Realtime
publishers

Strengthening Application Security with Identity Fraud Prevention Systems

The Essentials Series

The Evolution of Identity Verification and Authentication from Static to Data-Driven Questions

sponsored by

ACXIOM®
WE MAKE INFORMATION INTELLIGENT™

Ken Hess

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

The Evolution of Identity Verification and Authentication from Static to Data-Driven Questions

Data providers and application developers have learned much about data security over the past decade. The greatest lesson learned was that of using dynamic questions in the identity-proofing process. Data depth and breadth allow a more diverse data set from which to pull questions. Additionally, a large data set allows for more random sampling of the data so that the same questions are so rarely repeated that identity theft is discouraged.

Static Questions Are “Old School”

Security experts have correctly concluded that static knowledge-based authentication questions are outdated and susceptible to “low-tech” hacking and social engineering. Static knowledge-based authentication questions typically take the form of forgotten account user name or password verification. Static questions are easy to set up and maintain for the institution that creates and uses them. They’re also somewhat convenient for the end user. The downside is that static questions are absolutely the least secure method of implementing knowledge-based authentication. It’s really the “lazy” solution to a potentially very expensive problem.

Static Questions and Social Engineering Risks

Have you had the opportunity to receive a corporate email sent from the highest levels in your organization warning of the perils of social engineering yet? If you haven’t, you soon will. Social engineering is a low-tech and very effective method of hacking.

A popular method of social engineering is for a hacker to pose as an employee and to call an actual employee with an urgent need to connect to a system or to gain access to a password-protected Web-based application. The fake employee has lost or forgotten some critical piece of information or secure hardware token but needs immediate access to a restricted area or system.

Note

The Computing Dictionary defines *social engineering* as cracking techniques that rely on weaknesses in wetware (humans) rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system’s security.

Sometimes the caller will pose as a third-party service tech that doesn't have access to something that he needs hoping that you'll have access or can assist him in gaining it. The unsuspecting and eager-to-assist employee will often reveal passwords, access portals, or "loan" the hacker his own credentials. Clever hackers will assure the helpful participant with the advice that he should change his password immediately after the hacker has gained access, performed his necessary work, and left the premises.

Dynamic Questions and Risk Mitigation

Social engineering is ineffective against a dynamically-created set of knowledge-based questions. It's ineffective because the number of questions created make it unlikely that anyone could be tricked into answering a set of very personal and random questions generated from a database. These kinds of questions don't come up in casual conversations. For example, questions such as "Who holds your home mortgage?" and "What's your sister Janet's home address?" would be met with suspicion and a report to your bank that a hack attempt was made on you and your accounts.

Greater Data Depth and Breadth Allow for Greater Randomization

Think of a number between one and ten. Did you pick three? With only ten choices, your chances of guessing a number correctly are very good—so good, in fact, that data providers realize that your data isn't safe at low data depth and breadth.

If you were given the option of choosing a number between one and one hundred, you can see how the probability of guessing your response would decrease dramatically. Data depth and breadth allow for greater randomization of questions and therefore decrease the likelihood of correct guesses that lead to identity theft.

Avoiding Pre-Loaded Answers to Security Questions

Pre-loaded answers and static questions are an identity theft's perfect scenario. "What is your mother's maiden name?" is not a secure question nor is the answer. Anyone can easily find the answer to that question. But how many people would know how much your monthly car payment is or how much money is in your home mortgage escrow account? The next iteration of the dynamic exam would have new questions. Your mother's maiden name hasn't changed since the last time you forgot your password.

Business to Business Solutions

Business to business (B2B) applications that rely on network operating systems (NOSs) or Active Directory (AD) domains for authentication to an application rely on simple password challenge and response for that authentication. An attempt at an added layer of security using IP-based allowed hosts is also inadequate as a highly secure authorization method because IP addresses are easily spoofed (faked).

The threat of identity theft is too great to rely on simple password logons and allowed hosts lists. These methods have proven unreliable in multiple trials and in the real world with compromised security, hacked passwords, low-tech hacking—leading to rampant identity theft that costs businesses billions of dollars per year in lost revenue.

The Need for Multiple Layers of Identity Verification and Authentication

Simple password authentication schemes don't work. And it doesn't matter how many passwords you require a user to remember—the scheme is too weak for individual authentication and its weaknesses multiply when you consider the sensitive data exchanged between businesses. Password authentication is the poorest method of identifying and authenticating users to an application.

Security analysts realized the failure of password authentication for applications that need higher levels of protection against fraud and theft. The answer to the password security quandary revealed itself when multi-factor authentication became known. Identity proofing involves multiple factors and provides secure and reliable verification and authentication for online transactions.

Removing the Threat of Identity Theft

Identity theft incidents have increased by double-digit rates every year for the past 10 years. It is now the fastest growing technology-related crime threat in the world. From coordinated high-tech sponsored attacks to social engineering and low-tech "over the shoulder" password theft, identity theft is big business.

Identity theft prevention is the primary focus of data providers and the businesses that purchase their services and data. This focus led to the creation of secure connectivity schemes between user applications and the data they query. It also led to the creation of broad data sets from which to create dynamic knowledge-based exams. The *threat* of identity theft may never be fully removed, but data security, broad data sets, and secure application design can minimize the success rate to near zero.

Identity Theft Has the Government's Attention

On April 23 and 24, 2007, the Federal Trade Commission (FTC) held an authentication workshop titled "Proof Positive: New Directions in ID Authentication." The 250 participants from the public and private sectors discussed current authentication methods, future authentication methods, and the development of more effective authentication tools. The FTC created a Web site (http://www.idtheft.gov) dedicated to identity theft, the President's Identity Theft Task Force, victim's rights, and how to report an incident.

Mitigating Future Threats in Cloud and Mobile Computing

The promises of cloud computing are many but so are its risks. Opponents point to leveraged hosting locations that might provide less security to low price hunting consumers. Proponents state that cloud computing's basic model enhances security due to its sheer scale and homogeneity.

Cloud Application Security Risks

The adoption and evolution of cloud computing brings up a host of questions about security for businesses and individuals and the trustworthiness of cloud-based applications. Is cloud computing more or less secure than standard computing platforms? Are data owners equally protected regardless of the location where their data resides? Are cloud computing providers responsible for your data's security? Could cloud computing lower security risks for businesses? These questions and uncertainties justify the need for a verification step prior to gaining access to sensitive systems and services.

Unfortunately, opinions vary widely on cloud computing and security. But one opinion echoes throughout the security community: Don't put highly sensitive corporate data in public clouds just yet, which reinforces the need for a secure verification step.

Cloud computing relies heavily on virtualization. Virtualization by itself isn't what makes cloud computing a less than desirable technology for some business applications but rather the lack of long-term information about the overall safety of the platform. A group of US government experts weighed in on their doubts about cloud computing security during a recent survey. The results weren't pro-cloud computing. As Gregor Wilsusen, Director of Information Security at the Government Accountability Office (GAO), puts it, "The use of cloud computing can also create numerous information security risks. These risks generally relate to dependence on the security assurances and practices of a service provider and the sharing of computing resources."

Assumptions and opinions concerning potential cloud computing's security vary from Google's assertion that, "Cloud computing can provide higher levels of security than most in-house IT" to the European Network and Information Security Agency's 125-page analysis "Cloud Computing Security and Risk Assessment" and recommendations for cloud computing governance and security.

The solution rests on cloud computing users (data providers and application developers) to ensure that their applications and data are secure. Service providers have responsibility for maintaining network and OS security but no responsibility for individual customer's applications. Therefore, it is important to select a data provider that maintains an extreme level of security for their data and their business customers with consulting to mitigate cloud computing's security shortfalls.

Mobile Computing and Wireless Security

Like cloud computing, mobile computing is fraught with security concerns. The future success of mobile computing depends on two factors: wireless security and application security. In addition to security questions regarding mobile computing is mobile computing's human factor. Mobile devices, by design, are small, lightweight, and convenient to use. They're also susceptible to security breaches through loss, theft, or careless use. The numbers of devices compromised in these ways justifies extra security through additional authentication steps prior to gaining access to information or systems.

Wireless security, signal encryption, stateful firewall settings, and hotspot connectivity requirements are outside the scope of data providers and application developers. Knowing the limitations of this control requires the provider and developer to create secure environments with which to work.

Cloud computing and mobile computing security challenges can best be met with correct handling of identity proofing. Well-designed identity proofing strategies and encrypted data transfer will mitigate even the most heinous security flaws perpetrated by service providers.

Consider the worst-case scenario of a hacker that eavesdrops on your session at a coffee shop with a wireless hotspot while you attempt to retrieve your password from your credit card company. The eavesdropper sees the questions and your answers to those questions as the answers cross the room from your wireless network interface to the coffee shop's hotspot and out to the Internet. The eavesdropper doesn't realize that the information is useless to him because the questions were created dynamically. Any subsequent exam won't have the same questions or answers. But, if the questions were static, the eavesdropper would have an open door to your account because the questions and their answers would never change.

Summary

A large, diverse data set protects you and your customers from identity theft and fraud by providing you with enough data from which to draw a huge repertoire of dynamic questions. The evolution from static questions to dynamic ones has been an expensive and arduous lesson to learn for businesses and consumers alike. Data providers that have created databases with great depth and breadth to mitigate security breaches related to static identity proofing questions offer strong application security.