Wireless Transmission Security
using SONAbeam Free-Space Optical Communications

This application note examines the fundamental physics of wireless transmission equipment and demonstrates how SONAbeam™ Free-Space Optics (FSO) is among the most secure of all wide-area connectivity solutions with regard to transmission security at the physical layer.

Overview of Communications Security Issues:

The security and confidentiality of communications, whether through public or private networks, has become a topic of increased attention. Information security concerns tend to fall into two major categories: *transmission security*, related to the actual transport mechanism and physical medium, and *communications security*, related to the integrity of the information content itself.

Most of the security compromises by external intruders occur by hackers breaking through corporate firewalls and using a variety of techniques to breach higher protocol software layers and applications to compromise user data and information. The security of user data, both during storage and transmission, in large part relies on encryption techniques. This is the communications security aspect, which is relevant for all data and transmission applications. Encryption is a powerful security tool, and well-encrypted channels are highly secure because breaking them requires sophisticated and expensive computing technology and can take many months.

In this application note, we focus primarily on physical layer security (i.e., transmission security) which must also be considered for sensitive applications, especially when the communications links must traverse public space or public networks, even if between secure facilities.

Terrestrial infrastructures that use copper wire (commonly called the 'local loop') are the most easily intercepted, but with varying degrees of effort any physical medium can be tapped. Traditional bundled cabling, although relatively difficult to access, is very difficult to protect from interception, especially after exiting the building in locations such as underground tunnels

and sewers, at the demarcation point where telco services connect to customer premise equipment (such as an office building basement), and in unattended telco central office switching stations. Once access has been covertly obtained, a skilled person can intercept the transmission with relative ease and the integrity of the data transmission then relies solely on the robustness of the encryption technique used. As a result, physical monitoring and protection of the cabling is necessary.

Wireless Transmission Security:

Turning our attention to wireless transmission systems, it is widely known that most RF transmissions, both unlicensed and licensed, are readily subject to interception. Many RF systems, like cellular phones, police radios, and wireless LANs intentionally radiate signals in all directions, and hence have no physical layer transmission security: the signal is accessible to anyone with a receiver. This is particularly true of the newer Ethernet-based 802.11 WiFi wireless local networks that are deployed in office buildings, hotels, airports, coffee shops, etc. Such wireless networks have recently received bad press because, in addition to having no physical layer security, the data encryption algorithm and techniques employed in early versions were particularly weak.

In addition, the standard encryption schemes employed by Windows network software can be bypassed with little effort, so additional layers of signal encryption are often needed to reduce the effectiveness of a malevolent intercept. There are many anecdotal accounts of people prowling office parks or hotel lobbies and logging on to networks of unsuspecting companies for, as one hacker put it, “fun and profit”. For them the potential for exploitation is high, while the risk of exposure is very low.

In a somewhat different category of RF wireless transmission are point-to-point (PTP) microwave systems, which in most cases use licensed microwave bands, although there are some unlicensed bands that are also used. In this case, the RF transmission is highly directional instead of omnidirectional. The antenna radiates a cone-shaped beam of divergent RF energy, intended to optimize communication between two locations, with minimal RF energy radiated in undesired off-axis directions.

Depending on the antenna size and operating frequency, PTP microwave systems generally have a 1-10 degree beamwidth, which applies to both transmission and reception. Thus, the divergent transmit beam is vulnerable to intercept by an unauthorized receiver located within the beam, and the receiver is similarly vulnerable to jamming from within this acceptance angle. To get an idea of the vulnerability, consider a representative 18 GHz link with a 60 cm

(2 ft) antenna. The main beam is radiated in about a 2 degree cone of energy. At a receiver located 1.5 km (1 mile) away, for example, this RF beamwidth has a footprint about 60 meters (197 feet) in diameter. Thus, the footprint of the transmitted energy bathes the entire side of a building, where an unauthorized receiver can be located to intercept the transmission. A link operating in the 5.6 GHz band with the same size antenna would have a footprint 3 times larger, enough to bathe an entire city block.

The width of the main beam is not the only vulnerability of PTP microwave systems for a determined attack. Even directional parabolic antennas have sidelobes and a backlobe that radiate energy off-axis that are also vulnerable to intercept. In addition, reflected energy from buildings within or near the fresnel zone can be exploited for unauthorized access. In both the sidelobe and reflected energy cases, the unauthorized receiver can be located well off-axis to the main beam, and hence be quite discreet.

These vulnerabilities of RF systems, and especially those that radiate in all directions, have led many people to wrongly conclude that all wireless transmissions are highly vulnerable to intercept and compromise. *In fact, optical wireless transmission offers a very high level of transmission security*. For this reason, government and military organizations have deployed free space laser communication systems for video and broadband data communication due to its inherent low probability of intercept (LPI) and anti-jam (AJ) characteristics.

SONAbeam™ for Exceptional Wireless Transmission Security:

The primary features of free-space optics (FSO) that provide exceptional transmission security are the very narrow beamwidth and the lack of off-axis sidelobe emissions. As most people are aware from laser light shows, a laser beam can be highly directional from a small aperture. The fixed-pointed SONAbeam™ systems have a beamwidth of 2 milliradians, compared with 2 degrees in the RF example above. This FSO beamwidth is 17.5 times narrower, and at the same 1.5 km distance it only illuminates a 3.4 meter spot, compared to 60 meters for the RF example.

SONAbeam™ has an additional benefit, in its lack of sidelobes. The lack of sidelobes for an FSO system arises from a transmit aperture size that is about 20,000 times larger than the laser wavelength, thus avoiding the diffraction effects that cause sidelobes. This contributes to the stealth and LPI aspect of optical wireless for transmission security, since it can be very difficult to detect the laser emissions to even determine the origin of the transmission.

Eavesdropping on an FSO link is not feasible in the conventional sense. One cannot simply insert an optical probe, analogous to a whip antenna, into the beam. In order to intercept an FSO link, an adversary needs to intercept a portion of the transmitted beam - without physically exposing himself and his equipment. This optical intercept equipment, essentially a telescope with receiver electronics, must be placed directly in the very narrow beam, and must be precisely pointed back at the originating laser source. Such efforts are extraordinarily difficult and the chance of an attempted intercept being discovered is very real. The transceivers are normally installed at the edge of rooftops or behind office windows, high above street level, where access to the beam is generally limited to the two endpoints (i.e., the transmitter and receiver locations). Physical surveillance of both endpoint locations can be provided by webcams, as well as video surveillance boresighted to the laser beampath to ensure no intercept equipment is located within the very narrow beam.

Another formidable challenge is how to intercept the laser beam without altering the signal reception. Care would need to be taken by the intruder not to disrupt the beam. Although it is theoretically possible to insert an optical receiver into a beam without bringing down the link, an attempt at intercept could be discerned as an anomalous power loss at the receiver, which in turn could be transmitted as an alarm to the user network operations center. SONAbeam™ NMS management software has this capability.

The SONAbeam™ equipment has another feature that further mitigates against physical intercept of the wireless transmission. SONAbeam™ equipment uses much higher power lasers than any other FSO equipment on the market – 10 to 40 times more laser power than other systems. This much higher transmit power allows the SONAbeam™ to penetrate foul weather better than competitive products. However, from an intercept point of view, high power is not desirable in good weather, since it minimizes the size of the intercept receiver collecting aperture that would be needed. This is avoided by the adaptive laser power feature that is standard on all SONAbeam™ equipment. In good weather, the laser power is greatly reduced - by as much as 40-fold - primarily to prolong the life of the lasers. But this adaptive laser power feature also greatly impairs the feasibility of a small aperture device for intercept.

Finally, one might argue that an intercept could occur by placing an intercept receiver directly behind the intended receiver, located perfectly along the line of sight, to intercept the energy that overshoots. There are several ways to foil this approach. First, if the intended receiver is located in an office behind a window, there is no overshoot to intercept. Second, in a roof-to-roof deployment, the geometry will usually preclude being able to place an intercept receiver within the very narrow overshoot footprint. In the worst case placing the SONAbeam™ in front of a small wall will eliminate any overshoot.

There are obstacles to even detecting the presence of a SONAbeam™ link. The 1550 nm wavelength of the SONAbeam™ precludes the use of conventional optical instruments, video cameras, and even night vision goggles to detect the beam, since this wavelength is not detectable by any of these equipments. Off-axis scatter from particulates like snow or light fog can scatter some energy outside the highly directional beamwidth, but even if an instrument specifically designed to detect this wavelength is used, the multi-path scattering phenomenon not only weakens the signal, the inter-symbol interference destroys the ability of the intercept equipment to temporally resolve the energy associated with each bit, especially for high-speed data communication.

In conclusion, while there is no wireless communication system that can guarantee transmission security, the SONAbeam™ laser transmission equipment operating at 1550nm offers an excellent wireless transmission solution for the highest possible level of physical layer security.

For further discussions, please contact:

Dr. Robert T. Carlson, Chief Technology Officer
fSONA Communications Corporation
Richmond, British Columbia (Canada)
604-273-6333
http://www.fsona.com