Kestrel TSCM ® Professional Software

"Tap Capture Plot (TCP) ™ | The Importance of Power Line (PL) Energy Heat Mapping—Part I

May 2020 | Issue 59

Technical Research and Standards Group

Paul D Turner, TSS TSI

Pandemic | Lost Time or Opportunity?

The recent and unpredictable future of the global pandemic currently being experienced on an unpresented scale worldwide provides us with an opportunity to brush up on our technical expertise.

This months edition of the TSCM | SIGINT Newsletter is being released early so that those technical operators that find themselves with a little or a lot of extra time on their hands, can brush up on some of the latest new techniques and methodology offered by the innovative Kestrel TSCM ® Professional Software.

Power Line (PL) Analytics (Part 1 of 3)

Signal pattern recognition or RF visualization as it is referred to under the | TSB 2000 (Technical) Standard ™ | has not only been the goal of many technical operators to be better able to identify and localize RF events of significance; it has become the only means of easily identifying all RF energy sources that are present within a given area.

The ability to utilize the | Tap Capture Plot (TCP) ™ | process to baseline via a captured reference database and identify potential threat technology associated with the electrical power grid in near real-time, can be quickly achieved utilizing targeted Power Line (PL) geo-location heat mapping across the | Operator Defined Target Area (ODTA) ™ | and into the extend | Functional Target Area (FTA) ™ |, is a powerful new TSCM capability and methodology found within the Kestrel TSCM ® Professional Software application.

It is not all about the software (although that is a big part of it), it is more about the process (methodology) behind the software that has changed the way TSCM inspections are now conducted, based on significant scientific research and development; that the advanced concepts of RF Visualization propagation modeling have emerged.

The Kestrel TSCM ® Professional Software provides a modern means to utilize one of the most powerful new TSCM Software Defined Radio resources, in conjunction with the Kestrel ® 3D Energy Probe ™ (3DEP-10).

Remember, in a Moving Target Threat Model the Technical Operator is the Spectrum Analyzer...

The ability to walk the target area and capture localized Power Line (PL) energy patterns for all, or just targeted critical infrastructure as identified by the technical operator is now a powerful reality. The process is as simple as importing a floor plan image of the target area into the | Tap Capture Plot (TCP) ™ | OPT TCP module and loading a predefined or custom Power Line (PL) spectrum profile for mission specific requirements.

The resulting heat map visualization can be utilized immediately to identify potential ambient electrical power grid appearance points that require the operator's further attention, or serve as a powerful baseline reference database for future comparative analysis.

The local electrical power grid is perhaps one of the most vulnerable and reachable networks and has easily compromised communication paths in virtually every business or residential property for which technical security inspections are required. The electrical powerline grid is the one element that has no firewall, no isolation and extends freely beyond the confines of the generally secure exterior walls and doors. Even UPS systems are vulnerable and provide only a limited inconvenience and minor challenge during a targeted espionage related attack of critical infrastructure. Aside from the many existing PL threat technologies and countless existing use cases by the private sector, public utilities, government, transportation sector, etc., there are significant new emerging technological threats that utilize generally unlicensed, unregulated and unmonitored PL spectrum.

Time-challenged technology limitations that once prevented the wide-spread use of PL communication for wideband defensive, offensive, and professional commercial applications; in many cases are silently making a renewed appearance on the electrical power grid every day with staggering new modulation and data streaming capabilities compared to the older bandwidth limited technology of less than a decade ago, much of which changed very little during the past 100 years.

The ability of an attacker (or a compromise via an unintentional radiator) in both theory and practice, to make use of PL technology for active audio, video, and data streaming applications provides a somewhat invisible conduit or path to conductively, inductively, capacitively, or as a radiated Over-the-Air (OTA) signal, transfer vast amounts of intelligence.

Kestrel TSCM ® Professional Software

At Professional Development TSCM Group We Back Up What We Claim Kestrel ® Can Do—One Customer at a Time!

Professional Development TSCM Group Inc. **Technical Security Branch (TSB)**

Unintentional radiators relating to existing authorized, and sometimes unauthorized equipment within the target area that are not intended to pass signals or intelligence onto the ambient power line, but by design or intent of an attacker, accident, poor design, improper wiring techniques (accidental and deliberately), deteriorated physical condition, and many other factors make the inclusion of a competent Power Line (PL) analysis an essential practice for the technical operator during every deployment.

Unfortunately, only doing half of the job, will generally equate to a tenth of the anticipated or expected inspection outcome, as a motivated attacker will always defeat the unmotivated technical operator.

The electrical power grid clearly fits into this thought process and must be considered a technical security best practice.

Another key concern is the unintentional consequences of unauthorized devices being connected to the electrical power grid without an informed understanding of the potential technical vulnerabilities and security risks involved.

In-fact, many devices typically utilized within the private sector and government facilities for security purposes, such as access control systems, video surveillance system components leak potentially recoverable intelligence onto the Power Line (PL) infrastructure.

Very few organizations even give the electrical power grid a second glance when commissioning a new facility or when spending considerable time and financial resources on other aspects of the facility's overall security posture.

There has been a significant shift and surge of new Hybrid PL technologies that have started to appear within commercial and consumer product applications that may utilize an obvious technology that is readily identifiable, and may also have a hybrid Power Line (PL) component within the underlying technology which rarely is understood or assessed for potential technical security vulnerabilities.

Part (2 of 3) of this advanced technical briefing will appear in the June 2020 edition of TSCM | SIGINT Newsletter...

CTSC 2020 | CTO ™ Training Opportunity (Postponed)

The global pandemic has unfortunately required that we postpone the our March 2020 CTO training and the 15th annual Canadian Technical Security Conference (CTSC) ™ as scheduled from March 31, 2020 to April 02, 2020.

We are rescheduling and optimistically looking at July 2020. Please monitor our website for information relating to confirmed dates for both the CTO training and the CTSC 2020 conference event.

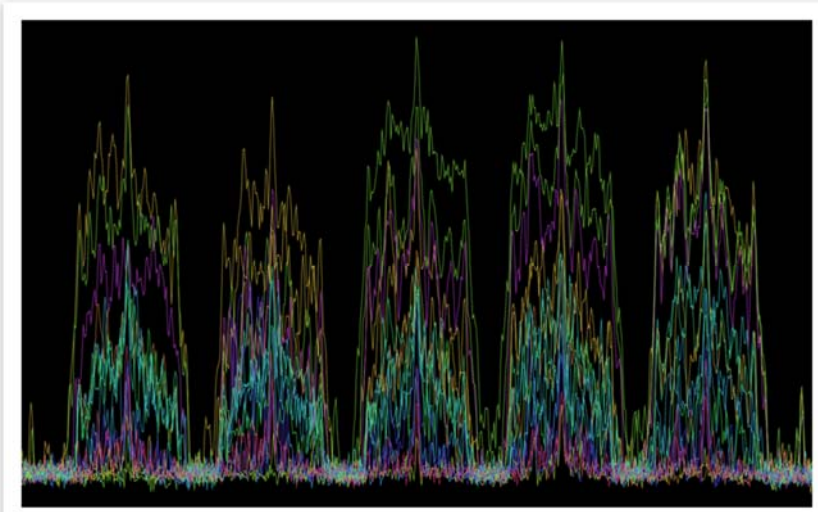
The new event dates are unconfirmed at this time. Please call or visit our website for the most current information.

Innovation is Simply the Beginning!

Visionary Software Beyond the Technology Limitations...

| www.pdtg.ca | www.kestreltscm.com | www.ctsc-canada.com |

| Paul D Turner, TSS TSI | pdturner@pdtg.ca
| Andrzej Wolczanski, TSS | awolczanski@pdtg.ca
| Gabriele Conflitti, TSS | gconflitti@pdtg.ca
| Carol Fairbrother | cfairbrother@pdtg.ca



They say that the value of art is in the eye of the beholder! Every day a new never before seen artistic spectrum is developed within the Kestrel TSCM ® Professional Software somewhere in the world. Whether impressionist, contemporary or abstract, the RF spectrum brings a commonly understood meaning for every professional technical operator who views it...

Kestrel TSCM ® Professional Software is innovative industry leading, disruptive technology, sold in 45 countries worldwide.