Feature

Vulnerability of Login Credentials at the Heart of Cyberhacks and Data Breaches

Jeff Maynard is the founder and chief executive officer of Biometric Signature ID *(www.BioSig-ID.com).* Maynard is the creator of several patents for gesture biometric and is a respected and sought-after speaker on the application of dynamic biometrics. Biometric Signature ID provides a software-only biometric system called BioSig-ID™, in which the signature reader resides in an ultra-secure cloud-based server. The BioSig-ID system is already installed and currently being utilized by early adopters in diverse industries such as health care, education, banking, financial and government institutions.

Corporate entities and retailers are scrambling to shore up network security by addressing the primary vulnerability of network security: the login. Unique behavioral biometrics may be the solution.

Welcome to the Age of the Cyberattack. Staggering numbers from security experts suggest that more than 95 percent of all corporations have experienced a data breach of some kind—many of which can go undetected for months or years.[1]

In the wake of the Sony hack and other high-profile data breaches at Target, Home Depot, Michaels, Chase and other institutions, corporate IT departments are scrambling to discover and implement solutions that will immediately shore up network security. At the heart of this search is finding solutions that address the user login, the primary vulnerability of network systems.

It turns out that accessing a network by obtaining the login of a credentialed user is at the center of the majority of the high-profile data breaches of the past year. The CBS News program *60 Minutes* called 2014 "the year of the data breach," and went on to state that forensic evidence shows that 80 percent of security breaches were caused by stolen or weak passwords.[2]

Once inside the system, cyberhackers are able to install information-stealing malicious software that can reside undetected on corporate servers for months, even years, capturing credit card and other information while slowly expanding its reach.

So, why is the login such a pesky problem for IT departments to solve? And why do usernames with personal identification numbers (PINs) and/or passwords fall so short in preventing unauthorized access?

At the root of this dilemma is how to effectively authenticate with an extremely high degree of accuracy that the individuals accessing the network are who they say they are.

To be effectively implemented, the solution must also meet two additional criteria: It must be easy to use and, ideally, it would require no additional hardware beyond a normal computer, tablet or smartphone device.

In the field of user authentication, meeting all three of these requirements is considered the pinnacle of online identification. Fortunately, a solution that checks off all these boxes may already exist.

Based on a unique subset of biometric verification, this tool can prove, with almost 100 percent accuracy, that the persons attempting to log in are who they say they are, while being nearly impossible to artificially replicate.

THE TROUBLE WITH LOGINS

The difficulty with login credentials is that they are based on possessing specific pieces of information, most commonly a username and PIN/password. Armed with that information, users can access everything from medical records and bank accounts to credit card information, emails and other sensitive information. The problem, of course, is that anyone armed with the same login credentials can also access the same information.

As widely reported, hackers apparently gained access to Sony's computer systems by obtaining the login credentials of a high-level systems administrator. Once the credentials were in the hands of the hackers, they were granted the "keys to the entire building," according to a US official.[3]

In this particular case, terabytes of information obtained (and, worse, deleted completely from company servers) were used (and still are being used) to wreak havoc on Sony's business interests.

In the case of the Target breach in late 2013 that exposed approximately 40 million debit and credit card accounts, login credentials were also the culprit. In this case, it is believed that login information stolen from a third-party heating, ventilating and air conditioning (HVAC) vendor was the source of the initial intrusion.

For Target, the losses are estimated at nearly US $500 million dollars. This includes reimbursement associated with banks recovering the costs of reissuing millions of cards and customer service costs, including legal fees and credit monitoring for tens of millions of customers impacted by the breach.

SEARCHING FOR THE IDEAL SOLUTION

The current gold standard in network security is called multifactor authentication, in which case two of three factors are required as security. Factors include something you have (e.g., token, cards), something you are (e.g., biometrics) and something you know (e.g., PINs, passwords). On 17 October 2014, US President Barack Obama issued an Executive Order, "Improving the Security of Consumer Financial Transactions," requiring the use of multiple-factor authentication due to the high level of identity crimes, breaches and payment card fraud.

Meanwhile, IT personnel have turned to a variety of techniques to improve the security of logins, including adding security questions and, in some cases, a secondary password.

However, these options are simply an extension of the same concept: possessing specific information that others can still acquire.

Another attempt currently in use involves throwing hardware at the problem. The logic is straightforward: Provide each user with a physical device, such as a flash drive or a token, that provides random authentication codes, credit cards or personal identification (ID) in various forms, including a smartphone. If someone has the item, he/she is legitimate. Unfortunately, this is just another form of possessing something, in this case, a piece of hardware instead of a piece of information.

Furthermore, the reason added hardware solutions are not always ideal is that they dramatically increase the cost of implementation, not to mention the logistics of upkeep. And because these items can be lost, borrowed or stolen, they still do not guarantee authentication of the user.

The answer, then, may boil down to the only way to truly identify a person: biometrics.

Biometrics is defined as something physically or behaviorally unique to an individual. Physical examples include fingerprints, iris scans, facial recognition and even vein scanning. While these deliver near-absolute verification, this type of identification again requires sophisticated, costly hardware. This is a significant barrier to implementation for reasons already stated.

Fortunately, there is a surprisingly effective form of biometrics verification in the behavioral category based on handwriting that requires no additional hardware beyond a typical computer arrangement or smartphone device.

Each person has a unique, measurable way of "drawing" letters and numbers that is extremely difficult for others to duplicate. This includes attributes such as length, height, width, speed, direction, angle and number of strokes. Passcodes can be entered at login using a finger or stylus for touch screens and smartphones, a computer mouse, or a laptop touchpad.

> "Using handwriting verification, accuracy rates as high as 99.97 percent are possible."

Once a simple setup process is completed, sophisticated software algorithms compare a user's current login attempt against the initial handwriting patterns collected and subsequent logins to confirm a match. Using handwriting verification, accuracy rates as high as 99.97 percent are possible.[4]

CONCLUSION

A major concern many organizations express with regard to implementing any additional layer of security is the potential consumer inconvenience. Many retailers have not implemented higher security measures because they do not want their customers to spend additional time going through extra security. Extra time, they believe, may mean the loss of clients and sales.

Therefore, an ease-of-use interface is a critical component of online authentication. If the added security has too many steps or is too cumbersome, it is doomed to fail. It is critical to emphasize keeping user interfaces simple and quick—taking only seconds to activate it.

Organizations have choices about which security solutions to use. They must consider the risk and the compromise, combined with the user experience (e.g., What happens when

lost/stolen? On what devices it can be used? Does it provide good false positives/negatives? What are the cost and level of convenience?) The last consideration for choosing a security technology is the use case. For example, physical biometrics are best suited for accessing physical buildings. Tokens with one-time passwords (OTPs), proximity cards and other technology are also useful for same-use cases and more, whereas dynamic biometrics are ideally suited for remote access since no special hardware is required.

To be sure, there are costs involved in implementing additional security solutions—even those that require no additional hardware. However, the collateral damage of a major data breach is much, much higher in both cost and potential loss of consumer confidence.

The problem, then, is not whether or not to invest in additional security, but in simply identifying solutions that meet all the requirements. In this Age of the Cyberattacks, this should start with securing the login.

ENDNOTES

[1] CBS News, *60 Minutes*, season 47, episode 11, first aired 1 December 2014

[2] *Ibid*.

[3] Brown, Pamela; Jim Sciutto; Evan Perez; Jim Acosta; Eric Bradner; "Investigators Think Hackers Stole Sony Passwords," CNN Politics, 19 December 2014, *www.cnn.com/2014/12/18/politics/u-s-will-respond-to-north-korea-hack/*

[4] In independent testing by the Tolly Group, a global provider of testing and third-party validation and certification services for the information technology industry, one biosignature recognition system, BioSig-ID, was found to be 27 times more accurate than keystroke analysis. Observed confidence ratings at 99.97 percent meant that the false-positive level of the biosignature software was three times better than guidelines put out by the US National Institute of Standards and Technology (NIST).