Security Current Whitepaper

User Authentication Gets Flexible

securitycurrent

It's no secret, password secrets haven't held up for quite some time against attacks targeting consumers and enterprise organizations. Breach after breach, credential compromise seems to be the path of least resistance. Why bother attempting to exploit a remote server against an unknown or even known vulnerability, when phishing a human will do just fine? Open, click, and enter credentials – it doesn't get any easier for an attacker. To make matters worse, the universal password is just that, it is universally re-used oftentimes across multiple sites. Harvest one set of credentials and chances are good it is re-used elsewhere. Time and time again this has been increasingly clear through interacting with everyday people who are the end users within our corporations. With dozens and dozens of different sites requiring a login, can you blame them for using weak or the same password across personal and corporate accounts? How many sites do you have to remember passwords for as a security professional?

The Password Conundrum

There are simply too many sites requiring only a username and password with little to no uniformity.

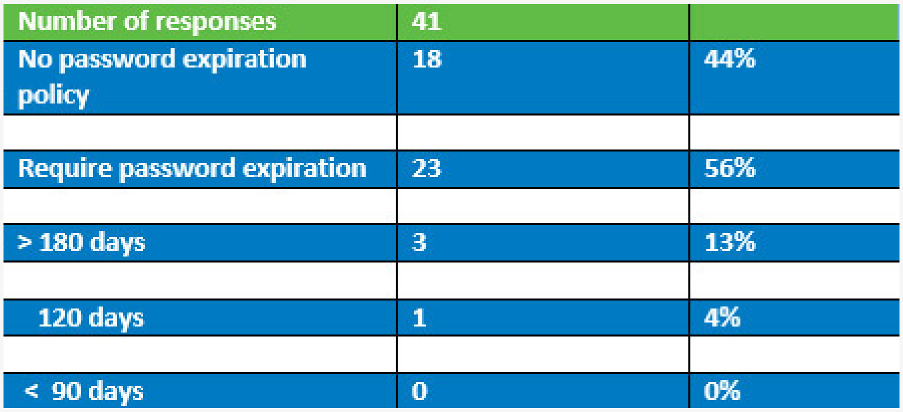
Strong passwords make sense in theory, but how well does that work with mobile devices? What about sites that don't have the same format or complexity requirements as another site? And just when the password is memorized and the rhythm is in place to type it regularly at a decent clip, it expires. People do what people do and in the case of authentication it is whatever is necessary to gain the access they need. When prompted to change a password in the middle of an online transaction, there's risk that the end user opts for a weaker password in the interest of convenience.

University of North Carolina (UNC) computer science students examined password expiration and found conclusive evidence suggesting password expiration as an effective security practice is not as beneficial as was once thought. UNC's study[1] shows that when expiration is more frequent, users opt for less complex, easier to guess passwords because they have exhausted their ability to create and remember a uniquely strong, complex password. The end result does just the opposite to what security would expect since users' behavior is to quickly create a password similar to the expired one. The more frequently passwords change; the lower user's satisfaction is with passwords and security.

Security and convenience have historically been at polar opposites. End users understand the value of stronger passwords, but what good is a strong password if it has stolen? Can we blame end users for opting for convenience even if they 'know better'?

At the end of the day, there are simply too many sites requiring only a username and password with little to no uniformity. End users opt for convenience. Authentify xFA™ bridges the gap between convenience and strong authentication.

A recent financial industry poll conducted questioned the frequency of password expiration in an online banking environment. The table (figure 1) examines 41 responses to the question as to how often, if at all, are customers required to change their passwords. In this study, 56% of the financial institutions have a password expiration policy for their online banking customers, of which many respondents remarked how much customers disliked the policy.



Number of responses	41	
No password expiration policy	18	44%
Require password expiration	23	56%
> 180 days	3	13%
120 days	1	4%
< 90 days	0	0%

Figure 1

[1] The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis
http://cs.unc.edu/~fabian/papers/PasswordExpire.pdf

If You Build It and Make It User-Friendly, They Will Use It

There's an easier option in this field of password dreams, and that is, the solution must not be difficult for the end user to use. Our world has gotten hectic in many ways, but technology generally seems to make things a bit easier than they were just last year. Convenience, regardless of technology, reigns supreme.

With people expecting technology to deliver convenient solutions, even the savviest security-paranoid person wants a flexible, adaptable solution to authenticate securely. But generally, these persons are not the weakest link because they are often more security savvy. Yes, there are high profile users with elevated access, but oftentimes the technology and security savvy are less likely to fall victim to an attack due to awareness and good security hygiene.

Phish, Infect, Steal, Repeat

As illustrated in the table above, as long as passwords remain vulnerable the attacks against them continue and actually remain the same. Why? Because the attacks are working! We're slowly learning something has to change in order to thwart attackers' chances of success. It has been said repeatedly that attackers take the path of least resistance. It's human nature, and an efficient use of the attackers' resources, to achieve the objective with as little effort as possible. Certainly if the end goal warrants hard work to be successful in the mission, it too will be done. But at the end of the day, the ability to phish, infect, and steal is winning and laying claim to the entry point of some of the most high profile breaches in history. Furthermore, forensics has shown infections don't have to come at the onset of the attack.

If a phishing exploit is credible enough to be opened at least once it will be reused. Credentials captured via successful phishing often provide enough access to result in a breach. Where does this leave a single-factor password solution? Vulnerable and ineffective.

Malware Driving Authentication Alteration

Even without phishing, drive-by malware presents a golden opportunity to compromise and maintain command and control over the infected endpoints. Money is the root of all evil and the financial industry has been dealing with fraud long before the online channel was introduced. With the explosion of online banking in the late 90's, the financial industry has been reeling in account takeover of consumers through malware. Currently, Vawtrak's Crime-as-a-Service (CaaS) polymorphic banking Trojan is evolving from its days as Gozi and has surpassed perhaps the most notorious, Zeus [3].

Information stealing Trojans harvest credentials as they are input into the browser and creates a simply mechanism to reuse single-factor solutions for financial gain. Through the years the financial industry has slowly countered with challenge questions, such as mother's maiden name, but it's not good enough against sophisticated Trojans. Is there a better answer? Yes, two-factor authentication albeit slow to adopt across consumers.

The irony of traditional endpoint-focused malware targeting financial institutions and payment services is that social networking sites are offering more in terms of out-of-band (OOB) and device-binding applications which greatly improves security against credential compromise without inconvenience. Twitter, Google, and Facebook are just a few of the early adopters offering two-factor authentication. With so much password reuse, it's naïve to think that this won't spill into the organization. How so? Employees' password reuse from personal to professional heightens a weak link for attackers to prey upon.

Employees' password reuse from personal to professional heightens a weak link for attackers to prey upon. But, there's an opportunity to leverage the benefits of social networking additional security through security awareness sessions.

When enterprise organizations do this, employees not only see the benefits of improving online security in their personal lives, but also within the enterprise. The end result is a win-win to improve adoptable security controls which provide real security value, and are convenient as well.

There is an opportunity to leverage the benefits of social networking additional security through security awareness sessions. When enterprise organizations do this, employees not only see the benefits of improving online security in their personal lives, but also within the enterprise. The end result is a win-win to improve adoptable security controls, which provide real security value, and are convenient as well. Ultimately, if you build stronger authentication tools and make them user friendly, people will use them. It's even better if that authentication strength is embedded and end users don't have to think about using it. The weakest links, the end users, are less likely to be victims if the process is simple – and automatic.

[2] http://www.bankinfosecurity.com/crimeware-as-a-service-threatens-banks-a-7690
[3] http://cm.bell-labs.com/who/ken/trust.html

Convenience and Security – There's an App for That – Authentify xFA™

Strong authentication has been achievable for years and has been primarily offered through two-factor authentication using hardware token solutions. While tokens were effective, adoption was limited to users, networks and applications at highest risk. The deployment effort, program management, and replacement process for lost tokens were complex and the costs too high. That's been changing with the increased power of mobile devices and distribution capability of app stores.

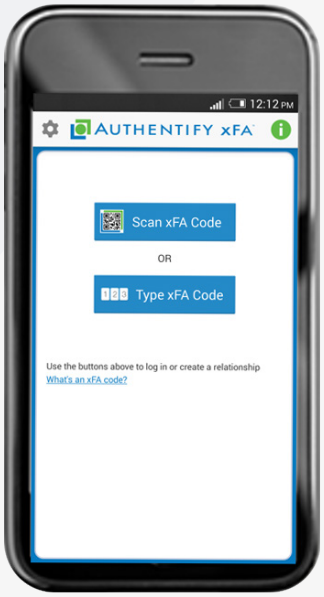
Authentify xFA ('x' factors) represents a third generation of mobile product from Authentify. Authentify is leveraging today's BYOD wave to provide strong authentication coupled with convenience. Through the power of app stores, Authentify xFA immediately presents end users with a familiar interface and positive experience.

Does the smartphone have the ability to read a fingerprint? What about keyboard pattern recognition? Furthermore, what is the preference of the user to claw back at some of the convenience the industry has taken away in years past? The Authentify xFA SmartChoice API was developed to relieve the enterprise of the support load when accommodating functionality that may or may not exist on a particular end user's device. The end result is leveraging BYOD to enable the smartphone to become a strong multi-factor authenticator that will be used. Authentify offers authentication options including:

- PIN or passwords
- Voice biometric
- Pattern/Gesture finger swipe
- FIDO support
- OTP's via voice, SMS Text or secure data channel
- Embedded PKI digital certificate
- Challenge response/KBA
- Fingerprint
- NFC
- QR code scans

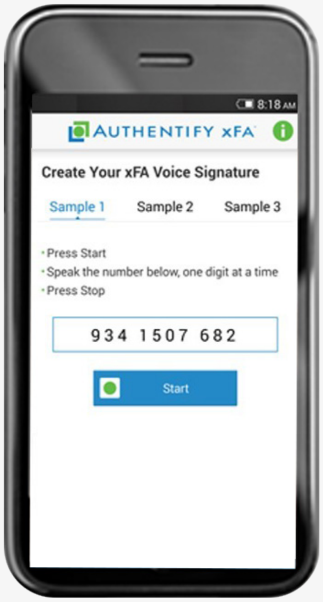
It Begins With a Simple Registration Process

The registration process is designed to provide a much better user experience than traditional multi-factor solutions. End users will be more likely to adopt a new technology if it is easy to use. Once the app is downloaded and installed on the users' smartphone, the user navigates to the enterprise service they are attempting to authenticate with. The site presents a QR code (figure 2) which is then used as part of the registration for the site accessed. Additionally, during registration setup xFA interacts with the end user to store voice biometric (figure 3) credentials within Authentify's Service Center.



Use the buttons above to log in or create a relationship
What's an xFA code?

Figure 2



Create Your xFA Voice Signature

- Press Start
- Speak the number below, one digit at a time
- Press Stop

934 1507 682

Figure 3

Application Design

Authentify xFA consists of three parties:

1. End users who download and run the xFA app on their device;
2. Enterprise organizations that offer the services supporting the xFA solution;
3. Authentify's cloud that enables enterprises and their end users to communicate securely.

Once users and applications are registered and configured, the relationships are established between the three parties to enforce security in-depth. The tiered architecture creates a unique relationship which binds together the user to Authentify, the enterprise to Authentify, and the end user to the enterprise. The architecture creates dependencies that are easy to maintain, and both robust and flexible (figure 4).

xFA's compartmentalized three-sided architecture delivers well-established security features including:

1. Embedded PKI digital certificates with split key protection for the xFA key store;
2. Biometric credentials which are anonymized and stored in Authentify's cloud;
3. A unique architecture in which compromise of one party does not place the entire system at risk.

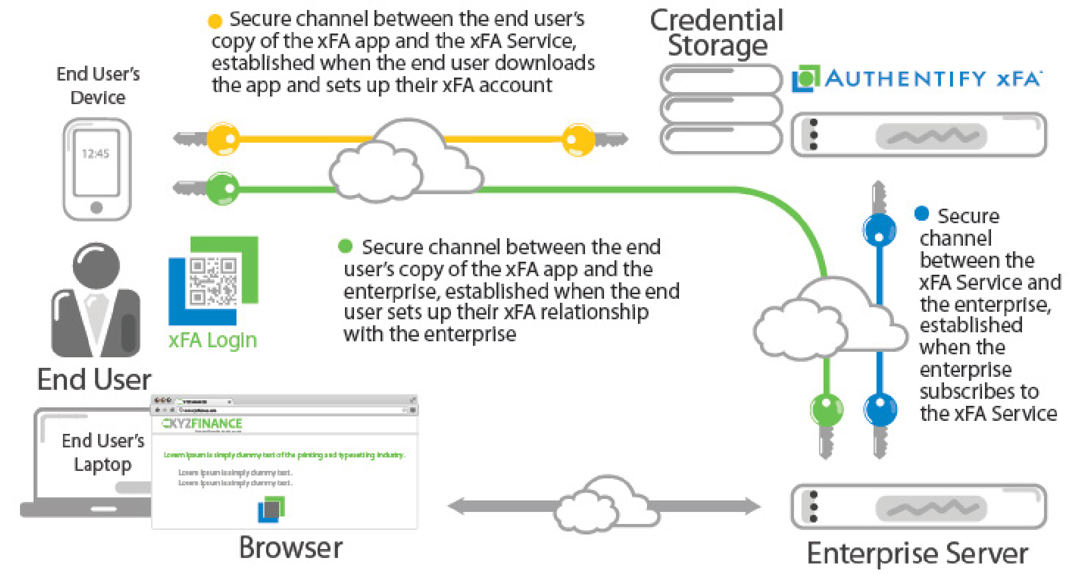

● Secure channel between the end user's copy of the xFA app and the xFA Service, established when the end user downloads the app and sets up their xFA account
Credential Storage
AUTHENTIFY xFA
End User's Device
12:45
● Secure channel between the end user's copy of the xFA app and the enterprise, established when the end user sets up their xFA relationship with the enterprise
● Secure channel between the xFA Service and the enterprise, established when the enterprise subscribes to the xFA Service
xFA Login
End User
End User's Laptop
XYZFINANCE
Lorem Ipsum is simply dummy text of the printing and typesetting industry.
Lorem Ipsum is simply dummy text.
Lorem Ipsum is simply dummy text.
Browser
Enterprise Server

Figure 4

Zero-Trust Architecture

Trust goes back to the early start of human cooperation and it is a core characteristic of human nature. Trust is crucial in society and essential in the business world. Suppliers, business partners, employees, and governments, are just a few entities that cannot work together without some level of trust. If trust is lost, it is tough to regain, if ever.

Naturally, trust is a fundamental component of security. Software code trust was classically demonstrated in 1974 by Paul Karger and Roger Schell, and later popularized in 1984 by Ken Thompson. "Reflections on Trusting Trust" illustrates the dependency on, in this case third party written code, which can be modified and then executed without detection of any wrong-doing. The trust placed in the code allowed for root logins without the need for a password, and the moral Thompson told us, was "You can't trust code that you did not totally create yourself."

Rather than building a solution whereby a single compromise renders the entire implementation at risk, Authentify does not place implicit trust from source to destination

…therefore, even if the xFA service is compromised, end users and the enterprise are not at risk because xFA's service does not have access to the private keys or digital certificates in use.

Forty years later this moral is as painstakingly true as it was then. The fundamental pillars of trust must be accepted at some point even when there is some skepticism. The adage, trust but verify, is echoed often in risk management discussions. This fundamental need for verifiable trust is what security architects strive to fulfill.

Authentify's architecture is designed to address the need for inherent trust knowing the best security focuses on the weakest points and the chinks in the armor.

Recognizing this, Authentify's zero-trust architecture ensures that if there's a compromise at any point then there is no value to the attacker. Rather than building a solution whereby a single compromise renders the entire implementation at risk, Authentify does not place implicit trust from source to destination. As such, this three party architecture ensures that if any one side is compromised, the entire solution does not collapse.

Therefore, even if the xFA service is compromised, end users and the enterprise are not at risk because xFA's service does not have access to the private keys or digital certificates in use. Furthermore with end users increasingly the weak point of attack, a compromise of the application and apprehension of the digital certificates does not jeopardize the deployment because the biometric signatures are protected within Authentify's cloud infrastructure.

Lastly, in the event that part of the enterprise is compromised separate key pairs are used so there is no cross-contamination between individual entities. Authentify recognizes there are no guarantees against a weak link becoming the point of compromise and negatively impacting the entire solution. As such, zero-trust helps to ensure a successful attack of one, does not grant access to many.

Per-App Binding Through Digital Certificates

With varying degrees of risk acceptance between enterprise organizations, having per-application bindings offers the flexibility to diversify and segregate based on the organization's risk tolerance. Organizations have historically been addressing concerns whereby a compromise within one entity could lead to multiple networks or applications becoming at risk. Said differently, gain access to one, and possibly achieve access to many through extended privileges.

Authentify has recognized that the segregation of applications linked to enterprises minimizes the inherent risk of compromise through a single point of failure. Per-app binding (figure 5) allows flexibility that can extend from employees, to customers, to third parties. This flexibility and separation is crucial in today's business-to-business and remote workforce environments.

Stepping back and looking at some of the more high profile breaches throughout 2014, third party exposure has risen to new heights due to the level of access third parties have to the internal networks of organizations. For a variety of operational reasons, these third parties are often granted a high degree of trust. The challenge is managing third parties to allow their high level of access but at the same time not succumb to typical weaknesses associated with usernames and passwords.

Per-app binding creates unique, trusted relationships between external entities and through a convenient user experience. The end result is the HVAC contractor, for example, is allowed trusted access to the resources requested, but without the risk of unauthorized access to other areas within the network. Access to higher value assets through credential compromise is prevented and high profile compromises are avoided.

Naturally, xFA's design extends to the enterprise's requirements to grant varying levels of access that go well beyond simple network authentication. Access to intellectual property, R&D, sensitive medical records regulated by HIPAA, and PCI DSS requirements, can all be enabled with multifactor authentication and isolated to the required applications.

Authentify's use of PKI (public key infrastructure) allows for different digital certificates to be used as a means of establishing trust. Authentify removes traditional digital certificate management challenges such as activation, distribution, and revocation. Separation allows for an SSO-like (single sign-on) experience but without the associated risks with SSO. xFA uses digital certificates for mutual authentication as well as an out-of-band network use to help protect against man-in-the-middle (MitM) attacks.

Authentify's use of PKI (public key infrastructure) allows for different digital certificates to be used as a means of establishing trust. Separation allows for an SSO-like (single sign-on) experience but without the associated risks with SSO.

xFA uses digital certificates for mutual authentication as well as and out-of-band network use to help protect against man-in-the-middle (MiTM) attacks.

In the event of a lost smartphone, xFA's use of biometrics will help thwart a compromise with this level of depth. This is a significant differentiator not only in terms of protection against credential compromise but also due to the simplicity for the enterprise and the end users who reap the benefits of the application doing the heavy lifting.

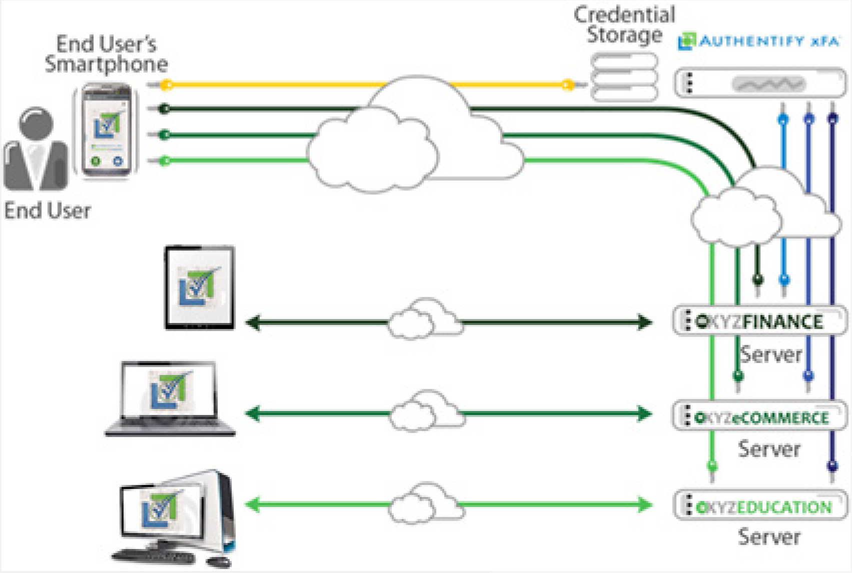


Figure 5

Consumer Use Case Scenario

The past several years have seen a dramatic increase in breaches as a result of credential compromise. This has led to primetime media coverage and is worrying consumers who have personally identifiable and financial information at risk.

Look no further than incidents in the financial services space. Whether it is cardholder data or unauthorized bank wire transfers, financially-motivated criminals are taking advantage of weak authentication deployments. Pick and choose a use case scenario, but for the sake of argument, the following example simulates xFA in a banking environment. As illustrated earlier, three parties are required to ensure zero-trust; consumers (client), the financial institution (enterprise), and Authentify for credential storage, completes this three-way handshake. In the simplest scenario, the following occurs.

1. The financial institution requires the xFA app to be downloaded from the appropriate app store;
2. After the smartphone application installation, the users' xFA authentication credentials are generated and stored within Authentify's cloud alongside voice biometric attributes;
3. The consumer navigates to the financial institution's site and authenticates as they normally do;
4. The financial institution requires xFA enrollment and sends a QR code to the consumer's terminal;
5. The QR code is scanned and when voice biometrics are requested the user is verified;
6. Creation of digital certificates are generated to be later used for mutual authentication;
7. Subsequent banking logins invoke biometrics and QR scanning process to authenticate the consumer without the need for typing and with the mutual validation between digital certificates between three parties.

Enterprise Third Party Use Case Scenario

The level of interest in regulated industries as well as non-regulated continues to draw attention due to some of the breaches involving trusted third parties. It's hard enough to manage the employee workforce let alone third parties. Regardless there is a need to manage external accounts and oftentimes their access is prey for an attacker who will seek out a weaker link in an attempt to gain access to their ideal enterprise target. Authentify xFA can be used to manage authentication to extranet portals or Web portals such as an employee benefit portal. Pick a financial industry scenario. Take, as an example, a third party collection service that logs onto the corporate accounting system to work the company's receivables. These individuals have access to sensitive financial and personal customer information within the organization's network.

1. The enterprise requires the xFA app to be downloaded from the appropriate app store and is mandated to be used by the third party collection agency;
2. After smartphone application installation, the users' credentials are generated and stored within Authentify's cloud alongside voice biometric attributes;
3. The collection agency representative navigates to the extranet site of the enterprise over an IPsec VPN and authenticates as they normally do;
4. The enterprise requires xFA enrollment and sends a QR code to the consumer's terminal over the trusted VPN;
5. The QR code is scanned and when voice biometrics are requested a comparison to the previously created credentials are verified;
6. Creation of digital certificates are generated to be later used for mutual authentication;
7. The third party now has access to the accounting system to service the company's receivables. Subsequent logins invoke the voice biometrics and QR scanning process to authenticate the collection agency's representatives without the need for typing and with the mutual validation between digital certificates between three parties.

Conclusion

The ability to authenticate and escalate privilege remains a key successful strategy for attackers. There simply have been far too many examples of serious breaches resulting from credential compromise. Recognizing this, Authentify's vision is leveraging some familiar tried and true mechanisms layered on forward-thinking architecture to eliminate any single point of failure.

xFA is an authentication platform that blends ease of use and security for a convenient end user experience and enterprise-grade security. Authentify's decision to architect their solution around PKI and zero-trust makes an attackers job harder while providing a user-focused experience. This is a differentiator. The positive aspects of xFA are numerous, but the big three are:

- The positive end user experience based on the use of devices with which they are already familiar – their mobile devices;
- Embedded PKI digital certificates and biometrics for strong authentication and industrial strength security;
- The SaaS from Authentify's cloud means an industrial strength deployment effort is not required.