A WALL NO TROJAN CAN LEAP
Remote Internet access faces its biggest challenge when the access computer does not undergo thorough security hardening on a regular basis. Accessing from a poorly secured computer is, and will largely remain, the usual situation when these computers are home computers located outside a controlled perimeter. This is because of the proliferation of mechanisms for introducing malware (usually called Trojans) in the access computers. Most antivirus and end-point-security applications on the market, for various reasons, are unable to provide a proper defense against rapidly evolving Trojans. Guaranteeing that the computers used for remote access are Trojan-free is therefore, at best, a tricky business when the computers are controlled by an organization and, at worst, a lost cause in the case of public or home computers under the control of their users.

codelogin uses the user’s cell phone to guarantee secure remote access from any computer, even if Trojan infected, and all in the most user-friendly way. Its innovative, patented concept can be applied to multiple cases, enabling for instance secure access to online banking and ATMs with a single device.

GMV
Isaac Newton, 11  P.T.M. Tres Cantos  28760 Madrid
www.gmv.es  marketing.tic@gmv.com
www.facebook.com/infoGMV
@infoGMV
The threats posed by Trojans can be broken down into two main groups:

- The theft of credentials or other sensitive access information.
- The execution of fraudulent operations and/or transactions unbeknown to the user.

Well-known solutions have tried to head off the first threat by using strong authentication devices based on one-time passwords or public key infrastructure. Both approaches have the drawback of needing a lot of management procedures, generally much more than required by traditional user names and password.

As for the second threat the only way of countering it is by using alternative platforms and channels that are considered to be secure (in the sense of trustworthy). Even robust authentication systems will only allow the computer-controlling Trojan (unbeknown to the user) to freely access the system, where it can then carry out such transactions as it may wish covertly.

SECURITY AND USABILITY

codelogin uses the user’s cell phone as an authentication token, as a secure execution platform, as a repository of private keys and as an alternative communication channel, authenticated and encrypted, using specific technology to minimize management costs.

codelogin only needs that the user’s cell phone be equipped with a camera and internet access, either using the cellular network or WiFi. It also supports NFC for cell phones featuring this technology. codelogin is just as simple as taking a cell-phone photo or approaching the cell phone to the NFC reader and has many advantages:

- codelogin enables secure access to a local or remote system using strong authentication technologies (two-factor authentication: “something you have” and “something you know”).
- codelogin is unaffected by Trojans due to dual-channel authentication preventing any malware already present in the client computer from manipulating sensitive transactions of the user or carrying out any fraudulent transactions.
- codelogin uses the user’s everyday cell phone as the authentication device (providing the “something you have” without the need of any additional token). You might lend out your token, but you will not lend out your cell phone.
- codelogin provides access without the user having to use any computer peripheral (neither keyboard nor mouse).

MINIMUM MANAGEMENT AND EASY SET-UP

Up to now the complicated management systems involved in setting up and running strong authentication systems have been a great obstacle to their more widespread use. The codelogin design includes unique characteristics to make the set-up and management processes much easier:

- It makes secure access compatible with the classic password/PIN based access, allowing a progressive phase-in and also allowing access in one-off cases where there is loss of mobile coverage.
- It maintains existing user experience when carrying out system transactions.
- It provides access based on certificate-less public key technology, taking management complexity out of the equation.
- Easy deployment enables authentication to several systems with minimum changes to these systems, under a common mobile user identity management platform which also manages mobile applications.
- No interference with existing identity management platforms.

TECHNICAL FEATURES

- codelogin includes identity-management modules that can be easily integrated into any platform and applications for deployment in the most commonly used cell phones.
- Access to codelogin mobile application can be protected with a local password (a password that never gets outside the cell phone). This password can be enforced with remotely managed security policies or be left at the user’s convenience.
- codelogin appliance features Identity-based Cryptography technology deployed on a FIPS 140-2 certified HSM from REALSEC.
- Security equivalent to 1024 bit RSA (or greater under request).
- Available for iPhone, Android, Windows Phone 7 and BlackBerry.