Wireless Communications Cyber Security

Dr David Lund
Head of Research and Development, HW Communications, Lancaster, UK
Board Member, Public Safety Communication Europe (PSCE) Forum, Brussels, Belgium

In our marketplace we have many new wireless communication options to choose from. They are built into modern 'attractive' devices, that the authors choose as they become new and popular, with the capability to communicate more than ever before. This study presents some of the basics of how wireless communication technology works and how it is used. The eagerness to embrace modern wireless technology has yielded us vulnerable. How do we understand that? What can we do to protect ourselves, and what is coming in the next generation of wireless technology which will be used to support some of the more critical and sensitive aspects of the daily work and life?

Introduction

In our increasingly connected world, we rely upon many different flavours of wireless technology. Wireless communication has numerous advantages. As consumers and workers, wireless technologies allow us the freedom to move around and yet remain online. Wireless connections allow us to distribute devices around our person, allowing for different types of inter- action with our information; a laptop, a tablet, a watch, a personal health monitoring device, even our vehicles. Wireless technology allows our everyday transactions; such as wireless ticketing, credit card transactions, ePassports, etc., to be convenient and speedy. Wireless technology provides commercial benefits in terms of reducing infrastructure and installation costs; minimising cable installation in buildings and using wireless LANs or long haul point to point microwave links, etc.

A famous quotation from Albert Einstein is often used to illustrate the benefit of wireless:

'The wireless telegraph is not difficult to understand. The ordinary telegraph is like a very long cat. You pull the tail in New York, and it meows in Los Angeles. The wireless is exactly the same, only without the cat.' In simple translation, the telegraph wire is not needed for 'wireless'.

Such benefits of wireless technology, albeit with the limited involvement of cats, have led to the increased transmission of valuable information over the air. Valuable information assets become attractive to attackers, and vulnerable when carried over poorly implemented or configured wireless systems. Coupled with the availability of low-cost devices for interception, there is a distinct need for our community to understand how to protect over-the-air trans- missions. How we use our wireless devices is also considered to be valuable in some contexts.

All wireless technologies rely upon a common physical resource – radio frequency (RF) Spectrum. In all cases, a wireless device has a physical interface with the air, or free space, to transmit and receive information using a specific frequency band.

RF spectrum is accessible by everyone. Regulations are in place both nationally (Ofcom in the UK) and globally (ITU) to allow for regulated and controlled use of spec- trum as a shared physical resource.

Analogue wireless technologies (frequency modulation, amplitude modulation, etc.), have been used for radio and TV broadcast, and push-to-talk voice calls for many years. Only a small amount of low-cost equipment is required to intercept and listen to content carried within RF signals. Hobbyists have been using analogue radio scanners for many years, to listen to police, fire and ambulance operators discuss operations as they walk by, or as their vehicles pass. Most of these listeners are simply curious and have no malicious intent whatsoever. However, users such as emergency service first responders will discuss and relay information which is much more sensitive than our everyday personal phone calls and social media interactions. This information may be attractive, for example, to those wishing to subvert emergency service operations in order to facilitate malicious and criminal activity.

Our personal information may be attractive to others wanting to know our business interests, personal life patterns, our purchasing interests or our general status of health.

This paper provides an introduction of the basic properties of wireless communication and how different systems protect both the resilience and confidentiality of information carried over the air.

The primary case study given in this paper covers the advent of the public safety community demanding mobile broadband capabilities to aid their operations. This reflects some challenges that are faced as we start to integrate wireless communication into more of our critical and sensitive infrastructures and operations.

At the end of this document, seven smaller case studies give examples of how wireless systems have been compromised in recent years.

Spectrum as a common resource

With RF spectrum as a common resource for wireless communication, access to transmissions can be easy. They can be easily received and, in some cases, modified. Therefore, a number of considerations are made to secure and protect our wireless transmission. This can be considered in three primary vectors with relation to classical consideration of confidentiality, integrity and availability:

Information throughput 'availability' – wireless communication resilience: Wireless network operators are keen to ensure that their networks remain 'Available'. Physical properties of RF transmission make it easy to go 'out of range', or many users sharing RF resource may have to wait until the spectrum is either clear for use, or our time-slot is available for use. The presence of interference needs to be mitigated to allow for reliable transmission and available information throughput capacity. Many, such as commercial cellular networks, rely upon availability of service to generate revenues from calling, texting and data services, or simply to maintain their reputation and customers.

Information 'confidentiality': Information carried over the air should be significantly difficult or impossible to decode, should it be intercepted. Cryptography and secure protocols play a key role here.

Information 'integrity': We should remain confident that the communication we receive is integral and has not been modified during transit over the air, or any associated wired network connection or equipment.

Properties of wireless communication systems

Whilst RF Spectrum is accessible by anyone, its access is somewhat limited by the physical properties of the transmitters, receivers, the protocols that they use and the environment. Parameters include:

Transmission frequency: Where in the RF spectrum is the system operating? Different frequencies have different physical properties. Lower frequencies typically propagate over longer distance than higher frequencies. Some frequencies are more susceptible to the physical environment than others. For example, 60 GHz communication systems (e.g. WiGig [1]) may be blocked by oxygen molecules in our air. Visible light communication [2] is simply blocked by physical objects, such as walls. All RF signals may be reflected and distorted when transceivers are moving with respect to each other and other objects in the sur- rounding environment, therefore making reception more challenging.

Transmitted power: Higher transmitted power yields longer transmission range. In simple terms range is typically controlled by the inverse square law, where transmitted power exponentially diverges as it propagates. Higher transmission powers typically demand more expensive transmission components (antennas, amplifiers, etc.) increasing cost, weight, size and battery life. Increased transmission range yields an increase in the possible range within which signals can be intercepted by an interested party.

Receiver sensitivity: Communication receiver technology is both susceptible to receiving interference, but also has a physical bound on how little power is needed for successful reception of a wireless transmission. Advanced silicon techniques and amplification may be used in receivers to improve receiver sensitivity. Increased sensitivity further increases the range between transmitter and receiver for both intended and unintended reception.

Coding, modulation and link protocols: Modulation determines the 'shape' of the energy transmitted. Different modulation methods provide different trade- offs between propagation properties, reception reliability and data throughput. Error control coding is a mathematical technique to provide extra redundancy to a communication, to allow for detection and correction of errors at the receiver. Link protocols attempt to keep both transmitter and receiver talking with the same modulation and coding, and to handle any lost packets, requesting retransmissions where necessary. Higher layers of protocols, such as in 2/3/4/5G maintain registration of the user and mobility of a wireless device. These protocols allow for carefully controlled access to allocated spectrum and handoffs between different base stations and different radio access tech- nologies as a mobile device physically moves. Protocols also ensure that the mobile device and user are authenticated and that wireless access is authorised. Usage is monitored and billed by commercial cellular operators as the user uses the service.

Vulnerable information

As already described, we exchange significant volumes of valuable information over wireless technologies and networks. The following gives a brief flavour of what we exchange and the potential consequences of our compromised information:

Commercially sensitive information

The mobile workplace, coupled with the 'cloud' continually increases the exchange of commercially sensitive information. Shared cloud and radio infrastructure makes a significant economic saving for large and small organisations alike, increasing this desire to transact wirelessly, online. Commercial information transferred includes financial data, intellectual property, location and mobility of staff, etc. Compromise of commercial information may disadvantage a commercial operation. For example, competitors may yield an advantage by knowing the details of competing products in development, staff, or of the financial capacity or internal movements and politics of a competing company. Personal data – ours and others: Information describing our everyday lives is carried over the airwaves. We commonly transact our personal information using online shopping services, banking and social networks. Wearable devices measure our heart rate and activity, and are wirelessly connected to our smartphones. We become our own data controller [3], controlling disclosure of our own information and that of our friends and colleagues. Some organisations may gain benefit from knowing our interests, our patterns of life or our physical circumstances. Marketing activities often try to understand our patterns of life, in order to target advertisements to our interests and therefore increase their probability of a product sale.

Monitoring and control information – consumer

The Internet-of–Things (IoT) is upon us [4]. Technologies today allow us to monitor our central heating and tele- vision recordings. Even cookers and washing machines are available which can be monitored and controlled from our mobile phones. Easy attacks yield an element of comedy by allowing the possibility of flushing next door's toilet via your mobile phone [4]. We find that the specific information and control related to interacting with our own appliances may not be so interesting to those listening. However, we may feel uncomfortable about our privacy being compromised. Such monitoring and control can demonstrate our patterns of life; which TV programmes we watch, when we are away or at home, what time do we turn our lights off at night and how often we use the toilet.

Monitoring and control information – critical infrastructure

On a more serious note, our critical infrastructures require continual monitoring and control. This class of information has very different levels of importance. Electricity and gas distribution networks, railways and highways, all require careful management to ensure that our services remain available. Disruption to any of these services can have a catastrophic effect. Loss of electricity supply has a significant cascade on other services, such as railways and the pumping of water, for example. Wireless communication networks underpinning critical services, should be considered as critical infrastructures them- selves as they also present as a cascade vulnerability where other societal services rely upon them [3]. The new European Networked Information System direct- ive came into force in 2016 [5]. This aims towards a more stringent consideration of critical information infrastructure protection. However, wireless technologies are not explicitly referenced, where the accountability and responsibility for the cyber security of both wireless and infrastructure aspects are left in the hands of the operator of the information infrastructure.

Wireless threat and vulnerability

The following describes aspects that threaten our wireless communication. These included both regulatory, environmental, inadvertent and potentially malicious threats.

Regulation and electromagnetic interference (EMI)

Spectrum is considered as a scarce resource and regulation somewhat limits its use. Since the first transatlantic radio communication in 1901 [5], access to spectrum has been regulated. Spectrum is segmented into bands and limits are imposed on transmission power. The new European Radio Equipment Directive (RED directive)

[6] superseded the R&TTE [7] directive in 2016. The RED directive places even more stringent emphasis on testing the receiver's susceptibility to interference, together with compliance to transmission specifications which will be linked to its transmission band and power. A primary goal is to allow radio equipment to coexist and to ensure one unit does not inadvertently interfere with another. This is considered in terms of both transmitting only within which spectrum and power levels permitted, and to be resilient in the face of other interference (e.g. due to legacy or faulty devices).

Electromagnetic interference is a primary threat to the availability and performance of wireless communication systems. Interference may be generated naturally around our environment [8], by poor quality devices, malicious interferers or jammers. Poor quality devices may generate non-linear responses; harmonics or intermodulation products which derive from the original signal, inadvertently interfering with intended transmissions in other bands. R&TTE and RED directives both seek to minimise out-of-band transmissions, and the RED directive extends to ensure that receivers are resilient to unintended interference. However, even with more stringent controls for product developments and approvals, not all devices are tested prior to sale and devices may degrade their performance over time, leading to out-of-band and inadvertent interference to other systems. See the case study on Television Interference Involving TETRA for an example of this.

Crowded spectrum

Spectrum regulation leads to crowding in some bands. The Instrumentation Scientific and Medical (ISM) and Short Range Device bands allow for a reasonably flex- ible use of spectrum by unlicensed users within set bands and transmission power limits. Wireless LANs, Bluetooth, Zigbee, etc. are all developed to use ISM bands. The prevalence of low-cost devices on the market, and our need to work wirelessly has led to crowding in these bands. The 2.4 GHz ISM band is es- pecially crowded in many urban locations. The major- ity of technologies that operate in ISM bands use carrier sense multiple access (CSMA) techniques. CSMA simply listens for presence of another transmit- ter and controls transmission to occur only when the spectrum is unused. As such, this can only provide a best-effort access to spectrum, commonly leading to reduced availability and delays in service where the system is used in crowded spectrum. Many arguments are made that ISM bands have led to more efficient use of spectrum, but at the expense of uncertainty of access [9]. New research and methods for sharing access to spectrum are needed to understand how to address this balance.

Advanced protocol analysis and manipulation

Easy access to spectrum allows for the possibility to analyse flows of traffic to ascertain typical operations and configuration. Simply listening to RF traffic, monitoring for modulation and coding type, packet sizes and regularity can identify both the protocol being transceived and key statistical signatures which can as- certain which devices are being used. Gathering information in this way can then lead to knowledge of alternative vulnerabilities and vectors for attack. See case *: case study on international mobile subscriber identity (IMSI) collection for an example.*

Presence detection and characterisation

Many mobile phone devices now contain multiple RF devices; WiFi, Bluetooth, 2/3/4G cellular, near field communication (NFC), etc. Silicon devices are highly integrated, allowing for multiple RF tranceivers to coexist within the same integrated circuit. With technology tightly integrated for the original purpose of providing advance wireless connectivity, these devices are also used to intercept and characterise our wireless communications.

Hence our current technologies are vulnerable, what about the future?

There is an increasing appetite to implement faster and more capable wireless communication systems (5th Generation Mobile – 5G [10]). On the other hand, we see activity to implement simpler and higher volume wireless devices (IoT [4]). Most importantly, communication technology for public safety, public protection and disaster relief (PPDR) and communications needed by critical infrastructures are key to safeguarding our society. These are often over- looked due to their low commercial volume.

In all cases, there are a number of common challenges to face both in terms of the disciplines required in consideration for the development of new secure wireless technologies, and the perceived needs for future generations of wireless technologies.

Multi-discipline development of future wireless

Engineering of wireless communication systems cannot yield secure solutions without the involvement of a collection of key actors. Primary actors include (with only a basic, underrated description):

RF and Information Theory Experts: To design the most efficient next generation methods of digital communication. RF experts cross the barrier between physics and the engineering of RF energy coupling and propagation. Information theory experts optimise cryptography and coding for more efficient, confidential and integral information transfer. Network engineers optimise interconnectivity and transfer of information between different systems.

Hardware Engineering Experts: to implement the hardware required to transceive RF energy, to develop low power processing capabilities, user displays and tactical/haptic interaction.

Software Engineering Experts: to implement efficient software to support the requirements of the RF, information theory, network and needs of the user application and information management systems.

Social Science Experts: to guide on how devices and applications will be used. If a device or application is not socially acceptable or useable, then there will be a limited acceptance and use. Ethical and psychological considerations play an important role here to ensure that the technology is pervasively integrated into daily operations, aiming to assist those operations, and not to burden them.

Legal and Regulatory Experts: to guide on the legal and regulatory barriers to the deployment of wireless systems. As described above, there are regulatory restrictions on how we may access spectrum. In terms of operational information, critical information infrastructure protection regulations aim to our critical services, and data protection regulations. Safeguard data protection and our privacy are prominent here. This expertise provides interpretation of the regulations and the means for the provision of standards and guidelines on how wireless devices should legally handle information.

Security Experts: This class of expert has the most difficult problem to cross all disciplines; to guide on the implementation of regulatory boundaries, the balance between protection and value added capability, working within social acceptance, and giving oversight to users and operators on the known methods of compromise to our wireless systems and the information that they carry.

Security spans the entire communication device, and the interrelation between physical operations and the different information systems that underpin our daily lives.

The security engineer has the most difficult and unenviable job, for which there is a limited skills capacity in many countries. Skills capacity is surely building on the malicious side. Furthermore, security skills are typically either broad and shallow to cover the basics of each aspect across these complex systems, or often lost in deep silos of specific capability, e.g. cryptography, or specific secure wireless protocols.

Can we protect ourselves and our systems?

Everyday, as consumers, probably not! Not with our low-cost devices and poorly perceived trust of the brands of the technology that we buy. In the consumer sense, we either need to be more vigilant on the default configuration of our devices, or simply trust the product that we buy. Sensibly, we cannot hope for much better than we have. The most difficult issue is keeping a wireless device's software up to date. If support to consumers can be improved, then consumers can be helped to protect themselves. This is evident through the regular updates and encouragement to install virus protection software on modern PCs. However, an equivalent level of protection is desirable for our consumer wireless devices to counter any new vulnerabilities which may be encountered after the wireless device leaves the factory.

With regard to critical communication systems, there is a more stringent process to follow to assure that software, wireless protocols and the information carried over wireless communication is going to protect and fulfil the sensitive needs of the critical application. This is typically arranged through contractual obligations for suppliers to provide continual support through a wireless product's lifetime; keeping systems operating reliably, tightly configured, software up to date and to support the hardware. Securing the supply chain is key here; hardware and software components may be vulnerable or even compromised even prior to integration and delivery of the wireless product.

The choice of how to implement a wireless system to maintain a secure existence considers a number of factors:

Physical Security: How to transmit? How easy is it to intercept the transmission? How to keep the processing equipment itself secure?

Protocol Security: How to control transmission? How easy is it to interpret and decode the transmission?

Organisational Support for Security: How to manage users of the wireless capacity? Does the organisational structure operating the wireless network have appropriate motivation to assure service access requirements to different classes of its users?

Societal and Operational Interaction: Do the users of wireless communication services honour their own obligations to keep information and applications secure and follow operational procedures? Interaction with devices must be carefully designed to ensure that they remain reliable enough for the purpose of use. Users must be supported by their technology to be able to:

- Easily and securely operate their applications and devices
- improve their operations and to not to hinder them

- too prevent a frustrated user from deciding to use an alternative and less secure method of communication to carry out their day job.

Consumers using social media are slowly learning what they can and should not share online with regard to their own personal situation and that of their friends and colleagues.

Case Study: wireless broadband for public safety first responders

This case study comprises of a number of factors surrounding wireless communication. We first cover aspects of economy of scale and spectrum allocation. We then consider challenges to the design aspects of the user interaction with those devices where wireless allows for communication during emergency and time critical situations.

Economics of spectrum

The public safety community has argued for many years to dedicate spectrum for use of broadband services by PPDR organisations and first responders. Their communication is mission critical and vital for saving lives. Sharing of spectral and network resources is highly controversial; a tension between economic and societal benefits. It is strongly argued that public safety communication should have an exclusive access to spectrum to be able to communicate immediately when necessary. On the other hand, the utilisation of spectrum will be relatively low compared to revenue generating commercial services that benefit mobile operators and governments alike. Traditionally, spectrum has been auctioned to the highest bidder to generate high revenues for governments. This is especially the case in the provision of commercial mobile networks, with a high consumer volume and, therefore, high revenues. For PPDR, the scale of use of communication technology is much lower than for consumers. There is therefore a limited argument supporting the competition for spectrum with low usage and a very different and more limited revenue model. However, the benefits are of a socio-economic nature, where technology is used to help saves lives, and recover from disastrous situations which may threaten our livelihoods and the economy. The London School of Economics argues the case for spectrum used as dedicated for public safety operations compared to being commercially allocated [11]. This study estimates that socioeconomic gain will be much greater if spectrum is dedicated for use by the public safety community than if spectrum is auctioned for use by a commercial cellular operator. A recent report made for UK Department of Culture Media and Sport [12] looks at the incorporation of social value into the consideration of spectrum allocation.

Whether spectrum is appropriately allocated for public safety, or where network sharing arrangements are made, significant socioeconomic benefits are expected to be made by improving the safety and security of our community; by better use and deployment of broadband wireless technology. This poses a bigger challenge for system development. Public safety first responders using secure broadband wireless technology will be able to use richer media, but will be making decisions under time pressure. If their devices and applications do not support their role in a timely manner with a high degree of accuracy, and therefore trust, they either would not use them at all, or make use of an alternative, more limited, possibly less secure, yet more reliable mode of communication.

Trustworthy commercial operation:

vulnerability induced by mobile network operation models Significant debate has been made in recent years with regard to the possible operational models for future broadband for PPDR. Commercial mobile networks commonly share resources between different opera- tors, such as base station antenna installations. Future considerations of network ‘slicing’ allow for sharing of other physical resources such as processing hardware and backhaul networking connectivity. Fundamental cost savings are made when sharing resources. This moves away from every mobile operator owning their own physical infrastructure.

The prospect of sharing these resources is controversial. Commercial mobile services can agree service level terms for sharing of resources on the basis that their individual service offerings to the consumer mobile user are similar. Sharing between high value consumer revenue generating services, and minimal revenue generating services for PPDR is a more difficult consideration, extending further the debate on dedicated spectrum as described earlier. Availability of PPDR services may be compromised in favour of fee paying consumer access. However, this may not necessarily be a conscious business decision.

This also requires functionality in the wireless and network technology to allow for critical services such as PPDR communication to be prioritised or to pre-empt consumer access. Whilst the mobile standards community have developed global technical standards for priority and pre-emption of services, no mobile operator has yet implemented and proven that wireless and network resources can effectively be shared between critical and consumer services. The UK Emergency Services Network [13] will be one of the first to test this sharing model.

Technology mistrust and subversion

The following gives and example of how a user of communication technology may inadvertently expose themselves. It is a common occurrence where users, frustrated with limited technology, will find other ways to communicate. In many countries emergency service first responders will carry both TETRA (or other push to talk voice system) and a typical mobile phone, using the typical mobile phone as a secondary communication medium to the secure and resilient TETRA system. Operational procedures will say that TETRA ‘must only’ be used for operational voice communications. However, one could anticipate what may happen when the TETRA device may develop a fault or is out of range, and where the mobile phone carries a long battery life and is in range. Would the first responder simply call back to base to report the problem, or continue to use the mobile phone to assist in the particular emergency? Similarly, the TETRA terminal will securely transmit GPS location of the responder, whereas the location of the mobile phone will most likely be easy to obtain. This example poses no problem during everyday regular activities, where the consequence of location exposure is simply not interesting to anybody other than an inquisitive scanning hobbyist. However, a group of adverse rouges with an intent to insight terror and disruption will surely find the location of public safety responders to be valuable. They may use this information to understand regular operations and protection strategies, and then divert their adverse activity away from responders for the most disruptive effect.

Disrupting the TETRA service by jamming or other means, may force users to choose their alternative technology, hence disclosing their operational picture, location of responders and the information services used.

‘Apps’ on the regular mobile phone may be found additionally useful to the first responder. Use of public information services is useful in many circumstances. However, there remains a risk of similar disclosure of responder situation and patterns of daily routine where mobile connectivity and information services are more widely accessible than those dedicated communication services which are specifically provisioned for the first responder, and their commanding colleagues.

Ad-hoc use of cheap COTs communication

On many occasions, cheap off-the-shelf communication systems have offered the best solution where installed mobile networks have been damaged or failed to deliver during a crisis. Backpacks can combine low-cost ISM band radios for voice and satcoms with wifi for data coverage. Allowing a small number of responders to communicate in adverse conditions is highly valuable for their collaborative effort. Whilst we consider this to be a less capable and often less secure mode of operation, having some communication rather than none at all is preferable. Where fixed mobile networks are installed, it is highly desirable to be able to integrate technologies such as this to allow access where some wireless capability fails, and other technology can take its place. However, these systems must deliver the same level of security. They must extend the approved mobile networks with the ability to work in isolation, but should not replace them with lower levels of security.

Secure wireless architecture design, implementation and operation

Developing wireless networks is a complex undertaking with all of the actors explained earlier playing key roles. Development of wireless networks to provide critical and secure communications to operate under critical and sensitive information assurance conditions is a challenge for all involved disciplines. Design and operation of the overall information system is key to yield and secure the benefits of future critically enabled wireless broadband. Such design must accommodate the true purpose of use, and both human use and misuse of the technology. Most importantly, misuse and malfunction is most commonly non-malicious; much more common than malicious subversion. Measures should be taken during technology development and installation, and be supported by operational procedures to maximise operational efficiency and to minimise misuse and malfunction.

Conclusions

This paper presents some of the basics of how wireless communication technology works and how it is used.

Throughout the paper we consider the threats and vulnerable properties of wireless, the types of information carried over wireless technologies, and examples of how wireless technologies have been hacked in recent years through small case studies (see case studies at the end of this paper).

We look at current activities to develop next generation wireless technologies and conclude with a need to build security into the next generation of wire-less communication systems from the outset, rather than to add secure features later.

Achieving wireless communication cyber security is a broad, multi-faceted and multi-disciplinary problem space. Challenges are posed for both the wireless and network technology aspects, but also the socioeconomic eco-system surrounding the need and use of the technology. Balancing these socio-technical aspects is key to protecting our personal and critical information that flows through the airwaves.

As with all considerations of cyber security, we live in a world of changing threat. Typical software technologies are now updated regularly. Wireless technologies are primarily comprised of software nowadays. Similar concerns should be considered with regard to the quality and longevity of the software that is implemented for our wireless components that are responsible for transmitting and receiving valuable information over the RF airwaves. Should we update or adapt RF transceiver software to cope with a changing RF threat environment, or do we simply rely on the disposable nature of consumer technologies to keep our wireless software up to date? Critical communication technologies typically have a lifespan of 20–30 years. Is it viable to maintain a long lifetime model like this? Or should these new technologies be made to be updatable or replaceable? Cost factors again come into play here.

A key concern could be with regard to the advent of the quantum threat [14, 15]. It is expected that modern strong cryptographic techniques will become vulnerable in the advent of the quantum computer within the next 10 years. Therefore, when considering long term deployment of new critical information infrastructure technologies, a strong consideration should be placed on the choice of cryptographic techniques which are known to be immune to the quantum threat.

International policy for cyber security is new. It is known that policy is much slower to update than the evolution of the information technologies that we use. Government actors must maintain close attention on the emerging cyber threat in order to assess the appropriateness and coverage of policy. In a similar manner technical standards may provide provisions to support the way in which wireless communication technologies may counter cyber wireless threat. In the changing threat landscape, standardisation bodies should assess that their security mechanisms protect against known threats but are sufficiently adaptable as threats change. Most importantly there is a skills shortage which must be filled and subsequently maintained.

Manufacturers and application developers must ensure that their products are fit for purpose. They should balance the usability and acceptance of the enabled information services with the mechanisms needed to keep information protected, as appropriate to its criticality and context.

Economic scaling will likely lead to shared spectrum and infrastructure models. Most importantly, operators of wireless networks must assure that wireless information services retain confidentiality, integrity, and availability. This must be achieved individually, differently and applicably for each of the many different classes of application and user. This then must provide a sustainable balance of priority and preemption for both critical communication services at lower volume and consumer use at high volume with larger economies of scale.

Wireless services enabling our critical infrastructures and consumer mobile and IoT applications must each be able to share resources without compromise of each other.

We, as consumers, simply need to be aware that others are using our wireless resources and be cautious and aware of the information that we share about ourselves, our family, friends and colleagues.

Acknowledgments

This work could not be compiled without the continued support of our team at HW Communications (www. hwcomms.com), and the constant discussion and liaison with our many collaborators in Horizon2020, InnovateUK, and other research projects with which we are involved. Special thanks to the members and partners of Public Safety Communication Europe (PSCE) Forum for the continued debate and hard work driving

towards solving the challenge towards resilient EU interoperable broadband communication (www.psc-europe.eu, www.broadmap.eu).

References

[1] 802.11ad-2012 – IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks– Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band

[2] 'White Paper – Visible Light Communication Technology for Near-Ubiquitous Networking'. Available at http://visilink.com/ wp-content/uploads/2012/03/Visilink-Technology-White-Paper-January-2012.pdf, accessed 23rd November 2015

[3] 'Methodologies for the identification of Critical Information Infrastructure assets and services', ENISA, February 2015. Available at https://www.enisa.europa.eu/activities/ Resilience-and-CIIP/critical-infrastructure-and-services/ Methodologies-for-identification-of-ciis/methodologies-for- the-identification-of-ciis, accessed 23rd November 2015

[4] Three 'Computer hackers can now hijack TOILETS: 'Smart Toilet' users in Japan could become victim to Bluetooth bidet attacks and stealthy seat closing'. Available at http://www. dailymail.co.uk/sciencetech/article-2384826/Satis-smart-toilets-Japan-hacked-hijacked-remotely.html, accessed November 2015

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[6] 'Overview of ITU's History'. Available at http://www.itu.int/ en/history/Pages/ITUsHistory-page-2.aspx, accessed 23rd November, 2015

[7] 'Key definitions of the Data Protection Act', UK Information Commissioners Office (ICO). Available at https://ico.org.uk/ for-organisations/guide-to-data-protection/key-definitions/, accessed 23rd November 2015

[8] The Radio and Telecommunication Terminal Equipment Directive 1999/5/EC. Available at http://ec.europa.eu/ growth/sectors/electrical-engineering/rtte-directive/

[9] RECOMMENDATION ITU-R P.372-12, Radio noise. Available at https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.372- 12-201507-I!!PDF-E.pdf

[10] Home Office Slips out and Android passport Reader. Available at http://forums.theregister.co.uk/forum/1/2013/ 06/20/home_office_slips_out_android_passport_reader/, accessed 23rd November 2015

[11] 'Before you use a WiFi Pineapple in Vegas during a hackers' security conference, you better know what you are doing.' http://www.networkworld.com/article/2462478/microsoft- subnet/hacker-hunts-and-pwns-wifi-pineapples-with-0-day- at-def-con.html, accessed 23rd November 2015

[12] '5G Innovation Opportunities', TechUK, August 2015. Available at https://www.techuk.org/insights/reports/item/ 6008-5g-innovation-opportunities-a-discussion-paper, accessed 23rd November 2015

[13] ‘Breaking radio silence: The value of communication in public services’. Available at http://www.lse.ac.uk/ businessAndConsultancy/LSEEnterprise /news/2014/Tetra.aspx

[14] The quantum clock is ticking on encryption – and your data is under threat. Available at http://www.wired.co.uk/article/ quantum-computers-quantum-security-encryption, accessed 6th February 2017

[15] SafeCrypto project. Available at www.safecrypto.eu, accessed 6th February 2017

[16] Radio Equipment Directive (RED) 2014/53/EU. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex: 32014L0053 [17] Ofcom RA419. Available at http://www.ofcom.org.uk/static/ archive/ra/publication/ra_info/ra419.doc

[18] ‘Technologies and approaches for meeting the demand for wireless data using licence exempt spectrum to 2022’. Final Report, Ofcom, January 2013, Quotient Associates. Available at http://stakeholders.ofcom.org.uk/binaries / research/technology-research/2013/demand-wireless.pdf, accessed 23rd November, 2015

[19] Dillinger, M., Madani, K., Alonistioti, N.: ‘Software defined radio: architectures, systems and functions’ (Wiley & Sons, 2003), ISBN 0-470-85164-3

[20] Mobile Network Security: a tale of tracking, spoofing and owning mobile phones. Defcon Moscow. OpenBTS & IMSI-catcher. – http://www.slideshare.net/iazza/dcm-final- 23052013fullycensored, accessed 23rd November 2015

[21] Hacking Wi-Fi is Child’s Play – 7 year old shows how easy it is to break a public network in 11 min. – http://www.dailymail. co.uk/sciencetech/article-2919762/Hacking-Wi-Fi-s-child-s- play-Seven-year-old-shows-easy-break-public-network-11- minutes.html, accessed 23rd November 2015

[22] https://cve.mitre.org/cve/cve.html, accessed 23rd November 2015

[23] ‘Research behind a hack of the Oyster card will be released which has serious implications for cards using the same MIFARE chip around the world’. Available at http://www. itpro.co.uk/604770/oyster-card-free-travel-hack-to-be- released, accessed 23rd November 2015

[24] ‘Gartner Says 4.9 Billion Connected ‘Things’ Will Be in Use in 2015’. Available at http://www.gartner.com/newsroom/id/ 2905717, November 2014, accessed 23rd November 2015

[25] UK DCMS, Incorporating social value into spectrum alloca- tions’. Independent Report, UK Department for Culture, Media and Sport, November 2015

[26] UK Emergency Services Network. Available at https://www. gov.uk/government/publications/the-emergency-services- mobile-communications-programme/emergency-services-network, accessed 18th September 2016

Case study

Additional examples of wireless compromise

Case study: television interference involving TETRA radio communication systems: In 2003 the UK Radio Agency (now OFCOM) published a document [16] in response to complaints about the use of new TETRA technology by the emergency services. This document clarifies that wideband TV amplifiers used on residential TV antennas are the most likely source of interference due to their own non-linear responses to the TETRA signals.

Case study: IMSI collection of 3G using 2G*:* Low-cost software defined radio [17] equipment can be used together with openly sourced code that can mimic a GSM base station. The 'man-in-the-middle' base station operates at a reasonably low power to avoid detection by the authorities and only for the time needed to carry out its operation. A 3G mobile device comes into range of the rouge base station. The rouge intercepts and notices the 3G operation of the mobile device. A jamming signal is transmitted which will naturally force the mobile device to fall back to 2G/GSM mode, registering itself with the rouge base-station and coming under its control. Further activity can be carried out to ascertain details of the phone, route calls, disable encryption or simply identify the presence of the user by identifying the IMSI which represents the SIM card and, hence, end user [18].

Case study: WiFi hacking*:* It is easy to obtain simple WiFi equipment with the capability to act as a man-in-the-middle access point to intercept, fool and even run routines to remove or crack encryption routines. A laptop offers a mere starting point. A seven year old recently demonstrated the ease of cracking a public Wi-Fi system in 11 min [19]. At the time of writing, searching for keyword 'WiFi' in the CVE database [20] yields 68 entries, the majority of which reside in the software within certain wireless devices.

Case study: Bluetooth hacking: With Bluetooth widely used for making phone calls, syncing contacts, 'Bluebugging' is the well-known method used to exploit vulnerabilities and take control of mobile devices. Power limitations typically reduce the range of Bluetooth devices to 10– 15 m. Directional antennas, similarly low cost, significantly increase that range. Searching keyword 'Bluetooth' in the CVE database [20] yields 109 CVE entries.

Case study: NFC reading – Oyster card: NFC allows for close proximity exchange of information with a passive device which is powered by the RF field generated by the reader device.

In 2008, a judge rules [21] that a hack found by Radbound University to reverse the algorithms in the Oyster Card (used on London Underground) should be made public. Free travel is therefore made available to all whom have the motivation to implement the hack until Oyster readers are updated.

Case study: NFC reading – ePassports: UK passports issued since 2006 include a NFC device now widely used for passage through auto- mated border control barriers. In 2013, the UK Home Office released an Android app [22] which can be used to decode your own, or anyone else's passport details using an Android device, most of which have built-in NFC transceivers.

Case study: Hackers on Hackers – Wifi hacking WiFi: There is a continuous challenge, to challenge and test each other. In famous conference Defcon22 in 2014, a well-known WiFi device, cheaply available and made easy to intercept WiFi transmissions was, itself, attacked [23]. Many hackers where known to have utilised this device in preparation to demonstrate their own interception and hacking prowess during the conference. To their dismay, all users find that their device itself had been hacked and rendered useless after connecting to the conference wifi network.