THE BUSINESS END OF DATA PROTECTION

SECURING DATA ON THE MOVE WHITEPAPER

SENETAS

Security without compromise

SENETAS
Security without compromise

THE BUSINESS END OF DATA PROTECTION

SECURING DATA ON THE MOVE

RECOMMENDED AUDIENCE:

Business managers, senior management, CEOs, CFOs, CIOs, CTOs, board members and company directors.

DESCRIPTION:

A business guide to the protection of data in motion through encryption. This paper has been created for business managers, to explain how data is vulnerable as it *moves* across data networks and why sensitive data should be encrypted. It can be used to understand the security issues and risks to data while it moves through computer networks. It will help you to navigate your way through what can otherwise be confusing technical information.

DO YOU KNOW WHAT HAPPENS TO YOUR DATA WHILE IT'S BEING TRANSMITTED TO ANOTHER LOCATION?

Most organisations underestimate the magnitude of risk to their business-critical data while it's in motion across public or private data networks.

If your data is somehow of value to others, that alone makes it a target for malicious attacks.

Encryption at Layer 2 in the network delivers best-practice data security with up to 50% greater network traffic speed and performance compared with Layer 3 encryption.

INTRODUCTION

The need to protect sensitive information within organisations is clear to us all. But do you really know what happens to your data while it is being transmitted to another location? From the moment data is in motion, you are actually no longer in control of it, and it can be easily and cheaply 'tapped' by cyber-criminals for all variety of unauthorised reasons.

In its 2012 Global Data Security Report, awarded information security experts – Trustwave, noted that 62.5% of data theft occurred while in transit. It also pointed to increasing cyber-criminal focus on data in transit.

Furthermore, data travelling through networks is not just exposed to risks of cyber-attack; there are also genuine risks of transmission to wrong locations. Human error and technical equipment failings are real risks that can manifest more often than you would think. The common issue that organisations face is a breach of data privacy and/or integrity as well as criminal damage such as the loss of valuable intellectual property, whatever the original cause.

However, these risks can be eliminated, and security assured, by automatically encrypting the data while it's in motion. If your data is sensitive – commercial, government or industrial – data, voice, video, or all three – it should be encrypted to protect your organisation and its stakeholders, especially when it leaves your control.

Consider this, would we ever mail unencrypted sensitive data? Would we leave unencrypted sensitive data on a laptop? Would we even hand-deliver unencrypted sensitive data? So, why would we ever transmit unencrypted sensitive data through a network?

It's often *assumed* that data networks are safe. The reality is they are not. Cyber-attacks, human error and equipment failings are all hazards that can lead to sensitive data getting into unauthorised hands. Ultimately, it's the encryption of data that provides genuine assurance that the encrypted data is useless to unauthorised parties – the last line of defence.

The optimal solution is not the protection of the data network; it's the protection of the data itself. By encrypting the data, you can be assured that however accessed by an unauthorised party, it is protected by that last line of defence. This is why governments and defence forces around the world have encrypted information for hundreds of years.

Typically, data networks used to transmit information are known as Layer 3, but when you encrypt Layer 3 networks, it's at a serious cost of up to 50% of network performance. On the other hand, Layer 2 networks do not suffer the same lost performance. They are used when high data volumes and performance needs demand more bandwidth and improved cost efficiency alongside best practice data security.

In this business guide, we take a look at the risks associated with data in motion across modern high-speed data networks, discuss the associated impact of cyber-crime, and explain some of the key components of data encryption along with where to encrypt data networks.

MISSION-CRITICAL CATASTROPHE

The 1999 Israeli Shayetet mission disaster is one of the most striking examples to underscore the criticality of encrypting sensitive data in motion. The Israeli secret service unit, Shayetet 13, transmitted a video detailing a planned top-secret military mission. Upon landing to commence their mission, the 12 mission operatives were unfortunately caught by surprise – all 12 were killed.

It was only 14 years later that revelations surfaced about the video having been intercepted during transmission without Israel's knowledge. Of course, the mission was doomed well before it commenced.

While a military example, this paper focuses on commercial risks and similar examples of why data encryption is also a serious business-critical issue.

BUSINESS DATA IS BOOMING

In recent years, the evolution of the high-speed network has had an enormous impact on business growth and performance. Business communications are now largely based on the collation, aggregation, storage, analysis and exchange of vast quantities of what's being called 'Big Data' – all of which places unprecedented demands upon core IT infrastructure, including the networks that move data around.

Essentially, fibre optic communications allow organisations to deal with more data, faster. This 'bandwidth boom' has not only revolutionised the way we act as consumers, it has also enabled most of the significant business trends of the 21st century. Trends such as Cloud computing, datacentre and desktop virtualisation, Bring-Your-Own-Device and workforce mobility are all recognisable innovations which aim to bring about greater efficiency and business performance.

But what of the threats to information security that accompany the growth of these data volumes and the networks that carry them? Many organisations using fibre optic cable networks internally and via service providers, mistakenly believe fibre networks are inherently safe. Unfortunately this is rarely the case, as telecommunications carriers often only offer the isolation of traffic or data without including best-practice data encryption.

THE 'TOTAL' THREAT TO DATA

The very same trends enabling business growth are increasing the threats to data security. The internet has become the de-facto medium for communication, and with virtualised systems and a more flexible workforce, more business is now conducted over public and private networks.

With an increasing number of publicised data theft stories, most organisations today are acutely aware about the ramifications of data security breaches and information 'loss' – damage to privacy and data integrity. The consequences range from revenue, intellectual property and customer data loss, damage to a company brand and reputation, costly legal liabilities, and the deterioration of customer trust and shareholder confidence. In some instances these 'data breaches' are considered a failing of corporate governance and even a breach of specific governance regulations.

While vast amounts of time and money are invested in securing data at rest (using intrusion detection systems, email and malware security, and firewall protection, etc.), organisations often underestimate the magnitude of the risk to their business-critical data while it's in transit across public or private data networks.

Intrusion detection, for example, is certainly important, but on it's own, it can lull an organisation into a false sense of security. It would be one thing if data was routinely kept secure within an organisation's perimetre walls, but most companies today need to send and receive data across the internet or external networks – locations which are immune to anti-intrusion and anti-virus protection.

Significantly, risk management principles indicate it's not a matter of 'if' there will be a data security breach, but rather 'when'! For this clear reason, the ultimate protection of data in motion requires a focus on protecting the data itself – ensuring that 'when' it's in unauthorised hands it is effectively useless. Therefore, that ultimate and genuine data protection is only made possible by encrypting it effectively.

In a climate of increasing cyber-criminal and malicious attack threats, organisations should regularly review their data security policies and plans. This would begin with assessing the types of data being handled and its corresponding sensitivity and value to would-be criminals. It is important to understand that if your data is somehow of value to others, that alone makes it a target for criminals.

Many organisations remain unaware that once their data leaves the perimetre of their control, it is open to attack and can be tapped with relative ease and little expense. Let's look briefly at how this is achieved.

TAPPING FIBRE – EASIER AND MORE WIDESPREAD THAN YOU THINK

According to Gartner, tapping fibre optic cable without detection is not only possible, but has been taking place for most of the last decade. This is a view shared by US security firm, the SANS Institute which states, 'It is alarming that there appear to be many organisations out there who are not aware of, and do not agree on, the ever increasing ease at which fibre optic cables can be attacked.'

So, how is it done? The technology that allows for fibre optic cable to be tapped, and for data to either be removed or added without breaking the connection, not only exists but is readily available. Fibre-clamping devices are available over the internet, legally, for as little as AUD$450.

The simple clamp bends the individual fibre, allowing some of the light to escape. This is sufficient to either extract the information travelling down the cable or to inject additional information. With high-speed networks handling up to 100 Gbps, it wouldn't take long to extract a significant amount of data.

So, if you can't prevent or detect fibre tapping, how do you secure your data in motion?

TECHNOLOGY FAILINGS AND HUMAN ERROR – THE INNOCENT DATA NETWORK BREACH

Before we look at how you protect data in motion, it's worth emphasising the risk of technology failings and human error. Risks to data are not limited to cyber-attacks alone.

Technology failings and errors caused by devices and technologies can unwittingly put sensitive data into unauthorised hands. Equally human error can innocently do the same. If your data is sensitive, the unexpected failings of technology and people can have serious consequences. The risks of such errors (often overlooked) can include information routed to an unintended destination by a faulty router.

It can be as simple as the wrong lead connected to a wrong port or a routing table error.

However by protecting the data itself through effective encryption, such technology failings and human errors do not lead to serious embarrassment – at the very least – or the even more serious ramifications discussed earlier in this paper.

ENCRYPTION – THE LAST LINE OF DEFENCE

The simplest and best approach is to provide protection that stays with the data, wherever it is being sent. Encryption does exactly that. Most organisations and executives are familiar with encryption, but what exactly is it, and what options are there?

At first glance, encryption seems an easy choice. After all, why expose confidential information to prying eyes when you can protect it with cryptography? This makes logical sense, because encryption ensures that when data falls into unauthorised hands, it is unintelligible and therefore rendered useless to a hacker, criminal or any innocent party who has received the data in error.

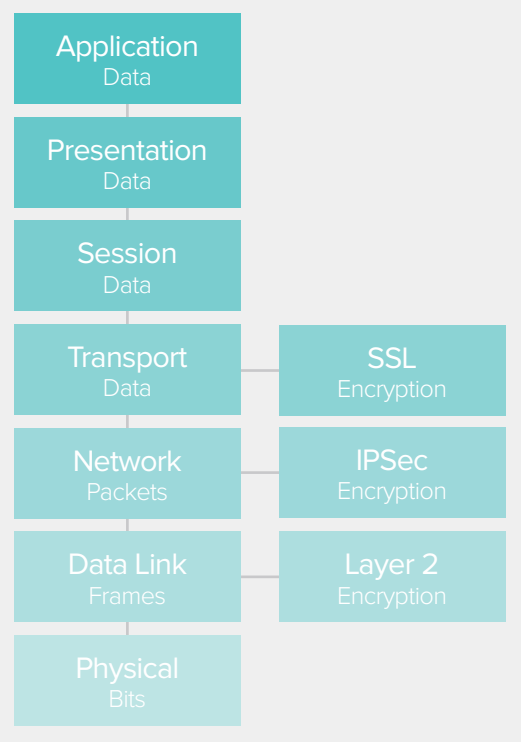
But before we get too far ahead of ourselves, let's look at where encryption should be applied.

WHERE TO ENCRYPT

This section is about as technical as this guide gets, but rest assured, we'll keep it simple and in practical business terms. The model for general networking comprises seven layers – as per the diagram on this page.

Layer 1 is the physical layer, comprised of the basic hardware elements of a network (cables, connectors etc.) Layer 2 is the data link layer, responsible for the transfer of data between devices on a network (Ethernet and fibre optic cable, for example). Layer 3 is the network layer, responsible for packet forwarding (such as IP – the internet protocol). Beyond that, we're looking at layers, which identify the software applications and the types of traffic flowing across the network.

If your data is traversing a geographically diverse public or private network, it is inherently insecure – this is as true for optic fibre networks as it is for other types of wired or wireless network. Given this, the question isn't whether or not encryption should be used; rather which approach to encryption offers the most secure and efficient solution.



BUSINESS BENEFITS – LAYER 2 VERSUS LAYER 3 ENCRYPTION

When it comes to encryption of data in motion, there are a number of options available, including:

- End-to-end encryption within applications
- SSL, Layer 4 encryption
- IPSec Standard, Layer 3 encryption
- Layer 2 encryption

It is generally accepted that the lower the layer, the more comprehensive the encryption and the more efficient the process. As such, Layer 2 and Layer 3 are most commonly chosen for encryption.

The next and important challenge lies in maintaining the performance and simplicity of a high-speed network while assuring the security and privacy of network traffic, whether that's voice, data or video.

Today, it is possible for the right encryption technology to provide *maximum* data protection *without* compromising data network performance. Let's look at how.

Layer 2 and Layer 3 encryption work in different ways. Layer 3 encryption devices are designed for IPSec encryption (standard internet encryption). IPSec uses a process that 'tunnels' the original IP packet in order to encrypt an IP 'header'. However, tunnels can result in an increase in overhead, complexity and, subsequently, network performance speed and processing time.

By comparison Layer 2 standalone hardware encryptors are optimised for Ethernet networks and fortunately don't need to tunnel the original IP packets in order to encrypt. This results in a *significantly* more efficient process – up to 50% greater network traffic speed and performance.

Naturally, organisations are always looking for an edge in network speed and performance, while retaining required levels of security. For this reason, Layer 2 encryption adoption is increasing the world over, while at the same time, Layer 2 has also come of age in affordability and accessibility terms.

In summary, when compared to encryption at higher layers, Layer 2 encryption has a number of distinct business advantages:

- Lowest impact on network performance
- No additional bandwidth overhead
- Reduced management complexity
- Transparent to media (voice, data, video etc.)
- Little or no configuration required
- Operates at wire speed up to 10Gbps

Ultimately, if the data your organisation moves through its data networks qualifies as being sensitive in any way to prying eyes, it should be encrypted. Only this approach provides the optimal assurance of protection – data privacy and integrity. At this time, the decision to use Layer 2 networks becomes compelling – less cost per gigabyte, lowest management overhead and best performance.

CONCLUSION

Increasing network speeds, new cloud and remote data centre services and more accessible network pricing introduces both advantages and security threats to organisations. The availability of greater bandwidth allows us to exchange information faster and more frequently, but the huge growth of often-sensitive data volumes transmitted across networks presents real risks.

The risks are real – from malicious attacks to innocent errors in transmission. Data networks are not inherently safe. Trustwave's 2012 Global Data Security Report makes that very clear. Furthermore with the exponential growth in information-rich data transmission and the rapid increase in data networks, the risks have never been greater.

Officially certified by independent international testing authorities, hardware-based data encryption at Layer 2 is the most effective way to protect data on the move, and that's because it's the only security solution that travels with the data on your own network, your service provider's network or any other network.

At the data network level, traditional Internet Layer 3 (IPSec) security is not well suited to modern environments. It is complex to manage, does not scale well to larger settings, and with its considerable overhead, can compromise network performance by up to 50%. Ultimately it delivers a less efficient cost per gigabyte.

Compared with Layer 3 (IPSec) encryption – Layer 2 networks can be secured and encrypted with dedicated appliances without any loss of speed and performance, minimal management, and greater reliability – resulting in a comparatively lower cost per gigabyte.

'IF ONLY WE ENCRYPTED THE DATA!'

Data has been encrypted for hundreds of years by governments and defence forces. Obviously enough, since cryptography was first invented, military leaders have looked to ensure that secret and sensitive messages would not be understood if and when they fell into enemy hands.

In days past the 'high-speed' network was a messenger on a fast horse. In more recent times it was microfilm, micro-data storage devices and other digital media. Importantly, any such secret or sensitive information was encrypted or 'codified'. Today, businesses and governments alike use 'high-speed' digital technologies to transmit their information on data networks.

So what has changed? Aside from 'network' types, nothing much. But too many organisations still fail to learn from the past. Risks are still taken, even when today, it's easier than ever to protect sensitive information by encrypting it. Today's encryption technology can ensure it could take up to 300 trillion years to 'crack the code'!

The failure to encrypt sensitive data has had serious consequences – the loss of reputation; litigation damages; risk of disaster, and even the deaths of many people. Here are just a few examples:

- **2011 & 2012** – Unencrypted command algorithms were stolen from a NASA laptop left in a car. Only the following year, the private details of 2,300 NASA employees were stolen from another unencrypted laptop.
- **2006** – An Australian Army Brigadier suffered major public embarrassment when she left sensitive, unencrypted information on an airplane seat. The media obtained the CD Rom and used it to embarrass the Australian Government and military's operations in Iraq.
- **2010** – A UK Nuclear power station manager left an unencrypted USB stick in a hotel room. It contained highly sensitivity business operations data.
- **2009** – In Canada, a $40m litigation was initiated against the Durham region, because the medical records of 83,000 patients were lost on an unencrypted USB stick.
- **2012** – The UK police force was fined £120,000 for losing secret information about 1,000 people, interviewed in a major drug investigation. It was a repeat offence.

Each case example in this very small sample had one key issue in common – all the devices were carrying data in transmission – with the data devices in transit. Obviously the best, and in fact, only way to properly protect such data is to encrypt it. Encryption is the last line of defence.

ABOUT SENETAS CORPORATION LIMITED

Senetas is an Australian listed public company (ASX: SEN), specialising in high-speed network encryption protecting data in motion whilst retaining maximum data network performance.

Senetas products are the world's only triple-certified encryptors of their type – Common Criteria (Australian and international), FIPS (US) and CAPS (UK) certification – for government and defence use and protect much of the world's most sensitive data.

Senetas secures: government information and secrets; defence and military information; commercially sensitive intellectual property, business and financial data; banking transactions; datacentre and Cloud services traffic; high volume CCTV networks; and critical industrial and infrastructure control systems.

Senetas uniquely designs, develops and manufactures in Australia. Senetas encryptors have market-leading performance characteristics and are trusted to protect data in motion in more than 25 countries.

These customers include high security organisations such as the US defence forces and Swiss banks.

www.senetas.com

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN series encryptors are supported and distributed globally by Gemalto N.V. under its 'SafeNet' encryption brand. Gemalto also provides pre-sales technical support to hundreds of accredited partners globally: systems integrators, networks providers, cloud and data centre service providers, telecommunications companies and network security specialists.

www.gemalto.com/enterprise-security/enterprise-data-encryption

SENETAS PARTNERS

Senetas works exclusively with leading systems integrators and network service providers across more than 35 countries worldwide.

Our master distributor, Gemalto, and its global network of partners have proven expertise in high-speed data networks and data protection.

What's more, Senetas partners are committed to investing in the latest technical training for network data protection, high-speed data encryption and customer needs analysis.

TALK TO SENETAS OR OUR PARTNERS

Senetas also works with customers' existing data network service providers, systems integrators and information security specialists to specify the optimal high-speed encryption solution for your needs.

The optimal specification of Senetas CN Series encryptors for your network data protection is dependent upon many factors, including IT and network environments, technical and business needs.

Wherever you are, simply contact Senetas to discuss your needs. Or, if you prefer, your service provider may contact Senetas on your behalf.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com