Wireless Communication Security: Software Defined Radio-based Threat Assessment

Ballantyne, Simon

Award date:
2016

Awarding institution:
Coventry University

Wireless Communication Security: Software Defined Radio-based Threat Assessment.

by

Simon NT Ballantyne CEng MIET MCGI

Degree of Master of Research

May 2016

Wireless Communication Security: Software Defined Radio-based Threat Assessment.

by

Simon NT Ballantyne CEng MIET MCGI

May 2016

A thesis submitted in partial fulfilment of the University's requirements for the Degree of Master of Research

ABSTRACT

The rapid evolution of radio technology into the software defined era, has accelerated the availability of advanced radio receivers that can cover very large portions of the radio spectrum (70MHz to 6GHz) at low cost. Coupled with the democratisation of knowledge that has occurred through the internet, the threat environment for Electronic Warfare (EW) has changed markedly over the last 5 years. Previously EW threat would have arisen from a state actor that could fund the expensive equipment and antenna arrays that would be required for the intercept and disruption of military signals activities. Instead it is now possible to download freely available software to launch EW attacks on widely publicised radio link standards.

The aim of this research is to explore the security of wireless communication systems when exposed to threats generated by Software Defined Radios (SDR). The research is aimed at exploring this vulnerability due to the rapidly decreasing cost and the lowering of skill barriers to launch advanced EW attacks on wireless communication systems.

The first objective was to understand what current knowledge exists on the EW threat on the RF environment, allowing an understanding of this advanced threat against wireless infrastructure. The literature review has showed that the vulnerabilities of wireless networks are in existence and there are potential methods of protection that have been studied, although these protection schemes do not seem to have been implemented in production quality systems.

The second objective is to validate this prognosis against a test bed, constructed as a threat source that could be typical of a hobbyist or script kiddie, allowing two threat scenarios to be demonstrated, validating the threat source. This research included the execution of two laboratory based attacks against wireless systems, namely a record and replay attack against the Personal Role Radio (PRR) and a Meaconing attack against GPS. These experiments showed that a flexible Vulnerability Analysis test bed can be assembled to conduct Vulnerability Investigation against wireless standards. Specifically, this also showed the Vulnerability of the PRR radio against record and replay attacks.

Keywords: Cyber Security; Software Defined Radio; Waveform Vulnerability; Threat Assessment; Cyber Vulnerability Investigation (CVI).

DECLARATION

I hereby declare that this project is entirely my own work and where I used the work of others it has been appropriately acknowledged. I also confirm that the project has been conducted in compliance with the university ethics policy and that ethics related

information submitted with the original proposal corresponds with the work actually conducted

ACKNOWLEGEMENTS

I would like to acknowledge the following people, who provided assistance to the creation of this thesis,

Siraj Ahmed Shaikh for the supervision and mentorship he provided during the study.

Tim Carlton MININCOSE MBCS who at the beginning of the research directed myself to appropriate people within Dstl for guidance. In addition, he also provided valuable research direction based upon current Dstl and MOD interests within the Cyber Security research programme.

CONTENTS

List of Figures

List of Tables

1 INTRODUCTION

1.1 Aims and Objectives

The aim of this research is to explore the security of wireless communication systems when exposed to threats generated by Software Defined Radios (SDR). The research is aimed at exploring the ability for SDR platforms to counter common wireless network security mechanisms for link layer protection. This research has been targeted at answering two specific objectives:

The first is a systematic threat characterisation using detailed literature review. This is documented within Chapter 3 and explores the historical context to understand the current threat to the wireless link layer and the current published research into countering these vulnerabilities from intercept, jamming and spoofing. This includes academic sources as well as sources from within the Hacking community.

The second is a threat validation experiment which sought to validate two specific link layer threat scenarios that explore the ability of record replay and meaconing attacks to disrupt wireless networks. These scenarios exploit the availability and performance of commercially available Software Defined Radio platforms that are available for the hobbyist and researcher. To complete this, a dedicated test bed was set up replicating the equipment and software that a low capability Hacker may have at their disposal.

1.2 Context

This research is being carried out within the context of an ever increasing integration of mobile computing elements within the United Kingdom's (UK) System of Systems (SoS). This architecture is providing ever more accessibility to data and Internet Protocol (IP) bearers to deliver critical information to decision makers. This is in parallel with the rise of the Internet of Things (IoT), which is interconnecting previously innocuous sensing technology to the Internet, in order to provide value added services to the wider community. As the IoT grows, it is likely that the enabling wireless infrastructure will come under attack from

researchers and hackers alike. This may see a widening of EW style attacks being used against civilian infrastructure by non-state actors[1].

These seemingly disparate applications will face common vulnerabilities to the passage of wireless data. Wireless systems are vulnerable to a multitude of attack vectors that if used against wired networks would require some level of physical access to that network to conduct. For instance, wireless networks are vulnerable to the injection of inconsistent or incorrect data, man in the middle attacks against the system integrity (eavesdropping), or simple jamming to deny the availability of the system.

Denial of Service (DoS) and Distributed DoS (DDoS) attacks against websites is prevalent on the Internet, causing disruption for organisations, either through the disruption of revenue in the case of an on-line store, or the reduction in credibility. Examples of this have already been reported within the UK. (Dunn, 2013) is a published report from a study by the UK Technology Strategy Board, where up to 100 GPS jamming events a day were identified to be originating from van drivers that have purchased illegal, but commercially available GPS jamming devices to stop their vans being tracked by employers. Searches of the Internet (jammer4uk, 2015) show how rapidly GPS, Wi-Fi and cellular jammers can be purchased and illegally operated.

Current wireless protocols and waveforms for civilian infrastructure such as 802.11 do not include protection against Jamming or Spoofing. Instead the wireless security is solely aimed at protecting the confidentiality of the data. As society becomes increasingly reliant on wireless communications to undertake our critical tasks such as banking, access to assets and handling medical data, the vulnerability of current security mechanisms will be pushed and increasingly exploited.

The same issues and threat mechanisms that are being explored within civilian implementations have been the focus of militaries since the days of World War 1. Militaries implemented cryptography to protect confidentiality swiftly followed by the implementation of techniques to conceal and obscure their wireless transmissions. It may be time where these techniques are considered for

[1] Non-state actors relates to threat sources that do not originate from the control of a nation state. i.e terrorist, individual hackers etc.

commercial systems. The tension between the publishing of standards openly along with the requirement of ubiquitous interoperability are counter to the principles of obscuring and securing wireless transmissions, ensuring the cycle of vulnerability and counter measures will continue for the foreseeable future.

1.3 Exclusions

This research was conducted using open source information sources and subscription based research journals. The MOD and Dstl (the UK MOD's research and development organisation responsible for the research and development of sensitive technology directly related to use by the MOD) have not contributed source material, in order to ensure this work is able to be openly publishable. Initial email discussions with Dstl has provided direct input to the direction of this research.

1.4 Thesis Structure

This thesis has been structured in order to outline the threat under which wireless networks operate as well as enumerating that threat and demonstrating example threat vectors.

Section 2 – Fundamentals of wireless security introduces the threat vectors that wireless networks are vulnerable to. This outlines the concepts of Information Assurance, Security and vulnerability in order to provide the fundamentals that the Systematic Threat Survey is conducted.

Section 3 – Systematic Threat Survey uses the literature in order to outline the known vulnerabilities to wireless networks. This covers all of the vectors as described within Section 2. The Threat Survey also catalogues some advanced mitigation techniques that have been identified as potentially beneficial in mitigating the identified vulnerabilities.

Section 4 – Methodology explains the summarised threat and defines the experimental construct as explored within Section 5. Section 4 outlines the test bed setup and the limitations imposed on the experimentation.

Section 5 – Results and analysis, explores the results from the experimentation conducted, this includes the two threat vectors explored, Record and Replay along with an attempted Meaconing attack against GPS.

Section 6 – Conclusion and future work concludes the thesis, within this section the conclusions arising from the experimental work along with its impact and recommendations for future exploration are made.

1.5 Contribution

Given the ubiquitous nature of modern digital transmission, and the threat from intercept and spoofing, more protection is required to prevent demodulation or even identification of these signals. Although encryption techniques such as ULTRA and SSL are technically very hard to crack under brute force attack, the common fact is that human imperfections in the implementation of that encryption has led to their vulnerabilities.

This leads to a fundamental conclusion that the physical wireless signal requires a new technique to either mask it or to prevent a third party from being able to de-modulate it. There appears to be no lack of viable protection schemes within the literature. Instead seemingly what is required is a commercial drive to implement a new generation of wireless protocols, enabling secure exchanges of information. With vulnerabilities relating to the introduction to Vehicle to Infrastructure, Vehicle to Vehicle or simply ad-hoc connections, the requirement to secure wireless infrastructure will only increase in importance.

2 FUNDAMENTALS OF WIRELESS SECURITY

2.1 Introduction

Before the specific threats to wireless security are explored, a definition of the threat vectors is required. This section explores the principles of wireless security and the potential threat vectors that exist for these systems along with the threat environment in which they operate.

2.2 Principles of Wireless Security

Security of electronic systems, whether wireless or wired can be attained to three different factors; the Confidentiality, Integrity or Availability of the information that is being either processed, communicated or stored.

2.2.1 Three modes of protection

The **Confidentiality** relates to protection of private information from an unauthorised third party. This can be related to the encryption of either the transport layer or payload within a production system. Technologies such as Secure Sockets Layer protect the confidentiality of data and is implemented within the transport layer as defined by the (ISO/IEC, 1989) Open System Interconnection (OSI) 7-layer model. This encryption can also occur within the Application and Presentation layers, dependant on the application under analysis.

Integrity is the assurance that the data received by an end system is unaltered by a third party. Typically, cryptographic authentication mechanisms can be used to protect systems against attacks surrounding their integrity. These may either take the form of message authentication codes or digital signatures, which use one-way cryptographic hashing to produce a unique code based on a shared secret key. This should not be confused with the use of Cyclic Redundancy Checks (CRC) as a mitigation for data corruption. CRC's are vulnerable to exploitation as they are normally based upon a linear stream cypher. This has been exploited to crack Wired Equivalent Privacy (WEP) that was used to protect early WiFi networks.

Availability relates to the presence of the signal or system to continue to deliver its intended function. For instance, the availability of Network Time Protocol can

cause clock synchronisation drift in systems where time synchronicity is a key control element, denying the systems prime purpose – for instance a cryptographic identity server protecting system logon requests.

An adversary may choose to use one, two or all three of these attack vectors in order to produce disruption for a targeted system. When relating these vectors to wireless systems, their broadcast nature can be interpreted as leaving them incredibly vulnerable to any of these attacks.

The three mechanisms of security are countered by three mechanisms of attack: Interception, Spoofing and Jamming.

2.2.2 The three mechanism of attack

Interception seeks to extract the information being communicated by a system, whether it's the digital payload or an analogue encoded voice message. Interception normally requires the third party to extract the information without affecting the integrity of the signal in question, however within a wireless system this is not required as passive techniques can be used to de-modulate and de-code the signal of interest without the target being aware. Due to this, it is difficult to detect an intercept attack that is in progress on a wireless network. These attacks can be carried out against the prime Radio Frequency (RF) emanations or against the unintentional RF emanations from electronics, a practice that has been given the code name of TEMPEST by western governments.

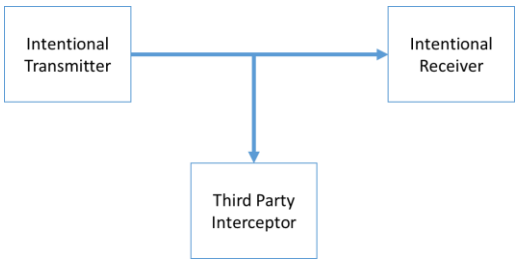


Figure 1 - Wireless Intercept

Spoofing typically involves injecting crafted packets into wireless systems causing either subtle effects, for instance an increase in Bit Error Rate (BER), or bulk errors in data. One of the most prominent examples of spoofing is the corruption of Global Positioning System (GPS) location data. Recent sources (Christian Science Monitor , 2011) have indicated that downing of a USA Department of Defence (DoD) Unmanned Air Vehicle was related to GPS

spoofing activity, however this has not been officially confirmed by the US air force.

The detection of spoofing events is feasible due to the active nature of the signal injection; however, a well-crafted spoof attack leaves no residual signature after the attack.

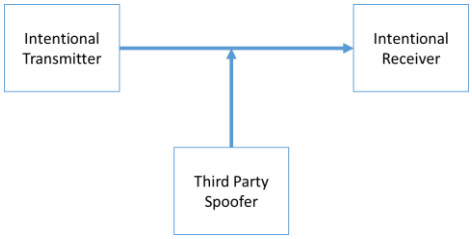


Figure 2 - Spoofing

Jamming is the process of injecting noise into a RF channel in order to deny its availability. There are various jamming techniques varying from Barrage, which indiscriminately blocks single or multiple radio channels; Reactive, which seeks to stay silent until the target waveform is detected; or protocol, where the protocol layer of the wireless signal is interfered with to disrupt its operation. Jamming attacks by their nature are noisy and easy to detect, however when conducted with sufficient power they are difficult to counter, unless the target systems has sufficient RF bandwidth that spreads the signal past the capabilities of the jammer. Jamming although easily identifiable is the easiest attack vector against wireless networks not requiring fundamental knowledge of the target waveform. Distributed and co-ordinated jammers have the potential for blocking access to wireless services over a large area. If applied to a service such as Tetra in the UK, could remove access to primary Blue Light emergency communications for a local area.

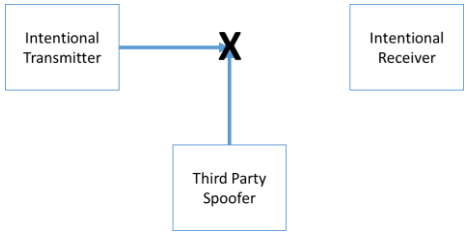


Figure 3 - Jamming

2.3 The Wireless Threat Environment

The nature of electromagnetic propagation ensures that when a wireless signal such as a Wi-Fi network, Personal Mobile Radio (PMR) or car remote key fob is used, it is not solely directed to the intended recipient, instead it is broadcast openly and is limited only by the rules of physics and the interplay of the physical waveform and its surrounding environment.

Given these constructs, equipment such as Low Noise Amplifiers, Directional Antennas and signal processing techniques can allow an adversary to recover signals far beyond their intended range. This ensures that no wireless transmission can ever be regarded as private and confidential. Given the increasing amount of personal data relating to banking, safety of life[2] being transmitted via wireless networks, the requirement to protect against an adversary increases.

Protection mechanisms exist to increase the protection of a systems Confidentiality, Integrity or Availability, however the cycle of protection mechanism and eventual defeat via threat technology[3] is testament to the continued vulnerability of these systems.

The wireless threat environment used to be restricted to those that possessed specialist knowledge and expensive equipment. These were normally Radio Ham operators who had access to limited equipment or Governmental/ Military specialists who had access to both complex equipment and the training in order to conduct these attacks. Developments of Bits to RF direct conversion, enabling a new generation of cheap Software Defined Radios have removed these limitations in terms of access to technology, and the Internet has democratised the access to knowledge leaving a potent mixture of enhanced risks that wireless networks are now exposed to. Given the ubiquitous nature and the sensitivity and safety in relation to data that is now passed over these connections, threats that were once related only to a military operation are now potential attack vectors that should be taken into account within civilian infrastructure.

[2] Such as emergency medical assistance, medical device connectivity or protective monitoring.
[3] Threat technology relates to any technology that defeats a security mechanism, this could be Software Defined Radio, a specific software vulnerability or jamming technique.

2.4 Impact from the loss of Wireless Communications Security and Integrity

The premise of this thesis was based upon the understanding and experience of threats to wireless networks within the Defence and Security environment. It is easy to understand that within this environment there is a direct correlation between the vulnerability of a wireless system and its impact on the safety of persons.

Within the Defence environment, wireless systems are used to pass information relating to the command and control of specific military capability. This could be a formation of troops, vehicles or large platforms such as a Submarine, Ship or Aircraft. These communication systems have been well protected in order to ensure their continued operation when under attack from a third party, preventing disruption to their operation. In this scenario it is perceivable that a vulnerability within the wireless connection could lead to a fire control order being erroneously raised, prior knowledge of an attack being gained or even direct control of a remote weapon system.

(Christian Science Monitor , 2011) has reported on real world examples where the Predator drone video downlink had been intercepted and used by insurgent actors in order to gain an understanding of the Predator operations against them. This relied on intercepting and decoding the signal that was being used by forward deployed soldiers to watch insurgent activity.

What hasn't been so clear has been the direct impact form these form of attacks on Civilian infrastructure, systems and services. Technology developments such as the Internet of Things, Vehicle to Vehicle, Vehicle to Infrastructure and Autonomous Vehicles will drive towards an increasing role of wireless communications that support safety critical services. These services could have direct impact on safety of life. Aside from these new developments, services such as Tetra, GPS and rail signalling all are based upon wireless standards that could be compromised and provide a real threat to life and safety if exploited.

2.5 Conclusion

Given the broadcast nature of wireless networks, they face a wider scope of attack vectors than physically cabled networks. This is a factor that has been recognised by Defence and Security users in the conduct of conflict. As wireless

networks are increasingly relied upon for day to day life, so will these networks come under attack from these various attack vectors.

3 SYSTEMATIC THREAT SURVEY

3.1 Introduction

This systematic threat survey has been written in order to place into historical context the threats that wireless networks face. This uses the military history of attacking wireless networks to demonstrate the evolution of protective measures, followed by an examination of typical and known vulnerabilities in key Civilian infrastructure. Lastly it covers research that has been conducted into the protection of systems, covering some new and novel approaches that could be used to counter the threats explored.

3.2 Historical Discussion of Wireless Vulnerabilities

Since the use of wireless communications technology within the military environment, the intercept of these communications and the use of intelligence arising has provided valuable advantages. (Bartholomew, 2002, 2006) documents the advent of electronic interception of wireless communications as early as the Boer Wars (1900), where the Royal Navy used early Marconi wireless sets in the late 1890's along with the British Army's use of some limited wireless communications. The Boers used captured British radio sets to transmit vital information, which was intercepted by the British forces.

The first properly documented examples of significant use of Wireless Intercept was prior to and during World War 1. The National Security Agency (NSA) (USA agency responsible for Signals Intelligence (SIGNT) and Information Assurance (IA)) has published papers on the history of wireless intercept. One paper, (Flicke, 1954) explores the early use of intercept from the perspective of a German intelligence officer. This paper describes clearly the military and political advantage that is sought and won through the intercept of sensitive communications. Since these early examples, most nations have taken part in these activities. Famously Winston Churchill was reported to have told King George VI ""It is thanks to the secret weapon of General Menzies, put into use on all the fronts, that we won the war!" further to this, Sir Harry Hinsley (Hinsley, 1996) argued that Ultra[4] shortened the war "by not less than two years and

[4] Ultra was the designation adopted by British military intelligence in June 1941 for wartime signals intelligence obtained by breaking high-level encrypted enemy radio and tele-printer communications at the Government Code and Cypher School (GC&CS) at Bletchley Park.

probably by four years"; and that, “in the absence of Ultra, it is uncertain how the war would have ended”.

In the years since World War 2, Military communications security has developed in order to minimise the risk of intercept and successful decoding of the contents. During and following World War 2, up to the 1980’s, the British military relied on the Slidex manual cypher system (Kruth, 1984), which was replaced with the Battle Code (BATCO) paper based cypher system, eventually replaced in 2010 by the secure Bowman communications system.

The UK Ministry of Defence (MOD) command and control systems have become increasingly interconnected over the last 15 years via the introduction of Network Enabled Capability (NEC) doctrine and technology development, around the time of the second Gulf War (2003). Since this advent Military doctrine has shifted towards being network rather than platform centric, allowing a modern military to maintain Information Superiority, the ability to get the right information to the right people at the right time. In order to achieve this, the adoption and exploitation of digital data services were central to the roll out and establishment of modern Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities. Early NEC enabling systems such as Bowman and the US Secure Channel Ground-Air Radio System (SINCGARS) relied on waveform security and secure encryption of data payloads in order to resist electronic intercept. The waveform security is generally provided by frequency hopping behaviours that continually change the transmission frequency based upon either a pre-determined look-up table or a proprietary algorithm. These behaviours are classified as having the properties of a Low Probability of Intercept (LPI) or Low Probability of Detect (LPD). The frequency hopping characteristics, along with nation specific encryption modules[5] provide a very secure means of communications, resistant to intercept and decoding.

During recent operations (Operation TELLIC[6] and Operation HERRICK[7]) the UK forces have operated within differing circumstances and facing a different threat to what existed during the Cold War. During Operations TELLIC and HERRICK,

[5] UK CESG Developed Pritchell II or USA NSA developed WALBURN, PADSTONE or WEASEL
[6] Codename for the United Kingdom’s military operations in Iraq between 19 March 2003 and 22 May 2011
[7] Codename for the United Kingdom’s military operations in Afghanistan between 20 June 2002 and 12 December 2014

threats faced by UK forces were asymmetric in nature and assumed to be lacking an Electronic Warfare element due to the lack of a nation state adversary. On this backdrop of threat and extended operations, the integration of services have evolved within UK and Coalition[8] operations to a point that data can reach from the UK Joint Forces HQ all the way forward to a theatre of operations, and even down to deployed individual sub-units via the Bowman communications system and its integration with high level communications such as Falcon and Reacher. This integration has been achieved by the increasing adoption of commercial standards and equipment in order to bring into service high bandwidth communications and interoperability between systems for Operation HERRICK.

Reporting by the international press highlighted the relative vulnerabilities that were appearing in US communications systems through the use of un-encrypted communications due to either complacency to threat or through the rapid deployment and evolution of capability such as the Predator Remotely Piloted Air System (RPAS) (Noah Shachtman, 2012). This vulnerability was exploited by insurgent forces to monitor the live feeds of Predators operating over Iraq. No publicly attributable data exists on how this may have affected operations, however at a minimum the insurgents would have been able to understand the Electro-Optic (EO) Surveillance capabilities, the techniques and tactics of ground forces being directed, surveillance patterns etc. This vulnerability was exploited through the use of a commercially available satellite TV decoder[9] and receiving interface. Over the preceding years the US military have rapidly fielded encrypted and hardened waveforms for the predator fleet in order to counter this specific threat.

These threat vectors, although seemingly specific to a military environment, have direct applicability to the Internet of Things (IoT). The IoT can be described as the proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data – primarily via wireless mechanisms. The IoT as well as developments for Vehicle to Infrastructure (V2i) and Vehicle to Vehicle (V2V) communications that enable next generation capabilities such as autonomous behaviours are currently vulnerable to wireless link layer attacks. These include demodulation and the cracking of encryption, all classical attacks that previous generation military

[8] ISAF – International Security Assistance Force, NATO lead coalition for security in Afghanistan
[9] SkyGrabber - www.skygrabber.com

systems were hardened against. The vulnerability of these wireless communication systems is being tested by hackers. Lessons that have seemingly been unlearnt within military communications may potentially provide answers to the future of securing the IoT against a range of attackers, ranging from the seemingly benign through to the malicious.

3.3 Threat Device Accessibility

"The power of choosing good and evil is within the reach of all." Origen

Since the conclusion of the Cold war (1945 – 1990) militaries such as the UK army have not faced a formal Electronic Warfare threat to tactical system. 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, 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, 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 (Johnson, 1985). This original concept gained traction with various US governmental agencies, from which the 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 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. From this basis the SDR has gained momentum and is forming the basis of Military radio architectures including the US Joint Tactical Radio System.

SDR 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[10] 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 as high as £6000. (NooElec, 2015) This removes the barriers of cost for access to high performance radio receivers (Jones, June 2012) that previously kept this capability out of the reach of the hobbyist or hacker.

Manufacturer	Model	Frequency Range	Instantaneous Bandwidth	FPGA	Retail Price
Ettus Research	USRP B210	70MHz - 6GHz	56MHz	Xilinx Spartan 6	£840.00
Ettus Research	UBX Daughter card and X310	10MHz- 6GHz	150MHz	Xilinx Kintex-7	£4,500.00
Great Scott Gadgets	Hack RF One	1MHz - 6GHz	20MHz	CPLD not FPGA	£243.00
Nuand	Blade RF	300MHz - 3.8GHz	28MHz	Cypress FX2	£419.00
Nooelec	RTL-SDR	24MHz-1766MHz	3.2 MHz	NA	£19

Table 1 Commercially available Software Defined Radios

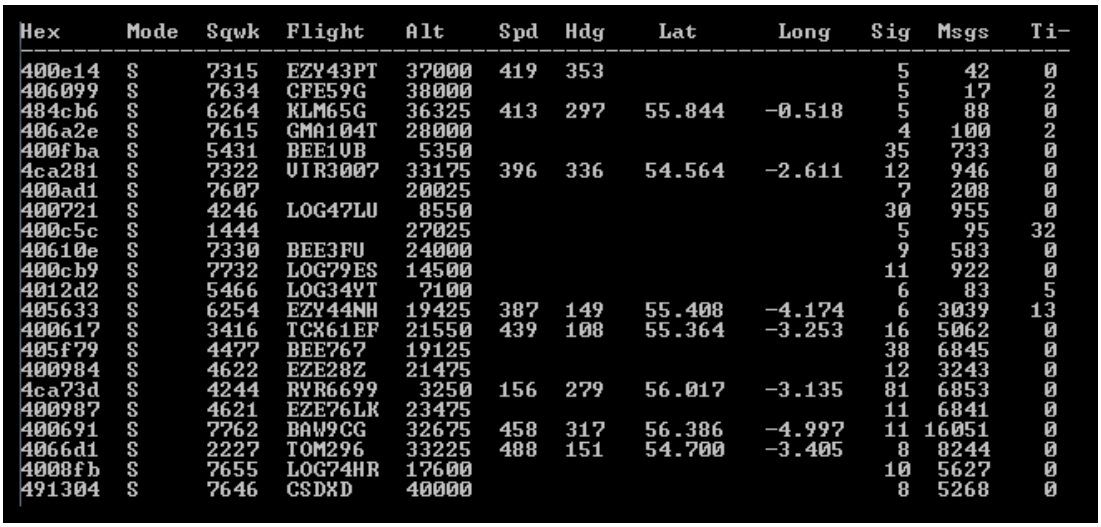
The SDR's presented within Table 1 are all compatible with GNU radio[11], which is an open-source software development toolkit that provides signal processing blocks to implement software radios. GNU radio provides a relatively easy graphical work flow interface in order to programme SDR platforms. This toolkit

[10] http://www.limemicro.com/
[11] http://gnuradio.org/redmine/projects/gnuradio/wiki

allows SDR applications to be created either through the use of a graphical flow chart or to be written in Python.

During a presentation to Defcon 21 (Defcon 21, 2013) Balint Seeber recognised 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 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 unexperienced 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	BEE1VB	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	LOG34YT	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	LOG74HR	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 noised, swamping the Signal to Noise Ratio of the Receiver or conduct an attack at a protocol level, inhibiting the data transfer.

(Jones, June 2012) argues that as 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 and CCTV and Critical National Infrastructure will have a common vulnerability and attack vectors due to the use of wireless and openly published protocols.

The following sections explore these two methods and the existing research surrounding the generation and protection against these methods of wireless network compromise.

3.4 Threat Vectors

3.4.1 What is the threat from intercept?

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[12] now allow people with little Radio Frequency (RF) engineering experience (described as 'script kiddies[13]' within the hacking community) can undertake interception of complex radio platforms such as Tetra (RTL-SDR, 2014) or ACARS (RTL-SDR admin, 2013) 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 vulnerabilities in systems that provide a portion of the UK's Critical National Infrastructure (CNI) to intercept by a third party. Internet sources highlight that this has been achieved in the UK against live TETRA systems (Shadow, 2013), but it is unclear what TETRA users (Ofcom, 2015) have been targeted or how much information was retrieved from the system.

3.4.1.1 ERTMS and GSM Vulnerability to Intercept

Further to the availability of intercept software for trunked radio systems, recent research conducted on the European Rail Traffic Management System (ERTMS) has shown that it is vulnerable to Cyber threats (Pultarova, 2015). In fact it appears to be vulnerable from electronic intercept from SDR, due to the use of GSM-R (derivative of GSM) bearer for trackside communications. Figure 6 (Banedanmark, 2008) illustrates the protocol specification for GSM-R, highlighting the implementation of the standard GSM protocol, suggesting that GSM-R may be vulnerable to the same link layer security vulnerabilities within GSM.

[12] www.gnuradio.org

[13] A person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own.

Figure 6 GSM-R protocol specification taken from (Banedanmark, 2008)

Several websites are available that show this vulnerability of GSM to intercept and decoding (Casanovas, n.d.) provides clear instructions on how this can be achieved, and provides step by step instructions on how to create a capable setup. (Gold, April 2011) explores the recent (since 2003) rapid circumvention of security within the GSM standard.

Several high profile security researchers such as Chris Paget (Defcon 18, November 2013) have demonstrated practical man in the middle attacks against the GSM standard via IMSI catching. During this attack, GSM handsets attach to a malicious base station and transfer all data and call traffic through the malicious base station, allowing intercept. Work by Karsten Nohl of Security Research Labs and Sylvian Munaut of OsmcommBB presented further enhancements on Paget's work by using a pre-computed table for all A5/1 encryption hashes. This work allowed the real time decode of all GSM calls on a nearby base station in real time (Info Security magazne, Dec 2009).

Clearly the potential for intercept and modification of data running CNI such as TETRA and the ERTMS systems is highly worrying and leaves questions open as to how the cyber security of these systems have been penetration tested or analysed against well published attack vectors. As stated previously in this paper, these attacks are well documented and are available to malicious actors that possess the technical credibility of 'script kiddies'.

3.4.1.2 Wi-Fi Vulnerability

In theory any wireless communication systems that can be de-modulated can be subject to this technical intercept. WiFi networks based upon 802.11abg are

vulnerable to the cracking of Wired Equivalent Privacy (WEP), Wifi Protected Access (WPA) and WPA 2 link layer encryption (Tsitroulis, et al., 2014).

In 2004 the Aircrack Wi-Fi password cracking suite was released, which allows the recovery of cryptographic keys from WEP and WPA-PSK secured Wi-Fi networks. This attack was generated, based upon a variety of techniques such as dictionary attacks, and Stream Cypher attacks (Stubblefield, 2001) (Flugrer, Mantin and Shamir (FMS)).

(Martin Beck, 2008) (Founder of Aircrack) demonstrated within his paper vulnerabilities within the WPA protocol. This paper explored a dictionary attack when a weak pre shared key (PSK) is used. The attack works if the network is using TKIP to encrypt the traffic. An attacker, who has about 12-15 minutes access to the network is then able to decrypt an ARP request or response and send 7 packets with custom content to the network. This shows obvious weakness in a previous thought to be secure protocol.

These examples of intercept, cracking of link layer encryption illustrates a requirement for protecting the wireless network from demodulation by a third party. (Katabi, 2010) explores a protection scheme for OFDM based wireless communications that prevents an unauthorised third party from de-modulating the signal of interest whilst maintaining a practical wireless channel. This is applicable to OFDM modulation schemes that are widely adopted by WiFI, WiMA, LTE and several commercial MANET implementations, potentially preventing previously mentioned attacks against WEP and WPA from taking place.

3.4.1.3 Distributed Intercept

For Defcon 21, Brendon O'Connor presented a distributed sensor network that combines wireless network intercept, distributed command and control along with a 3D Visualisation engine in order to demonstrate the ability to track people. This presentation demonstrated that with access to the packet header data (not encrypted payload) various aspects of the victim's device can be interpreted in order to either geographically tack between locations or to launch more detailed attacks against known vulnerabilities. Given that SDR with aforementioned attack programmes against the likes of GSM, TETRA, et al, it would be relatively easy to deploy a distributed attack network within an urban environment that could monitor multiple wireless networks and protocols within a co-ordinated SIGNINT

attack. Although only theoretical at this time, with up to 150Mhz bandwidth being available concurrent attacks could be conducted across large swaths of the electromagnetic spectrum, seemingly only limited by the processing power of the host computer and communication interface with the SDR.

Although seemingly a step away from military scenarios, the vulnerabilities that have been explored are directly applicable to military devices and systems. For instance, Military radios such as Selex's Personal Role Radio (PRR) are available via online resellers and could provide a test bed against which reverse engineering attacks could be researched and tested. Given the published data sheets by Selex it would be relatively straightforward to engineer an intercept. The link layer is based upon Direct Sequence Spread Spectrum Modulation (DSSM) transmitting at 2.4 GHz using CVSD to encode the voice traffic. The standard GNU Radio build includes all blocks required to intercept and decode the PRR. Given the lightweight nature and ease of use the PRR is a preferred medium of communication for the Dismounted Platoon and is used regularly as the prime radio network of the dismounted Platoon within the UK army. Further to this, modern radio solutions such as Persistent Systems MPU range of radios use standard 802.11 link layers that could be vulnerable to a decode and intercept attack.

3.4.1.4 Countering Intercept

iJam provides a PHY layer technique that protects sensitive pre-amble and header packets which can be exploited. Operation iJam is designed to work collaboratively by randomly jamming a repeated handshake packet. Due to the synchronisation of the receiver it can initiate communications, however this is not evident to a third party intercept. The paper presents threats from the interception and demodulation of wireless signals by an unauthorised third party. This allows the exploit of password protection schemes such as WPA2-PSK from openly available toolsets such as Backtrack and Kali Linux. The challenge is to inflict the jamming within an approach that is not susceptible to the detection of jammed bits from clean samples.

The research implementation is relatively efficient allowing a 16-QAM receiver to deliver a 512bit key within 14ms. This can protect the two nonces used to 802.11 WPA2-PSK passwords within 28ms.

Based upon a test bed of 20 nodes, in Line of Sight and Non line of Sight configurations, iJam was shown to provide a practical implementation. This resulted in the eavesdropper BER being close to 50%. Testing between random node pairs resulted in BER as a function of Signal to Noise Ratio for the intended receiver to be similar with and without the presence of the self-jamming signal even when an eavesdropper is experiencing a BER of circa 50%. This technique shows promise and could provide the basis for link layer protection.

(Katabi, 2010) presents a means to obscure the physical layer of a wireless transmission from eavesdropping within an OFDM system. This merits further investigation as it could provide a valid approach to prevent intercept of signals facilitating the analysis of low entropy packets and reverse engineering for signals intelligence purposes. This paper only targets the sensitive packets of a handshake process however the scheme could provide a platform to further this technique to cover the full wireless exchange.

3.4.2 Reactive jamming threat

Jamming is technically the injection of noise signal into the wireless channel of an intentional receiver or transmitter. This is generally conducted in order to disrupt or deny the communications channel via the lowering of perceived Signal to Noise Ratio (SNR) at the receiver. Jamming is a widely used military technique in order to deny your enemies access to the Electromagnetic spectrum whilst attempting to maintain your own wireless communications. Previously these techniques required customised hardware and high speed ASIC devices. Published research (Jones, June 2012) presents a reactive jamming implementation that has an 8ns reaction time and provides the ability to jam WiFi and WiMAX protocols. The reactive jammer is built upon a USRP N210 SDR along with GNU Radio framework to provide a low cost and open source starting point.

The core of the design is a custom packet detector and jamming controller that is integrated within the Direct Digital Conversion (DDC) chain. The custom packet detector is comprised of a cross-correlator and an Energy Differentiator. The cross-correlator is used to differentiate protocol and relies on the use of preamble inference based upon low-entropy portions of incoming signals devised from the I and Q portions of the base band signal. This provides a confidence-weighted analysis that can be customised to detect different protocols through user-based configuration from a host controller. The energy differentiator continuously compares the current energy level against the recent past in order to detect a rise or fall of RF energy. The energy differentiator provides a measure of channel occupancy if the cross-correlation coefficients are not available.

This implementation with the FPGA allows the DSP to initiate a jamming response within 1 clock cycle of a detection trigger. With the embedded Xilinx FPGA running at 100MHz this results in an 80ns response time between packet detection and jamming response. This response time allows the jamming of specific pre-amble packets or critical elements of the channel synchronisation process from a commercially available hardware platform. It is, in theory, possible to jam an 802.11g packet prior to OFDM symbol reception by the intended recipient. Lab testing demonstrated successful jamming against standards compliant WiFi and WiMAX networks, achieving a variety of effects from surgical

attacks aimed to reduce bandwidth through to attacks that denied access to the network under attack.

Prior to the availability of commercial SDR platforms, the above performance would have only been available through the use of custom ASIC design, ensuring the implementation would be prohibitively expensive and only technically available to governmental or military organisations. In theory now a dedicated enthusiast could assemble this style of device within a home lab and generate an advanced threat device that would pose significant disruption if deployed in a malicious manner.

It could be argued that jamming is becoming a threat and CNI based upon wireless networks should consider as a part of their baseline cyber risk assessment.

3.4.3 Protocol Aware Jamming

D.Nguyen et al (2014) presents a very credible approach to developing a protocol aware Reactive Jammer. Concepts within this paper could be used to generate a Counter Improvised Explosive Device (C-IED) jammer capability that is protocol re-active and extremely wide frequency bandwidth. In terms of threat technology, this paper demonstrates that further work is required to secure the physical layer of wireless communications to counter jamming and spoofing. Encryption only stops payload discovery and does not in itself prevent tampering with the data transfer process. The correlation and protocol ‘awareness’ could be a serious threat if deployed within a live environment. This would allow a threat actor to set the jamming to interfere with wireless connectivity, either injecting a low bit error rate, completely denying a link or behaviour that could emulate an erroneous link connectivity.

3.4.4 Detection and diagnosis of Jamming

(W.Xu, 2005) explores techniques for diagnosing the presence of an active jamming signal within an acceptable false alarm rate. The premise of the paper is that no signal measurement is capable of reliably classifying the presence of a malicious jamming signal. Therefore, a range of techniques is required in order to ensure consistency checking to remove ambiguity. Jamming signals have several attack vectors that range from Barrage (constant), Protocol (Deceptive), Reactive and Random. Each class of attack will have different signatures based

on the protocol compliance and detection techniques needed to take into account this spread of signatures.

Currently it is nearly impossible to determine whether the presence of an interferer is related to the presence of an intentional jamming or to a non-hostile in-band interferer. In order to build rugged wireless protocols it is necessary to diagnose and manage with the presence of a hostile jamming signal. The solution presented uses a blend of techniques that are able to (under laboratory conditions) diagnose the presence of the four classes of jammer. This technique was built from measuring the Packet Delivery Ratio (PDR) and consistency checking using a heartbeat signal along with packet counting.

The PDR technique is calculated from two points of view. The first is the transmitter, which keeps track of CRC packets. The second for the Receiver, which calculates PDR from the ratio of packets that pass CRC check vs packets received. The premise is that since a jammer would degrade the channel quality surrounding a node, the detection of radio interference relies on determining whether the communication node can send or receive packets. Within this study PDR was shown to perform reliably to differentiate jamming from congestion within the network. However, by itself it doesn't provide a reliable enough metric. Consistency checking was used within the study as a second metric to back up the PDR. This used a heartbeat to provide a stream of packets that could be measured for consistency. Each node exchanged a heartbeat signal with its neighbour. This traffic provides a baseline from which PDR can be measured. In the enhanced detector neighbours co-operatively exchange PDR measurements in order to determine whether the channel is jammed or not. The algorithm is based upon the assumption that if a neighbour has a high PDR value the interference or interruption in communications is not related to jamming.

(W.Xu, 2005) describes an interesting method of differentiating between the presence of a jammer. From the limited testing, this paper shows promising results, along with an assumption that jammers that are not very effective at interfering with the network behaviours that would make the PDR measurement increasingly discriminatory. In theory this would make PDR a powerful measurement tool for detecting interferers. Additional techniques based on Reed-Soloman codes are also outlined that could provide further enhancement

to the presented algorithm and may be worth further investigation for the application of frequency hopping.

3.4.5 Circumventing Jamming Attacks

The impact of jamming on a wireless network can be prevented in different ways. (J T Chiang, 2014) presents a paper that explores a code tree system for helping the physical layer of a wireless network to become resistant to jamming. This is simulated within a Fast Frequency Hopping Code Division Multiple Access (FH-CDMA) waveform. Techniques such as FFH-CDMA prevent link layer access to third parties due to its spread spectrum characteristics and hopping behaviours.

The notion of frequency hopping in radio systems was originally credited to Hedy Lamarr co-originator of the idea of spread spectrum transmission (Antheil George, 1942). She and her pianist were issued a patent for the technique during World War II. They discovered the technique using a player piano to control the frequency hops, and envisioned it as a way to provide secure communications during wartime. This technique was the basis for modern spread spectrum and frequency hopping techniques used in Bluetooth, COFDM, and CDMA.

The premise of the paper is due to the susceptibility of wireless networks to jamming attacks. An upper layer (of the ISO network layer model) feedback can improve the lower layer performance in areas such as transmit control. A spread spectrum physical layer technique provides a reasonable amount of immunity to jamming due to a multitude of frequency bands the transmission is made on. The spreading or hopping pattern can be viewed as a secret key that enables a secure transfer of information. The use of these systems within a live environment can be limited if the spreading or hopping codes are fixed in nature and therefore able to be reverse engineered.

The solution within the paper is to use a combination of FFH-CDMA, which allows the use of multiple hopping patterns (simultaneous transmit of multiple frequencies) that are coded via a binary tree structure, above the physical layer. In this approach each transmitter builds a balanced binary tree of randomly generated hopping patterns. The transmitter associates each legitimate receiver with a unique leaf in this binary tree, and gives this receiver the hopping patterns corresponding to that leaf and all ancestors of that leaf in the tree. During a normal operation without jamming influence, the system operates on a single

hopping pattern; specifically corresponding with the root of the tree. Once jamming has been detected the transmitter should avoid such hopping patterns in the future and instead use a different cover.

This technique was tested within a MATLAB simulation, consisting of a base station, 20 normal users and between 0 and 10 jammers. From this simulation, it was shown that in the presence of jamming (without knowledge of the coding scheme) 100% of the packets were delivered by using only one hopping pattern. Within this simulation a measure of PDR was used to determine the presence of a jammer (see paper 3). This technique also scaled to delivering 90% of packets in the presence of between 6 and 10 jammers, even when knowledge of the code use is gained by the jammers.

(J T Chiang, 2014) look at a promising technique for the protection of the physical layer. With the complexity imposed by the coding technique coupled with the FFH-CDMA, a reliably secure communication exchange could be constructed. This needs to be evaluated in system testing in order to ensure the practicability of the implementation along with management of the coding tree.

3.5 Meaconing Attack

3.5.1 Background

Electronic attacks against radio navigation systems has occurred over many years. During World War 2 with the Meacon long wave jamming station (Hepcke, 1999) used to deceive German Fighters and Bombers approaching the UK coast line. With the rise of Global Navigation Satellite Systems (GNSS) the Masking Beacon or Meaconing attack against in secure and ubiquitous navigation systems could be identified as a significant threat to modern CNI.

A significant amount of national infrastructure and critical systems rely on GNSS as either a timing source or as a source of high precision positional data. The ability for an assailant to spoof GNSS and cause disruption as opposed to Jamming has been assessed previously as having either a low, medium or complex attack vector (Todd E Humpherys, 2008) dependant on whether the assailant makes use of multiple spoofers to simulate a distributed satellite constellation, a simple record and replay attack, or a gradual takeover of a victims signal lock. (Rugamer, 2015) shows there are commercial GPS spoofing systems available that either simply inject a false NMEA stream into a navigation receiver

for a few thousand dollars or commercial GNSS RF-Signal Generators that cost upwards of $100,000 that could be used, although the cost of these systems could be seen as prohibitive to be considered as a wide spread threat vector.

3.5.2 Attack Generation

Significant work in the generation and demonstration of spoofing attacks against live platforms has been conducted by the Researchers within the Radio Navigation Laboratory for the University of Austin, Texas. (Todd E Humpherys, 2008) demonstrates the creation and use of an off the shelf GPS spoofer and its use against Smart Grid, UAV and a Yacht in live scenarios (Daniel P Shepard, 2012). Within these demonstrations it is shown how Meaconing attacks can be conducted in a straightforward manner without the intended victim being aware. The same attacks could be conducted using relatively low cost SDR platforms, further reducing the cost and complexity of successfully conducting Meaconing attacks.

Elementary Internet searches have led to finding several research and open source implementations for GPS spoofers via the use of generic SDR platforms. (Olson, 2015) (RTL-SDR.com, 2015) both sources provide synopsis of research conducted by Lin Huang from Qihoo 360, producing GPS spoofing in order to fly a UAV within restricted airspace. This vulnerability allowed the team to circumvent the GPS 'fencing' that restricts commercial UAV's from operating within restricted airspace. The software enabling the spoofing attacks is available on Git Hub (Ebinuma, 2015) and appears to compile and function. Section 4 will explore this software and whether this provides effectively a low cost, low technical approach to providing a GPS spoofing threat.

Meaconing attacks have been conducted within recent memory against Military targets, the most recently and widely publicised example is the downing of a US RQ-170 by the Iranian Revolutionary Guards. It is believed that this was achieved through the jamming of the UAV control channels and produced a Meaconing attack to force the UAV to conduct a landing within a 'safe' environment (Christian Science Monitor , 2011).

3.5.3 Countering Meaconing

Given that Meaconing is a well-documented vulnerability with GNSS, significant amounts of research have been conducted into countering this vulnerability

through augmenting GNSS receivers with anti-spoof algorithms and behaviours. A range of techniques exist and have been found to provide countermeasures against spoofing. Specifically (Mark L Psiaki, 2011) explores the viability of using the M-Code scrambled signal to cross-correlate the Civillian C/A code. In the study this approach was shown to be promising and provides a reliable way of detecting the presence of a spoofed signal. Even with the positive results it has been indicated that a Meaconing attack with enough RF bandwidth could defeat this anti-spoof mechanism. Further to this (Daniel Marnach, 2013) indicates that the analysis of receiver clock bias could be used to generate an anti-spoof algorithm, exploiting the inaccuracies present in GPS receiver real time clocks, when compared to the atomic clock sources within the GPS constellation. This research has shown good promise and showed repeatable results within lab testing. However further characterisation work is required against scenarios other than a simple record and replay attack. Again, further to clock bias and cross correlation (Ali Broumandan, 2012) explores the ability to use special correlation to detect spoofing attacks. This is based upon the hypothesis that a spoofing attack will originate from a single point of origin, allowing an algorithm to characterise the spatial information from a real GNSS constellation and therefore identify a Meaconing attack. Experimental results have shown that this spatial methodology has again good promise in detecting and protecting against spoofing attacks. Indeed, the published scientific literature has enough different approaches that there seems to be little to add to the subject area. However, through exploration of GPS sub-systems and System on Chip (SoC) suppliers, there seems to be little information of the actual implementation of anti-spoofing measures.

Thiel's (Andreas Thiel, 2009) white paper released by u-blox, who's GPS SoC's appear in a wide variety of applications, from simple developer kits for hobbyists, through to integration into high accuracy GPS solutions for Defence, Automotive and other industries. The white paper and marketing material released by u-blox indicates some internal protection against jamming, but does not indicate any protection against spoofing. Indeed, a further exploration of other suppliers, noticeably Novatel, Trimble and Garmin include no anti-spoof information with regard to their GPS solutions for automotive, naval or aircraft. Novatel have an active antenna technology, based upon beam forming and steering, however this is only for defence product use.

3.5.4 Impact

The use of civilian GPS receivers for military use is becoming common practice, due to the rapid development of civilian computing technology and the reduced Size, Weight and Power consumption. For instance, the Garmin Fortrex 401 has been a commonly used personal GPS receiver for use by Dismounted Soldiers to create 'honesty' traces of their patrols or for reporting position data for routes, areas of interest etc. It is unknown whether any anti-spoof or anti-jam analysis has been conducted, however due to the commercial availability of these devices it is highly unlikely[14], therefore allowing spread of vulnerabilities, increasing the ability of malicious actors to conduct Meaconing attacks.

[14] https://buy.garmin.com/en-GB/GB/outdoor/wrist-worn/foretrex-401/prod30026.html

3.6 Conclusions

The systematic threat survey has indicated the SDR can provide a very flexible platform that can be used for a variety of Cyber-attack scenarios, representing several threat vectors that can be launched from a single hardware platform. Commercially available SDR platforms such as the Hack RF and the USRP can present a threat in the 3 sub-categories of Electronic Attack;

- Intercept
- Jamming
- Packet Injection

Prior to the advent of these commercial SDR platforms the threat vectors as presented within the literature review would have required costly, highly specialised equipment along with deep RF expertise. Instead now, along with democratisation of information via the Internet, complex attacks against TETRA, GSM, GPS are achievable by 'Script Kiddies' and pose a wider risk than previously considered. Table 2 provides a summary of the vulnerably vs the mechanisms against the protocols covered by this literature review.

	Threat Vector		
Compromised Protocol	**Intercept**	**Jamming**	**Spoofing**
TETRA	x	x	
GSM	x	x	
GSM-R	x	x	
Mode S IFF	x		
AIS	x		x
ACARS	x		x
Wi-Fi	x	x	
GPS		x	x

Table 2 Summary of protocol vulnerabilities identified in Literature review

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.

4 METHODOLOGY

4.1 Introduction

Based upon the threats identified within the systematic threat survey, an experimental threat enumeration was used to understand the ease of exploitation for two of the identified vectors. This is based upon commercially available technology and open source software in order to understand the lowest common denominator in terms of threat actor.

4.2 Research objectives

The rapid evolution of radio technology into the Software Defined era, has accelerated the availability of advanced radio receivers that can cover very large portions of the radio spectrum (70MHz to 6GHz) at low cost. Coupled with the democratisation of knowledge that has occurred through the Internet, the threat environment for EW has changed markedly over the last 5 years. Previously EW threat would have arisen from a state actor that could fund the expensive equipment and antenna arrays that would be required for the intercept and disruption of military signals activities. The objective of this research will be to conduct some threat exploration, taking a commercial SDR platform and using it to conduct cyber-attacks against test subjects in controlled conditions.

As the literature survey has indicated, security tends to be focused on the encryption of the payload using techniques such as AES-256. Strong encryption techniques such as Enigma and AES-256 have suffered from vulnerabilities due to mistakes in the development or through the mistakes of users.

The objectives of this experimentation is twofold;

1) Explore practical record and replay attack against a products communication system within controlled circumstances

2) Use openly available software to generate a Meaconing attack against a GPS system.

4.3 Context and Constraints

This research has been conducted without access to MOD agencies and information. The background information and MOD specific elements of information has come from open sources and direct professional experience of working within the Defence Communications industry.

The UK MOD Independent Research and Development arm, Dstl was contacted at the beginning of this research in order to engage over threat information or to collaborate on research aims.

As Dstl did not collaborate within this research, targets were procured where possible from sources such as Ebay.

4.4 Test Bed Setup

The test bed was designed to replicate the capabilities of a typical hacker. This was based upon the use of an off the shelf SDR platform integrated with a computer in order to provide the processing and human machine interface.

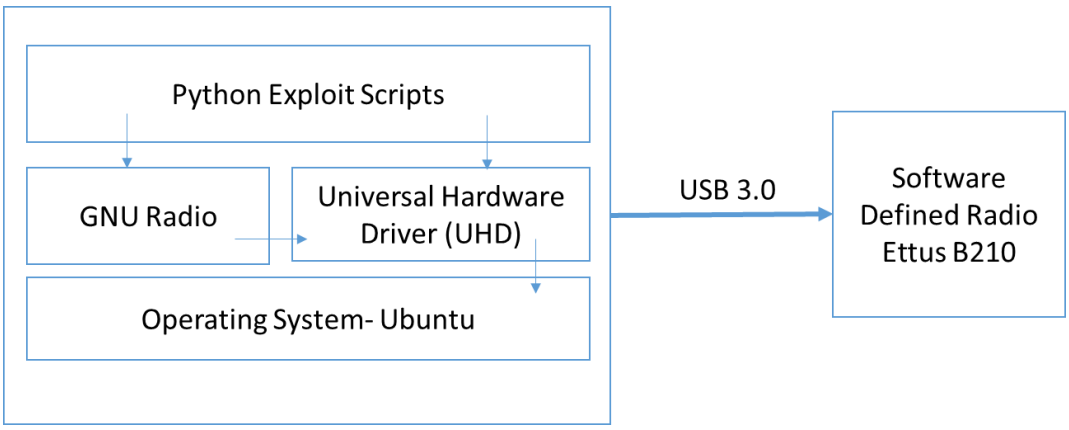


Figure 7 - Test Bed Architecture

Figure 7 illustrates the setup of the testbed. For this study, a Dell Precision T3600 with Ubuntu 14.04 was used as the host computer to provide sufficient RAM and processing resources. Ubuntu provides a software operating system that already has a large amount of open source SDR solutions that can be implemented. The operating system uses the Ettus Research Universal Hardware Driver (UHD) as an abstraction layer for their SDR's. This ensures the entire Ettus Research

product line integrates to software control applications through a common API set.

To implement the radio component design and signals analysis, GNU radio[15] was used. GNU radio is a framework of tools that interface C++ signal processing libraries that are implementations of common signal processing functions (such as FFT, Demodulators etc.) and interface them to a python module that provides a graphical interface in order to implement the executable code. Wireless exploitation scripts are written either through the use of the GNU radio visual flowchart. Gnu Radio also supports the writing of Python scripts which execute high speed Digital Signal Processing functions that are written and executed in C++ to allow rapid execution of complex DSP functions.

In order to ensure compliance to UK legal obligations for the transmission of wireless signals, all experimentation will be conducted through a cabled RF environment. For experiments involving open air transmission, a valid test site license would be required from OFCOM. Due to the targeted systems, the timeline for this license process fell outside of what would have been acceptable for this study. The cabled environment ensures that all transmitter and receiver equipment is connected by coaxial cable and does not broadcast interfering signals that could interfere with licensed operators. In order to ensure the system does not receive damage from saturated receivers, inline attenuators have been used to ensure the signal received in consummate with an open air transmission.

4.4.1 SDR platform Choice

For the research conducted a USRP B210 was purchased to act as a threat source, providing a typically available SDR platform. The B210 platform is based upon the Analogue Devices AD9631, which is an Integrated Radio Frequency Integrated Circuit (RFIC). This device provides continuous coverage of between 70MHz through to 6GHz, whilst allowing an instantaneous bandwidth of 56MHz sitting behind the RFIC is a Xilinx Spartan 6 Field Programmable Gate Array (FPGA) that provides a host processing capability that conducts the Digital Signal Processing (DSP) tasks of the SDR.

[15] Gnuradio.org

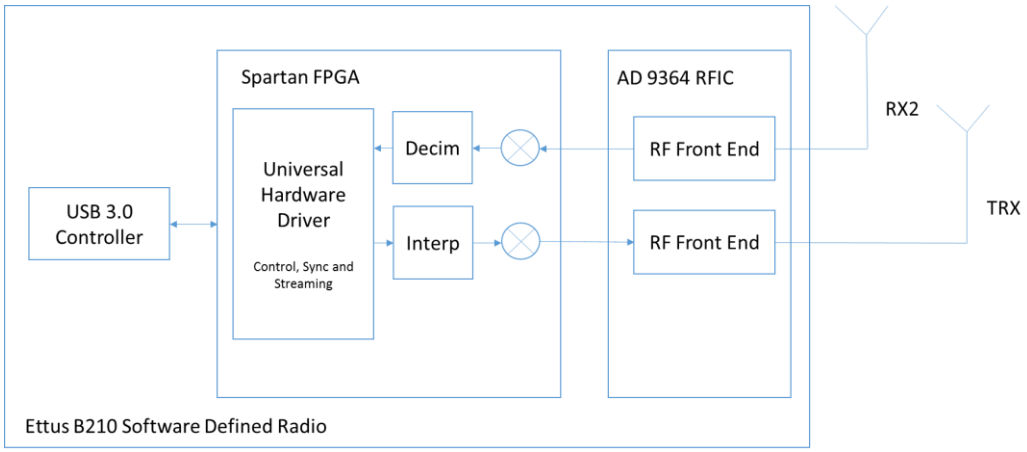


Figure 8 - Ettus Research B210

The B210 is provided with a USB 3 interface for connection to a host computer. This interface provides the digital IQ connection to a host processor for de-modulation and processing the baseband signals. The USB3 connection ensures the full 61 MS/s sample rate is available to application code executing on the host processor.

4.5 Attack Impact Assessment

The experimental strategy selected was to carry out a threat evaluation based upon an impact assessment of two specific attacks. The aim was to replicate several threat vectors within a laboratory environment and to measure their efficiency of affecting the target system and their credibility.

Based upon the literature review and availability of victim equipment, the following threat vectors were chosen to be explored,

4.5.1 Record and Replay Attack

Within this scenario a threat actor uses a SDR capability to cause confusion or disruption to a communications system via recording the local Electromagnetic environment and replaying it. This allows the threat actor to re-transmit the original signals with the aim of either causing confusion through spurious behaviour within the target system or denying access to the Radio Spectrum it requires.

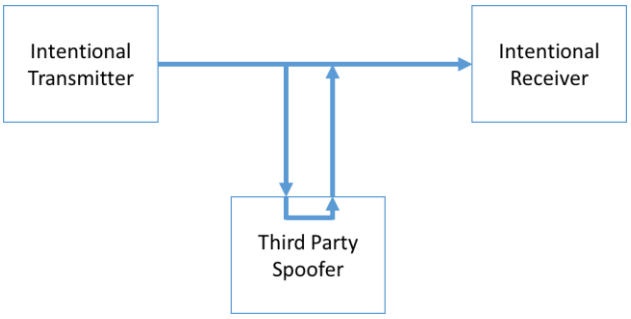


Figure 9 - record and replay attack

This attack takes advantage of the lack of signal validation within wireless networks in order to replay the original received signal in order to implement a spoofing signal. If implemented within a crude manner this would present confusion to an operator of a system as they would experience repeating transmissions and potentially a blocked radio channel if they are operating a simplex transceiver that can only transmit with an unoccupied radio channel.

This attack takes advantage of the wide bandwidth and processing capabilities of the SDR in order to record the raw baseband signals and to re-transmit them without the requirement to demodulate and to understand the signal of interest. This attack vector will be assessed against the ability for the SDR to inflict a valid signal on the threat system, resulting in spoofed receiver behaviour. The B210 SDR platform will be used as the third party spoofer as illustrated in Figure 9.

This experiment was based upon a theoretical scenario, where an adversary uses a wideband SDR platform to conduct a record and replay attack against a communications system. In theory this scenario could be extended to multiple spoofers to produce a distributed attack, leading to a much wider of area over which the effect can be sustained.

This scenario uses the assumption that the adversary has no direct knowledge of the modulation scheme in question and is looking to create disruption as opposed to confusion arising from spoofed information.

The threat target in this scenario is the Selex Personnel Role Radio (PRR) this radio provides the communications for the UK Dismounted Infantry at below Platoon formation. A Platoon is a military unit typically composed of three sections and containing about 30 soldiers. Platoons are organised into a Company, which typically consists of three Platoons. A Platoon is typically the smallest military unit led by a commissioned officer; the Platoon Commander,

usually a Lieutenant. He is usually assisted by a senior Non-Commissioned Officer; the Platoon Sergeant. In this scenario the PRR is used as the military unit requires voice communication over a relatively short range (less than a Kilometre).

The PRR is used by the British Army, Royal Marines, Royal Navy and the Royal Air Force Regiment. The radio has a designed range of 500 meters, weighs 1.5 kilogram and has 256 different radio channels.

The PRR was originally part of the wider Bowman radio project but the procurement was accelerated and the first of 45,000 units formally entered service in early 2002. Operating in the 2.4 GHz band, PRR has no integrated encryption devices and does not intercommunicate with the rest of the Bowman network, but is widely acclaimed as having revolutionised intra-squad communications and small-unit tactics.

The radio operates on spread spectrum and has been designed to have a good level of security, being designed with LPI.

Figure 10 - Bowman PRR

4.5.2 Network Spoofing (Meaconing Attack)

The second scenario is of a Meaconing Attack, where the SDR is used to spoof a navigation signal for nefarious means. The navigation system used within this study is the Global Positioning System (GPS). Given the reliance on GPS, the ability to produce a GPS spoofer from open source software and hardware would have worrying implications.

The second experiment conducted was a Meaconing attack against a commercial GPS receiver. This attack took advantage of Open Source software found during the literature review phase of this thesis (Literature review section 3.5). The GPS-SDR-SIM project, published to Github (Ebinuma, 2015) GPS-

SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms.

The aim of the experiment was to understand whether the open source software would allow a valid GPS Spoofer to be built and execute attacks against commercial GPS receivers.

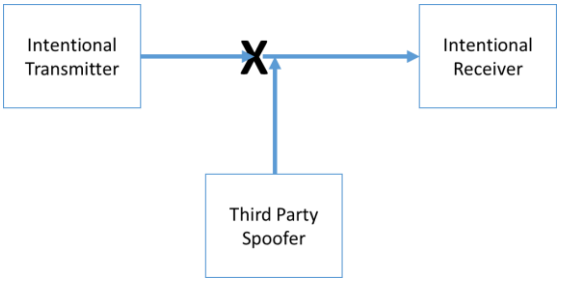


Figure 11 - GPS Spoofing Diagram

This attack functions by over powering the relatively weak GPS signal with a replacement signal. The replacement signal is constructed from true GPS constellation data and therefore should be detected as a valid GPS signal by the receiver. This attack is based upon software that has been published to Github under MIT license. The hypothesis being, is there software available freely that could provide a serious vulnerability to GPS using SDR?

GPS-SDR-SIM uses a user's defined waypoint information or static location to construct a dynamic model of position. This model is then parsed along with the daily GPS broadcast ephemeris file. This data is then parse by GPS-SDR-SIM to generate the simulated pseudo range and Doppler drift for the GPS satellites in view. This simulated range data is then used to generate the digitised I/Q samples which are fed to the SDR platform.

This attack will be assessed against the ability of the spoofer to enable the GPS receiver to resolve a position or valid time. This will also be assessed against the ability of the GPS receiver to report valid GPS satellites within view and their respective Signal to Noise Ratios.

4.6 Conclusion

The methodology chosen is able to take advantage of commercially available hardware and open source software to potentially attack a radio that is in daily use by the UK MOD and other defence organisations, which should be incredibly

concerning. The freely available radio from ebay would allow a prospective attacker to research the device in advance of any targeted attack, increasing the probability of its success.

The SDR platform used as a basis of the test bed is flexible, allowing it to be re-rolled from one format of attack to another. This allows the testbed to use a single SDR platform to target multiple wireless systems for vulnerability testing.

The availability of GPS spoofing software as freely available software is an interesting development; in practice this could be used to execute distributed GPS denial or spoofing over large areas when combined with relatively cheap SDR platforms. When matched with the ability for a relatively novice person to construct this platform, demonstrates that an Electronic Warfare threat is no longer solely the act of a nation state or sponsored actor.

5 RESULTS AND ANALYSIS

5.1 Introduction

The testbed was constructed and used against the attacks as defined within section 4. This section covers in detail the attacks conducted and the respective results.

5.2 Record and Reply Attack

5.2.1 Test Setup.

In order to generate the record and replay attack, a cabled RF architecture was used in order ensure no transmitted RF would interfere with other systems. Given the transmit frequency of 2.4GHz, it was a possibility that the PRR and the RF attack would interfere with local WiFi services. Figure 12 illustrates the architecture of the setup. Each PRR was attached to a leg of a 3-way RF splitter, with the B210 SDR attached to a 20dBi Attenuator and then the splitter. This was conducted to ensure the radio front end of the SDR or the PRR's would not receive damaging levels of RF energy whilst under test.

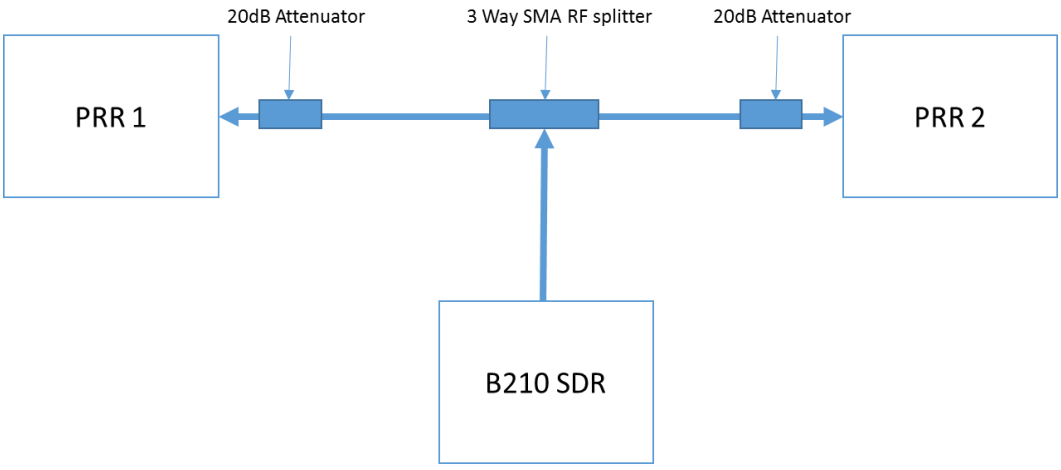


Figure 12 - Record and Replay test architecture

5.2.2 Results

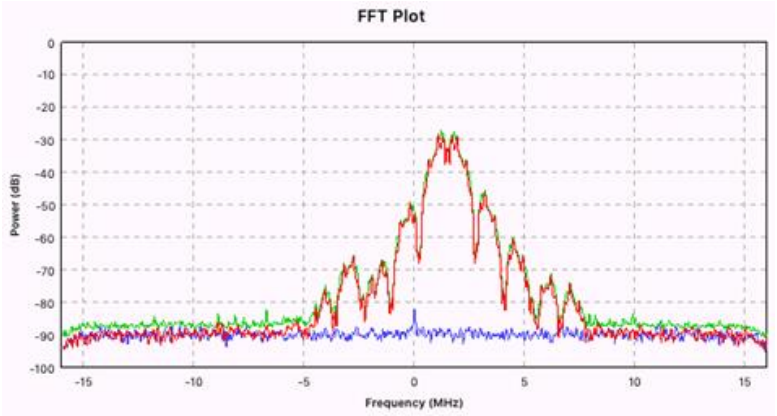
The first stage was to use the test bed to identify the transmit frequency of the PRR, identifying the basic characteristics of the waveform and to identify the range of transmit frequencies that are in use. The product data sheet (Selex ES

, 2013) for the PRR identifies the fundamental allocation as being at 2.4 GHz, from this information it was relatively easy to identify and measure the waveform as shown in Figure 13. For this exercise a relatively high sampling rate of 30MHz was used in order to capture the waveform with enhanced resolution, enabling the waveform to be clearly identified. From these measurements, Table 3 was constructed, which documents the measured channel allocation frequencies. From this measurement the channel spacing for the PRR is evidently 5MHz. In accordance with Nyquist Sampling theory: the sample rate for any record and replay should be twice or larger than the bandwidth of the signal in order to reduce the incidence of aliasing and distortion of the original signal. In the case of the PRR the minimum sampling rate should be in the magnitude of 10MHz.

Table 3 - PRR channel to frequency allocation

Identified Channel Number	Measured Frequency
Channel 1	2.40159 GHz
Channel 2	2.40659 GHz
Channel 3	2.41159 GHz
Channel 4	2.41659 GHz
Channel 5	2.42159 GHz
Channel 6	2.42659 GHz
Channel 7	2.43159 GHz
Channel 8	2.43659 GHz
Channel 9	2.44159 GHz
Channel 10	2.44659 GHz
Channel 11	2.45159 GHz
Channel 12	2.45659 GHz
Channel 13	2.46159 GHz
Channel 14	2.46659 GHz
Channel 15	2.47159 GHz
Channel 16	2.47659 GHz

The PRR implements a digital modulation and voice encoding scheme. According to the manufacturers data sheet this is based upon the Direct Sequence Spread Spectrum (DSSS) technique, this is confirmed by the ‘bell’ shape that the signal possesses. As a result, it should be possible to decode this signal using a custom built DSSS recovery and demodulation scheme within GNU Radio, however this experiment is centred around a simple record and replay attack against this waveform.



Key

--- PRR Captured Signal

--- Baseband Noise

Figure 13 - PRR Waveform captured by simple FFT

Once the fundamental waveform had been found, a simple record and replay attack could be constructed with the test bed. In order to conduct this attack, the raw RF channel will be recorded to the computer hard disk and used to buffer the raw IQ samples for replay. Due to the raw nature of this, along with the relatively high sample rate of 10Mhz, the replay files will be of considerable size (files used as part of this experiment were in excess of 700Mb for circa 30 seconds recording). During our experiment, file sizes of between 700 and 1.2GHz were common for recordings of less than 30 seconds, indicating the high resolution of the IQ data that was being captured. Figure 14 illustrates the simple flow chart used for the capture of the RF signal, as can be seen GNU radio only requires two fundamental code blocks to implement this attack, namely the USRP source (SDR API interface) and the File Sink for recording to hard disk. The FFT sink was added to verify the quality and presence of the signal received, but formed no part of the recording process.

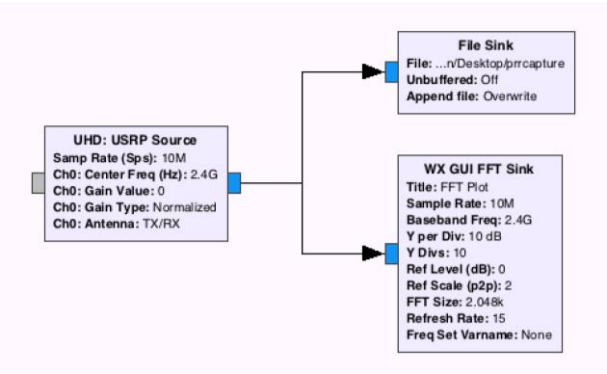


Figure 14 - GNU radio Flow chart for RF capture

The replay attack is conducted by feeding the raw IQ recording to the SDR for re-transmission. Due to the 50MHz bandwidth of the test bed, recreating the 5MHz bandwidth signal is straight forward. The DSSS signal implemented within the PRR contains no verification mechanism, therefore once the test bed starts to transmit the signal, it should be received and de-coded by the PRR. Figure 15 illustrates the flow chart used for replay of the signal. As can be seen only two code blocks form the fundamental attack configuration, the File Source block which feeds the raw IQ data to the UHD sink block which transmits the raw IQ data to the SDR for conversion in RF for transmission.

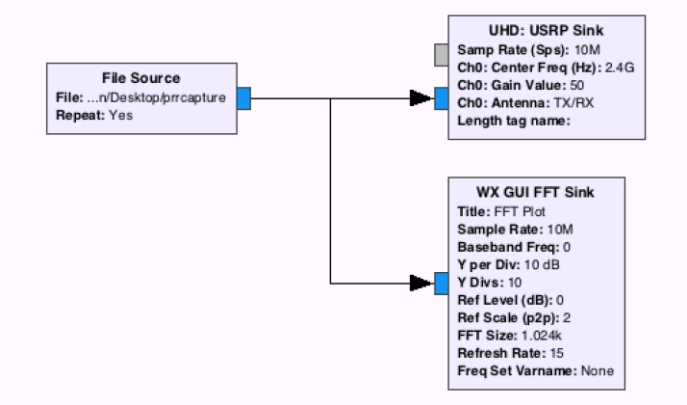


Figure 15 - GNU radio flow chart for RF replay

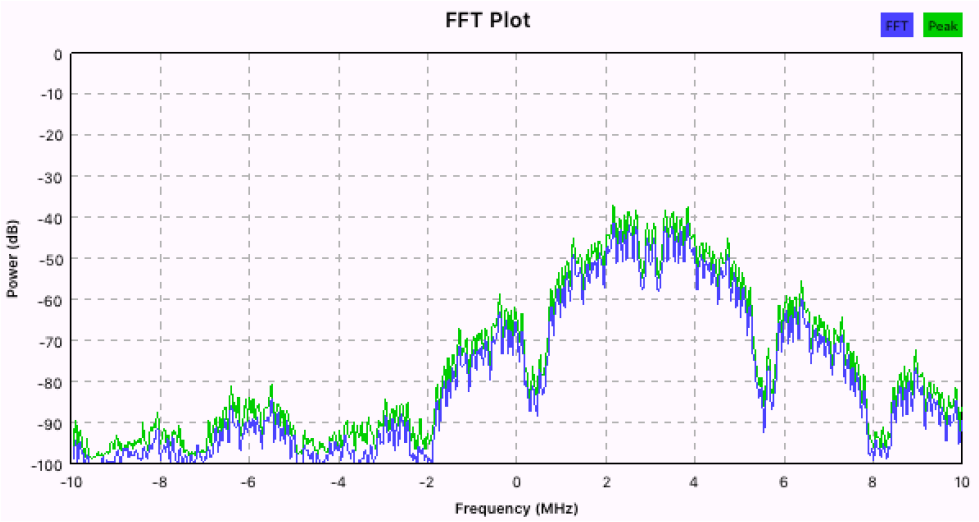
The execution of this resulted in the recorded signal being replayed and both PRR's emitting the audio recorded from the intercept, indicating this experiment has been a success. This demonstrated the signal was still recognised as valid and audible. Clearly no authentication of the signal or source device is used, allowing any third party to transmit a valid signal to these radios.

The original and replayed signal had been verified by checking the waveforms,

Key

captured by the SDR and shown in --- PRR Captured Signal

Figure 16: as can be seen; some distortion of the waveform has been introduced as part of the record and replay process, however it is still recognisable and still provides a valid attack waveform for this scenario.



Key

--- PRR Captured Signal

Figure 16 – Waveform during replay

Whilst the intercepted signal is being replayed, the PRR does not allow transmit to occur due to the RF channel being occupied, effectively this places the radio into a situation where a Denial of Service (DOS) attack is occurring. If this occurred within a military scenario, this simplistic attack would be countered via the use of an alternative radio channel selection. With further development, it would be possible to construct a relatively efficient energy detector algorithm to identify the occupied channel, record a pre-determined amount of that active channel and then to constantly replay that sample. In theory this would deny the use of all 16 potential channels as the SDR would be conducting a dynamic DOS against any valid transmission.

5.2.3 Discussion

This experiment has demonstrated that a rudimentary attack is possible for a very low skill level. There is no knowledge required of the fundamental underlying radio technology in order to disrupt and to confuse the transmissions, instead just the ability to identify a valid signal within a portion of the radio spectrum. Although this attack was conducted against a pair of radios used for voice communication, the literature also indicates that this is possible against GNSS systems.

This has been published (Jian Chen, 2013) where GNSS was spoofed via the recording and replay of a GPS signal. This paper showed it was possible to

generate a valid GPS signal, causing the receiver to display false position and timing data.

Clearly the ease in which these attacks is generated, along with the relatively low cost of equipment may lead this to be a credible threat against military and civilian infrastructure alike. This vector allows the attacker to generate legitimate signals, of which there is no validation conducted by the receiver. In systems such as HAVEQUICK II, a valid link is only ever established when pre-conditions for all users are met. In the case of HAVEQUICK, this is in the format of a pre-shared frequency list, which determines the order and speed in which frequencies are shifted during the transmission cycle. In theory this would stop a record and replay attack because the radio signal being replayed would have to line up with the skip pattern of the original signal to be decoded. Alternative mechanisms such as (Katabi, 2010) would enhance this as the additional noise being generated in band would obscure the original transmission.

5.3 Meaconing Attack

5.3.1 Test Setup

The second experiment conducted was a Meaconing attack against a commercial GPS receiver.

GPS-SDR-SIM was built using the instructions as supplied within the Readme file. The GPS-SDR-SIM application code was compiled using GCC on a Linux environment and built using the SDR interface code required to interface to the Ettus Research B210, in use on the test bed. The executable code used is provided in Annex C.

GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio. To produce the GPS spoofing signal, the user specifies the GPS satellite constellation through a GPS broadcast ephemeris file. The daily GPS broadcast ephemeris[16] file is a merge of the individual GPS site navigation files into one and published by NASA for precision

[16] GPS broadcast ephemerides are forecasted, predicted or extrapolated satellite orbits data which are transmitted from the satellite to the receiver in the navigation message. Because of the nature of the extrapolation, broadcast ephemerides do not have enough high qualities for precise applications. The predicted orbits are curve fitted to a set of relatively simple disturbed Keplerian elements and transmitted to the users GPS broadcast ephemeris

navigation. These files can be downloaded directly from Nasa[17]. The ephemeris and GPS co-ordinates files are then used to generate the simulated pseudo range and doppler for the GPS satellites in view. This simulated range data is then used to generate the digitised I/Q samples for the GPS signal for parsing to the SDR platform.

In order to legally test the utility of this code the following experiment was conducted within the confines of a RF shielded environment. This ensured the GPS spoofing signal would be contained and not propagated to interfere with in-service GPS receivers. Figure 17 shows the architecture of the test setup.

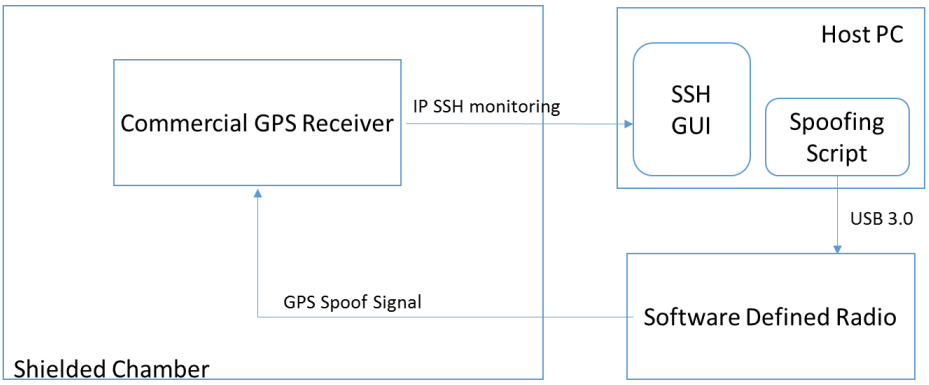


Figure 17 – Test architecture

A GPS test receiver subject was produced via integrating an off the shelf GPS daughter card that is equipped with a commercial UBlox receiver. This was interfaced to the Raspberry Pi's serial interface, in order to provide the NMEA GPS stream to the GPS decoding software running on the Raspberry PI. The open source CGPS framework and API was used in order to parse and format the GPS streams into a User format that could be used to monitor the GPS spoofing signal.

[17] ftp://cddis.gsfc.nasa.gov/gnss/data/daily/

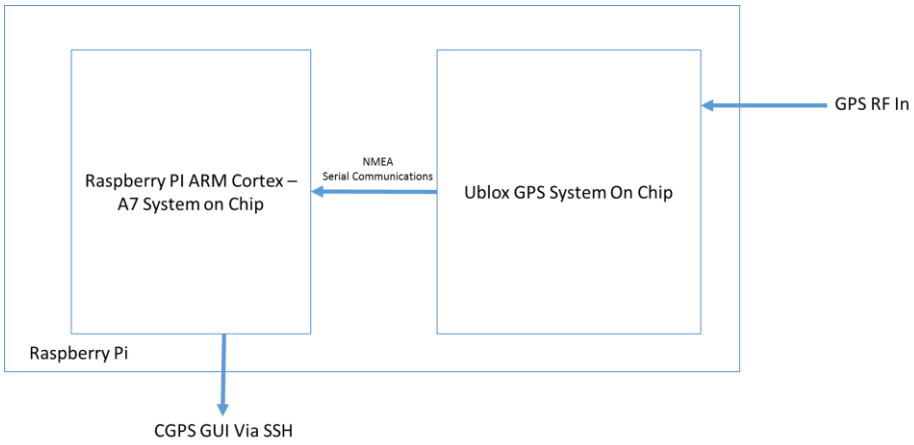


Figure 18 - GPS receiver architecture

The test setup placed the victim GPS receiver in the screened chamber along with an Omni-directional antenna, which was connected to the SDR platform for injecting the spoofing signal. This simulated the free space propagation loss and mixing that would occur between the spoofing source and victim receiver. During the experimentation it was important not to overload the input of the victim GPS receiver as GPS signals typically have a received signal strength of circa -130dBM it was important not to present the victim receiver with a spoof signal that would saturate the GPS receiver. To further ensure this was the case 20dB of attenuation was provided in the SDR transmit line.

During the experiment, the GPS reception was verified with a standard high gain GPS antenna which fed the signal to the Raspberry Pi, which used the CGPS client software to display position, time and individual satellite signal to noise ratio. For this experiment the signal to noise ratio along with the resolved position and time were monitored in order to identify the presence of the GPS spoofing signal. The spoofing signal was constructed using the ephemeris file and GPS motion file supplied with the software.

5.3.2 Results

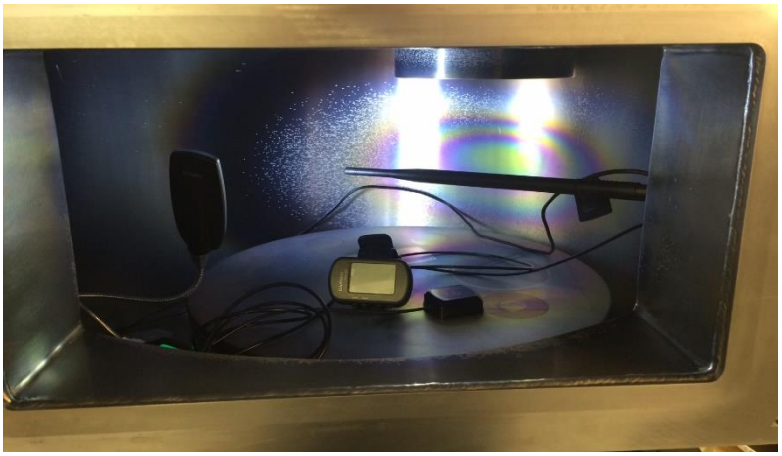


Figure 19 -RF shielded chamber with victim and spoofing antennas

The USRP B210 SDR is capable of delivering a variable power output of between 0 and 20 dBm. This translates to a maximum available power delivery of circa 100mW. Initially the experiment was commenced with 20dBi of attenuation in line between the SDR and the Antenna. This ensured a signal level of circa 1mW was delivered to the GPS receiver. During the experimentation the transmit level was increased in increments of 5dBm, through the increase of transmit power whilst observing for an improvement in signal reception.

These initial attempts did not result in any indicated signal reception at the GPS receiver. Due to the use of an antenna within the shielded chamber as opposed to direct injection via cable, it was decided to remove all attenuation and apply the full 150mW to the GPS receiver. At this point, the GPS receiver indicated a valid GPS constellation with the parameters as shown in Table 4. Unfortunately, at no point during the experiment did the receiver indicate a valid GPS lock for time or position, even though a valid constellation and satellite ID's were being reported. It was not possible to identify whether this was due to saturation of the receiver or the construct of the GPS waveform. This error condition was validated with differing ephemeris files, sourced direct from the NASA website. With the differing ephemeris files, no difference in behaviour was observed with the victim GPS receiver.

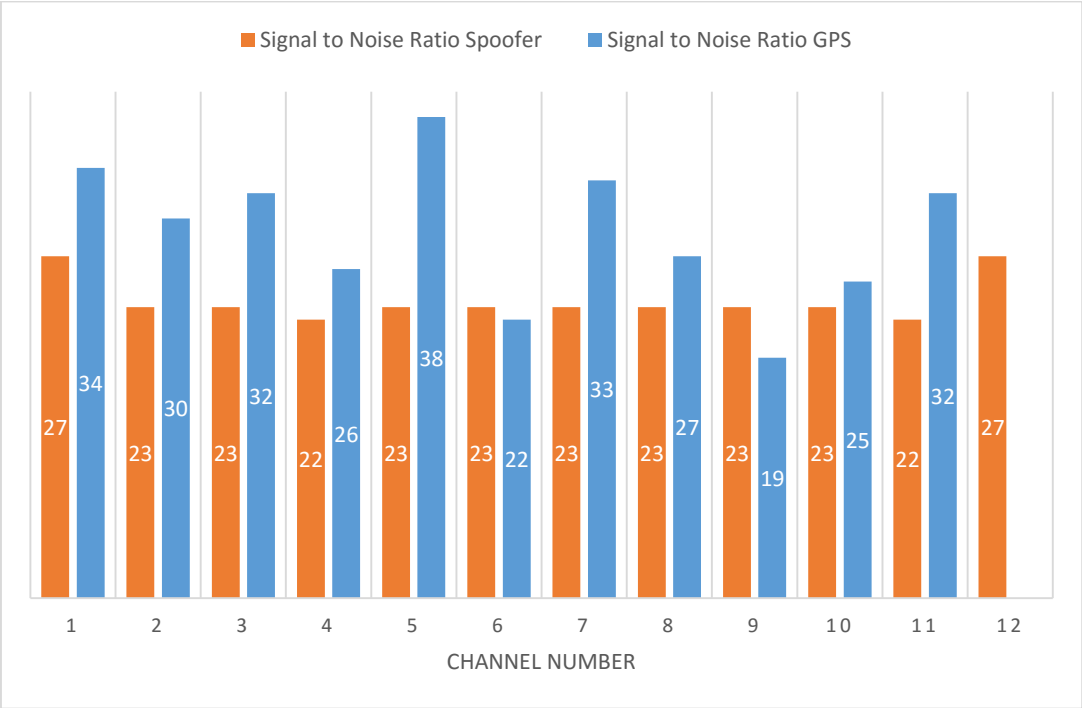


Figure 20 Comparison of Live GPS and Spoofer SNR values

Figure 20 is the resultant comparison of received Signal to Noise ratio from the spoofing experiment along with results from data capture from the live GPS constellation. This was produced in order to identify what a normal SNR profile would be for a GPS constellation. From live capture, it can be seen that the spoofing profile is not producing enough SNR for the satellites in order for the receiver to generate a valid lock. The spoofer only seemingly managed a peak SNR of 27dB across all attempts, however for a live capture the SNR values were consistently above 30 and peaking at 50 on occasion.

Table 4 CGPS output from Spoofing attack for GPS telemetry

Channel	PRN	Azimuth	Elevation	Signal to Noise Ratio Spoofer
0	2	301	39	27
1	3	101	17	23
2	5	284	6	23
3	6	242	66	22
4	7	160	25	23
5	9	159	84	23
6	16	69	2	23
7	17	211	2	23
8	23	64	49	23
9	26	43	6	23
10	30	180	1	22

Channel	PRN	Azimuth	Elevation	Signal to Noise Ratio Spoofer
11	33	196	30	27

In order to understand if there was a failure in the cabling or antennas, further experimentation was conducted via directly connecting the SDR to the GPS receiver.

The GPS RF input was directly connected to the SDR using a Bias T to protect the SDR from +5V DC supply voltage for the GPS active antenna. Along with the Bias T, up to 60 dB's of attenuation was added to simulate attenuation due to free space path loss. With this setup identical results were observed as was seen with the experimental setup within the screened environment, namely valid SNR for the satellites seen but no valid GPS lock witnessed.

In order to verify if the GPS receiver was still functional and was not subject to damage, GPS lock was again obtained from the GPS constellation. Lock was obtained within 60 seconds of establishing connectivity, demonstrating the GPS receiver was still operable and able to show valid position and time. During this test it was noted that the valid GPS constellation showed an average SNR value of circa 53 dB, leaving a question as to why the spoofer was only providing a 23dB SNR value.

Further analysis is required to understand the composition of the GPS spoofing signal and why it was unable to provide a valid signal for the GPS receiver. Seemingly it appears to be a case of signal distortion or saturation. However, validation with a correctly calibrated spectrum analyser would be required to confirm this theory. Unfortunately, due to limitations with this experimental setup that was not available. This goes some way to answering the question that a GPS spoofer could be built and used from open source software, however this must be tempered with the caveat that it does not appear to be as straightforward as with the record and replay attack as described in section 4.5.1.

5.3.3 Discussion

This experiment has not explicitly demonstrated the success or failure of the software in question, due to further analysis of the signal being required. What it does indicate is the viability of the spoofer, due to the ability to generate valid SNR for the simulated GPS satellites. Given the same SDR and test bed configuration was used for both our record and replay attack and Meaconing

attack, it illustrates the diversity of attack vectors that could be generated from a very simple SDR configuration available as a commercial product.

The ability to reverse engineer this constellation and doppler data from publically issued data seems to be of concern. GPS spoofing conducted by (Todd E Humphreys, 2008) and (A.J. Kerns, 2014) against live targets such as yacht and Unmanned Air Vehicles (UAV) indicate that it is technically feasible to engineer these forms of attacks using commercial hardware. Further to this, Qihoo 360 (Olson, 2015) recently published papers where a similar GPS spoofing device was produced and used to fly an UAV in restricted zones. In these zones the UAV is designed to be disabled due to manufacturer designed geo fences, the spoofing enabled its successful operation. The GPS spoofer effectively moved the UAV out of these zones and allowed it to operate.

GPS receivers may be able to protect against these forms of spoofing attack by using multiple sources of GNSS data. Since the launch of GLONASS and when Galileo comes into production, it may be feasible for a GPS receiver to receive GNSS positional data averaged over the 3 constellations (GPS, GLONASS and Galileo) if this is achievable it would allow the receiver to ignore incorrect or significantly divergent data from one of the three sources. Modern smart devices such as the Samsung Galaxy Note 2 are able to receive all of these GNSS sources, effectively enabling this to be implemented relatively simply. A rules based algorithm based upon three-way voting could be used to verify the sources. This methodology is used with high integrity, multilane avionic systems in order to reject data from a malfunctioning processor or algorithm when processing data or logic. As this style of voting mechanism is already cleared for high integrity functions, in theory a high integrity receiver could use this mechanism to claim resistance to a Meaconing attack.

Aside from mitigation with the use of differential sources, again this is an example where some fundamental validation of signal source is required to secure these systems against spoofing attack vectors.

6 CONCLUSIONS AND FUTURE WORK

6.1 Main Findings

This thesis set out with a hypothesis that payload encryption is simply not enough to protect infrastructure delivered via a wireless means. Since the days of World War 2, the encrypted payloads of transmissions have been intercepted and decoded due to insufficiencies within the implementation of the encryption schemes. Early work surrounding the obscuration of wireless signals with techniques such as Frequency Hopping and Spread Spectrum appear to be losing applicability when matched against the abilities of the latest generations of SDR, enabling the demodulation of these signals with ease. The concept of secret key encryption in military communications could be adopted to secure the baseband transmissions (W.Xu, 2005) again present a code tree methodology that could be used to identify sources of interference. Further to this, iJam (Katabi, 2010) appears to offer a scheme of signal masking that may provide a solution to preventing the unauthorised demodulation of a signal. This technique uses frequency agile transmissions to mask the signal against jamming an intercept.

Given the ubiquitous nature of modern digital transmission, and the threat from intercept and spoofing, more protection is required to prevent demodulation or even identification of these signals. Although encryption techniques such as ULTRA and SSL are technically very hard to crack under brute force attack, the common fact is that human imperfections in the implementation of that encryption has led to their vulnerabilities.

This leads to a fundamental conclusion that the physical wireless signal requires a new technique to either mask it or to prevent a third party from being able to de-modulate it. There appears to be no lack of viable protection schemes within the literature. Instead seemingly what is required is a commercial drive to implement a new generation of wireless protocols, enabling secure exchanges of information. With vulnerabilities relating to the introduction to Vehicle to Infrastructure, Vehicle to Vehicle or simply ad-hoc connections, the requirement to secure wireless infrastructure will only increase in importance.

Aside from civilian concerns, a fresh look at communications security for the Defence Domain is required. With the increased adoption of commercial modulation schemes protected via encrypted payloads it is recommended that further work is conducted to understand the feasibility of techniques such as iJam within a real demonstrable system.

6.2 Future Work

The threat enumeration undertaken used a very small portion of the test bed capabilities. Given further time it would be been possible to reverse engineer the PRR waveform, allowing the direct demodulation of the signal along with the ability to inject a reconstructed waveform into the unmodified victim radio. This could be assisted with development of automated analytical tools for GNU Radio, which could through the use of a look up library or through use of machine learning, identify the modulation schemes used by the victim and provide baseline settings to commence reverse engineering from.

Given appropriate funding and permissions it could be recommended that a transportable version of the test bed is constructed which could be hosted within a car or minivan, allowing testing of wireless networks within test environments. This could be used in conjunction with Vehicle to Vehicle and Vehicle to Infrastructure test environments as well as against autonomous vehicles within controlled test environments. Further to the aforementioned enhancements, if clearance could be obtained for transmission in an open environment, experimentation could be conducted against an operating Dismounted Platoon, in order to understand the vulnerabilities of the PRR to these attacks whilst operating in context.

The test bed constructed for the experimentation phase could be used as the basis as a wireless Cyber Vulnerability Investigation (CVI) capability, further research and development would be required to establish a tool framework that would enable use in line with products such as Kali Linux for network penetration testing. However, given wireless networks are not subjected to routing penetration testing when operational, such a CVI capability could be proven to provide great benefit in identifying weaknesses to configuration and deployment.

7 REFERENCES

A.J. Kerns, D. S. J. B. T. H., 2014. Unmanned Aircraft Capture and Control via GPS Spoofing. *Journal of Field Robotics,,* Volume 31, pp. 617-636.

Ali Broumandan, A. J.-J. V. D. J. N. a. G. L., 2012. GNSS Spoofing Detection in Handheld Receievers Based on Signal Spacial Correlation. *IEEE,* pp. 479-487.

Andreas Thiel, M. A., 2009. *Anti-Jamming Techniques in u-blox GPS recievers ,* s.l.: u-blox.

Anon., n.d. *Osmocom TETRA.* [Online]
Available at: http://tetra.osmocom.org/trac/
[Accessed 25 07 2015].

Antheil George, M. H. K., 1942. *Secret communication system.* USA, Patent No. US2292387 A.

Banedanmark, 2008. *Boundaries between ETCS and the GSM-R Network,* s.l.: s.n.

Bartholomew, L., 2002, 2006. Radio Spies - Episodes in the Ether Wards. In: s.l.:Bart Lee.

BBC News, 2009. *Iraq Insurgents 'Hack into Video Feeds from US Drones',* s.l.: BBC News .

Casanovas, F., n.d. *Cracking and sniffing GSM with a RTL-SDR.* [Online]
Available at: https://ferrancasanovas.wordpress.com/cracking-and-sniffing-gsm-with-rtl-sdr-concept/
[Accessed 18 07 2015].

Christian Science Monitor , 2011. *Christian Science Monitor.* [Online]
Available at: http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
[Accessed 22 10 2015].

Codenomicon, 2014. *The Heartbleed Bug.* [Online]
Available at: http://heartbleed.com/
[Accessed 18 July 2015].

Communications, S., n.d. *Personal Role Radio Brochure.* s.l.:s.n.

Danh Nguyen, C. S. B. S. N. K. K. R. D., 2014. A Real Time and Protocol Aware Reative Jamming Framework built on Sofware Defined Radios. *SRIF.*

Daniel Marnach, S. M. M. M. C. H., 2013. Detecting Meaconing Attacks by Analysing the Clock Bias of GNSS Receivers. *Artificial Satellites ,* 48(2).

Daniel P Shepard, J. A. B. T. E. H. A. A. F., 2012. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. *ION GNSS Conference.*

Defcon 18, November 2013. [Online]
Available at: https://www.youtube.com/watch?v=fQSu9cBaojc
[Accessed 25 07 2015].

Defcon 21, 2013. [Online]
Available at: https://www.youtube.com/watch?v=ZuNOD3XWp4A
[Accessed 25 07 2015].

DoD, U., 1991. *Joint Have Quick Planners Guide, Joint Tactics, Techniques and Procedures for Have Quick.* s.l.:s.n.

Dunn, J. E., 2013. *Techworld: GPS Jamming caused by moonlighting drivers.* [Online]
Available at: http://www.techworld.com/news/security/gps-jamming-caused-by-moonlighting-truck-drivers-research-suggests-3425947/
[Accessed 17 February 2016].

Ebinuma, T., 2015. *GPS-SDR-Sim.* [Online]
Available at: https://github.com/osqzss/gps-sdr-sim

Ebinuma, T., 2015. *gps-sdr-sim Git Hub Code.* [Online]
Available at: https://github.com/osqzss/gps-sdr-sim

Flicke, W., Undated. *The Beginnings of Radio Intercept in World War 1 - A Brief history by a German Intelligence Officer.* s.l.:National Security Agency (USA).

Gold, S., April 2011. Cracking GSM. *Network Security,* pp. 12-16.

Hepcke, G., 1999. *The Radar War.* s.l.:s.n.

Hinsley, S. H., 1996. *The Influence of ULTRA in the second World War.* s.l., s.n.

Info Security magazne, Dec 2009. [Online]
Available at: http://www.infosecurity-magazine.com/news/gsm-64-bit-encryption-standard-cracked-and-posted/
[Accessed 25 07 2015].

ISO/IEC, 1989. *7498-4.* First Edition ed. s.l.:s.n.

J T Chiang, Y. H., 2014. *Cross Layer Jamming Detectiona and Mitigation in Wireless Broadcast Networks,* s.l.: s.n.

jammer4uk, 2015. *Jammer 4 UK.* [Online]
Available at: http://www.jammer4uk.com/car-gps-jammer-c-1.html
[Accessed 17 February 2016].

Jian Chen, S. Z. H. W. X. Z., 2013. Practicing a Record and Replay System on USRP. *SRIF 2013.*

Johnson, P., 1985. New Research Lab Leads to Unique Radio Receiver. *E-Systems Team,* Volume 5, pp. 6-7.

Jones, G., June 2012. Mobile Menace: why SDR poses such a threat. *Network Security,* pp. 5-7.

Katabi, S. G. D., 2010. *iJam: Jamming Oneself for Secure Wireless Communication,* s.l.: s.n.

Kruth, L., 1984. The Slidex RT Code. In: *Cryptologia.* s.l.:s.n., pp. 163-172.

Mark L Psiaki, B. W. O. J. A. B. D. P. S. T. E. H., 2011. Civillian GPS Spoofing Detection based on Dual Receiver Correlation of Military Signals. *ION GNSS.*

Martin Beck, 2008. *Practical attacks against,* s.l.: s.n.

National Security Agency, 2010. *National Information Assurance Glossary, CNSS Instruction No 4009,* s.l.: s.n.

Noah Shachtman, D. A., 2012. *Wired.* [Online]
Available at: http://www.wired.com/2012/10/hack-proof-drone/
[Accessed 18 07 2015].

NooElec, 2015. *Amazon.* [Online]
Available at: http://www.amazon.co.uk/NooElec-NESDR-Mini-Compatible-Guaranteed/dp/B00P2UOU72/ref=sr_1_1?ie=UTF8&qid=1437220143&sr=8-1&keywords=nooelec+sdr
[Accessed 18 07 2015].

Ofcom, 2015. *List of TETRA generic user organisation.* [Online]
Available at: http://licensing.ofcom.org.uk/radiocommunication-licences/business-radio/guidance-for-licensees/airwave-emergency-services/airwave/generic_org/
[Accessed 18 07 2015].

Olson, P., 2015. *Hacking A Phone's GPS May Have Just Got Easier.* [Online]
Available at: http://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/
[Accessed 22 10 2015].

Panagiotis Papadimitratos, a. J., 2008. Protection and Fundamental Vulnerability of GNSS. *IWSSC.*

Pultarova, T., 2015. *Engineering and Technology Magazine (IET).* [Online]
Available at: http://eandt.theiet.org/news/2015/apr/network-management-

system-cyber-security.cfm
[Accessed 18 07 2015].

R Bauernfiend, B. E., 2014. Software-Defined Radio based Roadside Jammer Detector: Architecture and Results. *IEEE,* pp. 1293-1300.

RTL-SDR admin, 2013. *RTL-SDR Tutorial: Recieving Airplane Data with ACARS.* [Online]
Available at: http://www.rtl-sdr.com/rtl-sdr-radio-scanner-tutorial-receiving-airplane-data-with-acars/
[Accessed 18 07 2015].

RTL-SDR.com, 2015. *Spoofing GPS Locations with low cost TX SDRs.* [Online]
Available at: http://www.rtl-sdr.com/spoofing-gps-locations-with-low-cost-tx-sdrs/
[Accessed 22 10 2015].

RTL-SDR, 2014. *RTL-SDR Tutorial : Listening to TETRA.* [Online]
Available at: http://www.rtl-sdr.com/rtl-sdr-tutorial-listening-tetra-radio-channels/
[Accessed 18 07 2015].

Rugamer, A., 2015. Jamming and Spoofing of GNSS Signals - An Underestimated Risk??. *Wisdom of the Ages to the challenges of the Modern World. - SOFIA.*

Selex ES , 2013. *Personal Role Radio Data sheet.* [Online]
Available at: http://www.finmeccanica.com/en/-/prr-1

Seongkyun Jeong, S. L. J. K., 2013. Implementation and Test of GNSS Spoofing Detection Module. *2013 13th Internatonal Conference on control, Automation and Systems (ICAAS 2013),* pp. 536 - 538.

Shadow, S., 2013. *Osmocom TETRA Security Exploits Video.* [Online]
Available at: http://ukradioscanning.com/viewtopic.php?f=16&t=250
[Accessed 18 07 2015].

Stubblefield, A., 2001. *Using the Fluhrer, Mantin, and Shamir Attack,* s.l.: s.n.

Todd E Humpherys, B. M. L. M. L. P. B. W. O. a. P. M. K. J., 2008. Assessing the Spoofing threat, Development of a Portable GPS Civillian Spoofer. *21st International Technical Meeting of the Satellite Division of the Institute of Navigation .*

Todd E Humphreys, B. M. L. M. L. P. B. W. O. P. M. K., 2008. Assessing the Spoofing threat, Development of a Portable GPS Civillian Spoofer. *ION GNSS Conference .*

W.Xu, W. Y. T., 2005. *The Feasability of Launching and Detecting Jamming Attacks in Wireless Networks ,* s.l.: s.n.

8 ACRONYMS AND ABBREVIATIONS

ACARS	Aircraft Communications Addressing and Reporting System
AES	Advanced Encryption Standard
AIS	Automatic Identification System
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BATCO	Battle Code
BER	Bit Error Rate
C4ISR	Command Control Communications Computing, Intelligence, Surveillance and Reconnaissance
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
C-IED	Counter Improvised Explosive Device
CNI	Critical National Infrastructure
CRC	Cyclic Redundancy Check
CVSD	Continuously Variable Slope Delta Modulation
DDC	Direct Digital Conversion
DDOS	Distributed Denial of Service
DoD	Department of Defence
DOS	Denial of Service
DSP	Digital Signal Processing
DSSM	Direct Sequence Spread Spectrum Modulation
DSTL	Defence Science and Technology Laboratory
EO	Electro Optic
ERTMS	European Rail Traffic Management System
EW	Electronic Warfare
FFT	Fast Frequency Transform
FPGA	Field Programmable Gate Array
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GSM	Global System Mobile
IA	Information Assurance
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
ISO	International Standards Organisation
JTRS	Joint Tactical Radio System
LPD	Low Probability of Detect
LPI	Low Probability of Intercept
MANET	Mobile Ad Hoc Network
MOD	Ministry of Defence
NEC	Network Enabled Capability
NSA	National Security Agency
OFDM	Orthogonal Frequency Division Multiplexing

OSI	Open Systems Interconnection
PDR	Packet Delivery Ratio
PHY	Physical Interface
PMR	Personal Mobile Radio
PRR	Personal Role Radio
PSK	Pre Shared Key
RF	Radio Frequency
RFIC	Radio Frequency Integrated Circuit
RPAS	Remotely Piloted Air System
SDR	Software Defined Radio
SIGINT	Signals Intelligence
SoC	System on Chip
SoS	System of Systems
TKIP	Temporal Key Integrity Protocol
UAV	Unmanned Air Vehicle
UHD	Universal Hardware Driver
UHF	Ultra High Frequency
UK	United Kingdom
USRP	Universal Software Radio Peripheral
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WEP	Wireless Equivalent Privacy
WiMAX	Worldwide interoperability for Microwave Access
WPA	Wifi Protected Access

ANNEX A ETHICS APPROVAL

Certificate of Ethical Approval

Applicant:

Simon Ballantyne

Project Title:

Master of Science by Research, Cyber Security of MoD Systems of Systems.

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Low Risk

Date of approval:

17 March 2016

Project Reference Number:

P36574

ANNEX B TURNITIN RECEIPT

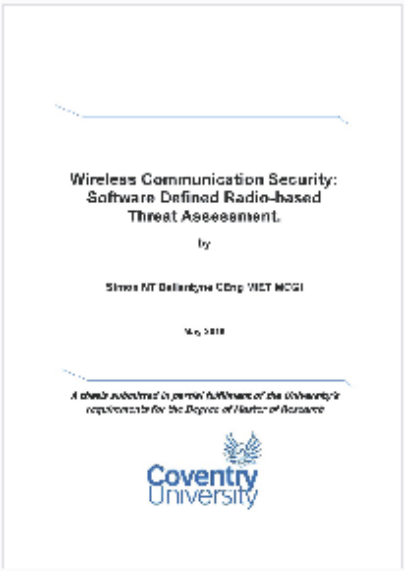
turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Simon Ballantyne
Assignment title:	Final thesis for submission - Part 1..
Submission title:	Wireless Communication Security: ...
File name:	ry.ac.uk_temp_turnitintool_184485...
File size:	2.18M
Page count:	70
Word count:	17,262
Character count:	103,248
Submission date:	20-Apr-2016 10:40AM
Submission ID:	56106448



Wireless Communication Security:
Software Defined Radio-based
Threat Assessment.

by

Coventry University

ANNEX C GPS-SDR-SIM APPLICATION CODE

```
#!/usr/bin/env python
# a small script to transmit simulated GPS samples via UHD
# (C) 2015 by Harald Welte <laforge@gnumonks.org>
# Licensed under the MIT License (see LICENSE)

from gnuradio import blocks
from gnuradio import eng_notation
from gnuradio import gr
from gnuradio import uhd
from gnuradio.eng_option import eng_option
from gnuradio.filter import firdes
from optparse import OptionParser
import time

class top_block(gr.top_block):

    def __init__(self, options):
        gr.top_block.__init__(self, "GPS-SDR-SIM")

        ##################################################
        # Blocks
        ##################################################
        self.uhd_usrp_sink = uhd.usrp_sink(
           ",".join(("", "")),
           uhd.stream_args(
                     cpu_format="fc32",
                     channels=range(1),
           ),
        )
        self.uhd_usrp_sink.set_samp_rate(options.sample_rate)
        self.uhd_usrp_sink.set_center_freq(options.frequency, 0)
        self.uhd_usrp_sink.set_gain(options.gain, 0)

        # a file source for the file generated by the gps-sdr-sim
        self.blocks_file_source = blocks.file_source(gr.sizeof_char*1, options.filename, True)

        # convert from signed bytes to short
        self.blocks_char_to_short = blocks.char_to_short(1)

        # convert from interleaved short to complex values
        self.blocks_interleaved_short_to_complex = blocks.interleaved_short_to_complex(False, False)

        # establish the connections
        self.connect((self.blocks_file_source, 0), (self.blocks_char_to_short, 0))
        self.connect((self.blocks_char_to_short, 0), (self.blocks_interleaved_short_to_complex, 0))
        self.connect((self.blocks_interleaved_short_to_complex, 0), (self.uhd_usrp_sink, 0))

def get_options():
    parser = OptionParser(option_class=eng_option)
    parser.add_option("-x", "--gain", type="eng_float", default=0,
                      help="set transmitter gain [default=0]")
    parser.add_option("-f", "--frequency", type="eng_float", default=1575420000,
                      help="set transmit frequency [default=1575420000]")
    # On USRP2, the sample rate should lead to an even decimator
    # based on the 100 MHz clock.  At 2.5 MHz, we end up with 40
    parser.add_option("-s", "--sample-rate", type="eng_float", default=2500000,
                      help="set sample rate [default=2500000]")
    parser.add_option("-t", "--filename", type="string", default="gpssim.bin",
                      help="set output file name [default=gpssim.bin]")

    (options, args) = parser.parse_args()
    if len(args) != 0:
        parser.print_help()
        raise SystemExit, 1

    return (options)

if __name__ == '__main__':
    (options) = get_options()
    tb = top_block(options)
    tb.start()
    raw_input('Press Enter to quit: ')
    tb.stop()
    tb.wait()
```