New system to combat online banking fraud

April 18 2013

CrontoSign device and image. Credit: Cronto

A security solution which protects against the most serious threat to online banking customers, responsible for millions in annual losses, is being rolled out across Europe by a Cambridge University spin-out.

Developed in collaboration with one of Germany's largest banks, the technology devised by Cambridge-based company Cronto is helping protect customers against the threat posed by "Man-in-the-Browser" Trojan malware.

A Trojan horse is a type of malware which, like its namesake, presents itself as a harmless gift in order to persuade users to install it, appearing

as a legitimate software program. Once installed, hackers gain access to the computer in order to steal information or harm the system.

The solution developed by Cronto protects against Trojan attacks by using a visual channel to transfer data securely from the bank to the customer. It allows the bank to generate a pattern of coloured dots – a proprietary two-dimensional barcode containing the data which the bank is trying to send to the customer, which is decoded by the customer using Cronto's mobile application or standalone hardware device. The company's technology provides a secure "envelope" around the data so that it can be displayed to the customer on a trusted display for verification in any environment over any unsecured channel. The Trojan can see the image being sent by the bank, but cannot change the secure data inside.

Trojan attacks are prevalent and growing. Security firm McAfee identified more than 1.5 million different Trojan malware variations in 2012, with financial services websites a popular target. Trojans are especially dangerous as they control both what the bank receives from the customer and what the customer sees in their browser – a type of attack known as Man-in-the-Browser.

In an example of a Man-in-the-Browser attack, a customer may log on to their account on a real banking website and initiate a transfer to another account. The Trojan will detect this activity and will both increase the amount of the transfer and change the destination account number to that of the fraudster. Once the bank confirms that the transfer has occurred, the malware will change what is displayed to the customer, making them think that their desired transaction has been carried out. Effectively, the malware can freely alter the web page as it is displayed to the customer, and modify the requests sent back to the bank, so neither can detect that the fraud is taking place.

Trojan attacks of this type can cause customers to lose millions: in 2012, a single Trojan attack known as "Eurograbber" was discovered to have illicitly transferred over €36 million from unsuspecting banking customers. "Man-in-the-Browser attacks in combination with social engineering techniques are the most present and active threat to online banking," says Dr Elena Punskaya, Affiliated University Lecturer in the Department of Engineering and Co-founder and Chief Technology Officer at Cambridge-based company Cronto. "A combination of the malware and social engineering allows fraudsters to build a plausible story in order to initiate and hide the fraudulent payments."

According to Igor Drokov, Cronto's CEO, security in the world of online banking has to go beyond identifying who a customer is, whether via a password, the street they grew up on or the name of their pet goldfish.

"That's not enough," he says. "To combat the level of sophistication poised by Trojan malware, the bank also needs to verify the action that the customer is trying to perform, whether it's a purchase, a transfer or a change of address."

Cronto's aim was to produce a solution that was easy to use for millions of customers, but robust enough to meet the security challenges faced by banks. Dr Punskaya, a specialist in advanced machine learning algorithms and statistical data analysis, developed a new unique visual symbology optimised for secure, fast and reliable data transfer.

The 2D barcode which the team developed allows the bank to securely transfer a message of over 100 characters that is decoded by the company's application or hardware device in fractions of a second. The specific features of the image have been developed by testing machine learning algorithms on large datasets of images captured in different conditions.

Using the application or hardware device, the customer scans the image. Providing the security conditions are met, the customer will see the message from their bank, which is typically asking them to confirm the action they are attempting to perform, highlighting any aspects of the transaction which are out of the ordinary. To confirm the transaction, the customer simply uses a six-digit code, generated by the app or device, and enters it into their browser. The code acts as the customer's signature for this specific instruction, and once received and validated by the bank, completes the transaction.

The technology can be used in any environment and is highly adaptable, as it gives the banks the ability to change the message they wish their customers to see, whether in response to an emerging security threat, or simply to allow the customer to perform a different type of transaction.

Dr Steven Murdoch, a member of the Security Group at the University Computer Laboratory and Cronto's Chief Security Architect, designed and developed a new transaction signing solution able to withstand both attacks from criminals and the reality of industry.

Working together with banks, in particular Germany's Commerzbank, Dr Murdoch and the Cronto team implemented a state-of-the-art security protocol that has been adopted by leading banks in Germany and Switzerland, having successfully passed their internal and external security evaluations.

While Cronto is currently focused on the online banking sector, the team also sees commercial possibilities for their technology in e-commerce, peer-to-peer online payments, or any other application where there is a need to create a trusted connection between two parties.

Provided by University of Cambridge