



Secure e-Banking

By



Table of Contents

Introduction.....	1
Types of Attacks	1
IDentiWall Technology.....	2
IDentiWall Authentication server.....	2
IDentiWall Verification server.....	2
IDentiWall Messaging server.....	2
IDentiWall HTTP Gateway	3
IDentiWall Messaging Gateway.....	3
IDentiWall Recording server	3
IDentiWall Location server.....	3
IDentiWall Session Risk Assessment server	3
IDentiWall Security Syndication	3
IDentiWall Functionality	6
IDentiWall Customer Benefits	6
IDentiWall Benefits for the Bank	6
IDentiWall multi-disciplinary support.....	7
IDentiWall Security Syndication Server.....	9
IDentiWall Authentication Server	8
IDentiWall Location Server	8
IDentiWall Verification Server.....	8
IDentiWall Recording Server.....	8
IDentiWall Session Risk Assessment Server.....	9
IDentiWall Investigation WorkBench	9
Conclusion	9

Introduction

The customer computer is the weak link in the e-banking security chain, raising complex challenges to online banking systems. The customer computer is the site of numerous attacks that are a clear and present danger to the reliability of the service, the reputation of the bank and its financial viability.

Made4Biz Security Inc. developed IDentiWall™ Secure Banking based on the experience of the world's leading banks. To meet the challenge posed by the ever-increasing sophistication and variety of attacks, Made4Biz constantly develops and improves IDentiWall, ensuring that it has the most effective means to meet the challenge.

Types of Attacks on eBanking

The currently known types of attacks on both customer computer and the bank web site's security that must be met include:

Man-in-the-browser – A "Trojan horse" changes the contents of the form that the customer submits to the bank website. The change is not noticeable in the form itself. It takes place only in computer memory before SSL encoding.

Man in the Middle - Rogue software is put in place at some point between the customer computer and the bank web sites and intercepts all the information transmitted between the customer and the bank.

Key Logging – Software implanted in the customer's computer that records all the keystrokes of the customer, providing a complete record of user IDs, passwords, pin codes, account numbers and transactions. Sometimes this is integrated with additional rogue software, and usually it sends the information it has collected to the hacker.

Session Hijacking – The session is hijacked by unauthorized use of the cookies deposited by the banking site.

Pharming – Pharming is diversion of traffic from a legitimate site to a rogue web site.

Phishing – Customer identity details are stolen. Typically, this is carried out in a place and context removed from the bank web site, such as a fraudulent e-mail asking for information.

Site Cloaking – Cloaking fools search engines by disguising one web site as another.

Cross-Site Scripting – A script is injected to one web site or web log, but it is operated at a different web site.

OS command injection – Injection of operating system commands to be carried out at the web site.

SQL Injection – Injection of SQL queries to be executed at the web site.

Cookie Tampering – Information in the cookie is changed to allow an attack.

Form Tampering (read-only and hidden fields) – Changes are made in hidden or read-only fields in the HTML form.

Outbound Data Theft – Data sent from the web site are intercepted for use in attacks. For example, that may include data about the software installed at the site, version number etc.

Application Denial of Service - Numerous types of attacks make use of the possibility of entering rogue information in input fields.

The above survey only highlights the major sources of attacks, which are constantly multiplying.

IDentiWall Technology

This section describes the technologies employed by the IDentiWall platform.

IDentiWall Authentication server

- Radius authentication
- LDAP authentication
- One-Time-Password (OTP) authentication
- Database authentication
- Workflow authentication
- MD5 authentication
- EAP authentication (TLS, ND5...)
- Token authentication
- Voice authentication

IDentiWall Verification server

- Multiple network-based verification
- Workflow verification
- Voice verification

IDentiWall Messaging server

- SMS
- MMS
- IM

- email
- Beeper

IDentiWall HTTP Gateway

- HTTP Session manager
- Layer 3 Redirector
- Intelligent Filtering
- Cyber Attack Defender

IDentiWall Messaging Gateway

- SMPP
- SS7
- Failover between networks

IDentiWall Recording server

- Archiving
- Playback

IDentiWall Location server

- Physical Location
- IP Location
- Cellular Location
- Navigation Location
- Credit Card Location
- Workflow Location

IDentiWall Session Risk Assessment server

- Location
- Content & Action
- Navigation typicality
- History

IDentiWall Security Syndication

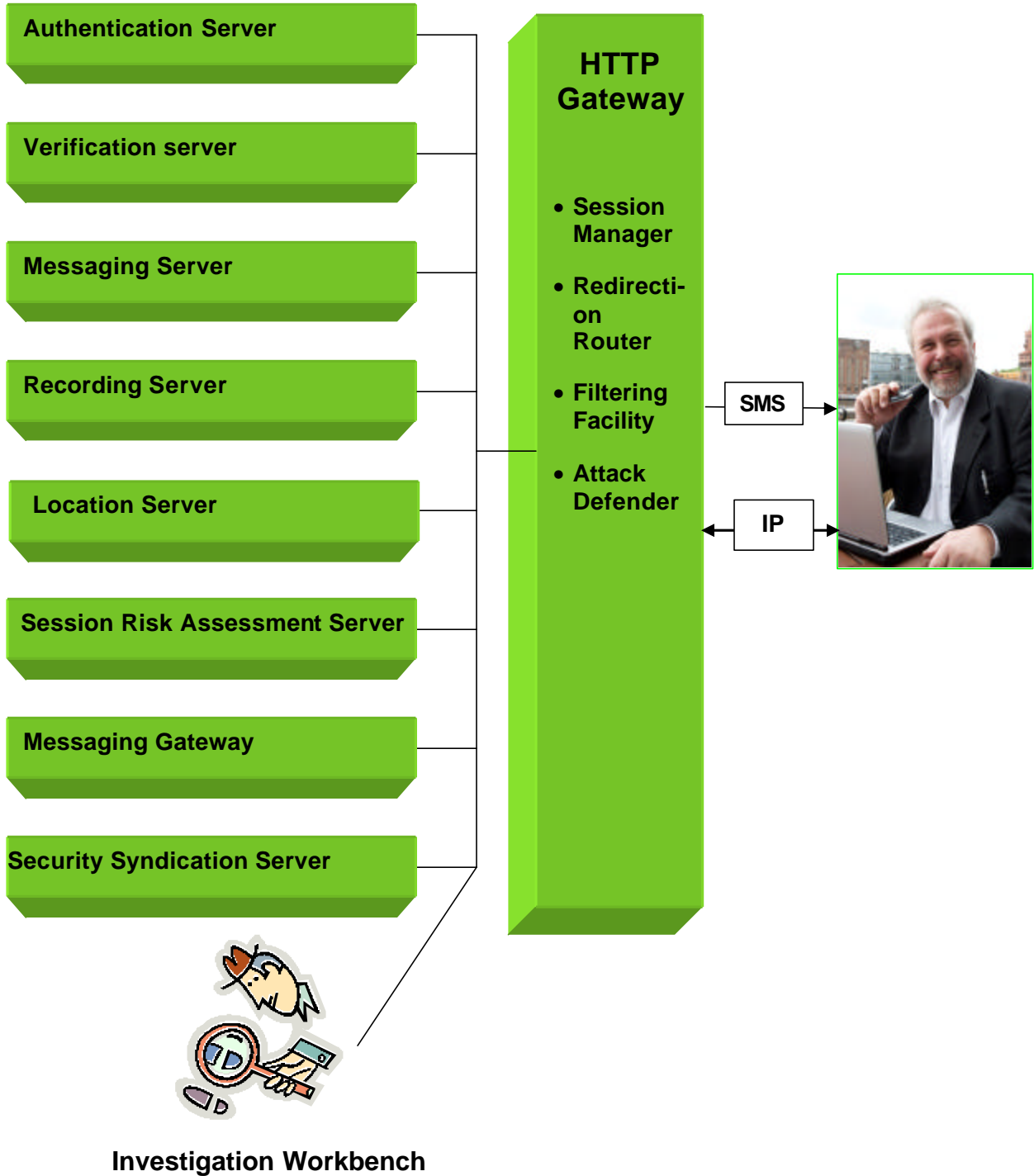
- Regional Syndication
- Web Site Syndication

- Line of Business Syndication
- Affiliated companies Syndication
- Branch Offices Syndication

IDentiWall Investigation Workbench

- Automated investigation triggered by behavioral irregularities
- Digital investigations against all IDentiWall's data sources
- Time line based event ordering

IDentiWall Schema



IDentiWall Functionality

IDentiWall enables active support for:

- Prevention of the results of rogue software attacks on customer computers.
- Prevention of the results of rogue software attacks on the bank we site.
- Assessment of risk levels of online customer activity and execution of appropriate policies.
- Integration of a variety of location data in evaluating the risk exposure due to online customer activities.
- Integration of online inputs of the customers.
- A digital investigation workbench and integration of automated investigative files.

IDentiWall Customer Benefits

The IDentiWall customer experience provides these benefits:

- Enhanced security everywhere in the world regardless of possible computer infection.
- Functional integration of the cellular telephone in the security procedures, without the need for software installation or a learning curve.
- Authentication at the site entrance followed by verification of the intent of customer online activities.
- Customer is informed whenever there is an unauthorized attempt to use their stolen user ID and password to access their account, even though the attempt is unsuccessful due to IDentiWall's protection.

IDentiWall Benefits for the Bank

IDentiWall provides these benefits for the banking network:

- IDentiWall operates outside the online banking application in a way that ***does not require any change in the source code*** of the application. This is extremely important, since it ensures that each stage of the transaction always reaches the web server only after the identity of the customer and the integrity of the transmitted information have been verified. This makes it possible to fight attackers before they have chance to commit the intended crime.

- Development and maintenance of the online banking application are isolated from the security function, preventing many problems during the lifecycle of the system.
- There is no need for customer training.
- There is no need to maintain token dispensers. Cellular telephone networks maintain customer telephones.
- Unlike the case for stolen token instruments, a customer whose cellular telephone is stolen will report it immediately to the cellular network operator, if only to prevent stolen calls. Customers usually delay reporting stolen token instruments to the "appropriate time."
- No need to install software in customer telephones or computers.
- IDentiWall handles special situations:
 - Customer is outside cellular network coverage.
 - Customer is abroad and has changed the SIM card to a local card.
 - A hacker may eavesdrop on the customer's cellphone and gets the One Time Password (OTP) sent to the customer.

Nonetheless, the hacker would be unable to use the OTP.
- All authentications, checking of intended operations, recording of activities, investigations and combating of attacks are handled in one place by IDentiWall.
- A digital workbench handles all online banking investigation functions.

IDentiWall multi-disciplinary support

IDentiWall is designed to actively combat the known types of attacks as well as those which will be devised in the future.

Special attention is given to support for multi-disciplinary fields, all of which are connected to the ability to provide a secure environment for online banking.

Whether the attack is directed at the online banking web site or the customer computer, if it succeeds, the result would be devastating for both the bank and the customer and put the existence of online banking itself in doubt. Therefore, IDentiWall is equipped with a variety of functions that serve as means to the end of enabling effective protection against the different types of attacks.

IDentiWall Authentication Server

There are many varied authentication methods, each of which is best suited for a given situation. Therefore, a special effort was made to support a variety of authentication systems with IDentiWall. As new authentication methods are developed, IDentiWall will support them as well.

Online banking is characterized by the need to handle large numbers of customers who are not necessarily used to using special security precautions. This dictates the need to emphasize ease of use and continuous availability of the authentication system.

IDentiWall Location Server

One of the parameters IDentiWall uses for estimating risk exposure for a transaction is a metric of location. In applications that allow data input from different remote locations, IDentiWall collects information about the location of the customer's computer, location of the cellular telephone handset, of the credit card and of the customer session in the bank web site and the route by which he or she arrived there.

IDentiWall uses sophisticated correlations to apply this information in estimating the effect of location metrics on risk exposure level.

IDentiWall Verification Server

The verification server ensures that the transaction that is executed is the one intended by the customer. The frequency of attacks that are based on misdirection of the intended actions of the e-banking customer grows daily, making the verification server a basic element in creating a secure online banking environment. The process of verifying customer intentions disables the capacity of the attackers to achieve their goals. It is executed over two separate communications networks, using a technique that prevents the attackers from carrying out their plan.

IDentiWall Recording Server

The effectiveness of a security system for online banking requires means of recording customer actions. These recordings have numerous uses in post-mortem investigations of security breaches, as part of the CRM, and in special cases, they may be used for real time surveillance of suspect customers or transactions.

IDentiWall also supports a playback facility that allows those responsible for security, monitoring and customer experience to perform an orderly reconstruction of customer actions.

IDentiWall Session Risk Assessment Server

Estimation of the risk caused by customer actions contributes the ability of IDentiWall to take into account different factors such as the risk involved in transactions, their location, past activities and the like, and to set the level of service accordingly. Thus for example, IDentiWall can block or delay a customer request originating from their fixed computer workstation if their wireless telephone handset is located in another country. Moreover, IDentiWall can take into account unusual activity such as transfer of funds to a new account that has no history, highlighting the need for a risk assessment system.

IDentiWall Messaging Server

Messages from the bank transmitted by IDentiWall to the customer can be routed through the Messaging Gateway. The function of the gateway is to ensure that the message actually reaches its intended destination even in extreme conditions when the SMS server is not providing the requisite quality of service. In that event, the Messaging Gateway will select a different SMS service vendor from the battery of available servers.

IDentiWall Investigation Workbench

The Investigation Workbench enables execution of digital investigations of issues related to IDentiWall and the knowledge bases connected to it. Information from the various sources undergoes correlative analyses, according to a requested sequence, for example, along the timeline, and is displayed to the investigator in clear and readable way.

The system also supports specification of automated investigations that are executed whenever a defined type of incident takes place. IDentiWall automatically registers the results of the investigation in a digital investigation file and sends an alert with a link to the file to the appropriate investigator.

IDentiWall Security Syndication Server

IDentiWall is designed to cooperate with other IDentiWall systems through the Syndication server. Cooperation in a syndicate means that whenever IDentiWall senses that it is the under massive cyber attack, it informs the syndicate of which it is a member.

In turn, the syndicate checks the policies it must execute upon receipt of the notification, and activates them.

Examples of this functionality can include:

- Sending alerts to other syndicate members to raise the security level by prohibiting certain activities on their protected web sites.
- Total shutdown of all online banking web sites if more than one bank is under massive attack.

Conclusion

The IDentiWall Secure eBanking platform is the ultimate solution for securing financial web sites.

IDentiWall continues to develop as new threats appear, based on the direct experience of some of the world's banking giants, ensuring that the platform will remain at the cutting edge of security services in the future.

Organizations that want to protect their web sites and their customers against every known type of attack will find an ideal solution in IDentiWall.