LET THERE BE LIGHT

Paul D Turner *examines the historical developments and emerging use of visible light communication (VLC) and – from a radio perspective – visible light modulation (VLM)*

Optical communication technology has been commercialised in the form of LIFI and has become widely utilised in government and military circles as an inherently or at least seemingly more secure option over the highly congested radio-frequency spectrum, of currently deployed wi-fi networks. A first glance, this seems a reasonable consideration on many levels, including a data transfer speed up to 100x faster than wi-fi. The ability to limit or contain optical emanations to within secure working areas at the facility level.

A review of various product marketing sheets, websites, manufacturers specifications and significant numbers of patent applications tend to give the technical security researcher a distorted view that VLC is a new emerging technology. The reality is this is better described as a technology modernisation of historical proportion. Visible Light Communication (VLC) dates back to 800 BC with the use of sunlight; 400 BC with the use of the heliograph and beacon fires and 1880 AD saw the advent of Alexander Graham Bell's Vibrating Mirror Modulation (VMM) system.

The optical source was again sunlight, and the technique utilised VMM to modulate the optical carrier, with a parabolic mirror used as the receiver. A distance of 213m in 1880 by Alexander Graham Bell is truly amazing!

Emerging use-case applications suggest that technical security professionals need to include a comprehensive, universal detection strategy for VLC and VLM, regardless of the optical source in coming years. Currently, only limited resources are available to conduct optical inspection, and most are ineffective at best. Any number of optical emissions may be outside of the design detection range or capability of any deployed detection resource. The effectiveness of any optical inspection protocol will depend in part on the type of the optical or photonic emission and the thoroughness of the applied inspection.

A common threat-actor attack is to install a technical surveillance device that's directly activated by the end-user via remote-control during meetings and video-conferences

A sensor-based approach is essential for the detection and identification of the presence of VLM and infrared light emissions, as neither are detectable by the human eye. Optical detection methods are used to evaluate artificial and ambient background (optical) noise levels and specifically identify the presence of optical transmitters via signal-level spectrum analysis of demodulated optical signal events.

The demodulation of AM and FM audio-based, optical emanations provides an essential detection component in a standards-based modern moving target threat model.

Technical operators must include a competent review of the facility-level optical spectrum, for all critical infrastructure, given the growing use of threat-actor optical deployed technology. Optical inspections are an essential technical security protocol given the emerging, renewed and advancing optical technology in use entering the commercial and espionage-based threat environment. Recent advancements in software-defined radio concepts at the hardware and software level ideally support simultaneous radio-frequency and optical-spectrum analytics, as required to effectively separate threat technologies from optical noise, within the bounds of limited time-on-target considerations.

Software defined radio that supports multiple-band, multiple-radio configuration is an absolute requirement in providing professional-level TSCM inspections and for SIGINT roles. SDR technology is well-suited for optical spectrum analysis. Many of the same deployment principles and techniques that are familiar to the technical operator and apply to existing radio-frequency based geo-location heat mapping, can be extended to a technique known as dimensional optical geo-location heat mapping. Periodic and continuous optical threat monitoring, such as Optical Spectrum Surveillance and Monitoring (OSSM), is strongly recommended within mission critical infrastructure for commercial, government and military at the national security level.

There are two primary detection resources that can be deployed. Passive stand-alone collection resources can be utilised in an operator assisted deployment search strategy or multiple, cascaded optical detection sensors can be simultaneously deployed along with radio-frequency antennas, across multiple radios and multiple spectrum bands to achieve a comprehensive dimensional optical geo-location heat mapping process.

There are a growing number of differing optical emitter types that are commonly encountered at the technical security level. Some optical emitter-types are likely to be more commonly found in the ambient optical spectrum environment at the commercial level, by way of authorised technology for which additional non-optical vulnerabilities are likely to exist when LIFI and other optical devices exist, even when authorised for use within the facility.

Evaluating only the LIFI component of the system, may mask vulnerabilities or compromises of the underlying driving technology. Failure to evaluate all aspects of the network infrastructure can result in the operator not identifying a significant vulnerability or compromise that may not be directly attributed to the LIFI infrastructure. The technical operator must inventory and evaluate all optical emitters and network hardware to determine the device's purpose, use, vulnerabilities and any potential hostile intent or system compromise. Penetration oriented testing is often the only way to surface inherent or undocumented, installation or setup vulnerabilities.

LIFI can be classified as nano-meter (nm) wave communication, with a range of frequencies and wavelengths that cover the infrared and visible light spectrum, specifically used for the transmission of optical-based communication. Visible Light Communication (VLC) is a method of providing optical visible light communication in the 400THz (780nm) to 800THz (375nm) range as an optical-based carrier used for data or audio-based transmissions.

OPTICAL TRANSMITTER

Optical transmitters convert the original input data or signal into a representative digital signal suitable for transmission via an LED array. This is typically, an on-off keying (OOK) process, which can be described as the simplest form of digital modulation. LIFI utilises considerably more complex modulation schemes and can be encrypted prior to the original data conversion process into the digital format.

OPTICAL RECEIVER

A photo-diode is used to detect ambient digital optical modulation, received in the form of On-Off Keying (OOK) states from an LED array. The data conversion process converts the received data back into the original signals state. If the signal was encrypted prior to the digitisation transmit process, the receiving data conversion process is utilised to perform the decryption process.

AV REMOTE CONTROLS

The most common type of periodic optical signal encountered are generally directional, invisible infrared (IR) light modulation, utilised for the transmission of command and control (data) signals in audio-visual and remote-control systems. Remote IR receivers utilise omni-directional sensors hard-wired back to the equipment rack. Wireless RF/IR repeaters may also be found in some installations.

IR audio-visual remote controls are excellent test and evaluation resources for both, initial operator familiarisation and training and demonstrate optical characteristics and detection principles.

TECHNICAL SURVEILLANCE DEVICES (TSD)

Similar in design to AV remote control devices, a similar technology can be used for remote technical surveillance device activation and for the control and programming of optical-based threat technology. The threat-actor can optically transfer recorded data stored on the device. Audio-enabled IR transmitters (authorised and hostile) can be positioned to intercept room-level audio and will require an optical path out of the Operator Defined Target Area (ODTA) via windows, door gaps, openings, holes, above and below a dropped ceilings or sub-floor structures.

OPTICAL TRANSLATION SYSTEMS

Many corporate boardrooms and public government facilities, including self-guided tour venues,

provide simultaneous translation systems utilising channelised professional broadcast level Infrared (IR) communications. The technology typically uses defused IR emitters, in a technique referred to as IR flooding to achieve adequate wide-area coverage. It is also possible to utilise highly directional, local area (exhibit) only coverage. The operator needs to look at potential underlaying technology vulnerabilities to determine whether a threat-condition exists outside of the optical system.

HEARING ASSIST (ACCESSIBILITY)

From an accessibility perspective, the same Infrared (IR) communication technology can often be found in public venues to meet the legal requirements for hearing impaired accessibility. The technical security challenge is to determine what the system is connected to within the AV system. Often, in order to meet accessibility compliance the compromise of intelligence-bearing optical emissions from the underlaying driving technology from the operator defined target area.

LIGHT FIDELITY (LIFI)

The emerging commercial use of Visible Light Communication (VLC) via pulse modulated light sources or dedicated Infrared (IR) devices to provide bi-directional, high-speed internet connectivity is becoming more and more common and requires greater attention by the technical operator. The operator must demonstrate the ability to detect and identify LIFI optical emanations and differentiate any modulation from ambient optical noise emanations.

MODULATED DIRECTED LASER (AUDIO)

The use of visible and invisible laser interception technology can be used to passively intercept room-level audio. An unmodulated laser source is directed at the targets window or can be focused on a reflective object within the room. The in-bound laser source is modulated with room-audio and the modulated laser is reflected back and recovered by the threat-actor. The intercepted intelligence-bearing signal is then recovered and demodulated to provide the threat actor with room audio.

BACK HAUL (OPTICAL COMMUNICATION LINKS)

Commercial Point-to-Point high-power, Infrared Communication Links (ICL) can be used to provide high-speed, high-bandwidth communication across multiple channels (internet, data transfer, VoIP, alarm monitoring, CCTV and access control). Back haul optical links are often found on roof tops to securely communicate between multiple buildings when other communication options are not available. It is unlikely the technical operator will identify the use of such technology without asking questions and conducting a competent physical inspection, including critical infrastructure roof tops.

OPTICAL ALARM SENSORS

Optical-based alarm sensors can be deployed for the purpose of intrusion detection and are also used for optical (visible) smoke detection across large open areas of a facility, such as a hotel lobby or industrial setting, and are easily compromised.

DATA COMMUNICATION EQUIPMENT (DCE)

The inherent ability to recover intelligence-bearing signal content from LED status displays is another possible vulnerability to be considered. Undertaking a threat evaluation is required to determine the potential for optical compromise. Determination of risk is essential for all network resources containing LED displays – across all data and audio processing devices. Particular attention of video-conferencing and telecommunications equipment, including the power status indicators for peripheral devices (hubs, routers, switches, and powered speakers), is required ●

Paul D Turner, TSS TSI is the President/CEO of Professional Development TSCM Group Inc. and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with over 40 years' experience in providing advanced certification training, delivery of TSCM services worldwide, developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.

An example of a typical passive optical sensor

Picture credit: TSCM Group