Submission by Senetas Corporation Limited to the Senate Select Committee on the National Broadband Network

Optical security for the National Broadband Network

August 2009

Introduction

The new National Broadband Network will compromise a national network of fibre optic transmission links used to connect individuals, businesses and government. Much of the information that will be transmitted across the NBN, including personally identifiable information and sensitive government and business data must remain confidential. It is important before building a network of this scale to take stock of how data should be handled and protected to prevent serious breaches.

The simple fact is that fibre optic networks are not secure enough to transmit confidential information that has not been encrypted. Whilst fibre optic is undoubtedly the fastest and most reliable way of transporting data across networks it is provably insecure due to new inexpensive technologies that make data theft easy using methods such as non-intrusive coupling.

Monitoring an entire optical fibre network is not practical therefore the simplest and most cost-effective remedy is to encrypt all critical and sensitive information before it crosses the network. It is pragmatic to acknowledge that mistakes will always happen due to people, process and technology failures but also important to realise that even should data be stolen then strong encryption will protect that information from disclosure.

In setting the foundation for this historic project we have an opportunity to address the critical issue of security from the beginning by having the foresight to design encryption into the core fabric of the NBN rather than trying to bolt it on as an afterthought. Security needs to be thought of as a part of the infrastructure of the NBN which is going to be the heart of communications for this and future generations of Australians.

Company history

In 1997 three Australian engineers started a company with a vision of securing the world's communications.

Today that company Senetas, is an award winning[1] engineering company and recognised as one of the world's leading developers of security technology. Exporting to more than thirty countries and responsible for protecting military, government and commercial secrets for some of the world's largest organisations, Senetas is an Australian success story.

From its roots in an anonymous Melbourne suburb and with funding from private investment and government research funding, Senetas engineers built a high speed encryption technology that built on modest local success and which was then chosen by the US Defence force to provide confidential communication across the entire Pacific Rim.

From that early success Senetas has built a business and patented technology platform CypherNet which is designed to protect information in transmission across networks where security must not be compromised.

Accredited to the most rigorous global standards for encryption[2] and trusted by governments worldwide, Senetas products are simple, highly secure, and reliable off the shelf solutions that encrypt fibre optic networks at wire speed *without* slowing down network traffic or compromising performance.

Senetas customers include many federal and state government agencies including law enforcement as well as Australia's largest banks and telecommunication providers.

[1] Frost & Sullivan APAC Technology innovation, AIIA innovation

[2]DSD approved Common Criteria EAL4 & FIPS140-2

The specific risk to fibre optic cables

Despite having the reputation of being more difficult to hack into than traditional copper cables, fibre optic can be tapped using a variety of methods, both intrusive and non-intrusive. Fibre cabling is easy to access, is typically protected by very weak physical security means and is accessible via publicly accessible pits in the street or in wiring closets found in many buildings.

Once physical access to the cable is achieved, light can be extracted from the fibre using different techniques.

Figure 1 illustrates some of the methods that can be deployed including optical splitting which requires the cable to be spliced and a device inserted to send the optical signal to down multiple paths.

Once a successful tap has been achieved the data sent across the fibre can be monitored, recorded and analysed. Invasive taps whilst effective do run a high probability of being detected as they require the optical signal to be interrupted for at least a short period.

More dangerous are non-intrusive tapping methods such as those shown in figure 1 in which bending the fibre or detecting the naturally emitted light (Rayleigh scattering) using sensitive amplifying photo-detectors allows information to be retrieved without disruption to the existing signal.

Using a readily available coupling device bought over the Internet (see figure 2), Senetas engineers are able to tap into a single strand of fibre and extract information. Senetas has produced a video demonstrating the ease with which information carried over the popular fibre optic data networks can be compromised.

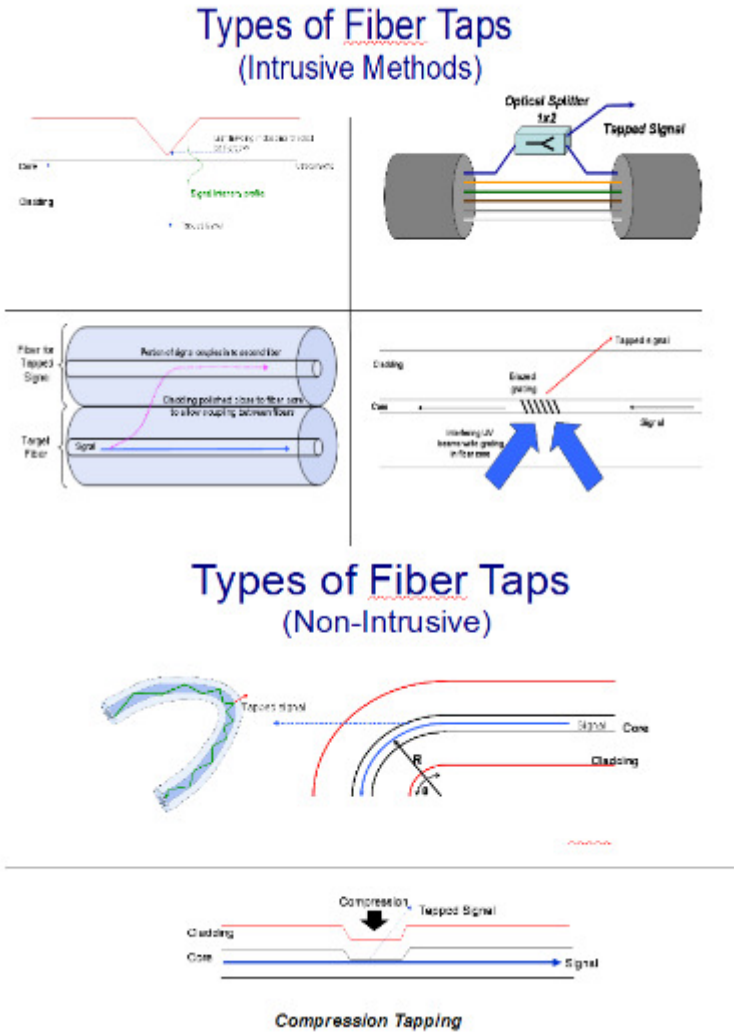

Figure 1: Fibre tap techniques

Demonstrating the interception of broadband information – in this case a video with audio streamed over fibre across a simulated corporate network - a coupler clipped on to the fibre was able to simply extract the same quality audio and video signal and send it to a third party or "hacker" laptop. The $500 optical tapping device takes advantage of a bend in the glass fibre to extract the signal without damaging the fibre or disrupting communications, and was virtually undetectable to either the original sender or the intended recipient.

However when Senetas CypherNet encryptors were employed to protect each end of the optic fibre, the encrypted video data stream could not be read even with the optical tap attached inline.

Figure 2: Fibre coupler

Senetas has shared the demonstration with governments, agencies and commercial organisations, particularly finance and banking, in Australia and abroad to warn of the risks to this popular network topology, fibre over Ethernet (also known as Metro Ethernet). This video is available for viewing online at: http://www.senetas.com/products/resources/media/Fibretap.htm

It is designed sends a strong message to organisations who were often sold on the myth that, because optical networks use photons of light rather than electric signals, that the fibre optic network is inherently more secure. Clearly it is not; using an optical tap device someone with mischief or malicious intent can read and store information being sent unencrypted between offices.

With more than 480 million kilometres of fibre deployed around the world over the past 25 years, and Australia about to embark on the NBN, data will be pumped along these fibres at up to ten gigabits per second, so potentially there's a lot at stake. Almost anywhere along those millions of kilometres, company-sensitive data and financial transactions could be extracted.

Risk Mitigation

Recognising that it is not possible to prevent physical access to an entire optical fibre network a sensible risk mitigation strategy should accept that information will be stolen and that mechanisms must be adopted to render that data unusable after theft.

Senetas believes its globally-certified network security is the fastest, simplest solution to immediately secure high speed networks which now carry immense information payloads. Up to 10 gigabits of data per second currently travel across these networks and 40 Gbps has already been announced, so massive data would be incurred even during a short data interception by hackers. Assuming the average size of a data packer is 6 Kb per personal record, network traffic travelling unencrypted at 10 Gigabits per second potentially puts 208,000 records at risk every second, and over a million every five seconds. Encrypting these high speed links using Senetas CypherNet immediately renders the information unintelligible, yet maintains high speed data throughput.

Senetas regards robust security as a business enabler, because unauthorized access to sensitive government, corporate or personal data not only affects the bottom line of organizations, it damages their public reputation.

Often criticisms of encryption are based upon the belief that it slows down the network traffic, however Senetas had developed, and was recently awarded an Australian patent for, a multiprotocol high speed Layer 2 hardware encryption, developed here in Melbourne and sold to some of the world's most security conscious governments, law enforcement agencies, military and enterprises.

Conclusion & Recommendation

Senetas asks the Senate select committee to consider the information presented in this paper and to consider its implications for the National Broadband Network.

It is our belief that the security of the NBN should be one of the major considerations in the planning for this landmark project. History tells us that it is far simpler and cheaper to design the right security measures in at the beginning of a project than try to shoehorn it in later.

Expenditure on security technology is difficult. In the absence of objective measurable data on the effectiveness of different approaches, security decisions can be too often swayed by emotion and fear leading to solutions that only superficially solve problems.

In a case such as this however where the vulnerabilities are unambiguous and a proven solution is readily available, an investment now in time spent thinking deeply about long term security problems will pay large dividends for the future.