

IBM Tivoli Security using Two-Factor Authentication against 'PHISHING'

IBM Tivoli Security

IBM Tivoli Security provides an integrated family of security products that provide a comprehensive and scalable solution for centralized Identity and Security management.

IBM Tivoli Security is widely used within Financial Institutions, including Internet- and telephone banking applications.

Still, if only static passwords are used, the customers are still vulnerable to 'Phishing'.

Phishing

(FISH.ing) pp. Creating a replica of an existing Web page to fool a User into submitting personal, financial, or password data. —adj. —phisher n.

Phishing is the term coined by hackers who imitate legitimate companies in e-mails to entice people to share passwords or credit-card numbers.

The term Phishing comes from the fact that Internet scammers are using increasingly sophisticated lures as they "fish" for Users' financial information and password data.

Recurring patterns

The Fraudster targets Static Passwords.

Static Passwords are widely used for all kinds of purposes.

Static Passwords can be easily re-used by Fraudster.

Typical Phishing scheme:

Email is broadcast from a fake server address, pretending to be the real company or Financial Institution, containing an invitation to verify or to enter Username password

The fake website looks like the real one from the Financial Institution.

A Microsoft Internet Explorer programming code bug is used to display the address of the real website, masking the fake website address.

This is based upon some characters in the 'url', which are masking the real address of the website

Phishing Fraud Scheme

The goal is to obtain the Users' static password by sending out massive amount of emails.

On the fake, but very real looking and feeling website, the Username/Password pair is collected.

In most cases, the gathered pairs of Username/Password can be processed in batch by the Fraudster any time afterwards. This is a batch process, which makes it more manageable, as the Fraudster has not to wait for Username/Password pairs to arrive.

Strong authentication solution against Phishing: Digipass Family

A Digipass is a token solution.

Digipass generates One Time Passwords upon request of the owner of the token, by entering PIN code on the token or pressing a button on the token.

Digipass contains internal real-time clock, which allows for Time-Based Passwords.

It is virtually impossible to misuse VASCO's solution:

The generated Passwords are not only for One-Time use only, but also Time-Based Passwords. Replaying of passwords is controlled by server verification software.

Being Time-Based, forces the Fraudster to operate in (almost) real time. Fraudster must sit in between Customer and financial institution for communication reasons between both parties.

Verification of passwords in real time:

This reduces the time for the Fraudster to act, due to expiration of the Password.

One Time Passwords:

Steal once, use one time only (and fast)

Batch processing of Username/Passwords is no longer possible for Fraudster.

This puts a time pressure on Fraudster.

Moreover instead of waiting for many passwords to be collected, the Fraudster now has to be present at the moment the Username/Password is revealed, as he has to use this pair immediately.

IBM Tivoli and Two-Factor Authentication

IBM Tivoli Access Manager for e-business is the leading platform for access control to web-based applications. TAM supports a number of authentication mechanisms out-of-the-box and provides an interface for other types, called CDAS (Cross Domain Authentication Service).

Based on years of experience in large Access Manager projects, SecurIT has developed its revolutionary C-Man™ concept, library classes and a methodology to speed-up the provision of such CDAS implementations according to the highest quality standards.

SecurIT partners with IBM and VASCO to provide an interface between the products, based on this C-Man concept, in order to allow Digipass-based authentication to access enterprise applications.

The solution is available in 2 flavours, each aiming at different customer requirements, and presently in production use at large organisations.

Digipass Tokens – how do they work?

Every User has a personalized token.

Upon request the User can generate a Time Based One Time Password.

The User enters the One Time Password into the Password field, next to the Username field, as requested by the Server.

Just like he always has done with Username/Password.

The software on the Server uses the Username to get data from the Customer Data Base and the real time clock of the System to recalculate the One Time Password for this User.

The software verifies both Passwords to authenticate the User.

Token types:

1) With PIN:

Having a numeric keypad.

Note: The PIN has to be sent by mailer in order to let the User use the Digipass. Another possibility is that the user needs to put in a PIN during first time usage.

Of course the PIN may be changed by User or can be forced to change during first time use.

2) Without PIN:

Easier to use and deploy

No PIN mailer to be sent (see argument above)

Less functionalities than with PIN, because no numeric keypad

Digipass tokens have several function possibilities:

- 1) Time-Based One Time Passwords
- 2) Time-Based Challenge/Response
- 3) Time-Based Signature function
- 4) Time-Based Host authentication

1) Time Based One Time Passwords

One time use only

One Time Passwords are time based

Typically 36 seconds before the next one is generated

The Server has a wider window than 36 seconds to accept the Password

The combination of unknown secrets, verification procedure and real time clock puts the Fraudster under time pressure. A wider time-window is decreasing the security. The length of the password is increasing the security.

2) Time Based Challenge/Response

First we have to explain the procedure of Challenge/Response:

- Users signs on with User ID
- Server/System to present Challenge to User
- User enters the Challenge into Digipass
- Digipass generates the Response
- User enters Response into System
- User gets authenticated by the System

This is a very complex process for Fraudster:

The Fraudster has to use Username immediately to get the appropriate current Challenge from the Server. So he needs to be connected already to the Server/Website.

Once he receives the Challenge, he needs to present the Challenge to the Customer.

The Customer can then generate a Response to Challenge using his Digipass. After receiving Response from the Customer, the Fraudster could try to make his fraudulent move, as the Response is again time based.

Not only the Fraudster has now to wait for a User to send Username, but the Fraudster now also needs to interact in the communication between User and Financial Institution passing the Challenge and getting the Response.

3) Signature function

A Financial Institution can request a Signature from the Customer for each transaction or important transaction.

This Signature contains encrypted data from the transaction:

Which can be Account number, Receiving Account Number, Amount, Date.

Moreover this Signature is again Time Based.

The transaction data cannot be altered, as the Signature needs to change too.

In this case there is no opportunity for Fraudster at all.

4) Host/website authentication

This solution allows the User to authenticate his Bank, in order to verify the authenticity of the website.

How:

A function on the Digipass allows for this.

Internally the Digipass generates a long Time Based One Time Password.

Only first part is shown to User on the display of the Digipass.

The User enters this part into the website of the Bank.

Bank receives Username & first part Password.

The system of the Bank calculates latter part of the Password and sends it to User.

The User enters latter part of the Password into his Digipass for verification.

If correct the Digipass will let know the User.

CONCLUSION

By simply adding the C-MAN concept to your existing Tivoli Access Manager and distributing any of the Digipass tokens to your clients, Phishing becomes a thing of the past.

Interested ?

Please visit <http://www.securit.biz/objects/Digipass4TAM.pdf> to find out more this solution has to offer.

SecureIT

SecurIT was established in Belgium in 1999 in order to focus on the application-level security requirements of large enterprises, and has rapidly gained recognition as experts in the design and implementation of a mission-critical security infrastructure. SecurIT is a Premier IBM Business Partner for the Tivoli Security product range and has also a partnership with ValiCert Inc. from Mountain View, California in the area of security proof management and transactional integrity.

www.securit.biz

VASCO Data Security – The Authentication Company

VASCO designs, develops, markets and supports patented strong user authentication products for e-business and e-commerce. VASCO's strong user authentication software is delivered via its Digipass security products, small "calculator" hardware devices carried by an end user, or in a software format on mobile phones, other portable devices, and PCs. For user access control, VASCO's VACMAN products guarantee that only designated Digipass users get access to the application. VASCO's target markets are the applications and their several hundred million users that utilize fixed passwords as security. VASCO's time-based system generates a "one-time" password that changes with every use, and is virtually impossible to hack, or break. With 10 million Digipass products sold and ordered, VASCO has established itself as a world-leader for strong user authentication with over 250 international financial institutions, approximately 1400 blue-chip corporations, and governments representing more than 60 countries.

www.vasco.com