VIA PadLock Security Engine

The World's Fastest x86 Military-Grade Security Engine

Technology Brief

VIA Technologies, Inc.

August 2005

Contents

Diagrams and Tables

I The Growing Importance of Computer Security

Every day, computers become a greater part of our digital world. Individuals, companies, governments and all manner of organizations are increasingly relying on them as a tool for communicating, transacting, creating, transferring and storing information.

People are storing more confidential aspects of their life on their personal computer than ever before, from financial and official identity information to private correspondence, photos and videos, and business information. Moreover, they are increasingly transmitting this information over unsecured Internet connections to friends, business associates, and commercial websites.

Businesses are completely reliant on IT as the principal medium for the creation and storage of company documents and information, so much so that almost every piece of sensitive information, from employee records to the whole spectrum of financial, operational, competitive, pricing, research and other data will be transferred across a network and stored on a hard drive at some point, whether created within the office or at facilities overseas, or by mobile executives on the road. Governments, too, recognize the efficiencies of the effective implementation of IT, and use it to create, store, and process information on their millions of citizens, as well as highly sensitive strategic documents of national importance.

Unfortunately, computers and their connections are seldom completely secure, opening the door to malicious attacks by hackers using techniques, such as:

- Lifting of data and personal information through the use of worms
- Identity theft through phishing attacks
- "Lunch time attacks", where hackers steal data through physical access to a PC during an employee's lunch break
- Exploitation of operating system weaknesses
- Exploitation of inadequate firewall technology
- "Man-in-the-middle" attacks, where hackers put themselves between two communicating parties and tap into the information being exchanged.

Through the local storage and communication of information, users have inadvertently started a new chapter in the fight against hacking and information theft.

Data Theft from Individual Users

The theft of any sort of data from a user can be devastating to the victim. As well as the material loss when an expensive computer is stolen, there is the loss of personal information and the potentially far greater financial losses that can ensue from its fraudulent misuse. On top of this, the emotional distress caused by the invasion of privacy can also be huge, as the deliberate hacking into a user's computer to steal information closely equates to physical burglary, whereby someone purposefully breaks in to steal your valuable and/or sentimental belongings.

Using the techniques described, hackers can steal credit card numbers, government identity information, and online bank account details to steal money directly, or illegally take on users' identities in order to make purchases using their financial and personal information. They can also resell personal information to criminal organizations that misuse the data for fraudulent intentions.

Hackers also steal passwords, photos and documents to deface or delete personal web sites, generate malicious emails, or use hacked systems to launch attacks against other computers.

These sorts of attacks and their consequences are seen across all levels and types of user; the news articles illustrate the growing awareness of the nature of the problem.

Hackers' New Strategy is to Steal Identifying Information

By Jon Swartz / USA TODAY
July 26, 2005

Instead of trying to crash corporate, government and university computers, hackers are focusing on stealing personal information such as your Social Security or credit card numbers from them, a new survey says.

Police say one type of criminal specializes in stealing names, addresses, birth dates, driver's license numbers, Social Security numbers, account logons and passwords. Another type makes use of stolen identifications to finance all aspects of elaborate schemes to move electronic goods and cash out of the United States.

Hackers Make Way for Criminals, Experts Say

By Lucas van Grinsven, European Technology Correspondent (Reuters)
Tue Jul 5, 2005

AMSTERDAM (Reuters) - Spotty teenage hackers who set off global email viruses are being replaced by serious online crooks whose stealth attacks don't make headlines but cause more damage, security software makers said on Tuesday.

"Two years ago we stayed up all night, concerned about a great mass-mailing worm," said Mario Juarez, a product manager at the security business unit of U.S.-based Microsoft.

"Today, we worry not about a virus that will take every machine down, but that may attack one machine or a set of machines," he said in an interview at a Microsoft Tech Ed developers conference.

"What you see more of are a variety of attacks that are carried out to make money, such as stealing credit card details or threatening a Web site with a denial of service attack unless it pays then money."

Data Theft from Businesses

Businesses are also lucrative targets for hackers. Through the use of all the described techniques, hackers seize company servers and gain access to valuable financial, employee and customer data which can be harvested to initiate bank or credit card fraud, or erased from the servers, with disastrous consequences.

Exposure of the theft of confidential customer information can destroy consumer confidence, especially in service industries such as banking or insurance where customer trust underpins the business, and can ruin a company's reputation. It is therefore no surprise to find some surveys reporting that around **90% of businesses that lose company data from such a disaster go out of business within two years**[1].

Moreover, the threat is growing. As executives become more mobile, an unprecedented volume of sensitive corporate information is being transmitted from notebooks across networks far beyond the protection of the company's internal network security set-up, such as from wireless hot spots at airports or over the Internet at home, and so is increasingly open to interception.

The local storage of company data on notebooks also makes it vulnerable to physical theft. With today's notebooks featuring hard drives as large as conventional PCs and delivering equivalent performance, notebooks are increasingly acting as mobile desktops for executives. When one takes into account the fact that as many as **10% of notebooks are stolen every year**[2], the inherent risk of the theft of critical data crippling a company is growing at an alarming rate.

The top news article on this page illustrates the scale of the problem, with hundreds of thousands of innocent people unwittingly exposed to potential identity and data theft due to the carelessness or misfortune of a single employee.

The bottom news article highlights the enormous potential for fraud enabled by spyware, one of the tools of the hackers' trade, facilitated by its ability to illegally divert private corporate financial and operational data.

Laptop Theft Puts Customer Data at Risk

By Paul McDougall, InformationWeek
March 30, 2004

A division of GMAC Financial Services has been quietly informing about 200,000 of its customers that their personal data may have been compromised because of the theft of two laptop computers from an employee's car at a regional office near Atlanta.

Massive ID Theft Ring Uncovered

Jaikumar Vijayan, Computerworld
Monday, August 08, 2005

Officials at Sunbelt Software, a Clearwater, Florida-based vendor of anti-spyware tools, say the company stumbled upon a massive ID theft ring that is using a well-known spyware program to break into and systematically steal confidential information from an unknown number of computers worldwide.

Sunbelt's research showed that the information being uploaded to the remote server included chat sessions, user names, passwords and bank information, he says. The bank information included details on one company bank account with more than $350,000 in deposits and another belonging to a small California company with over $11,000 in readily accessible cash, he says.

[1] Source: London Chamber of Commerce and Industry, UK
[2] Source: Gartner Group

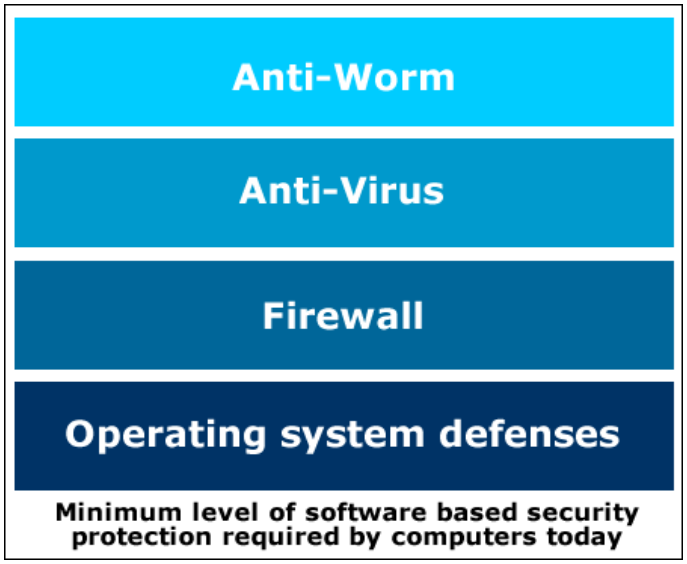
What's Being Done?

In the face of the rising tide of attacks, the software industry has mushroomed, with numerous companies springing up developing applications aimed at combating individual security attacks, such as anti-virus software and firewalls. Their efficacy is based on their ability to dynamically counter new threats, which is normally proportional to the strength of encryption used.

However, in an attempt to provide maximum protection against attacks from several fronts, users tend to install multiple security applications, which usually results in sluggish system performance and can disrupt running applications such as DVD playback, causing picture stutter. This is due in part to system bandwidth limitations when running multiple programs in the background and to the fact that the considerable computational complexity of encryption algorithms can individually utilize most of a processor's resources, even when running at speeds of 3GHz. The impact is even greater on notebooks, where processor efficiency directly affects battery utilisation; users often experience significant reductions in battery life when security software is enabled and layered.

As a result, frustrated users sometimes remove the security software altogether from their computers, or disable some of the applications in order to reduce the drain on their processor, but by doing so leave their system more vulnerable to attack.

Figure 1: Minimum Security Applications Running In Memory On Today's PCs



Therefore, if software is not the best solution to provide the necessary protection while ensuring the best user experience, with too many applications competing for processor time, then the answer must lie in hardware.

Some hardware design companies have identified the problems associated with software protection and have attempted to develop solutions that allow the offset of

these processor-intensive security computations to other hardware. The last three years have seen the integration into microprocessors of NX Execute Protection that prevents worm proliferation, the introduction of the Trusted Platform Module chip into high-end computers, and secure network processors in networking devices to encrypt network data. These products use hardware to offset the complex computational processes used in protection mechanisms, in order to allow the system to:

- Allocate resources to user applications rather than security applications
- Increase the strength of protection through the use and combination of more complex encryption algorithms
- Hide valuable primer data that is used by hackers to thwart protection mechanisms in a separate part of computer.

Whilst successful to a degree, all have been developed as a reactive response to individual threats, rather than as the result of a holistic approach towards enabling fully transparent security.

The advent of the VIA PadLock Security Initiative in 2003 marked the first practical implementation of a comprehensive set of hardware-based security tools to tackle the principal threat areas, and represents a major step forward in creating a robust security platform architecture for the first time.

II VIA PadLock Security Initiative

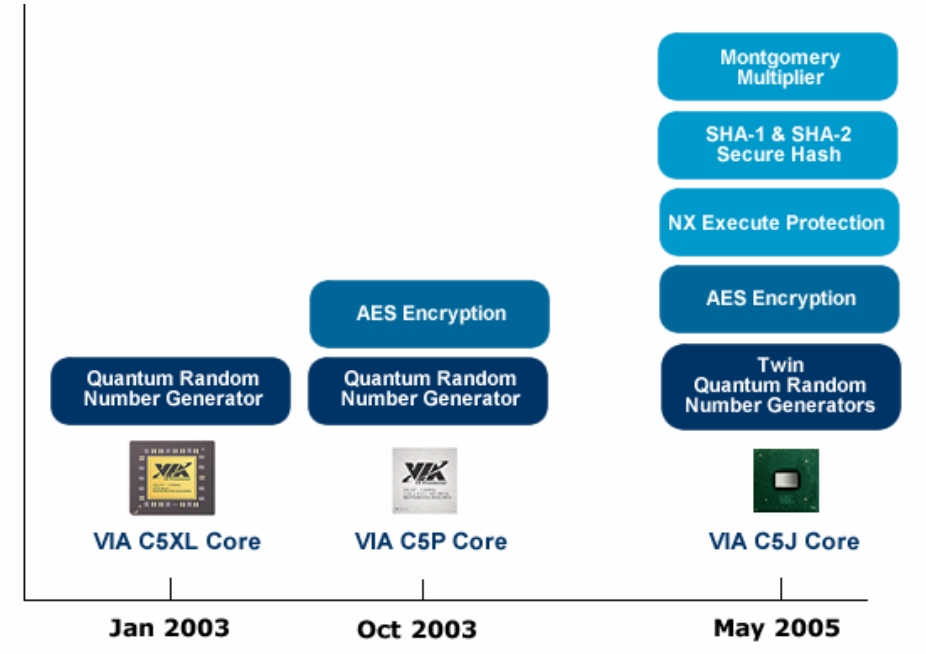
The VIA PadLock Security Initiative represents a pioneering approach to practical pervasive security, providing the most practical, efficient, and cost effective way of combating the onslaught of computer security issues across the x86 platform. Through the development of extensive suites of world-leading hardware and software technologies, VIA has combined the inherent efficiency and power-saving benefits of hardware-based random number generation and high level cryptography into the VIA PadLock Security Engine, the world's fastest encryption engine integrated into VIA processors.

Based on government-implemented open standards, the VIA PadLock Security Engine provides military-grade technologies that allow software developers to offer transparent security in applications by providing all the tools required to secure information with little or no impact on system performance. This technology, initially released in 2003, is the result of VIA's proactive approach to empowering developers with the tools to build a dynamic digital fortress that protects users' valuable personal and corporate information.

Evolution of the VIA PadLock Security Engine

The VIA PadLock Security Engine has been integrated directly onto the die of three successive VIA processor cores and has been continually enhanced over three distinct stages into the world's fastest and most feature-rich x86 security engine, as illustrated in Figure 2 below.

Figure 2: Security Features Integrated into VIA Processors by Core



Stage 1: Random Number Generation

VIA first implemented security functionality with the introduction of the VIA C3™ and VIA Eden™ processors based on the ground-breaking C5XL 'Nehemiah' core in early 2003, by designing an exceptional random number generator, the VIA PadLock RNG, directly onto the processor die.

Random number generation is of paramount importance, forming the very basis of the encryption process as the source of the keys needed to secure information, and its entropy[3] largely dictates the strength of both symmetric and asymmetric encryption processes in terms of their difficulty in being predicted, guessed or calculated. Put simply, the stronger the keys, the stronger the level of security. As the primary building block of security, this was the appropriate starting point for the future development of VIA PadLock.

The VIA PadLock RNG harvests its entropy using the quantum randomness experienced by oscillating particles at the sub-atomic level, providing large and exceedingly unpredictable random numbers at unprecedented speeds[4] well in excess of any software application available. Unlike the pseudo-random number generation seen in software applications, the VIA PadLock RNG does not rely on human-generated or –defined conditions to generate its randomness, such as keystroke patterns or mouse movements that can become predictable. Moreover, being implemented at the hardware level makes it extremely difficult to hack.

Stage 2: Advanced Cryptography Engine Phase 1

The first integration of cryptographic functionality came in October of the same year, with the release of a new range of VIA C3 and VIA Eden processors based on the enhanced, lower power C5P 'Nehemiah' core. Building upon the early VIA PadLock foundation, these processors integrated a powerful hardware-based AES encryption engine, the first of a two-stage implementation of the VIA PadLock Advanced Cryptography Engine (ACE).

With the VIA PadLock ACE, the benefits of hardware execution are the most striking, not only in the ground-breaking speed of this US-Government standard encryption, but also in the fact that it allows the offset of the extremely complex computations inherent in cryptography algorithms to the engine, enabling the encryption of data in real-time with little or no system performance degradation normally experienced by applications using a software based process and thus allowing security applications to run transparently in the background.

Stage 3: Advanced Cryptography Engine Phase 2

With the launch of the VIA C7™ processor family based on the C5J 'Esther' core in May 2005, VIA unveiled the most comprehensive VIA PadLock Security Engine to date, including new technologies to:

[3] Amount of randomness experienced during generation. Perfect randomness has an entropy of 1.
[4] The VIA PadLock RNG has been independently tested by Cryptography Research Inc.; the report is available for download on the VIA website.

- Operate and compute security calculations separately, so that hackers can not access valuable primer data used in computations;
- Process the computations used by encryption in real-time - its engine, the fastest of its kind in the world, allows this real-time encryption across multiple sources and runs at speeds of up to 350 times that of a serial ATA hard drive;
- Include all the essential tools required to make information secure. These tools again have been scaled to military specification, allowing end users to have peace of mind with applications that enable this technology;
- Use the theories of quantum mechanics to create large, truly random numbers quickly and efficiently.

Pervasive Military-Grade Security

Incorporated into the latest version of VIA PadLock are five key security features. Powered by the world's fastest x86 security engine, these five features, when enabled, provide unbreakable protection on a VIA PadLock-enabled device:

- **Secure Hash Algorithm SHA-1 and SHA-256:** Encrypting information at rates of 5 gigabits/second
  - Largely considered unbreakable by the security community, SHA-1 requires an enormous amount of computational power to even attempt to break it (a few thousand computers and about 10 years of your life!), while SHA-256 has been estimated to take about the age of the universe to break.

- **AES Encryption** (ECB, CBC, CFB, and OFB modes): Encrypting information at rates of up to 25 gigabits/sec (at 2GHz), up to 200 times faster than a standard network connection, and up to 25 times faster than the speed of most hard drives
  - These latest symmetric encryption tools are US Government standard and are used by governments and militaries around the world.

- **Montgomery Multiplier:** An invaluable tool to assists the enormously complex asymmetric algorithms of RSA/public key encryption

- **NX Execute Protection:** Builds a virtual wall in system memory to prevent most worms from proliferating

- **Random Number Generation:** Two quantum random number generators creating highly unpredictable random numbers at rates of 12 million per second.

VIA's industry leading, proactive approach to securing information empowered by the VIA PadLock Security Engine has given hardware-based security and encryption centre stage in the fight to protect information.

III Enabling Pervasive Security on the x86 Platform

The VIA PadLock Security Engine, through its inclusion of the world's fastest x86 security engine and a comprehensive set of tools, can act as a protection agent in a number of key business and personal cryptographic applications, and can be implemented on computers, server appliances or indeed any x86 based device.

Secure Hash Algorithm

This type of encryption is used in three ways:

1. To provide a unique signature for authentication, or to verify the contents of a message, providing clear evidence if a message has been intercepted, decrypted and its contents modified.
2. To transmit data (between two parties) across an unsecured connection such as the Internet. Common business applications include:
   - Businesses wanting to establish a secure and private connection between the employee and the main office.
   - For companies wanting to communicate confidentially to their employees in the field, a Virtual Private Network can be established using this type of encryption as the foundation for communication.
3. To encrypt data on storage devices such as hard drives, compact discs and removable media such as USB memory sticks, providing security in the event of physical theft and lunch-time attacks.

AES Encryption

AES provides powerful security through large and thus hard-to-guess key sizes, and is used to:

1. Securely stream information continuously across an unsecured Internet connection.
2. Encrypt data on a hard drive or device in real time to stop hackers using Internet-based tools to read information on the drive, or to stop thieves of notebooks reading the contents of the drive.

AES encryption is particularly well suited for electronic devices such as PCs, IP and mobile phones, PDAs, firewalls, and wireless standards, such as the high-speed 802.11g standard.

Montgomery Multiplier

Public key encryption provides ultra secure communications across unsecured connections in the following two ways:

1. Allows transmission of secure information across unsecured mediums, such as when companies want to broadcast messages and vital information to their employees without knowing their location (important in wireless networks).
2. Enables secure one-to-one communication across unsecured mediums, such as secure Voice over IP (VoIP) and videoconferencing.

Random Number Generation

Speed and high quality randomness (unpredictability) of random numbers are both essential in cryptographic processes to maintain sustained secure connections, such that random number and thus key generation happens at a faster rate than the speed of data transmission. This is particularly relevant for these applications:

1. Continuous secure wireless network transmissions
2. Virtual private networks
3. Hard drive encryption

Illustration: Virtual Private Networks

Virtual private networks (VPNs), used primarily by businesses and growing in popularity, provide a clear example of the securing of exchanged information. Protection of data is performed through cryptographic tunneling mechanisms that ensure the necessary confidentiality, authentication and message integrity required to communicate across unsecured mediums.

Implementations of virtual private networks are seen in a number of forms that include IPsec, SSL and PPTP. All use various encryption protocols such as SHA-1 and AES algorithms to secure data transmitted. By using the VIA PadLock Security Engine, a virtual private network can offset the encryption algorithm computations to the engine and use the power of the x86 security engine to protect information transmitted in real-time.

Offset of encryption computations to VIA PadLock can also be used secure any form of data transmitted across the Internet or unsecured network, including protection of Voice over IP conversations, banking data submission, and instant messaging.

IV Competitor Comparison

As is shown in Figure 3 below, both the VIA C3 and VIA C7 families of processors provide a far more comprehensive set of security features than are available in equivalent products from competitors, clearly demonstrating VIA's strategic commitment to provide a holistic approach to security.

Figure 3: Comparison of Security Features in x86 Mobile Processors

	AMD Sempron M	Intel Celeron M	Intel Pentium M	VIA C3-M	VIA C7-M
Secure Hash	No	No	No	No	Full SHA-1 & SHA-256 5Gb/s peak
Worm Protection	NX Execute Protection	No	NX Execute Protection	No	NX Execute Protection
Encryption	No	No	No	Full AES encryption & decryption ECB,CBC,CFB, OFB hardware modes 25Gb/s peak@2GHz	Full AES encryption & decryption RSA hardware acceleration (Montgomery Multiplier) CBC,CFB-M,AC, CTR modes 25Gb/s peak
Random Number Generation (RNG)	No	No	No	2 Hardware RNGs	2 Enhanced Hardware RNGs up to 12Mb/s Feeds output to SHA engine

In fact, as Figure 3 shows, the only security feature currently offered by both AMD and Intel® in their processors is enhanced anti-worm (NX Execute) protection. Whilst effective in stopping the propagation of worms on NX-enabled computers, this common feature provides only one of the many building blocks required to build a secure digital fortress in a computer.

V VIA PadLock Security Engine: A Closer Look

The VIA PadLock Security Engine empowers secure computing by adding extra functions to the main processor that give programmers the world's most comprehensive set of military-grade tools to make data unreadable to unauthorized users (data encryption) and help prevent attacks from hackers and worms.

These tools are a hardware implementation of the latest encryption algorithms that the government and military organizations around the world use to secure their information and communications.

A hardware implementation means that all the hard work to make information safe is done by circuitry inside the computer, rather than by using the operating system and software resources.

In addition to encryption tools, the VIA PadLock Security Engine in the VIA C7 processor family provides hardware based mechanisms to help prevent the spread and damage caused by computer worms.

To aid the level and sophistication of the encryption techniques used in the VIA PadLock Security Engine, a twin engine quantum random number generator is also included. This uses the world's best techniques to create these unpredictable numbers at speeds of up to twelve million random numbers (12,000,000) per second[5].

The VIA PadLock twin random number generators use the theories of quantum physics to create unpredictable random numbers. These random numbers play an important role in the techniques used to make information safe, in that the more unpredictable the numbers are, the harder it is for hackers to break into data.

This comprehensive set of military-grade security tools is powered by the world's fastest x86 security engine that enables real-time encryption, authentication and decryption of data across networks, storage devices and memory.

Why VIA PadLock Security is Stronger than Software

There are many software applications that provide similar tools to the VIA PadLock Security Engine. So what makes VIA PadLock better?

One of the main reasons is that the VIA PadLock Security Engine is housed in its own section within the processor. This means that hackers who could have used techniques to gain access to the valuable data during the encryption process find it difficult if VIA PadLock is used.

The VIA PadLock Security Engine also performs the encryption and decryption calculations at many times the speed than is possible in software implementations of the same techniques. This is achieved through the offset of computations to VIA

[5]Based on the VIA C7 processor. VIA C3 and VII Eden generate random numbers in the order of around 8 million per second.

PadLock, which through the power of the world's fastest security engine performs the computations at speeds faster than real-time. In fact, not only can VIA PadLock do them faster, but by offsetting the calculations, it frees up the processor to do the job the user wants it to do, such as playing a movie smoothly.

The quality of the keys used to secure data and the subsequent strength of encryption is far superior to software-based processes. Key generation using the VIA PadLock Security Engine allows developers to capture true randomness experienced only in the sub-atomic world and apply it to the generation of a truly random key. This thwarts hackers who rely on the statistical repeatability experienced in software random number generation and in the subsequent key generation to break secure code.

These key differences in the implementation of hardware based encryption versus software based encryption have a substantial impact on an applications ability to secure data quickly and efficiently.

Figures 4 & 5 provides a visual demonstration of these key differences.

Figure 4: AES Encryption Without VIA PadLock

Without the VIA PadLock ACE, unencrypted data bottlenecks when being processed into secure data. This increases significantly the load on the processor and reduces the potential throughput of the encrypted text.

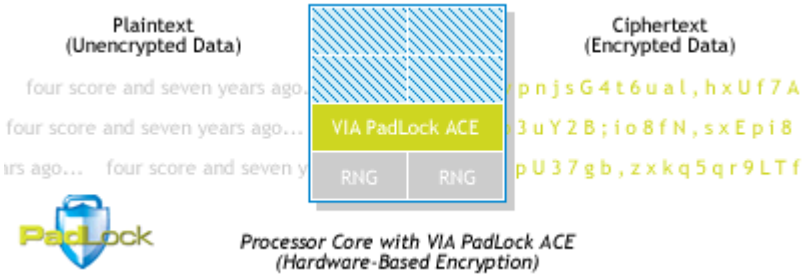


Figure 5: AES Encryption with VIA PadLock

In contrast, with the VIA PadLock ACE, unencrypted text can be converted to secure data in real-time without bottlenecking system resources.

Ease of Implementation for Developers

This comprehensive set of security tools based on open standards is enabled fairly simply through a set of extra instructions in the instruction set of the main processor, and avoids the issues associated with requirements for device drivers and/or alterations to the operating system.

Unlike other hardware security solutions, the VIA PadLock Security Engine has been enhanced to eliminate the need for extra program overhead and avoids potential stability and sequential issues caused by the offsetting of computations to security hardware such as a co-processor. In fact, its encryption and protection functions are executed through a simple set of extra instructions in much the same manner as addition and subtraction instructions are performed.

Developers are given full documentation and a suite of prewritten routines, with no licensing or developing fees involved, to empower easy and scalable inclusion of the technology in applications. Developers are further empowered by the inclusion of a comprehensive software development kit bundled free with recent VIA processors.

Both the software development kit and documentation are available for free download from the VIA Arena technology portal website at:
http://www.viaarena.com/default.aspx?PageID=5&ArticleID=75.

VI VIA PadLock Security Engine Performance

VIA PadLock is the world's fastest x86 security engine. This means that every security feature in the VIA PadLock Security Engine operates faster than any other security product on the market, including network processors that offer some similar features.

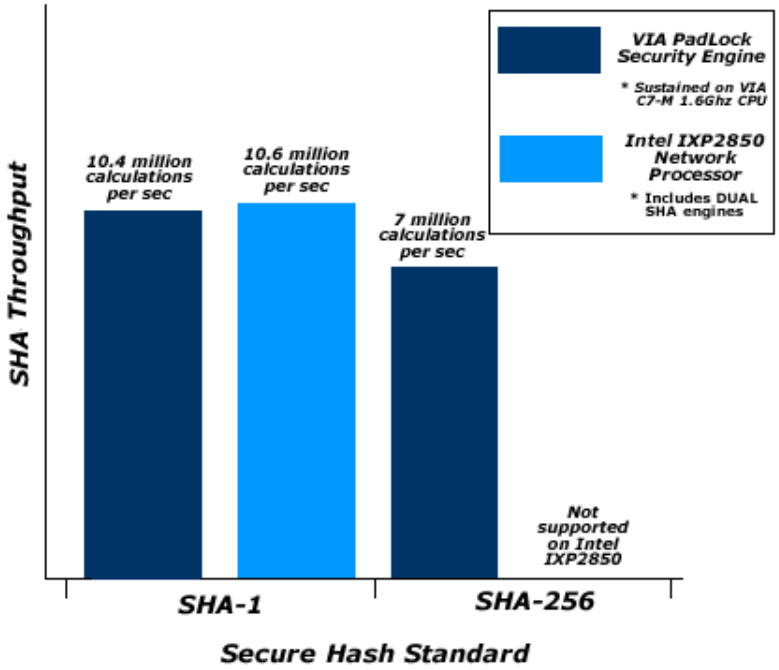
In fact, so comprehensive is the feature set of the VIA PadLock that no other hardware product on the x86 market approaches it; therefore, in order to demonstrate the effectiveness of VIA PadLock in relation to other hardware solutions, this section compares it with its closest competitor for each comparable feature.

Secure Hash Algorithm

The first feature of the VIA PadLock Security Engine to compare is the Secure Hash Algorithm. In comparison with Intel's flagship secure network processor, the Intel® IXP2850 processor, VIA PadLock performs both SHA-1 and SHA-256 algorithms whereas the Intel® IXP2850 performs only SHA-1 and uses dual SHA engines to boost the throughput of algorithms.

As Figure 6 shows, even using dual SHA engines the Intel® IXP2850 Network processor can only compute SHA-1 functions 1.8% faster than is possible using the single but highly effective SHA engine in the VIA PadLock Security Engine.

Figure 6: Throughput Comparison of Secure Hash



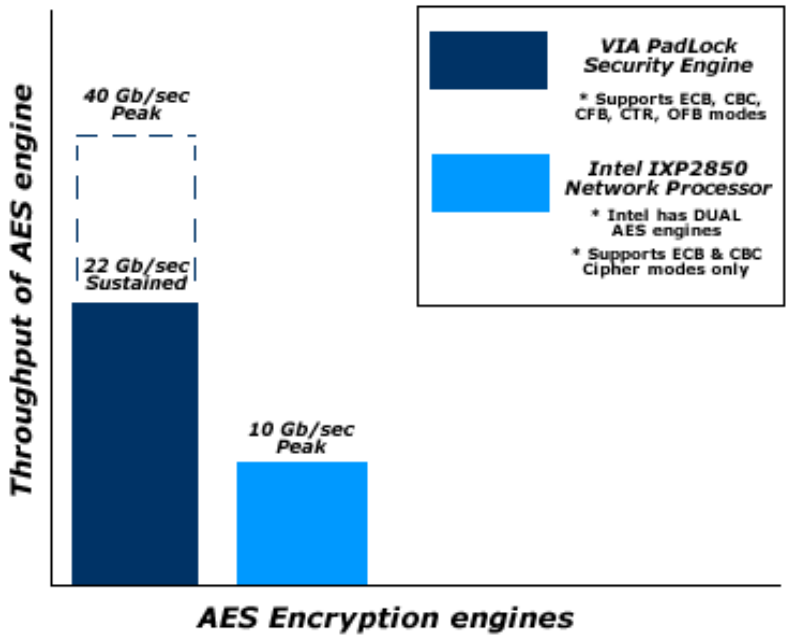
NB: The Intel® network processor supports SHA-1 only, whereas VIA PadLock supports both SHA-1 and SHA-256.

AES Encryption

AES encryption is widely adopted for securing data due to the immensely complex computations required by its algorithm, placing great demands on processors to execute. There are several hardware security solutions providing an AES encryption function, but the leading competitor against the VIA PadLock Security Engine is again the Intel® IXP2850.

As Figure 7 illustrates, this network processor designed to provide real-time encryption and decryption on high-speed Ethernet connections operates at only a quarter of the speeds possible using the VIA PadLock Security Engine.

Figure 7: Throughput Comparison of AES Encryption



NB: The Intel® network processor is a separate processor designed for supporting high speed network products that generates 10Gb/s peak throughput through the implementation of dual AES engines and supports only two modes of AES encryption.

Throughput when compared to software based AES encryption on a system two and a half times the speed of a VIA PadLock enabled processor also provides world leading results.

Figure 8 demonstrates the capability to encrypt 1GB of data on a 2003 release of the VIA Eden processor with the earliest version of the VIA PadLock ACE versus the ability of a 2.4GHz Intel Pentium 4 to perform the identical encryption.

Figure 8: AES Encryption Throughput Comparison: VIA PadLock Security vs Intel® Pentium® 4 Processor

Encryption Performance comparison with the VIA PadLock ACE						
Cipher Engine	**1GHz VIA Eden-N Processor**			**2.4GHz Intel Pentium 4 processor**		
	Encrypt (in Mbps)	**Decrypt (in Mbps)**	**Ciphering 1 GB data (in Sec)**	**Encrypt (in Mbps)**	**Decrypt (in Mbps)**	**Ciphering 1 GB data (in Sec)**
EBC	15073.28	133255.66	0.57	106.79	93.90	8.006
CBC	6196.13	6844.87	1.23	100.64	89.38	8.450
CFB	6315.29	6699.24	1.23	100.58	99.72	7.988
OFB	3245.59	3311.29	2.44	10.83	100.98	7.928
Avg. CPU Utilization	54%			99%		

As the table in Figure 8 shows, the 1GHz VIA Eden-N processor using the VIA PadLock Security Engine can encrypt 1GB of data in only 0.57 seconds whereas it takes the 2.4Ghz Intel® Pentium® 4 processor over 8 seconds to perform the identical encryption using software based AES encryption

These results also demonstrate the true power of the VIA PadLock Security Engine and illustrate its most important benefit: reducing the main processor utilization. Under these tests, the average processor utilization (i.e. how much of the processor's power is used in the test) for the 2.4 GHz Intel® Pentium® 4-based computer is 99% - leaving only 1% of the processor's resources to be allocated to functions other than the encryption of data.

The VIA 1GHz Eden-N processor, on the other hand, utilizes only 54% of the processor's power during the same task, leaving 46% available for other applications requiring the processor.

Montgomery Multiplier

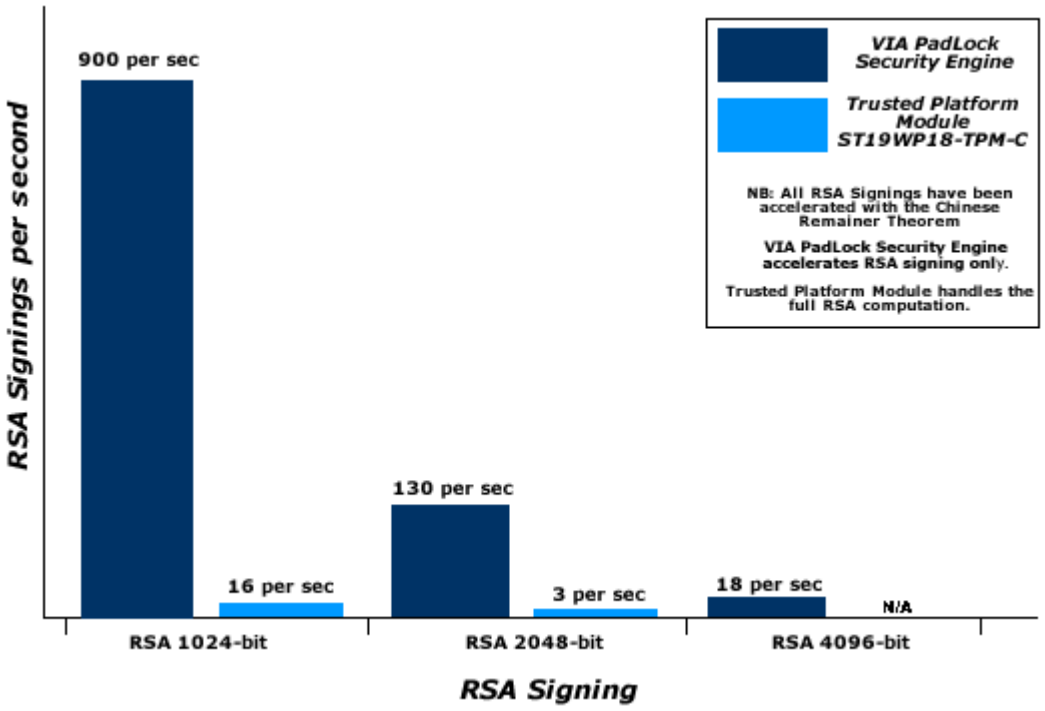
The VIA PadLock Security Engine includes technology for the processing of military-grade asymmetric encryption algorithms. Using a Montgomery Multiplier, VIA PadLock accelerates all forms of public key encryption including RSA algorithms.

This accelerator allows VIA PadLock enabled applications to perform up to 900 RSA signings per second. The closest competitor for this feature is the Trusted Platform Module (TPM), which allows only up to 16 RSA signings per second.

However, the Trusted Platform Module's RSA function differs slightly from the VIA PadLock Montgomery Multiplier in that the TPM computes all parts of the RSA algorithm whereas the VIA PadLock accelerates in hardware the algorithm's ability to perform the computations.

Figure 9 illustrates a throughput comparison of RSA signing through the Chinese Remainder Theorem of the STMicroelectronics Trusted Platform Module and the VIA PadLock Security Engine.

Figure 9: Throughput Comparison of RSA Signing



NB: The TPM handles the complete RSA sign whereas the VIA PadLock Security Engine accelerates the process through the implementation of a Montgomery Multiplier that can be applied across all asymmetric encryption systems.

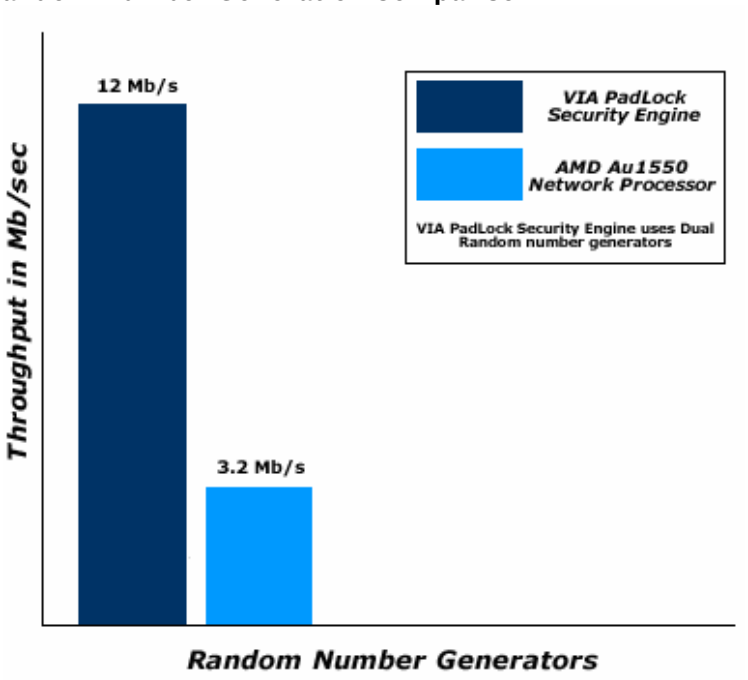
As Figure 9 illustrates, the VIA PadLock Security Engine can accelerate the computation of RSA algorithms to allow an output of up to 900 RSA signings per second. The Trusted Platform Module on the other hand outputs only 16 RSA signings per second. In other words VIA PadLock enabled applications can perform RSA signings 57 times faster than what is achievable on the Trusted Platform Module. VIA PadLock, unlike the TPM, also accelerates the world's strongest version of the RSA algorithm – 4096-bit keys at a rate of 18 signings per second.

Random Number Generation

The VIA PadLock Security Engine embedded in the VIA C7 processor family also includes dual quantum random number generators. These generators can produce up to 200 million bits of raw data per second. However, to further increase the quality of numbers generated, the engine also includes a whitener[6] function that increases the randomness (entropy) of numbers generated. When enabled with the whitener, the engine can output up to 12 million truly random bits per second.

VIA's closest competitor in speed and quality of random numbers generated is the AMD Au1550 network processor. As Figure 10 below demonstrates, this produces random numbers at a rate of up to 3.2 million bits per second (peak performance).

Figure 10: Random Number Generation Comparison



NB: VIA PadLock implements dual generators to achieve this throughput and uses the whitener to increase the level of entropy.

When compared to the VIA PadLock dual quantum random number generators, the AMD Au1550 produces random numbers four times slower.

[6] A whitener reduces bias and correlation in random number generated by VIA PadLock.

References

Intel IXP2850 Network Processor: Intel's latest, most comprehensive and fastest network processor.
http://www.intel.com/design/network/products/npfamily/ixp2850.htm

AMD Au1550 Network Processor: AMD's network processor solution.
http://www.amd.com/us-en/ConnectivitySolutions/ProductInformation/0,,50_2330_6625_10509,00.html

Trusted Platform Module: Developed by ST Microelectronics on the specifications of the Trusted Computing Group
http://www.st.com/stonline/bin/sftab.exe?db=rosetta&type=query&table=469&filter-XJE010_def=ST19WP18-TPM-C

VII Hardware Security Compared

There is much talk in the industry and the media about the various solutions and 'fixes' to the various security threats affecting the computer market today; the most commonly compared hardware solution for the PC industry is the Trusted Platform Module (TPM). While the VIA PadLock Security Engine was shown to have superior performance than the TPM in RSA signing, how does VIA PadLock measure up overall against this and other hardware-based security solutions?

Trusted Platform Module

The Trusted Platform Module (TPM) is the creation of the Trusted Computing Group, a collaboration of hardware manufacturers who together define the specification for this module and its software, and produce it.

TPM is a separate hardware module that includes embedded software to provide asymmetric RSA encryption and to store keys used in the process in permanent memory for re-use in future encryptions. The Trusted Computing Group created this specification to be used as a building block for developers and manufacturers to strengthen their security solutions. To be integrated into a solution, the module requires hardware redesign and application re-engineering to offset the storage and computation of keys.

The VIA PadLock Security Engine includes a similar function in its set of tools that accelerates the asymmetric RSA encryption to empower developers to achieve up to 900 RSA signings per second in their applications, versus the 16 RSA signings per second of the Trusted Platform Module[7] (based on a 1024 bit key).

Figure 11: Feature Comparison: VIA PadLock Security Engine vs Trusted Platform Module

Feature	Trusted Platform Module	VIA PadLock Security Engine
AES Encryption	Not available	Full AES encryption peaking at 22Gb/sec
Random Number Generator	Included on-die	Quantum based calculations at 12 Mb/sec
Anti-Worm Protection	Not available	NX Execute Protection
Secure Hash	SHA-1	SHA-1 & SHA-256
RSA Algorithm	Handles full computational load of RSA at 16 signings per second	Accelerates RSA algorithm at 900 signings per second

[7] Based on data supplied with the ST19WP18-TPM-C implementation of the Trusted Platform Module. Data for both VIA PadLock and TPM has been accelerated through the use of the Chinese Remainder Theorem.

Whilst the TPM Initiative helps solves one part of the security puzzle, the VIA PadLock Security Initiative provides all the tools required to solve the puzzle safely without the need of alteration in hardware and provides those tools free for developers to integrate into their solutions.

Intel LaGrande Technology

Intel® LaGrande Technology is a future initiative announced by Intel that incorporates the Trusted Platform Module and provides security functionality, though not without extensive modification of hardware, operating system and user applications.

From information available, the Intel LaGrande initiative will involve hardware modifications to the processor and all supporting chipsets, and requires the inclusion of a Trusted Platform Module. The modifications will then be enabled through a two-step software process involving modification to the operating system, user applications and the device drivers. When implemented, LaGrande is designed to provide a wall of protection to core elements of the system enabling this technology to thwart information thieves by disabling their ability to use tools to hack the system.

The implementation date of LaGrande Technology is not currently available.

Network Processors

Primarily incorporated into routers and high speed network devices, network processors provide an example of the types of functions needed in hardware-based security solutions. Most include various forms and strengths of symmetric and asymmetric encryption and are used to create secure virtual private networks and secure connections in WAN environments. However, their use is generally confined to server and networking equipment, and has not yet spread to desktop or notebook computers or other x86 devices.

VIA PadLock Security Engine

In comparison to other hardware security solutions, VIA PadLock provides the most comprehensive solution for an x86 device, and one that delivers levels of performance unmatched by any other implementation. Furthermore, VIA PadLock is available today, at no extra cost, and with no alterations required to existing hardware and operating systems.

IX Summary

The VIA PadLock Security Engine provides a new, innovative and open-standards based solution to the problem of information security. This technology provides the world's most comprehensive set of military-grade building blocks for developers to create a digital fortress for any x86 based device that requires protection against today's threats. Powered by the world's fastest x86 security engine, these building blocks feature the latest government-standard symmetric and asymmetric tools, secure hash technology with anti-worm protection and two quantum based random number generators to provide an unshakable foundation for securing data.

Compared to other initiatives such as the Trusted Platform Module, the VIA PadLock Security Engine provides the foundation and complete set of building blocks to create a robust secure platform rather than addressing just one aspect of security.

With the power-efficient VIA processor platforms ideal for all x86 markets, from desktop and mobile PCs to networking and server devices, as well as a whole host of digital entertainment, commercial and other embedded devices, the VIA PadLock Security Engine is designed to make data security less of a worry to users, service providers and corporate IT departments alike.

By combining the inherent efficiency and power-saving benefits of hardware-based security functions directly onto the processor die with a range of flexible, intuitive software solutions that take advantage of these in-built hardware features and support for developers, VIA has taken the first real step towards enabling true transparent security services to protect any x86 based device.

VIA Information Links

For more information about the VIA PadLock Security Engine please visit http://www.via.com.tw/en/initiatives/padlock/

To download the VIA PadLock Software Development Kit, please visit the product and technical information portal VIA Arena at:
http://www.viaarena.com/default.aspx?PageID=5&ArticleID=75

Independent Reports on VIA PadLock

- Evaluation of VIA PadLock ACE encryption engine
  http://www.via.com.tw/en/downloads/whitepapers/initiatives/padlock/cri_evalution_padlock_ace.pdf
- Evaluation of VIA PadLock RNG
  http://www.via.com.tw/en/downloads/whitepapers/initiatives/padlock/evaluation_padlock_rng.pdf
- Evaluation summary of VIA PadLock RNG
  http://www.via.com.tw/en/downloads/whitepapers/initiatives/padlock/evaluation_summary_padlock_rng.pdf
- Evaluation of VIA C3 PadLock
  http://www.via.com.tw/en/downloads/whitepapers/initiatives/padlock/via_c3_padlock_evaluation.pdf

Disclaimer

Performance tests and ratings contained within this document are measured using specific computer systems and/or components and reflect the approximate performance of VIA products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For further information please contact your sales representative.