PLAINTREE

Security aspects of infrared wireless links

Introduction

Infrared communications systems are enjoying a resurgence of interest on account of their potentially high payload capacities, small terminal size, absence of licensing requirement, speed of deployment and high security. They are increasingly seen as a powerful tool to provide broadband connectivity directly to user premises and between network switching nodes. This note examines the security issues concerning the use of infrared LED communication systems for transport of confidential data.

Link security review

There are several potential security issues for any communications system with respect to the activities of third parties:

- Can the existence of the link be discovered?
- Can the traffic usage and patterns be monitored?
- Can the traffic contents be read and understood?
- Can false data be covertly inserted?

There is no communication system that can offer unqualified content security. Different systems offer different levels and types of security.

Encryption, for example, is a powerful security tool. Well-encrypted channels are highly secure in the sense that only highly sophisticated and expensive computing technologies have a possibility to break them. Although a well encrypted channel can take many months or years to break, the use of protected channels will enhance the security of the communication by preventing illegitimate intrusions into the encrypted channel. A protected channel is one to which a potential eavesdropper has no easy access and is likely to be discovered before any sensitive information is compromised.

Some channels are very difficult to protect. A wire-pair, co-axial or fiber cable typically winds through a tortuous route between terminals, leaving the possibility of damage or unseen access at some location en route. Once access has been covertly obtained, the information can be relatively easily monitored. Optical fiber traffic is much more difficult to monitor because of the small size and relative fragility of fiber and the considerable sophistication of the equipment necessary to implement interception. However, unless the region surrounding the fiber is monitored in some way to detect physical intrusion, interception remains possible.

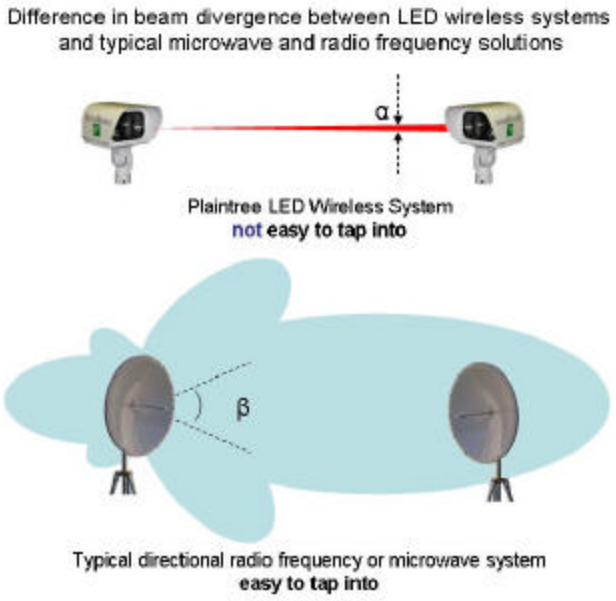
Current wireless radio and microwave systems are very easy to monitor as the radio waves spread, diffract and pass through walls, making covert intrusion relatively easy. Radio frequency or microwave systems can have beams as wide as 90° or more, compared to 1° beam divergence for Plaintree's LED wireless system. This, plus the resulting side lobes and reflections, make it easy to detect, locate and tap into the signal anywhere in the broadcast region.

LED wireless security

The security strengths of the LED wireless link derive from the wireless nature of the channel, the small terminals, and the close confinement and containment of the transmitted beam.

Narrow beamwidth

LED wireless systems, unlike radio frequency and microwave links, utilizes a difficult to detect narrow beam of infrared light (see diagram). Plaintree's infrared beam will not pass through or easily reflect off of opaque materials (i.e. Walls, trees, and buildings).



Invisible beam

Plaintree's LED beam is completely invisible to both the naked eye and infrared viewers. To locate the transmitter an infrared viewer must be directly in the beam path and aligned with the transmitter. Even when using infrared viewers, Plaintree's transmitter would look no different than the multitude of other sources of infrared light that exist in almost any situation, such as camp fires, lamps, or any other light or heat source.

Proprietary modulation

Plaintree offers a specific LED wireless product line that uses a proprietary modulation scheme suitable for ultra secure installations. For any intruder to try to intercept and decode the telecommunication signals of this specific ultra-secure model they would require an optical Plaintree's LED wireless equipment of the same type. Since Plaintree tracks all of its product sales, any potential intruder can be easily identified.

Use of encryption

Additionally, security can further be increased by encrypting the transmission data as stated above. Plaintree's LED wireless system supports the seamless transmission of encrypted IP data (e.g. IPSec).

Summary

In summary, LED wireless systems from Plaintree Systems offers a relatively high degree of telecommunications channel security. It is:

- Difficult to detect and locate
- Difficult to tap into
- Supports additional security techniques such as encryption
- Allows for immediate detection of intruders

Contact information:

WORLD-WIDE SALES & DISTRIBUTION

www.plaintree.com
sales@plaintree.com

Plaintree Systems Inc
110 Decosta Street,
Arnprior, Ontario,
K7S 3X1, Canada

Toll-free number: +1-888-831-8300
Phone: +1-613-623-3434 / Fax: +1-613-623-4647