueller.myopenid.com`



- 2005 von Brad Fitzpatrick entwickelt
- seit 2007 Vermarktung durch OpenID-Foundation

- Aktuelle Version: OpenID 2.0

Komponenten

- **End-Benutzer / End-User**

  Person, die sich bei einer Webseite anmelden möchte.

  Bsp: Herr Müller

- **Konsument / Relying Party**

  Webseite, auf die ein End-Benutzer zugreifen möchte.

  Bsp: zooomr.com, sourceforge.net, livejournal.com

- **OpenID-Anbieter / OpenID-Provider**

  URL-basierter Authentifizierungsdienst

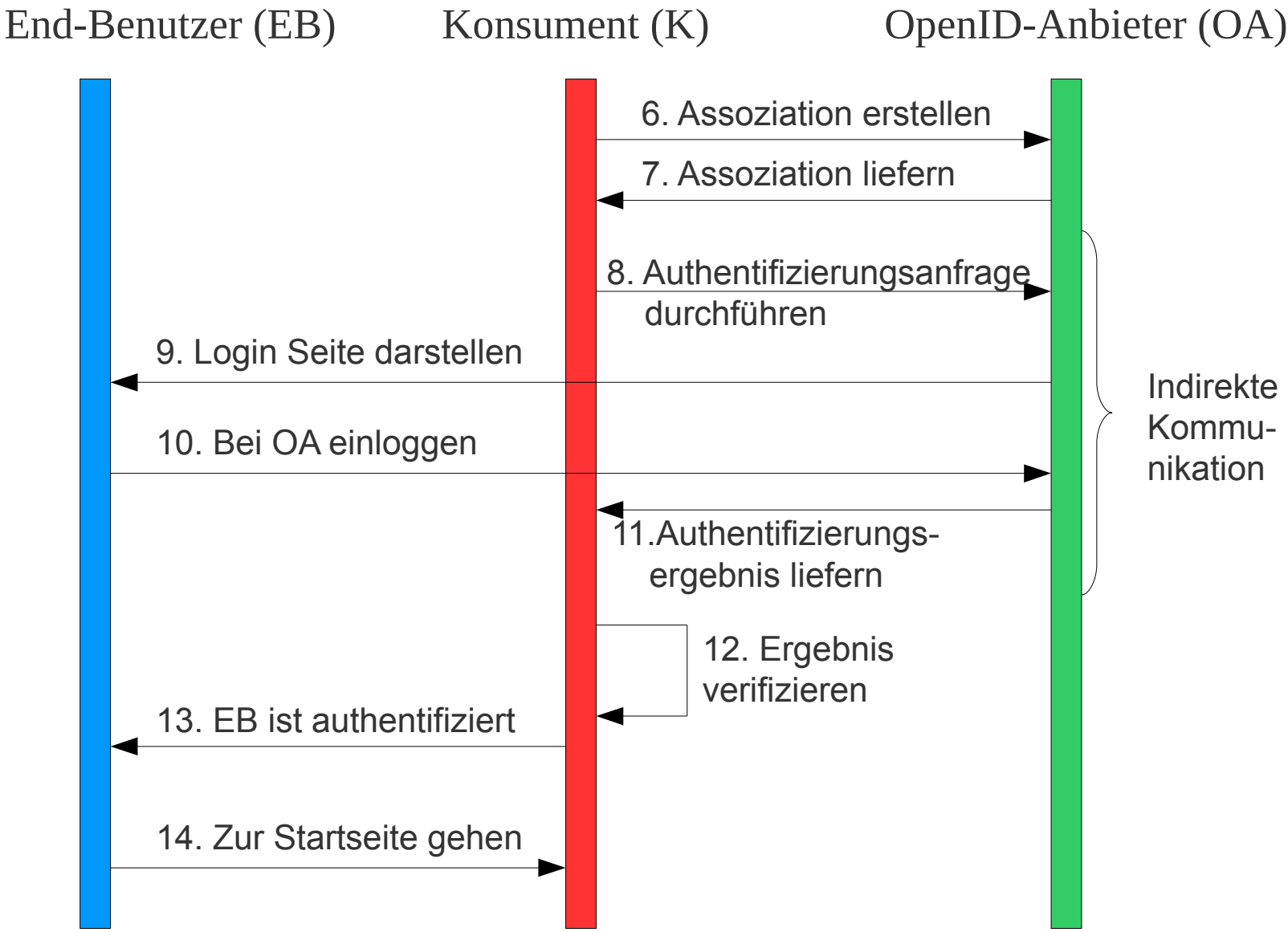
  Bsp: myopenid.com, verisignlabs.com, google.com, myspace.com, yahoo.com

Funktionsweise (1)

End-Benutzer (EB) Konsument (K) OpenID-Anbieter (OA)

(19)

Funktionsweise (2)



Integration bei einer Registrierung

- Problem:

  Nachträgliches Erstellen eines OpenID-Kontos, obwohl bereits Accounts bei Konsumenten bestehen.

- Lösung:

  Verknüpfung von Konten

Integration bei einer Registrierung (2)

Konsument

Konto vorhanden K. nicht vorhanden

Prozess A - - Registrierungsprozess durchführen - Konten verknüpfen	Prozess D - - OpenID-Konto erstellen - Prozess A ausführen
Prozess B - - Konten verknüpfen	Prozess C - - OpenID-Konto erstellen - Prozess B ausführen

Konto vorhanden Konto nicht vorhanden

OpenID-Anbieter

Spezifikationen von OpenID

Folgende Spezifikationen wurden festgelegt:

- OpenID Authentication 1.0/2.0

  Authentifizierungsspezifikation, Hauptteil im Open-ID Protokoll

- OpenID Provider Authentication Policy Extension (PAPE)

  Festlegung der Authentifizierungsart eines Nutzers bei einem OpenID-Anbieter

- OpenID Assertion Quality Extension

  Überprüfung der Attributsqualität

Spezifikationen von OpenID (2)

Folgende Spezifikationen wurden festgelegt:

- OpenID Simple Registration Extension 1.0 (SReg)
  Austausch von Identitätsattributen
  - openid.sreg.nickname
  - openid.sreg.email
  - openid.sreg.fullname
  - openid.sreg.dob
  - openid.sreg.gender
  - openid.sreg.postcode
  - openid.sreg.country
  - openid.sreg.language
  - openid.sreg.timezone

Spezifikationen von OpenID (3)

Folgende Spezifikationen wurden festgelegt:

- OpenID Attribute Exchange

  Austausch von Identitätsattributen wie bei SReg, jedoch...
  - ...Attributanzahl unbegrenzt
  - ...Attribute erweiterbar
  - ...Attribute selbst definierbar
  - ...Attribute je nach Webseite/Webdienst auswählbar

  Seit OpenID 2.0 implementiert

  → Ersetzt und erweitert damit SReg

Sicherheit & Kritik

„**Phishing** [f] werden Versuche genannt, über gefälschte WWW-Adressen an Daten eines Internet-Benutzers zu gelangen.“

Leistung aus Leidenschaft.

Deutsche Bank

Sehr geehrte Kundin, sehr geehrter Kunde,

Der technische Dienst der Bank fuhrt die planmassige Aktualisierung der Software durch Fur die Aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.

https://meine.deutsche-bank.de/mod/WebObjects/dbpbc.woa/407/wo/confirm.asp

Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.

Wir bitten um Verstandnis und bedanken uns fur die Zusammenarbeit

(20)

Sicherheit & Kritik (2)

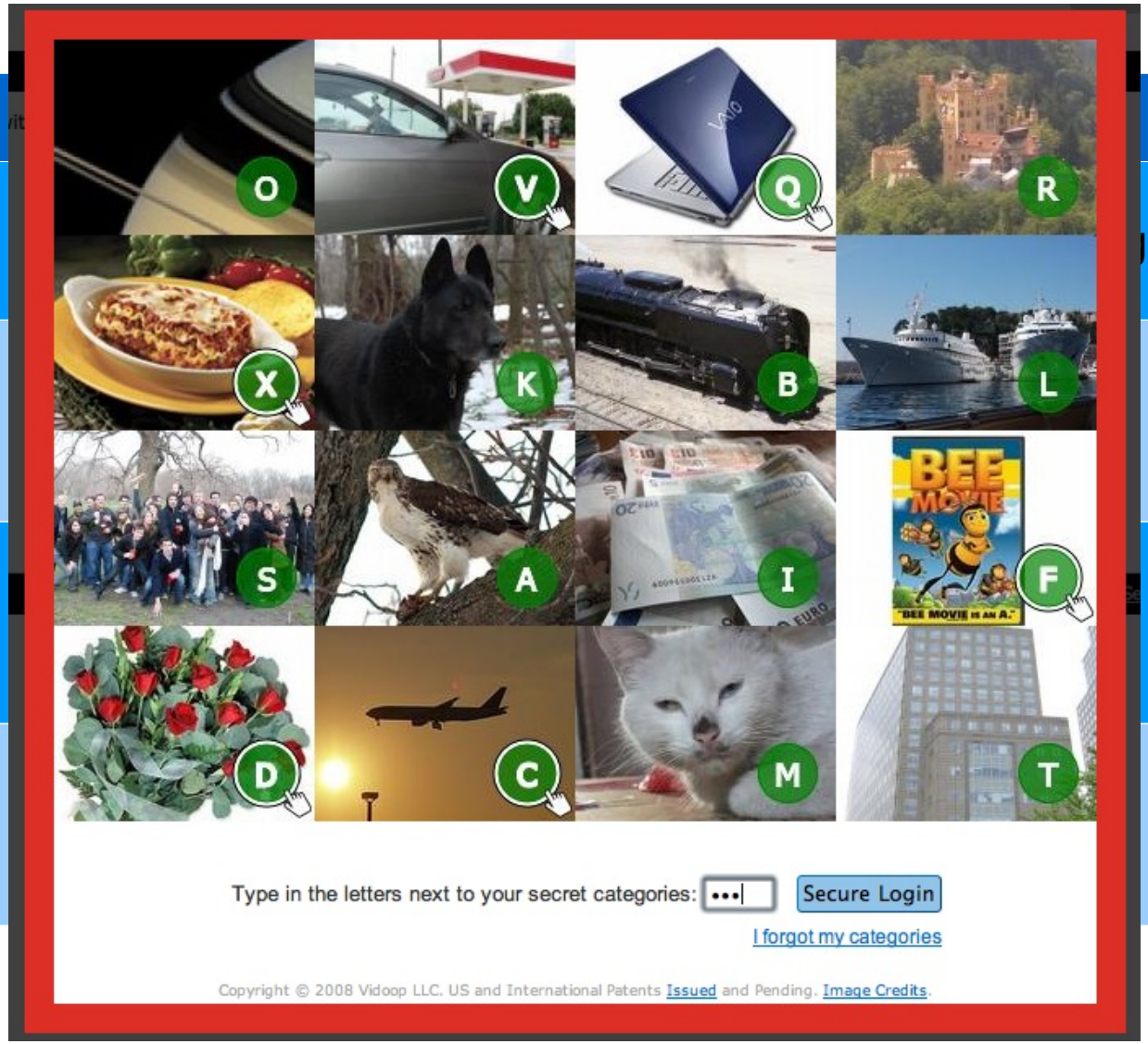
- Problem:

  Weiterleitung an eine „falsche“ OpenID-Login Seite und Abgreifen der Benutzerdaten

- Lösung:

  Spezielle Sicherheitsgewährleistungen der OpenID-Anbieter

Sicherheit & Kritik (3)



Sicherheit & Kritik (4)

- Phishing Gefahr:
  unsichere Authentifizierungsmethode
  → OpenID-Anbieter Blacklist
- Speicherung von Bewegungsdaten möglich
- Volles Vertrauen in den OpenID-Anbieter notwendig

Gliederung

- Motivation
- OpenID
  - „Was ist OpenID?“
  - Komponenten
  - Funktionsweise
  - Integration bei einer Registrierung
  - Spezifikationen
  - Sicherheit & Kritik
- **Vergleich: OpenID und OAuth**
- Zusammenfassung
- Quellen

Vergleich: OpenID & OAuth

- Wiederholung:

  OAuth:

  ...gewährt eingeschränkten Zugriff auf eigene private Ressourcen, ohne eigene Identität / Credentials zu verraten.

- OpenID:

  ...gewährt Zugriff auf Webseiten / Webdienste mit einer einzigen Identität

Vergleich: OpenID & OAuth (2)

- Gemeinsamkeiten:
  - Anwendungsfeld:
    Sicherheit und Identität im Web
  - „dezentralisiert“
  - Weiterleitung zum OpenID-Anbieter
  - „zentrale Kontrolle“

Vergleich: OpenID & OAuth (3)

- Unterschiede:

  Zweck:
  - OpenID:

    Authentifizierung
  - OAuth:

    Autorisierung

- Idee:

  Verwendung beider Dienste!

Zusammenfassung

- Problem: unzählige Logins im Web
- OpenID:
  dezentrales Authentifizierungssystem
  → ein Login (Identifier) für mehrere Webseiten
  → Weiterleitung beim Login
  → Sicherheit durch spezielle Loginverfahren
- OAuth: Autorisierung

Quellen - Bilderverzeichnis

(1) - http://www.rechenzentren-bayern.de/liste/rrze-logo-154x60.gif
(2) - http://localdemocracy.f les.wordpress.com/2009/06/ebay-logo.jpg
(3) - http://www.ahmadmesgarha.de/2008/uea/html/images/amazon-de-logo_000.jpg
(4) - http://www.djf av.de/main/kontakt/icq%20animated.GIF
(5) - http://www.mediaversand.de/blog/wp-content/uploads/2010/02/skype_logo.png
(6) - http://www.ingeeker.com/images/gallery/linux-logo/jabber_logo_2.jpg
(7) - http://www.pycomall.com/images/P/msn.jpg
(8) - http://www.poolstar.de/gomrecords/webde_logo.png
(9) - http://www.icetea.co.uk/images/news/google_mail.gif
(10) - http://livinglines.at/coachit/f les/2009/03/wordpress-logo-stacked-rgb.png
(11) - http://www.revitcomponents.com/userf les/265-blogger-logo.jpg
(12) - http://www.umwelttechnik.ws/bfs_09/Meine%20Homepage%20ali%20ce/image/youtube_logo.jpg
(13) - http://moritzbollf lms.de/media/Bilder/myvideo_logo.png
(14) - http://www.tepperis.com/nachhilfe/assets/images/Twitter-Logo.png
(15) - http://www.wvwc.edu/campus/cab/assets/facebook-logo.jpg
(16) - http://original-g.ch/enter/images/stories/myspace_logo.jpg
(17) - http://www.rankopedia.com/CandidatePix/61530.gif
(18) - http://www.jedinet.com/wp-content/uploads/2008/05/openid_big_logo_text.png
(19) – Screenshot: www.zooomr.com, aufgenommen: 21/06/2010
(20) - http://de.academic.ru/pictures/dewiki/80/Phishing.gif
(21) - http://shif ett.org/img/vidoop-image-shield.png

Quellen

[heise] – Artikel:“Identity Management: Authentifizierungsdienste mit OpenID“
Von Lofi Dewanto
Aufgerufen am 18/06/2010
http://www.heise.de/developer/artikel/Identity-Management-Authentifizierungsdienste-mit-OpenID-227202.html

[SASD] – Artikel: OAuth-OpenID: You’re Barking Up the Wrong Tree if you Think They’re the Same Thing“
Aufgerufen am 20/06/2010
http://softwareas.com/oauth-openid-youre-barking-up-the-wrong-tree-if-you-think-theyre-the-same-thing

[OPEN] - www.openid.net

[OAUTH] - www.oauth.net

[MR] – Artikel: „Netzweite Identitäten mit OpenID“
Von Martin Raepple
Aufgerufen am 20/06/2010
http://www.springerlink.com/content/755180g7h7741187/

[GRFOID] – Buch: „Get Ready For OpenID“
Von RAFEEQ UR REHMAN
Conformix Technologies Inc.

Quellen

[OID2.0] – Artikel: „OpenID 2.0 ist fertig“
Aufgerufen am 18/06/2010
http://www.golem.de/0712/56417.html

FRAGEN ???