Increasing fraud threatens to stall growth in internet banking

Fraud threatens to stall the growing popularity of mass market internet banking services, now increasingly regarded as a ‘must have’ for many bank customers. The problem banks are facing is how to introduce enhanced security measures to combat this threat without making their web-banking systems unusable for the customer.

Security solutions based on awkward and bulky authenticators have been rolled out by a number of banks, but are proving highly unpopular with customers. The mobility of today’s electronic banking users dictates a security solution that does not impede the ability to conduct their banking business from any location via the internet.

As the fraudster becomes ever more sophisticated, simple two-factor authentication is no longer sufficient to prevent ‘man in the browser’ trojan attacks combined with social engineering techniques. Fraud migrates to the point of greatest weakness and transaction integrity is now the critical issue rather than merely enhanced access control. Banks must act now to prevent a rapid growth in fraud that could destroy customer confidence in internet banking and permanently damage their brand.

Visual signing provides a simple portable solution

Cronto’s patent-pending VISUAL CRYPTOGRAM offers the ideal blend of enhanced strong security and simplicity of use for the customer. Visual signing of transactions removes the need for awkward authenticators and time consuming re-keying of challenge codes or transaction details.

Cronto visual signing works by generating an encrypted visual challenge to authenticate internet banking transactions. This challenge can be used to secure critical transactions, such as third party payment instructions, as well as at login to strengthen access control, preventing the threat of fraud.

Traditional challenge-based security solutions typically use numeric codes that need to be re-keyed by the customer into an external device. Cronto’s visual signing avoids this by utilising a unique visual challenge contained in a graphical cryptogram consisting of a mosaic of coloured dots displayed on the customer’s PC screen. Instead of typing challenge codes or payment details into a fiddly authenticator keyboard, the customer uses the camera in his mobile phone or a dedicated key-tag token to capture the cryptogram by photographing the screen. Cronto software downloaded into the customer’s phone or provided on the key-tag token is then used to authenticate the transaction. No re-keying is required.

Authentication is quick, simple and secure. No bulky and inconvenient authenticators are required. The customer is presented with critical transaction information, like payment details, on the screen of his phone or key-tag token to confirm that this information has not been tampered with. He is reassured that a fake criminal web site or trojan malware have not been used to alter his instruction. An authentication code is then generated and passed back to the bank’s server to complete the transaction.

“Cronto’s novel authentication solution provides a strong, efficient mechanism for safeguarding transactions against current and future threats”
Lyndon Lee, Head of ICT Security Research BT
By removing the need to re-key information and automatically confirming instruction details, the Cronto solution offers a far higher level of security than traditional external authenticator-based solutions. Criminals are aware that by using a ‘man in the browser’ attack and canning social engineering techniques they can potentially trick customers into entering the wrong information into their authenticators. Two-factor authentication is also prone to similar types of attack.

Cronto visual signing protects against ‘man in the browser’ and ‘phishing’ attacks and provides the strongest level of security for internet banking services without compromising the customer’s convenience to conduct his banking business anywhere he pleases.

Product Features

- **Unique patent pending visual cryptogram** – secure encrypted transaction authentication
- **True end-to-end security** – protects against both ‘man in the browser’ and ‘phishing’ attacks
- **Cronto client options**
  - Phone authenticator – using customer’s mobile phone
  - Desktop authenticator – using USB token
  - Dedicated authenticator – using camera key tag token
- **Support for majority of modern mobile phones** - requires only basic application access to the camera
- **Internet and mobile banking** – supports any browser-based solution
- **Server based encryption software** – generates unique visual cryptograms and authenticates response
- **Client software distribution** – automated download of client software to customer’s phone

Customer and Business Benefits

- **Customer convenience** – simple and easy to use, no re-keying using fiddly small buttons
- **Portable solution** – secure transactions anywhere, no bulky card readers or authenticators required
- **Low cost** – use customer’s mobile phone to authenticate transactions
- **Strong encryption** – unique visual cryptogram contains encrypted transaction details
- **Simple to deploy** – customer can download client software to his phone
- **Rapid integration** - no redesign required in bank server software

Technical Requirements

**Server platforms:** Java Runtime Environment 1.3.x and above or Microsoft .NET framework 2.0 and above, custom integration requirements are also supported.

**Mobile client platforms:** iPhone 2.1, J2ME with and access to the camera (JSR-138), Nokia S60 3rd Ed, Nokia S40 3rd Ed FP2.

Contact details

Cronto Limited, William Gates Building, 15 JJ Thomson Avenue
Cambridge, CB3 0FD, UK
Tel: +44 (0)1223 750001 Fax: +44 (0)8700 689597
Email: contact@cronto.com
Web: www.cronto.com

“Fellows and students have been using the Cronto visual signing technology to provide a unique authorisation code for each separate transaction. The application is provided on a memory stick or mobile phone, making the user experience easy and intuitive”

Professor Frank Kelly
Master of Christ’s College
University of Cambridge