

# Innominate mGuard Embedded Miniature Security Solutions

Innominate Security Technologies AG

28 March 2003

© 2002–2003 Innominate Security Technologies AG. All rights reserved.

Innominate Security Technologies AG  
Rudower Chaussee 29 • 12489 Berlin • Germany  
Telefon +49 (0)30- 6392-3300 • Fax +49 (0)30- 6392-3307  
<http://www.innominate.com/>

“Innominate” and “mGuard” are trademarks of the Innominate Security Technologies AG.

No part of this document may be reproduced or transmitted in any form, by any means without the prior written permission of the publisher. All other brand names or product names are trade names, service marks, trademarks, or registered trademarks of their respective owners. Contents are subject to change without notice.

Document Number 1419-057

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Traditional Solutions . . . . .	3
1.1.1	Software Solutions . . . . .	3
1.1.2	Dedicated Appliances . . . . .	3
1.2	Embedded Security Technology . . . . .	3
1.2.1	External Device . . . . .	3
1.2.2	Core Board . . . . .	4
1.2.3	Customized Appliances . . . . .	4
<b>2</b>	<b>Software Platform</b>	<b>4</b>
2.1	Transparent “Stealth” Operation Mode . . . . .	4
2.2	Router Operation Mode . . . . .	4
2.2.1	Native Address Translation . . . . .	5
2.3	Operating System . . . . .	5
2.3.1	Linux Base System . . . . .	5
2.3.2	Filesystem . . . . .	5
2.4	Firewall . . . . .	5
2.5	VPN . . . . .	5
2.5.1	IPsec Standard . . . . .	6
2.5.2	Encryption/Hashing Algorithms . . . . .	6
2.5.3	Hardware Acceleration . . . . .	6
2.5.4	Authentication Mechanisms . . . . .	6
2.5.5	Extensions . . . . .	6
2.5.6	Transparent “Stealth” Mode . . . . .	6
2.6	Content Scanning . . . . .	6
2.6.1	Protocol Analyzer . . . . .	6
2.6.2	Virus Scanning Engine . . . . .	7
2.7	Configuration and Updating . . . . .	7

# INNOMINATE SECURITY TECHNOLOGIES AG

2.7.1	Updates . . . . .	7
2.7.2	Configuration . . . . .	7
2.8	Rescue System . . . . .	7
2.9	Customization . . . . .	7
<b>3</b>	<b>Hardware Platform</b>	<b>8</b>
3.1	Processor . . . . .	8
3.1.1	Intel IXP425 . . . . .	8
3.1.2	VPN Performance . . . . .	8
3.2	Non-volatile Memory/Flash Memory . . . . .	8
3.3	RAM . . . . .	9
3.4	Interfaces and Peripherals . . . . .	9
3.4.1	Ethernet Interfaces . . . . .	9
3.4.2	Serial Interface . . . . .	9
3.4.3	Supplementary Interfaces . . . . .	9
3.4.4	Watchdog . . . . .	9
3.5	Customization . . . . .	9
<b>4</b>	<b>Software Developer Kit</b>	<b>9</b>
4.1	Cross Compiler Edition . . . . .	9
4.2	Native Development Support Edition . . . . .	10
<b>5</b>	<b>Conclusions</b>	<b>10</b>
<b>A</b>	<b>Technical Data</b>	<b>10</b>
	<b>Bibliography</b>	<b>10</b>

## Abstract

Today's security solutions are implemented by either software on the system to be protected or by special appliances intended for large organizations. Innominate's embedded security technology is prepared to fill the gap between these traditional approaches.

## 1 Introduction

Computer systems connected to the Internet are exposed to various threats, including direct attacks to services offered, attacks against traffic between the computer system and other hosts, and malicious software of various kinds. The threats have changed over time. Direct attacks became more present with increasing bandwidth on the Internet for both outgoing connections (allowing an attacker to work efficiently when searching for vulnerable systems) and incoming connections (allowing attackers good access to the systems). Viruses in the past were often distributed by infected software on physical media. Today viruses and other malicious software are mostly transferred by email or by download. New threats have become increasingly common due to the use of the Internet for business transactions, namely eavesdropping or intersection of messages and data.

A new field of security issues arises from the tendency to interconnect different communication domains into one large network. Traditional concepts in industry and administration had clearly separated networks for departments or organizational units. A network in the factory – being mission critical – was not connected to other parts of the company, maybe even using incompatible standards for hardware and software. Today the market demands fast time-to-market cycles at lowest costs, which can only be achieved by an efficient and flexible interoperation between technical and organizational units: sales, engineering, manufacturing, logistics, management... Of course, this interaction is highly sensitive with respect to reliability and security.

Therefore a security concept has to be realized for each computer connected to a network to protect both the computer, with its software and data, and the communication to the peers.

## **INNOMINATE SECURITY TECHNOLOGIES AG**

### **1.1 Traditional Solutions**

Currently both software based solutions and dedicated appliances are available. Software based solutions are computer bound and therefore apply to single computers in a stand alone, corporate or mobile environment. Dedicated appliances are currently only available on enterprise level to protect a number of computers in a LAN. Stand alone systems and mobile users are bound to software solutions.

#### **1.1.1 Software Solutions**

Various software solutions are available to protect computers, including firewalling, virus scanning and encryption techniques. Depending on the operating system (Microsoft Windows, Apple, Linux, etc.) these software solutions may be available as part of the base system or are provided by add-on software. The protection provided is on a per-system basis and can be “personalized” to meet specific requirements. The setup required is normally beyond the scope of average user’s skills. While the installation of a virus scanning toolkit can be done in an automated fashion, the configuration of a VPN with X.509 certificate authentication requires very specific technical knowledge.

All software solutions have the disadvantage, that they can be disabled or circumvented by attack software, so that their protective function is no longer available. Depending on the setup, it is also possible that a user accidentally (or intentionally) disables the security functionality. The security offered by pure software solutions running on the computer to be protected is therefore limited.

#### **1.1.2 Dedicated Appliances**

It is therefore common for companies to protect their internal networks by dedicated security appliances, realizing security functions on the enterprise level. These appliances are designed to handle large amounts of traffic and lots of connections in parallel. Most of these appliances are PCs or Workstations running dedicated applications.

The operation of an enterprise level security appliance is normally done by trained personal and/or under a support contract. As only security applications are running on these systems and no user operation is allowed, the security level is much better than that of personalized software solutions. On the other hand, the protection is only applied at the gateway against external attackers. Networks are often unprotected against internal attacks.

### **1.2 Embedded Security Technology**

With today’s technology it now becomes possible to bridge the gap between software solutions protecting single computers and large security appliances. Newly released network processors allow the building of inexpensive security appliances, that can be deployed on a per-computer basis. These appliances combine the advantages of both per-computer software solutions and dedicated security appliances:

- The protection is focused on a single computer. It therefore applies to all sources of attacks (including internal attacks) and is available also to stand alone and mobile computer systems. It can be configured to match the special requirements of the system to be protected.
- The embedded security appliance is still operating completely independent from the computer’s software and therefore cannot be disabled or circumvented, offering the same level of protection as “traditional” security appliances.

These embedded security computers can be designed in several ways offering different features.

#### **1.2.1 External Device**

The most universal type of device is an external security system, that is installed between the computer and the normal network connection. By realizing a “dongle-style” box that is inserted between the computer and the normal Ethernet cable, most applications can be covered. In order to make use simple, the device is transparent to the host computer, the configuration of which must not be changed when

## INNOMINATE SECURITY TECHNOLOGIES AG

the device is introduced. The device “learns” about its network configuration from the Ethernet frames running through it.

Firewalling can easily be performed at the full wire speed typically used today (100Mbit/s). Even more: cryptographic hardware acceleration makes it possible to operate VPN connections at throughput values touching the wire speed of the physical connection. Thus, it even becomes possible to encrypt the complete network traffic without significant performance impact.

### 1.2.2 Core Board

The “dongle-style” device is also suitable as an add-on for already existing systems like vending machines, slot machines, etc., when supplied as a single board, the “mGuard Core”. It can be introduced into the housing of the system and be supplied directly from the other system’s power supply.

### 1.2.3 Customized Appliances

Beyond the mGuard Core board and the dongle-style device, the mGuard hardware and software solutions are flexible platforms to provide customized solutions for particular purposes: new and additional functions implemented into the mGuard software, adapted hardware to match particular requirements.

## 2 Software Platform

Depending on the application scenario, the functions offered by mGuard are of different interest for the users. While firewalling is of common interest, a private user has limited application for VPN functionality, as he seldom has a peer to connect to. The virus scanning feature however is important. A user inside a company may need VPN to reach other computers with strict access limitations. Mobile (roaming) users greatly benefit from the VPN functionality, allowing them to access their company’s resources.

The configuration and update options differ similarly. Private users want to configure their security devices with a simple setup dialogue. As they may use their security devices on different computers, an interface using a standard web-browser meets their needs best, as no additional software installation is required.

Whatever the requirements are, the flexible mGuard technology is able to cover it.

### 2.1 Transparent “Stealth” Operation Mode

A major feature of the mGuard technology is its transparent operation. Normally security appliances act as IP routers, therefore requiring their own IP addresses and subnet setup. Using them for mobile applications means that the setup has to be adjusted for new locations with respect to the network environment.

Transparent firewalls have been built in the past, but only with respect to packet filtering aspects. mGuard’s transparent operation includes building VPNs and downloading software and configuration updates without becoming externally visible. This is realized by inserting the additional packets into the data stream using the client computers network parameters, thus working “piggy back”.

The transparent “stealth” mode should therefore be applied for applications with changing configurations, e.g. in DHCP environments as often used in offices or roaming scenarios. It is also very handy in applications where lots of single entities are equipped with individual security devices: the security devices do not require the setup of individual subnets.

### 2.2 Router Operation Mode

Additionally to the transparent “stealth mode”, the mGuard can also be configured to operate in the traditional router mode. This allows to use the mGuard as a normal VPN firewalling router.

## INNOMINATE SECURITY TECHNOLOGIES AG

### 2.2.1 Native Address Translation

In addition to static routes the mGuard implements NAT (Native Address Translation) to protect information about the internal network structure and to support the typical scenario of provider based access: the Internet connections is done over a link for which only one IP address is provided.

**Port Forwarding** Port forwarding support allows to specifically configure access permissions to internal resources.

**PPPoE Support** A very common scenario for NAT routers is the use behind a DSL modem to connect to the Internet. By supporting the PPPoE protocol in addition to static routes, the mGuard can be used as a DSL router.

## 2.3 Operating System

The security computer itself is running a complete operating system, as the tasks involved are too complex to be accomplished by a single application. This operating system is Linux, which is known to be a robust UNIX like system with several security features being already part of the base OS. Linux in its core is an OpenSource technology allowing inspection of the code and extensions where necessary.

### 2.3.1 Linux Base System

Innominate's mGuard is based on the Linux system kernel being enhanced with several extensions. A collection of tools and applications is added forming the base operating system. The system is specially built for the mGuard not relying on other distributions.

### 2.3.2 Filesystem

The operating system and data are stored in a journalling flash filesystem on the device (see Section 3.2), allowing easy updates and offering the opportunity to install additional tools and applications as required. The journalling flash file system is specially designed for embedded environments, providing high reliability and wear levelling.

## 2.4 Firewall

A powerful firewalling solution is already part of the Linux kernel: Netfilter [2]. Netfilter is a state-full firewall software with connection tracking and good extension options.

Several modifications are added by Innominate to allow fully transparent operation, since VPN packets must run "piggy back" on the normal data stream.

The firewall behavior is subject to several settings depending on the usage policy. A single computer user may want to allow all outgoing connections but no incoming traffic. On the other hand incoming connections may be required for certain services.

A centrally administrated device may have more restrictive settings allowing only certain outgoing connections or may even enforce only traffic that is sent through a VPN channel.

It is therefore possible to set firewall rules such that additional connections may be allowed or prohibited.

## 2.5 VPN

Remote access to resources at distant locations has recently gained popularity. Several techniques for secure remote access are available. While the TLS/SSL and the SSH (Secure SHell) protocol provide secure tunnel for single applications, a VPN (Virtual Private Network) is a powerful tool to fully provide the complete set of services to a remote user or location.

## INNOMINATE SECURITY TECHNOLOGIES AG

### 2.5.1 IPsec Standard

The mGuard supports the IPsec standard for VPN connections [6]. The implementation is provided by the FreeS/WAN project [3], with several add-ons to provide additional algorithms and extensions.

### 2.5.2 Encryption/Hashing Algorithms

The IPsec standard covers the use of the DES and 3DES encryption algorithms, packet authentication is performed using the MD5 or SHA-1 hash algorithms [9, 11]. Additional algorithms are currently discussed for inclusion into IPsec, the most important being AES for encryption and SHA-2 for hashing [10, 12]. Support for these additional ciphers is provided based on the current drafts being published by the IETF.

### 2.5.3 Hardware Acceleration

In order to utilize the special cryptographic hardware acceleration features of its host processor, Innominate has extended the IPsec code accordingly.

### 2.5.4 Authentication Mechanisms

In order to establish a VPN connection, both peers must identify themselves. While the PSK (Preshared Secret Key) method is supported for compatibility reasons, the use of public key authentication with X.509 certificates is the typical and preferred authentication method.

### 2.5.5 Extensions

Other protocol extensions are being worked upon. One major problem with the IPsec standard “as is” lies in the inability to pass through NAT (Native Address Translation). This problem can be handled by extensions on the NAT firewall itself, but not all firewalls support this feature. An IPsec protocol extension – currently in IETF draft status – to encapsulate the traffic into UDP packets has been added, that modifies the IPsec connections to properly pass through NAT firewalls.

### 2.5.6 Transparent “Stealth” Mode

In combination with the specific firewall and routing setup of the mGuard, transparent “stealth” VPN properties are provided. The mGuard analyses the destination addresses of traffic passing through it and redirects packets for certain destinations to the VPN module. By using this technique, the mGuard provides VPN services to devices or computers that normally do not support IPsec or removes the computational load from the computer. As the mGuard acts in place of another computer system (not router), it uses transparent mode for this service.

## 2.6 Content Scanning

Even though being a more or less “low tech” attack, large damage is still caused by “malware” attacks. Virus attacks are focused on Microsoft based operating systems, due to their insufficient security measures and design problems.

### 2.6.1 Protocol Analyzer

Virus scanning is performed on complete items, not on data streams, therefore emails and other files transferred have to be extracted and temporarily stored in memory. This is accomplished by an application level protocol proxy built into mGuard. The proxy software analyses the data exchange between the peers based on the protocol and extracts the payload (files, emails).

Rules allow to define what connections have to pass the protocol proxy, based on the peer of the connection and the protocol spoken. This allows to separate between “insecure” peers, for which the scanning has to be performed, and “secure” peers, for which no scanning is required. A secure peer could for example be mail server with a built-in virus scanning facility; a typical example would be a company’s mail server (that might be connected to via VPN).

### 2.6.2 Virus Scanning Engine

Innominate uses the Kaspersky Anti-Virus [7] engine to provide the virus scanning services. Updates are provided by Kaspersky to keep the virus database up-to-date. Updates are loaded automatically by the mGuard.

## 2.7 Configuration and Updating

The different functionalities offered must be configured and maintained.

The firewall setup only offers a few options and will not be changed often. Security problems in the Netfilter system as well as in the Linux kernel have been found in the past, so that updating might be needed, but not on a frequent basis.

The VPN software will require software updates on a regular basis for the foreseeable future, as both the standard undergoes changes and the Linux implementation is target of ongoing developments.

Because the virus scanning software has to be prepared to detect new viruses, updates have to be made available on a very frequent basis. New viruses are found and multiple patterns for recognition are generated everyday. It isn't practical to replace the complete engine (having a size of several MB) everyday, but most virus scanning programs provide a means to add single patterns for new viruses.

### 2.7.1 Updates

The frequency of required updates makes it necessary to keep the software of the security device on a re-writable medium and to provide a package management system that can handle independent updates of each of the system's components. An automatic update is required for the virus scanning software, as updates are very frequent and should not be postponed due to the high speed at which viruses spread.

Updates for other software components can be performed as well. The mGuard software platform is built modular, such that the software packages providing single functions may be updated. New functions can be installed.

The update can be performed by uploading new software packages to the system. The package management system assures that the system is always in a consistent state. The correctness and authenticity of the provided packages are checked by cryptographic signatures.

### 2.7.2 Configuration

The configuration of the device is performed over an easy to use web-interface. This allows to manage the mGuard without having to install additional management software, just using a standard TLS/SSL enabled web-browser.

## 2.8 Rescue System

The highly flexible mGuard concept allows to configure a lot of settings, to update software, and to install additional software that was self-designed or might have been provided by a third party. Consequently a rescue concept to recover from unwanted configuration settings or software failure has been designed in.

Simple devices having a fixed software only allowing user configuration can easily be recovered by removing the user data and settings and then re-enabling the factory defaults. This is not true for the mGuard, as parts of the system software might have been altered or removed. Therefore the mGuard is prepared to load a copy of the factory provided standard software via network interface. When using the rescue button in a pre-defined manner the mGuard looks for a network boot server and tries to reload the mGuard software. The rescue and installation process is protected by several security mechanisms including cryptographic signatures.

## 2.9 Customization

The use of a standard UNIX-like operating system allows the integration of other applications or configurations. Based on the Software Developers Kit (SDK, see Section 4), customers can implement their own applications or extensions.

### 3 Hardware Platform

The complexity of the functionality provided requires the use of a full featured operating system. The hardware platform must therefore be a processor that can handle all aspects of a modern operating system including memory management. Other components required are volatile and non-volatile memory and interfaces.

#### 3.1 Processor

A recent development in microprocessor development are SoC (System on Chip) and network processors for embedded applications. These processors provide full 32bit functionality including memory management, so that a UNIX like operating system can be used. The processor cores are either ARM [4] or MIPS based and are targeted for embedded low power applications. Manufactured with actual technology, a performance of 400-600DMIPS can be reached. The development of cores and technology are driven not only by the network processor market but even more by the market of small mobile computers (palmtop computers), so that further significant improvements can be expected.

The network processors are embedded processors with interfaces specially focused for network applications, here Ethernet interfaces are of importance. With the change of the export regulations of cryptographic products by the US government, it is now also possible to integrate cryptographic accelerator hardware into standard products.

##### 3.1.1 Intel IXP425

For the mGuard, Intel's IXP425 network processor has been chosen. The IXP425 is based on Intel's XScale core, a specially optimized ARM compatible design. The IXP425 does not simply have Ethernet controllers attached to the internal bus systems, but features NPEs (Network Processing Engines). The NPEs perform the actual task of sending or receiving network frames, unloading the processor core. Even more, the NPEs also provide hardware acceleration for cryptographic algorithms: DES, 3DES, MD5, SHA-1 (AES is being added in the B-stepping of the processor).

Starting with the IXP425, new models are added to the IXP4xx family of processors, allowing a broader choice between very economic and very powerful solutions.

##### 3.1.2 VPN Performance

The VPN throughput is determined by two major parts: the handling of the network packet and the application of the cryptographic algorithms.

**Software Implementation** Typically these operations are performed by the processor core of a computer system and the throughput is mainly determined by the CPU intensive task of encryption or decryption. The throughput achieved by the XScale core is suitable to match the full performance of today's DSL links as found in SOHO environments.

**Hardware Implementation** A significantly higher performance can be achieved using the IXP4xx with hardware acceleration. The specialized hardware implementing these algorithms achieves extremely high encryption speeds. Furthermore the processor core is not even loaded with the task of controlling these operations, as this management task is performed by the NPE. The processor core resources therefore can fully be used to manage the handling of the network packets.

Innominate has integrated the hardware acceleration interface into the IPsec component to achieve very high VPN throughput, depending on the processor version even coming near to the wirespeed of today's 100Mbit/s network cabling.

#### 3.2 Non-volatile Memory/Flash Memory

The operating system and configuration data have to be kept on the device, which must be running independent from the computer system to be protected. On the other hand, it must be updatable at all

## INNOMINATE SECURITY TECHNOLOGIES AG

times. Therefore flash memory is used to hold the operating system and configuration data (see Section 2.3.2).

### 3.3 RAM

All network processors including the IXP425 are currently equipped with SDRAM interfaces. Due to the increasing popularity of PDAs, low power versions of dynamic RAM recently became available, allowing to keep the power consumption of the mGuard at its low level.

### 3.4 Interfaces and Peripherals

For the external “dongle-style” device described in Section 1.2.1 only two Ethernet interfaces are required and accessible. The mGuard Core board provides additional interfaces to be used in embedded applications.

#### 3.4.1 Ethernet Interfaces

Current Ethernet installations use the 100Tx twisted pair technology. These installations are supported by the network processors having the standardized 100Mbit/s MII (Media Independent Interface) supporting the Ethernet protocol. To provide the connection to the physical media, PHY chips are used that handle the analog signals on the wire and negotiate physical parameters (wire speed) with the switch/hub. Automatic cross over detection (AutoMDIX) is provided. For the external “dongle-style” device one connector will be a CAT5 cable mounted directly. The similar add-on board has one RJ45 jack and one on-board connector to be used with a special plug.

#### 3.4.2 Serial Interface

The mGuard board is equipped with a serial RS232 interface including an isolating transceiver.

#### 3.4.3 Supplementary Interfaces

An additional connector makes available an I2C-bus interface, allowing to connect additional sensors, interface circuits, or memory.

#### 3.4.4 Watchdog

Correct function of the mGuard is supervised by a hardware watchdog circuit. An automatic reset is performed on failure.

### 3.5 Customization

Customized versions of the mGuard hardware, providing other or additional interfaces, memory etc. can be built basing on the available platform.

## 4 Software Developer Kit

In order to install additional applications onto the mGuard, software must be built to match the target platform. Therefore compilers must be available generating the necessary code. Tools to download the applications are required and various support tools can help in developments.

### 4.1 Cross Compiler Edition

In order to run pre-developed applications, a set of cross compilers running on another host system is sufficient. The cross compilers build working executables that can be downloaded and run on the mGuard.

## 4.2 Native Development Support Edition

Active development of mGuard applications can be performed more efficiently when having a full tool chain available at both the host system and the target platform. This full tool chain includes cross compilers to build on a host system and native compilers to build on the target platform itself. Additionally, development support tools, debuggers, and testing tools are provided.

## 5 Conclusions

The Innominate mGuard technology offers a large flexibility. The predefined stand-alone solution provides security “out of the box”. Customization of hardware and software allows to cover a broad range of applications.

## A Technical Data

Processor	Intel IXP4xx
Core frequency	266–533 MHz
Cryptographic Hardware Acceleration	DES, AES, SHA-1, MD5 (Version dependent)
Flash Memory	8–16 MB
SDRAM	32–64 MB
Ethernet Interface 1	RJ45 Jack
Ethernet Interface 2	Cable with RJ45 Plug (mGuard) or PCB connector (mGuard Core)
Serial Interface	RS232 with PCB connector (mGuard Core only)
Power Supply	5 V, max. 500 mA Optional: External Power Supply
Operating System	Innominate Embedded Linux
Operating Modes	Stealth and Router
Firewall	Configurable Ruleset
VPN Support	IPsec with extensions
Virus Scanning	Protocol Proxy

## References

- [1] 3COM 3CR990 Datasheet <http://www.3com.com/>
- [2] Netfilter Firewall <http://www.netfilter.org/>
- [3] FreeS/WAN IPsec Implementation <http://www.freeswan.org>
- [4] ARM Architecture <http://www.arm.com/>
- [5] Intel Network Processors <http://www.intel.com/>
- [6] IETF IPsec work group: <http://www.ietf.org/html.charters/ipsec-charter.html>
- [7] Kaspersky Anti-Virus: <http://www.kaspersky.com/>
- [8] FIPS: Federal Information Processing Standard, published by NIST (National Institute of Standards and Technology), U.S.A.: <http://csrc.nist.gov>
- [9] DES/3DES: FIPS PUB 46-3: DATA ENCRYPTION STANDARD
- [10] AES: FIPS PUB 197: ADVANCED ENCRYPTION STANDARD
- [11] SHA-1: FIPS PUB 180-1: SECURE HASH STANDARD
- [12] SHA-2: FIPS PUB 180-2: SECURE HASH STANDARD