

Volume

1

SENTRYCOM LTD.

MARCOM

VoiceProof® Online- Secure Transactions Solution

MARCOM

VoiceProof® Online – Secure Transactions Solution



POB 56263
Haifa, 34989, Israel
Phone (972) 4-8342392
Fax (972) 3-7255867
Email : info@sentry-com.net
Web site : www.sentry-com.net

Table of Contents

THE NEED FOR TRANSACTION VERIFICATION.	1
VOICEPROOF® ONLINE - TECHNOLOGY.	3
OUT-OF-BAND (OOB) AUTHENTICATION.....	5
LIVE VOICE BIOMETRICS.....	6
ADVANCED ELECTRONIC SIGNATURE.	6
<i>Legal:</i>	6
<i>Technological:</i>	7
TRANSACTION VERIFICATION	8
NON-REPUDIATION.	10
CONCLUSION	11

The need for Transaction Verification.

The increased sophistication in malware attacks requires Enterprises doing online business to incorporate transaction verification.

The volume of E-Commerce transactions was estimated by IDC as \$0.75 trillions for B2C and \$3.4 trillions for B2B.

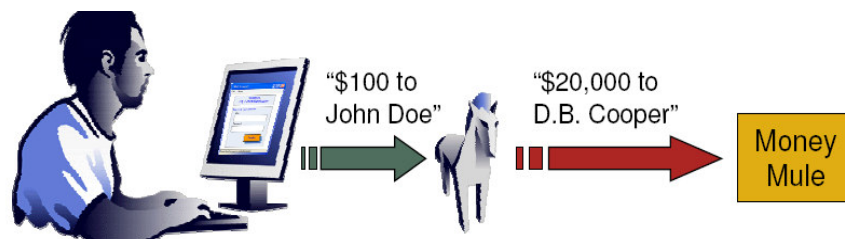
These huge numbers look to be very attractive to Crime world as well. “More money is now being made from cyber crime than the billions that come from drug trafficking”, AT&T's Chief Security Officer Edward Amoroso has told a US Senate Commerce Committee.

The increase in man-in-the-middle and Trojan attacks is further evidenced by the increased demand for malware on the black market. It is such a hot commodity that malware developers even offer upgrade packages that include service level agreements and technical support to buyers in the fraudster underground (source: RSA).

Man-in-the-Browser (MITB) is a latest form of security attack in which a software, typically Trojan malware, interjects itself between the user and the browser.

Such a program is capable of modifying the data between the user and the browser's security mechanism. MITB has no user observable symptoms: from user's point of view the web transaction is taking place normally. MITB can bypass authentication, modify web sessions at will and initiate fraudulent transactions.

In January 2008 SilentBanker Trojan targeted over 400 Banks worldwide including USA, France, Spain, Ireland, UK, Turkey, Brazil and others:



"I'd have to say it is one of the most sophisticated we have seen. What makes it more dangerous is it seems to be staffed by professional software developers," said Al Huger, vice-president for security response and security services at Symantec.

"They are writing this and maintaining it just like they would a piece of software you might buy. There is a lot of money on the line for them. It is certainly organized."

This brings inevitable conclusion that :

“Organizations that do business online should re-evaluate their solution road maps and incorporate transaction verification as a core component of their overall security strategy.”, Forrester, 2007.

Banks responded to this threat by call-back customers to verify transaction. In return fraudsters replied by penetrating phone channel:

Sometimes fraudsters will hack into a bank account and change the customer's contact phone number. Then, when a suspicious transaction posts to the account, the bank will call the fraudster instead of the customer.

In another scam, criminals activate automatic call-forwarding features to essentially takeover their victim's telephone lines for a period of time.

In any case – phone channel is susceptible for eavesdropping and is not regarded to be secure. US NIST labels such solutions as lowest level 1 (out of 4).

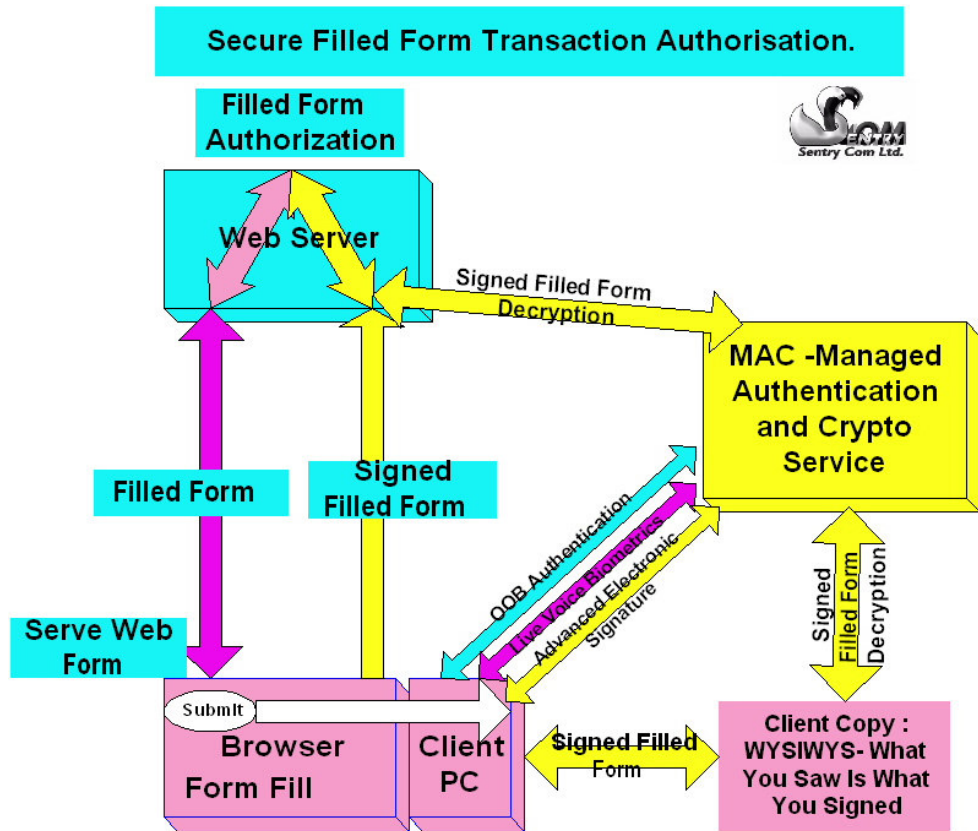
VoiceProof® Online - Technology.

Online Transactions involve processing of Web-forms. Transaction Verification involves Web-form signer and content authenticity verification.

Online Transactions are delivered by serving Web-Forms. This application involves Web-server and browser. The user fills the form, presses submit and “believes” in WYSIWYG - **What You See Is What You Get**- i.e. a system in which content displayed during editing appears identical to the final output, i.e. transaction. Man-in-the-Browser (MITB) is an attack on WYSIWYG and desired solution must protect the user from this threat. From other side Web site suffers from lack of confidence, about the signer’s identity as vividly shown below:



The VoiceProof® Online solution is described in the following Figure :



The components of the solution are as following:

User's side: Browser, such as MS Internet Explorer and SentryCom's VoiceProof® and VoiceShield® thin software installs.

Web site: Web server such as MS Internet Information Server (IIS) with addition of SentryCom Web extension. Web form HTML served by IIS includes SentryCom's JavaScript.

Web site Transaction Authorization station: SentryCom's VoiceProof® thin software install.

MACS – Managed Authentication & Crypto Service from SentryCom – Software-as-a-Service Internet Platform.

User fills web-form served by web server and presses submit for transaction. On submit – transaction “WYSIWYS” – What You Saw Is What You Signed is redirected to MAC for immediate processing.

MAC processing includes three inter-connected channels:

- Out-of-band (OOB) authentication
- Live Voice Biometrics
- Advanced Electronic Signature.

Out-of-band (OOB) authentication.

SilentBanker Trojan attack shows that hardware token One-Time-Password authentication do not provide an adequate answer to evolving security threats. Different paradigm, such as Out-of-band authentication should be utilized.

OOB Authentication requires that separate information channels be used for authentication and access. In the "Hype Cycle for Information Security", published in 2007-Out-of-Band Authentication technology is regarded by Gartner, Inc. as early mainstream.

Since access information channel is considered to be compromised by attacker (Man-in-the-Middle or Man-in-the-Browser)- it is believed that authentication information channel is secure. But is it the case? Many OOB schemes use telephony as authentication information channel. Since telephony is susceptible for eavesdropping – it cannot be considered as secure channel. These solution do not qualify above basic level 1 of US NIST requirements for open e-networks.

VoiceShield® and VoiceProof® software utilize OOB authentication using secure encrypted client-server authentication information channel. VoiceShield® and VoiceProof® exceeds US NIST Level 4 open network e-authentication requirements. For in depth discussion- please refer to to [NIST level 4 and beyond](#)¹.

The authentication strength is scalable with VoiceProof® from 2-factor to 3 factor.

2-factor authentication uses PC_ID and PIN , while 3-factor authentication adds Live Voice Biometrics. VoiceProof® Online uses 3-factor authentication by default.

It was emphasized by Gartner, that : "A Man-in-the-Browser (MiTB) attack can be programmed to corrupt a transaction 'in-flight' and prior to PKI encryption/transmission to the Bank. This means that (software) Digital Certificates can no longer be regarded as a form of non-repudiation since they are now vulnerable to Man-in-the-Browser attacks."

¹ <http://sentry-com.net/blog/2009/01/11/is-nist-level4-authentication-sufficient-for-critical-transaction/>

Live Voice Biometrics.

Biometrics may be defined as methods for uniquely recognizing humans based upon one or more intrinsic physiological or behavioral traits.

Voice is the non- intrusive, ubiquitous and economically feasible biometrics: it score highest in user acceptance surveys, can be applied on every PC and on every phone and does not require additional dedicated hardware.

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other physiological biometric source has been compromised it is compromised for life, because users can never change their fingerprints. The problem is effectively limited to cases where the scanned “live” biometric data is hacked.

SentryCom has [demonstrated](#)² its Live Voice Biometrics to have unique resistance to tape-record-and-playback attack. SentryCom extensively [tested and validated](#)³ its Live Voice Biometrics in Controlled Field Tests.

The usage of Live Voice Biometrics in the context of Transaction Verification precludes any possibility of remote malware attack.

Advanced Electronic Signature.

Legal:

An electronic signature is any legally recognized electronic means that indicates that a person adopts the contents of an electronic message. In many countries, including the United States, the European Union and Australia, electronic signatures (when recognized under the law of each jurisdiction) have the same legal consequences as the more traditional forms of executing of documents.

“DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures”

says that ‘advanced electronic signature’ means an electronic signature which meets the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using means that the signatory can maintain under his sole control; and

² <http://www.sentry-com.net/VoiceBiometrics.html>

³ http://www.sentry-com.net/files/SentryCom_VoiceShield_Functional_Test.pdf

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The same document also says that ‘certificate’ means an electronic attestation, which links signature-verification data to a person and confirms the identity of that person. It also says that ‘certification-service-provider’ means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

From legal standing CSP (certification-service-provider) may issue certificates for any internal application. In addition the Directive says that Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider,
- or not created by a secure signature-creation device.

This definition creates a ladder for creation of scalable solution where CSP may provide certificates for internal purposes and may link to Accredited CSP (such as Governments) for generation of qualified certificates.

SentryCom MAC serves as CSP and may be linked to Accredited CSP’s for generation of qualified certificates.

Technological:

VoiceProof® Online utilizes state-of-the-art Crypto technology complying with legal requirements:

- RSA public-key signature algorithm
 - 1,024 bits key length

Transaction Verification.

Transaction Verification is a two-fold process of signer and content authenticity verification.

User fills web-form transaction and submits to the Web site for authorization.

On submit the user is prompted for PIN and challenged to repeat random-digit combinations. The authentication will take less than 20 sec to complete and on success – the signed transaction together with filled web-form transaction will arrive to the Web site. If signed transaction matches filled web-form transaction – it will be authorized.

The authorization process is shown below as a following example:

Filled form entry calls for transaction from Steve Jones to Mike Willis, with amount of \$4500. This transaction is uniquely described by tracking number #877623 and time-stamp of April 3 , 2009 , 09_13_38 Universal Time (UTC) . This needs to be authorized.

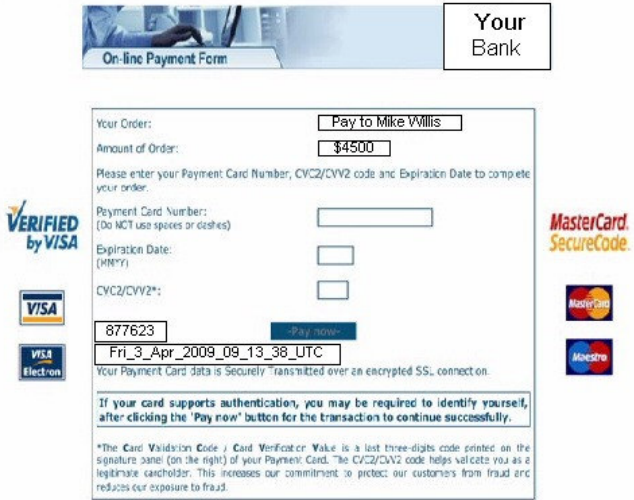
Relevant signed filled form file is easily retrieved . Clicking on file displays VoiceProof® certificate and transaction form as shown below:

Transaction Authorisation by E-Commerce Provider.

Tracking # for locating in signed transactions folder.

pending	Tracking #	Date/Time (UTC)	Transfer from	Transfer to	Amount (\$)	Authorize
	877623	Fri_3_Apr_2009_09_13_38_UTC	Steve Jones	Mike Willis	\$4500	OK
	620886	Fri_3_Apr_2009_09_14_18_UTC	Mary Smith	John Mitchell	\$3000	
	512996	Fri_3_Apr_2009_09_15_33_UTC	Jim Porter	Ann Carter	\$6000	

signed transactions folder \SentryCom_877623_Fri_3_Apr_2009_09_13_38_UTC.scz



The authorization consists of two parts:

1. As VoiceProof Certificate shows: the transaction (electronic message) was indeed digitally signed by Steve Jones as claimed in the form. Steve Jones was authenticated by MAC server on April 2 , 2009 at 09_03_35 Universal Time.
2. Original transaction, bearing tracking number and time-stamp as appeared in the form, requires payment of \$4500 to Mike Willis.
3. This transaction is therefore authorized.

Non-repudiation.

Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract.

In reference to digital security, *non-repudiation* means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

The transaction receipt is saved on user's desktop for two purposes:

1. Immediate verification (just to be on the safe side).
2. Future audit in case of dispute.

The transaction receipt is identical to the one received by the web-site:

Look at your desktop and verify integrity of your transaction.
Your receipt includes 2 parts :
transaction certificate from SentryCom (to the left).
and transaction just completed (to the right):



The signed transactions are time-stamped twice – at the time of submission and at the time of authentication. The signed transactions carry two unique identifiers: one for submission and one for authentication.

This allows auditing transaction independently vs. MAC and vs. web site.

Conclusion.

Existence of zero-day attacks on Online Banking such as SilentBanker calls for Transaction Verification. VoiceProof® Online Software-as-a-Service provides secure, convenient and cost-effective solution for the problem of Identity Theft.

The same solution is applicable for a number of important Internet sectors: For example:

- Need to ensure the person's authenticity in cases where Credit Card is used fraudulently,
- Need to ensure online prescription integrity in E-Healthcare applications,
- Need to ensure that e-Gov form has not been altered by saboteurs,
- Need to ensure that business-to-business transaction has not been altered within the Extended Enterprise.