

Future Proofing Digital Security

Protecting Digital Identity and Delivering Digital Privacy

Poy Chen
FrontOne Limited
poy.chen@frontone.com

Abstract:

The Digital Revolution has changed the global economic landscape and continues to play a pivotal role in shaping the modern society. As expected, many if not all the characteristics of real-world behaviour, and the consequences of them (for better or worse), have found their way and are playing out in the Digital World.

This paper provides an overview on the challenges the information security providers are facing, the characteristics of some well-known threats, and what counter-measures are available, as well as their effectiveness and or deficiencies.

To provide a more effective alternative, this paper outlines how JANUS can be deployed to mitigate and defeat existing and emerging threats to Web Applications. A global information security problem needs a promising new paradigm technology.

© FrontOne Limited. 2007-2010. Important Notice: This document is provided for private viewing only. It is not intended for reproduction or public distribution. For permission to publish or electronic distribution of this article, please contact FrontOne Limited, PO BOX 17385 Green Lane, 117-125 St Georges Bay Road, Parnell Auckland New Zealand. Email: info@FrontOne.com

Table of Contents

ABSTRACT:	1
INTRODUCTION:	3
DIGITAL IDENTITY CRISIS	3
IDENTITY FRAUD	3
PRESENT AND EMERGING ATTACKS	4
EVOLVING THREATS.....	4
THE MAN-IN-THE-MIDDLE (MITM) ATTACK	4
THE MAN-IN-THE-BROWSER (MITB) ATTACK.....	4
THE MAN-IN-THE-MACHINE (MITM) ATTACK	5
EMERGING ATTACKS.....	5
COUNTER MEASURES	6
TRANSPORT LAYER SECURITY	6
STRONG AUTHENTICATION	6
CLIENT SIDE PROTECTION	7
FRAUD DETECTIONS	8
OUT OF BAND TRANSACTION VERIFICATION	8
THREATS AND DEFENCE ANALYSIS	8
NEW CORE FOCUS	9
JANUS SOLUTION	9
DEFEATING CLIENT SIDE ATTACKS	9
DEFEATING IDENTITY THEFT.....	10
DEFEATING MITM AND MITB ATTACKS	11
DATA SENTRY	11
DEFENCE AGAINST EMERGING THREATS.....	11
CONCLUSION	12
ACKNOWLEDGEMENT	12
BIOGRAPHICAL NOTE	12

Introduction:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The latest IDC report has found that nearly 300 Exabyte (300 Billion Gigabytes) of information is created globally during the course of a year; and production of digital information is set to continue to increase exponentially¹.

In this expanding information economy, Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status, amongst other types of information.

Unfortunately, mirroring the physical world, individuals and organised cyber criminals are increasingly active and are launching technologically sophisticated attacks against individuals and web applications.

There is no question about the need of safe storage of confidential information as Governments are providing a legal framework with the aim of protecting individuals and organisations and are setting minimum standard requirements. With this in mind Industries are joining forces to provide technologies and solutions that provide system and access security to the wider community.

So why are there persistent gaps in the needs and the availability of adequate information security and privacy?

Digital Identity Crisis

For many, a unique username is Digital Identity, it has been the de facto standard, a popular choice to provide computer access, because it is easy to understand and it is also cost effective and it is verified with a password.

Technically, a username is only one form of digital identity in use which is incorporated into authentication processes. There are many others including Credit and Social Security numbers, however, most are linked to a password as the verifier. Even with the latest 2 factor authentication solutions, which utilise large encryption keys to protect data, rely in the end on a password as the enabler.

As societies move further into the information economy, information becomes more valuable and applications that rely on simply password protection will fall prey to cyber crime, due to its vulnerability to many low-tech and high-tech attacks including social engineering.

Identity Fraud

Identity based attacks (phishing, pharming, whaling) are increasing exponentially with the increase of commercial activities online, thereby creating a multi-billion dollar underground economy, trading stolen credit card and personal information.

¹ <http://www.continuitycentral.com/news04501.html>

The number of identity fraud victims has increased 22 percent in the U.S., costing 9.9 million victims a total of \$48 billion in 2008, according to the latest report by Javelin Strategy & Research.

Present and Emerging Attacks

The strong authentication strategy driven by the government legislation to protect consumers has seen the introduction of many two factor authentication solutions. These solutions have increased the barrier of attacks and have made some measurable differences in reducing e-fraud. As a result, attacks have become more targeted and more sophisticated. These attacks are also now being focused to the client side with Trojans that are able to avoid detection and by-pass 2-factor authentication.

Evolving Threats

Targeting the relative weakness of client side defence, emerging threats are more advanced and are successful in avoiding user detection. Modelling on existing Silentbanker² and Clickjacking³ (also known as UI redressing) attacks, a new class of attack is possible and will have a much bigger impact.

In this conceptual attack, the attack consists of multiple parts and is infiltrating several areas of the system over time. It is highly targeted with the capability to adopt itself to a changing attacking surface by receiving updates covertly. A threat with this type of capability has been discovered, confliker3 - a high profile computer worm that has reported to have infected more than 10 million computers around the world.

Another recent example of such an attack is a Trojan horse program (Infostealer.Banker.D, Zeus) that uses a HTML injection technique; when the user of an infected computer goes to the login page of certain websites, the Trojan intercepts the HTML page, checks for certain blocks of HTML code specific to that website, and injects some additional HTML code that presents the user with extra fields in the same login page. In some cases, additional warning messages are inserted, explaining that the extra information is required to “prevent fraud”. This is capable of fooling even those who practice the standard precautionary measures against online fraud.

The Man-In-The-Middle (MITM) Attack

The man-in-the-middle attack intercepts a communication between two systems. A MITM attack on a traditional TCP/HTTP is relatively easy with a transparent proxy. However, SSL/TLS based MITM attacks have also been detected. Some of the tools to carry out such attacks are freely available online and have been verified by security researchers and have even been demonstrated in the public forum.⁴

The Man-In-The-Browser (MITB) Attack

MITB is a recent form of Internet threat related to Man-In-The-Middle (MITM). It is a Trojan that infects a web browser and has the ability to modify pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application. In order to perform this attack, an attacker may progress thru the following steps:

² https://forums.symantec.com/syment/blog/article?blog.id=malicious_code&message.id=185&jump=true#M185

³ <http://en.wikipedia.org/wiki/Clickjacking>

⁴ <http://www.securityfocus.com/brief/910>

1. The Trojan infects the computer's software, either OS or Application.
2. The Trojan installs an extension into the browser configuration, so that it will be loaded next time the browser starts.
3. At some later time, the user restarts the browser.
4. The browser loads the extension.
5. The extension registers a handler for every page-load.
6. Whenever a page is loaded, the URL of the page is searched by the extension against a list of known sites targeted for attack.
7. The user logs in securely on to for example `https://secure.original.site/`.
8. When the handler detects a page-load for a specific pattern in its targeted list (for example `https://secure.original.site/account/do_transaction`) it registers a button event handler.
9. When the submit button is pressed, the extension extracts all data from all form fields through the DOM interface in the browser, and remembers the values.
10. The extension modifies the values through the DOM interface.
11. The extension tells the browser to continue to submit the form to the server.
12. The browser sends the form, including the modified values, to the server.
13. The server receives the modified values in the form as a normal request. The server cannot differentiate between the original values and the modified values, or detect the changes.
14. The server performs the transaction and generates a receipt.
15. The browser receives the receipt for the modified transaction.
16. The extension/BHO detects the `https://secure.original.site/account/receipt` URL, scans the HTML for the receipt fields, and replaces the modified data in the receipt with the original data that it remembered in the HTML.
17. The browser displays the modified receipt with the original details.
18. The user thinks that the original transaction was received by the server intact and authorized correctly.⁵

The Man-In-The-Machine (MitM) Attack

MitM is an attack that carries out a MITM attack in a form of a Trojan that resides in the victim's computer. This type of attack makes it more difficult to select specific targets but once it gets to the right victim it can carry out an attack more effectively.

Emerging Attacks

It is conceivable that an emerging attack could combine multiple attacking techniques. In this scenario, the attacker could take control of the user's computer screen and then dictate what the user can see and do whilst carrying out real time attacks emulating the user's actions and using the legitimate connection to the service provider, thereby leveraging the legitimate user's computer and using the original user's credentials. As a result the combined effect of the attack would be able to:

1. Utilise real user authentication;
2. Intercepts user inputs and modifying transaction data on-the-fly;
3. Modify account information to hide fraudulent transaction and activities;
4. Emulate human behaviour to evade advanced User Interface protection.

⁵ http://www.owasp.org/index.php/Man-in-the-browser_attack

Centre to this attack is its higher level of machine intelligence. It virtually takes control of a user's computer and it is conceivable that it could launch an attack without any user interaction against a website that has implanted only basic security measures. Utilising captured user credentials it navigates through the web form with "tab key" with the assistance of MITB that directs and confirms the location.

Counter Measures

Why do the information Security problems persist? According to Bruce Schneier - an internationally renowned security technologist and author, it is due to the continuous demands and supply of new functionalities; the information security has improved at a slower rate than the increase of system complexity.

Transport Layer Security

The Internet protocol (IP) by design only provides best effort delivery mechanism. Using the web application as an example, the information as part of the web page is not secure; protection is usually provided by **Transport Layer Security (TLS)** or **Secure Sockets Layer (SSL)**, a cryptographic protocol that encrypts the data before it leaves the Application server and a connecting TCP port or the destination client application.

Almost all online banking and e-commerce transaction uses transaction layer security. However, the security weakness in IP protocol design allows any intermediary to claim as the destination, it leaves many points of entry for Man-In-The-Middle attacks. Others choose to bypass the SSL/TLS protection and attack the data before it arrives to the application in an unprotected form.

Strong Authentication

There are many strong authentication solutions to raise the bar of attacks using physical token and one-time-password known as 2 factor authentication - Secure ID by RSA and Digipass by Vasco are leading products in this market, OTP delivered via text message are also very effective with many implementations.

2 Factor authentications significantly reduce the impact of phishing, as the static identify or password is no longer sufficient to complete a transaction. With that, the attacker shifts the focus on to the transaction data with sophisticated Man-In-The-Middle attacks. As a result, online banking fraud doesn't just affect the naive. Last year, Robert Mueller, a director at the US Federal Bureau of Investigation, admitted he'd come within a mouse-click of being a victim himself.⁶

Without question, the use of Chip Authentication Program (CAP) - a MasterCard initiative and a technical specification for using EMV banking smartcards for authenticating users and transactions in online and telephone banking, have further increased the barrier of attacks as it has been designed to verify the user as well as the transaction itself.

The CAP specification supports several authentication methods. The user first inserts their smartcard into the CAP reader and enables it by entering the PIN. A button is then pressed to select the transaction type:

⁶ <http://www.newscientist.com/article/mg20527455.400-benevolent-hackers-poke-holes-in-ebanking.html?full=true>

1. Identify: Without requiring any further input, the CAP reader interacts with the smartcard to produce a numerical one-time password, which can be used, for example, to log in to a banking website.
2. Response: This mode implements challenge-response authentication, where the bank's website asks the customer to enter a "challenge" number into the CAP reader, and then copy the "response" number displayed by the CAP reader into the web site.
3. Sign: This mode is an extension of the previous, where not only a random "challenge" value, but also crucial transaction details such as the transferred value, the currency, and recipient's account number have to be typed into the CAP reader.

In all three modes, the CAP reader asks the EMV card to output a data packet that confirms the cancellation of a fictitious EMV payment transaction, which involves the details entered by the user.

The deployment of CAP in UK for example is used for online banking in the offline mode which has resulted in potential vulnerabilities as has been detailed in the document named "Optimised to fail" - published by Cambridge university researchers. The security weakness is highlighted as follows:

- Mode 1 attacks: The Trojan could collect large amounts of Login codes (user must re-insert card for every login, it is easy to accept human error in data entries), to use it to login to the banking website at a later date.
- Mode 2 attacks: It is conceivable that a Trojan can conduct fraudulent transaction by modifying the amount and the destination account as the authentication code is created to verify the last four digits of the destination account number only. The attacker has a lot of account numbers to choose from without detection.
- Mode 3 attacks: The Trojan misleads the user to create a bogus account (specifically if the customer is paying a bill from an online store) and hides it from view and uses it to conduct a fraudulent transaction.

Client Side Protection

There are various approaches to bolster the security of application that user's use to interact with the service provider.

IBM ZTIC is a product that is aimed to provide a trusted user display in a form of USB hosted HTTPS message transporter that sits between the client browser and the destination web server. While the trusted display approach is sound, ZTIC only works on the transport layer. Because of this a Trojan could harvest digital identities and conduct fraudulent transactions unchallenged, because ZTIC does not sign the transaction, an attacker can simply withhold the current session and use the user data to initiate a transaction behind the scene as the application won't know the difference whether the ZTIC device is used in the transaction or not.

Some products take a different approach - ring fence the user inputs. Trusteer' Rapport and Prevx's secure-browser use various techniques to enhance the integrity of user inputs. It is developed as a browser plug-in or Add-on. Some incorporate malware detection to further strengthen its defence with additional targeted measures. For example, Trusteer rapport encrypts key strokes to prevent MITB attacks to successfully modify the data because it can verify the user data with its encrypted copy before submitting to the server. In the end, Rapport must send the server the user data in its original

form after the due process is done. How can Rapport guarantee that an adversary cannot launch an attack in between Rapport and the destination server? In addition, Rapport won't be in position to prevent an adversary from using the captured user data, which can then deliberately invalidate the session and start anew on its own terms.

Taking the client side protection further is the approach of hardened browsers. An example of this type of implementation is mIDentity (KOBIL Systems GmbH), a smartcard-reader in the shape of a USB-Stick, equipped with a flash-memory. The required applications (e.g. the internet-browser) are pre-installed and so there is no need for any installation. It uses a smart card to ensure highly secure and simple communication, and to prevent third-party access. It mitigates MITB attacks; however, it still leaves plenty of openings for advanced MITM attacks that embed attacking codes into the incoming web pages.

Fraud Detections

While it is outside the scope of this paper, principally because they are not pre-emptive actions or preventive measures, these server side processes are significant as to the security and integrity of the transaction systems and will help to reduce the impact of and financial loss from attacks:

- Monitoring user access behaviour
- Monitoring suspicious transaction values

Out of Band Transaction Verification

Due to additional costs, delays and inconveniences, the usage of full featured out-of-band transaction verifications are more selective in reality, which applies to high value and high risk transactions only with the help of Fraud detection software. The out of band transaction verification systems:

- Use text messages to send user transaction details and authorisation code
- Calls the user with automatic voice response system or by operator

Out of band transaction verifications have not addressed the risk of identity theft and are ineffective for other transactions outside financial transactions; Criminals have been known to successfully use social engineering techniques to trick users into verifying the "wrong" illegitimate transactions.

Threats and Defence Analysis

Based on the definition of Information Security, the job is not done until the user gets the intended data unchanged and confidentially. There are many reasons why we can't start afresh to build a new infrastructure from the ground up, but if we can identify what the core issue is, a better security can be delivered on existing infrastructures. In our opinion, the common deficiencies in current systems are:

Dependency on static user identities: Static identity is difficult to protect, especially in remote applications including web applications; this dependency is the main reason for the exponential increase in data breaches and identity theft activity.

Undefined End point: The true end point of information systems is the user, not the client/remote application. The layered solutions are designed to work within their own layer. For example, SSL encrypts data between two ends and passes on the data in plaintext, because it has completed its task. It has no capability to verify whether the end it arrived at, is the intended destination. Anyone along the route that can provide the information of the intended destination can pretend they are the

recipient (such as transparent proxy attack) and intercept the information. This inability to communicate between security layers amplifies the impact of security vulnerabilities.

New Core Focus

Deriving from the information above and lessons we have learnt thus far, a security solution must be simple to be effective. Providing secure and reliable digital identities is the most obvious place to start.

Dynamic Identity: According to the English dictionary, Dynamic means active and changing. Dynamic Identity can be characterized as an ever evolving identity, thus providing a higher level of security as it reduces the attacking surface. Unlike a static identity, dynamic identities can't be re-used, tracked or traced. Dynamic Identity defeats identity based social engineering attacks and reduces the risks associated with data breaches, as the value of personal data has a less important role in the transaction.

Continuous Mutual Authentication: At present, applications create a new, unique session for each user. As the number of active sessions grow, so does the resources required to manage all logged-in users. The large amount of live sessions gives the attacker more opportunities to exploit the system by leveraging authorised sessions. Continuous Mutual Authentication technology re-authenticates at random times or with every request, thus removing a range of risks that are linked to system and network exploits.

User Centric security: Move the security to user data instead of user and data separately. By delivering data securely to the end user with end-to-end (ETE) or Application-To-User (ATU) User Centric Security model, data confidentiality can be achieved.

JANUS Solution

JANUS is an innovative Information Security framework that provides strong authentication (ID sentry), client side UI protection and transaction integrity verification (Data Sentry).

JANUS is built with patented technologies. The core technology is based on "Message Dissemination", which allows JANUS the ability to create and use a dynamic and unpredictable messaging system to communicate discretely, and reduces the system's surface that is potentially exposed to hostile environments.

Defeating Client Side Attacks

Social engineering attacks harvest digital identities through computer malware such as Key logger or other techniques known as Phishing.

While email based phishing contributed the majority of phishing stories. A significant amount of identity theft is conducted through malware - a Trojan monitors browser events, and intercepts the form content that is being sent to the application server. When a Trojan resides inside the browser, it is possible to use the browser event (for example, onFocus) to start capturing key strokes. If a Trojan resides outside the browser, it could record all key strokes or monitor and record other screen based activities.

While 3AKey (see the next session of this paper) will defeat these types of attack, another good choice is HFA CAPTCHA. In this challenge, a One-Time-Password (OTP) is provided in the form of a CAPTCHA image, and the user is required to solve the CAPTCHA parcel and make up his/her unique password to his/her own preference; This new OTP is entered into a protected control, located outside the web form and the OTP is digitally signed locally by creating a HMAC⁷ which is submitted to the JANUS Server before the form is submitted to the application server.

With JANUS, both browser and external Trojans are defeated because:

1. the password is not static; and
2. the text string captured has no further use in any future transactions;

Defeating Identity Theft

As illustrated in the threat model above, identity based attacks impersonate an active or valid electronic credential. This type of attack is very difficult to defend against with traditional approaches because the attack works within the boundary of traditional authentication technology and circumvents its defences.

To defeat these types of threats, 3AKey would be the best choice because it uses dynamic ID, and **authentication is server initiated**. Systems, Servers or Applications that deploy 3AKey can also enjoy enhanced security as the result of continuous and mutual authentication and the protection of Distributed Local Authentication technologies.

3AKey is a secure HID device with the world first distributed local authentication technology. When a user is accessing privileged information, the application authenticates the 3AKey before the requested information is delivered. The process is completed seamlessly in the background:

1. JANUS makes an authentication query to the 3AKey;
2. 3AKey generates a Dynamic ID based on the previous transaction ID and the new and unique session ID;
3. JANUS derives the identity of the target 3AKey and creates a Server Access Token with a request for identity verification back to the 3AKey;
4. 3AKey responds with the One-Time token to verify itself if the Server Access Token is indeed valid, or a random number if the Access Token is invalid;

3AKey provides the means to carryout multi-factor mutual authentication in a single device in one operation (in this order):

1. the application verifies the computer terminal
2. the application verifies the user's computer profile at the local host
3. JANUS identifies 3AKey
4. the 3AKey validates JANUS;
5. the identity of the 3AKey is verified by JANUS;
6. Application is notified the true user identity;

⁷ Keyed-Hash Message Authentication Code (HMAC or KMAC). In JANUS, it is a message authentication code (MAC) calculated using a randomly selected cryptographic hash function in combination with a secret key

If the requested content warrants a higher security measure, the application would require the user to complete a Localised User Authentication (LUA) before continuing the transaction. To facilitate the LUA, JANUS will first suspend the 3AKey by sending a command to it, enabling a password dialogue to allow a user to enter his/her username and password to re-activate the 3AKey to allow the transaction to continue. This architecture ensures the user password is best protected and removes any back door to the application to enforce both security and privacy - the new terminology called Distributed Local Authentication (3AKey is your personal authentication server).

Once 3AKey is independently verified, the application proceeds with preparing the delivery of the information requested.

Whenever the 3AKey is removed from the host, the connection to the application server will be terminated automatically.

Defeating MITM and MITB Attacks

MITM attacks have the capability to modify the transaction data on-the-fly, making financial gain without the detection of both the user and the application server, leveraging legitimate user credentials. Therefore, user authentication has no relevance at all against this type of attack. The only way to counter a MITB attack is by utilising Transaction Verification.

One of the most effective methods in combating a MITB attack is through an Out-of-Band (OOB) Transaction verification process. This overcomes the MITB Trojan by verifying the transaction details, as received by the host (bank), to the user (customer) over a channel other than the browser.⁸

Data Sentry

JANUS Data Sentry provides a simple but reliable method to verify transaction data discretely.

When a web page is protected by a Data Sentry agent, special controls are created so they are identified exclusively to the randomly selected agent that accompanies the web page.

Before the application server commits to the transaction, it sends a HMAC created from the data received from the user to JANUS. A valid transaction occurs only when JANUS confirms the matching pair of HMAC that has been received. MITM is defeated as modified data doesn't have the same HMAC.

In contrast to the CAP offline approach, JANUS data sentry provides a simpler solution and delivers a higher level of security because the system uses a server generated one-time-password in real time, unlike the CAP which allows OTP to be generated in advance.

Defence against Emerging Threats

The sophistication of emerging attacks seems unstoppable; many feel the only option is Out-of-Band transaction verification or delayed transaction with manual authorisation. While these diminishing choices may work with current generation of attacks, it comes at a significant cost in the provisioning of support systems and usability compromise.

⁸ http://en.wikipedia.org/wiki/Man_in_the_Browser

In contrast, JANUS defeats these emerging online threats without disconnecting the user from the internet utilising 3AKey+. Additional to 3AKey, 3AKey+ has incorporated a control button and a trusted display, thus enabling the user to grant permission for the remote server to authenticate with their personal authentication server (3AKey+), verify and sign transaction digitally in a protected environment under absolute personal control.

Conclusion

There are challenges in securing the cyber space, disconnecting the society or commerce from the Internet is not an option. Therefore, "The time has come to take a quantum leap forward," Michael Chertoff, Secretary of the US Department of Homeland Security says. "We need a game-changer." ⁹ Addressing the fundamental weakness of current approaches is the best way forward.

This paper has introduced several new ideas on how the information can be delivered in confidence, to those who are authorised to receive it. Ultimately, this is a user centric data security solution; it empowers users to reclaim their digital freedom and have the means to protect their identities. These results can be achieved without impacting on usability in real world applications

From an economic perspective, deployment of the above described JANUS solutions will save organisations money. It is our strong belief that using JANUS or other solutions that models on the methods and processes described in this paper will enhance the security of all information systems and applications regardless of its size; safeguard the privacy of all online users and mitigating identity frauds.

Acknowledgement

This work would not have been possible without the help from the team at FrontOne. We also wish to thank the anonymous reviewers.

Biographical Note

Poy currently works at FrontOne Limited; he is the founding Director and the inventor of Message Dissemination and Human Factor Authentication technology - the foundation technologies of 3AKey and JANUS solution. Poy's profession interests are in electronic, information and communication security, he is the architect of JANUS and the lead designer of 3AKey and 3AKey+.

⁹ http://news.cnet.com/8301-10784_3-9741357-7.html