FINANCIAL SERVICES ISAC

R-CISC
Retail Cyber Intelligence Sharing Center

Protecting Merchant Point of Sale Systems during the Holiday Season

November 7, 2014

Executive Summary

This advisory was prepared in collaboration with the Financial Services Information Sharing and Analysis Center (FS-ISAC), the United States Secret Service (USSS), and the Retail Cyber Intelligence Sharing Center (R-CISC), and is directed towards retailers or companies which are processing financial transactions and managing customer personally identifiable information (PII) during the upcoming holiday season and beyond. This advisory serves to provide information on and recommends possible mitigations for common cyber exploitation tactics, techniques and procedures (TTPs) consistently and successfully leveraged by attackers in the past year. Many of these TTPs have been observed by the FS-ISAC, through its members, and identified in Secret Service investigations.

The TTPs discussed in this report include:

- Exploiting commercial application vulnerabilities
- Unauthorized access via remote access
- Email phishing
- Unsafe web browsing from computer systems used to collect, process, store or transmit customer information

This document provides recommended security controls in these four commonly observed areas to protect customer data and also provides recommendations to smaller merchants who should work with their vendors to implement these recommendations (see Appendix A).

This advisory is not intended to be a robust, all-inclusive list of procedures as attackers will modify TTPs depending upon the target's network and vulnerabilities. This report does not contain detailed information about memory scraping Point of Sale (PoS) malware that has been used in recent high-profile data breaches. Secret Service investigations of many of the recent PoS data breaches have identified customized malware only being used once per target. A list of observed PoS malware families is provided in Appendix B.

These recommendations should be analyzed by cyber threat analysis and fraud investigation teams based on their operational requirements. The information contained in this advisory does not augment, replace or supersede requirements in the Payment Card Industry Data Security Standard (PCI DSS); however, the PCI DSS version 3.0 recommendations are cited when appropriate.[1]

[1] For the full PCI DSS v. 3.0 guide please see https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Table of Contents

Executive Summary 1

Application Security 3

Recommendations 3

Remote Access Controls 3

Recommendations 4

Third Party Vendors 4

Recommendations 5

PoS Management 5

Recommendations 6

Points of Contact 7

Appendix A. Simple Network Controls for Small Merchants to Protect Customer Data 9

Appendix B. List of Common PoS Malware Family Names 12

Appendix C. Multi-Factor Authentication 14

Enable Two-Factor Authentication 14

Configuring Two-Factor Authentication 14

Two-Factor Authentication Tokens authentication methods for XenApp Web Sites 17

Application Security

During the past year attackers have continued to use brute force password attacks against network assets such as webservers or externally facing databases. According to a 2013 survey conducted by the security firm Alert Logic, brute force attacks increased from 30 to 44 percent among its customers.[2]

Once inside a network, hackers usually map the network to determine the most valuable data to steal. One method of connecting to the network devices storing that data is through software that is permitted to run on the network and connect to external destinations controlled by the hacker. Typically, these applications are allowed full outbound access through a firewall or proxy service facilitating the theft of that data.

There is a strong possibility that attackers will leverage highly publicized vulnerabilities such as Heartbleed, Shellshock (Bash), and POODLE to access a network.

Recommendations

- Perform Open Web Application Security Project (OWASP) audits on any web applications.[3]
- Implement all recommended vendor patches and test to ensure the patch is successfully integrated.
- Enforce up-to-date anti-virus (AV) signatures, but do not only rely on AV signatures alone.
- Test databases and web login portals against brute force password attacks.
- Monitor firewalls for outbound traffic to unknown or suspicious IP addresses and domains.
- Secure webservers that contain customer data. These include payment gateways and e-commerce applications.
- Ensure that no unauthorized code has been introduced to the production environment. Run a vulnerability scan against your approved applications. If any software is vulnerable, update and patch immediately. Re-run the vulnerability scan whenever new or updated applications are introduced.

Remote Access Controls

Criminals have successfully exploited databases and payment processing systems with remote access tools. There is a high probability that employees who have remote access to the company's network will be targeted especially if the attacker can steal virtual private network (VPN) logon credentials and leverage them to log in during normal business hours. For example, in August 2014, a health care provider's VPN credentials were stolen and hackers used these credentials to steal millions of patient's social security numbers.[4]

---

[2] http://go.alertlogic.com/rs/alertlogic1/images/alert-logic-spring-2014-CSR-pages-04-21-14.pdf?mkt_tok=3RkMMJWWfF9wsRolvKrKZKXonjHpfsX86OkuWqeg38431UFwdcjKPmjr1YAESMt0aPyQAgobGp5I5FEKSbnYRqJ4t6EOUg%3D%3D

[3] https://www.owasp.org/index.php/SQL_Injection

[4] http://www.reuters.com/article/2014/08/20/us-community-health-cybersecurity-idUSKBN0GK0H420140820

Implementing multi-factor authentication on remote access devices reduces the risk of attackers gaining access to the network. Too often, this added layer of security is not configured in remote access platforms, making it a common target for attackers in past data breaches. Appendix C contains examples for enabling and configuring multi-factor authentication for the popular and widely deployed Citrix platform XenApp. Most other remote access platforms provide similar support for multi-factor authentication.

Recommendations

- Corporate users who typically access a network externally should be forced to change their login credentials before and after the holiday season. Sophisticated criminal groups have likely already purchased stolen credentials to conduct an attack this season. Forcing regular password changes and enforcing complex password rules will help mitigate this risk.
- Multi-factor authentication should be required to mitigate risk for remote access. Many remote access appliances are provisioned to accept multi-factor authentication technology (See Appendix C).
- Segregate the payment processing systems from remote access applications when possible, and restrict the network resources remote access users can access.
- Implement all recommended vendor patches and test to ensure the patch is successfully integrated.
- Enforce up-to-date AV signatures, but do not only rely on AV signatures alone. Consider additional tools for the device being accessed such a host based intrusion prevention system (HIPS) and host based firewalls.
- Monitor the remote user accounts for login abnormalities such as frequent failed login attempts, logins during non-normal working hours, and abnormal duration of logon (e.g. very long or very short login sessions). Additionally, host based security logs should be enabled and reviewed.
- Lock accounts after multiple failed login attempts. The industry standard is not more than six failed login attempts.[5]
- Disable un-necessary services especially those that support remote access such as remote desktop protocol (RDP) and virtual network computing (VNC) when not required.
- Monitor firewalls for outbound traffic to suspicious IP addresses and domains.

Third Party Vendors

There is a strong possibility that third party vendors such as those involved in heating ventilation and air conditioning (HVAC), power, or other environmental and physical security controls on the network will be targeted. These vendors usually have login access to a central network or peripheral network that can be exploited to gain lateral access for payment information.[6] In December 2012, the cyber security firm Cylance stated that it found 12,000 US industrial control systems online indicating they can be

[5] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
[6] http://arstechnica.com/security/2012/12/intruders-hack-industrial-control-system-using-backdoor-exploit/

accessed externally and potentially targeted by an attacker.[7] The following May, Cylance researchers demonstrated vulnerabilities in an HVAC platform and successfully shut down a major technology company's air conditioning.[8]

Recommendations

- Vendors should not be allowed to remote access your network with out of date operating systems like Windows XP. For example, require Windows 7 or newer, or Mac OS 10.8.
- Identify third parties with remote access or physical access to the network perimeter.
- Require vendors to use multi-factor authentication for remote access when possible. If multi-factor authentication is not available to those vendors, then disable remote access services except when specifically requested and scheduled by the vendor. Force third parties to change their login credentials before and after the holiday season. Sophisticated criminal groups have likely already purchased stolen credentials to conduct an attack this season. Forcing regular password changes and enforcing complex password rules will help mitigate this risk.
- Enforce up-to-date AV signatures, but do not only rely on AV signatures alone.
- Establish baselines for each 3rd party vendor's normal network activity, including remote access and logins. Monitor their activity for anomalous behavior such as frequent failed login attempts, logins during non-normal working hours, and abnormal duration of logon.
- Evaluate and limit third party network access privileges. For example, whitelist third party network addresses on a firewall provisioned to control remote access by third parties.
- Segment the network if possible through the use of secured VPNs with managed access control.
- Conduct information security and risk assessments of all third party vendors that have access to your network.

PoS Management

In preparing for the holiday season, remember, the computers that run the PoS services must be secured like any other computer on your network. In a recent incident, investigated by Wapack Labs, the CEO of a small company used his company computer to surf the web. In doing so, a website containing spyware was accessed and the spyware was downloaded on the system. Unfortunately, the spyware downloaded the ZeuS crimeware and installed a serious piece of ransomware known as Cryptolocker. It cost the company $600 in ransom (paid in Bitcoin) plus $3,800 in forensic and cleanup fees. Every file on his laptop was encrypted, and when he connected to the corporate network, every one of his mapped drives were encrypted –including financials --all because he surfed the web from his company laptop.

During low volume hours, cashiers, clerks, and seasonal workers may find fun things to do on the web. Imagine if the attack described above occurred on a computer used to process payments or manage

[7] http://www.mocana.com/blog/2012/12/19/niagara-ax-framework-hack-more-serious-than-first-thought
[8] http://www.wired.com/2013/05/googles-control-system-hacked/

customer personally identifiable information (PII). How much more damaging and costly would that attack have been?

Recommendations

Overall

- Inventory and conduct a review of how customer data is stored, moved, and deleted. This should include the equipment and applications involved. It is likely that a sophisticated attacker will conduct reconnaissance on a target's network to identify where customer data is stored and how it is transmitted locally before being encrypted in a central database.

On the Network

- Ensure that your PoS systems have a firewall or proxy installed for protection.
- Deploy an appropriately configured intrusion prevention system (IPS).
- Employ proper network segmentation, such that PoS systems operate on a separate, protected subnet.
- All VPN access should be performed through the IPS and must use up-to-date authentication mechanisms.
- Segregate your PoS system from other network functions such as email and non-PoS related applications. If the PoS is attached to enterprise resource planning (ERP), inventory, or finance systems, use application gateways to ensure the PoS functionality is logically protected.
- Do not use PoS terminals or other computers with access to PoS systems for Internet surfing, checking email, or accessing social media.

Encryption

- Confirm what data is at rest on a PoS terminal and deploy endpoint encryption for those devices.
- Encrypting Card and PIN information before going into the payment terminal memory has been an effective technique to safeguard the payment data. There are several vendors who provide this technology and service.
- Some retailers have elected to replace their in store payment terminals with new technology to encrypt card account numbers and other track data as it is swiped in the mag stripe reader or read by the chip reader.

[**NOTE:** If the criminals capture the encrypted data it is typically not marketable in the criminal underground]

Internet Access and Software Updates

- If the PoS is processed by software operating on a single terminal consider not allowing that terminal Internet access, or restricting its internet access to only those destinations required for PoS functions (e.g. payment gateways).
- Consider requiring two or more employees approve any updates of the payment processing applications and, if possible, filter updates to that terminal's operating system (OS) though a controlled server on the network.

Physical Access and Multi-Factor Authentication

- Ensure that there are no active USB ports or other media drives open on a PoS terminal. If running a Windows OS, ensure that auto-run is disabled. Insider threats, both intentional and unintentional, are a real danger.
- Inform employees to be on the lookout for skimmers, USB sticks, or other devices connected to PoS systems. Check all PoS systems, including card swipe equipment, for connected devices on a regular basis (e.g. daily).
- Implement multi-factor authentication for the employees involved in managing the transactions of customer data and updating the applications protecting those transactions (See Appendix C).

White Listing

- If transactions are processed by a single software program operating on a single terminal, ensure that only that application is allowed to run on that terminal by enforcing a strict application white listing policy. If possible, log and configure alert updates for the security operations center for any changes made to that whitelisting policy by an individual user or business location.
- Record and change the default settings with any PoS hardware and software, including default passwords. Criminal groups have likely reviewed documentation and/or purchased the same software in order to exploit any default settings.

Anti-Virus and Key Logging

- Do not rely on AV signatures to find memory scraping malware. Criminals have customized this type of malware in recent attacks and likely tested this against the target network's AV solution.
- Implement anti-malware detection software that looks for anomalous and suspicious patterns of behavior.
- Enforce up-to-date anti-virus signatures to find older malware that is being reused. This may be targeted at smaller or medium sized businesses or used by criminal elements with less resources and time. For a list of recently observed PoS malware families please see Appendix B.
- Implement software to detect key-loggers on PoS terminals.
- If possible, deploy a host based intrusion prevention system (HIPS).

Points of Contact

For law enforcement assistance, please contact your local U.S. Secret Service Field Office/Electronic Crimes Task Force (ECTF) or the USSS toll free number at (877) 242-3375. The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial, electronic and cyber-crimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service has established successful partnerships in both the law enforcement and business communities – across the country and around the world – in order to effectively combat financial crimes.

The FS-ISAC encourages member institutions to report any observed fraudulent activity through the FSISAC submission process and login at http://www.fsisac.com/. This reporting can be done with attribution or anonymously and will assist other members and their customer to prevent, detect and respond to similar activity. Non-members experiencing suspicious activity are encouraged to reach out to the FS-ISAC SOC at soc@fsisac.us or to call (877) 612-2622 – prompt 2.

Appendix A. Simple Network Controls for Small Merchants to Protect Customer Data

[NOTE: If you outsource your PoS solution, please work with your PoS or payment processor vendor to ensure that the following controls are implemented**]**

- Reset default passwords for vendor supplied equipment.
- Require regular password changes (at least every 90 days) and change all passwords before and after the holiday season.[9]
- Enforce strong passwords (e.g. at least seven characters in length with both numeric and alphabetic characters).[10]
- Inform employees to be on the lookout for skimmers, USB sticks, or other devices connected to PoS systems. Check all PoS systems for connected devices on a regular basis (daily is recommended), especially ahead of the holiday season.
- Segregate your PoS system from other computers on the network. Do not use PoS terminals for Internet surfing, checking email, or accessing social media.
    - If a PoS terminal must be used for legitimate non-PoS functions, implement a commercial or open source web protection tool on the PoS terminal to limit access to harmful and inappropriate websites
- If PoS services operate on an older operating system, update them immediately and configure auto-updates.
- Update all AV signatures and software on a PoS terminal daily.
- Implement multi-factor authentication for all remote access operations.
- Implement a unified threat management (UTM) device.
    - This is a device that "allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console."[11] This simplifies the cyber security management process for any small and medium size business owner.
    - UTMs "are typically purchased as cloud services or network appliances, provide firewall, intrusion detection, antimalware, spam and content filtering and VPN capabilities in one integrated package that can be installed and updated easily."[12]
- If possible, hire an independent third party to assess your security needs.[13] After this inspection, consider hiring a monthly managed security service provider (MSSP) to manage based on the inspection results. MSSPs are out sourced services that manage network defenses such as firewalls and can typically be hired inexpensively. Below is a list of questions that the SANS cyber research institute has published for businesses evaluating a potential MSSP.[14]

---

[9] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
[10] Ibid.
[11] http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management
[12] Ibid.
[13] http://www.darkreading.com/risk/how-to-pick-the-best-mssp-for-your-smb/d/d-id/1138968?
[14] Ibid.

MSSP Evaluation Questions[15]

Business managers should consider the following questions before deciding to hire an MSSP.

- Does the service provider offer an assortment of solutions that can readily address a variety of environments or do they specialize in a one size fits all solution?
    - No service provider can be in expert in all possible solutions. They should, however, be able to offer a choice of products that can complement each other and provide a solution that offers an optimal amount of protection. [16]

- Do not overlook physical security. How secure is the facility from which the service is being provided?
    - Does the service provider utilize proper access controls and is access to management consoles provided only to those who need it.[17]

- What provisions are in place with respect to fault tolerance? How often are the security devices being polled and what process is in place for notification should a problem occur?
    - While a device may appear to be "up," any number of problems could arise. Is logging being checked periodically and how? Are critical processes that run on the sensor being monitored to determine if they are functioning properly? What about routine maintenance of the device such as checking for disk space? Is there a centralized log server in the event that the security device, itself, is compromised? How much activity is kept, that is, how far back is logging maintained? If a compromise is discovered well after the fact, can accurate data be pulled to help in the investigation?[18]

- Does the service provider have out-of-band access to managed devices?
    - Is there built-in redundancy or is the provider "blinded" and unable to access devices and receive alarms? If you run a high-profile site this is a potential point of attack.[19]

- Does the company specialize in security or is it merely and add-on to an existing business?

- How does the MSSP handle staff turnover? Are passwords routinely changed and do they utilize common passwords across multiple devices? Do they perform background checks on prospective employees and are they bonded?[20]

- What emphasis if any does the provider place on certifications?
    - While certifications do not in and of themselves guarantee expertise, they do provide a means of determining the level of knowledge that the staff has regarding intrusion detection. Look for non-vendor specific certifications, as well as vendor-specific certifications.[21]

---

[15] http://www.sans.org/security-resources/idfaq/mssp.php
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.

- To what extent does the service provider provide continuing education or training for staff members?
    - Intrusion detection is a field that is rapidly advancing. The service provider should be able to readily address and provide information regarding new exploits. Part of the benefit of out-sourcing intrusion detection is that the service provider should be able to provide up-to-date information that would be beneficial in addressing new threats. By providing a proactive approach rather merely reactive, they can more readily determine "patterns of activity" that could pose a threat to an enterprise ahead of time.[22]

- Is the service provider capable of writing custom signatures that can address "zero-day exploits" or are they limited to the signature that are provided by the manufacturer of the intrusion detection system. What assurance is there that the devices that are being maintained are continually updated with the latest signatures?
    - An intrusion detection system that is not updated is comparable to virus protection software that is out of date. It can provide a false sense of security that can fail when it is needed the most.[23]

[22] Ibid.
[23] Ibid.

Appendix B. List of Common PoS Malware Family Names

Table 1 contains a list of common PoS malware family names that have been used in the past. Sophisticated criminals will likely continue to use malware from one or more of these families, after testing a target's AV solution against their samples to evade detection.

[**NOTE:** Sophisticated criminals can make minor changes to existing families of malware, making it undetectable by signature-based AV solutions.]

Table 1. List of Common PoS Malware Family Names

Family Name	Description
Alina[24]	A family of PoS malware that targets applications containing Track data, applies basic encryption and exfiltrates the information. This malware has a command & control structure, which allows it to search for and install automatic updates when they are released.
Backoff PoS[25]	These variations have been seen as far back as October 2013 and continue to operate as of July 2014. In total, the malware typically consists of the following four capabilities. An exception is the earliest witnessed variant (1.4) which does not include keylogging functionality. Additionally, 1.55 'net' removed the explorer.exe injection component: • Scraping memory for track data • Logging keystrokes • Command & control (C2) communication • Injecting malicious stub into explorer.exe
BlackPoS/Kaptoxa[26]	BlackPOS infects computers running Windows that are part of PoS systems and have card readers attached to them. These computers are either infected by insiders or found during automated Internet scans because they have unpatched vulnerabilities in the operating system or use weak remote administration credentials. Once installed on a PoS system, the malware identifies the running process associated with the credit card reader and steals payment card Track 1 and Track 2 data from its memory. BlackPoS is a RAM scraper, or memory-parsing software, which grabs encrypted data by capturing it when it travels through the live memory of a computer, where it appears in plain text. The captured information is uploaded to a remote server via File Transfer Protocol (FTP).
Chewbacca[27]	Chewbacca appears to have been a short-lived malware designed to attack PoS systems and exfiltrate data over TOR. The malware itself has been well documented.
Decebal[28]	Romanian PoS malware released on January 3, 2014. It is written in Visual Basic Script and is capable of checking to see if the computer on which it's deployed is running any sandboxing or reverse engineering software. Decebal can also validate that the stolen payment card numbers are legitimate.

[24] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.
[25] https://www.us-cert.gov/ncas/alerts/TA14-212A
[26] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.
[27] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[28] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.

Dexter[29]	First discovered in December 2012, Dexter is a custom made malware tool used to infect point of sale systems. According to Seculert, Dexter steals the process list from the infected machine, while parsing memory dumps of specific POS software related processes, looking for Track 1 / Track 2 credit card data.
JackPoS[30]	JackPoS was likely first developed in October 2014 and developed through early 2014.[31] There are at least thirty three distinct malware samples of JackPoS in this timeframe.[32] Some indicators suggest that JackPoS has evolved from, or was inspired by the Alina PoS malware.[33] JackPoS is distributed by cybercriminals through drive-by attacks.[34] The malware is sometimes disguised as the Java Update Scheduler.[35] "Several of the found loaders used in detected 'Drive-by' download attack are written using obfuscated compiled AutoIt script, which became quite popular method to avoid AV detection in order to unpack additional binary malicious code and execute further instructions received from the command and control server."[36] "The bad actors have used some sophisticated scanning, loading, and propagating techniques to attack these vectors to look to get into the merchants system thru external perimeters and then move to card processing areas, which were possibly not separated in compliance with PCI polices."[37]
PoSCard Stealer[38]	PoSCardStealer is a name used by ESET, which appears to cover several types of PoS malware. Where the malware doesn't have another name known to ASERT, we will use "PoSCardStealer". Other anti-malware vendors use different naming schemes such as Troj/Trackr-K.
vSkimmer[39]	vSkimmer was disclosed by McAfee in March 2013. vSkimmer searches program memory for track data; however, it only looks for data matching Track 2 format. In addition to using HTTP to exfiltrate stolen data to a C2 server, vSkimmer can be configured to copy data to a specific USB device if it is unable to connect to the Internet. vSkimmer dumps its stolen data to a log file on a USB drive with a certain volume name.

[29] https://www.us-cert.gov/ncas/alerts/TA14-002A
[30] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf and http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[31] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[32] Ibid.
[33] Ibid.
[34] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] http://www.secureworks.com/cyber-threat-intelligence/threats/point-of-sale-malware-threats/

Appendix C. Multi-Factor Authentication

This is an example of multi-factor authentication for a Citrix application.

[NOTE: Many Citrix remote access and virtualization solutions should support multi-factor authentication.]

Enable Two-Factor Authentication[40]

Use the Authentication Methods task in the Citrix Web Interface Management console to enable two-factor authentication for users, if required.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit check box.
4. Click Properties and select Two-Factor Authentication.
5. Select the type of two-factor authentication you want to use from the Two-factor setting list and configure any additional settings as appropriate.

Configuring Two-Factor Authentication

The following steps were recommended by the security firms ActivIdentity Channel and Duo Security for configuring Citrix XenApp.[41] These include the following steps: configure Citrix radius settings, configure RADIUS shared Secret, and configure two-factor authentication settings.

For the XenApp:

1. Log in to the Citrix Web Interface Management Console.
2. Navigate to XenApp Web Sites and click on Authentication Methods.
3. Confirm that only Explicit is checked and click properties.

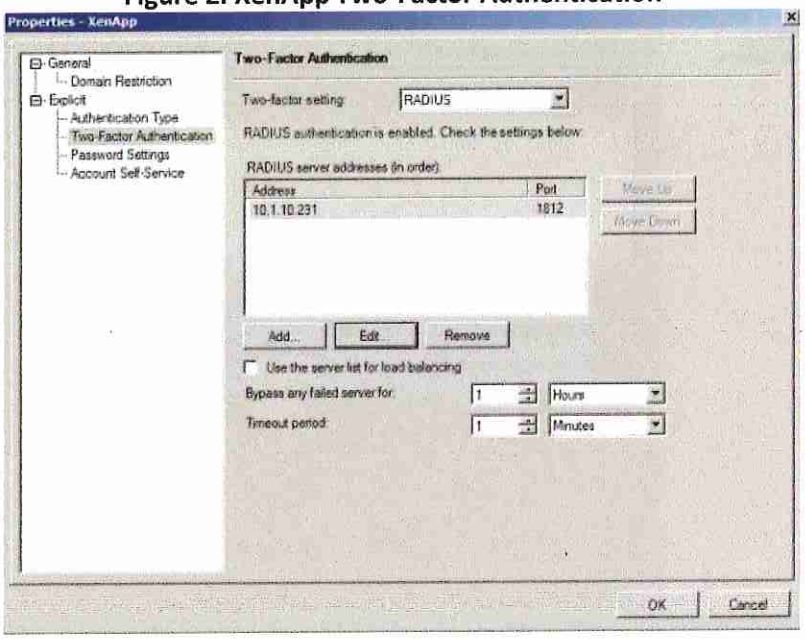
Figure 1. Configure Authentication Methods for XenApp[42]

[40] http://support.citrix.com/proddocs/topic/web-interface-hardwick/wi-enable-two-factor-authentication-gransden.html
[41] http://www.youtube.com/watch?v=ZRbi88JujO0 and https://www.duosecurity.com/docs/citrix_web_interface
[42] https://www.duosecurity.com/docs/citrix_web_interface

4. Click on Two-Factor Authentication and select RADIUS for the Two-factor Setting.

5. Add a RADIUS server and enter the AuthProxy IP address as the server address and 1812 for the server port. Configure the Timeout to 60 seconds and save your configuration.

Figure 2. XenApp Two-Factor Authentication[43]



[43] Ibid.

Figure 3. Adding the Radius Server IP Address[44]

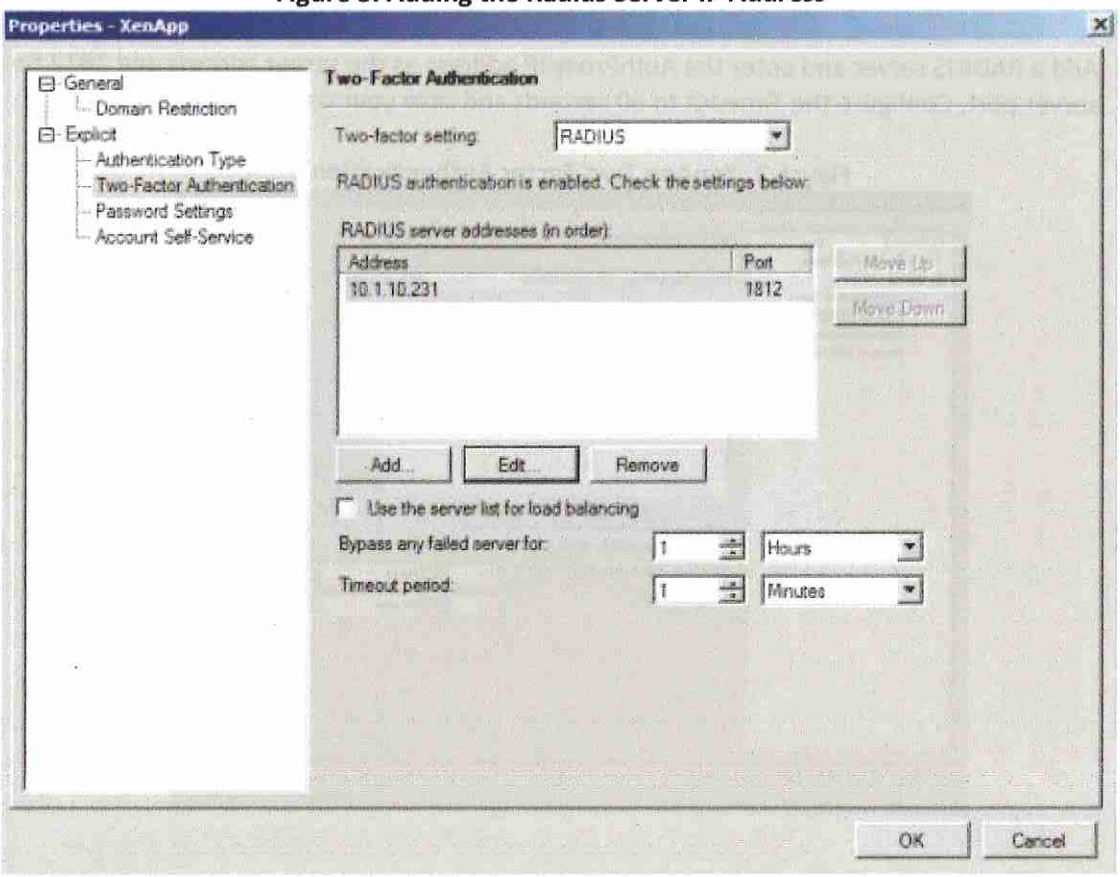
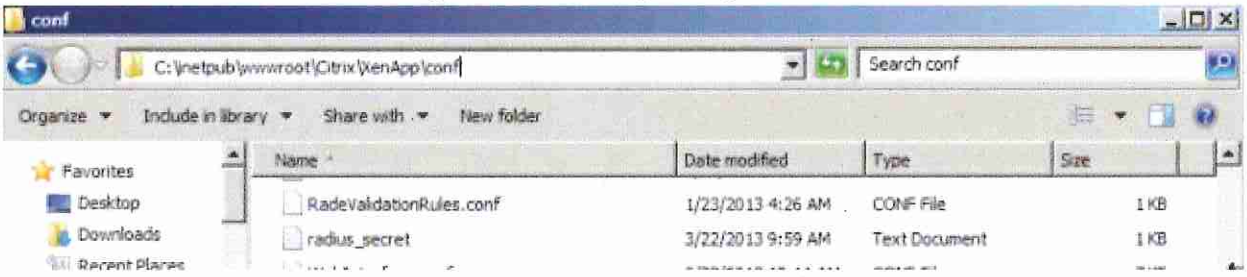


Figure 4. AuthProxy Configuration[45]



6. Create a new text file in the Citrix Web Interface \conf folder called radius_secret.txt. Type the radius_secret from the AuthProxy configuration in the radius_secret.txt file.

(The location for this file is given by the RADIUS_SECRET_PATH configuration value in the web.config file (for sites hosted on IIS) or web.xml file (for sites hosted on Java application servers). The location given is relative to the \conf folder for sites hosted on IIS and relative to the /WEB_INF directory for sites hosted on Java application servers.) Typically the location will be similar to: C:\inetpub\wwwroot\Citrix\Xenapp\conf.

---

[44] Ibid.
[45] Ibid.

7. On the Citrix Web Interface server open the web.config (IIS Hosted) or web.xml (Java Apps) file and add the Citrix Web Interface IP address as the "RADIUS_NAS_IP_ADDRESS".

Figure 5. Adding the Citrix Interface IP Address[46]

```
        <add key="RADIUS_SECRET_PATH" value="/radius_secret.txt"
/>
        <add key="RADIUS_NAS_IDENTIFIER" value="" />
        <add key="RADIUS_NAS_IP_ADDRESS" value="10.1.10.231" />
        <add key="AUTH:SERVER_ERROR"
value="/html/serverError.html" />
```

Two-Factor Authentication Tokens authentication methods for XenApp Web Sites[47]

- **Aladdin SafeWord for Citrix.** An authentication method that uses alphanumeric codes generated by SafeWord tokens and, optionally, PIN numbers to create a passcode. Users enter their domain credentials and SafeWord passcodes on the Logon screen before they can access applications on the server.
- **RSA SecurID.** An authentication method that uses numbers generated by RSA SecurID tokens (*tokencodes*) and PIN numbers to create a *PASSCODE*. Users enter their user names, domains, passwords, and RSA SecurID PASSCODES on the Logon screen before they can access resources on the server. When creating users on the RSA ACE/Server, user logon names must be the same as their domain user names. **Note:** When using RSA SecurID authentication, the system can generate and display a new PIN to the user. This PIN appears for 10 seconds or until the user clicks OK or Cancel to ensure that the PIN cannot be viewed by others. This feature is not available on PDAs.
- **RADIUS server.** An authentication method that uses the Remote Authentication Dial-in User Service (RADIUS) authentication protocol (as opposed to proprietary agent software). Both SafeWord and SecurID can be installed and configured to be presented as a RADIUS server. For Web Interface for Java Application Servers, RADIUS authentication is the only two-factor authentication option available.

[46] Ibid.
[47] http://support.citrix.com/proddocs/topic/web-interface-hardwick/wi-configure-two-factor-authentication-gransden.html