Using a Smartphone to Access Personalised Web Services on a Workstation

Faysal Boukayoua
KaHo Sint-Lieven, Ghent

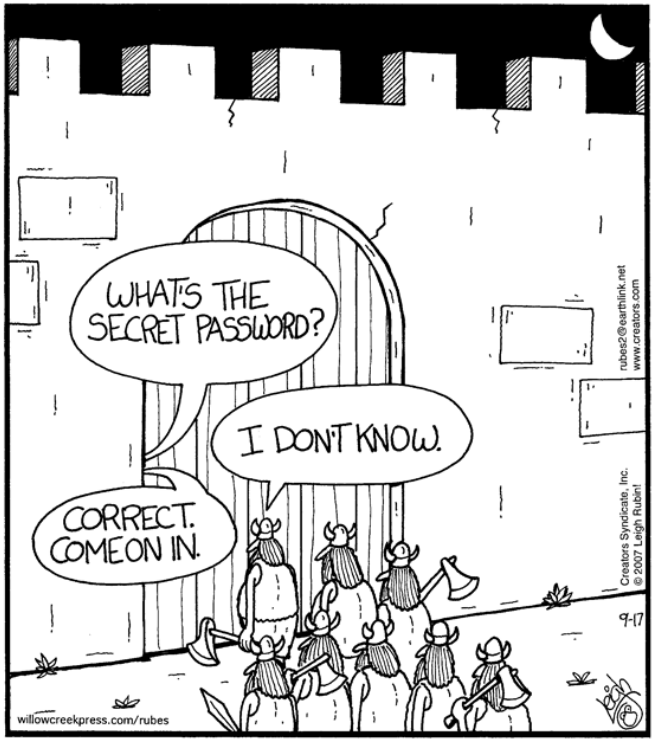
IFIP Summer school
Trento, 07/09/2011

Overview

- Motivation
- Application Overview
- Implementation
- Evaluation
  - Attacks
  - Comparison
- Future work

Motivation: Web authentication

Passwords



- Weak security
- Can be stolen by malware
- Human memory limitations
- No attribute provisioning

Motivation: Web authentication (2)

Smartcards



- Suitable hardware required
- Proliferation vs. usability
- Trust in workstation (PIN)

Motivation: Web authentication (3)

Security tokens





- Hardware cost
- Software tokens prone to malware
- Proliferation vs. usability
- No selective attribute disclosure

Motivation: Web authentication (4)

2-factor SMS authentication



- Password/token mgmt
- 2G GSM security questionable
- Part of credentials still malware-prone

Motivation: Web authentication (5)

Federated Identity Management





- Limited user control
- Identity provider can profile users
- One identity provider per user
- User impersonation
- Password/token mgmt

Motivation: recent trends



More mobility & more computers



Smartphones omnipresent



Mobile Internet penetration

Motivation: stakeholders

User



- Ubiquitous access to Web services
- Security & privacy
- Personalisation

Service provider



- Obtain reliable user info

Identity provider



- Provide reliable user info
- Authenticated provisioning

Interlude: QR codes

- What?
  - 2-dimensional barcodes
  - ~ 600 bytes of data
- Why?
  - Camera common in modern phones
  - Every workstation has a screen…



Application Overview



User



Trusted module



Workstation



Web Server

1. Go to Web service
2. Request Web service
3. Auth challenge (QR)
4. Auth challenge (QR scan)
5. Ask for consent
6. Review & give consent

alt

[consent given]

7. Mutually authenticate (out-of-band)
8. Confirm authentication

[else]

7. Abort

Implementation: trusted module







- Tamperproof
- Strong cryptography
- Secure credential storage

- Giesecke & Devrient Mobile Security Card SE 1.0

Implementation: trusted module (1)



- Trusted module is mediator between
  - Identity providers
  - Service providers
- Access to attributes controlled by
  - external authorities: certificates
  - user consent

Implementation: trusted module (2)

- Privacy properties
  - No profiling
    - by identity providers
    - by colluding providers
  - Access control to personal information
    - by audit authority
    - by user
  - No user impersonation



Implementation: mobile platform



- Samsung Galaxy S
- Android 2.2.1
- 3G connection
- Trusted module in SD card slot

Implementation: service provider







- Authentication valve as Tomcat filter
- No modifications, only extensions
- Required attributes list
- Secure, authentic channel with trusted module

Implementation: identity provider







- Simple webservice
- Attribute provisioning
- Secure authentic channel with trusted module

Evaluation: attack countermeasures

- Assumptions:
  - Trust in phone software while physically in presence of user
  - Access control & authorisation out of scope

Evaluation: attack countermeasures (1)



- MODEL 1: Physical control over phone.
  - Secure credential storage
  - Tamperproof trusted module
  - PIN authentication
  - Revocation

Evaluation: attack countermeasures (2)



- MODEL 2: malware controls workstation INCLUDING browser
  - Credentials stored on trusted module
  - Authentication out-of-band
  - Feedback on phone

Evaluation: attack countermeasures (3)



- MODEL 3: malware controls workstation EXCEPT browser
  - Credentials stored on trusted module
  - Authentication out-of-band
  - Feedback on phone

  - Malware cannot make user authenticate wrong session

Evaluation: attack countermeasures (4)



- MODEL 4: active and passive network eavesdropping

From	To	Channel
Workstation	Service provider	HTTP over TLS
Trusted module on phone	Service provider	Secure authentic channel
Trusted module on phone	Identity provider	Secure authentic channel

Evaluation: token comparison

	Password	Smartcard	Software token	Hardware token	Our solution
Strong security	No	Yes	Yes	Yes	Yes
Selective attribute disclosure	No	Typically not	No	No	Yes
Proliferation vs. usability					
Trust in workstation	Yes	Sometimes	Yes	No	No
Changes to workstation	No	Sometimes	Yes	No	No
Marginal hardware cost / new SP	Zero	>= 0	Zero	> 0	Zero

Evaluation: mechanism comparison

	Traditional authenti-cation	OpenID	Shibboleth	Windows Cardspace	Our solution
Multiple IDPs / user	No	No	No	Yes	Yes
Profiling by colluding IDPs & SPs	n/a	Yes	Yes	No	No
Phishing attacks	Yes	Yes	Yes	No	No
User-controlled attribute disclosure	No	No	Using plugin	Yes	Yes
Portability					

Future work

- Enforcement of trusted code in phone
- Standards interoperability
- Automate authentication decisions (policies)
- Integration in advanced Web apps
- Other short-range protocols
- Detailed performance statistics
- Registration, backup & revocation strategies

Questions?

