The emergence of new threats

In the last few years, two new types of Internet threats have appeared. These attacks, called “Man-in-the-Browser” (MITB) and “Man-in-the-Middle” (MITM), use sophisticated techniques to circumvent traditional multi-factor authentication technology like one-time password (OTP) tokens to compromise user accounts and commit financial fraud. These attacks highlight the need for financial organizations to securely authenticate users and ensure the integrity of transactions in the face of an evolving threat environment.

Man-in-the-Browser

A new threat is emerging that attacks browsers by means of trojan horses. The new breed of new trojan horses can modify the transactions on-the-fly, as they are formed in browsers, and still display the user’s intended transaction to her. Structurally they are a man-in-the-middle attack between the user and the security mechanisms of the browser. Distinct from Phishing attacks which rely upon similar but fraudulent websites, these new attacks cannot be detected by the user at all, as they are using real services, the user is correctly logged-in as normal, and there is no difference to be seen.

Philipp Gühring “Concepts against Man-in-the-Browser Attacks” 2006

The MITB threat utilizes a malware trojan on a victim’s computer that is able to modify Web transactions as they occur in real time. The trojan does not intervene until after a user has authenticated himself with his financial institution using any authentication technology, including OTP tokens, smartcards and PKI.

Once connected to the legitimate site and ‘piggybacks’ on a legitimate authenticated session between the user and the financial institution, the MITB attack alters the appearance of transactions in the user’s browser. As the alteration occurs in real-time, the MITB prevents the user from detecting the fraudulent
activity. For example, the user thinks he is transferring funds between accounts to pay bills, and the browser displays the transfer, when in fact the MITB attacker is actually transferring the user’s funds into the account of a third party. The user views and confirms what he thinks are his intended transactions, only to become an unknowing accomplice to raiding his own account.

An example of how an MITM attack would succeed:
1. Alice requests transfer of $1000 to Bob
2. MITB alters transfer request to transfer $21000 to Abe
3. MITB submits fraudulent request to bank
4. Bank requests confirmation of transfer of $21000 to Abe
5. MITB alters confirmation page to present user with original request
6. Alice reviews the transaction details and confirms request
7. Bank transfers $21000 to Abe

**Man-in-the-Middle**

MITM attacks rely on customers divulging their credentials on a fraudulent Web site. The attacker then forwards the legitimate credentials to sign onto the legitimate site (such as a bank portal), and then acts as a relay between the legitimate user and the legitimate site.

What is unusual about the MITM attacks is that they succeed in spite of customers using one-time password (OTP) tokens that generate a unique password every minute. The attacker immediately forwards the customer’s credentials to the bank portal, signing in before the token-generated one-time password can expire.

An example of how an MITM attack would succeed:
1. User clicks on link in a phishing email, goes to MITM site and enters credentials (including token-generated one-time password)
2. MITM site connects with Bank site and impersonates legitimate user using phished credentials
3. Bank site grants MITM account access
4. MITM displays phony page stating system is unavailable, or waits until user wants to log off, then displays phony page confirming log-off

By intercepting the traffic between the customer and the portal, an MITM attacker has the freedom to:
- Capture the user’s credentials and use them to gain repeated access to the portal posing as the genuine user (when the credential is a fixed password)
- Log into the system while presenting a “System temporarily down” or “I am unable to log you in” message to make the user think the portal is not available (when the credential is dynamic, such as with an OTP token)
- Log into the system and simply relay all activity between user and the portal until the user tries to end his session. Then provide a “You are now logged off” message while remaining logged into the user’s account (when the credential is dynamic, such as with an OTP token)

**False Sense of Security**

The success of the MITB and MITM attacks highlight the false sense of security that many types of authentication solutions can give IT/Security teams within organizations. In the case of MITB, deploying advanced authentication solutions like smartcards or PKI have long been considered sufficient protection against identity theft techniques. However, since the MITB attack piggybacks on authenticated sessions rather than trying to steal or impersonate an identity, most authentication technologies are incapable of preventing its success.

In the case of MITM attacks, the real-time relaying of legitimate credentials by the MITM to the legitimate bank site defeats the security of OTP generated by hardware or software tokens. The validity of such a password token is between 30 and 60 seconds, sufficient time for the fraudulent user to capture the temporary password and forward it on to the portal, while the password is still alive.
The root problem in an MITM attack is that a user has no way of verifying who is asking for his authentication information. Consequently, most two-factor credentials, including OTP tokens, risk analysis engines, personal assurance messages and so forth are vulnerable to this type of attack. Table 1 in the Appendix analyzes common authentication technologies and their vulnerabilities to MITM attacks.

The Arcot Solution Protects Against Both MITB and MITM
Arcot’s unmatched authentication expertise and patented technology offers organizations a unique approach to protecting online customers from sophisticated attacks like Man-in-the-Browser and Man-in-the-Middle attacks.

Defeating Man-in-the-Browser
Arcot addresses two fundamental problems exploited by MITB attacks
1) How to ensure the integrity of the data in a transaction between a legitimate user and financial institution
2) How to provide additional authentication of the transaction itself to allow the user and financial institution to have a high degree of confidence in the transaction

Ensuring data integrity is fundamental to preventing a MITB attack from succeeding, as there will be no indicator to the user that the MITB attack is underway and altering the transaction. Any successful approach to combating MITB will need to eliminate the browser as means with which to conduct transactions, as well as detect any variance between the transaction originally submitted by the user and the transaction as reported to the financial institution.

Arcot uses digital signing of forms to both bypass any browser-based trojan or helper application as well as detect when there has been tampering with the transaction data. One of Arcot’s technology partners, Adobe Systems, has embedded the ArcotID technology into every one of its Adobe Reader and Acrobat clients. The ubiquity of the Adobe Reader and Acrobat clients means that it is extremely easy to enable the digital signing of forms.

Digital signing of forms works as follows: when a user initiates a transaction, he is presented with a PDF-based form. It is this PDF form, rather than an HTML form, into which he enters all transaction details. Upon completing the form, the user then clicks on the ‘submit’ button which causes the Adobe client to invoke the embedded ArcotID technology. Arcot authenticates the user and digitally signs the PDF, enabling the completion of the transaction. The form data is never exposed to an MITB attack as it takes place outside of a browser environment.

Another technique used by Arcot to defeat MITB is the creation of a Virtual Private Session (VPS). Arcot’s patent-pending VPS creates a virtual session with the end-user, exposing any changes in the transaction made by malware in the browser, or any browser helper objects. The secure in-band authentication provided by the VPS allows the server...
Protecting Online Customers from Man-in-the-Browser and Man-in-the-Middle Attacks

Whitepaper

...to send a confirmation to the user that includes an OTP that the user must enter to approve the transaction. The OTP is time-sensitive, and its short life (e.g., 30 seconds) prevents the attacker from intercepting, altering, and resending the confirmation to the user before the embedded OTP expires. An example of how a Virtual Private Session would prevent MITB:

1. Alice requests a transfer of $1000 to Bob
2. Bank requests confirmation of transfer of $1000 to Bob
   a. If the MITB alters the transfer recipient or the amount, the confirmation image would show the altered request
   b. The MITB would have to reconstruct the confirmation image sent by the bank before the OTP contained in the image timed out
3. Alice reviews the transaction details and enters the OTP contained in the image
4. Alice confirms request
5. Bank transfers $1000 to Bob

The in-band nature of the VPS also eliminates the need for the financial institution from having to send an out of band confirmation to a user’s mobile phone, email, or voicemail. The secure VPS allows the financial institution to send the OTP via the same channel as the transaction itself, making it extremely easy to use.

Defeating Man-in-the-Middle

Arcot also provides a unique software-only solution to the authentication challenge posed by Man-in-the-Middle attacks. The ArcotID is able to automatically verify that the site requesting the authentication credentials is in fact the site that issued them. If the site requesting the credentials did not issue them, the ArcotID will not respond to requests for username or password, automatically preventing identity theft and fraud.

The Arcot solution is unique in its built-in ability to defeat MITM attacks through its use of Public Key Infrastructure (PKI) technology. PKI uses a challenge/response protocol to ensure a secure, authenticated communication session between the client and the application or portal.

Each ArcotID contains information on the web domain that issued that ArcotID. The ArcotID client checks the Arcot certificate to confirm that it is connected to the correct web domain before signing the challenge string. Even if a phishing site replicates the challenge from the domain server, the ArcotID client will not sign the challenge because the fraudulent site does not have valid domain information. Therefore, the attacker is unable to complete the authentication.

---

The ArcotID® Secure Software Credential

The ArcotID secure software credential provides strong, two-factor authentication and digital signing capabilities, completely in software. It enables you to add strengthen any username/password login without changing your users’ login process.

You can deploy multi-factor authentication to all of your customers, employees, and partners without the need for expensive hardware tokens or smartcards. The two authentication factors, a password (“something you know”) and the ArcotID secure software credential (“something you have”) deliver authentication strength while retaining a familiar password-like user experience.

The ArcotID combines a standard X.509v3 digital certificate with Arcot’s patented Cryptographic Camouflage private key concealment technology. Arcot’s solution is based on industry-standard public key infrastructure (PKI), but in practice, it hides all the complexity of the PKI. The user simply types in what looks like his familiar username/password to perform PKI-based operations: authentication, signing, or decryption.

The Flash client makes deploying the ArcotID transparent to your users. There are no pop-up browser messages, no security warnings, and no calls to the help desk. Your users log in as they always have with their user name and password, but behind the scenes the strength of PKI protects them.
The Arcot multi-factor approach to protecting and verifying user identities is invisible to end-users. The Flash client provides an opportunity for IT/Security teams to upgrade users to multi-factor authentication without requiring any change to the familiar username/password login interface. Users log in with their familiar credentials, and ‘behind the scenes’ the strength of PKI-based multi-factor authentication verifies and protects their identity.

The patented ArcotID acts as the second factor (“something you have”) for multi-factor authentication. All users have to do is enter their username and password.

There is no reliance on your users looking for an icon of a lock at the bottom of the browser, or verifying a text or image that is displayed, or noticing that the color of the border of a web page has changed — all of which are susceptible to errors.

**Additional Countermeasures**
Arcot also offers other countermeasures for organizations to deploy against online fraud and identity theft techniques. These include:
- The Arcot Risk Engine that measures the potential for fraud during the authentication process, or during transactions for risk analysis during the authentication process
- A virtual scrambled keypad to foil key loggers and mouse-click loggers
- Dynamic content such as a “Personal Assurance Message,” customized by each user, to confirm that they in fact are on the correct site before entering their credentials

**Summary**
Man-in-the-Browser and Man-in-the-Middle are sophisticated threats that can succeed in spite of organizations deploying multi-factor authentication solutions. These two attacks are representative of an emerging class of threats that accomplish identity theft and financial fraud by exploiting technology previously thought to be secure. For financial institutions to have confidence in the identity of their users and the transactions their users conduct, they must deploy security tools that can stay abreast of evolving threats. Consumer- and business-facing financial organizations can benefit from Arcot’s ability to deploy multi-factor authentication and digital signing solutions that protect against MITB and MITM attacks while retaining ease of use, ease of management, and ease of deployment.
<table>
<thead>
<tr>
<th>AUTHENTICATION TECHNIQUE</th>
<th>MAN-IN-THE-MIDDLE VULNERABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-Time Password Tokens</td>
<td>The one-time password is passed through by the attacker and used to login within milliseconds defeating the password 30-60 second interval update cycle.</td>
</tr>
<tr>
<td>IP Geo-location</td>
<td>The MITM proxy server is routed through a computer located in the same geographic region or ISP as the user’s computer.</td>
</tr>
<tr>
<td>Device Identification</td>
<td>The browser information is passed through unchanged from the original user’s computer. The phisher can easily spoof the HTTP header information to mimic what is received from the user’s computer.</td>
</tr>
<tr>
<td>Browser Cookie</td>
<td>Due to frequent roaming and cookie deletion, users get accustomed to answering secret questions. The MITM can trick the user into answering the secret questions at the phisher site and then use those questions to log into the real bank.</td>
</tr>
<tr>
<td>Personal Assurance Message (Picture or Text on Website)</td>
<td>After stealing the secret questions and resetting the cookie as described above, the attacker also has the picture and text that is unique to the user.</td>
</tr>
<tr>
<td>Virtual Keyboard</td>
<td>The password is stolen in transit after being entered on the virtual keyboard.</td>
</tr>
<tr>
<td>Out of Band (Phone or email)</td>
<td>Because the user is online performing transactions, when the phone rings with the passcode, the user answers and enters the code into the website. The attacker’s proxy site passes the code through, and a script changes the transaction that the code is verifying without the user knowing.</td>
</tr>
<tr>
<td>Identifying Questions</td>
<td>The attacker’s MITM proxy automatically passes the questions to the user, intercepts and steals the user’s answers then returns the user’s answers to the web site.</td>
</tr>
</tbody>
</table>