# Case study – white paper on information security systems

Business

However with 128 lions mallard programs written each yearly, banking institutions are only becoming more vulnerable to the threats of cyber-attacks. So it is no surprise that Panther Industries – a world leader in web-banking technology has itself become a target of these emerging threats. More specifically our systems have recently faced attacks from two newer forms of security threats namely ‘ Man in the browser’ (MITT) and ‘ Man in the middle’ (MITT) – two Trojan horse type programs. These two threats work by altering the confidential banking data of the users and Panther Industries’ security Achaeans.

MITT has targeted the two most widely used browsers – IEEE and Firebox by modifying their web assembly structure and stealing user information such as passwords.

MIT implements a similar technique of ‘ pushing’ by intruding verification and redirecting bank customers to a counterfeit server which captures the sensitive information. To retain clients’ confidence in Panther Industries strong authentication and transaction verification techniques need to be implemented to prevent fraud and identity theft. This white paper details the nature of MITT and

MIT attacks and their ability to intercept and modify an online banking transaction. As a protection against these threats this paper also offers as a solution the use of mobile phones and personal digital assistants (Pads) as software tokens to generate unique Digital Signatures that will lend security and authenticity to browser-based transactions. With the ever-increasing

advancements in next generation mobile commerce and smartened technology, this solution is not only secure but also convenient.

Another solution proposed in this paper is the creation of VSP or Virtual Private Sessions wherein the server sends a confirmation to the user which the user must approve for the transaction to be processed.

2. System Description The software architecture at Panther Industries is designed to provide stable enterprise functionality with a host interface that integrates with a back-end with in real-time. This architecture provides the convenience of defining and executing business functions through more than one customer channels.

The first tier of the software architecture is the user interface which is simply the web browser such as r Hereto uses Day ten Dank customers to slang-Len to tenet online Dankly account. Our banking clients require no special installation for this.

The second tier is a PH based secure application server that offers enterprise level application. At Panther Industries PH and not HTML was chosen for scripting as it is the most popular web development language which is used and recommended by MOM, Oracle, HP and many other technology leaders.

PH is a simple, flexible yet powerful and accessible programming language suited for coding and executing web applications. At Panther Industries PH has been the lead scripting language used for integrating banking functions and data from a range of existing systems and applications. The third tier consists of a database server which Panther Industries has developed per

ANSI 92 industry standard to be deployed on highly scalable database engines such as Oracle and Myself.

The software platform finds three ways of deployment namely centralized, distributed (inside) and distributed (outside).

In the centralized form of deployment, the central database could be accessed via a single point with the same intro panel for all system administrators and bank managers. When deployed as distributed (inside), the system supports head offices as well as branches. The system administrator module, back office and the primary servers – application server and database server are located in the head office with each branch retaining its own copy.

In the database (outside) type of deployment the two primary servers are installed on the tenanted facilities and on the network of the data center which is located outside the bank. This use of this software platform at Panther Industries is woo-fold. It is used by personal and corporate clients as well as the bank employees.

The client registration process consists of two stages. The first stage is the preliminary registration wherein the client fills out the personal details on the registration page which generates open and private keys for further use.

Upon acceptance of the bank service agreement the client’s user account is made active by the administrator. From that point on, the client can access and analyze various banking documents online. All the documents and

records accessed by the client are archived and business continuity is ensured as per the service agreement.

The system permanently removes all of the client’s financial information in case the service agreement is terminated. The other users of this are the bank employees namely the System Administrator (AS), Branch Administrator (BAA), Bank Manager (MM) and Technical Administrator (TA).

The AS acts as the supervisor for the system by registering all the bank employees and managing the user accounts. The control panel provides the AS with analytical and statistical reports about the bank activity. The BAA administers the managers and clients’ user accounts, assigns a bank manager for each account and schedules and synchronizes system operation.

The BMW is primarily responsible for processing clients’ financial documents, check for the accuracy of client’s activity and respond to client requests via mail.

The TA is responsible for the overall monitoring, administrating and configuring the system. 3. System Strengths and Weaknesses 3. 1 System strengths enterprise via a robust front-end architecture and with real-time integration with back-end systems via a host interface.

To proactively manage cyber-security risks Panther Institutes provokes I TTS clients Walt n ten Toweling securely tools: 1 encryption: Latest encryption techniques such as 128-bit Secure Socket Layer (SSL) are followed to ensure a secure transmission of data. 28-bit SSL ensures that the customer is

communicating with the banks website and not another computer impersonating the customer. This type of encryption also scrambles the sensitive data so that it cannot be read by hackers. At 128 bits, the data can be encrypted using 288 times the number of combinations as compared to a standard 40-bit encryption making this encryption a trillion times stronger. Panther Industries provides the technology to our clients to offer this encryption to 99.

99% of their customers. Lastly 128-bit encryption ensures that no data was altered or tampered with during transmission. . Session handling: To heighten cyber-security, Panther industries also provides its clients with session handling wherein the application server creates and assigns a new and unique session id after a successful user authorization. In this technique the session identifiers ensure that can each customer is working with their own financial information. 3.

Logging: Via this technique Panther Industries provides its clients an ability to log all customer and employee activity such as IP addresses, sessions etc. The log history generated via this technique provides for efficient supervisory and archival control. . 2 System weaknesses Despite of the strong security measures it provides, the system suffers from some weaknesses which can result in a compromise of customer’s financial data. More specifically the system is not secured against most recent and emerging threats as e have experienced recently – the MITT and MIT referenced in section 1. These two forms of attacks bypass the authentication measures by installing a false sense of security.

What makes these hard to detect is the fact that they use authenticated sessions to piggyback on.

The authentication techniques used at Panther Industries can successfully prevent attacks wherein hackers are trying to impersonate or are trying to steal identity. But since authenticated sessions are used by hackers that deploy MITT or MIT, our authentication techniques cannot prevent these forms of attacks. Another characteristic of these attacks is that they relay legitimate verified credentials in the real-time. Since these are validated credentials, they are able to successfully fool the user-session tokens created on the server.

This technique buys the hacker 30-60 seconds – enough time to steal sensitive information such as passwords. 4. System protection options To provide our banking clients with a robust approach to tackle these emerging threats, we have outlined a few protection options in this section. 4. 1 Protection from Man-Len-The-Browser attack 1 .

Digital signatures: To offer protection to the customers from a Man-Len-The-Browser attack we need to (I) ensure the integrity of the transactional data between the bank and the customer and (it) offer a higher degree of authentication to the transactions.

So to successfully curb this form of attack we need to discontinue the use of a browser as a means to conduct transactions and even detect the variation in the transactions. This will take away the medium that hackers use to mount the attack in the first place. This can be achieved by offering digital

signatures which can be used o sign digital PDF forms rather than conventional web-based HTML or PH forms. So when ten customer clacks ten sodium Dutton ten International travels Vela a PDF Tort which is digitally signed by him.

The submitted information, therefore, is never exposed to the browser environment and therefore cannot be intercepted by the MITT technique.

2. Creation of Virtual Private Sessions: As the name suggests Virtual Private Sessions (VSP) are virtual sessions created with the end-user wherein the server alerts the user of any modifications made to a transaction. The transaction goes through only if the user approves it. The duration of such a session is very small and expires in 30 seconds, which doesn’t give the interceptor enough time to capture, alter or modify the data. .

2 Protection from Main-Len-The-Middle attack To prevent the MIT attacks we propose the use of Public Key Infrastructure (PKZIP) technology. In this technique, a challenge protocol is used to ensure a safe and authenticated transaction between the customer and the bank portal. The challenge protocol helps the PKZIP to validate the website which is requesting the authentication is the banks website which issued them in the first place. This validation is done automatically and will thwart any surname and password requests made via an unverified URL. .

Risk mitigation strategies The risk management strategies to mitigate any risks that arise from the MITT and MIT attacks primarily consist of educating our client about the constantly changing landscape of the cyber-security for

online banking operations and the solutions that we offer via our technology. This will help the banking institutions that use our software platform to have a clear strategy in offering their customers a safe and secure online banking experience.

The checklist should include the following best practices for online banking for the bank employees to prevent fraud: (I) Most current versions of anti-virus programs as well as firewall should be installed on all computers. (it) A designated network engineer should be tasked with the responsibility of regularly updating the bank software (iii) Disable the services and / or conduits that are not in use (v) Provide limited access to the internet to abate the risk of connecting to a malicious website (v) Not all employees should have the ‘ administrator privileges’ on the computers.

Such privileges should only be granted to system administrator or higher management. (v’) Make sure that the employees have scanned their mobile devices before connecting them to the banking software.

(vii) Bank employees should make use of an email client that block the most commonly used email attachments which are used by hackers to install a mallard on any computer. (viii) A reputable pop-up blocker should be installed on all computers.

Ox) Internal bank documents used by employees are always the most recent and virus- free. (x) Unusually high transactions should be immediately brought to the attention f upper management. (x’) Banks should encourage

their customers to check their account balance daily so that they can detect any suspicious transaction on their account at an early stage.

(xii) Ensure that all bank employees have a high-level of awareness and follow good security practices overall. 6.

Conclusion We need to acknowledge the sophistication of the Man-Len-The-Browser (MITT) and Man-Len-The-Middle (MIT) attacks that clients of Panther Industries can face. Despite the secure authentication and encryption techniques that Panther Industries as developed, these mallard programs can steal identity and create a financial fraud in the banking sector by combining a Trojan horse program with pushing. To retain our clients' consonance, Panther Institutes NAS to develop new technologies to stay a step ahead of these cyber-threats.

To counter the threats presented by MITT and MIT, Panther Industries should provide its clients with multi-tier authentication and digital signature technology described in section 4. The digital signature is created by encrypting the customer's private key and associating the transactional ATA with it. The banks system validates the same and compares it with the user's decrypted public key and authorizes the transaction.