Realtime publishers

Strengthening Application Security with Identity Fraud Prevention Systems

The Essentials Series

Overcoming the Regulatory, Security, and Compliance Concerns of Knowledge-based Authentication

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

Overcoming the Regulatory, Security, and Compliance Concerns of Knowledge-Based Authentication

Data security is a major concern for end users, customers, and data suppliers. On an almost daily basis, you read about massive security breaches of credit card information and user data. You want to know how secure your data is, how secure a data supplier's data is, and how knowledge-based authentication protects you and the consumer.

Understanding the Risks of Using Knowledge-Based Authentication

Knowledge-based authentication falls under the "something you know" category of multi-factor authentication. Knowledge-based authentication's basic premise is that there are things about you that you know but no one else does. But what's wrong with this concept? What's fundamentally wrong is that the common bits of information about you are not unknown to others and often they're easily guessed or they're easily extracted from you.

The "20 Questions" Test and Standard Knowledge-Based Authentication

If you spoke to a stranger and answered 20 questions about your pets, family, hobbies, vehicles, and personal beliefs, would he have your passwords to your bank accounts, computer, or credit card accounts? It's likely that he would. How will your new account be verified once it's created? Will the online application use a question and answer from the 20 questions bag or will it use something more sophisticated?

Standard Knowledge-Based Authentication Questions

- What is your mother's maiden name?
- What is your father's middle name?
- What was your first pet's name?
- What's the name of the elementary school you attended?
- What was your first car?

Standard knowledge-based authentication questions draw from a very small question bank (10 or fewer) and require a response from the user that others may know or find out through casual conversation.

Are You Hackable?

It's a fact that people love to talk about themselves. It's simple to find out just about any tidbit of information, no matter how personal, from someone by being a good listener and careful questioner. If a hacker knows where you bank or hold an online account, he can easily find out the limited list of questions used for knowledge-based authentication, match your answers, and hack into your account.

Revealing security secrets via friendly conversations, either in person or by phone, to a hacker is known as *social engineering*.

> **Note**
> Social engineering is the purposeful, egregious, and criminal act of manipulating an individual into revealing confidential information about themselves, others, or a business in order to exploit that information for personal gain.

Social engineering is one of the most successful forms of hacking because it doesn't require access to your personal property nor does it require any specialized software. In essence, it doesn't require the hacker to directly commit any unlawful acts against you in order to collect sufficient information necessary to gain access (or potential access) to your account information.

Appropriate Use of Knowledge-Based Data

You want to know that the entities using your information have a legitimate need to do so and that your privacy isn't compromised in the process. Known data about you that's kept in a database comes from dozens of sources. These sources and those who use them are subject to strict laws and rules about how the data are used. The federal government created laws protecting the privacy of individuals and have recognized the need for stringent guidelines regarding the access and the use of sensitive information.

How Are Data Points Gathered?

Data providers gather data points from a variety of public and private primary data sources. The following list shows potential data sources from which data providers might purchase or gather data:

- Drivers' license bureaus
- Voter registration
- Hunting and fishing licenses
- Recreational vehicle registration
- Carrying concealed weapons (CCW) registration
- Professional licensure
- Property information
- Legal information—Bankruptcies, judgments, and liens
- Aircraft registration
- Pilot registration
- Telephone directories
- Proprietary sources—Various national databases

Some data sources are preferred over others. Drivers' license information, for example, is considered to be the "gold standard" of data because its accuracy, currency, and completeness tie directly into states' legal systems for positive face-to-face and online identification of the licensee. Drivers' license data and records can include arrests and convictions associated with the license holder. Voter registration and property records also provide a very thorough set of data points for individuals.

How Secure Is My Data?

Data providers and agencies that use that data must comply with several federal laws concerning individual privacy. Laws are in place to govern the use and misuse of private information by credit reporting agencies, prospective employers, lending institutions, and anyone using consumer information upon which to make decisions for any kind of screening that might involve privacy risk, negligence, or discrimination. In addition to the Fair Credit Reporting Act (FCRA), companies that use this data must comply with the Fair and Accurate Credit Transaction Act (FACTA), Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), and others. Extracting, reporting, and using personal information is highly regulated. In addition to regulatory compliance, data providers, agencies, and employers use secure methods when querying and using online data.

The two-step identity proofing process also provides you with assurance that your data and your privacy are secure. It might seem that multi-factor authentication is painful for the legitimate user, but it is a process that's designed to be more painful for an identity thief to pose as a legitimate user.

What Are the Issues?

Too often, we hear of hacks, cracks, break-ins, and security compromises and think that it's just another part of our online life. It isn't. And it doesn't have to be. Security isn't a "nice to have," it's a requirement of any online transaction. Security is, or should be, a primary concern for any data provider. There's too much at stake for the provider, the individual, and the data customer to use less than the best available security technology, techniques, software, and hardware for protection. Your data provider should have multiple layers of physical, network, and data security in place.

Other issues of concern for data consumers are the number of data points available in the database you're accessing and the availability of customized data. The number of data points has to do with the breadth and depth of data gathered by the provider. Customized data refers to the provider's ability to deliver a subset of their data to you.

Security

According to the Federal Trade Commission (FTC), nearly 10 million people fall victim to identity theft annually. This costs consumers more than 5 billion dollars in losses and businesses lose more than 48 billion dollars. These dollar amounts make identity theft a very lucrative venture and increases the risks for businesses and consumers who want to conduct business online.

Data Points

Companies that need consumer data to securely do business with their clients often lack the expertise and the ability to adequately gather enough data points to offset security concerns with standard knowledge-based authentication. More data points equals greater security and greater protection for the business user and the consumer. Few data points leads to inadequate diversity and a limited bin from which to draw random quiz questions.

Customized Data

Businesses often don't need a "shotgun" approach to data. They need a more targeted approach on which to focus their efforts. Businesses with a limited range of influence won't need data from a population outside their defined commerce region. If a business only conducts business within 50 miles of Dallas, Texas, that company doesn't need or want data from Miami, Florida. Other than regionally customized data, providers can tailor data to fit almost any business need, demographic, or cross-section.

How Can a Third-Party Data Provider Reduce My Risk?

A third-party data provider reduces risk by giving you a one-stop shop for your aggregated data needs. The third-party provider, as a single contact point for your data, makes life easier for you because the provider takes care of regular updates, regulatory compliance issues, data store security, and data use licensing.

Added Security

Using a third-party data provider can reduce your risk as a data consumer, but their security has to be the best available. Security policies and acute vigilance are the primary defenses against over-the-network security breaches. A provider reduces your risk with their security measures and compliance with federal security mandates.

Security is a major issue for providers, their customers, and the individuals whose data rests on that security; the following list highlights key features of security policies and procedures that work:

- Regular security audits and network penetration testing
- Encrypted file transfers and communications
- Client site inspections and audits
- Disaster recovery
- Antivirus, anti-malware, and anti-phishing software
- 24×7×365 security monitoring
- The use of network buffer zones or DMZs
- Security-hardened operating systems (OSs)
- Stateful firewalls

Broader Data Set

A broad data set ensures that questions taken from that data represent a wider variety of possibilities and create questions that make correct answers far more difficult to guess. For example, if you lose your wallet, the answer to the question, "What is your monthly car payment?" probably wouldn't be something your wallet "finder" would know. Unlike, "What are the last four digits of the last credit card you used?" or "What is your zip code?," the car payment question is likely a question only the account holder would know. A broader data set allows you to pose several exam questions and several versions of an exam if a legitimate user should fail one.

Summary

With data security a major consideration, you want to know how secure your data is, whether a data supplier's data is secure, and whether your being protected by effective knowledge-based authentication methods. This article explored security and compliance issues surrounding the gathering and use of data assets. Next, we'll look at how data delivery has and will continue to evolve as well as the risks presented by cloud and mobile-based interactions.