Seguridad Informática.

E-Banking Security

FGA, Barcelona, February 2008
Table of content

1. E-Banking Applications

2. Common attacks
   - Server Side Attacks
   - Cliente Side Attacks
   - Examples of current attacks

3. Protection Measures

4. Best Practices

5. Real Life Examples
E-Banking Applications

Why Security of E-banking applications:

• The risks inherent to E-Banking sites are representative of those faced by the majority of the other sites, but with a higher degree of potential impact and higher interest from attackers ($$$)

• This presentation focuses mainly on E-banking applications, but of course, most of the concepts and technologies discussed can also be applied to other types of web sites (transactional sites, sites with confidential information, corporate extranets, etc.)

• Sensitive sites such as E-banking are generally better protected than regular web sites. Generally also means “not always” 😊
E-Banking Applications

Main characteristics of E-Banking Sites:

• **Consultative**: users can only view their current position, history of transactions or payments, etc.

• **Transactional**: users can transfer money between accounts (towards their own accounts, other national accounts, or international)

• **Home vs corporate E-banking**: home E-banking is targeted at end users, whereas corporate E-banking is targeted at other branches, offices, or large customers (more complex applications in general). In corporate banking, different kinds of operations are possible, different limits, specific authorization flows, delegation of rights, users management in the application, etc.
E-Banking Applications

Most banks now provide their clients with access to their accounts (at least in consultation mode) via the Internet, be it for commercial, marketing, or cost saving reasons.

But due to the complexity and cost of E-banking environments, it is still common to find banks vulnerable to different types of threats and they remain the target of many attacks recently.

Deloitte is used to perform the design, review and testing of these sensitive applications around the world, and most of the information that follows derives from our experience.
Table of content

1. E-Banking Applications

2. Common attacks
   - Server Side Attacks
   - Cliente Side Attacks
   - Examples of current attacks

3. Protection Measures

4. Best Practices

5. Practical Examples
Common Attacks

There are 2 main categories of attacks:

- Server Side Attacks (SSA)
- Client Side / Browser Attacks (CSA)

This categorization in SSA and CSA is not following any standard/common classification (only common sense). Additionally, in some cases it could even be contested or be inadequate, since some attacks could result from the combination of server side and client side issues.

This classification was established solely for the purpose of this presentation, and only intends facilitating audience comprehension.
Common Attacks

**Server Side Attacks:** These attacks are performed directly towards the E-Banking site, either from the Internet, or from the internal LAN of the bank. SSA are performed straight on the web server, their impact is generally higher, or with a larger population impacted than the Client Side Attacks.
Common Attacks

Examples of Server Side Attacks:

• Data Injections:
  – XXX
• Login Attacks
  – XXX
• Information disclosure (comments, debugging messages, etc.)
• Vulnerable configurations, non patched services
• Buffer/heap/stacks overflows,
• Unprotected Administration interfaces
• Abuse of admin privileges
• Denial of Service
• Abuse of Business logic
Common Attacks

**Client Side Attacks:** These attacks take place or are targeted at the system/browser of the client using the Banking application. CSA have for objective to take control of the client system and use his identity to execute specific code and perform illicit action.
Common Attacks

Examples of Client Side Attacks:

• **HTML code injection:**
  – XXX

• **MITM:**
  – XXX

• **Client system or browser control:**
  – Malicious Mobile Code (Virus, Trojans, Rootkits, Malware, Backdoors)
  – Intrusion of client system or applications

• **Resilient information (e.g. Browser cache, persistent cookies)**

• **Social Engineering**
Common Attacks

Scenario 1 – Typical Phishing/MITM (1):
• Gathering of email addresses on the internet (web sites, forums, mailing lists, hacks)
• Mirroring of target E-banking site, setup of fake site (including DNS spoof, erroneous name, fake cert, http clear text)
• Mass mailing sent to target addresses (maintenance, information, security issue, prize)
• Obfuscated link (visible : www.realbank.com , effective : www.fake.com)

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/generalcustverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
Common Attacks

Scenario 1 – Typical Phishing/MITM (2):

• Some users click malicious link (even some without clicking, images embedded, )
• Users are asked to enter their credentials on fake site (login and pwd or even OTP)
• Users are gently redirected to the real site (or fake site as relay).
• Attacker can use or reuse the credentials to login on real E-banking site (OTP/replay issues) and perform transfers, etc.
• Role of Mules
Common Attacks

**Phishing Principle:**

A hacker sends a fake or "spoofed" email that appears to be from a trusted company.

The email usually instructs the user to login to verify information, and contains a link.

The link in the email directs the user’s web browser to a fake website operated by the hacker.

The fake website looks exactly like a company’s real website, and requires the user to login.

Any information the user enters into the fake website is immediately delivered to the hacker, which they can use to access the user’s accounts.
Common Attacks

Scenario 2 – Typical Phishing with XSS or Session Fixation:
• No need to setup fake site
• Using only original server to perform attack
• No anti phishing software would detect it
Common Attacks

**Scenario 3 – Trojans:**

- Depends on Client security only
- Outside of Banks control, no effective protection mechanism (even certificates, OTP, etc.)
- No antivirus will be able to detect them on day 1
- Very elaborate, stealth
- Key logging, mouse activity logging, screen shots triggered by specific actions
- IE plug-in
Table of content

1. E-Banking Applications

2. Common attacks
   - Server Side Attacks
   - Cliente Side Attacks
   - Examples of current attacks

3. Protection Measures

4. Best Practices

5. Real Life Examples
Protection Measures

**Data Transfer mechanisms:**
- HTTP / HTTPS
- Anonymous SSL / Authenticated SSL (*warning with canvas*)
- Custom (obscured data, IIOP)

**Authentications mechanisms:**
- Identifier + static password (clear, base64, hashes, custom, ntlm)
- Identifier + semi OTP passwords (scratch list, codes table)
- Identifier + real OTP (software, sync/challenge, with keypad, unconnected card reader)
- Identifier + certificate (software, hardware with SC, SC reader with screen/keypad)
- Identifier + biometric (fingerprint)
- *Purpose of virtual keyboards, captchas*
Protection Measures

OTPs
Protection Measures

**OTPs with Smart Cards:**
Protection Measures

Web Application Firewalls:
• WAFs appliances/software
• Reverse proxy with filtering
• Filtering inside the web application (data dictionary)

Web Application Testing:
• Web testing (automated, manual)
• Source code review

Applicative IDS:
• IDS inside the application (business level, correlation of events)
Table of content

1. E-Banking Applications
2. Common attacks
   • Server Side Attacks
   • Cliente Side Attacks
   • Examples of current attacks
3. Protection Measures
4. Best Practices
5. Real Life Examples
Best Practices

**Design - Infrastructure:**
- Layered infrastructure, best practice, 3 Layers (separate components)
- Firewalls and security components from different manufacturers
- Avoid All-in-one components (authentication, authorization, auditing, etc.)
  - XXX

**Design – Software Modules:**
- Secure SDLC
- Blueprint validation
  - XXX

**Misc.**
- Don’t rely on obscurity (xyz protocol or programming language)
- Don’t trust developers to **evaluate or report** security risks, not their job (plus segregation of duties would be impaired). Security is a specialty, should be done by specialist (independent is a plus).
- Exhaustive testing before production (Quality + **Security**)
- Security is only as strong as its weakest link
  - XXX
Best Practices

**Future**: Server Side security is easier to control, but on client side, there is not much to be done, out of control range.
⇒ Need to delocalize the trust from the client system or browser to a trusted “zone”, like:
XXX
⇒ Permanent challenge, so make the attackers go for your neighbors site (his door should be weaker... 😊)
Table of content

1. E-Banking Applications

2. Common Attacks
   • Server Side Attacks
   • Cliente Side Attacks
   • Examples of current attacks

3. Protection Measures

4. Best Practices

5. Real Life Examples
Real Life examples

• 2 Stats about Spain:
  • 1st source of Phishing,
  • 3rd rank as target
• Strong authentication with any Spanish bank?
Real Life examples

• XXX
Questions?

©2008 Deloitte. Todos los derechos reservados
Deloitte Touche Tohmatsu es una organización de firmas independientes, dedicadas a la prestación de servicios y asesoramiento profesional de máxima calidad, y que se centran en el servicio al cliente mediante una estrategia global aplicada a nivel local en cerca de 140 países. Con acceso a un enorme capital intelectual de casi 150.000 personas en todo el mundo, Deloitte presta servicios en cuatro áreas profesionales (auditoría, asesoramiento tributario, consultoría y asesoramiento financiero) a más del 80% de las empresas más importantes del mundo, así como a grandes empresas públicas, aunque por diversos motivos, entre los que se hallan las regulaciones específicas de cada país, no todas las Firmas miembro de Deloitte prestan toda la gama de servicios.

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu (Swiss Verein), sus firmas miembro y respectivas filiales y asociadas. Al tratarse de un Verein suizo (asociación), ni Deloitte Touche Tohmatsu ni ninguna de sus firmas miembro es responsable de los actos u omisiones de las otras. Cada firma miembro es una entidad independiente con personalidad jurídica propia que opera bajo los nombres de “Deloitte”, “Deloitte & Touche”, “Deloitte Touche Tohmatsu”, u otros nombres asociados. Los servicios son prestados a través de las firmas miembro y sus respectivas filiales y asociadas y no por Deloitte Touche Tohmatsu (Swiss Verein).