

VIA TECHNOLOGIES, INC.

ACE-CNIX

W H I T E P A P E R

The need for improved security

The development of smarter consumer devices and automated enterprise systems is leading to the increased need for higher security. The advancement of such devices and systems, bring convenience and efficiency through the use of ubiquitous networks. But the presence of a network connection inherently presents two issues with security: data in transit and data in situ.

Data in transit can be intercepted through a man-in-the-middle attack. In the event of such an attack, the confidentiality of intercepted data is compromised. Imagine if the communication had been between a company and a potential customer. The company could lose the potential customer to a rival company if the intercepted data was obtained by the rival company.

Data can also be easily stolen even if it is not in transit. Computer viruses and other forms of malware float around in the vast nebulous cloud of the Internet. Malware designers employ all sorts of methods from laying traps, proactive seek-and-destroy, to a digital version of the proverbial “five-finger discount”. Imagine if a company had a database of 1 million customers on a server. Suddenly, the company discovers that a rival company has been contacting their customers using information obtained from their database.

Current security solutions

So what can be done to halt such heinous acts of industrial espionage or invasion of personal privacy? In an attempt to address such security issues, various sorts of security technology have been developed to protect data, whether in transit or in situ. But most of these security solutions either have flaws, are complex to implement and maintain, or have significant costs for implementation.

VPNs to protect data in transit?

To date, VPNs have been proven to work well for protecting data in transit. However, the complexity of managing, maintaining, and upgrading existing VPNs can become an IT person’s nightmare. A 2-site VPN is not much to worry about. But when the VPN grows to 100 sites, adding another node can become a real headache.

In a VPN, every site connected to the VPN must be identified by the node to which it is attempting to communicate. Therefore in a 2-site VPN, site A has site B’s ID and vice versa. But in a 100-site VPN, every site would have to have 99 other site IDs. Imagine even adding 1 new site to a 100-site VPN. Expanding a

VPN can be tedious and laborious — resulting in many man hours and ultimately high costs for hiring specialists.

Firewalls to protect data in situ?

Today in any corporate environment, a firewall is a necessity. But is it enough? It has been proven that even firewall security can be breached. Firewalls should never be considered the be-all and end-all of network security. They are only the frontlines. One thing no firewall can protect against is physical infiltration.

For example, company A has a disgruntled employee. One day the disgruntled employee decides he will take some company secrets à la USB stick and either sell it to a rival company or start his own rival company. No firewall on Earth can stop the disgruntled employee.

The power within

Now that two of the major weaknesses in VPN and firewall solutions have been exposed, it is possible to define a security solution that can address the shortcomings. To recap, the following shortcomings were identified earlier: 1) exponentially increasing complexity with each additional new VPN site, and 2) failure to protect from the physical infiltration and theft of data.

When VIA first created the C3[®] line of CPUs, a visionary product was birthed. At the time, most people focused on the frequencies of the processors. Far ahead of its time with respect to integrated hardware security, the C3 was the first and only x86 processor to include a hardware engine designed especially for handling cryptographic encryption, decryption, and random number generation.

With each iteration of the VIA CPUs, advances in the CPU technology continued to bring faster and more efficient power usage — all the while never giving up on its integrated hardware security. Today the VIA Nano™ CPU — a fraction of the size of its predecessors — not only brings superscalar processing power to its integrated hardware security, but also an improved hardware security engine.

As the world's only x86 processor design company to integrate a security engine into the CPU, VIA has the distinct advantage for innovating in this area. The inclusion of an on-chip Advanced Cryptography Engine enables VIA's customers the unique opportunity to apply data encryption without the hassles of additional hardware. Organizations using VIA hardware can enable a range of security implementations that use data encryption as the central security strategy — making data free to be stored, processed, remotely accessed, or moved from place to place across a network without the worries of theft.

VIA is currently the only x86 processor vendor that has a range of security features embedded in the core of its products. These include a secure hash

algorithm, AES Encryption, Montgomery multiplier and a random number generator — all designed to offer customers an alternative security infrastructure based on the principles of data encryption.

So how does an integrated hardware security engine help with the aforementioned security issues? First off, the integrated hardware security engine greatly simplifies protected communication between members of an organization regardless of its size. The same technology that works for an organization of two people can just as easily work for an organization of 10,000 people. Instead of hiring security specialists to spend hours upon hours of costly labor setting up 100,000,000 different policies just for establishing site IDs of the 10,000-site VPN, all that is needed is a public key directory that can be accessed for sending protected data.

This is where VIA's visionary CPU architecture shines. With its integrated hardware security engine, an organization already using hardware with VIA CPUs does not need to worry about the complexities of integrating additional security hardware to their existing systems. A simple software update is all that is required to exploit the power within the VIA CPU

Secondly, the integrated hardware security engine can protect data by encrypting it so that if the data is stolen, it will be useless. Going back to the disgruntled employee example, assume company A is now using servers powered by VIA CPUs. The disgruntled employee sneaks in a USB stick and succeeds in copying company secrets and takes it home. Rival company B purchases the secrets, but finds that the data looks garbled and therefore company A's secrets remain secret.

Exploiting the power of VIA CPUs made easy

In an effort to help customers get the most bang for their buck, VIA launched a new service called ACE-CNXX (pronounced as "ace connects"). This service aims to help customers connect with VIA's resident security experts so customers can build their security infrastructure according to their requirements.

To qualify for the ACE-CNXX service, the customer needs to have purchased products from a list of eligible products. The customer then contacts VIA Embedded about the ACE-CNXX service. If the customer has already signed up for the ACE-CNXX service at the time of purchase, then the customer should communicate directly with VIA's ACE-CNXX technical support team.

When communicating with the ACE-CNXX technical support team, the customer needs to detail their security needs and provide detailed information about their hardware setup. The ACE-CNXX technical support team will then assess the situation and define a solution that will best fit the customer's needs. This includes providing a customized ACE SDK to the customer along with a recommended security solution.

After receiving the customized ACE SDK, the customer should build their own software to exploit the power of the integrated hardware security engine. The beauty of the ACE-CNX service is that the communication between the customer and the ACE-CNX technical support team does not stop after the customer receives the customized ACE SDK. If the customer faces a problem they cannot solve, the ACE-CNX technical support team will collaborate with the customer until the problem is solved. This ensures that the customer will have the confidence to continue developing their customized security application.

Scenarios

Data protection

Suppose Vaulton is looking to bolster their existing security infrastructure. After a security audit, Vaulton has identified a vulnerability that poses a serious threat to the security of their proprietary knowledge. Even with their state-of-the-art hardware firewall and iron-fist IT policies, Vaulton has a glaring hole. None of their data is protected from physical infiltration. Lucky for Vaulton, their IT department had just ordered new servers powered by VIA Nano™ processors.

Without having to make any more hardware purchases, Vaulton can now take advantage of the built-in hardware security engine in the VIA Nano processors. Vaulton contacts VIA to discuss how to make the most of the built-in security. After learning about the benefits of the new VIA ACE-CNX service, Vaulton decides to purchase the service. VIA coworks with Vaulton to develop a specific security solution that fixes the problem with Vaulton's security infrastructure.

Firmware and Software copy protection

AutoDeck specializes in developing car PCs. Their main value is in developing proprietary software that makes the car PC function less like a PC and more like a user-friendly consumer device. Having already successfully designed and sold 100,000 units of their first car PC design, AutoDeck is getting ready to develop an upgraded version.

Because of AutoDeck's experience using a VIA platform board, AutoDeck would like to build on their existing experience and take advantage of the great customer service they received from VIA. However, AutoDeck is a little concerned that their proprietary software can be copied and re-applied to the first version of their car PC. After discussing with VIA their security concerns, AutoDeck learns that VIA provides a service, called ACE-CNX, that will enable AutoDeck to add hardware-based copy protection to their proprietary software. AutoDeck decides that ACE-CNX is the way to go.

Telecommuting protection

Coolco is a hip company with the latest tech gadgets integrated into their network infrastructure. Not only is Coolco on the bleeding edge of technology, but Coolco gives its employees freedom to roam and telecommute — contributing to their hip image. Everybody wants to work there.

Most of Coolco's employees have a smartphone and notebook. Some employees do their work in coffee shops, while others check their email on the road. But with such heavy reliance on the Internet, security is a prime concern to Coolco's IT department. While Coolco has already implemented a VPN solution, the company's increasing number of numbers is giving their IT department a headache. Coolco is looking for a security solution that simplifies the tangled complexity of their existing VPN solution.

Luckily, fortune smiles on Coolco because all of the company's servers and standard issue notebooks have VIA CPUs. Without having to purchase additional hardware, Coolco can sign up for the ACE-CNX service and easily implement a security solution. VIA helps Coolco develop an on-the-fly encryption solution to keep their data protected while traveling on the Internet. And the sun continues to shine on Coolco as they find out that even their employees' home computers can still have on-the-fly encryption (although not as fast as with a VIA CPU).

Secure end-to-end protection

Bank Kaching has noticed the current trend in online banking and wants to get in on the action. But, Bank Kaching has no idea where to start. One thing Bank Kaching knows is they want to provide their customers with ultra tight security to give their customers peace of mind.

After hearing about the VIA ACE-CNX service, Bank Kaching decides to give the service a shot. VIA devises a plan to help Bank Kaching not only provide ultra tight security to their customers, but also increase their customer base. With help from VIA, Bank Kaching implements the security solution.

Bank Kaching officially launches a promotion for their new online banking service. Bank Kaching gives away free netbooks with VIA CPUs to every new account with a minimum \$500 deposit. The netbooks are preloaded with the security software VIA helped Bank Kaching to develop to securely connect to their online banking servers. Ka-ching!

Concluding remarks

Realizing that the power of the VIA CPUs were not being fully exploited by most customers, VIA decided to take action to ensure that all customers would have the chance to develop secure solutions without feeling lost. With the ACE-CNX

service, customers now have the assurance that they can embark on the endeavor of meeting increasing security demands and accomplish their security goals successfully with VIA's ACE-CNXX technical support team guiding them if need be.

To find out more about the ACE-CNXX service, visit <http://www.viaembedded.com> or contact VIA Embedded at embedded@via.com.tw.

