

Understanding the FDIC's Report on Account-Hijacking Identity Theft

Executive Insight Series

Jonathan G. Gossels & Richard E. Mackey, Jr.

Introduction

On December 14, 2004, the Federal Deposit Insurance Corporation (FDIC), released a report that presents the FDIC's findings on unauthorized access to financial institution accounts and how the financial industry and its regulators can mitigate these risks. The report is entitled, *Putting an End to Account-Hijacking Identity Theft* and can be found at:

http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf

This report comes at a time when virtually every financial institution is rethinking its requirements for remote customer authentication. The industry is starved for guidance in this area. In addition, it explains the types of attacks, gives background from various sources citing statistics on the likelihood of attacks, and provides a summary of technologies that can help prevent account-hijacking attacks.

While it is challenging to distill a 41 page report into a few bullet points, SystemExperts believes that the study's key findings are:

- "...single-factor, password-based authentication methods may no longer be sufficiently secure for customer remote access to online banking systems"
- "The FDIC anticipates that as customers become more aware of actual instances of, or the potential for, account-hijacking, they will expect financial institutions to implement solutions that protect their funds and their identities, while maintaining or increasing the level of convenience for them in accessing financial services"

Its primary recommendation is:

- "two-factor authentication should be considered as a new security baseline for remote access to computer systems"

The FDIC report does not address the business or practical issues of implementing two-factor authentication solutions. Compared to today's username/password authentication approach, two-factor authentication mechanisms are expensive to deploy, expensive to maintain, and inconvenient to use. Financial institutions will need to fully understand the costs and user-experience issues associated with these authentication mechanisms before implementing the FDIC's recommendation.

Background and Focus of Study

The Federal Trade Commission (FTC) has estimated that almost 10 million Americans were victims of identity theft in 2003, with a total cost to businesses and consumers approaching \$50 billion. Identity theft is one of the fastest growing types of consumer fraud.

The FDIC study focuses on a subset of identity theft – unauthorized access to and misuse of existing asset accounts primarily through phishing and hacking. The study uses the term *account-hijacking* to describe this particular form of identity theft.

The study makes the point that precise statistics on account-hijacking are not available. However, it asserts that unauthorized access to checking accounts is the fastest growing form of identity theft and the FTC estimates that approximately two million U.S. adult Internet users experienced this fraud during the twelve months ending April 2004. Not surprisingly, more than half believed responding to a phishing e-mail to be the cause.

The study notes that a 2002 survey conducted by the American Bankers Association reveals that identity theft fraud is the top concern among financial institutions of all sizes.

Definitions

The term *identity theft* is new. The definition was first codified as part of the Identity Theft and Assumption Deterrence Act of 1998 (ID Theft Act). This law made identity theft a Federal crime. Later, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) amended the Fair Credit Reporting Act (FCRA) to include a civil definition of identity theft as well. Under FACTA, the Federal Trade Commission was charged with further refining the definition and it has recently addressed a prior deficiency by specifying what constitutes *identifying information*.

“The term “identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any –

- (1) Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) Unique electronic identification number, address, or routing code; or
- (4) Telecommunication identifying information or access device...”

How Accounts are Hijacked

There are several ways to hijack deposit accounts; each relies on the misuse of information:

- Phishing – collecting identity information by directing users to fraudulent web sites via email requests.
- Hacking – direct cyber attacks on web sites, transactions with web sites, or systems housing personal information.
- Retrieving hard copy documents (dumpster diving) or looking over someone’s shoulder.
- Insider data gathering – attacks from inside an organization entrusted with personal information.
- Key stroke logging – a particular form of hacking that attacks the client system and records user names, passwords, and other personal identifying information for use by the attacker.

The study notes that 70 percent of identity theft is committed with confidential information stolen by insiders. It also notes that phishing is easy to implement and produces higher volume results than the other techniques.

Industry Response

The FDIC report makes the point that financial institutions can help reduce identity theft, including account-hijacking, by encouraging information sharing so that identity theft frauds are thwarted sooner. It describes a number of information sharing efforts including Financial Services Information Sharing and Analysis Center (FS-ISAC), the Anti-Phishing Working Group (APWG), the Identity Theft Assistance Corporation (ITAC), and the FBI’s Infragard program. Of these, let’s look at two in particular.

The Anti-Phishing Working Group is an industry association with 630 members composed of financial institutions, e-commerce providers, Internet service providers, and vendors of e-mail services and software. As its name implies, its purpose is to eliminate identity theft and fraud resulting from phishing and e-mail spoofing. It is seeking to provide resources, technology, vision, and expertise to facilitate the rapid deployment of a solution to e-mail phishing scams.

On December 12, 2003, the APWG published a white paper entitled, “Proposed Solutions to Address the Threat of E-mail Spoofing Scams.” The whitepaper offers four solutions:

- Strong web site authentication
- Mail server authentication
- Digitally signed e-mail with desktop verification
- Digitally signed e-mail with gateway verification

While these are good solutions, they require industry cooperation and user adoption to be effective. Realistically, these solutions are a long way off.

Another industry initiative has been the establishment of the Identity Theft Assistance Corporation (ITAC). Formed under the auspices of the Financial Services Roundtable and the Banking Information Technology Secretariat (BITS), ITAC’s purpose is to help victims of identity theft to recover their financial identities and restore their credit ratings.

Technology Survey

Approximately half of the FDIC report is dedicated to a survey of technologies that may be effective in mitigating account-hijacking. The FDIC staff evaluated three types of technologies: scanning tools, e-mail authentication, and user authentication. The FDIC then applied relative ratings based on ease of implementation, portability, effectiveness, and ease of customer use.

The technologies evaluated included:

- Scanning tools to find web sites with text that matched specific alert patterns (e.g., match an institution's name, trademark, or slogan)
- Server log analysis software to help detect suspicious activity
- E-mail authentication (Sender ID) to verify that each e-mail message originated from the Internet domain from which it claims to have come
- User authentication to verify the identity of a person or entity
 - o Shared secrets
 - o USB tokens
 - o Smart cards
 - o Password generating tokens
 - o Biometrics
 - Fingerprint recognition
 - Face recognition
 - Voice recognition
 - Keystroke recognition

Challenges

The report recognizes that choosing a technology to deliver an effective two-factor authentication system for financial institutions presents some unique challenges. Customers expect to have immediate and unobstructed access to their accounts regardless of where they happen to be or what time it is. Currently, as long as a user remembers his password, this access is delivered reliably. Two-factor authentication must be capable of providing that same level of dependable access while also satisfying the financial institution's requirements for reliability, security, value, ease of implementation, and operations.

Findings

In the report, the FDIC finds that there are two major reasons why the frequency of phishing and other types of attacks have been increasing and have become more effective at perpetrating account-hijacking.

- User authentication by the financial services industry for remote customer access is insufficiently strong.
- The Internet lacks e-mail and web site authentication.

It recommends that financial institutions and government should take the following steps to reduce on-line fraud:

- Upgrading existing password-based single-factor customer authentication systems to two-factor authentication.
- Using scanning software to proactively identify and defend against phishing attacks. The further development and use of fraud detection software to identify account-hijacking, similar to existing software that detects credit card fraud, could also help to reduce account-hijacking.
- Strengthening educational programs to help consumers avoid online scams, such as phishing, that can lead to account-hijacking and other forms of identity theft and take appropriate action to limit their liability.
- Placing a continuing emphasis on information sharing among the financial services industry, government, and technology providers.

Final Word

SystemExperts applauds the FDIC for taking a stand on this important issue. The information provided by the report will help financial institutions and consumers to better understand the problem, potential mitigation approaches, and the limitations of those solutions. However, without addressing the practical issues of deploying two-factor authentication systems at a large scale and without addressing the numerous ways account-hijacking can occur even with two-factor authentication, SystemExperts believes that the report's finding that two-factor authentication is required is exaggerated and premature.

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, VPNs, and Windows security at USENIX, Network-Interop, CSI, and many other conferences are among the highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio. Every single full-time staff member is certified in some critical security area.

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long-term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients. www.systemexperts.com/services.html

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. Some of the more frequent tests that we perform include "White Hat" penetration testing, web application vulnerability assessments, dial exposure ("war-dialing") reviews, firewall analysis, host hardening analysis, IP services inventory, wireless LAN inventory, VPN assessments, and denial of service reviews.

Security Blanket, Emergency Response & Incident Response "Scrimmage"

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment. We can also help you prepare for these inevitable events by practicing your response through our acclaimed Incident Response "Scrimmage" Training Exercise. With our Security Blanket™ service, you'll be able to sleep at night knowing a team of security experts is on your side and *watching your back*. In addition to performing quarterly penetration tests, we'll notify you of virus attacks and vendor vulnerabilities that affect your infrastructure, and monitor a collection of hacker sites and alert you if your organization is ever mentioned.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest intrusion, firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in Windows, Unix, and other heterogeneous environments. We also provide interim staffing up to the CISO level.

Accelerated Security AssessmentsSM & Code Reviews

Using our innovative and highly interactive Accelerated Security AssessmentSM methodology, our consultants will work with your team to perform a quick but comprehensive review of the security of applications or systems in their full environmental and business context and help you to understand and apply industry best practices. You may use this as the jumping off point for planning and prioritizing security initiatives. Our clients value both the short duration and the immense knowledge transfer that occurs during these intense Accelerated Assessments.

SystemExperts uses this Accelerated Security AssessmentSM methodology in a wide range of services including:

- ISO 17799 Assessment
- Sarbanes-Oxley Security Assessment
- COBIT Assessment
- Wireless Security Assessment
- Best Practices Security Assessment
- Application Service Provider Security Assessment
- Authentication and Authorization Security Assessment
- Application Security Assessment
- PeopleSoft Security Assessment
- Billing System Security Assessment
- Anti-Virus Security Assessment
- Security Architecture Assessment

Security Policy, Best Practices, & Strategy

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice. Over the past ten years, we have assisted some of the largest financial institutions in the world in developing their overall security architectures.

Intrusion Detection & Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston

Los Angeles

New York

San Francisco

Tampa

Washington DC

www.SystemExperts.com

info@SystemExperts.com