Xi SYSTEMS
Innovative technology for extreme environments

COTS EW Threat

Following the conclusion of the Cold war (1945 – 1990) militaries such as the UK Army have not faced a formal Electronic Warfare threat to tactical systems. This, coupled with the rise of integrated computing systems that have gateway access to the Internet have refocused threat assessments and risk mitigations toward Cyber vulnerabilities including Malware and Advanced Persistent Threats (APT) rather than the hostile act of locating, de-modulating and intercepting the communications on a wireless connection. This, however, will change with the advent and commercialisation of advanced Software Defined Radios (SDR's).

Software Defined Radio (SDR) has its origins in work conducted by the US Department of Defence in the 1970's with the term Software Radio established in 1984 by a team of engineers working for a division of E-Systems. This original concept gained traction with various US governmental agencies, from which modern SDR programmes have developed.

The United States of America's Department of Defence has had several programmes to develop SDR technology towards practical use from these early days. Specifically, the SPEAKeasy programme was developed to demonstrate the

COTS EW Threat

practical use of SDR for the air force that could tune in a range between 2MHz to 2GHz, allowing the integration of Ground, Air, Naval and Satellite radios. Since inception, these new types of radio are beginning to be widely adopted for military and civilian use.

SDR's themselves establish elements of the analogue radio receiver in software, allowing the designer to establish flexible radio designs. Prior to the establishment of SDR platforms, a radio (once designed) was generally fixed in function until a circuit modification was conducted to re-purpose the receiver either for a different frequency band or modulation scheme.

Relatively recent System on Chip solutions from companies such as Lime Micro Systems and Analogue Devices, offer direct Radio Frequency to digital interfaces. These chipsets provide a very wide RF front end (typically KHz – GHz) with RF bandwidth ranges of between 50 and 150MHz. These products, when integrated with a powerful Field Programmable Gate Array (FPGA) and Digital Signal Processing (DSP) produce a powerful SDR platform.

Companies such as Nuand and Ettus Research have developed commercially available implementations that can be integrated with open source software platforms such as GNU Radio and GQRX in order to provide a functioning SDR solution.

These provide a low cost and wide bandwidth capability that can be used to survey a very large portion of the electromagnetic spectrum instantaneously. The pricing of these devices range from as little as £19 up to £6000. This removes the barriers of cost for access to high performance radio receivers that previously kept this capability out of the reach of the hobbyist or hacker.

During a presentation to Defcon 21 Balint Seeber presented a comprehensive overview of the possibilities of using GNU radio along with an Ettus Research USRP SDR platform for intercepting and decoding a wide variety of radio protocols. Using GNU radio as a signals intelligence toolkit Balint was able to intercept Mode S IFF transponders, 2G GSM, 802.11agp, Automatic Identification System (AIS), Aircraft Communications, Addressing and Reporting System (ACARS) along with the automatic toll payment system FasTrak.

The presentation of this research to a wide community of security researchers and self-proclaimed Hackers, started an increased interest in what a SDR can be used for and

COTS EW Threat

what systems could be compromised via the use of traditional EW and SIGINT techniques. The presentation of these techniques and wide availability of source information via the Internet could be seen as a lowering of the technical barrier for these attacks. Since the Defcon 21 presentation, intercept software for AIS and ADSB intercept as shown in Figure 4 and Figure 5 is widely available and easy to install for an inexperienced enthusiast, allowing them to track all commercial shipping traffic within the local area, and using the Internet to identify individual vessels along with information surrounding their route and cargo.

Figure 4 : ACARS intercept as presented by Balint Seeber.

Hex	Mode	Sqwk	Flight	Alt	Spd	Hdg	Lat	Long	Sig	Msgs	Ti-
400e14	S	7315	EZY43PT	37000	419	353			5	42	0
406099	S	7634	CFE59G	38000					5	17	2
484cb6	S	6264	KLM65G	36325	413	297	55.844	-0.518	5	88	0
406a2e	S	7615	GMA104T	28000					4	100	2
400fba	S	5431	BEE1UB	5350					35	733	0
4ca281	S	7322	VIR3007	33175	396	336	54.564	-2.611	12	946	0
400ad1	S	7607		20025					7	208	0
400721	S	4246	LOG47LU	8550					30	955	0
400c5c	S	1444		27025					5	95	32
40610e	S	7330	BEE3FU	24000					9	583	0
400cb9	S	7732	LOG79ES	14500					11	922	0
4012d2	S	5466	LOG34VT	7100					6	83	5
405633	S	6254	EZY44NH	19425	387	149	55.408	-4.174	6	3039	13
400617	S	3416	TCX61EF	21550	439	108	55.364	-3.253	16	5062	0
405f79	S	4477	BEE767	19125					38	6845	0
400984	S	4622	EZE28Z	21475					12	3243	0
4ca73d	S	4244	RYR6699	3250	156	279	56.017	-3.135	81	6853	0
400987	S	4621	EZE76LK	23475					11	6841	0
400691	S	7762	BAW9CG	32675	458	317	56.386	-4.997	11	16051	0
4066d1	S	2227	TOM296	33225	488	151	54.700	-3.405	8	8244	0
4008fb	S	7655	LOG24HR	17600					10	5627	0
491304	S	7646	CSDXD	40000					8	5268	0

Figure 5 Raw ACARS messages decoded by open source software and a RTL-SDR SDR dongle.

As can be seen, modern SDR platforms are highly capable and with software such as GNU radio available, provide a very capable threat source to all wireless networks. This threat can be characterised in two distinct ways:

- Intercept – the capture and decode (by a third party) of messages transmitted between two other parties.

- Jamming – the prevention of wireless transfers either through the use of in band RF noise, swamping the Signal to Noise Ratio of the Receiver or conduct an attack at a protocol level, inhibiting the data transfer.

COTS EW Threat

Most radio systems are deployed without physically testing the vulnerability of the link layer, it is probable that many wireless systems have been deployed with an inherent vulnerability due to miss-configuration.

This is relevant outside of the Military domain as systems such as Vehicle to Vehicle, Vehicle to Infrastructure, Industrial Control, Security & CCTV and Critical National Infrastructure will have a common vulnerability and attack vectors due to the use of wireless and openly published protocols.

SDR's are a threat to the RF transport layer previously thought only to be vulnerable to either a very well trained third party equipped with a large Electronic Warfare capability or a stolen radio receiver from the intended target. SDR products such as the Ettus Research E310 along with GNU radio now allow people with little Radio Frequency (RF) engineering experience (described as 'script kiddies ' within the hacking community) can undertake interception of complex radio platforms such as Tetra or ACARS via a download of plugins for the GNU radio platform. Largely these intercepts are achieved due to the reverse engineering of known protocols and the use of the SDR to provide a wide bandwidth and high speed receiver. This highlights vulnerability in systems that provide a portion of the UK's Critical National Infrastructure (CNI) to intercept by a third party. Internet sources highlight this has been achieved in the UK against live TETRA systems but it is unclear what TETRA users have been targeted or how much information was retrieved from the system.

As military communication adopts a more commercial based architecture, the security of these waveforms and modulation techniques require deeper analysis. In contrast the commercial use of these waveforms and protocols need protection from Intercept as the EW threat that used to be confined to nation state actors, such as Intelligence or Military units, is now available to hobbyists and hackers alike, providing an increased likelihood of the threat.

If this subject interests you, please get in contact (contact@xisystems.co.uk), we are happy to provide assistance and training.

+44 (0) 1458 730140 | info@xisystems.co.uk | www.xisystems.co.uk
The Timber Store, Great Bow Wharf, Bow Street, Langport, Somerset, TA10 9PN
Company Registration No: 07423264 | VAT Registration No: 100754064 | Registered in England and Wales.