Global Information Assurance Certification Paper

Daisy Chain Authentication

GIAC GSEC Gold Paper

Author: Courtney Imbert, courtneyimbert@gmail.com

Advisor: Rodney Caudle

Accepted: 06/19/2013

1. Abstract:

An attacker can piece together a collection of accounts within an organization using public information and compromised data, building a "daisy chain" to a target. With the upsurge of cloud-based services and web-facing applications, many organizations face a larger attack space for compromise. Since the process isn't highly technical, and the steps of the process fall within normal business procedures, it can be difficult to detect until the data is gone. Traditional approaches to information security, like securing individual systems and rule-based perimeter intrusion detection, fail in the face of attacks that use normal transactions to infiltrate networks. However, it is possible to detect such an attack with a holistic and multi-layered approach that includes an emphasis on identity assurance.

2. Introduction

"Daisy chain authentication", a term originally coined by *Wired* writer Mat Honan, is defined as an attacker using normal but alternative authentication methods to break into an account, building upon public or previously compromised data to gain access to other accounts. (Honan, 2012) Similar approaches have been called "island hopping" or "pivoting". Creating a daisy chain via authentication requires little technical skill. In many cases, it can be done by researching publicly available answers to security questions, using data available to one account to gain access to another, or using insecure password reset mechanisms.

Daisy chain authentication attacks have several components that make them challenging to protect against and detect. The attack does not necessarily require a high level of technical aptitude – just intelligent reconnaissance. In 2008, David Kernell researched simple biographical details about U.S. vice presidential candidate Sarah Palin, and used Yahoo!'s password recovery mechanism to obtain access to her email account. (Stephy, 2008) Though the media dubbed him a "hacker", his approach was a low-tech one that could have been used by anyone. An attacker with better technical ability increases his chances of compromising the weakest link or finding the data necessary to continue the chain.

In addition, an attacker building a daisy chain can be difficult to detect. In many cases, the weakest link in a daisy chain is outside the control or oversight of the target organization. A weak link could be a re-used password in an unencrypted user database on an unrelated site. Since these attacks exploit normal methods of logging in, recovering passwords, or accessing data, most intrusion detection systems would not alert on the activities of the attacker.

Daisy chain authentication is not a new problem. In its simplest form, an attacker can gain access to an email account that is used to recover passwords from another account. However, trends in the way organizations access and store data may increase the frequency and potential damage of daisy-chain authentication attacks. The growing popularity of cloud storage, "bring your own device" infrastructure with web-facing applications, and the linking of data between systems through APIs all contribute to an

Author: Courtney Imbert, courtneyimbert@gmail.com

ideal environment for an attacker seeking an entry point. Mechanisms meant to make things easier for users, like automated credential recovery and cached passwords, also make compromise easier for attackers. More personal information is available publicly than ever before, and social networking sites like Facebook provide a treasure trove for attackers targeting credentials.

Using an authentication chain to penetrate a network can comprise a single piece of an Advanced Persistent Threat (APT), or all of it. The challenge of daisy-chain authentication attacks lies in the complexity of interconnected systems. While each system in an organization may be considered individually secure, multiple systems may become compromised when taken as a group.

3. Case Studies

How likely is a daisy chain authentication attack? Though data isn't available on data breaches specifically caused by exploiting alternative authentication methods, clearly web-based authentication is a tempting attack vector. 55% of hacking attacks in 2011 involved the exploitation of default or guessable credentials, and 54% of breaches were initiated through a web application. (Verizon RISK Team, 2013) Several incidents have been made public over the last few years that highlight the emerging threat of a daisy chain.

3.1 Mat Honan's "Epic Hacking"

In August 2012, Mat Honan wrote an article about a process used by hackers to compromise multiple accounts in a short period of time. The process began with Honan's personal website, which listed his email address and physical business address. The attacker called Amazon and added a falsified credit card number to Honan's account. At the time, the addition of a credit card to a user account was authenticated at a lower level of security than other transactions – by providing the user's name, email address, and billing address. The attacker then called Amazon back and claimed to have lost access to both his account and to the associated email address. Amazon required the account holder's name, email address, and a credit card number associated with the account to add a new email account for password recovery. That was simple, since the attacker had just added a bogus credit card number. Once the attacker gained access to the target's Amazon account, he could see the last four digits of any stored credit card numbers.

Next, the attacker called Apple and claimed he had lost his access to the Apple cloud storage service, including the associated @me.com email account. Apple required the user's name, secondary email address, and the last four digits of the credit card associated with the account – all pieces the attacker already had in his daisy chain. Once he gained access to Honan's @me.com account, he activated Google's password recovery feature, which sent a password to the @me.com account. From there, he could reset or recover the passwords of any of Mat's accounts that used email for password recovery. He used this capability to overtake Honan's Twitter account, which was his ultimate target.

It is worth noting that Amazon's password recovery system was not the weakest link in the chain. Though the attacker started there, the attack could just easily have begun with a compromised point-of-

sale system or a dishonest restaurant server noting a credit card number. The lynchpin was the Apple cloud password recovery system, which used easily available information to authenticate and contained private, high-value data, as well as a pivot point to additional accounts.

This simple but layered attack gained the attacker access to Honan's Amazon account, Apple cloud account including photos, documents, email, and calendar information, his Google account, and his Twitter account. *Wired* magazine replicated the process with several test users with success. The article spurred a review by Apple and Amazon of their security policies related to credential recovery. (Honan, 2012)

3.2 Twitter Corporate Compromise

In 2009, an attacker calling himself "Hacker Croll" publicly released hundreds of confidential corporate documents originating from Twitter. They included personal information about Twitter employees, financial projections, and executive meeting notes. Magazine *TechCrunch* interviewed the attacker and published the details of the attack after Twitter closed their security holes.

The attacker began by compiling a catalog of information on Twitter using public search engines and databases. For his entry point, he selected the Google email account of one of Twitter's employees. In a method similar to the Honan attack, he derived the password recovery email for the Google account. Though Google obscures the email address for password recovery (******@h******.com), it was reasonable to guess it was a Hotmail account with the same prefix as the Google account. When the attacker attempted the password recovery process with the Hotmail account, he discovered the account was inactivated. He recreated the Hotmail account, and sent a password recovery email from Google. Once logged into the target's Google email account, he managed to hide the compromise by resetting the Google account password to one found in an email within the account, then waiting to ensure the target could log back in. The first step was complete.

Because the target had reused his Google password across accounts, the attacker compromised multiple accounts without detection. He was able to use the password to log into the user's work email account. From there, he was free to peruse sensitive documents. He used the data in the target's email address to compromise more employees, including three senior executives. Twitter was unaware that they had been compromised until hundreds of sensitive documents were already released to the public.

Multiple security problems may have resulted in this daisy chain, including a lack of two-factor authentication, password reuse on the part of the user, insecure password policies, and inadequate logging or alerts on the corporate network.

The author of the *TechCrunch* article summarizes the fundamental problem that makes the daisy chain so challenging:

"The list of services affected either directly, or indirectly, are some of the most popular web applications and services in use today – Gmail, Google Apps, GoDaddy, MobileMe, AT&T, Amazon, Hotmail, Paypal and iTunes. Taken individually, most of these services have reasonable security precautions against

intrusion. But there are huge weaknesses when they are looked at together, as an ecosystem. Like dominoes, once one fell (Gmail was the first to go), the others all tumbled as well. The end result was chaos, and raises important questions about how private corporate and personal information is managed and secured in a time when the trend is towards more data, applications and entire user identities being hosted on the web and 'in the cloud'." (Cubrilovic, 2009)

4. Identity Assurance

In a daisy chain authentication attack, the attacker takes advantage of systems that associate user accounts not with a specific identity, but with other accounts or with the possession of credentials. The process of confirming that the person providing the credential is the user's "true" identity is known as *identity assurance*.

Electronic identity assurance is best described as a new, yet basic concept. It pulls together multiple components of information security, including nonrepudiation, authentication, integrity, and confidentiality. One non-profit professional association, the Kantara Initiative (kantarainitiative.org), was formed in 2009 to promote interoperability among electronic authentication systems. The organization has since presented an Identity Assurance Framework (IAF). The framework includes a certification program and documents to define and implement an identity assurance program. The program provides four levels of identity assurance, from no assurance (for actions like signing up for a public newsletter) to high assurance (for actions like high-value bank transfers). NIST also provides electronic authentication guidelines that parallel Kantara's IAF. (NIST, 2011) Obviously, as the level of identity assurance increases, so does the cost of confirming an individual's identity, and transactions usually become more inconvenient.

Identity assurance can quickly become a complex and expensive endeavor for an organization. A product-focused approach is not the best one in this area; since the area of electronic identity assurance is still in development, most products aren't mature enough to provide a full solution to the problem. However, organizations can implement some identity assurance using resources they already have, creating a multi-faceted approach to prevent, detect, and alert on false identities. Each of the following approaches provides additional assurance that the person who just authenticated has the correct identity.

4.1 Baseline Development for Context-Aware Security

Preventing a daisy-chain authentication problem can be a technical challenge; after all, the attack works by traversing and logging into systems in a seemingly normal way.

A context-aware security policy restricts access to data based on some factor, including the identity, classification, and history of the user. Context awareness is a relatively young feature of security products. However, there are a few basic technical controls that can be customized to reduce the attack space and make security controls more "context aware" as they relate to groups of users, locations,

networks, or systems. If these controls are implemented, it makes a daisy chain attack easier to detect early and less likely to succeed.

Network baselines have long been used to identify and troubleshoot problems with networks, but they can also be useful to identify compromise. For the sake of preventing a daisy chain attack, baselines should focus on typical user behavior. The types of questions asked should include things like:

Do users log on from a specific IP range, or geographical location?

Do users tend to log on at specific times, like during business hours in a time zone?

Do users ever have a reason to have more than one session active at the same time?

Do users log on to accounts from a single computer, or do they access data from multiple computers?

Do users use specific devices to access their accounts, like mobile phones?

What software or protocols do users use to access their accounts?

How much data do users typically download or access? For example, it may be unusual for a user to download more than a month's worth of data from an ERP system.

It's important to differentiate acceptable use policies from baselines. A security policy states what users *should* or *shouldn't* do, while a baseline represents what users *normally* do. Activities outside a security policy are prohibited, but activities outside a baseline simply mean something unusual is happening, like a team uploading large files the day a project goes live.

Once the threshold of normal user behavior is determined, technical controls can be implemented. Controls can prevent unusual behavior, log/alert on it, or require additional authentication to perform the action. These controls can either interrupt the daisy chain, or quickly alert IT staff to an intrusion.

In Internet-facing systems, a threshold governor can be highly useful in preventing daisy chain attacks. Threshold governors are measures that prevent the overuse of paths like account registration and password resets. Account lockout mechanisms, even temporary ones, can be highly useful in slowing the attacker down enough for the security team to respond. On web services, lockouts should be enforced against both same username/many passwords and many username/same password attacks.

Because organizational needs are complex and always changing, baselines must be revisited and adjusted on a regular basis. Determining network and user baselines is not a simple task. There are many points at which a control can be placed, from the border of a network to within the logic of an application. Additionally, several actions can be taken when behavior falls outside the normal threshold. Setting baselines and applying corresponding controls must take into account business needs, usability, security requirements, and historical data.

4.2 Event Correlation

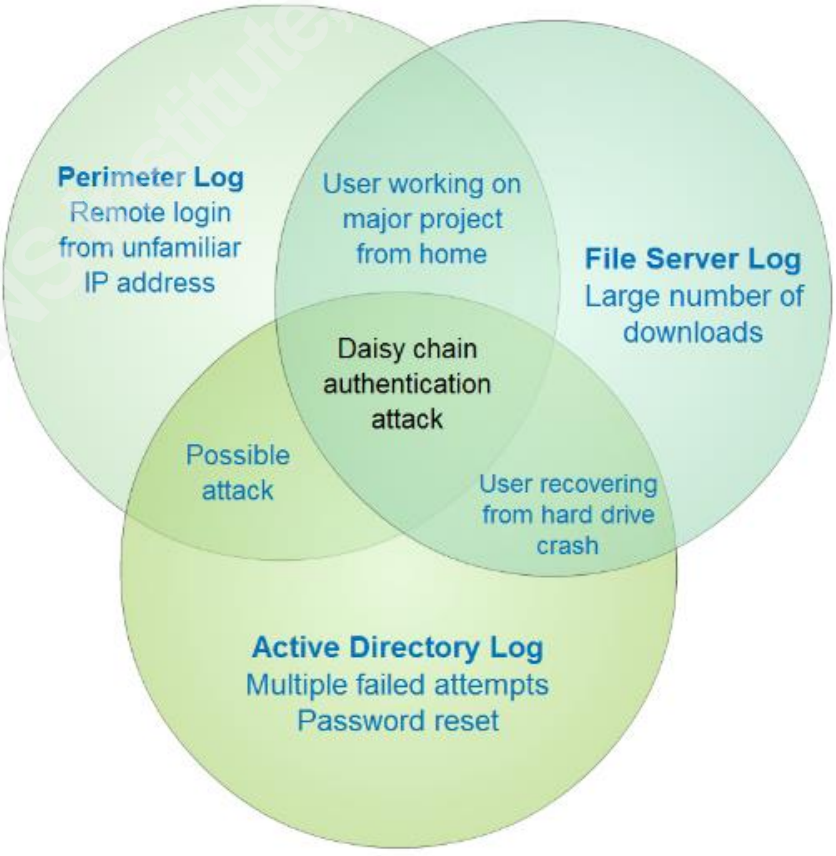
Author: Courtney Imbert, courtneyimbert@gmail.com

Event correlation is a technique for pulling together individual events from multiple sources to identify a single, larger event. The technique is often used for root cause analysis, issue tracking, and problem management. It is highly relevant to incident response, especially APTs and other multi-phase attacks. Event correlation succeeds where individual log monitoring fails. It achieves higher levels of situational awareness by combining multiple minor events. This technique is perfect for preventing, detecting, and reacting to daisy chain authentication attacks.

For a simple demonstration of the power of event correlation, see the Venn diagram below. In the diagram, multiple events that might be considered minor combine to alert on a possible attack. By removing any one of the log sources, awareness of the event is impaired.

Notice that of the four outcomes possible from the three log sources, two are benign and two require additional investigation. Part of the power of event correlation is distinguishing between normal and abnormal events. Minimizing false positives is key to rapid incident response.

Currently, event correlation almost exclusively relies upon logs. It can be stateless, or stateful with a "sliding window" of time or events. For performance purposes, most organizations correlate warnings or failures rather than successful or informational events. However, even successful events can be suspicious – for example, an administrative user logging into a large number of servers in a short period of time. Combined with the baseline identification process addressed in section 4.1, event correlation can be a powerful tool for identifying attacks comprised of multiple otherwise "normal" transactions.



Author: Courtney Imbert, courtneyimbert@gmail.com

4.3 Identity and Access Management (IAM) Systems

"Put all your eggs in one basket, and watch that basket."

– Mark Twain

The goal of IAM is to identify individuals in an organization and control access to resources. Typically, IAM systems connect multiple accounts together with a single profile and primary key or user ID per user. An IAM system should provide three functions:

Authentication: checking whether a user is who he says he is

Authorization: checking whether the user is permitted to perform an action

Auditability: providing detailed documentation of past user actions

Each of these components provides significant protection against a daisy chain attack. It is important to note that identity management does not negate the need to secure each individual system in an organization. Because implementing IAM requires enumerating each user-accessible system in an organization, it also provides a unique opportunity to review and adjust the authentication policies for each system.

Once Identity and Access Management is implemented, organizations can aim for Identity Activity Monitoring. Identity Activity Monitoring is an IAM system combined with event correlation. It's an approach to identify what end users are doing within an environment by correlating traces of their activities. This can be an extraordinarily powerful tool to provide identity assurance. For example, it may be particularly suspicious that a user just swiped his smartcard at his workstation, yet is already logged in from a remote location.

Though Identity Management can provide additional protection against daisy-chain attacks, it presents a potential security challenge: single sign-on, or SSO. SSO provides a tempting target for attackers, as well as a single point of failure. The risk for an insecure Identity Management product became apparent in 2001 with Microsoft Passport. The single sign-on service, used by more than 200 million people and 70 websites, contained a series of vulnerabilities, including race conditions, password reset attacks, and logout failures. The compromise of any given Microsoft Passport account provided authentication to multiple websites, credit card numbers, and contact information. (McWilliams, 2001) Because of the broad access provided by compromising a single sign-on account, any single vulnerability within an SSO system can became a significant problem. Single sign-on credentials should be highly secure, with an emphasis on multi-factor authentication and secure password recovery.

Because Identity and Access Management systems are adjusted to fit each environment in which they reside, customization may introduce vulnerabilities that didn't exist in the original product or in the

network before SSO was implemented. Therefore, each organization that implements Identity and Access Management system should rely on defense-in-depth, perform a security audit on the IAM implementation, use a change management process, and continue to assess its systems periodically for vulnerabilities.

4.4 Multi-Factor Authentication

Authentication requirements can be divided into three categories:

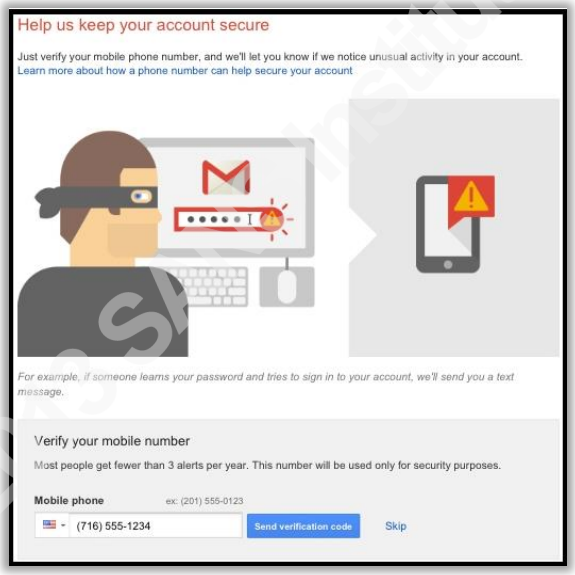
Knowledge – "something you know" (like a password)

Possession – "something you have" (such as a smart card or digital certificate)

Inherence – "something you are" (generally, biometric data).

Two-factor authentication requires the user to present proof in two of those categories. Requiring multiple pieces of a single factor, like having a user answer three security questions, may bolster security, but according to the Open Web Application Security Project, it is *not* two-factor authentication. (OWASP, 2012)

Two-factor authentication does not completely mitigate the risk of a daisy chain, but on any given system, it is the best protection against it. Two-factor authentication requires the attacker to compromise both factors, which adds a layer of defense. Compromise of two-factor authentication is not impossible. However, in the majority of the cases studied by the author of this paper, the compromise would have been stopped or slowed if any system in the chain used a two-factor authentication scheme.



For ease of use, many services simulate the possession factor by sending an SMS text to a mobile phone. There are a few problems with SMS as an authentication factor. Malicious users can use social engineering to authenticate to the service provider, then port the number to their own device and intercept messages destined for that number. Data-siphoning malware on mobile devices is growing ever-more sophisticated, and traffic can be sniffed over wireless networks. Organizations that choose SMS messages to represent an authentication factor should be aware of the potential risks, and protect access to the mobile phone number associated with the account.

The use of two-factor authentication requires some user training in order to be effective, or users may inadvertently lower security to single factor. Kevin Mitnick presented an example of obtaining one factor

(an hourly-changing number on a physical token) from an employee through a targeted social engineering attack, by posing as an employee who had lost his own token. (Mitnick, 2002) Employees may also write their password on the back of their smartcards, cache their password in their mobile phone's browser, or simply store their password in a note on their mobile phone. In each of these cases, the authentication scheme is reduced to a single factor – possession of the mobile device or card.

Two-factor authentication can be challenging to implement, particularly for web-based, publicly accessible services. However, the field is maturing, and the number of two-factor authentication solutions is rapidly increasing.

4.5 Killing the "Security" Question

The strength and secure storage of a password does nothing to protect data if the account allows entry by answering insecure personal knowledge questions. The weaknesses of the "security question" have been documented by a number of security researchers. Security questions are often an alternative to the account holder's primary credentials, and used much less often. Therefore, the answer to the question must be easy to remember and unlikely to change. To prevent guessing, the question must have a broad range of potential answers. It must also be private enough to foil reconnaissance attempts. In practice, it is nearly impossible to select a personal knowledge question with all of these qualities. Allowing users to create their own security questions opens a new vulnerability, since the user himself may select a poor question. As an authentication scheme, personal knowledge questions are often insecure or ineffective.

Even attackers trawling through security questions with no prior knowledge of the user have good odds. According to a 2010 study, one in 84 accounts using a mother's maiden name as a security question could be compromised within three tries by guessing common names. (Bonneau, 2010) Social networks, social engineering, and public resources boost the odds for attackers with specific targets.

For ease of use, many organizations opt to use security questions for password recovery. With careful design and defense-in-depth, they can be used successfully as a *part* of authenticating a user. For guidelines on designing quality personal knowledge questions, see OWASP's guidelines for choosing and using security questions (https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet).

5. Mitigating the Risk of a Daisy Chain Authentication Attack

Because daisy chain attacks do not exist in a vacuum, they are naturally difficult to protect against. The public information and systems used by attackers are not always within the control of the organization being targeted.

Author: Courtney Imbert, courtneyimbert@gmail.com

Defense in Depth is an effective approach against any attack, and infiltrating an organization through a daisy chain is no exception to that rule. An effective defense-in-depth security program protects not only against technical attacks, but social engineering ones. Though authenticating through a daisy chain is heavily reliant on reconnaissance and social engineering, there are several options organizations can use to lower their risk of a successful attack.

5.1 Entry Point Mapping

If you aren't mapping your own network, a sophisticated attacker almost certainly will. Remote and internal attackers will attempt to identify points of entry, desirable targets, and a pathway from one to the other. It's a helpful exercise to map the different methods of authenticating to your own network, identifying links that could lead to potential compromise.

Mapping a network to identify potential authentication attacks

1. List systems, or groups of systems, under the organization's control that require authentication to access data.

2. For each system, document:

Trust relationships with other systems, like a corporate email account used for password recovery or a web portal with data from the ERP system on the dashboard

Important data made available by logging in

The primary method of authentication

Any secondary methods of authentication

Security measures enabled on the system to protect against fraudulent authentication

3. Identify systems with a high attack surface. Some organizations have already performed a risk assessment in the past that identified at-risk systems. Systems that may require a higher level of identity assurance include systems that are public-facing or accessible from the Internet (like web-accessible email), and systems that have trust relationships with multiple other systems.

4. Identify systems with particularly critical or sensitive data, like ERP systems.

5. Start with critical systems and trace paths through their origins to determine what information would be needed to start a daisy chain.

See the next page for an example of a simple authentication map. Once the map is created, we can identify services that play important roles in the network, and trace potential attack paths. In the following example, the red arrows indicate a system can be used to recover a password for another system, with a line connecting two entities if there's two-factor authentication. A blue arrow indicates a trust relationship – one system grants access to another without any additional authentication, or in the

case of the Payroll/HR system, the blue arrow means an authenticated user may specify a trusted device by changing his contact information. Either arrow can be part of a daisy chain leading to a target. Using this map, we can determine:

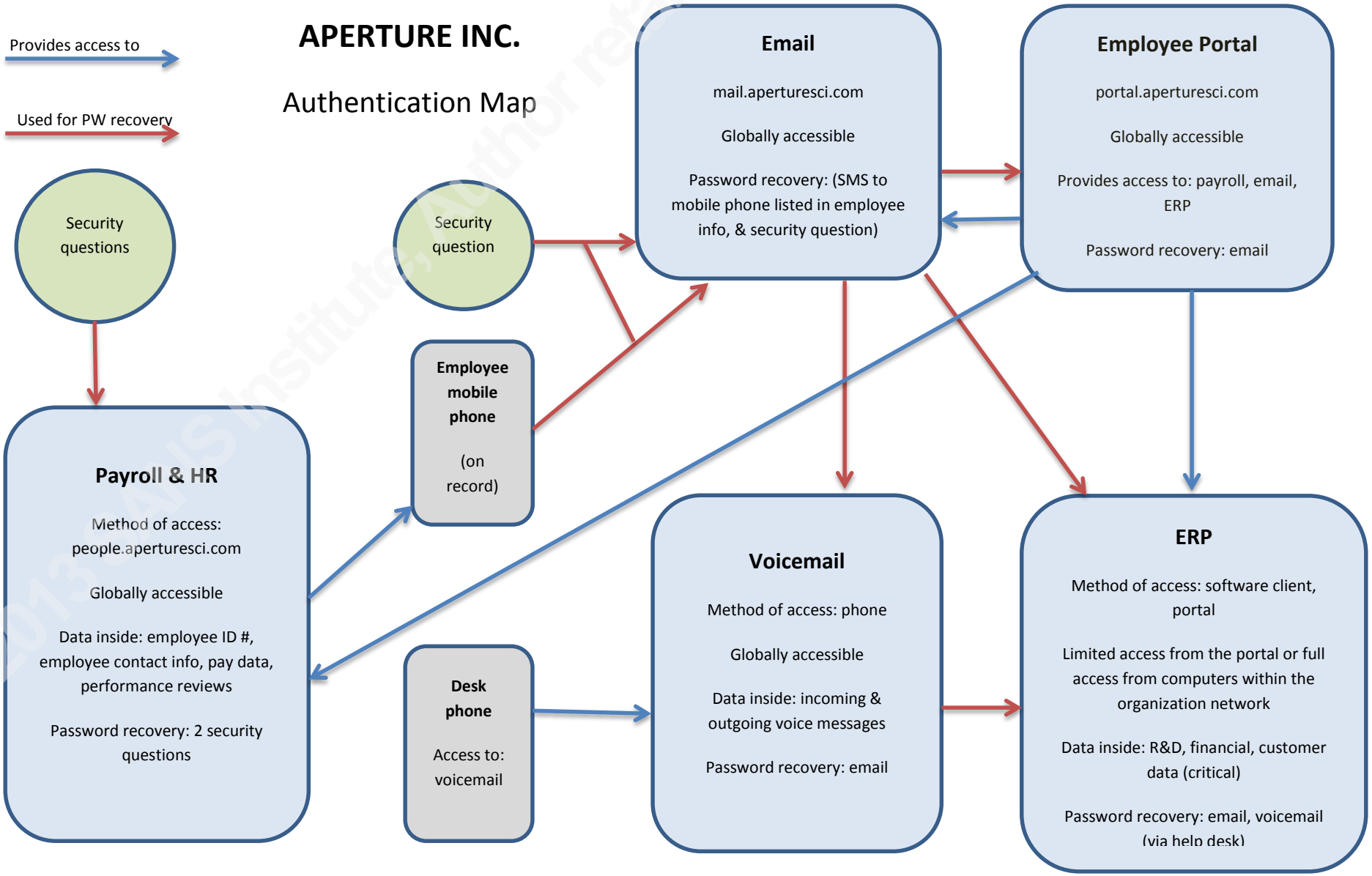
The most critical data resides on the ERP server. It could be compromised in multiple ways. If an attacker can determine the answers to the three security questions required for email and payroll/HR, he can change the employee contact info and retrieve employee email. If an attacker were at another employee's desk, he could retrieve voicemail without a password and get a password reset for the ERP system via the help desk. For simplicity, the help desk was not included as one of the authentication systems, but weak policies or poor training on the part of a help desk can easily lead to compromise.

Email is a critical system to most daisy chains, since it is a password recovery mechanism to multiple other systems. The employee portal is also critical, since it has a trust relationship with most other systems in the organization. Both of these systems should provide for a high level of identity assurance in their authentication process.

The Payroll & HR system is highly vulnerable. Because the HR system gives users the ability to change their contact information in a database email uses for password recovery, the system becomes a doorway into all the other systems in the organization. There are a few ways to address this problem. Security questions should be reviewed and eliminated if possible, actions like changing contact information could require a higher level of security, or the email system could be configured to pull the mobile phone number from another, more secure location.

The authentication network map can quickly become complex, but it's not meant to be. The purpose is not to deeply dive into an organization's architecture, but to create the perspective an attacker might have based on publicly available reconnaissance. The map is not a panacea, and will not identify all potential attacks. For example, it doesn't distinguish between the different data access levels users have. However, it can identify organization-wide pathways to compromise, and create a clearer picture of the best places to focus remediation efforts.

Author: Courtney Imbert, courtneyimbert@gmail.com



Author: Courtney Imbert, courtneyimbert@gmail.com

5.2 Employee Training

In many cases, the human element is the easiest link in the daisy chain to exploit. An effective information security program should include policies, procedures, and user awareness training.

5.2.1 IT Staff

Fortunately, self-service password recovery and identity management solutions have reduced the need for human intervention in resetting passwords. If the IT help desk does have the ability to reset passwords, a process must be designed to authenticate a user and communicate the password in a way that cannot be intercepted by the wrong party. Providing the IT help desk with written policies and procedures provides a secure method of resetting passwords, as well as solid support when someone attempts to subvert procedures for password recovery. In the absence of a written procedure, a help desk associate could make a misjudgment on authentication, like assuming caller ID is enough verify a user's identity.

Multiple accounts should not be set to the same initial password by the IT help desk; possession of a shared initial password can easily lead to compromise by an attacker, especially an internal one.

In an environment with self-service password recovery, the help desk may be the last option after failing previous attempts – so it is particularly important to confirm the user's identity. A given account's defense is only as strong as the weakest method of authenticating to it. Be sure to consider the security of the information used to communicate a password. Who can change the information on the phone list? If your method of communicating a new password is sending an SMS to the user's phone number as published on the list, it means anyone who can change that phone list can also retrieve another user's password. One of the more secure methods of communicating an initial password is providing one part of a credential (like a password or smart card) to a liaison who can personally verify the identity of the requestor, like the user's manager. The other piece of authentication can be provided to the user.

Although help desk associates can be exploited as a method of gaining access to an information system, they can also be an invaluable resource in detecting unusual actions that still fall within the range of normal behavior. The help desk often has visibility to social engineering attempts that evade technological detection. Help desk associates should be trained to quickly review a recent history of changes and requests on the part of the customer, and carefully document each request made by a customer. For example, if a customer contacts the help desk to have a password sent to him via SMS, an astute help desk employee may notice a recent request to update to the employee's contact information and notify the information security team before proceeding.

5.2.2 User training

With the advent of bring-your-own-device and browser-based access, it can be challenging to enforce a division between work and personal use. Organizations should develop a policy that defines acceptable use and access of corporate systems. Obviously, the risk associated with storing organizational data on personal devices is high. Whether or not users access corporate resources from personal devices, they

should be trained to avoid using a single password between multiple accounts. A daisy chain can easily be started with a compromised password from a rarely-used site, which is then attempted against other systems. Additionally, users should be encouraged to report stolen hardware that could contain organizational data – even if the data was on a personally owned device, or if they violated a data storage policy.

Users should be trained to protect their credentials and avoid storing credentials in an email account, unencrypted on their hard drive, or written down. Though many daisy-chain attacks do not necessarily require knowledge of user passwords, users should select secure passwords, and avoid using slight variations or guessable patterns across multiple accounts or after a password expires.

Since password recovery mechanisms are often easier to exploit than a password itself, password resets are common in daisy chain authentication attacks. Users should not dismiss an unexplained password change or account lockout as a "glitch". An unexplained change in credentials should be reported and investigated as a security incident.

It is true that organizations with well-developed policies can still be exploited by a determined attacker, as occurred with Apple's password recovery policy in the Honan case. However, if an organization doesn't have a clear policy for providing access to users, the attacker needs only to reach the "least common denominator".

5.3 Data Classification and Access Control

The ultimate goal of information security can be summarized in three words: "protect the data". Data can be categorized by nearly any criteria. More common criteria include sensitivity (for example, public, internal, confidential, secret, etc), topical content, date, and job role. Once the data is classified, access controls and monitoring can be assigned to data categories. Generally, data should be held to the principle of least privilege, meaning it should be provided only on a level justified for a given purpose. Data classification and access controls provide strong protection against a daisy chain compromise in two ways:

It helps prevent potentially sensitive information from becoming part of the public domain, and therefore contributing to the start of a chain

Once the attacker has compromised an account, prohibiting access to sensitive data can prevent continuation or completion of the chain

Particularly sensitive access, like system administrator access, should be segregated from everyday access by way of re-authentication (preferably two-factor) or a separate account. As with any security control, periodic audits can provide assurance that the process is working correctly.

Though software exists to assist with data classification, how to classify data is a business decision best made as a collaborative effort within the organization. Data classification can be a significant undertaking, but provides significant protection from a motivated attacker.

Author: Courtney Imbert, courtneyimbert@gmail.com

6. The Role of Mobile Devices in Identity Assurance

Mobile devices, such as tablets and smartphones, present both opportunities and challenges for information security professionals. Though comprehensive mobile device security is beyond the scope of this paper, it is important to recognize that obtaining an employee mobile device can be one of the simplest ways to enter a daisy chain. Organizations should have a clearly defined mobile information security policy, and stay up-to-date on developments in mobile phone security.

6.1 Using Mobile Devices to Improve Identity Assurance

Mobile devices can actually strengthen an organization's security at a low added cost. Because they are so ubiquitous, they are one of the simplest and most scalable ways to implement a multi-factor or multi-channel authentication scheme. Currently, an SMS text message is most commonly used to simulate two-factor authentication. Though there are legitimate concerns with malware or sophisticated attackers intercepting messages, any form of two-factor authentication will help an organization's chances against a daisy chain attack.

Once secured and if properly implemented, mobile devices can provide high levels of confidence in a user's identity in multiple ways. Mobile devices offer unique potential for using built-in hardware to add context to authentication. Capabilities like location services could be used as part of a behavioral profile to provide additional assurance of a user's identity. Martin Griss, director of Carnegie Mellon's CyLab Mobility Research Center, said: "While it is not surprising that using context other than location is still in its early stages since most context-aware work is still in the realm of research, simple behavior monitoring to detect abnormal patterns, perhaps combined with location, is feasible today, and can significantly strengthen mobile security." (Power, 2011)

6.2 Mobile Devices as a Link in the Chain

Mobile devices provide the ability for business users to work anywhere – but that means carrying data into an untrusted world. Data stored on a mobile device is in danger both at rest and in transit on unsecured networks.

A unique risk to mobile devices lies in their tendency to be lost or stolen. In the McAfee Mobility and Security Survey of 2011, 40% of organizations surveyed had lost mobile devices to theft or negligence, and half of the lost devices contained business critical data. (Power, 2011) Mobile devices may tempt otherwise well-intentioned finders to access confidential data. In 2012, Symantec "lost" 50 smartphones across five cities as an experiment. Of the 50 phones, half were returned. However, 96% of the people who attempted to return a phone accessed private data first, and 80% of the finders attempted to access corporate information that was clearly identified with labels like "HR Salaries". (Haley, 2012)

There are plenty of features that make mobile devices less vulnerable to data loss. However, some of these features, especially strong passwords and brief automatic lockout windows, are at odds with

usability. Although the need for mobile security is clearly recognized, there is often a gap between secure policy and reality. “Bring Your Own Device” (BYOD) programs, though tempting for budget-conscious IT departments and employees, may place mobile device security decisions on unaware employees. In many cases, a distracted employee and a four-digit PIN is all that’s standing between an attacker and a glut of organizational data.

Cached passwords for email and network-facing applications are commonplace on mobile phones, placing sensitive data at risk and reducing the effectiveness of two-factor authentication. Even if *no* business-critical information is stored on a smartphone, it could still become the first link in the daisy chain. Password managers, personal email, SMS messages, voicemail, history, notes, bookmarks, calendars, and contact lists all provide valuable information for pivoting into organizational systems. Approximately half of users store credentials or credit card information on their mobile devices. (Power, 2011) The consequences of a single compromised mobile device are potentially devastating.

6.2 Mobile Device Authentication Solutions

Stringent policies may not be the best solution to the unique challenges presented by mobile devices. Since mobile device usage often blurs the line between personal and work data, and organizations have limited control over user-owned devices, user education is the most powerful protection against mobile daisy chain attacks. Users should be educated about the importance of protecting their devices, shown how to view and change security settings, and informed about effective security practices.

The risks of theft and loss can be reduced by enabling automatic locks paired with encryption. Four-digit PINs are better than no lock protection, but they’re one of the less secure methods of locking a device. Beyond the relatively small set of 1,000 possible PINs, users often select PINs from an even more limited set: calendar dates or years. (Jakobsson, 2013) Passwords or phrases are a better option, but can be difficult to enter on a small screen. Several mobile device manufacturers are introducing promising ways to unlock mobile devices, like facial recognition and unlock patterns. Not all authentication methods are created equal, however. Some methods offer more accurate authentication than others, and capabilities change with the introduction of each new device model. Whichever method is selected, brute-force attacks should be thwarted with maximum attempt thresholds. Organizations should explore up-to-date methods of encrypting data and authenticating users, and select models that work with their usability requirements and level of security risk.

To further reduce the risk of lost or stolen organization-owned devices, remote Mobile Device Management (MDM) systems provide the ability to set global policies and remotely wipe devices. Time is of the essence – in order for this security feature to be effective, employees must inform the IT department as soon as they notice a device is lost.

Since so many mobile applications are interconnected, users can disclose confidential data accidentally. Devices increasingly automate syncing data to the cloud or sharing data with other mobile applications. Users should be aware of the ways their data is synchronized and shared, and review the permissions requested by applications as they’re installed. The most secure configuration is one that requires

authentication to each mobile application, and has automatic syncing or inter-application sharing disabled.

Users should be aware of the dangers of connecting to untrusted wireless networks. Since mobile application data is still sometimes left unencrypted for the sake of performance, it would be simple for an attacker to intercept credentials by sniffing network traffic. Accessing a service provider's network is generally more secure than accessing a wireless network. If an untrusted wireless network must be used, VPN tunnels can prevent snooping.

There is no silver bullet for the concerns raised by mobile devices. However, carefully designed defense-in-depth can prevent attackers from accessing data on mobile phones. Malware threats should be addressed appropriately in the organization's mobile device policy. Apps on organization-owned devices, particularly ones that cache or store passwords, should be vetted for security. Finally, both corporate policies and user education programs should identify appropriate ways to dispose of mobile devices without putting data at risk. Organizations need to apply security policies with a risk-based approach that maintains the delicate balance between usability and security.

7. Conclusion

Ultimately, daisy chain authentication is a method that combines social engineering and common sense. Because the technique usually requires targeted reconnaissance, it could be considered an Advanced Persistent Threat (APT), but the process seems far from advanced. After all, how advanced is it when an attacker can simply pick up a lost mobile phone, browse through a user's email, and use a password reset link to access a web application?

It may seem unbalanced that such an easy technique requires such sophisticated mitigation. Data classification, event correlation, activity baselining, and identity access management are all significant undertakings for any information security team. But working through a daisy chain is just one example of the types of attacks that are becoming the norm. Attackers take advantage of the growing size and complexity of networks. Technologies that make day-to-day business easier, like globally accessible web applications and trust relationships, expose a greater attack surface. It's never a good idea to focus on a single type of attack when developing a security program. However, daisy chain authentication is a good example of how a broad, context-aware information security design can protect against other seemingly indefensible attacks like zero-day exploitation and APTs.

Information security teams can no longer protect entire organizations on a piece-by-piece basis; nor can they expect a single out-of-box product to protect them against threats. Holistic, proactive, and in-depth protection is the most successful way to protect against insidious, multi-stage attacks like daisy chain authentication.

Author: Courtney Imbert, courtneyimbert@gmail.com

References

Anderson, R. (2008). Security engineering: A guide to building dependable distributed systems. (2 ed.). New York, NY: Wiley.

Bezroukov, N. (2002). Event Correlation Technologies. Softpanorama. Retrieved from http://www.softpanorama.org/Admin/Event_correlation/index.shtml

Bonneau, J. Evaluating statistical attacks on personal knowledge questions [web site]. (2010). Retrieved from http://www.lightbluetouchpaper.org/2010/03/04/evaluating-statistical-attacks-on-personal-knowledge-questions/

Boyce, J., & Jennings, D. (2009). Information Assurance: Managing Organizational IT Security Risks. Woburn, MA: Butterworth-Heinemann.

Cubrilovic, N. (2009, July 19). The Anatomy Of The Twitter Attack. TechCrunch. Retrieved January 3, 2013, from http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/

Cisco. Baseline Process Best Practices [web site]. (2005). Retrieved from http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014fb3b.shtml

Covington, M.J., Fogla, P., Zhan, Z. & Ahamad, M. (2002). A Context-Aware Security Architecture for Emerging Applications. (Academic paper). Georgia Institute of Technology, Atlanta. Retrieved from http://www.acsa-admin.org/2002/papers/71.pdf

Haley, K. Introducing the Symantec Smartphone Honey Stick Project [blog post]. (2012). Retrieved from http://www.symantec.com/connect/blogs/introducing-symantec-smartphone-honey-stick-project

Honan, M. (2012, August 6). How Apple and Amazon Security Flaws led to my Epic Hacking. Wired Magazine. Retrieved from http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

Jakobsson, M. (2013). Mobile Authentication Problems and Solutions. New York: Springer Science & Business Media.

Kaushik, N. What happens when Telcos Declare SMS 'Unsafe'? [Blog]. (2012). Retrieved from http://blog.talkingidentity.com/2012/11/what- happens-when-telcos-declare-sms-unsafe.html

McWilliams, B. (2001, November 2). Stealing MS Passport's Wallet. Wired Magazine. Retrieved from http://www.wired.com/science/discoveries/news/2001/11/48105?currentPage=all

Mitnick, K. (2002). The Art of Deception: Controlling the Human Element of Security . US: Wiley.

National Institute of Standards and Technology. Electronic Authentication Guideline [Web site]. (2011). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

Author: Courtney Imbert, courtneyimbert@gmail.com

Open Web Application Security Project. Choosing and Using Security Questions Cheat Sheet [Web site]. (2012). Retrieved from https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet

Open Web Application Security Project. Guide to Authentication [Web site]. (2009). Retrieved from https://www.owasp.org/index.php/Guide_to_Authentication

Power, R. Mobility and Security: Dazzling Opportunities, Profound Challenges [White Paper]. (2011). Retrieved from http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf

Prasad, G. & Rajbhandari, U. (2010). Identity Management on a Shoestring. Los Angeles, CA: C4Media, Inc.

Stephy, M.J. (2008, Sept. 17). Sarah Palin's Email Hacked. Time Magazine. Retrieved from http://www.time.com/time/politics/article/0,8599,1842097,00.html

Stone, M. Data Discovery and Classification in 5 steps [Web page]. (2009). Retrieved from http://trendedge.trendmicro.com/pr/tm/te/document/DLP_Data_Discovery_and_Classification_in_5_Steps_090630.pdf

Verizon RISK Team. 2012 Data Breach Investigations Report [White paper]. (2013). Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Villavicencio, Frank. Identity Activity Monitoring [Blog]. (2010). Retrieved from http://blog.identropy.com/IAM-blog/bid/31405/Identity-Activity-Monitoring

Author: Courtney Imbert, courtneyimbert@gmail.com

Last Updated: July 26th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event