



Identity Theft is knocking our doors.

This paper will focus on technological aspects of Identity Theft and possible solution for its prevention.

US regulator, FFIEC, requires from Financial Institutions, to perform risk audits and take necessary steps for Fraud prevention. FFIEC do not take a stand regarding the Best-of-Breed technological solution as long as the Institution knows how to explain the Auditor how the chosen solution answers the challenges posed by current and future threats.

It appears that the pace of threats development is increasing beyond the imagination. If in 2005 the main threat was Phishing , then in 2006 we are getting more and more sophisticated threats such as Man-in-the-middle (MITM) and Trojan.

In April 2005, a paper was published in ACM magazine, written by Bruce Schneier , US expert on IT security . In this paper Mr. Schneier forecasted that Financial Institutions will spend millions on technological solutions that were developed to deal with Phishing and that are incapable of dealing with MITM and Trojans.

About at the same time it was published that ETRADE is about to become a pioneer in providing its clients with OTP Token for 2-factor authentication. Analysts from Forrester immediately welcomed this move intended to answer the phishing threat. But 'history clock' was ticking fast .In October 2006 ETRADE has announced that Trojan attack caused huge losses estimated as high as \$22 millions.. Schneier's forecast was accurate. What was surprising – how fast it occurred.

If we add to this - recent Man-in-the-middle attack on Citibank customers – we can safely conclude, “the future is here”.

We can “short-list:” few possible solutions to the problem:

- The fastest and cheapest solution for financial institutions is so-called “stronger authentication”, where password is strengthened with knowledge-based authentication. This method is based on Q&A based on text or pictures, and requires that user enrolls into the system with some known personal choices. The major problem with this approach –users do not remember things used rarely (as they forget passwords). This approach will also fail when MITM occurs.
- More expensive and more complicated solution is so-called “strong authentication” , where users possess some hardware devices such as smart card or biometrics readers.. Although these solutions solve the problem of “forgetting things”, but they do fail the goal of resisting active attacks, as predicted by Bruce Schneier . Mr. Schneier emphasizes the importance of per transaction authentication. On his opinion : safe login is not sufficient to ensure safe transaction.

We will take now more closer look on implementations of stronger and strong authentication:



Stronger authentication is intended to strengthen security with minimal interference to user's experience . Such approach includes two prime components: TAD – Transaction Anomaly Detection and PC agent software.

- TAD is intended to find suspicious transaction and
- PC agent software is intended for 2-factor authentication

This approach brings along a number of problems:

- TAD is intended to detect unusual behavior, but “unusual” and fraud are not the same thing. Buying cheap stock is not “unusual “ but was fraudulent in the case of ETRADE. The desire not to interfere with day-to-day ”usual” activity leaves too many doors open...
- If one desires to authenticate each and every transaction using manual calls to the customer – this solution is impossible in real-time (i.e. stocks trading) and definitely not scalable to serve millions of transactions.
- The PC-limited agent do not have solution for AnyPC roaming
- There is no solution for Man-in-the-middle
- There is no solution for Call Centers

OTP Token based Strong Authentication is capable of solving the roaming problem, but on expense of user's convenience (carrying multiple-token “ necklace “). This solution is incapable of dealing with Man-in-the –middle and Trojan as shown in the ETRADE incident.

Strong authentication using Out-of-band verification is an approach capable of solving Man-in-the-middle attack by creating triangle including Client-Server-Application sessions . The attacker cannot be in two places (Client-Application and Client-Server) at once.

The usage of mobile phone for out-of-band and integration “Back office” with Server and Application enables to overcome MITM. The usage of Voice Biometrics is a natural extension of this approach. The back up of mobile phone with desktop phone and PC-based microphone allows using the same technology any-where, any-place, anytime over Internet and Call Centers.

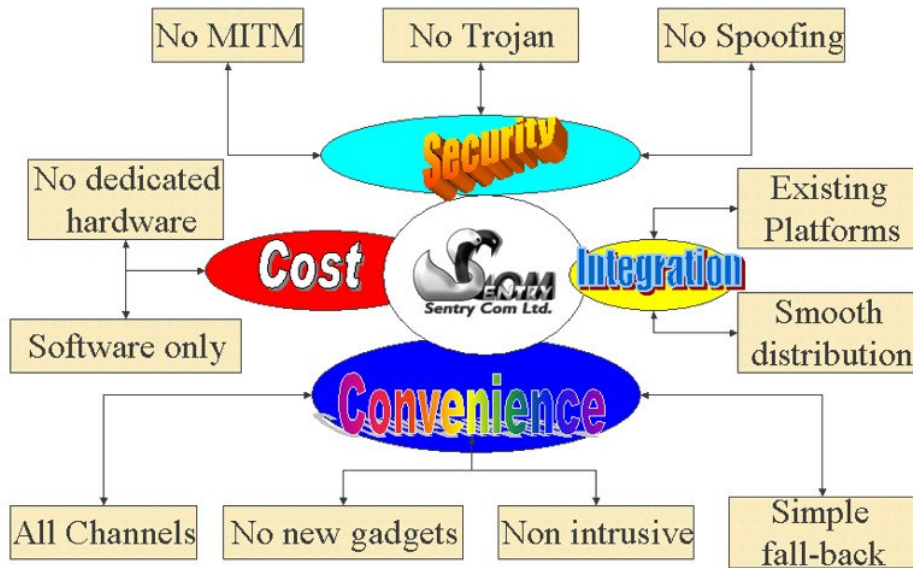
It is important to quote the Forrester Analysts criteria for successful deployment of large-scale consumer facing solutions:

- Let customers use it anywhere
- Be easy for customers to us
- Be cost effective
- Provide appropriate levels of security
- Be easily manageable
- Work across different channels of interaction



The following is SentryCom approach to the problem in accordance with Forrester's aforementioned criteria:

Our Value Proposition :



Scalable to secure any transaction anywhere anytime anyplace

For more information, please contact us at SentryCom.

Dr. Eli Talmor
 CEO
 SentryCom Ltd.
 The Authentic Voice of Security
www.sentry-com.co.il
 tel : 972-4-8342392

