UNIVERSITÄT SIEGEN

Security of Online Social Networks

Lehrstuhl IT-Sicherheitsmanagment

Universität Siegen

April 19, 2012

Overview Lesson 02

Authentication

Web Login Implementation

- Common Fails

WebID

OpenID

Authentication

Authentication Classes

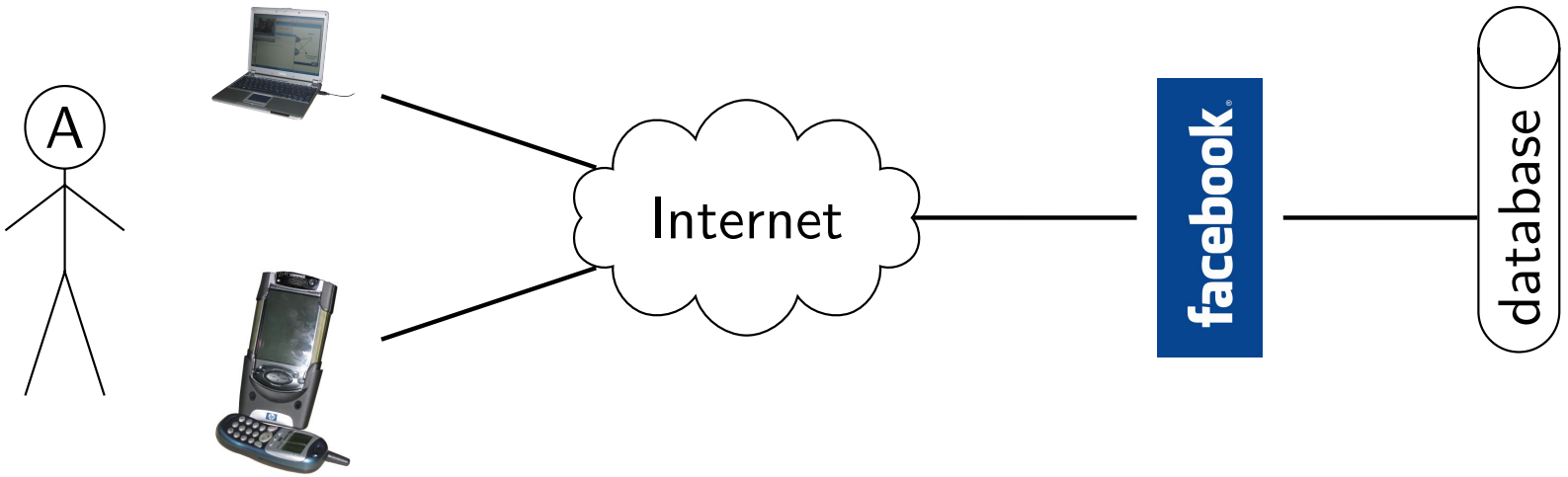
"Proof of Identity"

- Knowledge
- Ownership
- Biometric

Examples:

- Key(card)
- Password
- Iris
- Fingerprint
- Writing Dynamics

SNS Scenario



Authentication Subjects

- Person
- Agent/Process
- Computer
- Service (url)

Web Login Implementation

Overview

- Most often Uname/Passwd
- Web Formular
- Common Password Handling
  - repeated use of password
- see `https://www.owasp.org`

Standard Operation Procedure

1. Login Formular
   - Uname/Passwd/SessID
2. GET/POST Request
3. Reply Contains Session ID
4. Keeping the Session Safe

- depends on your Attacker Model.

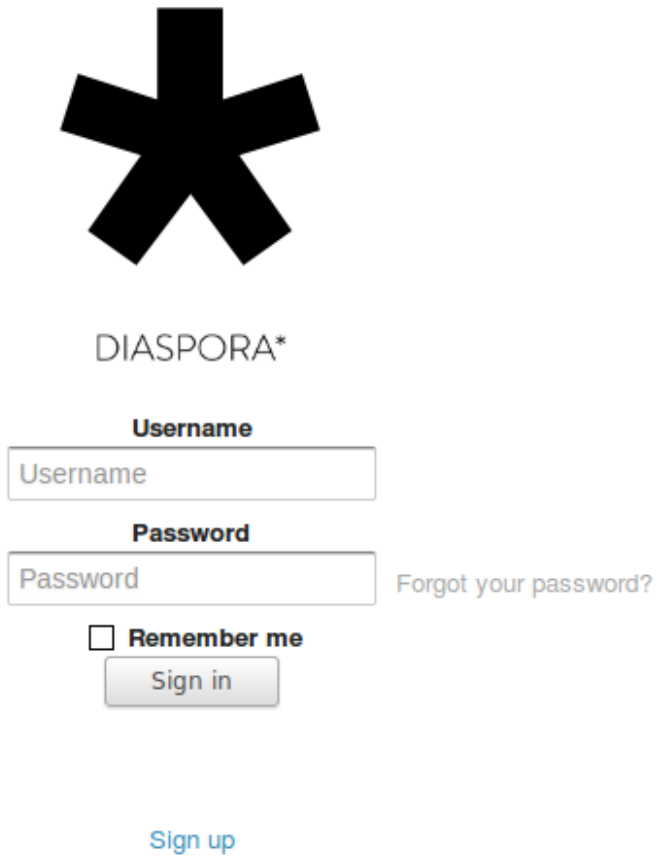
Attacker Models

Attacker Objectives:

- User Password
- Private Data
- Manipulation
- . . . ?

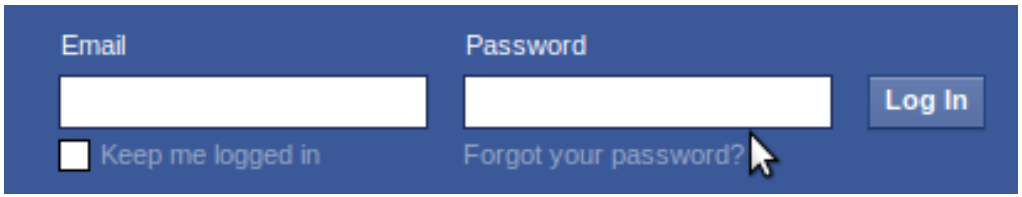
Attacker:

- Third Party (e.g. XSS)
- Network Operators
- OSN Provider
- . . .


DIASPORA*
Username
Username
Password
Password
Forgot your password?
Remember me
Sign in
Sign up

```
<form accept-charset="UTF-8" action="/users/sign_in"
      class="user_new" id="user_new" method="post">
  <input name="utf8" type="hidden" value="&#x2713;" />
  <input name="authenticity_token" type="hidden"
         value="g7yEV/17mKFopOpb0tjfIGTFcKKPoe8g6g7nwBTUoHc=" />

  <label for="user_username">Username</label>
  <input id="user_username" name="user[username]"
         placeholder="Username" size="30" tabindex="1" type="text" />

  <label for="user_password">Password</label>
  <input id="user_password" name="user[password]" placeholder="Password"
         size="30" tabindex="2" type="password" value="" />
  <a href="/users/password/new" id="forgot_password_link"
     tabindex="5">Forgot your password?</a>

  <input name="user[remember_me]" type="hidden" value="0" />
  <input id="user_remember_me" name="user[remember_me]" tabindex="3"
         type="checkbox" value="1" />
  <label for="user_remember_me">Remember me</label>

  <input id="user_submit" name="commit" tabindex="4" type="submit"
         value="Sign in" />
  <a href="/users/sign_up">Sign up</a>
</form>
```

Facebook Login



Facebook Login Messages

http://www.facebook....	GET	/?_fb_noscript=1	✔	☐	200	33062	HTML
https://www.facebook...	POST	/login.php?login_attempt=1	✔	☐	200	19935	HTML
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	19258	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1014...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1229...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1283...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	93457	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	89770	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1182...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1126...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1077...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1861...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1460...	
http://safebrowsing-c...	GET	/safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc...	☐	☐	200	1909...	

Facebook Login Request

```
POST /login.php?login_attempt=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:11.0) Gecko/20100101 Firefox/11.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.facebook.com/?_fb_noscript=1
Cookie: datr=WfGOTzEK_UszlQ4Z5peB3Bgm; lsd=AVp23RDa;
        reg_fb_gate=http%3A%2F%2Fwww.facebook.com%2F;
        reg_fb_ref=http%3A%2F%2Fwww.facebook.com%2F; noscript=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 219

lsd=AVp23RDa&email=keit2h.bbnoprsx%40safetymail.info&pass=XXXXXXXXXXXX
default_persistent=0&
charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%84&
timezone=&lgnrnd=095243_8Jab&lgnjs=n&locale=en_US
```

Facebook Login Response

```
HTTP/1.1 200 OK
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: Sat, 01 Jan 2000 00:00:00 GMT
P3P: CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"
Pragma: no-cache
X-Content-Security-Policy-Report-Only: allow *;script-src https://*.facebook.com http://
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Set-Cookie: datr=WfGOTzEK_UszlQ4Z5peB3Bgm; expires=Fri, 18-Apr-2014 16:53:29 GMT; path=/
Set-Cookie: reg_ext_ref=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; domain=.
Set-Cookie: reg_fb_ref=https%3A%2F%2Fwww.facebook.com%2Flogin.php%3Flogin_attempt%3D1; p
Content-Type: text/html; charset=utf-8
X-FB-Debug: fBYcu8Si/QaovM9ChJi/iUkicUKTvdf0AomcVOE4Eqw=
X-Cnection: close
Date: Wed, 18 Apr 2012 16:53:30 GMT
Content-Length: 18820

<!DOCTYPE html>
<html lang="en" id="facebook" class="no_js">
<head><meta charset="utf-8" /><script>function envFlush(a){function b(c){for(var d in a)
```

Common Fails

Insecure Transfer

- not using/dropping TLS
- Plaintext transfer in
  - URL
  - Request-Body
- Session ID in URL

Security Questions

- e.g. “Your mother’s maiden name.”
- The worst since “no password”
- see “WarGames” 1983
  - uname “Falken” pwd “Joshua”
  - Criticism:
    - public knowable
    - insufficiently non-random

[Wikipedia `File:Wargames.jpg`]

Telltale Errormessages

- Different for Username/Passwd
- Errordump contains userlist

Password Plaintext Storage

- Danger of Leakage (see Facebook)
- e.g. `http://www.skullsecurity.org/wiki/index.php/Passwords`
  - Facebook, Hotmail, MySpace, Hak5, ...

Session Fixation

- Attacker fixes Session ID
- e.g. malicious link `http://bad-o.sn/?sid=123454`

1. Set up trap-session
2. Transfer session to victim
3. Session Entrace

Best countermeasure:

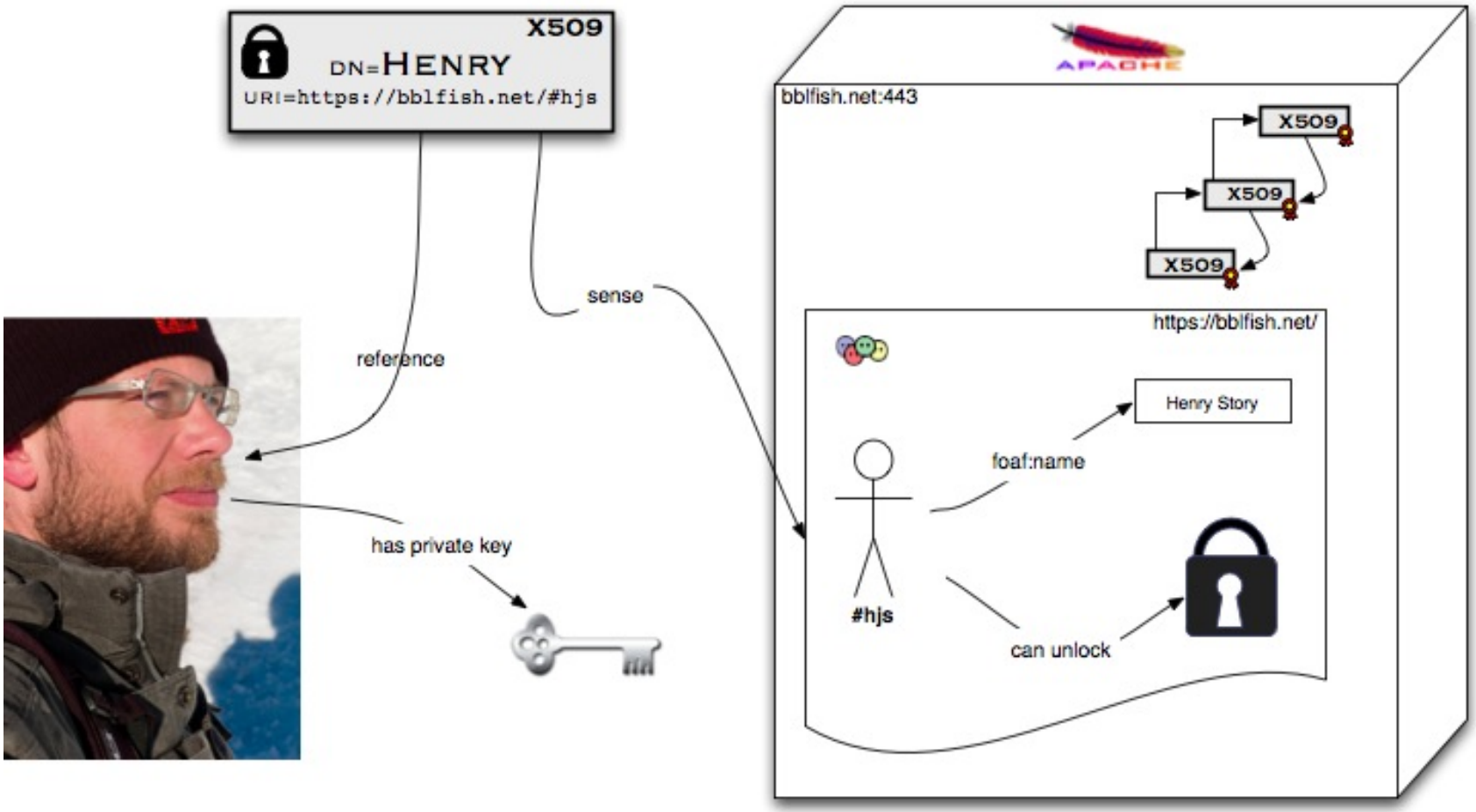
- change Session ID
  - during login
  - with each request

[See Kolsek 2002 [1]]

WebID

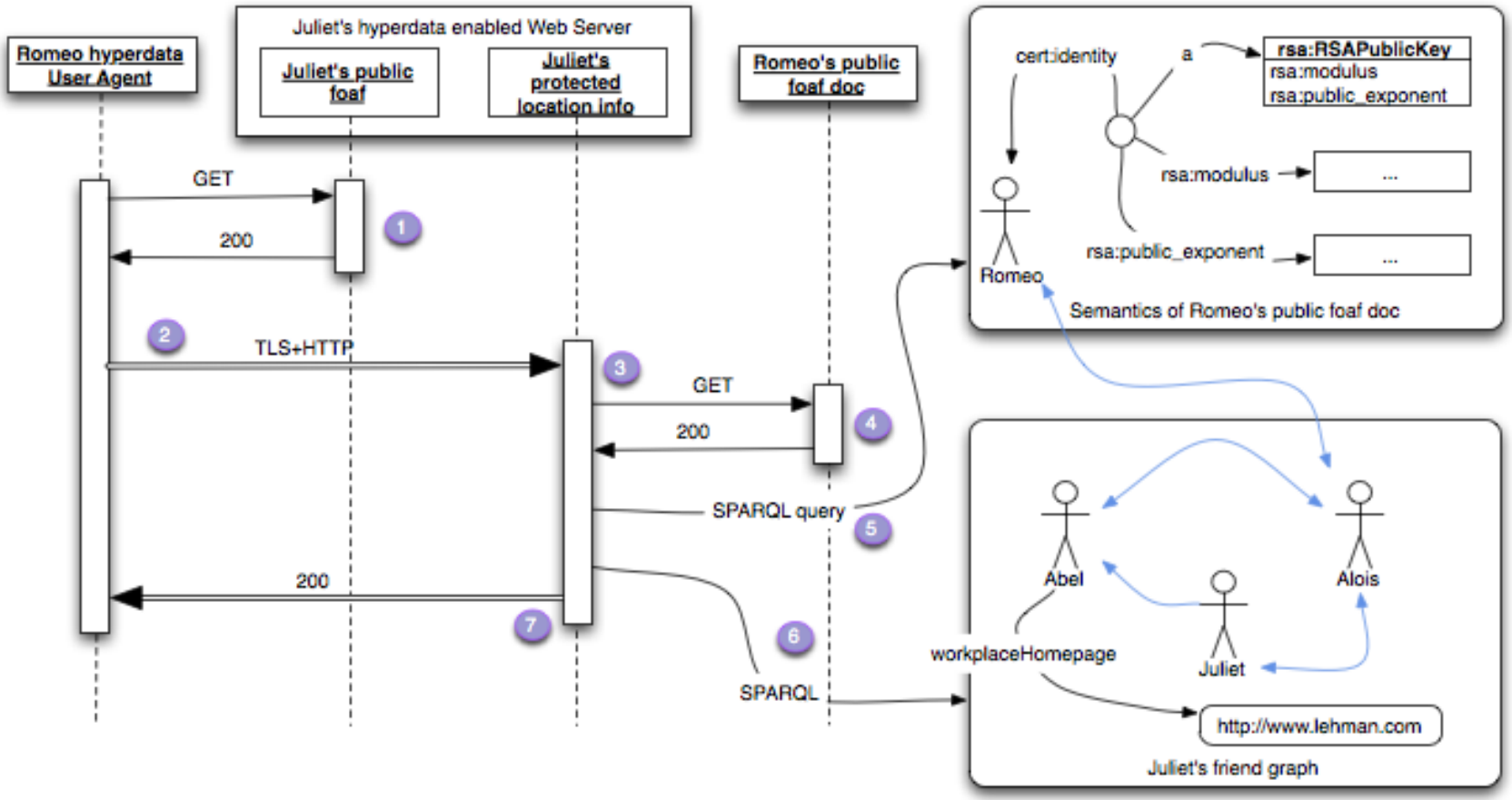
WebID Overview

- "WebID" Dan Brickley, Tim Berners-Lee (2000)
- URI defined identity
  - `http://danbri.org/foaf.rdf`
  - `http://www.w3.org/People/Berners-Lee/card.rdf`
  - `https://bblfish.net/#hjs`
- HTTP + SSL + RDF:FOAF
- WebID 1.0 — Web Identification and Discovery [2]



[http://www.w3.org/wiki/WebID]

Authentication Sequence



hfill[http://www.w3.org/wiki/Foaf%2Bssl]

Certificates

Bind Name to public key
X509 `http://tools.ietf.org/html/rfc5280`
Formats: PEM, PKCS#7, PKCS#12

X.509 Certificate I

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 207481227 (0xc5de98b)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Universitaet Siegen, OU=Zentrum fuer Informations- und Mediented
        Validity
            Not Before: May 29 08:40:27 2008 GMT
            Not After : May 28 08:40:27 2013 GMT
        Subject: C=DE, O=Universitaet Siegen, OU=ZIMT, CN=xims.uni-siegen.de
        Subject Public Key Info:
                                    ⋮
```

X.509 Certificate II

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:c4:c7:af:46:87:7b:90:89:76:bc:6b:45:02:52:
            2f:8d:54:da:68:c4:49:2b:4b:57:34:e9:c8:2f:4d:
            bc:b5:28:25:66:1c:e8:26:db:b6:7a:88:b4:4f:ac:
            2e:f5:a5:bd:92:93:51:09:f2:7e:96:b9:76:de:d5:
            a3:9b:e2:fb:81:46:a9:d9:3b:ac:51:40:1f:68:6a:
            b0:36:66:32:92:1b:14:74:08:77:c4:90:4a:54:19:
            63:57:fa:29:70:2f:a6:c0:6b:36:c6:00:eb:85:ea:
            90:c1:a1:50:aa:33:2b:db:e4:96:26:38:c1:e8:90:
            82:45:ea:bc:13:a4:21:3d:05:b3:be:79:8e:bb:c3:
            5b:51:96:c3:95:61:9f:b8:9f:ea:16:41:9e:c4:d6:
            b4:1e:43:eb:e9:ff:cc:24:88:e1:44:64:af:b0:90:
            9b:5f:77:1b:06:59:5d:0d:9a:0d:f5:e2:a4:7b:9b:
            b1:42:58:c9:af:a0:ee:d6:e8:56:e6:48:97:05:dd:
            80:97:40:08:cb:5e:7d:f1:ae:d2:05:c8:a3:67:1d:
            43:ba:d8:3e:af:aa:ed:cf:4f:11:59:3b:b4:c2:3a:
            dc:9a:6c:3e:1b:b6:c1:cd:d6:6d:bf:2c:cd:fc:b9:
            ea:cb:b9:ff:31:68:32:58:18:23:0e:a6:8f:6a:92:
            72:e7
        Exponent: 65537 (0x10001)
X509v3 extensions:
                        ⋮
```

X.509 Certificate III

```
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
    X509v3 Subject Key Identifier:
        D3:9D:F5:70:C7:E0:14:00:3A:C7:2F:2F:4E:01:AB:53:DA:1F:C0:77
    X509v3 Authority Key Identifier:
        keyid:FF:74:C2:69:3A:F0:84:9F:9C:02:93:CD:9F:9E:F7:DD:FF:01:C5:65

    X509v3 CRL Distribution Points:

        Full Name:
          URI:http://cdp1.pca.dfn.de/uni-siegen-ca/pub/crl/g_cacrl.crl

        Full Name:
          URI:http://cdp2.pca.dfn.de/uni-siegen-ca/pub/crl/g_cacrl.crl

    Authority Information Access:
        CA Issuers - URI:http://cdp1.pca.dfn.de/uni-siegen-ca/pub/cacert/g_cacer
        CA Issuers - URI:http://cdp2.pca.dfn.de/uni-siegen-ca/pub/cacert/g_cacer
                                    ⋮
```

X.509 Certificate IV

```
Signature Algorithm: sha1WithRSAEncryption
     4c:18:b0:04:2e:01:ae:67:d8:c4:79:cb:85:1b:a1:6d:ec:ff:
     ba:84:3c:e1:50:9d:95:91:b0:5e:ca:75:4c:6a:4f:69:0e:7e:
     c8:6f:eb:3e:2c:4e:e9:19:8b:35:9e:1f:19:0d:10:b4:88:a3:
     fb:8b:b4:f2:da:10:08:e0:83:4f:d8:15:90:5d:4a:b3:fd:10:
     2b:94:5b:79:61:e5:8e:d4:1d:4f:11:ac:c2:2a:44:bb:11:4e:
     2c:42:54:13:15:2a:a1:a5:bd:20:89:c4:83:8c:db:aa:66:28:
     5c:99:44:00:36:e1:1a:d9:a8:87:e8:a9:24:bc:56:39:63:0e:
     10:84:f2:03:7e:85:88:70:a1:2b:da:39:75:c5:b7:2f:3a:41:
     4f:b1:53:ba:c1:66:5c:0b:a0:5a:ff:0f:65:20:bd:b0:1f:2c:
     3d:42:ca:6a:f8:4c:73:af:20:93:98:9d:ca:a9:17:49:7a:9c:
     04:d8:5d:1e:2e:1b:36:85:f5:8f:83:a6:ab:49:ef:a5:2b:d0:
     7b:9e:80:a6:eb:87:1d:8f:16:79:d5:a2:4f:f1:e6:6e:4d:0c:
     ea:f1:a1:95:ec:db:dd:02:8e:41:14:9b:47:f6:6c:46:1a:f6:
     7b:85:9b:d6:80:0b:29:0e:54:b4:fb:e6:ab:2a:1b:09:64:aa:
     a4:44:3c:68
```

X.509 Certificate PEM encoded

-----BEGIN CERTIFICATE-----
MIIFAjCCA+qgAwIBAgIEDF3pizANBgkqhkiG9w0BAQUFADCBhDELMAkGA1UEBhMC
REUxHDAaBgNVBAoTE1VuaXZlcnNpdGFldCBTaWVnZW4xOTA3BgNVBAsTMFplbnRy
dW0gZnVlciBJbmZvcm1hdGlvbnMtIHVuZCBNZWRpZW50ZWNobm9sb2dpZTEcMBoG
A1UEAxMTVW5pLVNpZWdlbiBDQSAtIEcwMjAeFw0wODA1MjkwODQwMjdaFw0xMzA1
MjgwODQwMjdaMFcxCzAJBgNVBAYTAkRFMRwwGgYDVQQKExNVbml2ZXJzaXRhZXQg
U2llZ2VuMQ0wCwYDVQQLEwRaSU1UMRswGQYDVQQDExJ4aW1zLnVuaS1zaWVnZW4u
ZGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEx69Gh3uQiXa8a0UC
Ui+NVNpoxEkrS1c06cgvTby1KCVmHOgm27Z6iLRPrC71pb2Sk1EJ8n6WuXbe1aOb
4vuBRqnZO6xRQB9oarA2ZjKSGxR0CHfEkEpUGWNX+ilwL6bAazbGAOuF6pDBoVCq
Myvb5JYmOMHokIJF6rwTpCE9BbO+eY67w1tRlsOVYZ+4n+oWQZ7E1rQeQ+vp/8wk
iOFEZK+wkJtfdxsGWV0Nmg314qR7m7FCWMmvoO7W6FbmSJcF3YCXQAjLXn3xrtIF
yKNnHUO62D6vqu3PTxFZO7TCOtyabD4btsHN1m2/LM38uerLuf8xaDJYGCMOpo9q
knLnAgMBAAGjggGmMIIBojAJBgNVHRMEAjAAMAsGA1UdDwQEAwIE8DATBgNVHSUE
DDAKBggrBgEFBQcDATAdBgNVHQ4EFgQU0531cMfgFAA6xy8vTgGrU9ofwHcwHwYD
VR0jBBgwFoAU/3TCaTrwhJ+cApPNn5733f8BxWUwgYsGA1UdHwSBgzCBgDA+oDyg
OoY4aHR0cDovL2NkcDEucGNhLmRmbi5kZS91bmktc2llZ2VuLWNhL3B1Yi9jcmwv
Z19jYWNybC5jcmwwPqA8oDqGOGh0dHA6Ly9jZHAyLnBjYS5kZm4uZGUvdW5pLXNp
ZWdlbi1jYS9wdWIvY3JsL2dfY2FjcmwuY3JsMIGkBggrBgEFBQcBAQSBlzCBlDBI
BggrBgEFBQcwAoY8aHR0cDovL2NkcDEucGNhLmRmbi5kZS91bmktc2llZ2VuLWNh
L3B1Yi9jYWNlcnQvZ19jYWNlcnQuY3J0MEgGCCsGAQUFBzAChjxodHRwOi8vY2Rw
Mi5wY2EuZGZuLmRlL3VuaS1zaWVnZW4tY2EvcHViL2NhY2VydC9nX2NhY2VydC5j
cnQwDQYJKoZIhvcNAQEFBQADggEBAEwYsAQuAa5n2MR5y4UboW3s/7qEPOFQnZWR
sF7KdUxqT2kOfshv6z4sTukZizWeHxkNELSIo/uLtPLaEAjgg0/YFZBdSrP9ECuU
W3lh5Y7UHU8RrMIqRLsRTixCVBMVKqGlvSCJxIOM26pmKFyZRAA24RrZqIfoqSS8
VjljDhCE8gN+hYhwoSvaOXXFty86QU+xU7rBZlwLoFr/D2UgvbAfLD1Cymr4THOv

Certificate in FoaF

```
<cert:key>
  <cert:RSAPublicKey>
    <cert:label>Lars Fischer</cert:label>
    <cert:modulus
      rdf:datatype
        ="http://www.w3.org/2001/XMLSchema#hexBinary">
BAAFB2E38A4E4FD49F9F0285D5929CA45EB1833607425E60CBB28AD3
    </cert:modulus>
    <cert:exponent rdf:datatype
        ="http://www.w3.org/2001/XMLSchema#integer">
    65537
    </cert:exponent>
  </cert:RSAPublicKey>
</cert:key>
```

WebID Summary

- SSL based authentication
  - Browser has private key
  - any user action authenticated
- identifier: URI
- Webservices to write


OpenID

OpenID Overview

- Federated Authentication
- Standardisation `http://openid.net`
- URI based ID
- Roles: End-User, Relying Party, OpenID Provider
- Relying Party learns attributes

next week

Literatur I


M. Kolsek, "Session fixation vulnerability in web-based applications," ACROS Security, Tech. Rep., 2002. [Online]. Available: http://www.acrossecurity.com/papers/session_fixation.pdf


M. Sporny, T. Inkster, H. Story, B. Harbulot, and R. Bachmann-Gmür, *WebID 1.0 — Web Identification and Discovery — W3C Editor's Draft 12 December 2011*, W3C Std. [Online]. Available: http://www.w3.org/2005/Incubator/webid/spec/drafts/ED-webid-20111212