Engineering and Physical Sciences Research Council TOSHIBA University of BRISTOL ROKE GCHQ

University Lead: Professor Mark Beach (University of Bristol)
Business Lead: Dr Woon Hau Chin (Toshiba)

Project Title: Secure Wireless Agile Networks (SWAN)
Training Grant Reference: EP/T518219/1

SWAN
SECURE WIRELESS AGILE NETWORKS

EPSRC Prosperity Partnership Annual Report 2020

Grant Reference: EP/T005572/1

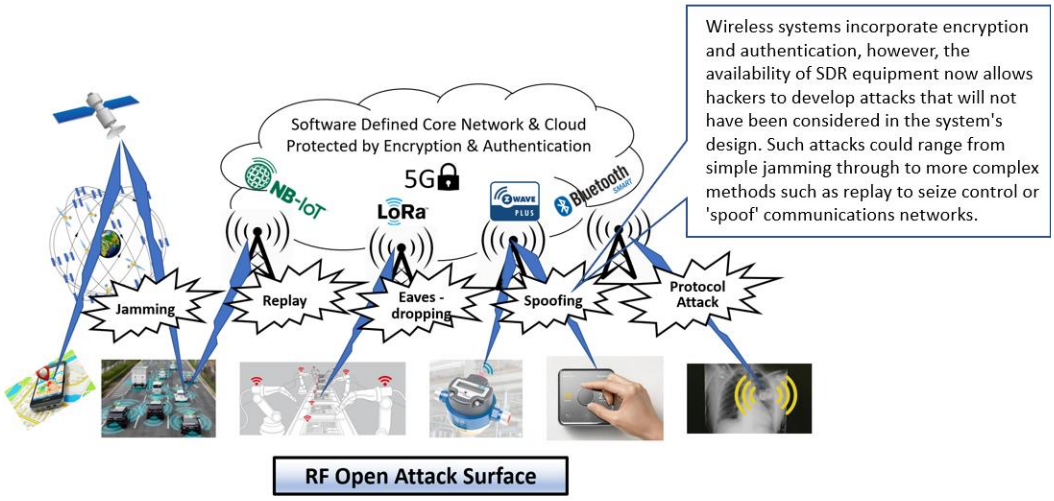
1. Summary

Wireless access is essential to the networks that underpin modern life, but many networks which rely on Radio Frequency (RF) interfaces are especially vulnerable to cyber-attacks or other failures. Jointly funded by EPSRC, Toshiba Europe Limited (TEUR), Roke Manor Research Limited, GCHQ, and the University of Bristol, the SWAN Prosperity Partnership focuses on the creation of Secure Wireless Agile Networks (SWAN) that are resilient to both cyber-attacks and accidental or induced failures through a 5-year collaborative partnership.

2. Introduction and background

SWAN aims to create both hardware and software enabling technologies for radios that can truly be software defined and *Secure by Design* down to the basic levels of system functionality, such as operating frequency bands, modulation, and multiple-access protocols, as well as the surrounding frameworks needed to make resilient and secure systems. In order to achieve these goals, SWAN's key aims are:

- To identify vulnerabilities in RF interfaces;
- To develop techniques to detect and mitigate against the effects of cyber-attacks and other subversion;
- To create enabling technology for Software Defined Radios (SDR) following *Secure by Design*[1] principles;
- To develop systems that are more resilient and secure, to enable robust Dynamic Spectrum Access.



Wireless systems incorporate encryption and authentication, however, the availability of SDR equipment now allows hackers to develop attacks that will not have been considered in the system's design. Such attacks could range from simple jamming through to more complex methods such as replay to seize control or 'spoof' communications networks.

As a Prosperity Partnership project, SWAN brings together key expertise from academia, industry, and government to deliver a co-created and evolving research programme that will have real-world industrial applications of national importance against a type of threat that is continually developing.

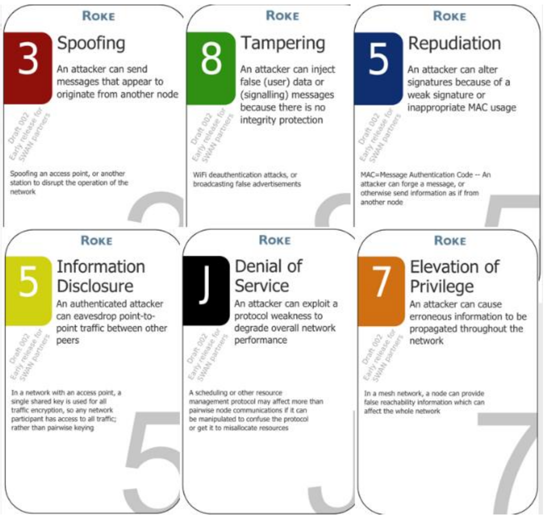
The University of Bristol has a leading role in SWAN, contributing world-class expertise in the areas of physical layer wireless research, RF technologies, and Dynamic Spectrum Access. As the Lead Business Partner, Toshiba brings more than 140 years of experience as a technology pioneer and an investor in cutting-edge research. Toshiba has a special interest in cyber security, particularly when applied to wireless and broadcast systems, once of its key business areas. This expertise is complimented by the leading-edge cyber defence capabilities of Roke, and the advisory capability of GCHQ, the intelligence and security organisation responsible for providing signals intelligence and information assurance for the government and armed forces of the UK.

Throughout the 5-year programme, SWAN will deliver impact through our business partners, Toshiba and Roke, embedding technology and know-how in products; a series of multi-faceted external dissemination activities; influencing standards, policy and regulation; as well as encouraging the adoption of *Secure by Design* within engineering curricula through University degree programme accreditation.

3. Project achievements: outputs, outcomes and impact

Though still in the first year of the project, and despite disruption due to the Covid 19 pandemic, the SWAN team have been able to make considerable progress towards establishing the research fabric of the partnership through the completion of initial deliverables, the upskilling of key team members, and developing a network of stakeholders through engagement activities.

Key technical deliverables:


ROKE
3
Spoofing
An attacker can send messages that appear to originate from another node
Draft 002 Early release for SWAN partners
Spoofing an access point, or another station to disrupt the operation of the network
ROKE
8
Tampering
An attacker can inject false (user) data or (signalling) messages because there is no integrity protection
Draft 002 Early release for SWAN partners
WiFi deauthentication attacks, or broadcasting false advertisements
ROKE
5
Repudiation
An attacker can alter signatures because of a weak signature or inappropriate MAC usage
Draft 002 Early release for SWAN partners
MAC=Message Authentication Code -- An attacker can forge a message, or otherwise send information as if from another node
ROKE
5
Information Disclosure
An authenticated attacker can eavesdrop point-to-point traffic between other peers
Draft 002 Early release for SWAN partners
In a network with an access point, a single shared key is used for all traffic encryption, so any network participant has access to all traffic; rather than pairwise keying
ROKE
J
Denial of Service
An attacker can exploit a protocol weakness to degrade overall network performance
Draft 002 Early release for SWAN partners
A scheduling or other resource management protocol may affect more than pairwise node communications if it can be manipulated to confuse the protocol or get it to misallocate resources
ROKE
7
Elevation of Privilege
An attacker can cause erroneous information to be propagated throughout the network
Draft 002 Early release for SWAN partners
In a mesh network, a node can provide false reachability information which can affect the whole network

RF STRIDE card deck threat assessment system developed by the Roke team.

<u>SWAN White Paper on RF Vulnerabilities:</u> As defined earlier, one of SWAN's specific aims is to understand the vulnerabilities of the RF interface. With the goal of forming an overarching project reference document for SWAN, our research team have produced an extensive internal paper on RF vulnerabilities (D1.11). From this deliverable, we have established that two additional versions of this paper will be produced: a document aimed at the general public to be published on the SWAN website (D1.12), and a full white paper to be published in one if the peer reviewed IEEE, IET and Blackhat conferences or journals aimed at the security professional community (D1.13). These additional papers will be completed by the end of 2020/beginning of 2021.

This white paper sets out to define RF vulnerabilities and identify different types of attack including jamming, spoofing, and sniffing. The paper draws on a modified version of the Microsoft STRIDE model developed by the Roke team to facilitate the identification and assessment of threats over the RF interface.

Through the examination of several use cases, including GNSS, Wi-Fi rogue base stations, keyless car theft, and Internet of Things (IoT) LoRaWAN, the white paper demonstrates the types of threats that can be mounted against RF interfaces and the subsequent need to detect and mitigate these types of attacks.

<u>SWAN Testbed:</u> A key element of the SWAN technical work packages involves the development of a testbed, which will be used to authenticate and assess identified threats, to verify techniques to discover and eliminate threats, and to test enabling RF technologies. The SWAN research team have outlined the architecture and requirements of this testbed in the Initial Test-bed Specification (D6.1) and have completed a follow-up paper on RF Attack mechanisms & test bed needs (D2.1).

<u>Other technical work packages in progress:</u>

- (WP2) Threat Synthesis & Assessment: Manish Nair (University of Bristol), Steve Wales (Roke)
  - Modelling of RF cyber vulnerabilities in commercial wireless systems: synthesis and analysis
  - Synthesis (MATLAB and Simulink) - development of threats targeting the PHY and MAC control signals of specific systems such as LTE, WiFi and 5G.
  - Analysis of quality metrics to identify threats against a dynamic signal environment - variations in wanted signal occurring due to the channel, the presence of other interfering signals, and, possibly the evolution of new metrics or approaches to identify threats in this type of environment.
- (WP3) Detection & Defence: Vaia Kalokidou (UOB)
  - Selection of state-of-the art detection and defence mechanisms (relevant to SWAN use cases)
  - Development of a model based on SWAN use cases (priority to LTE/WiFi Rogue BS and LoRaWAN) - in conjunction with WP2 - simulating possible threats (such as spoofing and jamming)
  - Introduction of current and novel detection methods on this model to evaluate system performance

- (WP4) Enabling RF Technology: Eyad Arabi & Manish Nair (UOB), Gavin Watkins (Toshiba)
  - Transmitter: Investigation of RF fingerprinting as a method for security enhancement. The focus will be on the design of the RF transmitter for improved feature extraction.
  - Receiver: Frequency agile and secure receiver design is investigated. Wideband linearisation techniques based on feedforward and post distortion in cascade low noise amplifiers (LNAs) is proposed for high interference environments, not all of which may be hostile. Limiting circuits based on switched diode-clampers, and, modelling of hostile interferes as blockers which affect the spurious free dynamic range (SFDR) such receivers, is of interest for robust operation in jamming scenarios.
  - Simulate a multi amplifier architecture in ADS and characterise the load pulling effect between the individual amplifiers.

Training and career development of the SWAN team:

One vital pathway to impact for SWAN is the development of both academic and industrial leaders to influence the next generation of RF systems on a global scale. The industrial engagement designed into SWAN includes a strong training element that is aimed at exposing the research team to knowledge transfer, technology transfer and industry practices as well as direct feedback, guidance, and training from partners.

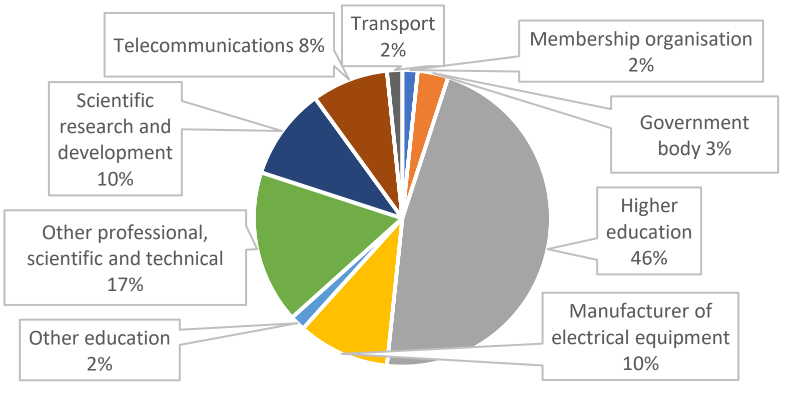
In the initial stages of the programme, we have been focussing on developing the knowledge and skills of our research team, building on the expertise of our industrial partners and external collaborators to put our researchers in as strong a position to begin tackling the SWAN Research Challenges. We have delivered several training sessions aimed at developing these skills, including:

- Introduction to Cyber Security – Theo Spyridopoulos (Toshiba Europe Ltd)
- An Introduction to Risk and Threat Modelling – Alex Collins and Professor Mark West (Roke)
- Internet of Things Security and Security by Design Principles (Copper Horse)
- Several equipment demonstration webinars delivered by external collaborators Rohde & Schwarz, Anritsu, Keysight, and Spirent.

Given the importance of defending against RF attack, it is vital to understand fully how best to disrupt a communication link in the most efficient and covert way possible. This underpins the need for an RF style hackathon in early 2021, delivered in a format that can be Covid secure. We are currently in the process of developing a remote hackathon activity with partners Roke and GCHQ which will incorporate a number of practical exercises designed to challenge internal teams to use a variety of commercial software defined radios to generate jamming signals against candidate RF communication technologies.

Engagement and dissemination:

Figure 1: SWAN Newsletter Subscribers by Sector



Another of SWAN's main objectives is to propagate wireless *Secure by Design* principles to the wider community and to build links with key security organisations and networks. We have taken several important steps towards building this network of stakeholders in both industry and academia through a series of engagement activities throughout the year.

The SWAN website is now live and fully developed. This site will be a critical platform in the dissemination of SWAN outputs, papers, relevant blog posts, and events. We have been able to increase engagement with the website through building our social media presence on both Twitter and LinkedIn.

In Autumn 2020, we launched the first issue of the SWAN Quarterly Newsletter, a regular overview of the latest SWAN activities, updates on recent blog posts and events, and opportunities to get involved in our research. We have been able to build a strong initial network of 60 subscribers from higher education, government, and multiple technical industry sectors (see Figure 1).

Alongside these engagement activities, SWAN team members have been able to present about the programme at several virtual events, including the Bristol Cybersecurity Innovation Meetup (May 2020), 5G Week (September 2020), the Smart Internet Lab Network and Data Infrastructure Security (NDIS) workshop (November 2020) and the University Defence Research Collaboration Signal Processing Workshop (November 2020). The first SWAN External Advisory Board took place in July, allowing the partnership to take on board feedback and insights from industry, government, and academia.

4. New collaborations

Throughout the year, the SWAN team have built several new collaborative relationships with parties both external and internal to the consortium, including: Copper Horse, UltraSoC (now Tessent), Active Building Centre (ABC), Pen Test Partners, u-blox, Rohde & Schwarz, Anritsu, Keysight Spirent, and Bristol Cyber Security Research Group. These relationships have the potential to develop into collaborative activities in the year ahead, including delivering additional training webinars, joint events, and PhD student mentorship.

Additional funding arising from new collaborations aligned with SWAN:

- SYNERGIA - Innovate UK Security for IoT Networks Award - £2.2m project awarded to SWAN Business PI Woon Hau Chin and teams at Toshiba, University of Bristol, and other external partners
- CELTIC-NEXT Innovate UK Award: 'AI-enabled Massive MIMO' (AIMM) – project involving SWAN PI Mark Beach and other team members from the CSN Group with partners BT. Looking at the use of AI in network management, aligning with SWAN's focus on AI methods to detect intrusion
- National Security Technology and Innovation Exchange (NSTIx) pump-priming project investigating the use of ML techniques for detecting intrusion in non-cellular IoT. Designed to test the concept of co-creation whereby Industry, Academia and Government work together on a common project instigated by GCHQ.

5. Staff Highlights

SWAN benefits from a team of highly skilled researchers and PhD students from across the partnership. Since the project kicked off in February 2020, SWAN has welcomed several new team members, including:

- Jiteng Ma – Fully funded by Toshiba, Jiteng started his PhD in February 2020 and is focussing on Agile, Linear and Power Efficient RF transmitters through the application of Digital Power Amplifiers (DPA).
- Dr Manish Nair – Dr Nair joined the SWAN team in April 2020 as a Senior Research Associate RF Transceiver Architect. His research with SWAN focuses on MAC-PHY security with a strong focus on RF active circuit design, passive circuit design and the design of SWAN transceiver, which will implement advanced signal processing and ML algorithms for RF cyber-physical security.
- Dr Tommaso Cappello - Dr Cappello joined the CSN Research Group at the University of Bristol in May 2020 as a Lecturer. His current research interests include RF and power electronics and digital signal processing techniques for high-efficiency transmitter applications.

An additional academic post, a lectureship focussing on Artificial Intelligence and Machine Learning in Wireless Networks, will soon be aligned to the project. The project will shortly be advertising several topics for PhD studentships who will be due to commence their research in early 2021.

Papers acknowledging SWAN published by aligned research associates and PhD students:

- S. Ozan, M. Nair, T. Cappello, M. A. Beach, (2020) "A High Linearity Wideband Low Noise Amplifier for Mid-Band 5G Receivers" to be presented at *APCCAS 2020*.
- E. Arabi, K. M. Morris, M. A. Beach, (2020) "Analysis of the Coverage of Lossy Tunable Matching Networks" to be presented at *APMC 2020*.

6. References

[1] Department for Digital, Culture, Media & Sport (DCMS) (2019) Secure by Design. https://www.gov.uk/government/publications/secure-by-design. Accessed 22 Oct. 2020