Title : In action – Taking on the security challenge

Source : Security Advisor Middle East – Issue 15

Dated : January 2005

security
ADVISOR | MIDDLE EAST

ISSUE:15
JANUARY 2005

PUBLISHED BY:
CPI
CORPORATE PUBLISHING INTERNATIONAL
IDC

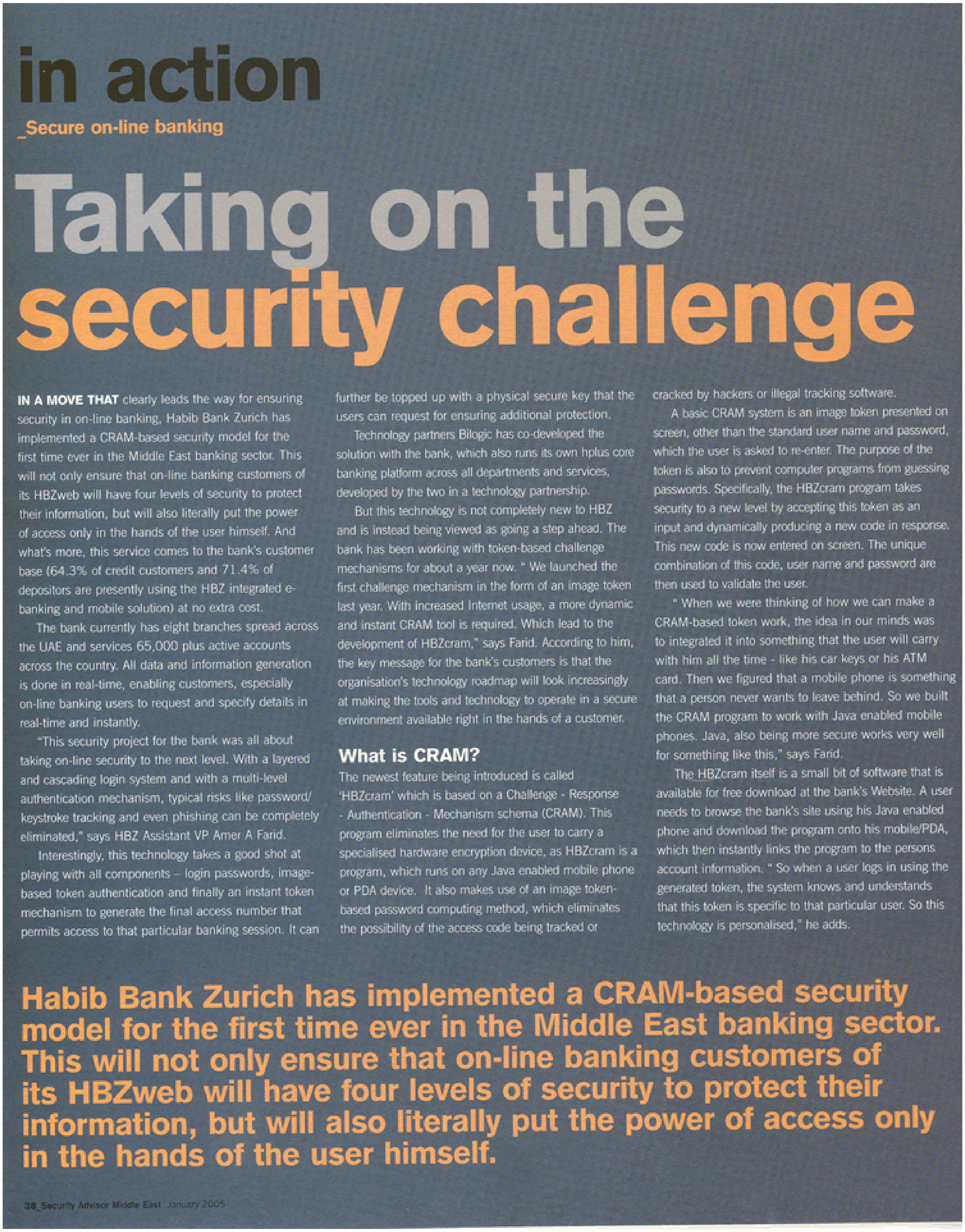
MAKING BUSINESS SENSE OF IT SECURITY

WWW.CPILIVE.NET

SPYWARE

Do you know who's watching you?

PLUS: SECURITY EVENT MANAGEMENT | CORPORATE BLOGGING | MEITSEC 2004 | CRAM SECURITY | DISASTER RECOVER



Taking on the security challenge

IN A MOVE THAT clearly leads the way for ensuring security in on-line banking, Habib Bank Zurich has implemented a CRAM-based security model for the first time ever in the Middle East banking sector. This will not only ensure that on-line banking customers of its HBZweb will have four levels of security to protect their information, but will also literally put the power of access only in the hands of the user himself. And what's more, this service comes to the bank's customer base (64.3% of credit customers and 71.4% of depositors are presently using the HBZ integrated e-banking and mobile solution) at no extra cost.

The bank currently has eight branches spread across the UAE and services 65,000 plus active accounts across the country. All data and information generation is done in real-time, enabling customers, especially on-line banking users to request and specify details in real-time and instantly.

"This security project for the bank was all about taking on-line security to the next level. With a layered and cascading login system and with a multi-level authentication mechanism, typical risks like password/ keystroke tracking and even phishing can be completely eliminated," says HBZ Assistant VP Amer A Farid.

Interestingly, this technology takes a good shot at playing with all components – login passwords, image-based token authentication and finally an instant token mechanism to generate the final access number that permits access to that particular banking session. It can further be topped up with a physical secure key that the users can request for ensuring additional protection.

Technology partners Bilogic has co-developed the solution with the bank, which also runs its own hplus core banking platform across all departments and services, developed by the two in a technology partnership.

But this technology is not completely new to HBZ and is instead being viewed as going a step ahead. The bank has been working with token-based challenge mechanisms for about a year now. " We launched the first challenge mechanism in the form of an image token last year. With increased Internet usage, a more dynamic and instant CRAM tool is required. Which lead to the development of HBZcram," says Farid. According to him, the key message for the bank's customers is that the organisation's technology roadmap will look increasingly at making the tools and technology to operate in a secure environment available right in the hands of a customer.

What is CRAM?

The newest feature being introduced is called 'HBZcram' which is based on a Challenge - Response - Authentication - Mechanism schema (CRAM). This program eliminates the need for the user to carry a specialised hardware encryption device, as HBZcram is a program, which runs on any Java enabled mobile phone or PDA device. It also makes use of an image token-based password computing method, which eliminates the possibility of the access code being tracked or cracked by hackers or illegal tracking software.

A basic CRAM system is an image token presented on screen, other than the standard user name and password, which the user is asked to re-enter. The purpose of the token is also to prevent computer programs from guessing passwords. Specifically, the HBZcram program takes security to a new level by accepting this token as an input and dynamically producing a new code in response. This new code is now entered on screen. The unique combination of this code, user name and password are then used to validate the user.

" When we were thinking of how we can make a CRAM-based token work, the idea in our minds was to integrated it into something that the user will carry with him all the time - like his car keys or his ATM card. Then we figured that a mobile phone is something that a person never wants to leave behind. So we built the CRAM program to work with Java enabled mobile phones. Java, also being more secure works very well for something like this," says Farid.

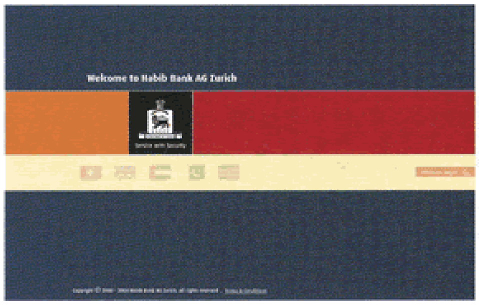
The HBZcram itself is a small bit of software that is available for free download at the bank's Website. A user needs to browse the bank's site using his Java enabled phone and download the program onto his mobile/PDA, which then instantly links the program to the persons account information. " So when a user logs in using the generated token, the system knows and understands that this token is specific to that particular user. So this technology is personalised," he adds.

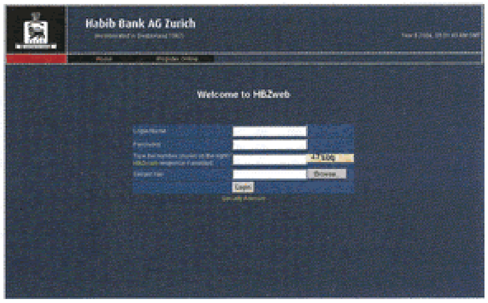
Habib Bank Zurich has implemented a CRAM-based security model for the first time ever in the Middle East banking sector. This will not only ensure that on-line banking customers of its HBZweb will have four levels of security to protect their information, but will also literally put the power of access only in the hands of the user himself.

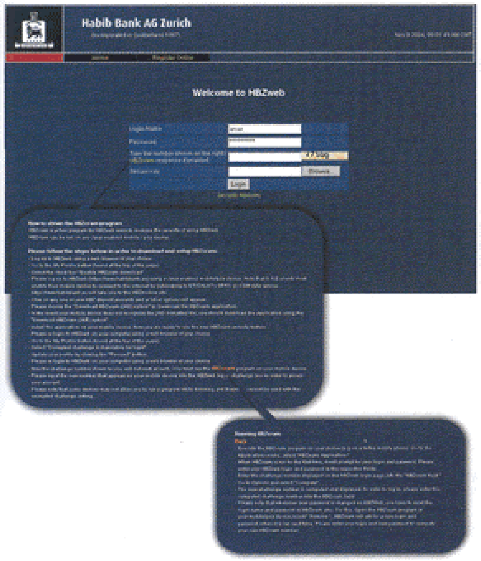
How does this work?

Level 1

First of all, this entire system puts together four levels of security and authentication/ validation. At the first stage, the user accesses his on-line banking site and inputs his regular login and password that is traditionally used to gain access.





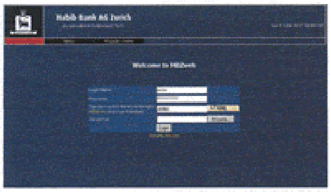


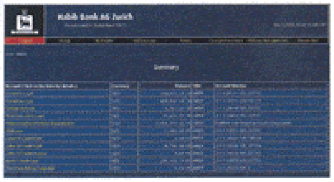
Level 2

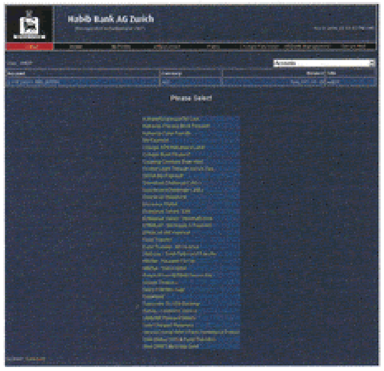
Once the level 1 is complete, the user now needs to use the image token, which appears on the login screen. This image token will give the user the number combination to enter into the HBZcram software on his mobile.

Level 3

The user now inputs the image token number into his HBZcram software and computes it. The software instantly scrambles the number and computes the combination and comes up with an instant password for the user. This password can be used to enable just that one session with the bank and is disabled if not used within a certain frame of time.







Level 4

User enters the session using this password and begins his banking session, on-line.

Level 5

Customers can request for an additional secure key that will work on top of all these levels. This offering is a hardware device (a CD or USB) which holds secure key numbers that are linked to account