

Fault Tolerant Modems and Embedded Security – The New Wave of the Telecom Expansion

Jerome L. Krasner, Ph.D.

February 2004

EMBEDDED MARKET FORECASTERS

American Technology International, Inc.

Embedded Market Forecasters

Research and Consulting
for Embedded Products,
Markets and Channels



Copyright 2004 by Embedded Market Forecasters, a division of American Technology International, Inc, 1257 Worcester Road #500, Framingham, MA 01701. All rights reserved. No part of this document covered by copyright hereon may be reproduced or copied without expressed permission. Every effort has been made to provide accurate data. To the best of the editor's knowledge, data is reliable and complete, but no warranty is made for this.

Table Of Contents

Overview	5
Business Market Forces.....	5
Global Connectivity and Security – Market Driving Forces	6
Encryption (or lack of)	7
Lack of Certified Encryption.....	8
The Federal Information Processing Standards (FIPS): Why embedded vendors, OEMs and developers need to incorporate FIPS 140-2.	9
Lack of Management & Monitoring Abilities	10
Painful & Expensive Patch Management with Minimal Accountability	11
Summary.....	13

This page intentionally blank

Fault Tolerant Modems and Embedded Security

The New Wave of the Telecom Expansion

Overview

Technology guru Michael Murphy describes the three-waves of technology growth that involved semiconductors. The First Wave occurred in the mid 70's driven by mainframe computers; the Second Wave occurred in the mid 80's driven by the PC revolution; the Third Wave occurred in the 90's and was driven by the Internet explosion (not to be confused with the dot-com sector). Each Wave generated a 500% growth over the preceding Wave. Murphy, along with embedded market researchers (e.g., Embedded Market Forecasters – EMF), express the view that we are at the onset of the Fourth Wave – Murphy calls it “Universal Connectivity”, EMF calls it “Communications & Connectivity”.

The technology is at hand to provide the bandwidth (and software) to provide an “electronic skin” that promises to change the way business is conducted. Manufacturers service centers can connect to their deployed end-user devices to offer better service; every printer, elevator, air conditioner, vending machine, etc. can report its status, financial receipts and maintenance requirements as they occur. Millions of workers are now able to connect communications devices to their VPN to support sales, CRM and product availability. This ability will increase as the world moves to 2.5G or 3G wireless technology. Key to this emerging technology wave is the presence of a reliable, fail-safe inexpensive and secure modem – both in hardware form and as a software upgrade to the installed base of millions of embedded modems.

Business Market Forces

Enterprises are constantly looking for ways to increase revenues by developing new products, markets, or ways to enhance service to their existing customers. In fact, a company's success depends on its ability to identify and establish long-term relationships with its most valuable customers. In today's competitive marketplace, it is essential for the enterprise to understand these customers' needs and expectations and to develop their products, services and business processes accordingly.

Through a combination of ubiquitous technologies—the Internet, wireless, and the computer-based chip, or “pervasive computing”, technology that controls almost every system, machine, instrument or sensor made today can be monitored. This enables product manufacturers with the opportunity to connect with their end-users to gather not just the “snapshot” usage profile that a warranty card or electronic registration provides, but ongoing usage and performance data. This data creates an invaluable market research channel to support decisions about product line upgrades, extensions and additions. This helps the manufacturer better service it's installed base, and also enables the manufacturer to add new service offerings.

ConnectForte has developed the technology that used in infrastructures to securely monitor, manage and service intelligent products deployed at end-user

sites in a manner that can be easily configured and assembled using “off-the-shelf” technologies and services. An Integrated Product Support System (IPSS) enables manufacturers of products ranging from under \$100 to thousands of dollars to better serve their end-users and generate new revenue streams with minimal overhead.

Key to these applications is a highly reliable (fault tolerant) modem with fast connect and expedient data throughput. From a marketing perspective, the ability to convert deployed modems to fault tolerant, real-time, rapid connect devices via a software upgrade addresses a very large installed base of devices thus extending their usefulness. Additionally, the company has integrated a FIPS 140-2 certified encryption module required by the U.S. government for the purchase of any datacom system regardless of the degree of security required. This level of security meets the standards established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for medical data exchanges and is consistent with GLB requirements for financial transactions.

ConnectForte’s modem family of rapid connect, real-time and fault tolerant modems encompass all major applications from basic connectivity (e.g., from an appliance) to secure transaction for financial applications. The diversity of its modem technology and the ability to add functionality onto each of the family of modems creates an efficient, low cost opportunity for suppliers, customers and OEMs to buy from ConnectForte as opposed to wasting resources to attempt to build their own. This diversity also is a deterrent to potential competitors.

Global Connectivity and Security – Market Driving Forces

We are entering an age of unlimited bandwidth and enhanced connectivity – the new marketplace will revolve around those technologies that waste bandwidth to achieve comprehensive connectivity (handhelds to enterprise to Internet access, etc.) – not to those technologies that foster yesterday’s packet switching SS7 infrastructure.

Security will be a necessity of all embedded systems that employ connectivity of any sort. Hackers have not yet focused on embedded systems (traffic lights, power plants industrial controls) but the chances of such as we move into a new age of connected devices is a virtual certainty.

The service industry will take on new dimensions as connected devices become pervasive. Home appliances that can be remotely monitored or investigated will dramatically lower the cost of service and make such offerings more profitable. Can a manufacturer of refrigerators or microwave ovens afford to send technicians out on warranted service plans without knowing what part or component is required when their competitors can service such remotely? If modem connect times are reduced from a 30-second handshake to a few seconds, it would make better sense financially for utility companies to remotely call into water, electric and gas meters rather than send out service drivers to read the meters. Neighborhoods could use 802.11 wireless connectivity to

enable the reading of all meters from all homes – provided that absolute security was built into the connectivity once the transmission reached the wireline.

Point of sale systems depend on dial up connectivity and fault tolerance combined with security. The economics of connectivity again dictate the required technological solution. Credit card processing companies have stated that if they could save one cent per transaction, they would realize an annual savings (direct to the bottom line) of \$70 million. Set top box vendors report that their greatest expense is for telephone connect time wherein an OS or application software failure results in unlimited 800 calls.

Embedded systems/software development design complexity is reaching disturbing proportions. Market Intelligence studies by Embedded Market Forecasters illustrate the magnitude of the situation.

Embedded developers in these studies report that nearly 50% of final designs are not within 30% of pre-design expectations (>33% are not within 50% of expectation!). Some 13% of design starts are cancelled – but the time between design start and cancellation is an average of more than 4 months! More than 50% of embedded designs fall behind schedule, and are more than 3.9 months late.

Executives of companies that purchase software, boards, tools, etc., have become aware of the enormous cost of these design shortcomings. Software currently exists to create an application layer on the OS that permits incident-reporting data to be gathered. Embedded vendors see the value in placing a secure modem in shipped systems that permits them to monitor systems operation subsequent to shipping. Clearly, a secure modem (containing a FIPS 140-2 certified module) that can report on systems performance can result in substantial savings to OEMs and to their suppliers.

We have already entered a market for handheld devices capable of accessing enterprise level data. Millions of people are working at remote locations that need to access customer and company information. Truck drivers and delivery employees need to report deliveries and gain new pickup destinations that might change due to computer-based analysis of demand and availability. Sales people need CRM and inventory data – CFOs need updated company financial information that is accurate to the minute as they make client presentations.

Whether by WiFi, by dial up or by broadband, secure communications in a fault tolerant environment will play a major role in the growth of the worldwide-embedded marketplace.

Encryption (or lack of)

Protection of the confidentiality and integrity of sensitive information is a critical foundational component of any secure system. Typically, encryption algorithms,

like DES, AES, RSA, or countless others implement this protection at least in part.

Unfortunately, many networked embedded systems lack robust encryption to protect sensitive information. This may be due to resource limitations (strong encryption requires substantial processing, memory, and power), cost restrictions, design limitations, or possibly the extension of an internal, legacy, hard-wired system onto an open network such as Ethernet or IP, without considering the associated security implications.

Regardless of the reason, the potentially disastrous results are the same. Intruders or malicious insiders can read, intercept, modify, or remove communications at will. If proprietary wireless RF links are involved, the danger is further amplified, as anyone with suitable equipment can attack the system, potentially from a substantial distance given a high-gain antenna.

In many cases, damage resulting from eavesdropping on sensitive information pales in comparison to damage resulting from forged or modified communication. Consider a gas pipeline monitoring system, which uses wireless RF links between sensors nodes along a gas pipeline, which monitor and report on line pressure, temperature, purity, and other critical data. If the system lacks strong encryption, an attacker could easily damage or destroy the sensors at a vulnerable point on the pipeline, then substitute his own device that generates false sensor data, while the attacker damages the pipeline. Alternatively, the attacker could generate false readings indicative of a leak or fire, diverting maintenance and response personnel from the intended point of attack.

Clearly, insufficient cryptographic protection can lead to substantial compromises, many of which are not immediately obvious at system design time. A prudent embedded system designer must consider the implications of intercepted, deleted, modified, and forged information from all components of a networked system, and take steps to provide encryption to protect against such attacks.

Lack of Certified Encryption

Even if a system employs strong encryption to protect its security, in many cases that is not sufficient. In many markets or domains, some form of official certification must be obtained for a product or system before it can be used. A familiar example of this outside of the security field is the DO-178b certification required for embedded systems in safety-critical applications such as avionics.

In the realm of security certifications, one of the most important is the Federal Information Processing Standard (FIPS) number 140, revision 2--or FIPS 140-2 for short. FIPS 140-2 is a standard and certification process for encryption software and hardware, which is mandatory for all information systems used by the Federal government to process "sensitive" information.

The Federal Information Processing Standards (FIPS): Why embedded vendors, OEMs and developers need to incorporate FIPS 140-2.

Although the FIPS standards are surprisingly unfamiliar to embedded vendors, developers and OEMs, they play a crucial role in the future of embedded commerce as the new world of connected devices and network security unfolds.

The Federal Information Processing Standards are a suite of information security guidelines promulgated by the National Institute of Standards and Technology (NIST) on behalf of the United States Government. Each of the FIPS addresses a particular information-processing topic, ranging from the specification of an encryption algorithm to recommended utilization of a particular security standard. Though there are dozens of FIPS, the most important FIPS, and the subject of this section, is FIPS 140-2.

The major fact that embedded vendors, OEMs and developers alike must understand regards FIPS 140-2 certification: if you offer products which perform any kind of encryption (such as IP-sec, SSL, or SSH stacks), you must affirm that all such encryption is performed by a FIPS 140-validated cryptographic module, or you can kiss federal dollars goodbye.

Of particular interest to the embedded industry is the following:

- In effect, anything that is worth encrypting **MUST** be encrypted using software certified under FIPS 140 version 2
- Federal agencies may **ONLY USE** FIPS 140-2-certified encryption products to protect sensitive but unclassified information on their computer systems. This means that even a product with certification under another FIPS, such as FIPS 46-3 specifying DES, is not sufficiently certified to meet Federal acquisition requirements.
- Even if your company does not sell directly to the government, FIPS 140-2 certification enables government contractors doing business with the Federal government to use your product as a part of their solution.
- By obtaining FIPS 140-2 certification—either in-house or through licensing of a third-party component—embedded products such as medical devices, monitoring systems, alarm and surveillance systems, and all other network-aware embedded solutions can immediately differentiate themselves and open themselves to the substantial Federal government market, as well as to private contractors developing Federal systems.
- FIPS 140-2 is likely to emerge as the standard of “reasonable compliance” for corporate fiduciary responsibility, HIPPA, GLB.
- Certain FIPS (including FIPS 140-2) are mandatory for computer systems used by Federal agencies. In particular, Federal agencies may use only FIPS 140-2-certified encryption products to protect sensitive but

unclassified information on their computer systems. This point is sufficiently important that it bears repeating: **Federal agencies may use only FIPS 140-2-certified encryption products to protect sensitive but unclassified information on their computer systems.** This means that even a product with certification under another FIPS, such as FIPS 46-3 specifying DES (Digital Encryption Standard), is not sufficiently certified to meet Federal acquisition requirements. The product still requires FIPS 140-2 certification to qualify for use by Federal agencies. In effect, a validated module, certified under FIPS 140, must encrypt any information that justifies encryption.

- FIPS 140-2 is simply a cryptographic module certification. It is not a security protocol like SSL, and thus does not address any real-world secure protocol issues. An SSL stack, for example, could easily have FIPS 140-2 certification; they are not competing protocols.

Lack of Management & Monitoring Abilities

Regardless of the extent of a system's protections, it must be monitored for accidental failures and deliberate attacks, and may require management of configuration parameters, performance counters, etc. Most PC's and network equipment provide management and monitoring capabilities through an SNMP implementation (though it may be buggy), and some sort of logging facility, either by writing to a local log file, or using a distributed logging service such as syslog to aggregate events into a central location. The combination of these two abilities makes it substantially easier for limited IT resources to manage and monitor a large, widely distributed ecosystem of network-connected devices, in some cases even from the remote network operations center of a managed security services provider (MSSP).

Though many embedded systems used in telecom or networking equipment already provide manageability features, many other systems—in some cases, highly constrained systems—lack even basic remote event logging capabilities. As a result, the total cost of ownership of these devices is much higher due to additional management burden, and attacks on these devices are less likely to be detected due to the IT “blind spot” created by a lack of event reporting abilities.

In many cases, SNMP and *syslog* implementations are available and can be incorporated into a system design to provide the necessary functionality. In many other cases, however, standard protocol implementations are not available, and depending upon system design constraints, may not even be possible. In these situations, some form of proprietary management and monitoring functionality may be called for, perhaps with a separate component providing a bridge to standard protocols.

No matter the circumstances, embedded systems stand to benefit the most from remote management and monitoring functionality, due to their wide distribution, frequent inaccessibility, and the critical nature of their functionality. Not only does remote management and monitoring functionality contribute to the security of a system, it also lowers cost of ownership for the customer, and remote diagnostics or configuration abilities may also lower maintenance costs for the manufacturer, as routine diagnostics and initial repair orders may be conducted remotely from a central location, instead of a truck roll.

Painful & Expensive Patch Management with Minimal Accountability

For all the protective measures described above, past experience has shown that no real-world software system can be guaranteed free of bugs, regardless of the extent of security precautions taken during its design and development. Therefore, one must assume that patch management—the process of obtaining, validating, testing, and deploying patches—will be a key component of any security strategy. In the PC networking realm, myriad patch management offerings are available from software vendors, ranging from operating-system-specific patching tools to cross-platform, cross-enterprise systems. Some tools even support embedded systems to some extent, such as those found in network devices and printers.

Any network-enabled embedded system must provide some means of post-deployment firmware updates. Ideally, the update mechanism should provide the following functionality:

- Ability to determine the current firmware version remotely over the network. Without this feature, asset tracking and patch management tools will be unable to automatically detect systems with out-of-date firmware revisions
- Ability to patch firmware remotely over the network. If this feature is absent, the substantial time and cost associated with patch deployment will act as a disincentive to patching vulnerable systems, which in turn reduces system security and increases cost of ownership
- Ability to authenticate and verify patches. If remote patching is supported, it is critical that some means of authentication is provided, so that only authorized users can apply patches. Furthermore, firmware patches should be verified as authentic prior to application, ideally by a digital signature applied by the vendor prior to the patch release. If these features are not present, attackers could easily install firmware patches which either disable the devices, or introduce back doors for future attack

In addition to these technical issues, the designer of a system must ensure that all software components of the system are developed and maintained according to a process, which facilitates rapid development and testing of patches as bugs are removed and features added. This means that not only must software

vendors provide patches; they must also employ extensive, automated regression testing frameworks, to ensure that the resulting patch fixes the intended bugs, adds the intended features, and does not break existing functionality or introduce new bugs. Without this basic assurance of validity, deploying a vendor's patches becomes a gamble, wherein one must weigh the risk from use of an unpatched system against the risk that the vendor's patch will break the system, possibly so badly as to require manual reprogramming.

Unfortunately, apart from some network devices and printers, most embedded systems provide minimal patch management support, resulting in an expensive, time-consuming patching process, which discourages active patching, and minimal accountability to verify those patches which have been deployed. As long as this trend continues, the effected systems will suffer from substantially reduced security.

Compounding the problem, many highly constrained systems lack the resources to implement a robust patch management scheme. In almost all cases, additional costs are justified to implement over-the-network reprogramming, due to the substantial reduction in total cost of ownership realized by this feature. Failing that, all network-connected systems must provide, at the very least, some means of automatically determining the firmware revision currently installed on each device, so that even if patch deployment cannot be automated, it can at least be planned, estimated, monitored, and verified.

Unfortunately, off the shelf tools are unlikely to provide this type of functionality, as it is highly system-specific. Nonetheless, some commercial software components are available which could be assembled into a patch management solution.

Though the cost of patch management functionality may be high, the cost of a lack of patch management functionality is almost always higher; anyone designing a network-connected embedded system is strongly urged to consider the logistics of patch development and deployment, from the first line of code to the last updated device.

Summary

We have begun to enter a world of ubiquitous connectivity driven by a large and economically viable available bandwidth. The ability to remotely monitor and service products and devices is not only changing the economic viability of the embedded marketplace, but the standard of living for the world.

Credit card handling, medical record/data requirements, financial transactions, and installed home appliances are examples of how the New Telecom environment is emerging.

Central to this new infrastructure is:

- The ability to rapidly connect to remote devices and technologies
- The ability to insure secure transmission of data
- The ability to software upgrade existing modem installations to fault tolerant, rapid connect and secure status.
- The ability to remotely and securely provide “patch” security upgrades to embedded systems

And most important, to be able to economically deliver such aforementioned technology to currently installed systems and to new systems. ConnectForte’s fault tolerant modem family and FIPS-140-2 certified encryption module, depending on application, provides a family of solutions ranging from \$50 to \$500 per system.

Can any embedded vendor, OEM or device manufacturer afford not to incorporate such technology?

A detailed report of embedded security and issues embedded vendors, OEMs and manufacturers need to know about embedded security is located on the Embedded Market Forecaster’s web page (www.embeddedforecast.com).

Embedded Market Forecasters
Research and Consulting
for Embedded Products,
Markets and Channels

