

# Analyzing the Security of Internet Banking Authentication Mechanisms

By Christos K. Dimitriadis, Ph.D., CISA, CISM

The provision of electronic services, such as corporate and personal funds transfer and retail account management, by banking organizations evolves and spreads with the introduction of enhanced communication technologies. However, this novel business opportunity for the provision of banking products and services increases the need for security, especially due to the sensitive nature of the information exchanged.<sup>1</sup> Furthermore, attacks against Internet-banking authentication mechanisms evolve,<sup>2</sup> decreasing the user's trust and, as a consequence, the spread of Internet banking applications in the market.

The specific nature of Internet banking systems creates the requirement for specialized knowledge on security issues to be able to effectively conduct an auditing or security evaluation process. More specifically, the information systems (IS) auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking.<sup>3</sup>

Following that requirement, this article studies possible attacks according to which state-of-the-art authentication mechanisms are evaluated. An attack tree is created to propose a guide that an auditor, a security consultant or a security officer may use for conducting a security analysis. A case study presents a security analysis of an Internet banking authentication mechanism conducted for a major bank, describing how the attack tree may be deployed.

## Internet Banking Security Standards

The need for standardizing the security of Internet banking was identified quickly, causing the creation of a number of guidance documents and best practices, such as those published by the Basel Committee. The Basel II framework describes a standard for capital adequacy that national supervisory authorities are now working to implement through domestic rule-making and adoption procedures.<sup>4</sup> Within that framework, a number of Internet banking security controls should be implemented, including authentication of Internet banking customers; nonrepudiation and accountability for Internet-banking transactions; appropriate measures to ensure segregation of duties; proper authorisation controls within Internet banking systems, databases and applications; data integrity of Internet banking transactions, records and information; establishment of clear audit trails for Internet banking transactions; and, finally, confidentiality of key bank information.

Additionally, the guidance for banks issued by the Federal Financial Institutions Examination Council (FFIEC) describes enhanced authentication methods underlining the

ineffectiveness of single-factor authentication.<sup>5</sup> More recent standards, such as the International Organization for Standardization's ISO 21188:2006, describe a framework of requirements to enable certificate-based solutions for secure Internet banking applications.<sup>6</sup> ISO 21188:2006 defines security targets, as well as procedures that guide and facilitate the risk management process.

Finally, the ISACA IS Auditing Guideline for Internet Banking<sup>7</sup> describes the recommended practices to conduct a review of Internet banking initiatives, applications and implementations. The guideline facilitates the identification of risks and controls toward risk reduction. Moreover, the guideline proposes that a number of aspects should be studied, including the organization, policy, planning, IS infrastructure, telecommunication infrastructure, authentication and third-party service provider aspects.

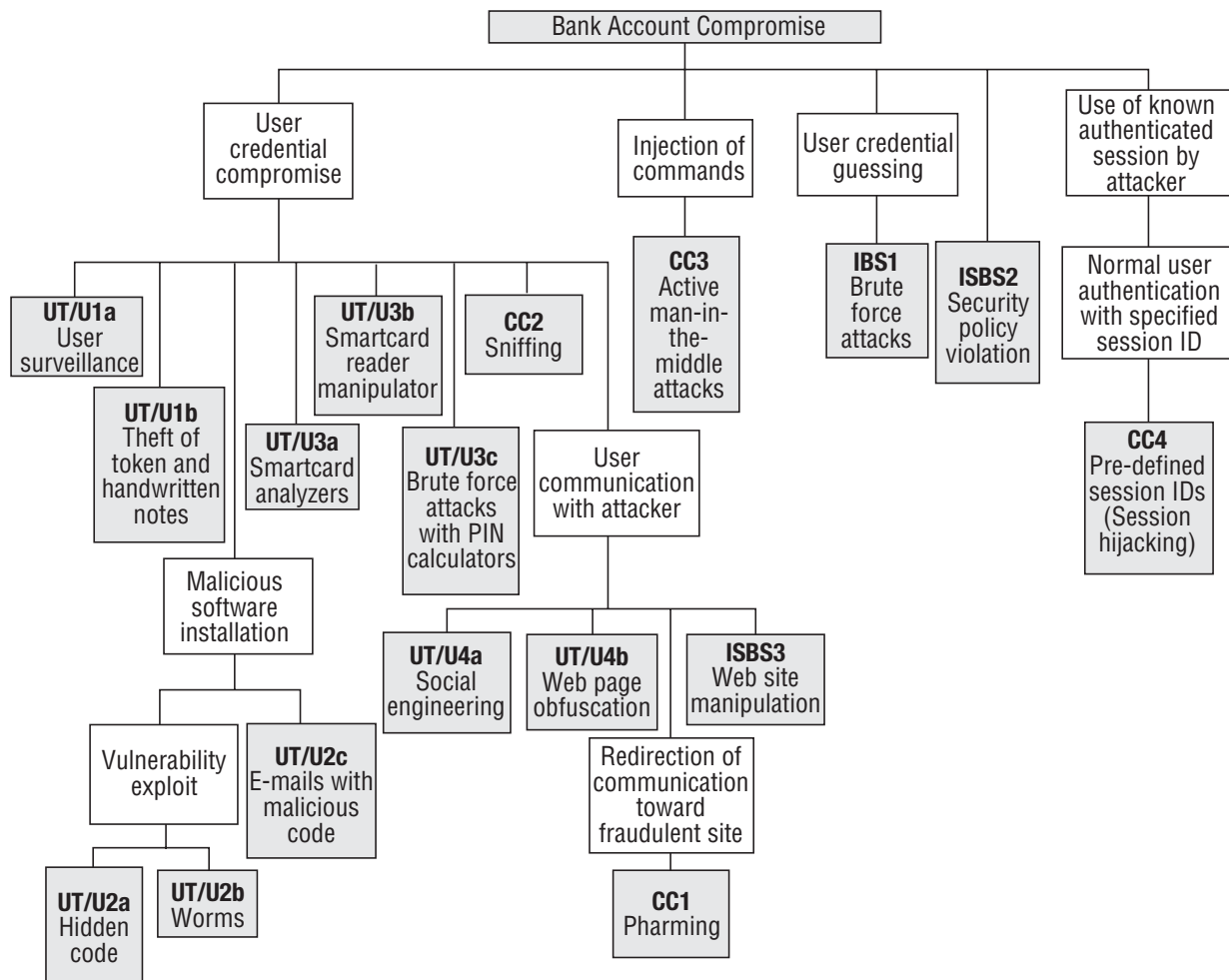
## Attack Trees

To implement the guidelines provided by the standards, more specific attacks and countermeasures should be studied. Attack trees<sup>8</sup> provide a formal methodology for analyzing the security of systems and subsystems. They provide a way to think about security, capture and reuse expertise about security, and respond to changes in security. An attack tree has a root node and leaf nodes. The root node represents the target of the attack, while the leaf nodes represent the means for reaching the target, which are the events that comprise the attack. The attack tree is depicted in **figure 1**.

The attack tree has one root node, representing the final target of the attacker, which is the compromise of the user's bank account. An intruder may use one of the leaf nodes as a means for reaching the target. To categorize Internet banking attacks, each component of the process should be examined: the user terminal/user (UT/U), the communication channel (CC) and the Internet banking server (IBS). The following types of attacks are identified:

- **UT/U attacks**—These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user himself/herself. UT/U attacks include:
  - UT/U1—Procedural attacks:
    - UT/U1a: User surveillance (piggybacking)—Similar to the personal identification number (PIN) thefts facilitated by the installation of cameras in automatic teller machines (ATMs); the user's actions may be monitored to capture credentials.
    - UT/U1b: Theft of token and handwritten note stealing—Internet banking usernames are usually long and have to

Figure 1—Attack Tree



be written down. Users may also keep their passwords written, despite the security guidance provided by their banks. Notes may be stolen, providing access to the user's credentials. Tokens may also be stolen, providing the attacker with one authentication factor that, when combined with other types of attacks (such as PIN calculators), can lead to identity theft.

- UT/U2—Malicious software installation. The embedding of malicious content for compromising the user's login information and password (e.g., keyboard loggers or screen capture in image or video files) may take place via a number of different methods, including:
  - UT/U2a: Hidden code—This is the use of hidden code within a web page that exploits a known vulnerability of the customer's web browser and installs malicious software in the user terminal. The exploit may target permissions on Java runtime support, ActiveX support, multimedia extensions, and automated download and running of software through the browser.
  - UT/U2b: Worms and bots—Worms search vulnerabilities and exploit them automatically. This includes the exploit of instant messaging and chatting communication software (that allows the embedment of dynamic content), which

may automatically be deployed using bots.

- UT/U2c: E-mails with malicious code—This is the submission of e-mails with malicious content, such as executable files or HTML code with embedded applets.
- UT/U3—Token attack tools:
  - UT/U3a: Smartcard analyzers—Attacks against smartcards, such as power consumption analysis or time analysis, may expose the security of the smartcard by revealing cryptographic keys and passwords.<sup>9</sup> Such attacks are sophisticated and not easy to implement, but are very effective, especially if the necessary countermeasures (noise generators, time-neutral code design) against these types of attacks are not implemented by the smartcard manufacturer.
  - UT/U3b: Smartcard reader manipulator—This is applicable to noncertified smartcard readers with insecure interfaces, which may expose the contents of the smartcard by conducting unauthorized operations.<sup>10</sup>
  - UT/U3c: Brute-force attacks with PIN calculators—These attacks focus on breaking the security of tokens that generate random PINs. The attack exploits the fact that a time window is necessary, for synchronization reasons. In some implementations, except from the present PIN, the

subsequent and preceding codes are active for the same purpose. It is reported that it is possible to break such mechanisms with a minimum window of three PINs.<sup>11</sup>

- UT/U4—Phishing.<sup>12</sup> These attacks use social engineering techniques—masquerading as a trustworthy person or business in an electronic communication—in an attempt to fraudulently acquire sensitive information, such as passwords and credit card details. The term was initially used in the mid-1990s by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. These attacks include:
  - UT/U4a: Social engineering—These attacks focus on the compromise of the user’s credentials by nontechnical means, such as phone calls or the submission of e-mails masquerading as an official bank, asking the user for username and password.
  - UT/U4b: Web page obfuscation—These attacks are based on links that do not correspond to the destination they describe, or the use of Internet Protocol (IP) addresses instead of universal resource locators (URL) for confusing the user. Other techniques deploy hidden frames. These are used for covering the real activity of a web page by using several frames with malicious content, while the user sees only the URL of the master frame set. Other methods use graphics that spoof the interface of a web browser, such as the address bar.
- **CC attacks**—This type of attack focuses on communication links. Examples include:
  - CC1: Pharming—These involve compromising domain name servers (DNSs), altering DNS tables and connecting the user to fraudulent sites, instead of the official bank’s site, where information regarding the user’s account may be derived.
  - CC2: Sniffing—Active sniffing attacks masquerade the two communicating entities to each other (user client and the Internet banking server) to capture information, such as username and password. Passive sniffing captures information from the communication medium, without interception.
  - CC3: Active man-in-the-middle attacks—This type of attack regards a schema where the attacker receives and forwards information between the UT and the IBS. The attacker sends malformed user packets or injects new traffic, such as transfer commands, from one account to another.
  - CC4: Session hijacking—Attacks that force the user to connect to the IBS with a preset session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user’s identity.
- **IBS attacks**—These types of attacks are offline attacks against the servers that host the Internet banking application. Examples include:
  - IBS1: Brute-force attacks—Brute-force attacks in certain password-based mechanisms are reported to be feasible by sending random usernames and passwords.<sup>13</sup> The attacked mechanisms implement a scheme based on guessable usernames and four-digit passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username- or password-based

calculation. This attack may be combined with username filtering methods for determining the identity of the user. These methods filter the different responses of the server, in the case of valid or invalid usernames.

- IBS2: Bank security policy violation—Violating the bank’s security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer’s account.
- IBS3: Web site manipulation—Exploiting the vulnerabilities of the Internet banking web server may permit the alteration of its contents, such as the links to the Internet banking login page. This may redirect the user to a fraudulent web site where his/her credentials may be captured.

## Security Analysis

The attack tree is used to gain a comprehensive view on the different types of attacks, the analysis of which should facilitate the process of studying the adequacy of existing countermeasures used by banks. This article focuses on the state-of-the-art authentication mechanisms and studies their robustness against the attack tree. **Figure 2** presents the applicability of attacks in different authentication mechanisms.

UT/U3 attacks are examined only for hardware tokens, while IBS2 attacks are applicable to all types of authentication methods, since they are attacks from the inside and may bypass them all. The terms in **figure 2** are explained in the following subsections.

### Static Password

The most common authentication mechanism, the static password, is based on proof by knowledge. Password-based mechanisms are widely utilized in Internet banking applications. Even in the case of custom non-web-based Internet banking software, the authentication process is usually password-oriented. This mechanism is prone to all types of attacks, excluding those customized to smartcards, which are not applicable, and IBS2, which regards an internal attack. Capture, replay, guessing or phishing are common and effective attacks. It is taken for granted that password authentication takes place through a Secure Sockets Layer (SSL) channel after authenticating IBS, which is a standard approach that banks follow. Static passwords, however, may be captured when attacking the secure channel establishment process (e.g., by deploying sniffing attacks as described later in this article, where the SSL channel is split to one SSL channel between the UT and the attacker and another between the attacker and IBS). The splitting may be performed in one-way SSL authentication (using only the certificate of the IBS) by sending fraudulent certificates to the user, who usually does not check the true origin and validity.

### Soft-token Certificate/SSL-TLS

This mechanism conducts mutual authentication between the UT and IBS, based on certificates stored in the user’s browser. The mechanism is prone to UT/U2 attacks, which compromise the UT, where the user certificate is stored. The latter may permit access to the user certificate, resulting in identity theft.

**Figure 2—Applicability of Attacks in Different Authentication Mechanisms**

Attack/Authentication Method	Static Password	Soft-token Certificate/SSL-TLS	Hard-token Certificate/SSL-TLS	One-time Password/Time-based Code Generator	Challenge-response	Biometrics	Knowledge-based
UT/U1a: User surveillance	A	X	X	A	X	X	X
UT/U1b: Token/notes theft	A	X	A	A	X	X	X
UT/U2a: Hidden code	A	A	A	A	X	A	A
UT/U2b: Worms	A	A	A	A	X	A	A
UT/U2c: E-mails with malicious code	A	A	A	A	X	A	A
UT/U3a: Smartcard analyzers	X	X	A	A	X	X	X
UT/U3b: Smartcard reader manipulator	X	X	A	X	X	X	X
UT/U3c: Brute-force attacks with PIN calculators	X	X	A	A	X	X	X
UT/U4a: Social engineering	A	X	X	X	X	A	A
UT/U4b: Web page obfuscation	A	X	X	X	X	A	A
CC1: Pharming	A	X	X	A	A	A	A
CC2: Sniffing	A	X	X	A	A	A	A
CC3: Active man-in-the-middle attacks	A	X	X	A	A	A	A
CC4: Session hijacking	A	X	X	A	A	A	A
IBS1: Brute-force attacks	A	X	X	A	X	A	X
IBS2: Security policy violation	A	A	A	A	A	A	A
IBS3: Web site manipulation	A	X	X	A	X	A	A

**Legend**  
A: Applicable  
X: Not Applicable

**Hard-token Certificate/SSL-TLS**

This mechanism is based on the “proof by possession” principle, since the user possesses an object as a token toward authentication. The use of hardware tokens addresses the vulnerabilities of storing the certificate in the user’s browser. This mechanism, however, is prone to a number of hardware (UT/U3) and software attacks, which analyze the operation of the hard token. Other attacks (UT/U2) exploit vulnerable interfaces of the hard token, which may permit unauthorized hard-token commands, such as digital signing, leading to identity theft. Token theft (UT/U1b) is also an issue, but it has to be combined with the PIN compromise.

**One-time Password/Time-based Code Generator**

This mechanism may also fall in the category of proof by possession authentication mechanisms. One-time passwords are generated by a random calculator, using a seed that is preshared between the user’s device (protected by a PIN) and the IBS. In mobile banking, the random codes may be submitted to the UT by the mobile operator through SMS, or generated by an application downloaded to the user’s mobile device. The user reads the SMS or software/hardware-generated code and provides the one-time code to the banking application for authentication. These mechanisms are prone to a number of attacks, including the regular device theft attacks (UT/U1b), combined with user surveillance (UT/U1a) or notes theft for obtaining the PIN. More sophisticated attacks are deployed exploiting the PIN time window (UT/U3c). This fact makes brute-force attacks possible (IBS1), since the likelihood

of guessing possibilities is increased. Other attacks (UT/U2, CC, IBS3, UT/U1a) are also possible since the codes are submitted through the browser, but for a very limited time frame (as long as the code is active plus the time window). Hardware attacks (UT/U3) are also possible by deploying the hardware analysis methods presented in the attack tree description.

**Challenge-response**

This mechanism is similar to the previous one, adding uniqueness to the authentication process. IBS generates a challenge that is processed by the UT/U for producing a response. Challenge-response is prone to man-in-the-middle and session hijacking attacks (CC), since an entity may intercept the communication between the UT/U and IBS, and capture and replay messages or use the predefined session method described in the attack tree description.

**Biometrics**

Biometrics provide strong authentication by adding the “proof by property” principle, completing or substituting the existing “proof by knowledge” and “proof by possession” mechanisms. Biometrics-based mechanisms, however, should be created by following best practices and standards to reach an acceptable security level.<sup>14</sup> Internet banking applications incorporating biometrics have been introduced by realizing the common scenario of identity verification by the remote comparison of a biometric template (comparison of the enrolled template at IBS, with a template generated by a

biometric measurement at the time of authentication). Other state-of-the-art scenarios describe local biometrics authentication for gaining access to a device or token. Biometrics are prone to malicious code attacks (UT/U2), phishing attacks (UT/U4) and communication links (CC) that may expose the user's personal data and threaten the whole security chain, since biometric templates may be compromised and replayed. For example, phishing techniques in architectures that require remote biometric template comparison may request the submission of the user template (even in encrypted form) and resend them to the IBS for compromising the user's bank account.

### **Knowledge-based**

This mechanism consists of a number of questions that the user has to answer to gain access to the account. This could be also considered as behavioral biometric authentication, depending on the content of the questions or, instead, a more sophisticated combined password mechanism. Although this mechanism is resistant to UT/U1 attacks, it is prone to most of the remainder attack types, since malicious code may copy answers and create a knowledge database for the user (UT/U2). The user may also answer questions from an attacker, due to being tricked by phishing (UT/U4), man-in-the-middle attacks (generally CC) or malformed IBS web sites (IBS3). Brute-force attacks are difficult to deploy due to the multitude of possible answers.

### **Countermeasures**

To reduce risk, the IS auditor, security consultant or security officer should be able to propose countermeasures to reduce risk. To implement security, authentication mechanisms that complement each other's resistance to attacks may be confined by identifying the appropriate patterns in **figure 2**. For example, hard tokens may be combined with biometrics and supported by a number of countermeasures toward a mechanism that is resistant to all of the attacks described in the attack tree. Specific additional countermeasures are described in **figure 3**.

To explain more clearly the role of countermeasures in the whole process, as well as to demonstrate the function of the proposed framework, the results of a security assessment that was conducted for the Internet banking authentication mechanism of a major bank are presented in the next section.

### **Case Study**

The security assessment was implemented to evaluate the security level of the Internet banking authentication mechanism, taking into account all entities involved in the process, and propose the necessary countermeasures for risk reduction. The Internet banking authentication mechanism was based on three different methods that the user was able to choose, depending on his/her particular needs: password-based authentication, PIN calculators and software-based certificates. The system also displayed a short security policy for the end user. The bank was also already audited for compliance with Basel II.

The first step was to collect information about the system. This information was collected from the system's manuals, implementation reports, on-spot visits and interviews with personnel. System information included system design, implementation details, history of security events, configuration files and existing audit reports.

The second step was to deploy the attack tree for identifying vulnerabilities and deciding on the applicability of attacks. For this purpose, the information gathered from the first step was analyzed.

The third step was to identify the appropriate countermeasures from **figure 3** and create a blueprint of combined countermeasures to enhance the system's security level. The report, including vulnerabilities, possible attacks and countermeasures, was delivered to the bank's security officer, and an executive summary was presented to the bank's management for decision making. The results of the assessment are:

- UT/U1a: User surveillance (piggybacking)/UT/U1b: Theft of token and handwritten notes—The introductory notice of the system did not include all necessary precautions and was written in the form of a paragraph. The use of bulleted items was proposed to display more clearly a few important user awareness rules, including rules on using strong passwords and focusing on the importance of token physical security, as well as the following:
  - Do not write down passwords.
  - Do not enter passwords with other people watching.
  - Do not share passwords.
- UT/U2a: Hidden code/UT/U2b: Worms and bots/UT/U2c: E-mails with malicious code—To address this issue within the framework of the assessment, a set of policies was created for guiding the users in protecting their personal computers. This involved the creation of an e-mail policy for secure attachment handling (basic directions are provided in COBIT). A set of guidelines was also created for installing the appropriate types of security software, including antispyware, personal firewalls and intrusion detection systems, involving all types of countermeasures included in **figure 3**.
- UT/U3a: Smartcard analyzers/UT/U3b: Smartcard reader manipulator—The characteristics provided by the smartcard and smartcard reader manufacturer were analyzed. Noise generators were implemented in the smartcards, and the specifications indicated the necessary countermeasures for a neutral code architecture.
- UT/U3c: Brute-force attacks with PIN calculators—The PIN calculator provided by the bank produced a six-digit PIN. The number of digits is considered adequate and no changes were proposed.
- UT/U4a: Social engineering—The user policy developed also covered the countermeasures presented in **figure 3**.
- UT/U4b: Web-page obfuscation—To address these attacks, a combination of countermeasures was proposed. First, a rule was added in the user policy, stating that the user should store the exact URL of the bank and use only this URL for accessing the Internet banking service. Furthermore, it was suggested that the bank should monitor names similar to the bank's domain names to be alerted. The registration of similar

**Figure 3—Additional Countermeasure Selection**

Attack	Countermeasure
UT/U1a: User surveillance	Security policy according to CoBIT <sup>15</sup> and ISO 17799 <sup>16</sup> regarding token and password handling, clear desk policy and screen surveillance
UT/U1b: Theft of token and handwritten notes	
UT/U2a: Hidden code	Operating system/browser patching Code installation blockers Antispyware software Antiphishing software (URL inspection) Firewall for blocking inbound and outbound connections to unauthorized ports Intrusion/anomaly detection Browser security best practices (cookies, window pop-ups, java support, etc.)
UT/U2b: Worms and bots	Operating system/browser patching Code installation blockers Firewall for blocking inbound and outbound connections to unauthorized ports Intrusion/anomaly detection Browser security best practices Antispyware software Custom application secure coding
UT/U2c: E-mails with malicious code	E-mail policy according to CoBIT and ISO 17799 Code installation blockers Attachment blocking HTML code blocking Antispam software Antispyware software Antiphishing software (URL inspection) Firewall for blocking inbound and outbound connections to unauthorized ports Intrusion/anomaly detection
UT/U3a: Smartcard analyzers	Noise generators Power- and time-neutral code design
UT/U3b: Smartcard reader manipulator	Secure smartcard interface design and implementation <sup>17</sup>
UT/U3c: Brute-force attacks with PIN calculators	Increased number of digits—at least an eight-digit code <sup>18</sup>
UT/U4a: Social engineering	Security awareness Simple, easy-to-remember URLs Antiphishing software (URL inspection)
UT/U4b: Web page obfuscation	Use of a predetermined list of valid URLs Prohibiting the use of IP addresses instead of URLs DNS monitoring
CC1: Pharming	DNS security countermeasures: prevention, detection, reaction countermeasures (e.g., depending on the implementation, appropriate firewall, intrusion detection and prevention, patch management), DNS SEC <sup>19</sup> best practices, Internet Engineering Task Force (IETF) requests for comments (RFCs): 4033, 4034 and 4035
CC2: Sniffing	Mutual authentication and encryption through client-server SSL Use of predetermined SSL certificates
CC3: Active man-in-the-middle attacks	Mutual authentication and encryption through client-server SSL Use of predetermined SSL certificates
CC4: Session hijacking	State management to prevent session ID specification in the message, session ID rotation and life cycle management
IBS1: Brute-force attacks	Prevention, detection and reaction countermeasures (firewall, intrusion detection and prevention) to detect and block attacks (the use of adequate mechanisms from <b>figure 2</b> is mandatory)
IBS2: Bank security policy violation	Security policy implementation according to CoBIT and ISO 17799
IBS3: Web site manipulation	Standard prevention, detection and reaction countermeasures (e.g., depending on the implementation, appropriate firewall, intrusion detection and prevention, patch management, web server security best practices—depends on the web server deployed)

domain names to the legitimate ones is a common method that phishers use for attracting victims. This domain name monitoring service is available on the security market. Finally, it was suggested that domain name expiration should

also be taken into account, and updates should always be conducted on time.

- CC1: Pharming—The DNS server was hosted by the bank. A gap analysis was conducted with the specifications of DNS

SEC best practices; this involved an examination of the server's architecture and configuration files. Since compliance was not identified, specific suggestions were made, including the use of digital signatures for message origin authentication and integrity, specifically for data regarding the DNS zones involved. Technical details can be found at IETF RFCs 4033, 4034 and 4035.

- CC2: Sniffing/CC3: Active man-in-the-middle attacks—SSL authentication and tunneling were implemented by the bank. However, it was strongly suggested that the bank at least provide to users a disk with the bank's digital certificate, upon registration. This low-cost solution should at least ensure that the user uses the correct server certificate for the SSL handshake, ensuring the creation of legitimate SSL tunnels. Otherwise, tricking the user with phishing attacks and providing fake certificates makes the use of SSL between the user terminal and the other end useless, permitting man-in-the-middle attacks and credential compromise through sniffing.
- CC4: Session hijacking—The Internet banking authentication application was analyzed. Although the session IDs provided were unique, there was a possibility to receive session IDs within a URL by the application. This would permit stating a specific session ID of an already authenticated session and compromising the user's account. This important flaw was reported to the bank, with the guideline to implement a rule for discarding duplicate session IDs (in that way, the authenticated session may exist but the attacker would not be able to hijack it) and not permit that type of information within the HTTP packets sent by the user. An expiration time for the session IDs was also suggested for additional security.
- IBS1: Brute-force attacks—The intrusion detection systems and firewalls were appropriately configured to discard information from sources that send abnormal amounts of authentication requests.
- IBS2: Bank security policy violation—The security policy was developed according to ISO 17799 and certified according to British Standard (BS) 7799:2. Several audits were implemented, including COBIT and Basel II compliance.
- IBS3: Web site manipulation—A number of vulnerability assessments were conducted for the servers hosting the Internet banking web site, separating work in three parts: operating system, web and application server, and Internet banking application. The assessments did not indicate any major inconsistencies, the operating systems were hardened, the web and application servers were configured according to the security best practices, and the analysis of the application code did not reveal vulnerabilities.

The final step was to ensure that the proposals addressed the vulnerabilities of each authentication technology used by the bank, by deploying **figure 2**. All vulnerabilities applicable for the three authentication mechanisms (password, PIN generator and soft certificates) were addressed by the countermeasures proposed.

## Conclusion

Assessing the security of Internet banking applications requires specialized knowledge on vulnerabilities, attacks and

countermeasures, to gain an understanding of the threats, how they are realized and how to address them. The case study in this article demonstrated that the use of the attack tree should facilitate the work of auditors, security consultants or security officers who wish to conduct a security assessment of an Internet banking authentication mechanism.

## Endnotes

- <sup>1</sup> Schaaf, J.; "E-banking—Five Online Banking Trends in 2005," Deutsche Bank research paper no. 13, 2005
- <sup>2</sup> Hole, J.K.; V. Moen; T. Tjostheim; "Case Study: Online Banking Security," *IEEE Security and Privacy*, vol. 4, no. 2, 2006, p. 14-20. Hiltgen, A.; T. Kramp; T. Weigold; "Secure Internet-banking Authentication," *IEEE Security and Privacy*, vol. 4, no. 2, 2006, p. 21-29. Ollman, G.; *The Phishing Guide—Understanding and Preventing Phishing Attacks*, NGS-NISR, 2004.
- <sup>3</sup> ISACA, IS Auditing Guideline, Internet Banking, G24, 2003
- <sup>4</sup> Basel Committee on Banking Supervision, "Risk Management Principles for Electronic Banking," July 2003
- <sup>5</sup> Federal Financial Institutions Examination Council, "Authentication in an Internet-banking Environment," 2001
- <sup>6</sup> International Organization for Standardization, "Public Key Infrastructure for Financial Services—Practices and Policy Framework," ISO 21188, 2006
- <sup>7</sup> *Op. cit.*, ISACA
- <sup>8</sup> Schneier, B.; "Attack Trees," *Dr. Dobb's Journal*, vol. 24, no. 12, 1999, p. 21-29
- <sup>9</sup> Gandolfi, K.; C. Mourtel; F. Olivier; "Electromagnetic Analysis: Concrete Results," *Lecture Notes in Computer Science*, vol. 2162, 2001
- <sup>10</sup> *Op. cit.*, Hiltgen, Kramp and Weigold
- <sup>11</sup> *Op. cit.*, Hole, Moen and Tjostheim
- <sup>12</sup> *Op. cit.*, Ollman
- <sup>13</sup> *Op. cit.*, Hiltgen, Kramp and Weigold
- <sup>14</sup> Dimitriadis, C.; D. Polemi; "Biometrics—Risks and Controls," *Information Systems Control Journal*, vol. 4, 2004, p. 41-43
- <sup>15</sup> IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, 2005
- <sup>16</sup> *Op. cit.*, Hole, Moen and Tjostheim
- <sup>17</sup> *Op. cit.*, Hiltgen, Kramp and Weigold
- <sup>18</sup> *Op. cit.*, Hole, Moen and Tjostheim
- <sup>19</sup> [www.dnssec.net](http://www.dnssec.net)

## Christos Dimitriadis, Ph.D., CISA, CISM

is a researcher at the University of Piraeus (Athens, Greece), where he specializes in prevention, detection and response IT security mechanisms. His research interests include 3G and 4G security architectures, identity management (he is a founding member of the Mobile Government Study Group), honeynets, and security protocol design and testing. He has been invited by several organizations, including the International Telecommunication Union, US National Institute of Standards and Technology and several agencies of the European Union, to provide lectures.

*Information Systems Control Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© Copyright 2007 by ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

[www.isaca.org](http://www.isaca.org)