Systemy pojedynczego logowania (Single Sign-On)

Paweł Kaczorowski

Opiekun pracy: prof. dr hab. inż. Zbiegniew Kotulski

24 stycznia 2011

Plan prezentacji

1. Wprowadzenie
2. Motywacja
3. Zagrożenia
4. Prywatność
5. Przykładowe rozwiązania
6. Problemy

Wprowadzenie (1/3)

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Wprowadzenie (2/3)

- samodzielne implementwanie mechanizmów uwierzytelnienia jest trudne
- zalecane jest korzystanie z gotowych rozwiązań
- następstwa dziurawych mechanizmów:
  - przechwycenie sesji
  - kradzież hasła
  - kradzież tożsamości !!!

Wprowadzenie (3/3)

Pojedyncze logowanie (Single Sign-On)
Proces uwierzytelnienia podmiotu, który pozwala na jednokrotne wprowadzenie danych uwierzytelniających (np. login i hasło), a następnie na dostęp usług bez ponownego wprowadzania tych danych.

- jednokrotne logowanie
- brak potrzeby uwierzytelnienia do każdej usługi oddzielnie

Motywacja - Dlaczego stosować SSO?

Motywacja - Dlaczego stosować SSO?

- dużo haseł do wielu systemów = słabe hasła

Motywacja - Dlaczego stosować SSO?

- dużo haseł do wielu systemów = słabe hasła
- kosztowna infrastruktura, administracja (problem szczególnie w organizacjach)

Motywacja - Dlaczego stosować SSO?

- dużo haseł do wielu systemów = słabe hasła
- kosztowna infrastruktura, administracja (problem szczególnie w organizacjach)
- problem utraty uprawnień

Motywacja - Dlaczego stosować SSO?

- dużo haseł do wielu systemów = słabe hasła
- kosztowna infrastruktura, administracja (problem szczególnie w organizacjach)
- problem utraty uprawnień
- oszczędność czasu

Motywacja - Dlaczego stosować SSO?

- dużo haseł do wielu systemów = słabe hasła
- kosztowna infrastruktura, administracja (problem szczególnie w organizacjach)
- problem utraty uprawnień
- oszczędność czasu
- lepsze zarządzanie tożsamością

SSO - Zagrożenia

SSO - Zagrożenia

- "key to castle"

SSO - Zagrożenia

- "key to castle"
- single point of failure (DoS)

SSO - Zagrożenia

- "key to castle"
- single point of failure (DoS)
- ryzykowna wymiana danych uwierzytelniających pomiędzy stronami

SSO - Zagrożenia

- "key to castle"
- single point of failure (DoS)
- ryzykowna wymiana danych uwierzytelniających pomiędzy stronami
- syndrom Big Brothera

SSO, a prywatność (1/3)

PII - Personally identifiable information

- jednoznacznie wskazują na osobę
- mogą być użyte do stworzenia połączenia, kontaktu, lub zlokalizowaniu osoby której ta informacja dotyczy
- cechy i preferencje osoby

SSO, a prywatność (2/3)

Examples
National identifiers (e.g. passport number)
Customer number
Biometric identifier
Bank account or credit card number
Name
Gender
Date of birth
Home address
Personal telephone number
Personal e-mail address
IP address
Photograph or video identifiable to an individual
Trade-union membership
Sexual orientation
Criminal convictions or committed offences
Financial profile
Personal identification numbers (PIN) and passwords for financial accounts
Any information collected during health services
Disabilities
Racial or ethnic origin
Religious or philosophical beliefs
Age or special needs of vulnerable individuals
Personal or behavioural profile
Employees' salaries and human resources files
Any PII identified as such
Location derived from telecommunications systems
Product and service preferences
Personal interests derived from tracking use of internet web sites

SSO, a prywatność (3/3)

Dane osobowe

- chronione przez prawo
- cenne
- rzadko świadomie zarządzane

Systemy informacyjne

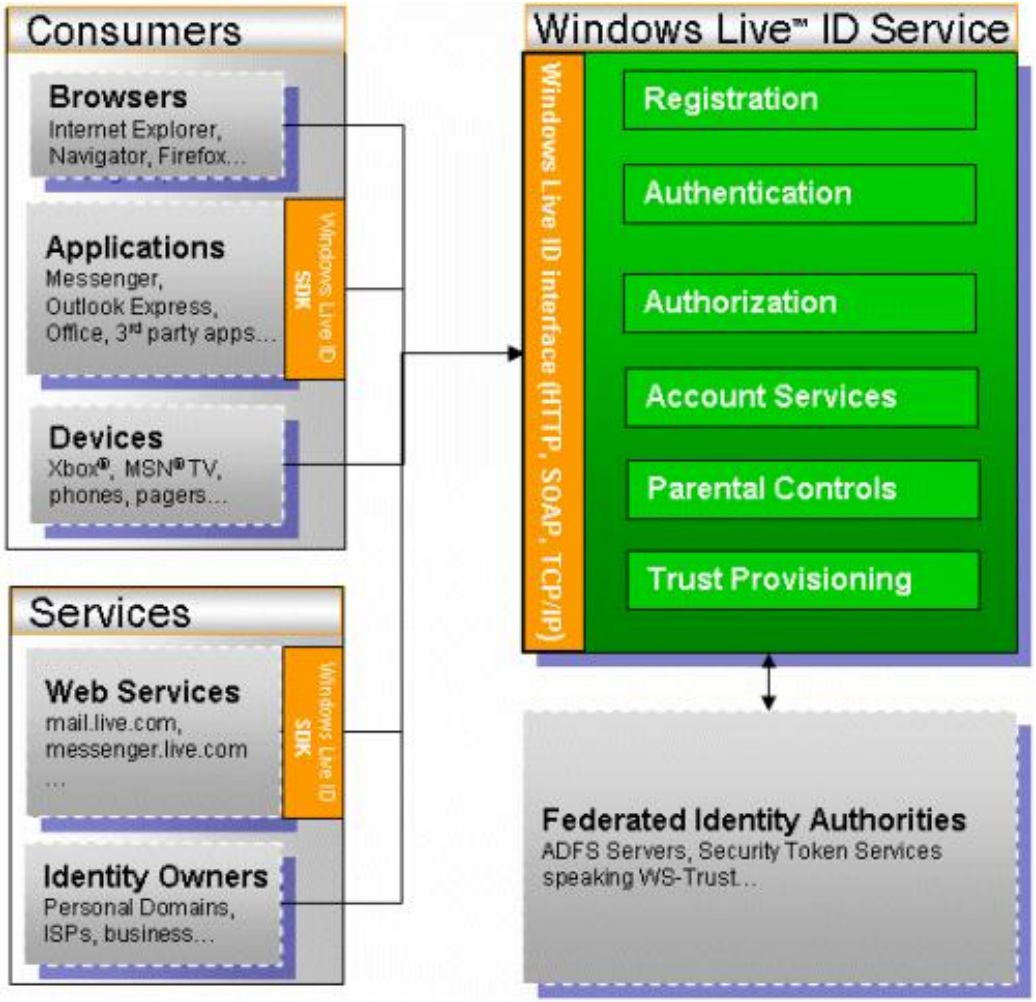
- zgodne z prawem przetwarzanie danych osobowych
- umożliwienie kontroli nad swoimi danymi

Stosowane rozwiązania

- w praktyce wiele Identity Providerów (IdP)
- wspólne wylogowanie (Single Sign-Off) - wylogowanie z jednej usługi powinno implikować wylogowanie ze wszystkich zalogowanych w ramach jednego IdP
- komunikacja za pomocą protokołu HTTP (Page Redirect , sniffing!)

Przykłady rozwiązań systemów SSO (1/4)

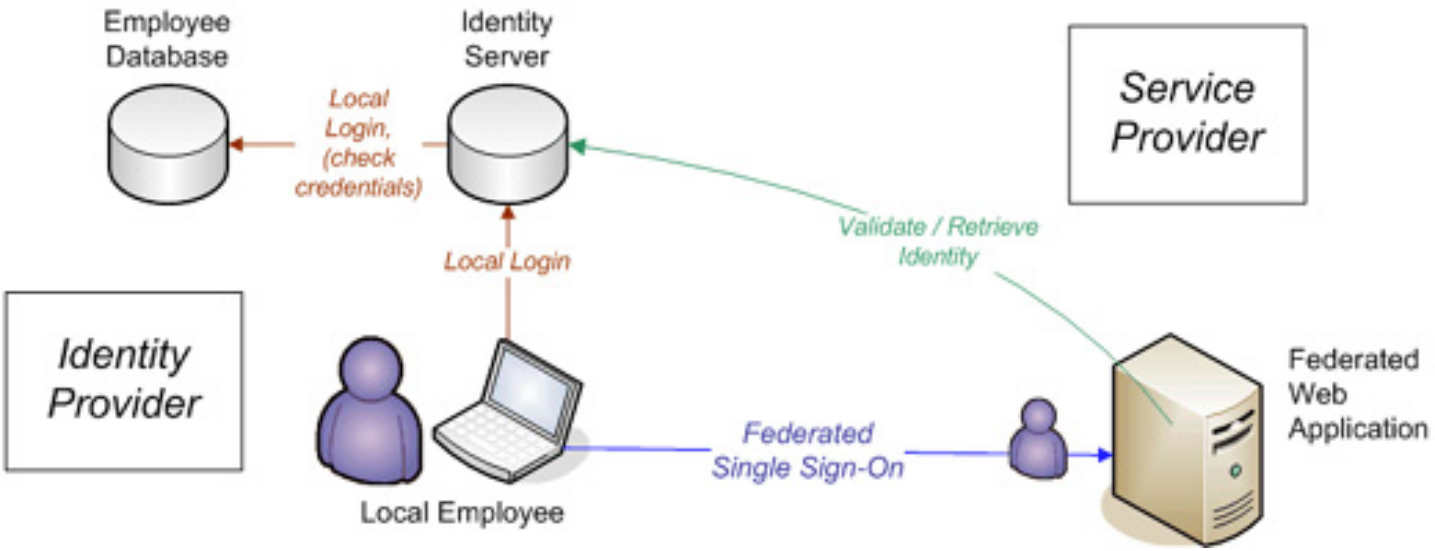
Windows Live ID



- zorientowane na produkty firmy Microsoft
- scentralizowane
- Windows Live ID Web Authentication SDK

Przykłady rozwiązań systemów SSO (2/4)

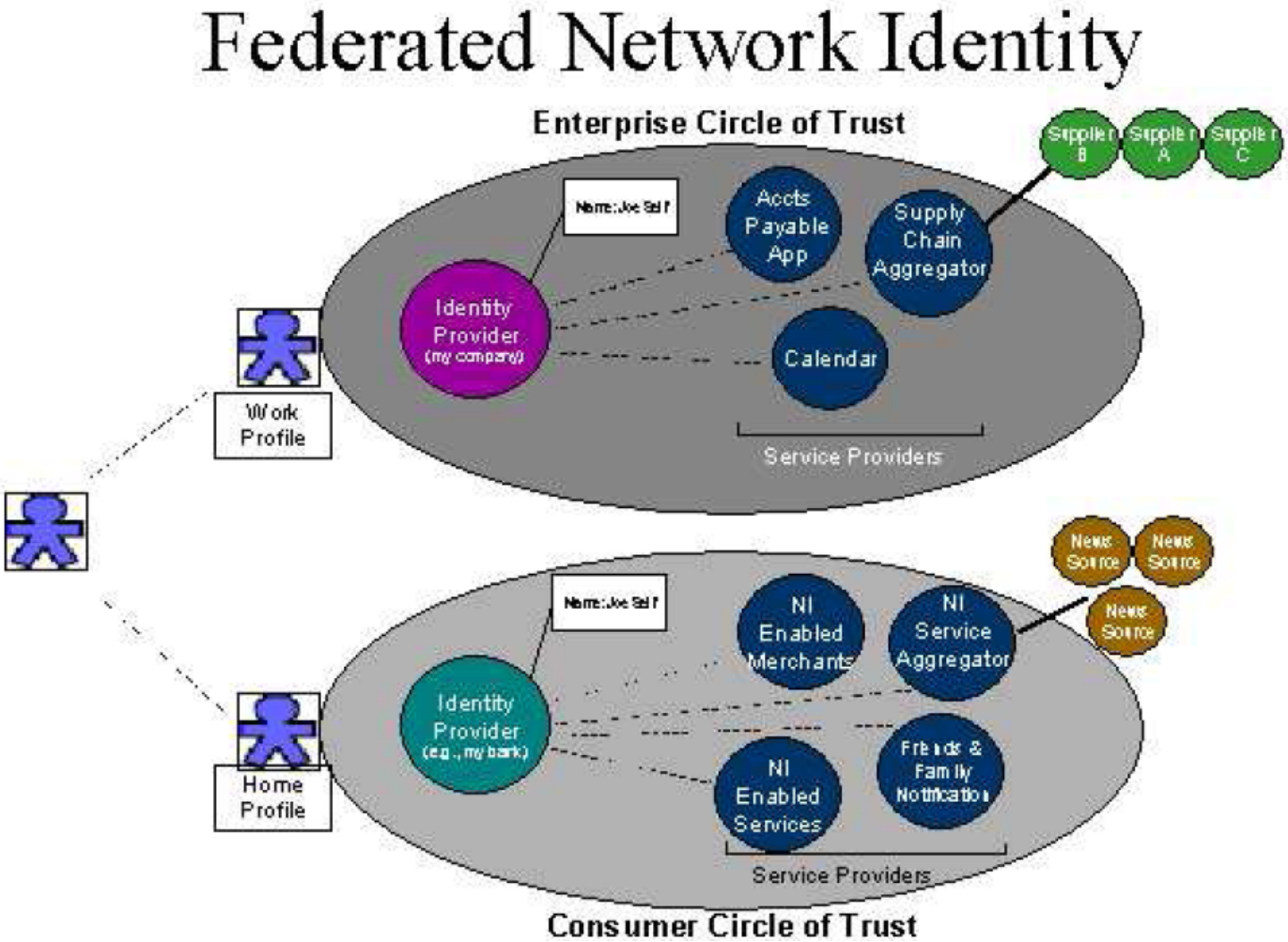
Liberty Alliance Identity Federation Framework



- Circle of Trust
- SAML (ang. Security Assertion Markup Language)

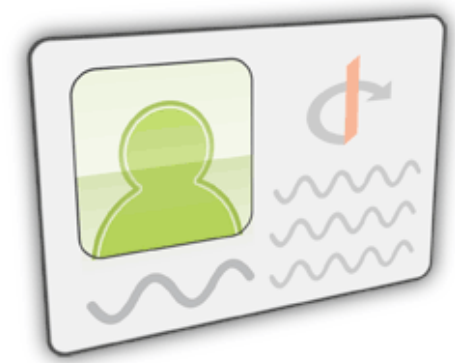
Przykłady rozwiązań systemów SSO (3/4)

Liberty Alliance Identity Federation Framework



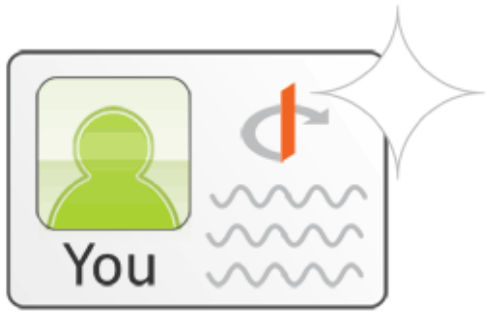
Przykłady rozwiązań systemów SSO (4/4)

Open ID



OpenID is a free and easy way to use a **single digital identity** across the Internet.

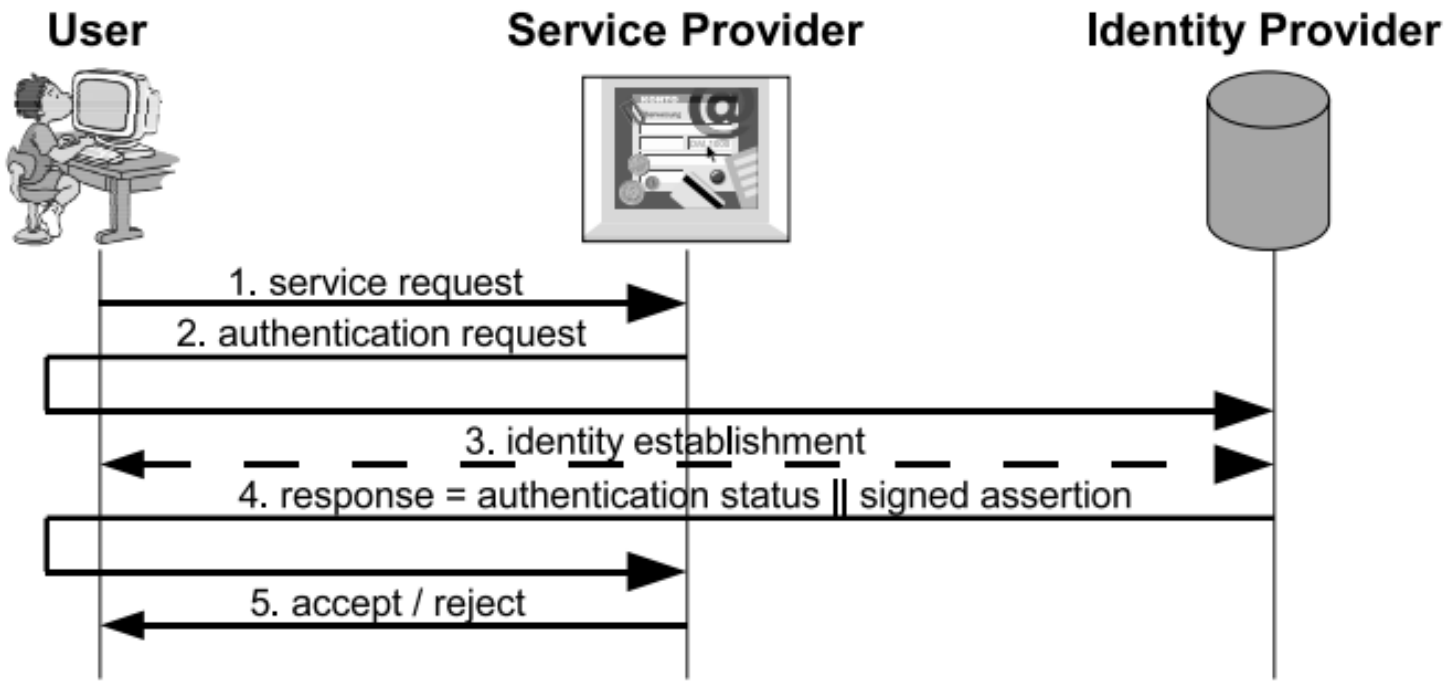
With one OpenID you can login to all your **favorite websites** and forget about online paperwork!



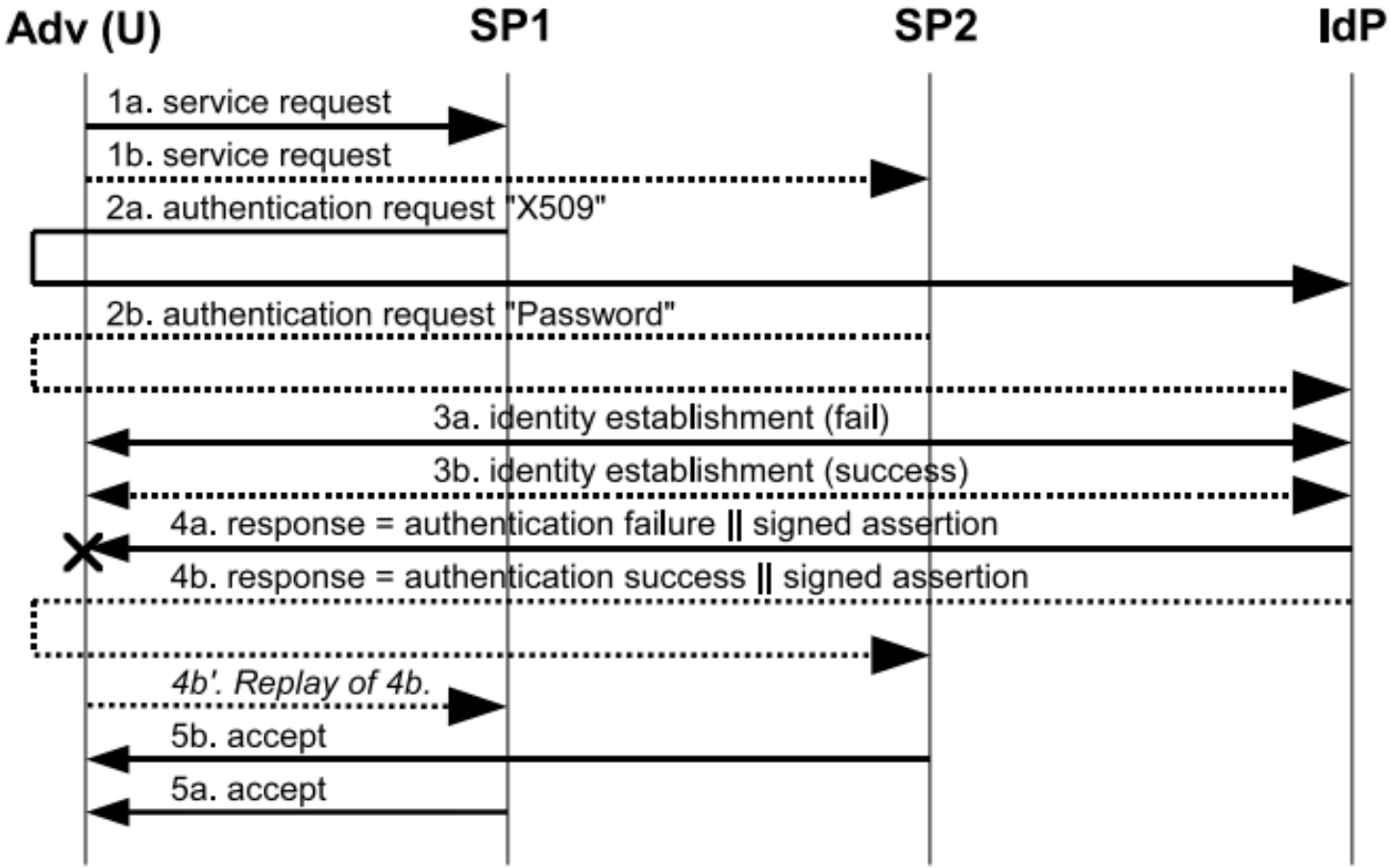
Now, you get to choose the login that's right for you. **Get an OpenID** today!

- decentralizacja - identyfikator jest równocześnie adresem serwera
- kontrola prywatności - użytkownik wskazuje, jakie informacje może pobrać serwis
- dużo IdP, a mało chętnych

Weakest Link Attack (1/2)



Weakest Link Attack (2/2)



Problemy

- W jaki sposób przypisywać poziom bezpieczeństwa dla poszczególnej usługi?
- Integracja z dostawcami usług (nieuczciwy dostawca, phishing).
- Kontrola prywatności.
- Stosowanie cookie (global cookie, local cookie, circle of trust z jednego DNS)
- URL Rewriting

Praca magisterska

1. Analiza rozwiązań.
2. Propozycje modyfikacji.
   - integracja systemu z dostawcą usług
   - profile prywatności
   - profile bezpieczeństwa
3. Implementacja prototypu.

Dziękuję za uwagę

Bibliografia

1. Yuen-Yan Chan, "Weakest Link Attack on Single Sign-On and Its Case in SAML V2.0 Web, COMPUTATIONAL SCIENCE AND ITS APPLICATIONS - ICCSA 2006 Lecture Notes in Computer Science, 2006 SSO".
2. "OWASP Top 10", 2010 The OWASP Foundation.
3." Liberty ID-FF Implementation Guidelines", Liberty Alliance Project.