Realtime publishers

The Essentials Series: Architecting the Right Solution for Strong Authentication

The Perils of Weak Authentication

sponsored by

by Jeffery Hicks

The Perils of Weak Authentication 1
What Is Weak Authentication? 1
How Weak Authentication Affects Your Business 2
Weak Authentication and the Bottom Line 2
What Is Strong Authentication? 3
Regulatory and Compliance Requirements 4
Strong Authentication and the Bottom Line 4

Copyright Statement

The Perils of Weak Authentication

In today's corporate IT environment, insufficient security (both data and physical), weak authentication, and silos of compliance reporting are hidden currents, much like an undertow at the beach, that can lead to data breaches and compromised systems. Your IT environment remains vulnerable to pervasive threats both internal and external. These limitations drive up the cost of compliance reporting, promote ad hoc solutions to security challenges, can hinder employee productivity, and decrease the company's ability to deliver competitively appropriate levels of customer service.

Fortunately, the right strong authentication solution (or strategy) can address these issues. With a combination of consolidated identity management, single sign-on services, and comprehensive compliance reporting, these systems can reduce compliance costs, improve security, and remove significant drags on productivity. Collectively, I'll refer to this as a strong authentication solution. However, it may be comprised of different elements from a variety of vendors depending on your business and sector requirements. Before you can realize the benefits of strong authentication, you must first understand ways in which weak authentication can hamper business operations and productivity.

What Is Weak Authentication?

To understand the need for strong authentication, it makes sense to understand and define its opposite. *Weak authentication* is generally the system we have had in IT for decades. A user attempts access to a resource and is challenged to identify themselves. As long as the user supplies the expected answer, such as a password, authentication is approved and access granted. I'm sure you can see the inherent weakness.

Imagine a user, Alice, approaching a locked door with a small slot in the center. Alice comes to the door and knocks. A voice from behind the door asks, "Who goes there?" Alice replies, "Alice" and takes a piece of paper from her purse, which she slides through the slot. After a moment, the door opens admitting Alice. Bob, being a curious and particularly nosy fellow, also wants to see what is behind the door. He knocks and announces himself. Bob scribbles something on a piece of paper and slides it through the slot since he observed Alice. The voice behind the door says, "Go away. You are not allowed." Bob repeats the process but announces himself as Alice and slides another piece of paper through the slot. The voice says, "Go away. You are not Alice." Later that day Bob sneaks into Alice's purse and makes a copy of her paper slips, or perhaps looks over her shoulder when she is creating them. Bob returns to the door, announces himself as Alice and slips in his purloined slip of paper. The door opens admitting Bob. Bob has effectively fooled the doorman into thinking he is Alice.

I'm sure you would agree that this authentication system is inherently weak. Bob can say he is anyone and the only proof is a slip of paper that confirms the identity. The problem is that there any number of ways Bob can obtain that very important slip of paper.

How Weak Authentication Affects Your Business

Weak authentication, as I've just illustrated, can have a negative impact on your company or organization. The most devastating impact is loss of data or services. Let's go back to Bob who has gained access to a room he's not supposed to be in. He may stumble around in the room breaking things or interfering with the operations within the room. It doesn't necessarily matter if his intentions are malicious or not, the consequences are the same.

> **Authorization vs. Authentication**
>
> Even though Bob has been authenticated and granted access to the room, he can only do things in the room for which he has proper authorization. Because he has been authenticated as Alice, he can do all the things that Alice can do; if Alice can turn off the lights, so can Bob. The problem with many IT organizations is that they neglect to look at authorization and focus solely on authentication. If Alice has no job requirement to be able to turn off the lights, then she shouldn't be authorized. However, if she is authorized, then protecting authentication becomes even more important.

To make it harder for Bob to pretend to be Alice, the company may ask Alice to use a very complicated password. She complies but because she has trouble remembering it, she keeps a copy taped to her monitor.

Some companies might ask Alice to frequently change her password, which she does by recycling old passwords that may or not have already been discovered by Bob. Or Alice may be in the middle of a major project only to be interrupted with a need to change her password.

Weak Authentication and the Bottom Line

Imposing password management responsibilities on Alice adds to her workload and reduces her productivity. If Alice is forced to come up with her own shortcuts to circumvent these responsibilities, this increases the likelihood of Bob stepping in—and who knows what Bob will do. The company could suffer a loss of data, which has a number of consequences from financial to regulatory and compliance failures to loss of goodwill.

Another problem with authentication is that most modern companies have multiple systems that require some sort of authentication. Here's a small sample. How many apply to your organization:

- Physical access to the building or a room
- Local Area Network (LAN) authentication
- Wireless network authentication
- Remote access and virtual private network (VPN) authentication
- Intranet authentication
- Internet-access authentication and control such as a proxy server
- Database authentication

- Internal application authentication
- Third-party or vendor authentication
- Extranet, vendor, or partner authentication

More than likely, poor Alice has to manage multiple passwords, all of which take time out of her day. Most likely, Alice will use the same password repeatedly, which means if Bob acquires her password for one silo, he has access to all of them.

Managing multiple passwords is not only a burden for the user but also for the IT administrators who must manage these siloed systems. More than likely, each system has its own requirements—not to mention the increasing number of regulatory and compliance requirements that often include some sort of auditing. The IT administrator cannot be efficient and productive when forced to manage these diverse and typically weak authenticated systems.

What Is Strong Authentication?

The answer to many of the issues raised is *strong authentication*. Let's return to Alice, Bob, and the locked room. Alice approaches the door and announces herself. She inserts her slip of paper through the door slot. However, now she also inserts her hand. The doorman on the other side checks the piece of paper *and* measures Alice's hand and compares it with her hand measurement on file. Since the measurements match, Alice is admitted. Bob approaches the door and announces himself as Alice. He inserts his copy of Alice's paper and then puts his hand in the slot. However, since his hand is different than Alice's, Bob is refused admittance. Short of lopping off Alice's hand, there is no way Bob can pretend to be Alice. Weak authentication is often referred to as *something you know* and strong authentication is *something you possess*. Strong authentication is often referred to as *two-factor authentication*. As in this example, Alice must not only present her password but also a second factor, her hand.

Strong Authentication Is Not Perfect Authentication

There is one potential flaw to strong authentication as presented in this scenario. Alice's hand, her strong authentication factor, must be initially measured so that future comparisons can be made. If Bob shows up in Alice's place and has his hand measured, he has effectively become Alice. To prevent this, Alice's company must have secure enrollment procedures that verify Alice's identity. In addition, great care must be taken to protect Alice's hand measurements lest Bob acquire them and construct an artificial hand built to Alice's precise specifications. There are many types of strong authentication systems, many of which might overcome these challenges, but most likely will introduce challenges of their own. Don't be complacent and assume that once you have a strong authentication solution all your problems disappear.

Today, strong authentication mechanisms typically fall into these categories:

- One-time passwords or tokens
- Smartcards
- Proximity detectors
- Biometrics such as fingerprint, voice, or retinal scans

Strong authentication isn't limited to only one item from this list. In fact, the United States government defines strong authentication as a *layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.* The challenge is to find the right balance of security and authentication that meets business, regulatory, compliance, end-user, and systems administrator needs without placing an undue burden on any individual requirement.

Regulatory and Compliance Requirements

In today's IT environment, one area of responsibility that seems to increase on a weekly basis is regulatory and compliance requirements. More and more organizations are facing industry-specific requirements and regulations. From the Sarbanes-Oxley (SOX) Act to the Health Insurance Portability and Accountability Act (HIPAA) and everything in between, companies face greater challenges to maintain data security. The penalties for failure can be devastating. A healthcare organization that exposes confidential patient information can be hit with civil complaints or even lawsuits. Strong authentication decreases the likelihood of these types of problems.

Many compliance requirements include some sort of auditing provision. Can you prove who accessed what, when, where, and why? If you have siloed systems each with a different reporting or auditing mechanism (assuming one exists to begin with), can you easily prepare a comprehensive and complete report?

Although it is not impossible to meet regulatory and compliance requirements with weak authentication, historically, these solutions provide limited auditing information. You might be able to capture who accessed a critical piece of data and when, but that's about it. And of course, we've already seen that you can't even be sure who really accessed the data. Was it really Alice or was it Bob in disguise?

Strong Authentication and the Bottom Line

Without a doubt, a strong authentication solution can have a positive impact on the bottom line. Strong authentication reduces the password management tasks on end users and administrators alike. End users can spend more time working and servicing customers instead of managing authentication to required resources. Whereas weak authentication is often an obstacle to efficient workflow, a well-planned strong authentication solution should be practically invisible to the user.

In addition, the systems administrators face fewer password-related calls to the Help desk. Security is increased, which also means less time spent investigating unauthorized incidents. Ideally, a single strong authentication solution can be implemented across a variety of systems, which reduces the number of management tools and licenses. Consolidation also makes the administrator more efficient by offering a single management interface instead of several. Strong authentication typically meets most compliance requirements and definitely reduces the chance of data or security breaches. This saves the company money in remediation efforts, not to mention possible civil consequences.

In the next article, I'll discuss what to look for in a strong authentication solution and how to select one.