

WHITE PAPER

Phoenix
Embedded World[™]

Secure from the START

Reliability, Security and Recovery
for Today's Embedded Systems



Developers of networked embedded systems must deal with the same security challenges that plague general-purpose desktop PCs and servers. Phoenix Technologies provides a selectable stack of solutions to secure embedded systems from the first electron through the application space—and to recover faulty systems safely and automatically without the need for installation disks or even a bootable OS.

Today's embedded systems are literally revolutionizing industry, entertainment, retail, finance, science and home life. The same force that drove the explosion in desktop computing in the late 20th century is now driving the progress of embedded systems. Network connectivity, and especially Internet connectivity, has transformed the very nature of what's possible in the embedded world.

Point of Sale (POS) kiosks, network-configurable gaming devices, touch-screen voting machines, industrial robots, remote sensing devices, digital surveillance systems, consumer electronics—all of these and more are networked to provide functionality that would not be possible in a stand-alone device. The ability to network embedded devices offers a great opportunity for device designers looking for ways to create new usage models—and generate new profits.

But there's also a serious downside to Internet connectivity. Just like desktop PCs, embedded systems that are connected to a public network are in danger of being exposed to malicious intrusion and malware. To give just a few examples:

- Next-generation video gaming machines allow casino operators to download new code to tailor games to their customers' preferences. But if machines can be repurposed, they can also be loaded with illicit code that violates gaming laws or even steals from players.
- Touch-screen voting requires a validated and certified software stack. But on Election Day, officials rarely have any way to verify that the stack has not been altered.
- Remote sensors and digital surveillance systems are prime targets for organized cyberterrorists seeking to disrupt or steal intelligence.
- As DVRs, set-top boxes and Internet radios revolutionize consumer entertainment, content providers need to ensure that the devices can't be repurposed to steal or redistribute content.

A worldwide epidemic of hostile cyber attacks, and the increasing threat of organized cyberterrorism, have made security and trust a key market differentiator influencing the success of embedded solutions. We could give many more examples of how connected systems can be compromised via the network, and how compromised systems can in turn damage the entire network. But you get the idea.

Suffice it to say that networked embedded systems offer incredible opportunities—if they incorporate strong security to prevent intrusion or corruption via the network connection.

Securing Embedded Systems from the First Electron

The traditional approach to security is to protect the perimeter of the network using a firewall. However, firewall security, in itself, isn't enough. Any firewall can be breached by a sophisticated and determined hacker. And even if you could defeat every potential intruder, no firewall can protect against threats originating inside the perimeter. These threats can arise from both user error and malicious attack, and include tampering, fraud, repurposing of hardware, noncompliance with policies, altering of the software stack, reflashing of system firmware and more.

That certainly doesn't mean it's time for companies to dismantle their firewalls. It does mean that firewalls for networked embedded systems need to be supplemented by a "secure from the start" strategy. Before the firewall even comes into play, embedded developers need to build mechanisms into their systems that ensure device integrity, trusted network connections, trusted applications and reliable data recovery.

Phoenix Technologies has pioneered this "secure from the start" approach, with Core System Software and Trusted Applications that secure systems from the first electron, through the OS, to the application space, to the network. By selecting the right Phoenix products for their specific needs, embedded systems developers can create a root of trust anchored in secure firmware and security services performed below the OS level—where users can't make mistakes and hackers can't interfere.

Phoenix security solutions for embedded systems allow you to ensure that certified and authenticated relationships can be established between every element in the runtime environment—devices, networks, users, data, and applications.

Automating Data and Application Recovery

"Secure from the start" trust is the most important factor in ensuring the integrity of applications and data. But even with the best-protected system, things can go wrong.

No developer can guarantee bug-free software, and one application may cause unpredictable conflicts with another. A power surge can knock things out of whack, and a complete power failure can leave data in an unrecoverable state. Users can—and often do—delete things by mistake. The bottom line: If a system is critical enough that you can't afford to lose access to it, or to lose some or all of the data stored on it, then you need backup and recovery capabilities.

Embedded systems often give users less direct control over backup and recovery operations than desktops and other general-purpose systems. For example, the failure of a remote weather station or a pilotless manufacturing system may go unnoticed for a long time, causing a major loss of valuable data. And when things go wrong, system buyers and users tend to blame you, the system designers—potentially damaging your product reputation and your bottom line.

The solution is to incorporate diskless backup and restore capabilities—and even pre-OS recovery capabilities—into your embedded system designs. These technologies allow users to restore data and recover system images to their factory-installed state, without the need for software media or even a bootable OS. There's no need for a support call, which saves your customers money and builds a reputation for the availability and reliability of your products.

As the leader in "secure from the start" solutions, Phoenix has the back side covered as well. Phoenix FirstWare products integrate easily into your embedded system designs, allowing you to provide your customers with the built-in peace of mind they're looking for when shopping for a system vendor.

Real-World Examples of Embedded Security and Recovery

Embedded systems developers in virtually every industry are choosing Phoenix solutions in order to gain a real advantage in the marketplace. Here are two prime examples.

Trusted Game-Development Software

Taito Corporation, a leading maker of arcade games and console game software, has adopted the Phoenix Security Software Development Kit (SDK) in its Taito Type X game system platform, creating an open, secure Windows based game development environment.

The worldwide gaming industry was valued at around \$35 billion at the end of 2002, which rivals the size of the music industry. Widely acknowledged as one of the most competitive industries, it is critical for game developers to protect their software from hackers and copyright infringement.

The Phoenix Security SDK provides programmers with easy-to-use developer tools to integrate device authentication and other cryptographic security functions into their applications. Taito Type X operates on a specialized version of Windows XP, allowing game developers to cut both development time and costs in creating titles for the arcade board by using normal Windows development software. Developers won't need to learn specific details about new hardware because the board is based on standard PC architecture.

The addition of Phoenix Security SDK will allow Type X to meet its true potential as a secure, low-cost, expandable and powerful board—bringing Half-Life 2 to arcades in the summer of 2005, along with an ongoing supply of new games for the PlayStation 2.

Recoverable Test and Measurement Equipment

Iwatsu Test Instruments Corporation, a Japanese electronics pioneer specializing in test and measurement equipment, has developed a new digital oscilloscope that includes Phoenix Technologies Recover Pro and Console applications. The addition of the Phoenix applications enables restoration of the operating system without the need for backup media. This ensures that important data is always saved and available to the user in the event of an operating system failure.

The new Iwatsu WaveSurfer digital oscilloscope, developed jointly by Iwatsu and LeCroy Corporation, does not include a CD-drive. Instead, it relies on the Phoenix Technologies FirstWare Recover Pro and Console applications to power the automatic, incremental backup of important data and test results.

The Recover Pro application provides system backup and recovery—including access to Web-based support from the pre-OS environment—and gives the user a choice to restore the entire hard drive or only a specific partition. Other products on the market that Iwatsu evaluated were not appropriate because they delete all the stored data on the hard drive. Recover Pro allows easy restoration of an original hard drive image so workers can remain productive even after a system crash.

Phoenix Solutions for Embedded System Security and Recovery

To be successful, embedded systems developers need to clearly set their products apart from the competition. In today's vulnerable, networked world, the best way to do that is to provide unmatched security and recovery capabilities. At the same time, developers need the flexibility to choose the capabilities that best suit their applications, customers and budget.

Only Phoenix offers a selectable stack of services that can be mixed and matched to meet your exact requirements for securing any type of embedded device—from the most basic consumer electronics to the most advanced systems for scientific analysis, manufacturing, surveillance and more.

With Phoenix solutions, you can choose the ideal mix of:

- Trusted firmware
- Trusted, manageable Core System Software
- Trusted applications
- Trusted network connections
- Diskless storage of secure OS and application images
- Diskless and pre-OS recovery of damaged systems
- Easy-to use tools for securing applications and extending functionality to today's and tomorrow's embedded technologies

Some of the major Phoenix products that provide security and recovery for your embedded system designs are described below.

Refer to the following diagram to see where these products fit in the overall embedded system architecture.

Phoenix SecureFlash

Embedded systems, like all systems, depend on trusted firmware. This is the code that runs before the operating system or anything else loads, and so the integrity of the entire system depends on it. However, the ability to install and upgrade firmware through software that “flashes” the firmware with new code opens up systems to a fundamental vulnerability. By maliciously reflashing firmware with a corrupt image, hackers can potentially destroy data and applications, spy on passwords and other user input, or even kill systems by preventing them from booting at all.

Phoenix SecureFlash eliminates these vulnerabilities by ensuring that a firmware image is authenticated and verified by the OEM as appropriate to the target system before the image can be loaded into Flash ROM. Once the authenticated image has been installed, Flash ROM is “locked down” so that it can't be reprogrammed again, except by another authenticated and verified image.

SecureFlash acts as an antivirus solution for the Core System Software—but with an important difference from traditional antivirus products. Instead of detecting and quarantining viruses after infection, SecureFlash actually “hardens” the Core System Software so that worms and viruses never reach it in the first place.

Phoenix TrustedCore Embedded

With the firmware secure, the system can safely load the Core System Software that controls basic hardware functionality and supports the operating system. Phoenix TrustedCore Embedded goes far beyond traditional BIOS to provide unprecedented manageability and security for connected devices, protecting against both malicious attacks and accidental damage to the system software image.

TrustedCore Embedded combines with Phoenix TrustConnector (described below) to create a strong public key encryption security kernel that protects the Core System Software and extends trust to the managed application environment, the operating system and applications. TrustedCore Embedded supports a protected application area for embedded management and recovery applications, providing a built-in security kernel to safeguard the environment against malicious or accidental alteration.

System builders can tie their applications into this secure execution environment, using the Phoenix Security SDK (described below) to provide “secure from the start” applications that authenticate to the system using the public key encryption technology built into Trusted Core Embedded.

Phoenix TrustConnector

Phoenix TrustConnector extends the “secure from the start” environment to the network connection, ensuring that only trusted devices with trusted users and trusted applications can connect. Traditional authentication solutions are all designed to authenticate user credentials only. This leaves networks open to possible corruption via stolen passwords, copied certificates, transfer of credentials to unmanaged machines, and so on.

TrustConnector plugs into the Microsoft CryptoAPI security interface, enabling applications in the user space to take advantage of the Phoenix encryption/decryption technologies secured below the user level. TrustConnector hardens traditional authentication methods by ensuring that credentials belong to and can only be used on the system to which they are issued.

Phoenix's exclusive platform sensing technology determines the specific hardware fingerprint of every embedded device. Even if devices are identically configured, TrustConnector can tell them apart. TrustConnector then uses this fingerprint as part of the authentication process, ensuring that only the unique combination of trusted user and trusted device can connect to the network. With TrustConnector, the device itself becomes its own nontransferable security token.

TrustConnector also takes advantage of the TrustedCore encryption engine to lock down keys and perform authentication operations below the operating system level. With this architecture, there's no way for a hacker to observe or interrupt security processes—and even if a key or secure application could be moved to another device, it simply wouldn't work.

Phoenix Security SDK

The Phoenix Security Software Development Kit (SDK) makes it easy to integrate device authentication and other cryptography functions into your applications. This is the final link in the “secure from the start” chain, extending Phoenix security to your applications in the runtime environment.

Application developers who need security services usually have to choose between two imperfect solutions. They can use hooks to security services within the operating system—which is vulnerable to hacking. Or they can add security hardware that drives up the expense of the system and takes up valuable space—an unappealing approach for embedded systems developers who are typically targeting small, lightweight and affordable designs.

The Phoenix Security SDK offers easy-to-use tools that enable developers to seamlessly integrate Phoenix security technology into their applications to provide a wide range of hardened security functions. With the Phoenix Security SDK, you can prevent software piracy by automatically locking software to the hardware it's installed on, using the TrustedCore device key. You can also provide automatic verification of the software's digital signature to ensure that the software has not been tampered with in any way. And you can offer Phoenix security services as an integral part of your applications—gaining a strong competitive advantage.

The Phoenix SDK allows you to easily integrate leading security technologies with minimal disruption to your engineering processes, market schedules or end-user experience. You can have all the cost and space advantages of software-based security solutions, along with the superior tamper resistance you would expect from a hardware-based solution. And you can give your users transparent access to unsurpassed security features—there's nothing new for them to learn or remember beyond the credentials that your application would normally ask for.

Phoenix CoreArchitect

Phoenix CoreArchitect is an advanced firmware development environment that helps developers build secure, reliable devices of all types—strongly differentiating their products and bringing them to market faster. Building on the powerful Microsoft Visual Studio .NET Professional graphical interface, CoreArchitect provides Phoenix-customized tools for incorporating device authentication and other security features into any x86-based device.

Moreover, developers can use CoreArchitect to integrate network standards such as XML, HTML and TCP/IP within the device core, enabling high-performance grid, blade and cluster network architectures. CoreArchitect makes it easy to add new functionality and extend the framework of networked embedded devices, enabling inventive new application models that open the door to new markets.

Phoenix FirstWare Recover Pro Manufacturing

FirstWare Recover Pro is an advanced backup and recovery solution that allows users to quickly and easily recover their applications and data in the wake of virtually any malfunction. Whether it's a minor glitch, a major virus attack or a complete system failure, recovery is only a few mouse clicks away.

FirstWare Recover Pro is built into the core managed environment of the device, and stores backups of user data, applications and the operating system in the secured host-protected area (HPA) of the hard drive. As part of the Phoenix core managed environment, the HPA is safe from viruses and tampering—so users can always safely restore systems to their original state or a more recent state no matter what goes wrong in the runtime environment.

Because all the information needed to restore a system is in protected storage on the system, there's never a need for factory-supplied restore CDs, and there's never a worry over losing updates that have been installed over the original system image. Moreover, FirstWare Recover Pro establishes a preboot recovery environment on the device, so systems can be recovered even if the operating system won't start.

The FirstWare Recover Pro Manufacturing version allows manufacturers to quickly and easily install a backup of the device image as it exists when shipped. This enables customers to return devices to the original state after a crash without placing a support call or searching for backup CDs. By offering devices with this complete, built-in recovery solution, device manufacturers can strongly differentiate their products from the competition, offering their customers solid protection against downtime and data loss.

Phoenix FirstWare Vault

Similar to FirstWare Recover Pro, FirstWare Vault provides a host-protected area (HPA) on the hard drive for storing a tamper-proof copy of the operating system, critical applications and drivers. From the end-user's point of view, the HPA appears as a virtual CD/DVD drive containing copies of application and system software.

A simple Windows application allows users to install and access virtual CDs and DVDs. Storage within HPA keeps software safe from viruses and other malware, and the virtual CD/DVD format enables users to reinstall applications and drivers using the Windows auto-run feature, without requiring access to the software's physical media.

By providing Phoenix FirstWare Vault with device designs, you improve the end-user experience by empowering users to automatically repair or reinstall software themselves, without the disks, wherever they may be—a particular advantage for mobile embedded systems. At the same time, you reduce support calls and on-site service costs, so you can direct more of your resources into developing innovative products. You increase the usefulness and reliability of your products, building your company's reputation in your chosen market space. And you can use the secure, virtual CD/DVD area to offer value-added applications, fee-based services, trial software and more.

Putting it All Together: The Benefits

Phoenix SecureFlash, TrustedCore and TrustConnector—along with the Phoenix Security SDK and CoreArchitect—enable you to provide a complete security environment for embedded systems that:

- Eliminates the threat of accidental or malicious reflashing of firmware with an improper image
- Provides a manageable, secure execution space for the operating system and applications
- Allows enforcement of device-specific security policies
- Provides strong, tamper-resistant storage of user credentials without the need for any additional hardware
- Helps prevent data loss, business interruption, hacking and other threats
- Offers seamless compatibility with existing network infrastructure and security products
- Is easy to deploy and manage on new and existing machines, providing a cost-effective alternative to other security solutions
- Works transparently—with no changes to the user experience—so no additional user training or support is required to achieve truly trusted computing
- Integrates seamlessly with your applications to decisively differentiate your products from the competition
- Adapts easily to both current and future technologies, boosting the security and value of your line of embedded systems.

In addition, Phoenix FirstWare Recover Pro and FirstWare Vault provide pre-OS and diskless recovery for operating systems and applications. By building these capabilities into your products, you can provide:

- Automatic backup with virus-protected storage for system files, applications and data
- Quick, user-driven recovery, with no need for the original installation CDs or DVDs
- Pre-OS recovery for systems that can't boot
- Diskless auto-run capabilities
- Value-added software and secure storage features
- Product differentiation, with systems that are more reliable and easily recoverable
- Freedom from excessive support-desk calls, so you can be more responsive to customers while freeing resources for product development and marketing.

Secure from the START

Phoenix Technologies is a global market leader in device-defining software that enables endpoint security from the start. The company first established dominant industry leadership over 25 years ago with BIOS software. From this unique foundation of core level expertise and firmware offering the highest levels of reliability, Phoenix has created a portfolio of innovative software products that simply and easily identify and restore devices, thereby assuring users unparalleled endpoint security and availability.

Phoenix Technologies Ltd.

915 Murphy Ranch Road
Milpitas, CA 95035 USA
408.570.1000 main
408.570.1001 fax

800.446.9202 North America sales
781-BUY PTEC Outside North America sales

©2005 Phoenix Technologies Ltd. Phoenix and Phoenix Technologies are registered trademarks of Phoenix Technologies Ltd. All rights reserved worldwide. All other brand or product names are the trademarks and property of their respective holders.

0000-XX000