ePA und OpenID

Konzept für eine Master-Thesis

It-sa Nürnberg 2009
MesseCampus, Halle 5, Auditorium
15. Oktober 2009

Sebastian Feld
feld (at) internet-sicherheit (dot) de

Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
Fachhochschule Gelsenkirchen

Grundsätzliches

- Motivation
  - „Web statt Windows“
  - Passwort-Dilemma
  - Identität im Web
- OpenID
  - Web Single Sign-on
  - Dezentraler Mechanismus
  - Identitätsverwalter frei wählbar
  - URL-“Besitz“ bestimmt Identität
  - Akteure: Anwender, ID-Provider, Dienst

OpenID: Login-Ablauf

- Ganz grob …
  - 1. Login-Formular mit OpenID füllen
  - 2. Benutzer wird zum ID-Provider weitergeleitet
  - 3. Tatsächlicher Login beim ID-Provider
  - 4. ID-Provider bestätigt dem Dienst die Identität
- Anders ausgedrückt
  - 1. Dienst: „Ja, bitte?“ - Ich: „Ich bin's, Sebastian!“
  - 2. Dienst: „Kannst du es beweisen?“
  - 3. Ich: „Hier ist Sebastian, Passwort lautet 'geheim'!“
  - 4. Provider: „Bestätige vorgegebene Identität!“

OpenID: Kritik und Probleme

- Größte Kritik
  - Bewegungsdaten der Nutzer
  - Erstellung von Bewegungsprofilen

  → ePA-gestützer, anonymer Ablauf (folgt)
- Größtes Problem: Phishing
  - Betrügerischer Dienst schickt Nutzer an gefälschten ID-Provider
  - Username/Passwort wird abgefangen

  → Authentifizierung mit Username, ePA und PIN

MA-Thesis: Ideen und Ziele

- Implementierung von OpenID in Kombination mit ePA
  - Sichere Anmeldung mittels ePA
    - Kein Username/Passwort

    → Phishing wird eliminiert
  - ePA-gestützter, anonymisierter Ablauf
    - Keine Möglichkeit zur Profilbildung

    → Nicht nur datenschutzkonform, sondern technisch nicht möglich (!?)
- Theoretische Auseinandersetzung
  - Erreichbarer Anonymisierungsgrad
  - Abschätzung der Sicherheit im Ablauf
  - Diskussion der Angriffsszenarien

ePA und OpenID

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Besuchen Sie uns in
Halle 5, Stand: 5-522

Sebastian Feld
feld (at) internet-sicherheit (dot) de

Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
Fachhochschule Gelsenkirchen

if(is) internet-sicherheit.