Multifactor Authentication: Its Time Has Come

Jim Reno

> *'What does it mean by* speak, friend, and enter*?' asked Merry.*
>
> *'That is plain enough,' said Gimli. 'If you are a friend, speak the password, and the doors will open, and you can enter.'*
>
> *'Yes,' said Gandalf, 'these doors are probably governed by words. Some dwarf-gates will open only at special times, or for particular persons; and some have locks and keys that are still needed when all necessary times and words are known.'*
>
> *The Fellowship of the Ring*
> J.R.R. Tolkien

Transactions of any value must be authenticated to help prevent online crime. Even seemingly innocent interactions, such as social media postings, can have serious consequences if used fraudulently. A key problem in modern online interactions is establishing the identity of the user without alienating the user. Historically, almost all online authentications have been implemented using simple passwords, but increasingly these methods are under attack. Multifactor authentication requires the presentation of two or more of the three authentication factor types: "What you know", "What you have", and "What you are". After presentation, each factor must be validated by the other party for authentication to occur. Multifactor authentication is a potential solution to the authentication problem, and it is beginning to be implemented at websites operated by well-known companies. This article surveys the different mechanisms used to implement multifactor authentication. How a site chooses to implement multifactor authentication affects security as well as the overall user experience.

Introduction

The last year has brought news of a number of prominent security breaches centered on authentication, with, in some cases, severe consequences. A not uncommon pattern is a revelation that some server has been hacked and a large number of account passwords have been potentially exposed. *Potentially* because while we know files containing things such as password hashes have been copied, there is often no subsequent information on actual fraudulent use of the data or real damage done. An example of a security breach where damage actually resulted is the attack on the Associated Press Twitter account of April 2013. A bogus tweet about explosions at the White House caused a brief, but serious, disruption to the financial markets (Selyukh, 2013; tinyurl.com/d6zozam).

The industry is slowly reacting to password attacks and is starting to try to find better ways to prevent them. Media attention is growing. In particular, each publicized password attack is usually followed by a series of articles decrying the "end of the password" and calling for implementation of multifactor authentication (MFA). An online site using MFA is harder to attack – to "break into" – than a site authenticating users with only

Multifactor Authentication: Its Time Has Come

Jim Reno

a single factor such as a password. The widespread adoption of MFA would improve online security and help reduce fraud.

MFA is not a new idea. Consider a Roman soldier guarding the Senate door and requiring senators to show a ring and speak a password. This is an example of two-factor authentication. MFA has been implemented in online systems for many years. Until recently, however, MFA has rarely been deployed successfully in very-large-scale websites intended for communities such as consumers. In the light of the increasing password attacks, practices are beginning to change.

In this article, the next three sections describe the types of authentication factors, examine the authentication solutions users want, and introduce emerging authentication systems. Then, examples of authentication implementations used in websites of well-known companies are reviewed. The last section includes the conclusions.

Types of Authentication Factors

Authentication factors can be categorized as: "What you know", "What you have", and "What you are". What-you-know factors include passwords or answers to secret questions, and are by far the most commonly used of the three types. What-you-have factors are things you physically carry and must have in your possession in order to authenticate. What-you-are factors measure characteristics of your person, such as fingerprints.

Within a given type, a factor can be more or less secure, such as a password that is more or less easily guessed. But, the real increase in security comes from requiring more than one factor of different types. Two factors of the same type are not enough; the reason is that different types require an attacker to mount separate and unique attacks. Consider the case of "phishing" – a general term for emails, text messages, and websites fabricated and sent by criminals. These messages are designed to look like they come from well-known and trusted senders in an attempt to collect personal, financial, and sensitive information (Royal Canadian Mounted Police, 2010; tinyurl.com/mjqpt78). A phishing email might get your password (i.e., what you know) but cannot get your hardware token (i.e., what you have); conversely, a pickpocket might steal your token (i.e., what you have) but will not get your password (i.e., what you know).

What-you-know factors

Passwords are the most common of the what-you-know factors and are the target of much criticism. But, the death of the password has been greatly exaggerated. Even if everyone moves to MFA, a what-you-know factor in the form of a password will almost certainly be one of the factors. Moreover, even though technologists think of passwords as "old technology", in broader consumer terms, they are not. Most consumers really only started becoming comfortable with passwords as a result of the adoption of email and online services (e.g., home banking), going back perhaps 15 years. After passwords, the next most common what-you-know factors are answers to "secret questions", sometimes called knowledge-based authentication.

Password systems have a number of problems. Today, most users access too many distinct systems requiring passwords, leading to poor security practices such as password reuse or passwords being written down. Knowledge-based authentication suffers when the secret is not-so-secret because it is based on information about the user that is available from public sources.

The rise of social media has aggravated the knowledge-based authentication problem because facts about users that previously might have been known only to a few close friends are now online and widely shared. As a result, what-you-know systems are subject to different attack vectors (i.e., paths or means by which a hacker accesses a computer or network server in order to commit fraud). Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Attack vectors that target what-you-know systems include phishing and spearphishing (Associated Press, 2013; tinyurl.com/ahjw9bd). Phishing and spearphishing messages, usually emails, appear to come from a trusted source. Phishing messages often appear to come from a large and well-known company or website with a broad membership base. In the case of spearphishing, however, the apparent source of the email is likely to be an individual within the recipient's own company, often someone in a position of authority.

Other attack vectors that target what-you-know systems include: attacks on password recovery and reset systems (Honan, 2012; tinyurl.com/c2ao8ur); malware; and server-side attacks (Ku, 2012; tinyurl.com/kh55qkb).

What-you-have factors

The most common what-you-have factors are hardware one-time-password tokens and smart cards. One-time-

Multifactor Authentication: Its Time Has Come

Jim Reno

password tokens are small devices with a display that generate a periodically changing code. Authentication requires entry of that code (usually along with a password), so the user must be in possession of the token. A more recent variant is an application for a mobile device that replicates the function of the token, which has the advantage of using something the user is already carrying. Smart cards are credit cards with an embedded microprocessor that securely store secrets such as cryptographic keys. Authentication involves the card communicating with some other system, such as the user's personal computer or a point-of-sale system, and executing some authentication protocol. In addition to authentication, both of these choices can perform other functions such as digitally signing a transaction.

What-you-have factors are costly and inconvenient. Tokens must be purchased, inventoried, distributed, and managed. Users must remember to carry them; they can be lost, stolen, or broken. Also, backup systems for forgotten tokens are an issue. Often, these systems fall back to knowledge-based authentication, which then becomes an attack vector that bypasses the what-you-have factor.

Application variants are decreasing the cost and increasing the convenience of what-you-have factors. Tokens, however, are popular solely in enterprise deployments. Smart cards have had success in government situations that require high security or where their use can be mandated. The largest consumer smart card deployment has been the EMV credit card (tinyurl.com/3k8puz) or "Chip and PIN" card. EMV stands for Europay, MasterCard, and Visa, a global standard for authenticating credit card and debit card transactions that is widely used outside the United States. The wide adoption of EMV took many years: the first EMV standard was set in 1995. There have been a few attempts to use EMV online, however, it is almost entirely used at point-of-sale terminals. So far, there has not been a successful consumer deployment of smart cards used for online authentication.

Token theft is one possible attack for what-you-have factors. There have been some server-side attacks, such as the breach of RSA Security's keys (Rashid, 2011; tinyurl.com/kub4l8a). Targeted malware can also attack tokens and smart cards, by intercepting the one-time-password, session hijacking, or by causing the card to sign data other than what the user intended.

What-you-are factors

What-you-are factors, or biometrics, include: fingerprints, handprints, face or eye geometry, voice prints, typing patterns, and behavioural analysis. Many of these factors require some sort of sensor to measure a physical characteristic, adding to the cost and complexity of the solution. Enabling things such as facial recognition using hardware that is already in the user's hands (e.g., cellphone cameras) is one way to lower both cost and complexity.

Biometrics is very different from other authentication factor types due to false positives and false negatives. Although a password check is a binary test (i.e., it either matches or it does not), the outcome of a biometric authentication event has only a probability of correctness. There is an explicit tradeoff. Systems that are more secure will also reject more legitimate users; conversely systems that reject few legitimate users will be less secure. Some biometric products allow this tradeoff to be explicitly tuned, giving implementers the ability to set their own policy.

Possible attack vectors for what-you-are factors include replicating the physical characteristic and fooling the sensor. Although this is a common theme in movies, it is difficult to implement in real life. But it is possible. There have been demonstrations of successful attacks in popular media, such as the television show "MythBusters" (tinyurl.com/kekbbj9), in which the presenters successfully duped a thumbprint scanner. As with other factors, server-side attacks on the stored characteristic data are possible, as well as malware on the user system.

Authentication factors in online systems

In the physical world, the factors types identified above are very distinct. Imagine a door with a guard. To open the door, you must have the proper key, be recognized by the guard, and speak the correct password: three-factor security. For online systems, however, the types overlap and their distinction is somewhat fuzzy. This is because they all end up represented as data inside a computer – usually the user's personal computer and eventually some server.

One what-you-have mechanism used by some organizations is the "bingo card", which is a card printed with a matrix of short codes. During authentication, the server asks the user to enter the code from, say, row 3 and column 4. If the user memorizes the entire card, is it still a what-you-have factor? Or does it become what-

Multifactor Authentication: Its Time Has Come

Jim Reno

you-know? Used alongside a password, is that really MFA? Attack types also can overlap: one-time-password tokens can be attacked by phishing. Approaches that use more complex protocols, such as public-key infrastructure-based smart cards, can avoid these attacks.

A real-life attack that demonstrates this overlap is what is commonly called "ATM skimming". In a skimming attack, a device is placed over the card reader slot on an Automated Teller Machine (ATM). The device is built to appear as if it is part of the ATM, so the user does not notice its presence. As the card is inserted into the ATM, it passes through the device, which reads the magnetic stripe on the card. The device also usually includes a tiny camera, focused on the ATM keypad, to capture the user's personal information number (PIN). The captured data might be saved within the device in memory, and retrieved later by the attacker, or it may be transmitted wirelessly to the attacker who lurks nearby. Using the captured magstripe data, the attacker can create a duplicate of the ATM card using almost any other card as a "blank" – even, for example, a hotel key card. The attacker then has a duplicate of the what-you-have factor (the card) and, with the PIN, can withdraw funds from the user's account.

This attack is possible partially because the what-you-have factor in this case simply holds a bit of data that is read by the ATM. The ATM has no way to distinguish whether that data came from the legitimate card belonging to the user or from a copy. Data is data; inside the ATM, both factor types – what you have and what you know – look the same.

Malware

Malware on the user's system is the bane of all factor types. It can target the authentication system directly by intercepting the data entered by the user or read by a sensor. Even for systems using cryptographic protocols, sufficiently targeted malware can hijack a session after authentication or can cause the data presented to the user, and the actual transaction being executed, to be different. In this context, "transaction" refers to any user action, including the act of authenticating or communicating to exchange an asset for payment.

The financial industry understood this problem many years ago and solved it through hardware mechanisms. Point-of-sale systems that accept credit cards and debit cards typically use a tamper-proof, integrated pad. This single device reads the card, displays the transaction information, reads the user's PIN, and contains cryptographic keys to encrypt information before it leaves the device. For security, the device depends on its physical tamper-resistance and the inability of an attacker to insert code into it. That approach will not work for general-purpose computers, although there are efforts to put secure hardware components, such as the Trusted Platform Module (tinyurl.com/on9vqcj), into personal computers.

What Do Users Want?

Given that there is a wealth of authentication mechanisms available, it is worth considering the needs and preferences of users, which highlight the tradeoff between security and convenience. Users want security, however, their willingness to accept inconvenience depends on their perception of the immediate threat. Consider the case of people who live in a neighborhood they perceive to be "safe". They may tend to leave doors unlocked – until they hear of a nearby break-in. Then they are careful, and lock up when leaving – until time passes and complacency sets in. Even though identity theft receives a reasonable amount of attention from the press, for online systems, the threats are more esoteric and harder for non-technologists to understand. To the majority of users, technology is supposed to be convenient and "just available" – such as television, where you do not have to log in to use it.

A number of user behaviour patterns have emerged. One is for users to share credentials across many sites. By using a single password in many places, the user (even if unconsciously) is opting for convenience over security. Similarly, the selection of weak passwords is also the result of users opting for convenience over security.

Another popular pattern supported by many online services is to leave the user logged-in semi-permanently. For example, a website might require re-authentication periodically or when the user attempts a sensitive operation such as changing the password. The overall user experience is smoother because the user is required to authenticate less frequently.

To businesses, the security versus convenience tradeoff directly affects their success. Greater inconvenience risks alienating users and driving them to competitors; yet, weaker security can lead to direct monetary loss. This tradeoff is commonly resolved based on the real or perceived value of the assets the business controls. Financial websites, such as those for home banking, deal with high-value assets where real monetary loss is pos-

Multifactor Authentication: Its Time Has Come

Jim Reno

sible. Often, they also typically have regulatory responsibilities, so high security is important. On the other hand, businesses want an easy-to-use experience for their customers. As a result, they do not use the "always-logged-in" model and require authentication for every session. Session lifetime is limited to a short period, usually measured in minutes. However, few businesses have opted for MFA, and they typically only use it for accounts with very high value. For example, tokens may be used to provide access to corporate accounts or brokerage systems that move or trade large amounts of money.

Websites with lower-value assets opt for approaches that decrease inconvenience for the user, typically by requiring authentication only occasionally. Most browser-based email systems operate this way. A cookie set on the user's system establishes the session when the user logs in. The cookie can be thought of as a what-you-have factor, and the act of logging in exchanges a what-you-know factor (i.e., the password) for the cookie. Social media websites have used this pattern often. However, recent incidents are changing their perception of "low-value", and some websites are starting to implement stronger authentication.

Emerging Authentication Mechanisms

Emerging authentication mechanisms include risk analysis and use of an alternate channel. These mechanisms are helping organizations address the problem of increasing security while minimizing user inconvenience. The use of risk analysis during authentication, or when the user attempts a sensitive or high-value transaction, is one of these mechanisms.

Risk analysis focuses on the characteristics of the event – independently of the actual authentication – by searching for suspicious patterns. Comparisons can be made against historical data for the user as well as common patterns for fraudulent access. Examples of questions that drive a risk analysis include:

- What device is being used? Has this user used this device in the past? Has this device been used to commit fraud?
- Where is the user located? What time is it? Are these patterns consistent with past usage?
- Has the user moved physically in an impossible way (e.g., logged in from San Francisco, then from New York only moments later?)
- Is the transaction typical for the user? Is the user executing an unusual number of transactions?

Risk analysis is popular because it layers with other authentication mechanisms and is invisible to the user. The result of the risk analysis must be acted on, according to organizational policy. For example, transactions scored as "very risky" might be blocked. Moderate risk might trigger additional authentication, such as asking the user a security question.

Another emerging mechanism is the use of an alternate channel during authentication. This mechanism is receiving the most amount of attention because of the widespread adoption of mobile computing devices. Alternate channel involves establishing some communication between the user and the server over a path that is different than the one being used to log in. Most often, the alternate channel is the user's mobile phone. For example, if a user logs in using a personal computer, the server might send a code using Short Message Service (SMS) to the user's phone. SMS is a text-messaging service component of phone, web, or mobile communication systems that allows the exchange of short text messages between fixed line or mobile phone devices. To complete the login, the user must enter the code at the user's personal computer in addition to providing a password. SMS, voice calls, push notifications, and emails are among the possible channels. The interaction can be simple or may involve a more complex sequence with the user. Transaction details might be sent to the alternate device for the user to review and approve. Quick response codes or bar codes might be used and read by the phone's camera. Moreover, cryptographic keys and protocols can be involved.

From the perspective of factor types, this kind of authentication is difficult to characterize. Ostensibly it is what-you-have authentication because the user must be in possession of the phone. However, it really is based on ownership of the phone *number*, not the device itself. Therefore, the security of the approach actually depends on how well the phone carrier has secured the network. Similarly, email as an alternate channel depends on the security of the email account, which often depends on just a password, and so it is arguably a what-you-know factor. Alternate channels can help with the malware problem. It is possible to devise an alternate-channel system that would require the malware author to attack both devices. For example, with a single device, the malware can always take over the session after the user has authenticated, regardless

Multifactor Authentication: Its Time Has Come

Jim Reno

of the authentication technology being used or the number of factors. Such malware might subsequently submit fraudulent transactions using that session, or modify transactions entered by the user. With an alternate channel, however, the server can send transaction details to the second channel – say, the phone – where the user could verify them. Because the malware is on only one device, the user is protected. However, that protection is lost if there is no second device – such as when the user is originating the transaction from the phone itself, as opposed to a personal computer and phone. If the malware is sufficiently "smart", it can target whatever authentication mechanisms are being used or attack the user's session after authentication.

Implementation

This section provides examples of the authentication mechanisms used by well-known organizations, including large organizations with large user communities – sometimes with hundreds of millions of users. Many of these organizations are seen as industry leaders, especially in terms of user experience. These examples are worth examining to understand how these organizations have tried to add authentication factors and balance the convenience–security tradeoff. Other organizations are likely to follow their lead, and their success or failure will likely have a big impact on future implementations of MFA.

The mechanism names vary – "two step" instead of "two factor" or "verification" instead of "authentication" – but, effectively, all of these examples describe forms of MFA. Also, the specific time of usage varies. For example, some organizations use MFA at every login, whereas others use it only occasionally or in special circumstances.

Financial institutions
Card associations, such as Visa and MasterCard, have a long history of security innovation. The EMV smart cards were a major advancement in physical card security and required significant investment over many years. More recently, financial institutions have addressed online fraud using systems such as 3-D Secure (tinyurl.com/38qjke), a protocol designed to be an additional security layer for online credit card and debit card transactions. The protocol ties the financial authorization process to online authentication based on a three-domain model:

1. **Acquirer domain:** the merchant and the bank to which money is being paid
2. **Issuer domain:** the bank which issued the card that is being used
3. **Interoperability domain:** the Internet or Message Passing Interface (tinyurl.com/qxwe2)

For online access, such as for home banking, many banks have implemented risk analysis systems, often in response to regulatory pressure. These systems are layered with simple passwords. Fallback systems, used when the user forgets a password or when an account is locked, often use knowledge-based authentication. Banks have an advantage over many purely online sites in that they have a physical presence (branches) and call centres that can be used for fallback. The costs of servicing users this way, however, are significant.

Google (tinyurl.com/d27xnr7)
Google implemented a system called "two-step verification" using alternate-channel authentication. In addition to a password, the user could receive a text or phone call. They also support the alternative of using one-time-password applications. Computers can be designated as trusted by the user, such that two-step verification is not required when logging in from those systems. There are multiple fallback approaches. More than one phone number can be registered. During enrollment, the user can print and save a set of backup codes to use in the event of a lost phone. Finally, if all else fails, an account recovery form can be sent to Google.

Google also has a mechanism for handling account access from mobile devices. A common problem with MFA is that users access their accounts from many devices, some of which might not support the MFA technology very well. For example, a fingerprint reader might be present on a user's personal computer, where a driver could be loaded and the reader could be used when logging in. But, if the account requires access from an application on a phone, there may be no reader available; plus, it is unlikely that the application will support more than simple password authentication. Google allows the user to generate, on a personal computer, "application passwords" that can be used specifically by the mobile applications. Because these passwords are long-lived, this method arguably reduces

Multifactor Authentication: Its Time Has Come

Jim Reno

the overall solution to a single-factor. However, these passwords are phishing-resistant (unlike user passwords), because they are not used regularly and are not required to be memorized by the user.

Apple (tinyurl.com/czwun9b)
Apple also uses the term "two-step verification" for their approach. Their system is based on three elements: i) a password; ii) an alternate channel with SMS and push notifications; and iii) a 14-character recovery key that is generated at setup. MFA is not used at every authentication; it is only used when the user wants to perform sensitive operations such as account management or changing a password. This method solves the problem of application access because normal authentication involves only the password. Resetting any of the three elements requires the user to have two elements. For example, to reset a forgotten password, the user must have the recovery key and be able to receive a code through the alternate channel.

One concern in the use of this two-step verification approach is that there appears to be no other fallback mechanism. If two of the factors are lost – say the user forgets the password and has lost the recovery key – Apple suggests that the user should create a new AppleID. Given that purchases are tied to the AppleID, presumably this means that the user loses access to them.

LinkedIn (tinyurl.com/k3cwqcv)
LinkedIn also calls their approach "two-step verification". As the alternate channel, they use a code sent via SMS. Applications are handled by appending the code to a regular password and giving that to the application. This approach depends on the application remaining logged in for a long time. Fallback mechanisms seem unclear. The website's help page has an "ask us" form that can be submitted in the event of a problem.

Twitter (tinyurl.com/paya4rj)
Twitter has implemented "login verification" in two successive steps. In the spring of 2013, they implemented alternate-channel authentication via SMS messages, with some limitations. Only one phone number was allowed per account, and only one account was allowed per phone number. Applications could be handled by generating a temporary password with a one-hour lifetime, so, as with LinkedIn, the application is usually expected to remain logged in continuously. The fallback mechanism was to contact support. There was no apparent provision for multiple users on the same account, which was a problem for corporate accounts that handle tweets from multiple employees.

During the summer of 2013, Twitter has added an additional mechanism that involves a cryptographic key that is stored on the user's phone. When logging in at a personal computer, a notification is sent to the phone. The user must approve the login using the Twitter application on the phone. The application communicates with the server using the key and a cryptographic protocol, and the login proceeds. The new mechanism also provides backup codes generated at the phone that can be used for fallback. The multiple-user problem is addressed by allowing the phone application to support multiple simultaneous accounts. Therefore, a user can be logged in to both the user's personal and corporate accounts at the same time. Multiple users of the corporate account can be logged in, each user using his or her own phone.

Facebook (tinyurl.com/3ocrlc3)
Facebook uses a mechanism referred to as "login approvals". Alternate-channel authentication via SMS is supported, as well as one-time-password generation in the Facebook application or via third-party applications. MFA is used only if the login device is not recognized. Fallback is supported by reset codes that the user can print in advance or by contacting support. Applications are handled by one-time application passwords that can be generated by the user.

Conclusion

Solving the online authentication problem – improving security without alienating users – is a critical and growing need. Authentication attacks are increasing every year and attackers are becoming more sophisticated. MFA will be one important tool, but it is a complex and evolving concept. Although the history of MFA goes back many years, for many online sites it is only now being applied. However, a rethinking of authentication is happening across the industry. The future of MFA will depend on how well popular sites – such as those mentioned above – implement it, and on how well users like it. No data is available yet on adoption rates. The common trend of using an alternate channel, particularly mobile devices, is likely to continue given its selection by well-known companies.

There are steps everyone can take. Businesses with online sites should implement some form of MFA. User education is also important. The adoption rate of MFA can increase by helping users understand why they need more than a simple password. Partnerships between industry, academia, and governments can help fund research into new authentication technolo-

Multifactor Authentication: Its Time Has Come

Jim Reno

gies and the effectiveness of existing authentication technologies.

Individual users should examine the options presented by the sites they frequent and consider enabling MFA, particularly for those services where high-value assets are involved. If MFA is not available, users should reach out and try to influence those organizations to use MFA. Often, businesses will not move to adopt MFA until after an attack; however, they can be influenced by customer demand. Given the increasing frequency of highly publicized attacks, it is better to proactively prevent them than to reactively respond.

About the Author

Jim Reno is a Distinguished Engineer and Chief Architect for Security at CA Technologies. He joined CA with the Arcot acquisition in October 2010. At Arcot, Jim led the development of strong authentication and risk management systems. He has more than 30 years' experience in software development, working on operating systems, databases, networking, systems management, and security. Jim is one of the inventors of the 3-D Secure protocol used in the Verified by Visa and MasterCard SecureCode programs. He holds multiple patents in the area of credit card verification and authentication. At CA he guides the overall architecture of CA's security products as well as security aspects of the entire CA portfolio.

Citation: Reno, J. 2013. Multifactor Authentication: Its Time Has Come. *Technology Innovation Management Review*. August 2013: 51–58.

Keywords: multifactor authentication, authentication mechanisms, online security, authentication attacks