OVER THE AIR

PD Turner *examines the TSCM implications of Wireless Power Transmitters*

The future is here, and the utilisation of the electro-magnetic radio-frequency spectrum for air-charge refueling is a reality and brings benefits and technical security concerns.

The potential for mass IoT sensor wireless charging and the emerging ability to perpetually power upward of 30-billion IoT devices by 2030 rapidly surfacing worldwide is identified as a growing and dangerous trend in sustainable espionage threat technology that is fast becoming a reality.

Wireless power transmission is already here and used for over-the-air charging of a variety of wireless devices and IoT technology, such as AirCards, similar in design and function to AirTags, which so far require a replacement RS2032 battery about once a year in practice.

Radio-Frequency Identification (RFID) is a relatively short-range example of transmitting power wireless with low level data structures. RFID is a technology often used for identifying and tracking objects using radio-frequency energy. It does not transfer data in a traditional sense, but can be used for inventory management and electronic access control purposes.

The transmission and delivery of wireless power is more than a century old, for those TSCM practitioners who see such modern capability, as only a future TSCM threat consideration.

The importance of proactive surveillance of the electrical power utility grid is a well-documented and essential TSCM practice, however the detection, identification and counter measure protocols for the radio-frequency transmission of power, rather than for organised-intelligence detection, is a growing concern among competent professional TSCM practitioners.

Imagine the ability to perpetually power a sophisticated surveillance device that does not contain a battery or picture a platform that can recharge the battery over-the-air wirelessly, utilising power that is transmitted via a radio signal carrier from more than 150 feet away, and you can begin to appreciate the implications for TSCM professionals across the commercial, government, military and national security sectors.

Wireless power transfer can emit energy through various materials, meaning that surveillance devices can be concealed within any suitable ambient objects and still be wirelessly air-charged or directly powered.

A wireless power transmission platform has more than a 150-year-old history in theory, concept and practice; demonstrating the ability to generate a time-varying electro-magnetic field capable of not only remote charging, but also delivering continuous operating power; not to mention the ability to power on-demand sophisticated threat technology remotely from outside the intended fixed or deployed target.

Important discoveries, among many of the well-known brilliant-minds in history, set the foundation for today's advanced work on the subject of wireless power delivery.

Andre Ampere's Circulatory Law discovered that electric current flowing through a conductor will produce a magnetic field, in the year 1826. Michael Faraday developed Faraday's Law of Induction and demonstrated that electro-magnetic energy gets induced across an air gapped conductor when it comes in contact with a time varying magnetic field in the year 1831. James Maxwell's application of these laws and early experiments and equations of the characteristics and properties of electrical energy and magnetism helped establish a consistent theory known as Maxwell's Equations in the year 1862.

Important discoveries progressively strengthened the core foundations of Nikola Tesla's scientific discovery that led to the successful powering light bulbs from a 140-foot Tesla coil in the 1890s and is said to have burned out a dynamo at a local powerplant in the process, so the story goes; and perhaps in a more civilized experiment to power multiple electric-light bulbs via a wireless power source approximately 60 feet (18m) away using electro-magnetic induction (resonant-inductive coupling), leading to a patent in year 1907.

The questions and the challenges we are often asked about during Certified Technical Operator (CTO) training, tend to be framed around "at what distance and conditions can charging and or air-powering a device via a radio-frequency transmission be accomplished and/or sustained efficiently, and can the process support the transmission of data-based, 'hostile intelligence'?"

The answer to these important questions remains somewhat illusive given the state of fast-emerging and highly-competitive competing technologies and developing standards.

Relatively short ranges are currently realised; the wireless range-of-interest can easily utilise frequencies in excess of 40GHz and see power levels of 500W or more in some proposed applications, requiring regulatory special authorisations as the technology develops.

DEVELOPING STANDARDS

Qi is a wireless charging standard, for example, that supports wireless charging of smartphone related devices; referred to as "Qi Data over Wireless Power", enabling the transfer of data (mostly limited to authentication and device identification), alongside the wireless charging process. Technical operators must gain the knowledge and ability to identify and recognise the spectral characteristics of wireless transmission systems, and the effect on the spectral noise-floor. The vast number of operators either fail to recognise emissions for what they are, or classify the emission as unknown noise.

Apparent spectral noise cannot simply be dismissed any longer and must be properly investigated and resolved by the technical operator; as many surveillance devices may be missed under the misclassification of: "it must be just noise" category.

The ability to transmit parallel data is currently limited, whereas the ability to charge or perpetually power devices is an emerging threat technology of significant concern given the fact that the transmission of power can be specific to certain device types; ignoring others that do not provide a unique handshake acknowledgement between the device and the power emitter – utilising a sort

THE IMPORTANCE OF PROACTIVE SURVEILLANCE OF THE ELECTRICAL POWER UTILITY GRID IS VITAL

of pairing that can target specific device types and ignore ambient IoT technology that may also be in use within the range of the wireless power emitter. The handshake may contain encryption for communication purposes during the authentication and wireless charging process.

It's essential to understand that while wireless transmission technologies can support data transfer in conjunction with the wireless power capability, they are currently not suitable or designed for high-speed, high bandwidth data transfer, yet!

If a wireless power transfer device supports formal data transfer, it will likely need to be classified as a regulated intentional radiator, rather than an unintentional radiator.

Wireless power transfer can emit energy through various materials, including plastic, glass, wood and other similar materials for enhanced durability, making them suitable for outdoor, ruggedised, and concealed applications. This means that surveillance devices might be concealed within any suitable ambient objects and still be wirelessly air-charged or directly powered.

EMERGING TECHNOLOGY

Like all emerging new technologies, most are developed from historical concepts. The subject of wireless power transfer has taken on many handles and directions as different competitive interests apply and build on scientific research and development of uniquely proprietary applications with different and often competing technology approaches.

A radio-frequency emitter is utilised to transmit power across free space to a receiver sub-system, such as a wireless IoT device that is designed to extract or harvest energy, for the purpose of charging, recharging or perpetually powering the device at various physical distances from the emitter.

TECHNOLOGY APPROACH

There are numerous emerging competitive methods of accomplishing the art of wireless power transmission; including Inductive-Coupling that requires that the transmitter and receiver coils be closely spaced and carefully aligned to facilitate the transfer of current flow and charge a battery.

Inductive-Coupling is a wireless air-gap charging method that utilises electro-magnetic fields to inductively transfer power between a transmitter coil in the charging pad and a receiver coil in the device being charged. When the coils are properly aligned electrical current flows through the receiver coil, to charge a battery or directly power the device. Low-level handshake protocols allow the device to determine the correct charging parameters and identify the type of wireless charger.

WIRELESS POWER TRANSFER CAN EMIT ENERGY THROUGH GLASS, PLASTIC AND WOOD

In resonant Inductive-Coupling platforms, power transfer is significantly improved through the application of resonance, where the transmit and receive coils are tuned to the same resonant frequency resulting in a higher and more efficient power-transfer ratio of transmitted energy. Resonant Inductive-Coupling is a generational extension of Inductive-Coupling air-gap charging, which uses tuned-resonance to improve power transfer efficiency.

This method involves tuning the transmitter and receiver coils to the same resonant frequency, providing more efficient power transfer over greater distances. Phase shift is a common method used to improve the efficiency of the charging process, discussed further in part two of this article.

TSCM IMPLICATIONS

As the number of wireless charging systems continues to grow, it will become extremely difficult to determine the ambient-friendly platforms from potentially hostile systems.

Power is delivered in the same way WI-FI networks are commissioned and the transmitter might be concealed in any object suitable for the area in which it is deployed to cover a specific room or an entire facility. The wireless charging apparatus might easily be part of the threat actors intercept platform, installed along with the actual surveillance device.

Wireless power emitters can by design, employ smart-detection and identify a device's specific beacon signal and then direct power accordingly – and, yes, the power control side can be managed via the cloud in some designs.

There are many emerging use cases being identified and actively developed that are just now starting to surface, and will have direct implications for the technical security practitioner.

It is essential that a solid understanding of wireless power transmission techniques be acquired as part of a proactive training programme, which requires specific training and skills development.

The Energiser Bunny might have a reputation for going and going, but might just need to take early retirement with millions of batteries that will no longer need be replaced in IoT and threat actor surveillance devices, with powerful long-distance radio-frequency power transmission platforms now emerging on the commercial and military market.

Picture a wireless-charging platform that is capable of transferring a Kilowatt of power (or more), with the ability to tolerate misalignment and overcome positional considerations, add address propagation challenges.

THREAT TECHNOLOGY

A threat actor, having installed multiple IoT surveillance devices, might selectively utilise a radio-frequency energy emitter from well outside the traditional Operator Defined Target Area (ODTA) or even the external Functional Target Area (FTA) to enable a dormant device lurking in standby for an extended period of time, consistent with the threat actor's agenda, and accomplish the intent of the intercept at a chosen point in time.

This makes it possible to install devices months or years before an activation event, and most certainly well before proactive countermeasures are even being considered, let alone implemented for the targeted event.

It is necessary for the professional technical operator to research, experiment and fully explore the operating frequencies; determine the emission characteristics from a TSCM perspective and better understand how to detect and identify a power transmission signal that does not contain recoverable surveillance-oriented intelligence.

Wireless technology may only charge a dormant device for a short period of time prior to becoming an active surveillance device with a functional, but limited operational window, before the device completes the intercept, forward processes the intelligence, and returns to a totally dormant state ●

Next month Part II of this feature will explore the technical operator process for the detection, identification and characterisation of wireless power emitters from a TSCM deployment perspective.

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 45 years' experience in providing advanced operator 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.

Apparent spectral noise cannot simply be dismissed any longer and must be properly investigated and resolved by the technical operator