Secure Wireless Agile Networks (SWAN) EPSRC Prosperity Partnership

Email: swan-programme@bristol.ac.uk | **Website:** www.swan-partnership.ac.uk
Twitter: @PartnershipSWAN | **LinkedIn:** linkedin.com/company/swan-prosperity-partnership

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

SWAN
SECURE WIRELESS AGILE NETWORKS

ABOUT THE PROGRAMME

Creating secure, resilient, agile and sustainable wireless technology for future communications systems.

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.

In a five-year joint research programme, the Partnership will work to identify vulnerabilities in RF interfaces, enabling the development of techniques to detect and mitigate against the effects of cyber-attacks and other forms of subversion.

SWAN aims to create enabling technology 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.

Key aims:

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

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

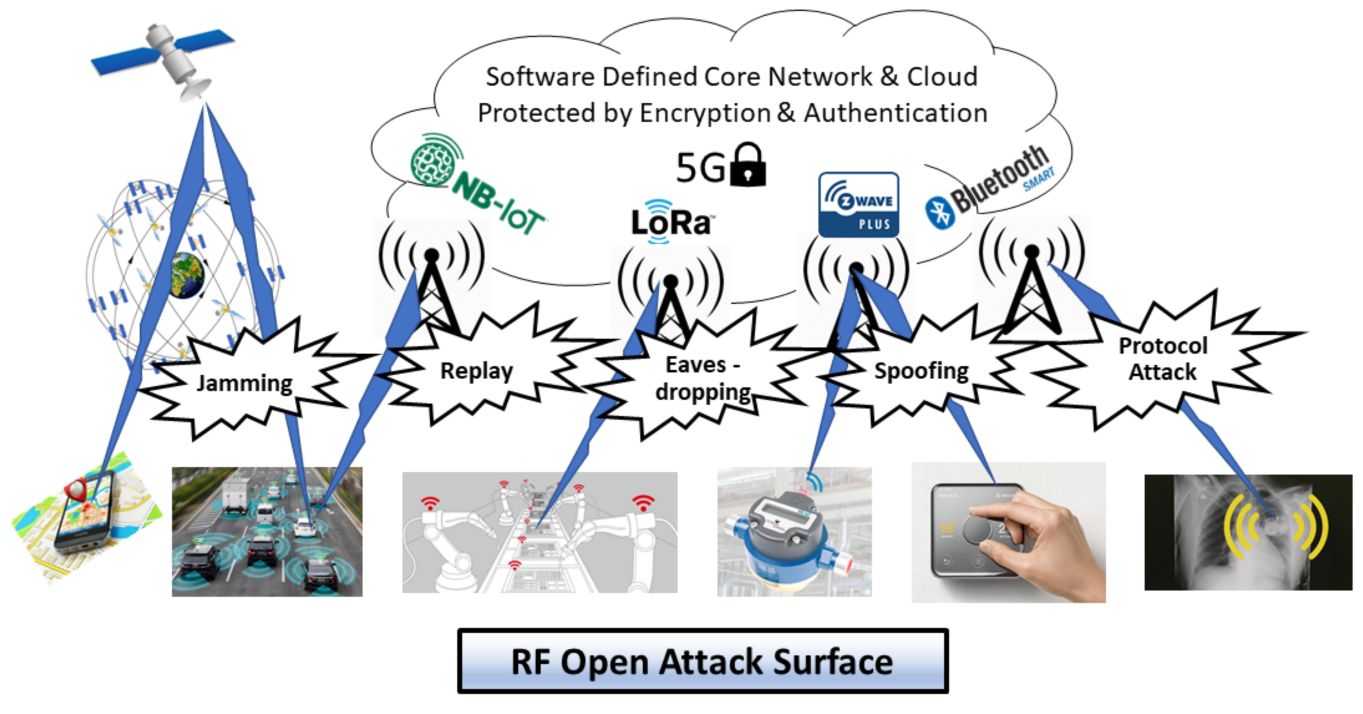
THE PROBLEM

Though modern wireless systems incorporate encryption and authentication, the availability of software-defined radio 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.

In the worst case, vulnerabilities in mass market mobile phones might be exploited to distribute “RF malware”, for example to jam large numbers of cell sites.

It is important to proactively identify and understand these vulnerabilities and develop protective measures, which should ideally include the ability to field-update every aspect of the physical layer radio operation, in line with key principles of secure design.



PROGRAMME OBJECTIVES

SWAN will extend key Secure by Design principles to the radio interface and enable the fundamental parameters and architectures of wireless systems to be:

- Adaptable to new spectrum and interface specifications;
- Resilient against accidental or induced failures (such as jamming and replay);
- Resistant to cyber attack.

SWAN will therefore strengthen the UK's ability to defend its critical infrastructure and bring new secure radio technologies to market, as well as addressing secondary attacks upon wireless simple devices to render large complex installations inoperative (e.g. smart city IoT infrastructure).

Programme Objectives:

1. Establish a methodology to understand and synthesize attacks on communications systems vectored through the radio interface
2. Develop methods for effective and efficient RF threat detection, analysis and mitigation
3. Develop methods to design and implement agile and resilient transceivers
4. Develop a testing methodology and resource for radio networks to evaluate threats and mitigations, avoiding the tendency to “group-think” that could exclude various types of attack or defence
5. Apply SWAN’s secure agile and robust RF technology to Dynamic Spectrum Access to enhance spectrum utilisation whilst mitigating misuse
6. Train SWAN’s academic and industrial team to embed Secure by Design principles in future wireless devices, systems and standards
7. Propagate wireless Secure by Design principles to the wider community, including undergraduate and taught postgraduate education
8. Engage with the security community by building links with RITICS, PETRAS, NCSC, and other key organisations and networks

SECURE WIRELESS AGILE NETWORKS

RESEARCH CHALLENGES

RC1: Threat Synthesis and Assessment

- Vulnerabilities of wireless to RF cyber attacks have received little attention.
- For critical infrastructure, impact of denial of service and manipulation of data and control need to be understood, as well as understanding the mechanics of such an attack.

RC2: RF Cyber Detection & Defence

- Power and cost-effective solutions required for large-scale monitoring of potential attacks.
- Resilient waveforms, robust protocols and enhancement spatial processing techniques are required to defend assets.

RC3: Cyber Secure Radio Design

- Need for RF architectures which are more resilient to attack and facilitate the detection of an adversary.
- RF transceivers which can offer enhanced frequency agility and thus support dynamic spectrum access (DSA).

RC4: Secure Dynamic Spectrum Access

- Understanding the vulnerabilities of sharing protocols is essential if DSA is to be secure.
- Need for enhanced RF transceiver technology to support a change from fixed spectrum allocation.

[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

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