Entrust® Securing Digital Identities & Information

Man-in-the-Middle Attacks

Helping to eliminate the threat without impacting the business

September 2008

© Copyright 2008 Entrust. All rights reserved.

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2008 Entrust. All rights reserved.

Table of Contents

© Copyright 2008 Entrust. All rights reserved.

1 Introduction

Well known in the cryptography community, man-in-the-middle (MITM) attacks have long been recognized as a potential threat to Web-based transactions by security experts. But in the summer of 2006, and ongoing through 2008 and beyond, these attacks became much more widely recognized as a serious and real threat when a large, global financial institution's business customers were targeted by attackers using MITM tactics.

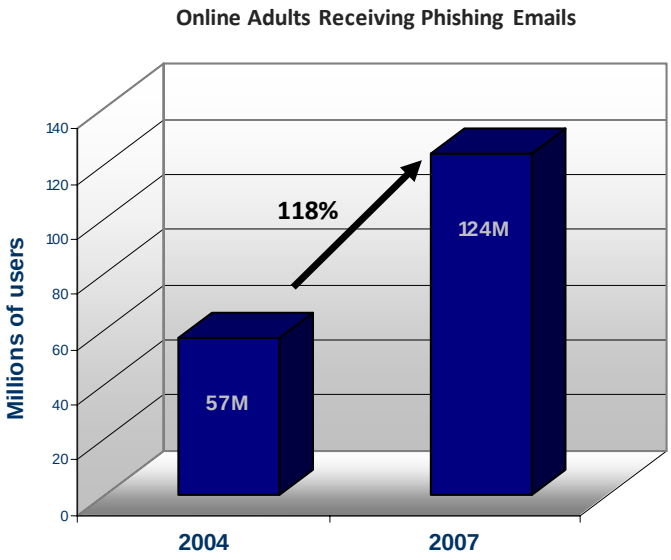
Leveraging one of the most serious methods of compromising Web transactions, MITM attackers "get in the middle" — or between a customer and a legitimate Web-based application. From this position, they intercept all communications and can not only observe but also modify transactions.

In the past, it was commonly believed that deploying a single, second-factor authentication mechanism could provide protection and prevent MITM attacks. But, as this incident illustrates, MITM attackers can bypass security that relies on a single authenticator as the sole layer of defense.

> $3.2 billion was lost to phishing in 2007 … 3.6 million adults lost money to phishing attacks in 2007, compared to the 2.3 million the year before that ...
>
> *Source: "Phishing Attacks Escalate, Morph and Cause Considerable Damage," Avivah Litan, Gartner, Inc., December 13, 2007*

Increased attention on MITM attacks comes at a critical point in Web security[1]. Attackers are no longer random hackers simply seeking attention or notoriety. Instead, attacks are targeted, purposeful and organized. They are designed for profit and are frequently launched by sophisticated criminal organizations that systematically employ sophisticated phishing sites and/or malware to help orchestrate complicated MITM and other password-stealing schemes.

The results of these attacks on organizations are well known: lower revenues because of customer anxiety; higher operating costs from remediation and recovery efforts; and damage to the corporate brand image and reputation, which can be difficult to quantify.



Single security measures, such as tokens or passwords, can improve security, but they do not provide sufficient protection to stop a sophisticated MITM attack.

Defending in depth — using a layered approach — can be a better solution in helping to prevent attacks from known MITM forms. Using an open, standards-based approach has proven to be one of the most viable from an investment perspective, allowing for evolution and rapid response to the ongoing innovations of the criminal element.

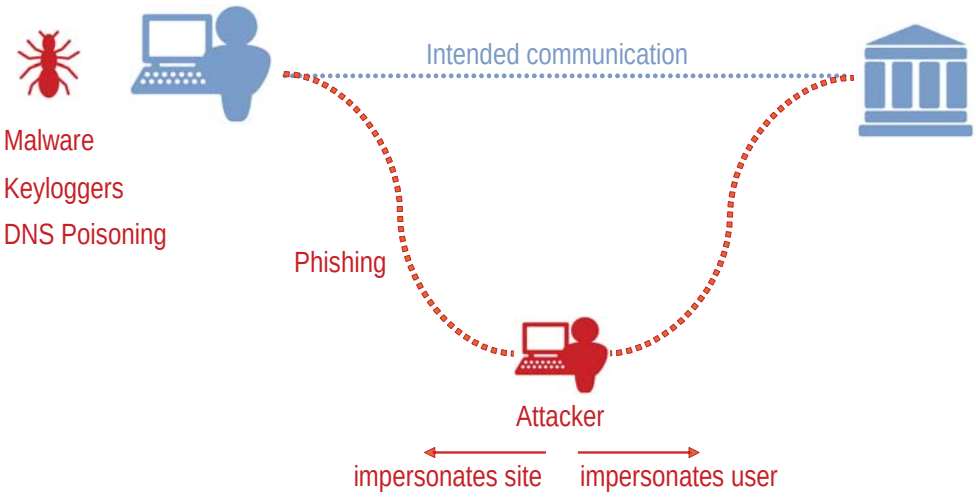
[1] Graph Source: *"Phishing Attacks Escalate, Morph and Cause Considerable Damage," Avivah Litan, Gartner, Inc., December 13, 2007*

© Copyright 2008 Entrust. All rights reserved.

2 Definition: Man-in-the-Middle Attacks

What is a man-in-the-middle attack? Very simply, MITM attacks occur when an attacker attempts to intercept communications between two parties, such as a customer and a financial organization, without their knowledge.

By doing so, the attacker becomes "the man in the middle." Both parties are unaware of the attacker's presence. So, acting as a proxy, the attacker can both review and manipulate the contents of the messages he is relaying between the two parties.



As an example, the following illustrates a typical MITM attack scenario against a site protected with user names and passwords:

1. An attacker sends an e-mail that appears to come from a legitimate financial services company, directing customers to log in to their account and verify personal information. The e-mail does not direct customers to the legitimate company's site, but to a carefully designed replica.

2. As a customer enters the site and uses their user name and password to log in, the phishing site passes this data on to the legitimate site and logs into the user's account. The attacker has now essentially hijacked the customer's online session.

3. The customer proceeds to perform transactions, unaware that the attacker can modify requests or initiate new transactions.

The attack scenario does not change if some additional authentication factors are used:

- If tokens are used, the MITM attacker can intercept and replay the one-time password (OTP) within the 60-second validity period.

- If challenge questions are used, the MITM attacker can simply observe the challenge question and present it to the user, replaying the response to the legitimate site.

© Copyright 2008 Entrust. All rights reserved.

In addition to these known MITM attack scenarios, new variations of both MITM and other attack types are occurring and evolving regularly. Attackers often use malware, leveraging new social engineering tactics to plant spyware, keystroke loggers and redirectors to capture personal information. Past occurrences have been general and aimed at mass numbers of consumers. But recent occurrences have been targeted attacks, most frequently directed at financial institutions.

In a recent example of a successful attack combining social engineering with phishing and malware, more than 20,000 senior corporate executives were fooled into clicking a link in an e-mail that purported to be a subpoena. The resulting malware installation enabled a man-in-the-middle attack to be successfully completed without the end-users' knowledge.

Preventing MITM attacks and blocking phishing scams requires more sophisticated security measures than simply adding a second factor of authentication. Of course, there are some security benefits to this approach, but devices like hardware tokens alone can't provide the layers of security required to defend in depth against sophisticated MITM attacks.

There are second-factor authentication technologies that can be more difficult for MITM attackers to hijack, but they often involve challenging deployment and usability issues. It is important to understand the full impact of additional authentication mechanisms, both in terms of their ability to help prevent sophisticated attacks and to the feasibility of their deployment.

When evaluating security solutions to defend against MITM attacks, consider the following key criteria:

Defense in depth	Look for a solution that provides multiple layers of security. By using a layered security approach, even if a savvy attacker is able to defeat any one of the single security components, protection is still provided by the remaining security layers.
Impact on customer experience	Look for solutions that can help minimize changes required to the customer experience, including how customers interact with Web applications. Downloading software, deploying physical second factors and altering the primary functions that customers use to make transactions can have dramatic impacts on help-desk costs and customer retention.
Future attacks, future growth	Look for solutions that can easily adapt and change to respond to future attack variants and also can effectively grow to accommodate changes in scale and transaction type.
Flexible defense mechanism	Look for solutions that can provide flexibility as opposed to a one-size-fits-all approach. For example, one method of authentication may be best suited to address a subset of high-value customer transactions, yet it might not be the best option for other customers who perform less-risky online transactions. A solution should be able to address multiple-user communities with differing risk factors using multiple security measures to defend in depth.

© Copyright 2008 Entrust. All rights reserved.

3 Preventing MITM Attacks without Sacrificing the Business

Preventing MITM attacks without sacrificing core business operations or disrupting customer interactions can be achieved using a layered approach. In addition, the need to be flexible while accommodating future growth and responding to future attack variations all reinforce the need for a layered approach.

There are three primary security layers that organizations can employ to help prevent MITM attacks without compromising the user experience:

1. ***Extended validation (EV) SSL certificates*** so customers can clearly see whether a site is safe or unsafe.

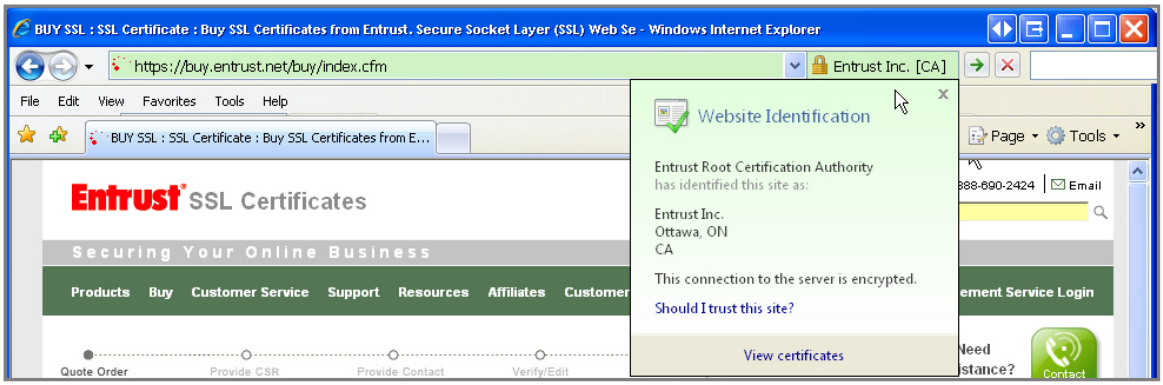
2. ***Multifactor authentication*** methods that are more difficult for attackers to compromise, yet only minimally impact the customer; includes the ability to combine authentication with options like digital signatures for increased MITM protection.

3. ***Fraud detection*** to transparently monitor online activities in the background and help block fraudulent transactions in progress or prevent them from occurring.

Extended Validation SSL Certificates

The first security layer, EV SSL certificates were developed by a working group of browser vendors and certification authorities (CA) called the CA/Browser Forum. Extended validation represents a new tier of SSL certificates with very high standards for validation and assurance. Led by Entrust, the CA/Browser Forum also defined consistent browser security user-interface elements that are being supported by newer versions of browsers, including Microsoft Internet Explorer 7 (IE 7), Mozilla's Firefox 3 and Opera 9.5.

For the consumer, EV SSL certificates provide clear, simple visual cues in un-modifiable parts of the browser interface that indicate whether a site is legitimate and should be trusted. For example, IE 7 displays a green background behind the address bar for sites with an EV SSL certificate. IE 7 also shows the corporate identity and the name of the issuing CA (e.g., Entrust) in a scrolling user-interface element beside a more prominent padlock icon.



In order to obtain an EV SSL certificate, the organization must go through an extensive vetting process, including validation of their business information from government sources. This registration process captures information about registrants and can prevent phishers from rapidly switching between newly registered Web sites and domain names.

© Copyright 2008 Entrust. All rights reserved.

From the perspective of the end-user, all one must do is look to see the prominent green address bar before beginning to use a Web site. If a customer sees the green bar, they can be confident that the Web site is registered to the stated organization.

If the bar is red, the certificate used on that site is in some way false, quickly highlighting that caution is warranted. In this way, EV SSL certificates can stop phishing sites and MITM attacks cold by communicating to the user that the site can or cannot be trusted — quickly and easily.

Multifactor Authentication

A second security layer that can protect against MITM attacks is multifactor authentication. Beyond simple single-factor mechanisms such as username and passwords, there are many different authentication methodologies that provide a range of protection from MITM attacks.

Each methodology offers a different balance point between increased security and increased user complexity. Each typically has different costs of ownership and deployment processes. For each business need, there is an authentication approach that can provide another layer of security and can address cost and user-impact requirements

While reviewing different authentication methodologies, it is important to consider the following:

- ***Security*** – ability to help prevent MITM and other attack types
- ***Customer acceptance*** – ease of use, transparency
- ***Deployment & management*** – day-to-day operational considerations including cost, scalability and interoperability
- **Extensibility** – the ability to combine other security techniques, such as digital signatures on transactions, with authentication for a deeper level of strength

Table 1: Public Key Infrastructure (PKI) Authentication Options

Methodology	Security	Customer Acceptance	Deployment & Management
PKI using client software – Uses a client-side application for authentication and key/certificate management	Correctly deployed, can be very effective at preventing MITM attacks as the private key can not be stolen or compromised	Customers can be resistant to installation of client software; client software also requires broad operating system support for customer coverage	Client software deployment can be expensive due to user installation issues, deployment of patches/updates, ongoing customer installation support; key management expensive if not automated
PKI without client software – Uses native O/S or zero-footprint client for authentication and key/certificate management	Very effective at preventing MITM attacks as the private key can't be stolen or compromised	Transparent and easy to use as the PKI operations are typically transparent to the end-user.	Without client-side software, easy to roll out and maintain; key management expensive if not automated

© Copyright 2008 Entrust. All rights reserved.

Table 2: Multifactor Authentication Methods

Methodology	Security	Customer Acceptance	Deployment & Management
IP-Geolocation – identifies where a user's currently assigned IP is geographically and whether it is normal or appropriate for the user	Can help identify an MITM attack based on allowable and/or normal IP for a user; can be exploited so best used with other layers	Transparent to users	Initial registration of an IP done transparently, as with profiling of a user to understand patterns of normalcy
Machine Fingerprinting and Tagging – stores and validates a profile of the customers system	Tagging resistant to MITM as cookies or flash objects difficult to steal; fingerprinting can be exploited so best used with other layers	Transparent to the user if consistent machine or non-cookie methods used	User must register each machine but minimal ongoing support if non-cookie method used
Knowledge-based authentication – queries that require specific knowledge to answer	May be exploited by MITM attacks; best used in conjunction with other layers	Intuitive and easy to use; no need to deploy anything physical to the end-user	Initial registration can be done online; easy and inexpensive to support if questions are chosen and answers processed carefully
Out-of-Band – phone call, e-mail message or SMS text message that delivers one-time passcode and transaction summary	Very effective at defeating MITM attacks as this bypasses the communication channel the attacker has compromised	Easy to use as leverages existing communication mechanism; more appropriate for higher value or risky transactions versus each login	Beyond initial registration of communication method (e.g., phone number), little management required
Non-Hardware One-Time-Password – Grid card with coordinate lookup	May be exploited by MITM, but grid challenge can be hardened to make it more challenging for attackers	Portable and easy to use; may be physical or electronic; can be lost or forgotten	Inexpensive to produce and deploy physical tokens; electronic versions easily distributed in real time
Hardware Tokens – one-time password-generating hardware devices	May be exploited by MITM attacks during small time window; best used in conjunction with other layers	Portable and easy to use; can be lost or forgotten	Initial device purchase, deployment and replacement can be more costly than non-physical options, although there are cost-effective options now available on the market that may be appropriate for some or all users

© Copyright 2008 Entrust. All rights reserved.

In addition to authentication, assessing a solution on its ability to provide additional mechanisms to prevent MITM attacks is important. For example, the combination of strong authentication with cryptographic functions like hashing and digital signatures can provide a strong defense against man-in-the-middle attacks.

Coupled with out-of-band authentication, adding a cryptographic check of the originating and completed transaction (a hash), along with binding of the transaction to a user with a signature, can significantly increase the security of an online transaction. This can be achieved both with the deployment of digital certificates to end-users, as well as through server-side techniques that remove the need to deploy digital certificates altogether.

Selecting one or a combination of these authentication methods, in conjunction with other security layers, can effectively stop MITM attacks. The key to selecting a solution is to ensure that it is both flexible and open. Standards-based solutions do not lock organizations into specific authentication methods but provide a range of authentication methods.

In addition, organizations should consider the impact to both the customer and to the operations of the business. Proprietary, one method solution — such as PKI using client software — not only limits the available authentication methods to one, but also are costly and complex to deploy, support and maintain.

Fraud Detection

Fraud detection monitors transactions to help detect and prevent MITM attacks and other forms of fraud. It provides a third layer of protection in addition to EV SSL certificates and multifactor authentication by detecting fraudulent intent and providing notification of fraudulent transactions.

Fraud detection finds anomalies by examining:

- ***Access*** – fraud detection determines where and when the user is logging in and compares this to typical access patterns to find anomalies.

- ***Transaction*** – fraud detection looks for unusual transactions such as those involving high values or large bill payments to new payees.

- ***Behavior*** – robust fraud detection solutions monitor the sequence of transactions within and across user sessions to spot fraudulent activity patterns (e.g., completing a change of address and then ordering new checks). It should also examine behavior and compare it to past navigational sequences to identify if the user is logging in at an unusual time of day, performing a transaction involving an unusual payee, or unusual amount.

Fraud detection provides transparent monitoring and can help stop suspicious transactions by proactively contacting customers, blocking transaction access or requesting additional authentication. It is invisible to the attacker and is difficult to circumvent using MITM attacks or other attack variations.

As an example, the much-publicized MITM attack against a large financial services company likely could have been prevented if fraud detection had been used. Fraud detection could have spotted the unusual transactions and anomalous behavior associated with the attack and alerted the company even if the attacker had hijacked the user's session and logged in using valid credentials. Once the unusual activity had been detected, the financial institution could have acted in time to allow any fraudulent transactions to be reversed.

© Copyright 2008 Entrust. All rights reserved.

4 The Entrust Approach

As discussed, the best security strategies use the defense-in-depth approach to help prevent MITM attacks. Organizations should implement layered security to provide more complete protection than any one defense mechanism. Entrust provides organizations all three of the recommended security layers that help prevent MITM attacks:

1. Entrust Extended Validation SSL Certificates make it easier for users to detect when they are being targeted by an attacker's fraudulent site.

2. Entrust's versatile authentication platform, Entrust IdentityGuard, provides a range of authentication methods that make it harder for MITM attackers to steal credentials without disrupting the user experience. It also includes the ability to cryptographically validate and sign a transaction for increased security.

3. Entrust's zero-touch fraud detection platform, Entrust TransactionGuard makes it easier to detect when attacks are happening and helps intercept fraudulent transactions.

These layers provide protection from MITM and other attacks while providing flexibility, minimizing the impact to the customer experience.

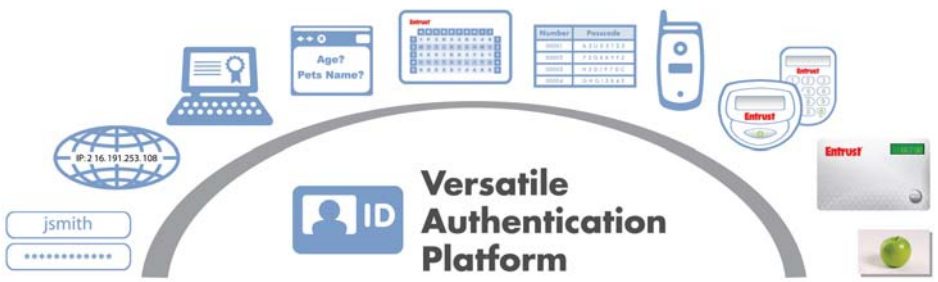
Entrust Certificate Management Services — EV SSL Certificates

Managing the purchase and administration of SSL certificates for multiple Web servers — sometimes in many different locations — can be time consuming and costly. For organizations that have multiple Web servers that need SSL, or have many, distributed SSL-enabled devices, Entrust Certificate Management Services helps ensure they are organized, valid and managed properly.

The Entrust Certificate Management Service features a self-service tool that helps streamline the procurement and administration of SSL certificates, including EV SSL certifications that help defend against MITM attacks.

Acting as a centrally managed, self-service system, the Certificate Management Service reduces administrative hassles and lessens the risk of inadvertent certificate expiration by allowing customers to synchronize and control the timing of SSL certificate expiration. The Certificate Management Service also enables administrators to "re-use" or "recycle" SSL certificates to maximize usage and minimize costs.

Entrust IdentityGuard — Versatile Authentication Platform



© Copyright 2008 Entrust. All rights reserved.

Entrust IdentityGuard is a versatile authentication platform that enables companies to apply the right level of strong authentication, tailored to the risk associated with the user or user transaction.

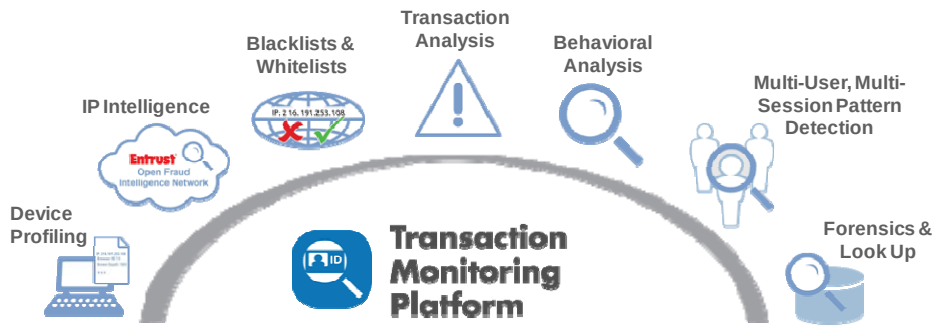
The platform can be integrated into an existing environment to provide a range of affordable authentication options that can be implemented, as required, without the need to deploy expensive hardware or introduce significant changes to the user experience.

The range of authentication methods includes IP-geolocation, machine authentication, grid authentication, out-of-band authentication, hardware tokens and many more. Because Entrust IdentityGuard is an open, standards-based platform for authentication it:

- ***Manages cost and complexity*** by providing a range of authentication methods from a single platform.
- ***Streamlines administration*** using centralized policy management to help reduce the risk of policy inconsistency and compliance issues.
- ***Is ready for what comes next*** thanks to a stable, open platform and a commitment to adding new and innovative authentication options.
- ***Is a proven solution*** used today by numerous large organizations around the world.

Entrust TransactionGuard — Zero Touch Fraud Detection

Entrust TransactionGuard is a zero-touch fraud detection solution that searches for fraudulent behavior and access patterns. It rapidly translates the massive volumes of data streams generated by transactional Web sites into intelligible information about customer behavior. The Entrust solution examines this information and then compares it to customer behavior profiles, business-risk thresholds for transactions and fraud patterns observed across the financial services industry.



Entrust TransactionGuard performs real-time fraud detection without impacting existing business applications, which dramatically reduces the time to implement the solution. Also, because no changes to existing applications are required, it is easier and faster to adapt to evolving fraud patterns as they develop.

Entrust TransactionGuard identifies potentially suspicious behavior and high-risk activities with no impact on system performance or the user experience.

© Copyright 2008 Entrust. All rights reserved.

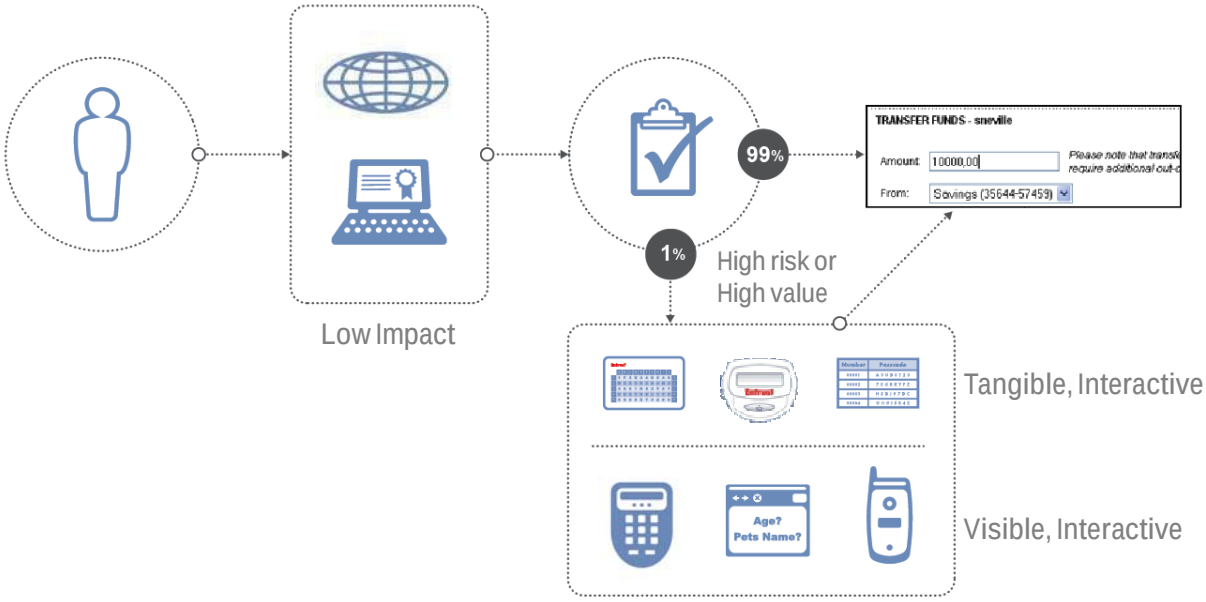
Entrust TransactionGuard provides:

- ***Zero-touch fraud detection*** that requires no changes to applications or the user experience, resulting in fast deployment.
- ***Rapid response*** to new threats with no change to business applications.
- ***A powerful analytics engine*** that can help identify emerging threats.
- ***Proven technology and an approach*** used by large organizations around the world.

Risk-Based Authentication

Combining multifactor authentication and fraud detection provides layered protection while further minimizing the impact on customers. Extending the transactional security by leveraging proven cryptographic functions, such as digital signatures, can further strengthen the online session.

Integrating fraud detection and multifactor authentication means that the user experience is only interrupted when there is a threat such as a MITM attack. Based on risk, transaction and behavior patterns, fraud detection can be used as a suitable solution so customers are not burdened with stronger interactive authentication mechanisms when they are completing routine transactions.



For example, a financial services organization is using machine authentication and IP-geolocation information to authenticate users to their online banking portal. A user logs in from an unknown PC in Russia, instead of their typical PC in Iowa. Entrust's risk-based authentication capabilities can "step up" the authentication required for this user to complete a transaction (e.g., triggering an out-of-band e-mail to the customer with the details of the transaction and a one-time password).

"**Recommendation:** Custodians of consumer financial accounts should protect those accounts from phishing and other malware-based attacks through fraud prevention, stronger user authentication and transaction verification."

"Phishing Attacks Escalate, Morph and Cause Considerable Damage,"
Avivah Litan, Gartner, Inc., December 2007

© Copyright 2008 Entrust. All rights reserved.

5 Conclusion

As with other potential threats to online business, MITM attacks require organizations to improve security using a layered approach. When looking at any proposed solution, it is important that organizations evaluate them within these key criteria:

- **Defense in depth**
- **Impact on customer experience**
- **Future attacks, future growth**
- **Flexible defense mechanisms**

Simply moving to the use of EV SSL certificates can help prevent many attacks. Next, adding risk-based, multifactor authentication and fraud detection provides even more robust protection that can further deter MITM attacks.

Although some non-layered approaches may provide limited protection today, they often do so using proprietary and invasive client software technology. These approaches provide limited protection at great cost as inflexibility can lead to more customer help-desk calls and abandoned transactions as customers suffer through a frustrating and confusing online experience.

In contrast, using a multilayered, open-standards-based security approach has proven to be the most flexible approach financially and operationally. It allows for quick responses to changes in the business environment, such as a dramatic increase in the number of customers, or in the technological environment, such as a dangerous new security threat that can be rapidly and easily managed.

6 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in more than 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

© Copyright 2008 Entrust. All rights reserved.