Security of National eID (smartcard-based) Web Applications

Raul Siles
raul@taddong.com
BruCON 2012
Sep 26-27, 2012
Outline

- Introduction to eID
- eID security state-of-the-art
- Pen-testing eID web-apps
  - HTTPS, eID & session management
- Results & Recommendations from real-world pen-tests
  - HTTPS, eID & session management
- Conclusions
eID (or e-ID)

- **(National) electronic IDentification (eID)**
  - Username/password, mobile, **smartcard**…

- **By example: Spanish eID (DNIe or eDNI)**
  - DNIe internal layout
    - Zones: public, private (PIN) & security
    - Biometric data (fingerprint, picture & signature)
  - ISO 7816 (PKCS#15 evolution)
  - Certificates (& two associated key-pairs)
    - Identification (KeyUsage = Digital Signature)
    - Signature (KeyUsage = contentCommitment)
  - Legal validity & CWA 14169: Secure signature-creation device (EAL4+)
The eID is Secure…
The New eID is 10-Times More Secure…
Real eID Security Threats

- Physical eID access and PIN knowledge
- End-user computer compromised
- Examples: (eID/smartcards)
  - “Man-In-Remote: PKCS11 for fun and non-profit”. Gabriel González. RootedCON 2011
    - Remote PIN & PKCS#11 invocation
  - Sykipot trojan variant – China (AlientVault)
    - US DoD smartcards PIN acquisition
    - Keylogger + Windows certs. memory access
    - Remote user impersonation (proxy)
      - December 2011 (March?)
The eID is Secure, But...
Where Is It Being Used?
Who Has an eID? (in Spain)

- 25 million eIDs dispatched (Sep 29, 2011)
  - Project started in 2005
  - More than half of the Spanish population
- Spain is a **worldwide leader in electronic signature-based smartcards** (electronic ID)
  - 26 countries all over the world (smartcard & signature)
- National Home Office (police department)
  - +1,500 dispatch offices (+341M €)

What Do We Use the eID For?

• Personal Computers
  – Login (user authentication)
  – Sign documents (e.g. invoices)
  – Get access to Wi-Fi and VPN networks
  – VoIP call authentication...

• Madrid & Barcelona airports
  – Automatic frontier control project
    • ABC System (Indra) & National police
  – Self-service
  – eID + picture + fingerprint

• ATMs
• TDT (eAdmin via digital TV)
• Mobile phones (mDNI)
What Do We Use the eID For?
In Reality...

- e-Banking
- e-Government
eID is Used in Web-Apps

- Critical web applications
  - Public sector
    - e-Government services
      - March 2011: 2,015 online services
      - 99% procedures from the Central Government
  - Private sector
    - Financial (e-Banking), insurance, and utility companies (telecom, electricity, water, gas...)
    - e-Commerce
  - Most secure authentication method
    - Username/password (backup)
eAccessibility vs. eSecurity

Status of Web content accessibility (government websites), by country

- **Grand Total**
- **Total EU Countries**: 39%
- **Czech Republic**: 35%
- **Denmark**: 36%
- **France**: 41%
- **Germany**: 27%
- **Greece**: 30%
- **Hungary**: 32%
- **Ireland**: 43%
- **Italy**: 40%
- **Portugal**: 76%
- **Spain**: 25%
- **Sweden**: 44%
- **The Netherlands**: 61%
- **United Kingdom**: 39%
- **Total Non-EU Countries**: 42%
- **Australia**: 38%
- **Canada**: 35%
- **Norway**: 42%
- **United States of America**: 38%

European eID Regulation

• European Commission Press Release
  – June 4, 2012 (... 2014)

• Digital Agenda: new Regulation to enable cross-border electronic signatures and to get more value out of electronic identification in Digital Single Market
  – National electronic identification schemes (eIDs)
  – Electronic identification, signatures and trust services
    • Acceptance of cross-country citizen transactions

eID by Country

- **eID (EU): smartcard**
  - Belgium, Estonia, Finland, Germany, Italy, Portugal, Spain, Switzerland

- **Pseudo eID (EU): user/pass + SMS, cert…**
  - Austria (2), Czech Republic, Denmark, Holland, Iceland, Liechtenstein, Lithuania, Luxemburg, Slovakia, Slovenia, Sweden
  - Holland (July 2012) + 7 years
    - DigID 4.0: username & password (+ SMS code)
    - Future: Smartcard-based eID…

- **Outside EU**
  - Hong-Kong, Morocco, Saudi Arabia, South Korea, UAE
The eID is Secure, It Is Used in Web-Apps, World-Wide, But... Is It Used in a Secure Way?
eID (Smartcard-Based) Web Applications

• eID web-based authentication
  – HTTPS protocol
    • Standard and transparent solution
    • Built-in client-based digital certificate (X.509) authentication in all web browsers
  – Web-based client components
    • Custom Java Applet or ActiveX control
  – eID cloud-based authentication

• eID web-based signatures
  – Web-based client components or JavaScript
    • JS: Proprietary IE (CAPICOM) o Firefox (crypto.signText() )
    • Client components: local permissions required?
Pen-Testing eID Web-Apps
Get Authorization
Pen-Testing eID Web-Apps
Research Areas
HTTPS Authentication: Client Certs.
Assessing HTTPS (SSL/TLS)

- TLSSLeled (v1.2 - October 2011)
  - Web server SSL/TLS (HTTPS) implementation security assessments
  - sslscan & openssl (GNU/Linux & Mac OS X)
  - SSLv2, SSLv3/TLSv1, TLSv1.1/v1.2 (BEAST), NULL cipher, weak (40/56 bits) & strong (AES 128/256 bits) ciphers, MD5-signed certs., cert. key length, subject, issuer (CA), validity period, STS header, (un)secure cookies, RFC 5746: secure SSL/TLS renegotiation…
- Upcoming version at the end of 2012…

eID

dni electrónico
Assessing eID Integration in Web-Apps

• In-depth web-app security analysis
  – Registration & authentication using the eID
  – Access controls

• Interception proxies: smartcard constraints
  – Commercial & open-source tools (Java)
    • Client certificate errors (HTTPS)
  – Need smartcard drivers or libraries
    • Built-in integration required

Main focus: OWASP ZAP…
Session Management
Secure Web-App Session Management

• Top web vulnerabilities: SQLi, XSS, CSRF…
  – Session management? OWASP Top 10 (A3)
• Malware: OddJob (February 2011)
  – Hijacks users sessions and keeps them active
    • US & EU banks
• OWASP Session Management Cheat Sheet
  – v1.0 (July 2011) & v2.0 (February 2012)
  – Challenges: HTTP is stateless, complexity, security
    on the developer’s hands, cookies, HTTPS…

http://blog.taddong.com/2012/02/owasp-session-management-cheat-sheet.html
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet
eID: PKCS#11 & Java
• Statically (e.g. keytool)
  – Based on the OS: Win, Linux or Mac
  – %JAVA_HOME%/lib/security/java.security

security.provider.10=sun.security.pkcs11.SunPKCS11_C:/Program Files (x86)/Java/jre6/lib/security/dnie_pkcs11.cfg

– Configuration file for SunPKCS11:

# Provider.getName() = SunPKCS11-DNIe
name = DNIe
# DNIe library
library = C:\WINDOWS\SysWOW64\UsrPkcs11.dll
• Statically (e.g. keytool)
  – Based on the OS: Win, Linux or Mac
  – $JAVA_HOME/lib/security/java.security

```java
security.provider.10=sun.security.pkcs11.SunPKCS11
/usr/lib/jvm/java-6-sun/jre/lib/security/dnie_pkcs11.cfg
```

– Configuration file for SunPKCS11:

```java
# Provider.getName() = SunPKCS11-DNIe
name = DNIe
# DNIe library
library = /usr/lib/opensc-pkcs11.so
```
PKCS#11 (eID) & Java: Mac

• Statically (e.g. keytool)
  – Based on the OS: Win, Linux or Mac
  – $JAVA_HOME/lib/security/java.security

```
security.provider.10=sun.security.pkcs11.SunPKCS11
/.../1.6.0.jdk/Contents/Home/lib/security/dnie_pkcs11.cfg
```

– Configuration file for SunPKCS11:

```
# Provider.getName() = SunPKCS11-DNIe
name = DNIe
# DNIe library
library = /usr/lib/opensc-pkcs11.so
```

32-bit Java VM: $ java –d32 ...
PKCS#11 (eID) & Java: Query eID

• Java keytool (e.g. Windows)
  – List eID contents (PKCS11 token)

```markdown
C:\> keytool [-v] -keystore NONE -storetype PKCS11 -list
Escriba la contraseña del almacén de claves: ...
```

– With no provider setup in java.security

```markdown
C:\> keytool -keystore NONE -storetype PKCS11
   -providerClass sun.security.pkcs11.SunPKCS11
   -providerArg "C:\Program Files(x86)\Java\jre6\lib\security\dnie_pkcs11.cfg"
   -list
```
PKCS#11 (eID) & Java: Code

... Add PKCS11 provider
String cardConfig = "dnie_pkcs11.cfg"; // or InputStream
Provider pkcs11 = new sun.security.pkcs11.SunPKCS11(cardConfig);
Security.addProvider(pkcs11);

// Init the keystore
KeyStore ks = KeyStore.getInstance("PKCS11", pkcs11);
    ks.load(null, pin.toCharArray());

KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");
    kmf.init(ks, pin.toCharArray());
KeyManager[] kms = kmf.getKeyManagers();

X509TrustManager trustManager = new X509TrustManager() { ... }
TrustManager[] tms = new TrustManager[] {trustManager};

// Init SSL context
SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(kms, tms, new java.security.SecureRandom());
OWASP ZAP: Zed Attack Proxy

- Web interception proxy & much more…
  - Open source (Java)
    - Multiplatform: Windows, Linux & Mac OS X
  - Paros & Andiparos (& WebScarab) evolution
- Supports client-based certs. & smartcards
  - Tools - Options - Certificate
    - Keystore: PKCS11, PKCS12…
  - Unsecure SSL/TLS renegotiation
  - eID failed access attempts (PIN): PUK

http://code.google.com/p/zaproxy/
ZAP DNle Support

• PKCS#11 (after installing the DNle drivers…)
  – Windows: (XP & 7 – 32 & 64 bits)
    • C:\Windows\System32\UsrPkcs11.dll
    • C:\Windows\SysWOW64\UsrPkcs11.dll
  – GNU/Linux: /usr/lib/opensc-pkcs11.so (or /usr/lib64/)
  – Mac OS X: /Library/OpenSC/lib/opensc-pkcs11.so
    • /usr/lib/opensc-pkcs11.so (link) & Java 32 bits

• drivers.xml (OWASP ZAP SmartCard Project)

http://blog.taddong.com/2012/04/owasp-zap-smartcard-project.html
How To Get The Slot (eID & OS)?

• Adding support for new eIDs (or countries)
  – keytool –D… (debug)

C:\> keytool -keystore NONE -storetype PKCS11 -list
       -J-Djava.security.debug=sunpkcs11,pkcs11
Escriba la contraseña del almacén de claves: ...

– Result:

... 
All slots: 1 (ó 0,1,2,3..., 15)
Slots with tokens: 1
Slot info for slot 1:
...
Token info for token in slot 1:
  label: DNI electrónico ...
The eID is Secure, It Is Used in Web-Apps, Now We Can Assess Its Security, So... (Again) Is It Used in a Secure Way?

Results & Recommendations From Real-World Pen-Tests
Motivation, Scope & Goals

• Multiple penetration tests on eID-based web applications
  – Both national public and private sectors
  – Different online services (web-apps) using the eID for user authentication (Java, ASP .NET, PHP…)
  – May-December, 2011
• Security assessments focused on authentication (eID), access controls, and session management
  – Beyond SQLi, XSS, XSRF…
• Target web-apps: 15 (very relevant ones)
Pen-Testing eID Web-Apps

Vulnerable Areas


2. dni electrónico

3. Cookie
Impact of Vulnerable Areas

1. HTTPS (SSL/TLS) implementation
   - Native integration with eID & client digital certificates
   - Web traffic decryption, MitM attacks, DoS, etc

2. eID-based user authentication and registration
   - Manipulate authentication & registration data
   - Complete user impersonation (citizens)

3. Web-app session management
   - eID = session ID (cookie)
   - Complete user impersonation (citizens)

…but the eID is secure (we are were confident)
HTTPS
HTTPS Results (1/2)

![Graph showing CA distribution by strength and protocol version with algorithms.](image-url)

- **CA Distribution**
  - FNMT C2: 31
  - APE CA: 38
  - Others: 31

- **Protocol Version**
  - TLSv1.1/1.2: 100
  - SSLv3/TLSv1: 46

- **Algorithms**
  - Strong (128/256+): 62
  - Weak (40/56): 85
HTTPS Results (2/2)

TCP/80 (HTTP)

<table>
<thead>
<tr>
<th></th>
<th>Redirection</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>42</td>
<td>50</td>
</tr>
</tbody>
</table>

Client renegotiation (HTTPS)

<table>
<thead>
<tr>
<th>Traffic (CVE-2009-3555)</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC5746</td>
<td>38</td>
</tr>
</tbody>
</table>

DoS (CVE-2011-1473)

HTTP(S) headers

<table>
<thead>
<tr>
<th></th>
<th>STS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Redirection

! RFC5746

RFC5746

… & enabled
HTTPS Renegotiation

- Secure HTTPS (SSL/TLS) renegotiation
HTTPS Authentication

(Using web-based client components...)

HTTPS, component signature, permissions...
eID
(User Authentication and Registration)
eID-based User Registration Results

- Web-app requires user registration (eID)
  
  Step 1: eID authentication
  
  Step 2: Registration details web form
  
  - Lack of verification?
  
  - It is possible to manipulate all the victim user info: ID, name & surname, address, phone…

- Is it possible to manipulate registration details?
  
  - Only 25% web-apps required registration

![Bar chart showing 67% vulnerability](chart.png)
eID-based Authentication Results

• One or multi-step procedures and proceedings
• Is the eID required to access all resources?
  – User impersonation: anonymously or eID

[Bar chart showing distribution of eID use]

• Matching between eID and session ID

[Bar chart showing matching between eID and session ID]
Session Management
Session ID = Credentials

- Session management attacks trying to bypass advanced authentication mechanisms
- ID is equivalent (temporarily) to…
  - PIN & Passwords
  - Passphrases
  - Certificates
  - Smartcards
  - Biometry
So The eID in Reality is Like…
Session Management
Results (1/2)

Session ID
- Cookies: 75%
- Params.: 17%
- N/A: 8%

ID entropy
- Low: 36%

Session fixation
- Vuln.: 64%
Session Management Results (2/2)

Cookie attributes

Secure
HttpOnly
Domain
Path

Session finalization (timeouts):
Relative
Absolute
Button/Link (remains open)

33% of those with button/link

52
Copyright © 2012 Taddong S.L.
www.taddong.com
The eID is Secure, It Is Used in Web-Apps, But... It Seems It Is NOT Being Used in a Secure Way
Conclusion
Warning
Solution
Thank You