

## Wandering through the Two-Factor Authentication Maze

Back in October, the FFIEC published a recommendation that financial institutions needed to incorporate two-factor authentication into their online banking applications. What made this unusual was the end of 2006 timeframe put on the recommendation. This short time period caught everyone off guard and has left everyone in the financial community on the hunt for solutions. For me though, what came as quite the surprise is that even with all the publicity about identity theft, outside of the banking space, this security recommendation found very little press. I would bet that if you talked to the average person, they would have no idea that financial institutions were facing this mandate.

Two-factor authentication comes in many forms and numerous levels of security. As with any technology, there are some versions that are simple to use and make perfect sense while others are so confusing that it becomes more of a liability than an asset. When you visit your average online banking application, you are prompted for your user name and a password. This solution, though simplistic, does not offer the most secure solution. Take for example the rise in Phishing scams. The user is tricked into typing their user name and password into a malicious web site that records the information. That information is then used by the owner of that malicious site to gain access to the real account.

With two-factor authentication, this risk is supposed to be resolved. I say *supposed* to be resolved because not all two-factor solutions actually work. I will get back to that thought later. With most two-factor, the user is required to provide more than just a simple user name and password. Instead the user will be required to provide something that should be unique to them. So the user might be required to provide their user name, password and then a third piece of data. For example, a code that is automatically generated from a key fob the user is required to carry. This code might be based on a time stamp that continually changes and is tied back to the specific user. With this setup, the user logging in would need to hold the key fob for the specific account or else they would be unable to login. Obviously this would resolve the phishing attack since even if the malicious site were to retrieve the user name and password, the code from the key fob would be unusable to them since when they visited the real site, the time would be different and therefore the code would no longer be the same. Ultimately the idea of two-factor authentication is to give that added level of security to stop the average user from being victim to someone stealing their password.

The merits of two-factor have been questioned in the past and there is no doubt that the debate will continue. Some people claim that even with two-factor, an account could still be breached through attacks such as man in the middle. This is where a malicious site catches all the data entered while letting it continue to pass to the real destination. Then once a user has passed the point of login, the malicious site in the middle takes over the communication completely and drops the real user. This is a valid concern and I personally have written several applications to demonstrate this exact attack. However,

the reality is that this type of attack is far less common than Phishing and significantly more difficult to perform, especially in large volume.

In reality, the real issue with two-factor authentication is not if it works, but that there are some many products that organizations have put out claiming to do two-factor authentication that it is difficult for the consumer to understand what is best for their environment. I recently read an article where the writer who I am convinced had suffered some sort of head trauma was advocating that financial institutions should not use two-factor authentication. His argument was not that the security wasn't sound but that with this higher level of security, the risk would instead be shifted back to the physical security and therefore that would be a bad thing. I am serious. Of course this idea was about as justified as saying don't lock the door to your house because then a burglar will break your window to get in.

When looking into two-factor authentication, an organization should be far more concerned with how they will deploy and manage the product. A bank for example with 30,000 customers needs to understand that if they choose a solution that requires a token or key fob, they will be required to send that device out to each and every one of those customers. In addition they will be required to then manage and maintain those devices when they expire, battery dies, they get lost, stolen, or broken. Though these devices are proven technology, there is no doubt that the costs to maintain this kind of a program in most cases becomes prohibitive when dealing with a large scale rollout. For this reason it is not realistic to expect that financial institutions will embrace this technology.

Another solution that absolutely confuses and frightens me is the "bingo" card. Let me be clear right from the start that this is the most ridiculous and insecure solution that I have seen on the market. This was designed to be a cost effective offering that allows an organization such as a bank to send out a very inexpensive card that is about the size of a drivers license and is often printed on heavy card stock. The card looks very similar to a bingo card with anywhere from 9 to 16 boxes. The one I tested yesterday had 9 and that is the one I will speak specifically to though even with more boxes, my issues still remain the same. In each box there are 3 to 5 random characters. When a user visits a web site and enters their user name and password, they are prompted with an image that looks just like their bingo card. However, on the image one of the boxes will be highlighted. The user is then instructed to enter the characters that from their card that are in the box that is highlighted on the screen. There is no doubt that this is a simple solution. The card of course is unique to each customer and the cost for printing is cheap. In addition, there are no concerns about the battery dying or the card expiring.

So what's the rub? Let's use that 9 box card as the most obvious example. A user with one of these cards falls for a phishing scheme. They go to a malicious web site that looks just like the real site. They type in their user name, password and it shows them the highlighted box in the bottom right. They type their characters from this little bingo card and instead of getting logged in, they get a message saying the site is down for maintenance and to try back later. The user chalks it up to technology and goes on their merry way. Now, the malicious site has the users name, password and the characters for

the bottom right box. Now that malicious user goes to the real site. The user types in the login name and password and the site posts the picture with the box in the upper left highlighted. Well the malicious user doesn't have the information for that box so they just type random characters. However, they are allowed to try again. This time when they type in their user name and password they get another box and again type the wrong information. The next time they try it, it shows the bottom right box. Cha Ching, they have that one and so they type in the correct response and are now logged in. Of course you're thinking in your mind, "Well don't they lock the account after a certain number of failed attempts?" The simple answer yes. But suppose that they lock the account after 3 failed attempts. That would mean that on a bingo card with 9 boxes that you have a 1 out of 9 shot that it will be your box. Each time you log back in you reduce those odds. So if you have 3 attempts then that means you have a 3 out of 9 or reduced it is a 1 out of 3! That's right so your odds of getting the box you need is one in three. Now imagine if someone told you that they could guarantee that you had a one in three chance of getting run over by a car, would you like those odds? Unless you have been married for over 10 years, you would probably answer no. Now also keep in mind that many sites allow up to 6 failed attempts which reduces the odds even further. It should be clear by now that this solution falls far short of what anyone could consider a strong two factor authentication.

A few organizations have started to offer behavioral solutions. This is where the user is profiled while they do their transactions. So if a user for example always logs in from the same computer every single time and then one day they log in from a separate computer, the software would catch that and block the user from gaining access until they prove who they are. This is often done via a phone call or email verification. In addition the software can track movements throughout the web site. If a user makes a large transaction for example, a bill pay or money transfer, this might also be flagged as a potential issue and again they user would need verification. Because the software for the most part is hidden from the end user, (no key fob, token, bingo card, etc.) it does seem to be the most user friendly solution. I have only played with the software a little bit and have yet to form an official opinion. One concern I would have is when multiple people are in the same home. For example roommates who use the same computer. How would the software differentiate between the two? In addition, how far could someone browse through an account before it would notice a difference? If for example, a husband and wife were to separate, and the husband wanted to monitor his wife's movements via her account, it seems the software would be flawed. The husband only needs her login and password and would now have access to peruse as he liked. Without the additional level of authentication at login, the system seems to fail. Obviously this would be the exception to the rule but still something to consider.

The last solution I will mention is software based. Because the organization I am with offers this type of solution I feel that any opinions I express will come across as biased. Therefore I will only list how the technology works without expressing any personal opinions. Software based solution require software to be loaded on the end users computer in order to authenticate. This solution is designed to eliminate the need for devices such as tokens, key fobs and bingo cards while still giving the user something

that they will physically have in order to complete their verification. One of the biggest concerns related to software is the ability to cover all operating systems. This is a valid concern and the solution must be able to support Windows, Apple and Linux in order to cover the majority of all end users. Because the solution is software based, the limitations will be based on the design and implementation. When looking at this solution, be certain it is easy to deploy, manage and most importantly it must be extremely user friendly. As with all two-factor solution types, there are a number of software based offerings and it is important to make sure that every need is met.

Ultimately, when selecting two-factor authentication, an organization will have to make some very tough decisions. Price, management, deployment and customer satisfaction must all come into play. It is not a one size fits all environment. What works for one organization may not work for another. At the end of the day, if you are faced with making the decision, the most sound advice would be to compare between 5 and 10 different solutions. No two are exactly the same and though every vendor will be convinced their solution will be the best, it should become clear as you go through them which solution works best for you.

**Author: Jim Stickley, CTO at TraceSecurity, ([www.tracesecurity.com](http://www.tracesecurity.com)), a provider of enterprise-class vulnerability management solutions and security assessments. Jim can be reached at [jstickley@tracesecurity.com](mailto:jstickley@tracesecurity.com).**

**\*\*\*Originally published by IT Defense Magazine.**