eAuthentication today, Arnnei Speiser, Mega AS Consulting Ltd, July 2006

What is at risk – or why should we….

This article is not about statistics and theories; it is about facts and real problems. If you need the statistics you can easily Google them.

Fact, most Internet users will look for a commodity on the Internet and will compare prices before making a purchase.

Fact, most businesses have a web site that publishes their services. Any business that wants to market itself sees a web site as a necessity.

Fact, the biggest problem the Internet faces today – is security.

Today, Internet users are aware of Spyware, Trojan horses and Phishing. As the Internet becomes a vehicle for eCommerce and eBanking (etc), it attracts more and more Hackers as the potential gains are growing. On one hand is the future of commerce and services and on the other grows the Internet "terrorism" that is endangering it all.

Within 2-3 years, a web site that will not protect its customers from Identity Stealing, will not have registered clients. Simply because – there will be similar web services that WILL offer such protection.

The Virtual World

To understand what is needed, we first need to understand this new and wonderful world of Internet. In other words – the Virtual World.

The virtual world is a place where there are no real persons. Every "identity" is virtual. A real person may have a number of identities, which he may use at different occasions, and different "corners" of the Internet.

Some of these identities have real properties and has to be verified by a service provider, for example when you are using an eBanking system, you are usually required to get your User ID and Password directly from the Bank. You can't just register to their services. In other occasions, like when purchasing, you need to provide "real" information like your real credit card details etc.

Mega AS Consulting Ltd.
P.O.Box 55227, Mission Bay, Auckland, New Zealand
Tel: +64-9-448-1244
E-mail: sales@megaas.co.nz support@megaas.co.nz WWW: http://www.megaas.co.nz /

But, all these identities are susceptible to Identity Stealing – whether a service provider provides them or they are generated when the identity is registered online to a service (forum, site etc).

Nobody wants his password stolen and somebody else to get access to their information on the web. It does not matter if the information is harmful, if money can be lost or if it is a simple networking forum with consequences information. Nobody likes to come home and find somebody else was there – even if that somebody did not take anything physical or damaged the home.

What is needed

Simple. There is a need for an Authentication solution that while it does not require the Identity to expose its real self, it will prevent others from stealing the identity. The solution has to be easily deployed. How would you Authenticate a casual identity from China, that registered at your site for your services.

Such a solution, if it is affordable, will replace the existing fixed User ID and Password that are used today by most Internet Sites.

Since most SMEs are using Hosting companies to host their web sites, and can't install an Authentication package at their site as part of the deal, these companies will need third party Authentication services, thus – eAuthentication, in order to get the Login approved.

EAuthentication service is similar to Credit Card verification in eCommerce sites. The purchasing customer enters his credit card details, which are then sent to a third party company to verify and transact. The customers receive an acknowledgement or error message.

The same is with eAuthentication service. When the customer opens the web site Login page, he enters his Authentication details such as User Id and Password. The details are then sent to a third party that eAuthenticates the details. The user enters the site or gets a message.

Mega AS Consulting Ltd.
P.O.Box 55227, Mission Bay, Auckland, New Zealand
Tel: +64-9-448-1244
E-mail: sales@megaas.co.nz support@megaas.co.nz WWW: http://www.megaas.co.nz /

The old stuff

The Authentication business started with Networks long before Internet was available. After the Networks came the Dial-Up services and then last came the Internet.

There are 2 types of Authentication technologies. Those that are biotechnology and authenticate a person by parts of his body, and those that are not biotechnologies.

The current status of biotechnologies is that they are too costly, have insufficient authentication success rate and they require the real person identity which means that they are not suitable as a solution for the Internet environment.

On the other hand, the industry recognized the Two Factor Authentication (TFA) methodology and One Time Password (OTP) as the best solution for the Identity Stealing problem.

In general, the idea is that the customer doesn't have to remember his password anymore (and thus he would not use the same password for over and over again…). He gets a token that generates a password for him for the particular server every time he needs to access that server. These tokens are proprietary hardware that costs between 30 to 100 dollars per person – per server or account.
When the token is proprietary hardware, it means that the token has to be delivered physically to the identity thus exposing the true person behind it. With that and with the costs associated with the token and its deployment, these old proprietary token are not suitable as an Internet solution. They were designed as an enterprise solution for internal security.

During the last few years, there have been a number of tests and products trying to achieve security by using an SMS mechanism. But, as RSA, the biggest security company in the industry, discovered, the SMS mechanism was insecure, unpredicted and had a huge hidden cost. As a result, RSA withdrew from marketing the SMS based tool that they have developed.

Best solution

So is there no solution? No, there is one. A TFA OTP solution that was designed for eAuthentication and Internet Services.

Mega AS Consulting Ltd.
P.O.Box 55227, Mission Bay, Auckland, New Zealand
Tel: +64-9-448-1244
E-mail: sales@megaas.co.nz support@megaas.co.nz WWW: http://www.megaas.co.nz /

The Cellular Authentication Token (CAT) is an authentication product that has all the advantages:

- It is as secured as the old proprietary hardware tokens
- It is deployed over the Internet and does not require to know the personal details. Even your customers from China can download it.
- It is free for the customer (**no** 30 to 100 dollars per person)
- It can manage any number of sites with the same token (**no** 30 to 100 dollars per site)
- You can have an in-house installation (one time charge) or as an eAuthentication service (monthly charges)
- Easy to implement
- Using advanced Cellular technology

The CAT is software token. The customer can download it (for free) to his enabled Cellular like a cellular game or ring tone. Once downloaded, he can activate his site identity at the CAT. Using the Cellular means that the customer does not have to carry additional proprietary hardware and he is familiar with the Cellular menus.

The CAT then shows him the OTP (one Time Password) for his Login on the Cellular screen (no need for SMS or communication). The customer can add any number of identities and sites to his CAT.

Once the customer wants to enter a web site that is CAT secured, he opens the web site Login page. At the page he is requested to enter his Identity code (User ID) and his OTP (One Time Password). The customer looks at the Cellular screen for the CAT generated OTP and enters it into the Login page.

The server will either verify the User ID/OTP locally with CAT Authentication Server, or it will request eAuthentication from a third party server.

More details

Finding details today is simple, Google for: Cellular Authentication Token or for Mega AS Consulting Ltd – the manufacturer, or simply visit the site: www.megaas.co.nz

Mega AS Consulting Ltd.
P.O.Box 55227, Mission Bay, Auckland, New Zealand
Tel: +64-9-448-1244
E-mail: sales@megaas.co.nz support@megaas.co.nz WWW: http://www.megaas.co.nz /