WHITE PAPER

Phoenix cME TrustConnector

...enabling trust in connected devices

phoenix technologies
www.phoenix.com

June 2005 - ISPAB
Handout of Albert E. Sisto
President + CEO

Phoenix cME TrustConnector™

...enabling trust in connected devices.

Introduction

The world of networked computing provides incredible benefits to individuals and businesses. But it also comes with significant risk. Confidential information, such as personal assets, corporate intellectual property, business and government secrets, and even our privacy are potentially vulnerable to compromise if not properly protected and managed on enterprise and service provider networks.

Enterprises have networks that are largely based on industry standard x86 architecture systems. The biggest challenge for the Information Technology (IT) department is to know who is on the network – not just the user, but also the type of device and how they access the network. In the past, it was believed that most of the threats come from inside the enterprise. However, recent studies have shown that external threats like viruses and worms far outweigh the internal threats. Enterprises have invested and deployed a number of perimeter security products to protect their networks. However, most of the protection and security has been at the network and user level. These products do not check the integrity and security of the specific x86 device that is connected to the network.

In the final analysis, network vulnerability can be reduced only if the devices on the network are trustworthy.

To move from thinking about new "security products" to "secure, trusted products" is a real paradigm shift for both the industry and the enterprise IT leaders. Perimeter-based network defense is an absolute necessity for the modern enterprise or service provider, but given the rise in spam-based attacks, it is insufficient to stem the tide of today's threats. Tokens, smart cards, and biometrics are great innovations. However, they are confined to identifying the user on the network, not seamlessly identifying the device as an integral part of the network, as is the case with an ATM, for example.

For the PC and connected device industries, we have to move in the direction of delivering not just "strong user authentication" but we need to think in terms of *"self-authenticating devices."* That is, we must enable networks to move beyond simple user name and password-based authentication to transparent authentication that is seamlessly incorporated into to the very foundation of the device and the fabric of the network. This will be a great step forward, and it must be done while providing backwards compatibility with the installed base that includes hundreds of millions of systems worldwide. In other words, one must deliver truly "native" (i.e. built-in and standards-based, not added-on) device authentication for old and new devices on the network.

Phoenix Technologies, a company providing the majority of the Core System Software (CSS) in personal computers since 1982, has developed a solution that can help solve this problem. Phoenix cME™ TrustConnector™ is a software product that enables authentication in devices so organizations can "lock-down" their networks, better enforce security policy and enhance the protection of digital credentials on networked computers. This paper discusses how Phoenix cME TrustConnector works. As you read it, you will learn how Phoenix cME TrustConnector enables device authentication and enhances security for Windows applications and clients on wireless and wired networks.

Trusted Networks Need Trusted Devices

Phoenix cME TrustConnector is a software product that enables seamless, built-in authentication of x86 devices to the network while enhancing the protection of identity credentials for Windows applications. Phoenix has extended its concept of a "chain of trust" directly into the Windows operating system through Phoenix cME TrustConnector. This is a universal CSP (cryptographic service provider) component for Windows machines that incorporates native "platform sensing" technology to examine the unique hardware fingerprint of every x86 system and to activate the highest trust level possible for that system within the context of enterprise or personal security policy.

Think of this as "trusted computing today" for the installed base of systems that currently connect to enterprise networks and the Web. TrustConnector also coexists with embedded hardware security subsystems and chipsets that support the Trusted Computing Group (TCG) standard. By supporting both new systems and legacy systems, TrustConnector is the first solution to implement native, *non-disruptive standards-based innovation in the trusted computing universe.* Phoenix cME TrustConnector delivers a device-centric, policy-aware chain of trust today, not tomorrow. This built-in trust can be leveraged by the entire ecosystem of device OEMs, ODMs, Independent Software Vendors (ISVs) and both enterprise and individual users.

By deploying Phoenix cME TrustConnector on Windows PCs, an organization can enhance network security policy by creating a network of trusted devices. TrustConnector will turn Public Key Infrastructure (PKI)-based policy enforcement features of common software applications and network infrastructure products into policy enforcement mechanisms to deny network access to unauthorized devices.

Native x86 Architecture Credential Storage

Phoenix cME TrustConnector provides strong, tamper-resistant storage of user credentials (such as private keys) by redirecting them from the Windows registry to a highly secure container encrypted with a strong, 128-bit Advanced Encryption Standard (AES) key specially created on each single device. This method ensures that the credential is protected from tampering. The AES device key is generated with the use of proven, strong cryptography methods and the detailed knowledge Phoenix has of industry standard x86 PC hardware architectures.

This x86 domain knowledge has been accumulated by Phoenix over more than two decades of enabling hundreds of millions of systems, and it is a critical element in ensuring each device key is unique. As the key encrypts the user credentials, it also binds them to the PC, thus assuring the identity of both the user and the device because the credential will not work on any other system.

Phoenix cME TrustedCore Raises the Bar

Phoenix cME TrustConnector will further enhance security if it is installed on a system that uses Phoenix cME TrustedCore or Phoenix cME FirstBIOS CSS. On a TrustedCore or FirstBIOS system, TrustConnector communicates with StrongROM™, a patent-pending embedded crypto engine.

On a TrustedCore or FirstBIOS system, credentials are stored in the hardware-based secure storage capability provided by StrongROM and secure silicon. The keys, which are actually stored on a hard disk, are encrypted using a strong device key that is not accessible by the operating system. This mechanism effectively protects the keys against unauthorized disclosure, modification, or substitution.

Additionally, on a Phoenix cME TrustedCore system, a credential is decrypted and used outside of Windows memory only in a memory partition called System Management Memory (SMM) that is not visible to a Windows-targeted attack. The level of security is increased, yet the TrustConnector CSP and driver ensure that Windows and all applications work seamlessly, with no visible effect to the user. TrustConnector automatically detects the existence of TrustedCore or FirstBIOS upon installation and utilizes their secure storage features when available.

Configuring Phoenix cME TrustConnector with Windows Applications

Microsoft Windows provides the ability to communicate securely across the Internet and the Web. A digital certificate based on public key cryptography is a confirmation of your identity and it contains information used to protect data or to establish secure network connections.

Windows applications are able to use public key technology to secure files, messages, and transactions that are exchanged over networks. To enhance this security, Phoenix cME TrustConnector can be used in conjunction with Windows software. This enables storing of unique digital credentials in a secure storage area, providing the following benefits:

- Digital credentials are protected by two-factor security – something that you have (your platform) and something that is known (a pass phrase or PIN)
- Digital credentials are bound to the platform and cannot be copied from your workstation's hard disk to another