Dean La-Vey presents an overview of the development of surveillance devices and TSCM receiver technology, and examines the latest equipment available to TSCM operatives

TSCM: RISE OF THE SPEED KINGS

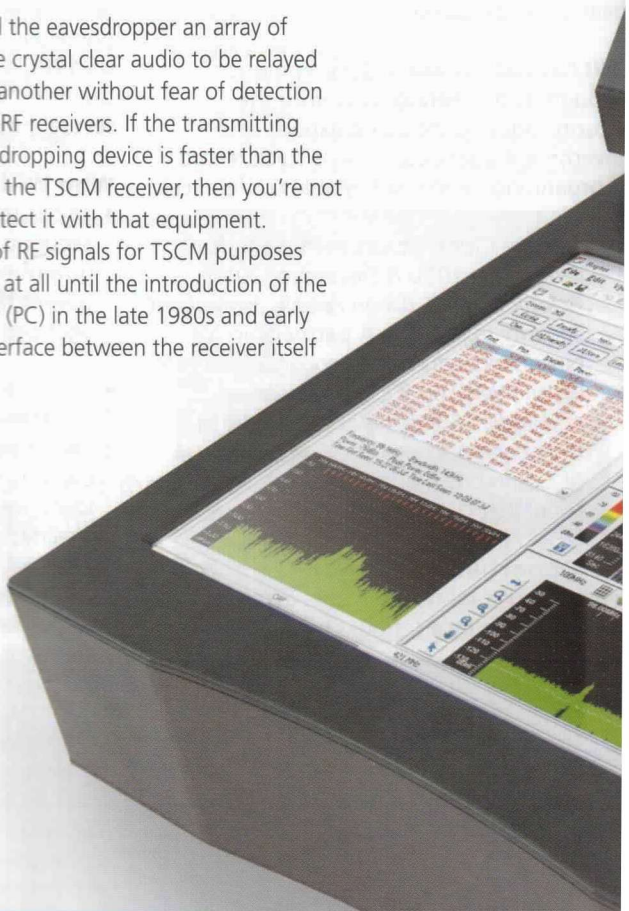
Not so long ago, the search for electronic transmitting eavesdropping devices required a plethora of different receivers, antennas and, more often than not, a 30kg spectrum analyser. It was a long-winded exercise, with each particular band having to be manually tuned into and checked for illicit transmissions. In the 1970s and 1980s, before – GSM, WiFi, Bluetooth and Tetra, etc – it was an easier process following the introduction of harmonic-based receivers to detect such devices primarily via the signal power output of the device itself. The radio spectrum itself was also not that busy. In short, the RF device would have the strongest signal strength in the target area and the RF detection equipment would lock onto it.

The process all changed in the mid 1980s when commercial use of radio transmitters increased dramatically, especially in major cities. The airwaves started to get busy, and bandwidth became crowded. In the UK, the 25kHz commercial bandwidth was halved to 12.5kHz to make more space. More commercial RF traffic allowed eavesdroppers to hide their signals among the abundance of new signals springing up on a daily basis. To confuse things further, the persons (and companies) manufacturing bugging devices offered up new operating facilities on their transmitters, such as sub-carrier and single side band modes of transmission.

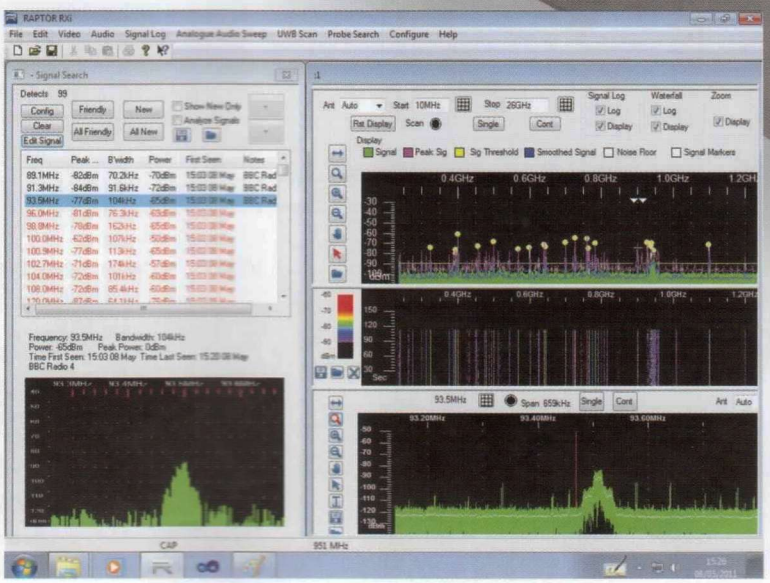
TSCM hit back with demodulation circuits for various transmission modes as attack techniques and countermeasure equipment continued to evolve. Eventually, the eavesdroppers would utilise new methods of transmission using both analogue and digital encryption – transmitters that would hop frequencies, and devices using spread spectrum modes of transmission. It's fair to say that "round one" went to the eavesdropper.

RF (Radio Frequency) eavesdropping transmitters are produced in many formats, with the predominant aim of relaying useable audio and evading detection by dedicated RF detection equipment. Printed circuit board and power management technology of early devices meant that a great many RF devices lacked adequate noise suppression and signal stabilisation. Fast forward to 2011 and it is a seriously different situation. Surface-mounted components, nano technology and, most importantly, speed of transmission afford the eavesdropper an array of options that enable crystal clear audio to be relayed from one point to another without fear of detection from conventional RF receivers. If the transmitting speed of the eavesdropping device is faster than the detection speed of the TSCM receiver, then you're not going to readily detect it with that equipment.

The processing of RF signals for TSCM purposes didn't really evolve at all until the introduction of the personal computer (PC) in the late 1980s and early 1990s, and the interface between the receiver itself



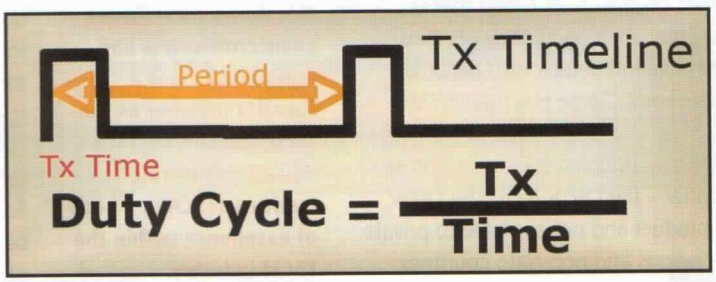
The Raptor RXi



and the software that analysed the signals. It would take some 20 minutes to do one pass up to 3GHz, but you could see both the signals and the signatures of different types of transmission. Having the PC-based receiver allowed storage of signals for future search referencing – albeit only one trace at a time with a monochrome screen. It was, however, a defining point in RF detection equipment. By the time the Intel Pentium processor, low cost memory chips and colour laptops came around, RF detection equipment started to become quite formidable. The time taken for a search from 10kHz to 1.5Ghz was reduced on some equipment down from 20 minutes to around four seconds. Band-by-band searches allowed very detailed inspections of all the signals within the band at a high resolution, and you didn't have to be a rocket scientist to operate the equipment itself.

As computer processing became faster, so the ability to analyse received radio signals became more comprehensive and detailed. Specific types of digital transmissions could now be clearly identified. You couldn't demodulate them, but you could see the physical characteristics of the signal itself, such as the Taj Mahal shapes of spread spectrum transmissions. Inevitably, the speed of the PC greatly exceeded the scanning speed of the receiver itself and things remained static. REI's OPC software package for its Oscor 5000E equipment greatly enhanced its analysis capability and allowed for the first time what is now known as RF mapping. This technique allowed the operator to collect RF data from various places within a search area and then, by trace signal comparison, ascertain where within the area the transmission was coming from. Colour coded reference files could also easily be displayed alongside real-time data. Using the "inverse square law", the search for covert transmitters had become an exact science.

At the serious end of the eavesdropping transmitter family are a group of devices that were developed to deal specifically with existing countermeasure receiver technology. Indeed, some of the manufacturers of such devices purchased TSCM receivers to test their response to custom-made devices. Costing upwards of $6,000 these devices rely on pulse coded technology or packet data transmission. In general, the audio is compressed and transmitted in millisecond bursts and not visible in real time. This meant the receiver had to be run over specific bands for a considerable length of time in order to capture one burst. It could take a period of hours depending on the type of transmission because the receiver technology was not fast enough. A burst transmitter has two modes of operation. The first is the reception of the audio itself and the second is the actual transmission. It is commonly known as the "duty cycle".



TSCM: RISE OF THE SPEED KINGS

The mathematics is not difficult to work out. If your receiver sweeps 1500MhZ in four seconds, how long do you need to run the receiver to catch something transmitting every three seconds in 250 millisecond burst? (answers to intersec). Please note that there are devices that use a combination of spread spectrum, frequency hopping and burst technology.

To research and develop a dedicated TSCM receiver that will adequately detect fast frequency hopping and packet data transmitters involves a great deal of time, expertise and a considerable financial investment. It also requires a support and training programme. This is, however, a two horse race. The Winkelmann Raptor and the REI Oscor Green are light years ahead in the field of TSCM receiver technology. Let's consider the numbers. An Oscor 5000E is a superb piece of equipment that scans 0-1500MHz in around 4.5 seconds. The Oscor Green scans 0-24GHz in under one second, the Raptor to 26GhZ in around 2.5 seconds. LIGHT YEARS AHEAD! Sure, you could get a Rhode & Schwartz or a Tektronix handheld spectrum analyser, but these are not TSCM receivers and are not designed as such. The Oscor Green and Raptor are dedicated TSCM receivers and designed specifically for that purpose.

Both the Raptor and Oscor Green utilise touch screens and integral antennas, although the Raptor is considerable larger in size than the Oscor Green. Both allow rapid detection and analysis of received signals, have built in demodulators and require no set up. Both allow simultaneous display of real time and multiple colour-coded reference data as well as waterfall display and automatic signal list generation. In addition, both have real time oscilloscope and a detailed signal zoom facility. By far the most important feature of both units is the sheer speed of the signal processing. Consider that 0 to over 24GHz takes less than a second. When you narrow the band down you're sweeping in milliseconds, and when you can do that, you can find the most sophisticated of eavesdropping transmitters. The days of waiting hours in the hope of seeing one burst from a packet data transmitter are well and truly over. Round two goes to TSCM.

There is inevitably the question of which is better – the Raptor or Oscor Green? This is a bit like the argument over PC or MAC. There are features on one that some will consider better than the other and vice versa. Certainly the larger screen on the Raptor has specific advantages for some, but the smaller high-resolution screen on the Oscor Green makes no real difference to the job at hand. As with third harmonic non-linear junction detectors, it becomes a matter of personal choice. Some practitioners will have both.

It is also worthwhile mentioning here a small note on the other contender – the Oscor Blue. The Oscor Blue is a restricted product and not available to private practitioners, corporations and non-Nato countries.

Oscor Green is not, as some believe, a dumbed down version of Oscor Blue

Dean La-Vey is specialist security consultant dealing with specialised products and techniques for the government and private sectors worldwide. He frequently lectures and trains such bodies in the use of telephone surveillance countermeasures and equipment. He is a founder member of the Technical Surveillance Countermeasures Institute (TSCMi), a body of excellence within the TSCM industry.

To that effect, there has been an assumption that the Oscor Green is a "dumbed down" Oscor Blue. It's not. In fact, the only difference is that the Oscor Blue has a waterfall trace data recorder and the Oscor Green doesn't. Is it an essential feature TSCM practitioners need? No it's not. The Oscor 5000 had a basic waterfall data recorder and how many peop actually used it? Those that did found it ate up the PC's memory in half a day.

High sales of both the Raptor and Oscor Green will lead to further research and development by both manufacturers, which can only be a good thing. TSCM practitioners must always be aware th eavesdroppers will always come up with new ways relaying audio. You can equate it to those who inve computer viruses and those who develop anti-virus software – it is a constant battle. As good as the Raptor and Oscor Green are now, they can only get better. As to which one this author would have – o of each.