Proposed PhD Research Areas

I am looking for strong PhD candidates to work on the projects listed below. The ideal candidate would have a mix of theoretical and practical skills, achieved a distinction or merit from the ISG MSc in Information Security, taken the IY5606 module and completed a Smart Card Centre related project. Of course other equivalent candidates (from other institutions) will be considered and are encouraged to contact me.

1. Fault Attacks for Virtual Machines in Embedded Platforms

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

The concept of introducing fault attacks while cryptographic algorithms are executing in embedded systems and more specifically in smart cards, has been studied extensively. At the same time, progressively more embedded devices like smart cards and mobile phones are relying on virtual machines for secure application execution. However, these execution platforms (e.g. Java Card, Globalplatform, Multos, and Android OS) can be subjected to a number of fault attacks in order to bypass the security mechanisms of the underlying platforms. This project aims to examine how fault attacks can be combined with logical attacks in an efficient way towards a relatively controlled abuse of the underlying platforms. The main aim of the work involves identifying practical vulnerabilities and more importantly, proposing countermeasures so that the platforms will be in position to identify these attacks, attempt to reduce their significance and at the same time recover the platform in a safe state.

2. Mobile Devices and Platform security

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

I am interested in a broad range of new research projects relating to mobile devices, their security and applications. The spread and use of mobile devices, including mobile phones and tablets, has proliferated over the last few years. Although these devices offer powerful execution and communication capabilities, it is this very feature that poses significant risks. This thread of research effort involves the identification of similar critical challenges in an attempt to propose efficient solutions. In particular, we are interested in the following three areas:

- Mobile device malware and botnets. Modern mobile devices present close resemblance to traditional computing environments. It is evident that traditional challenges (e.g. viruses, root-kits and malware) will attempt to find their place into these “new” and more-or-less always connected to the internet devices. The proposed work should investigate ways in which mobile devices can be infected with malware and propose adequate countermeasures. The work should extend into the design and implementation of desired functionality, based on the above principles of root-kits and mobile agents that will improve the overall security of these devices.

- Investigate whether applications and services fulfill their pre-download claims after they are downloaded in these devices. For example, a number of applications state their requirements in terms of access to services and personal data (e.g. call lists, contacts, sms, diary) when they are about to be downloaded. This should form a “contract” between the application and the underlying platform. This work should examine how this notion of “contracts” can be formalised, enforced and extended to cover other cases as well.

- Malware is one of the most challenging threats the information security community is facing today, with antivirus vendors receiving thousands of malware samples every day. Malware authors increasingly invent new ways to bypass antivirus detection and are doing so with great success, as most antivirus solutions are based on known malware signatures in order to identify malicious programs. This research thread aims to investigate dynamic-based detection methods on PCs and mobile devices, including obfuscated (including polymorphism) malware along with anti-emulation techniques, including methods like encryption and steganography.

- The concepts of Trusted Execution Environments (TEEs) and Trusted Service Managers for mobile devices have been proposed both by industry bodies and by academic propositions. However, there are significant opportunities for improvement at the overall architectural design and operation of these proposals. More specifically in terms of their integration with the underlying platform, their process scheduling and execution methodologies, context switching algorithms, etc. Finally, all the above might create opportunities for new attack vectors that could be exploited. This research thread should investigate innovative methods to tackle some of the above issues.

3. E-Voting

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

A number of e-voting protocols have been proposed in the academic literature. At the same time, a number of real world implementations based on different technological propositions have been utilised in trials and actual elections. The project requires a thorough review of these proposals, identification of major attacks (existing and new ones). More importantly, the work involves the identification of new and verifiably robust (for all participating entities) e-voting propositions that will take into account the specific requirements of mobile devices and embedded systems. Furthermore, it involves the utilisation of various mechanical and formal verification tools (e.g. Casper/FDR, AVISPA, etc) in order to verify the correctness of any proposed protocols.

4. Societal Health, Inclusion and Security

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

Mobile devices have access to a variety communication channels (e.g. GSM, WiFi, Bluetooth, NFC) and, at the same time, they have enough processing power that allows them to execute relatively demanding applications. There are also a number of calls (at European, national and local government level) requiring that all citizens should feel and actually be included in the society. This research thread aims to investigate various methods that will enable the secure and interoperable communication of different devices (e.g. mobile phones and set-top-boxes) along with a variety of sensors (e.g. RFID, WiFi, etc.). This will investigate further on into secure and reliable methods that will enable “vulnerable” citizens (e.g. elderly, young, special care) to have access to personalised care and other social activities (e.g. e-learning, communication and advertising).

5. Machine-to-Machine (M2M)

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

"The technologies which allow embedded processors, smart sensors, mobile devices, actuators and computers to communicate directly with one another, take measurements and make decisions based on those measurements – often without human intervention – are described with the term `M2M`". It is true that there are M2M communications that are encountered in automotive, smart grid, health care, routers, smart metering, etc. For example, in the automotive industry, there are proposals which include the provision of such communications between different car components (e.g. brake pad sensors, engine, etc.) with the central car computer. There are even proposals which suggest car-to-road and car-to-car communications. There are also a few proposals which explore the issues around smart metering systems, mainly for electricity meter,s but also for road tax purposes. All these proposals deal with fundamental information security principles (Confidentiality-Integrity-Availability) along with overwhelming operational characteristics. The project intends to realize an extensive security investigation of the M2M systems, in order to analyze potential attack strategies and to formulate countermeasures.

6. Processor and Micro-controller Security

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

A large number of embedded systems rely heavily on microprocessors with restricted processing power and storage capabilities. It is often the case that these embedded systems have specific security requirements (e.g. in terms of authentication, authorisation, execution and communication) that will have to be addressed by such microprocessors. This research thread can take a variety of directions including exploring these specific security requirements and providing efficient solutions to very fundamental problems of:

- Secure application execution in embedded microprocessors.
- Code adjustments for different execution environments.
- Extend the application execution between "multi-core" execution environments.
- Distribute application/storage execution between different components/processors
- Examine the security requirements for micro kernel operating systems.
- Software based attestation.

7. Embedded Device Security

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

It is often the case that mobile devices (e.g. mobile phones) are also considered as embedded devices. It is envisaged that increasingly often, these devices will be involved in a number of sensitive operations such as payment, social/professional networking, etc. Anonymity techniques for maintaining privacy protection in mobile/embedded systems is receiving a lot of attention. At the same time, enabling these devices to retain anonymity but ensuring fair-exchange of goods and products, is also a whole research area by its own. A concept which is closely coupled together with the secure use of these devices (though the use of cryptographic protocols) is related to their ability to generate random numbers. These devices offer a whole new range of sources of randomness. This project aims to explore some of the above security requirements in an attempt to provide efficient and scalable solutions.

8. Security and Privacy Issues in Crowd based Cloud Computing

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

The concept of the crowd based cloud-computing deals with the way in which individual devices in a locality come together in a fluid, dynamic and ubiquitous way to accomplish a task or collection of tasks. It differs from the cloud computing as the service is decentralised and participated by individual devices that advertise their services – in exchange for some services from the requesting entity. Applications of such architectures are in the field of mobile phones, tablets, and sensor networks. Therefore, the project will investigate the security, privacy, anonymity, accountability and sharing requirements of such an operational scenario, in order to propose novel protocols that will address the above security requirements.

9. Security and Trust for Swarm Intelligence Architectures

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

Swarm intelligence deals with the collective behaviour and the limited features of decentralised and self-organised systems. In nature, the ant and bee colonies base their decision on swarm intelligence that governs their choice of route and management of the colonies. In this project, we will explore the concept of swarm intelligence and how it can be deployed in variety of operational scenarios, e.g. vehicular systems, network security, malware, with particular emphasis on embedded systems. Such a swarm structure would require security, privacy and trust architecture. The project will examine different ways in order to provide such architectures.

10. Gait Based Authentication for Mobile Devices

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

Modern smart phones have the ability to measure the GPS location, motion and motion direction (3D accelerometer). This research thread aims to examine how these technologies can be combined, in order to provide the principles of gait based authentication. This work will be termed as “Walk and Get Authenticated”.

11. Financial Systems and Payment Cards

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

The Europay-MasterCard-Visa (EMV) standard has played a crucial role in the provision of a unified, relatively secure and robust infrastructure for chip based payment transactions. EMV is widely adopted across the globe as the interoperable standard for card based payments. Since its adoption (in the so called Chip-and-PIN programme) in the UK, there has been a dramatic fall in card present transaction fraud levels. However, over the last few years, a number of EMV protocol weaknesses have come into light which, if exploited, may have the effect of undermining consumer confidence in the payment technology. At the same time,, new payment vehicles, e.g. contactless cards, mobile phones, Near Field Communications (NFC), peer-to-peer payment protocols have reached maturity and they have been deployed in a number of real world environments. This project will investigate the critical aspects of “card” based payment standards including:

- EMV payment specifications against known, assumed vulnerabilities.
- The use of contactless, mobile/NFC devices as the underlying payment platform.

- Explore countermeasures against a number of practical and theoretical attacks, including relay attacks.
- Identify new innovative ways in which payments can be linked with delivery of physical and digital products.

12. Cyber Physical Systems for Security Critical Services

Supervisor: Dr Konstantinos Markantonakis, K.Markantonakis@rhul.ac.uk

The need for trusted hardware grows as computer technology converges more and more with our every day tasks, ranging from secure payment, mobile communications, etc. At the same time, embedded systems include a number of different devices ranging from smart card microprocessors, RFIDs, smart tokens, mobile devices, etc.

This research thread aims to provide a thorough understanding of the uses of embedded devices, in order to provide security critical services. It will take into account the limited processing resources of these devices and explore various operational characteristics that should take into account remote management requirements, micro-kernel attestation, device authentication, and secure communications.

NOTE

There is limited funding, mainly in the form of full-time PhD EU/Home fees, to be offered to some of the research topics. The decision as to which successful projects/candidates will be funded is entirely up to the ISG Smart Card Centre. Please request more information when you contact the dedicated supervisor (i.e. Dr Konstantinos Markantonakis).