FROM CAESAR TO CYBER
THE CASE FOR ENCRYPTION WHITEPAPER

SENETAS
Security without compromise

SENETAS

FROM CAESAR TO CYBER

THE CASE FOR ENCRYPTION

Over the past 10 years, very few factors have had as much impact on business growth and performance as the evolution of the high-speed network. Business communications are based on the collation, storage, analysis andexchange of vast quantities of data; all of which places unprecedented demands upon the core ICT infrastructure.

Fibre optic communications allow organisations to deal with more data, faster. Whilst this is a very simple principle it has wide-ranging implications for the way we do business. 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.

- **Unified Communications**
- **Workforce Mobility**
- **Datacentre & Desktop Virtualisation**
- **Business Continuity**
- **Bring-Your-Own-Device**

In this publication we will take a brief look at the risks associated with data in transit across modern high-speed networks. We will talk about the associated impact of Cyber Crime and reflect on the need to secure data within both the public and private sectors.

We will highlight the role of encryption in securing data and explain some of the key components of data encryption along with where to encrypt. We will also outline the importance of the key global standards of accreditation for encryption technology and what to look for.

What we won’t be doing is talking about the nuts and bolts of encryption. The world of algorithms, keys, certificates, certification authorities and quantum key distribution will have to wait for another time.

RISK

Data has become an organisations most valuable asset and securing that data is a priority for any IT department. Whilst vast amounts of time and money are invested in securing data at rest, organisations often underestimate the magnitude of the risk to their data whilst it's in transit across the public or private networks.

> TA significant proportion of this cost comes from the theft of IP [ntellectual Property] from UK business, which we estimate at £9.2bn per annum. [1]

> TThe cost to UK business of security breaches has increased by more than 50% in the last 10 years and the scale of the threat is set to increase with 60% of companies expecting threat detection to get harder.". [2]

You may feel safe in the knowledge that you only store data on approved servers or storage media, that you only send data down the private carrier network and that any information exchanged over the web is controlled by access privileges and passwords. However, just because you've never had a report of data being lost or compromised, doesn't mean that it hasn't happened.

The Cabinet office published its first report into Cyber Crime in 2011; it estimates the cost of Cyber Crime to the UK to be £27bn per year.

As data has become more valuable, it has also become more vulnerable. Those very same trends that are enabling business growth are increasing the threats to data security. As the workforce becomes increasingly mobile, more systems become virtualised and more business is conducted over the public and mobile networks. The internet has become the de-facto medium for communication, with over 97% of all businesses making use of it.

The number of high profile incidents in recent years has been increasing – from the phone hacking scandal of the News of the World to the security breach that took down Sony's PlayStation Network as hackers gained access to the personal information of over 70 million users. The average UK company will be suffering security breaches on a daily basis; the bigger the business, the greater the number of breaches. Only 1% of UK businesses have a comprehensive approach to identity management and, worryingly, 20% of wireless networks are still unprotected.

1. Detica report in partnership with the Office of Cyber Security & Information Assurance

2. IDC Report, 2011

IMPLICATIONS OF A SECURITY BREACH

The implications for a serious breach of data security are wide ranging. Whilst the "big number" of £27bn per year is significant in its own right, what does that number mean to an individual organisation?

COMMERCIAL BUSINESS

Commercial organisations are dependent upon the data they collect, process and store. This data not only contains commercially sensitive information but also a wealth of personal information about customers that they are legally required to protect. This same data is made available enterprise-wide, across private and public networks.

Loss of IP, as we've seen, accounts for £9.2bn per year. IP is often the life-blood of a business; it's the key point of differentiation and is at the heart of its competitive advantage. Imagine how Coca Cola would feel if someone stole their secret recipe!

Whilst loss of sales is a major effect of Cyber Crime, it is not the only financial implication. Long-term business security can be adversely affected by the loss of information relating to future innovation or business strategy.

Loss of sensitive data pertaining to consumers or 3rd parties also exposes organisations to significant legal costs. A 2011 report by Symantec Corporation, conducted by the Poneman Institute, concluded that 16% of the costs associated with a breach were directly attributable to legal defence or compliance costs.

For most, the business asset closest in value to data is brand. The negative impact of a public breach in terms of brand value is slightly less tangible but no less significant.

Finally, with negligence or individual error still playing a major role in data loss, the implications for the career on individuals responsible for major breaches is catastrophic.

GOVERNMENT

By their very nature, Governments collect, process and distribute high volumes of sensitive information; not only classified material pertaining to national security, but a wealth of personal data relating to the public. With a geographically diverse infrastructure, this data is transmitted across the country utilising the latest fibre optic networks.

The information held by Government makes them a high profile target for malicious attacks and information theft so they have a duty to ensure that every precaution is taken to protect data both within systems and whilst in transit.

PUBLIC SECTOR

Local Government, law enforcement agencies, emergency, defence and health services are all entrusted with sensitive information and can become targets for malicious attacks and information fraud.

These public sector organisations need to take the necessary precautions to protect the wealth of personal and sensitive information they hold as it passes between their geographically diverse locations, traversing both public and private networks.

In addition, as National Governments look to connect disparate public sector organisations together to share information and provide better service to the public, the need to ensure end-to-end security of information is ever more vital.

CRITICAL INFRASTRUCTURE

Gas, water, electricity, communications and transport networks all form part of a country's critical infrastructure. Any failure in service not only has a major impact on the public but also, potentially, the country's economy. It is the controlling networks, often referred to as SCADA (Supervisory Control and Data Acquisition), that are vital in managing our critical infrastructure. They collect key information from different parts of the grid, such as power demand and water pressure, and are then used to control critical components of the grid from a centralised location.

It is these controlling networks that present vulnerability to utilities and infrastructure organisations; not only from the theft of sensitive data being transmitted, but also the consequences of data flows being disrupted or manipulated as part of a malicious attack.

INFORMATION ASSURANCE MEASURES

There are a number of measures that can be taken to reduce the risk of data loss from within an organisation. Whilst it's by no means an exhaustive list, the following constitutes good practice:

1. Understand the constraints of your network and its ability to handle data securely
2. Encourage awareness of the need for risk management
3. Revisit your data security risk register on a regular basis
4. View information assurance as a holistic need
5. Prepare for the unexpected
6. Have a robust business continuity plan in place

HOW EASY IS IT TO TAP FIBRE?

We live and operate in the information age. We are reliant upon the availability of data wherever and whenever we have network connectivity and pay little attention to the journey that data has had to take before it arrives on our screens.

> "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."

With the growth in data centre and cloud computing we are becoming increasingly reliant on our high-speed, highavailability data networks to securely and reliably handle business critical data. However, many organisations are unaware that once their data leaves the perimeter of their facilities it is open to attack and can be tapped with relative ease and little expense.

According to Gartner, tapping fibre optic cable without detection is not only possible but has been taking place for most of the last decade. A view shared by the SANS Institute:

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 from the internet, legally, for as little as £300.

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.

Whilst it can be argued that the increase in attenuation resulting from this tap will lead to detection, it will be a case of closing the stable door after the horse has bolted. With high speed networks handling up to 100 Gb/sec it wouldn't take long to extract a significant amount of data.

For a little more money, cyber criminals can invest in an evanescent tap that results in significantly less attenuation and remains virtually undetectable to network monitoringdevices.

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

ENCRYPTION

The best way to ensure your data is secure as it traverses your networks is to utilise encryption. Make sure your encryption devices are both decoupled from your network architecture and accredited against the recognised world-wide security standards.

WHAT IS CRYPTOGRAPHY?

Cryptography (the literal translation is secret writing) is not a new concept; some of the earliest references date back 4,000 years - to Egyptian hieroglyphics. It is the science of converting plain text into cipher text through encryption and back again via decryption. The key to decrypting cipher text is, well, the key.

Early ciphers were either substitutional, where letters and numbers where swapped with alternatives, or transpositional, where letters and numbers were moved around within the text. The drawback of these methods of encryption was that they were relatively easy to crack.

Over the years there have been many famous, or infamous, cryptographic cases. Julius Caesar was known to employ a simple cypher to ensure the integrity of his messages to his generals. The early 20th century saw the invention of machines to encrypt and decrypt – perhaps most notably the Enigma machines used by the German military during World War 2.

Modern cryptography could be said to have its origins in the work of the code crackers of Bletchley Park as they developed Colossus, the first digital, programmable computer used to crack the German ciphers used in the 1940s. Ironically, the development of computers to aid cryptanalysis made it possible to develop more complex ciphers and computing soon replaced linguistic cryptology for both cipher design and analysis. To this day, cipher complexity outpaces the code crackers.

Cryptography is now used to deliver against 4 key business objectives:

- **Authentication –** where the sender and receiver of information are able to identify each other
- **Confidentiality –** where the information can only be understood by the party it was intended for
- **Integrity** – where the data in transit cannot be captured or altered without detection
- **Non-repudiation** – where the creation, transmission and receipt of information can be tracked

WHERE TO ENCRYPT

At first glance, encryption seems an easy choice. After all, why expose confidential information to prying eyes when you can protect it with cryptography?

Add to this the fact that modern systems make it possible to deploy hardware encryption to secure information at full line rates up to 10Gbps and it makes for a compelling argument. But where should you implement encryption?

The Open Systems Interconnection (OSI) model for general networking comprises 7 layers (Fig1.). 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, for example). Layer 3 is the network layer, responsible for packet forwarding (such as IP).

When it comes to the 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**

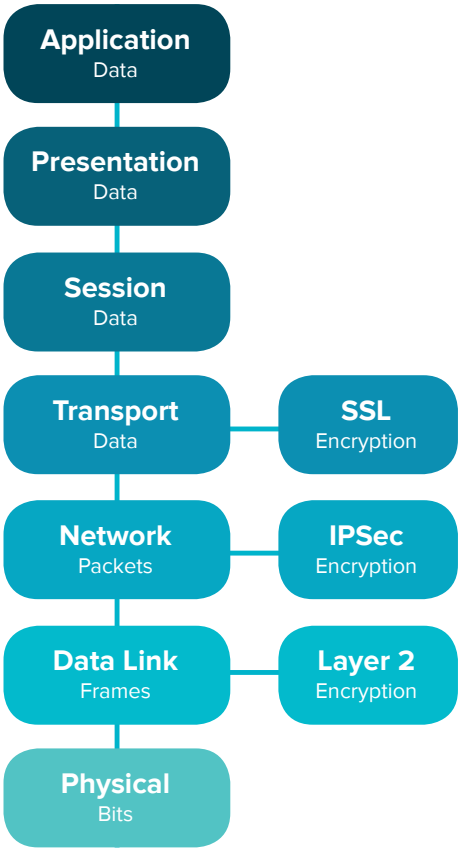
The challenge lies in maintaining the performance and simplicity of high speed networks while assuring the security and privacy of user data, whether voice, data or video.

BENEFITS OF LAYER 2 ENCRYPTION

Layer 2 encryption is often referred to as a "bump in the wire" technology. The phrase conveys the simplicity, ease of maintenance and performance benefits of Layer 2 solutions that are designed to be transparent to end users with little or no impact on network performance.

In a recent study by the Rochester Institute of Technology (RIT), it was determined that Layer 2 encryption technologies provide superior throughput and far lower latency than IPSec VPNs, which operate at Layer 3.

The RIT study concludes: "Enterprises that need to secure a point-to-point link are likely to achieve better encryption performance by shifting from traditional encryption with IPSec at Layer 3 to the overhead-free encryption of frame payloads at Layer 2."



When compared to encryption at higher layers, Layer 2 encryption has a number of advantages:

- **Lowest impact on network performance**
- **Reduced complexity (bump in the wire)**
- **Transparent to media (voice, data, video etc.)**
- **Little or no configuration**
- **Operates at wire speed up to 10Gbps.**
- **No additional overhead (Layer 3 IPSec typically adds significant overhead - over 40% of available bandwidth for smaller packets)**

Outsourcing of routing tables is also seen as a weakness of Layer 3 VPN services because many corporations don't want to relinquish control or even share their routing schemes with anyone, not even their service provider. They prefer Layer 2 network services, such as Ethernet, MPLS or ATM, as they are simpler in architecture and allow customers to retain control of their routing tables.

GLOBAL ACCREDITATION

There are two major global standards – Common Criteria and FIPS 140. Both provide the all-important, independent assessment of an IT security product or service against a pre-defined set of qualifying criteria.

Independent testing raises the quality of security products and allows for a meaningful comparison of solutions. Without these recognised standards, end-users would be forced to rely solely upon a manufacturer's assurances of security and reliability.

Common Criteria for Information Technology Security Evaluation

(abbreviated to Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification that is acknowledged in more than 25 countries worldwide. By mutual agreement, a solution evaluated in one country is automatically accredited to the equivalent local standards in each participating country.

The Common Criteria is used by governments globally as a security benchmark for the procurement of cryptographic products and services.

The Federal Information Processing Standard (FIPS 140)

is an information technology security accreditation program administered by the National Institute of Standards and Technology. It specifies the security criteria required for the cryptographic modules within a security system, which may include both hardware and software components.

The FIPS 140 standard is applicable to all US federal agencies that utilise cryptography in their ICT systems, whether designed and operated by the agency itself or under contract by a third party.

ABOUT SENETAS

Senetas Europe is a wholly owned subsidiary of Senetas Corporation Limited (ASX:SEN), specialising in high-speed network encryption. Our Layer 2 encryptors provide the last, best line of defence for data in transit for governments, the public sector and leading commercial organisations worldwide.

We manufacture the world's only triple-certified, high-speed data encryptors; certified to Common Criteria (Australia and International), FIPS (US) and CAPS (UK) as suitable for government and defence use.

Our products are used to secure network data for cloud computing services, payment systems, big data applications, CCTV networks, datacentres and critical infrastructure and control systems in more than 25 countries.

Senetas encryptors are suitable for networks of all types from point-to-point to fully meshed, multipoint network infrastructures. Our core products operate from 10Mbps up to 10Gbps and support Ethernet, Fibre Channel, SONET/SDH and LINK protocols. These high performance devices use AES 256bit encryption and operate in full-duplex mode at full line speed with no packet loss; delivering security without compromise.

CONTACT:

Gareth Jones
Senetas Europe Limited
Worting House,
Church Lane,
Basingstoke RG23 8PX

E: gareth.jones@senetas-europe.com
T: +44 (0) 1256 345599

SENETAS
Security without compromise

FIPS 140-2 LEVEL 3 VALIDATED

Common Criteria EAL4+ CERTIFIED

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