Proposal for research on Model-based Security Testing for RFIDs in Automotive

SAKET UPADHYAY, Vellore Institute of Technology, India

Robust security strategies and protocols' security for communication, authentication and validation have been an important topic of interest in Radio Frequency based Identification (RFID) devices and Vehicular Communication.
This work is a proposal for Coventry University's doctoral cotutelle project with Deakin University on "Model-based Security Testing for RFIDs in Automotive", where we will discuss common findings and interests in the domain. In this application, we will start from our motivation for the project eventually building upto 3.5 years execution plan, covering a brief literature survey, common objectives, candidate's experience and their potential contribution in realising the target objectives while keeping the program's expectations from a potential candidate in mind.

Key Words and Phrases: [redacted]

Contents

1 MOTIVATION/RATIONALE

Radio-Frequency Identification (RFID) devices are being extensively used for vehicle access control, fuel dispensing, part identification, border crossing supervision, vehicle inventory, fleet management, and more.[1] While the extended use includes (but is not limited to) vehicle's speed monitoring and traffic control using active RFID solutions.

Over the years the integration of RFID tags with automotive industries has exponentially increased due to its properties which makes it cheaper to manufacture and easy to use. As it can work passively by relying on the RFID scanners for the power requirements, we can manufacture an air- and water-tight enclosure for our RFID equipment which makes them remarkably durable in long term. But due to general RFID's heavy dependence on the reader and supporting infrastructure for any privacy protection features and lack of decent processing power, it allows a wide range of security vulnerabilities.
Given the widespread use of RFID technology, the attack surface is also very large and as we progress towards fully autonomous systems for the automotive industry, we must develop robust security solutions and strategies for the deployment of RFID components in upcoming vehicles.

The work on "A New Secure RFID Anti-Counterfeiting and Anti-Theft Scheme for Merchandise", even though not directly related to automotive communication, gives a good insight into RFID security application and its elements. [1] "security analysis for the proposed protocol based on the strand space method to prove that the proposed protocol is secure" was something new to me as I used to wonder how one establishes the authenticity of the proposed protocol. The approach used two RFID tags instead of a traditional approach of one, with a reading station and two remote servers (Anti-counterfeiting server and Anti-theft server) for computing selected part of the handshake.

This approach (with many others in the field) is enough to pique our interest in RFID based security research and inspire us to think about different non-traditional ways in which we can improve existing solutions.

2 LITERATURE SURVEY

RFID is a pretty aged and readily available piece of technology nowadays, but the security for the same appears to be not up to speed with exponentially increasing area of application.
Technically, RFID is any Radio Frequency device used for personal IDentification of people, animals or assets. [redacted]

[redacted]

[1] https://skyrfid.com/RFID_Vehicle_Management.php
[2] https://www.iso.org/standard/73596.html

Low-cost RFID cards don't have enough processing power to execute any kind of encryption routine, but when we [redacted] and presents enough evidence for the need for more research and innovation in the field.

2.1 RFID in Vehicular Communication

"Radio Frequency Identification (RFID) technology provides for a lightweight and small tagging technology for passive communication for a range of applications, including in the automotive manufacturing and supply chain, and also vehicle on-board systems (such as Tyre Pressure Monitoring Systems)."[3]

[redacted]

[redacted] are expected to have more processing power than the former and can support some limited computation.

In another similar proposal, Vinod Kumar et al. [6] talks about vehicular cloud computing or VCC where they propose an "RFID based secure and efficient authentication protocol for vehicular cloud computing". In the proposed approach the tag computes a part of the ECC key and the RNG is handled by the server, the reader just [redacted] handles the information exchange.

And discusses the following attack models (based on their proposed protocol) -

- An attacker E may want to break the communication among the RFID-assisted tags, or readers or database server via an insecure channel.
- E can either apply active attack, passive attack or a combination of both categories to deal with the readers and the tag.
- In the progress of applying aggression, E can either apply rouge readers or tags in the structures to spoof/masquerade as the appropriate readers and tags.

[6] also compares the computational cost with other similar proposals by [7–14] using MIRACL [6] which is a C software library that is widely accepted as standard open-source SDK for elliptic curve cryptography (ECC), also used by [15] (which is not related to RFID in vehicular communication but compares different cryptographic approaches for RFID).

2.2 Rationale for a standard testbed/testing framework

While going through all the works discussed above, we notice that there is no standard testing framework. [redacted] of any such proposal at the industrial or consumer level.

3 OBJECTIVES

The objectives of our work in 3.5 years would be -

(1) [redacted]
(2) [redacted]
(3) Analysis of an RFID use case in the context of automotive manufacturing.
(4) [redacted]
(5) [redacted].
(6) Assessment for a combination of software and network attack vectors.
(7) [redacted]

4 HOW MY EXPERIENCE CAN CONTRIBUTE IN OUR OBJECTIVE?

I've been working on security research with my professor and guide Dr Shishir Kumar Shandilya for the past 3 years (specifically on nature-inspired cybersecurity and adaptive defence for the past 2 years) and learning all about academic research and its standard procedures.

Keeping the above goals in mind, I've categorised my experience that matches the specific objective-

(1) Our recent research on "AI-assisted Computer Network Operations testbed for NICS" is published in Future Generation Computer Systems with IF of 7.187, We've designed a testbed for testing and comparing Nature-Inspired Algorithms for network defence and optimisation. The testbed has a support automated network structure generation which can also be defined by the user and an API for attaching the user's

[6] https://github.com/miracl/MIRACL

NICS algorithm to test it for defensive operations. We have also registered for a copyright for the same as "NICS-based Network Testbed for Adaptive Defense Analysis" under the registration number "23470/2021-CO/SW". This experience will help us in completing our first objective of "Development of a tailor-made novel testbed for accelerated prototyping and testing."

(2) Our work on "PACE: Platform for Android Malware Classification and Performance Evaluation" [7] won the "best paper award"[8] at IEEE BigData Conference 2019.
PACE and "PACER: Platform for Android Malware Classification, Performance Evaluation and Threat Reporting"[9], a natural development of former, were our attempts to create a standard platform to accommodate all researches in machine learning-based malware detection and classification to aid in research reproducibility and comparison, which was well received and appreciated by the community.
The objective of "development of a model-based security testing framework for RFID" can benefit from the skills gained during the creation of a standard platform for ML models and malware detection.

(3) When we were preparing the application for our patent on hardware-based adaptive security device called "A scanning device, a system and a method for characterization of external devices" [10] which got granted on 16th of June, 2021; I learned a lot about prototyping, pre-production testing and the whole legal process of the patent application. During the process of prototyping, we also covered a lot of edge-case testing and looked into different domains of software and hardware validation required as per the government's official guidelines for a patent application.
Our another Australian patent filed on 20 August 2021 named "Nature-inspired adaptive defence system for early intrusion detection" (20211006268) is a natural extension of our recent research with a similar name. The experience of prototyping and testing can help us in smoother completion of our objective of "Exploration of test input domain, test case generation and coverage analysis"

(4) When working for Renault-Nissin-Mitsubishi (RNTBCI) as a Research Intern in the summer of 2020 on the general topic of "autonomous vehicle security" I was fortunate enough to learn more about vehicular networks and communication strategies like V2V, V2I and V2X making me wonder about their security and performance constraints. During that time, we worked on the project of "communication security in autonomous vehicles" by looking for solutions and optimization techniques in nature-inspired algorithms and ideas. We've also covered concepts of attack trees and threat evaluation which can come in handy in understanding the current state of RFID security and model-based security concepts.

(5) At my current internship as a Security Research Intern (SRI) in Uptycs, a cloud and endpoint security company, we are researching endpoint security and threat analysis. As an SRI my job here is to do malware analysis, threat detection and researching optimisation techniques for malware detection for enterprise endpoints. Where we classify malware families and design optimisation strategies specific to the malware family's attack signature, along with analysing different attack vectors registered in the global threat intelligence database.
I can see the things I am learning here being used in my future researches in threat modelling, exploration of test input domain, test case generation, coverage analysis and assessment of software and network attack/threat vectors.

(6) My final year capstone project is strategically selected to help me focus and work more on RFID security, the proposed research-oriented project titled "RFID++: Testing existing security of RFID cards for next-gen authentication systems" aims to dive deep into the requirements of current RFID applications, their needs and constraints while trying to understand limitations of existing proposals and identifying the research

[redacted]

gaps in the field if any which can give us a head start in our objective of "Analysis of an RFID use case in the context of automotive manufacturing." as we can use some results and data from the capstone project.

(7) Recently I also wrote an invited chapter on "Nature-inspired malware anomaly detection in android-based systems" for the forthcoming book "Advances in Nature-inspired Cyber Security and Resilience" which is accepted for publication by Springer and is under the final stretch of publication. During this time, I learned how to organise vast information under a given word limit. This was also my first single-author academic publication, which was a great opportunity to put everything that I've observed so far into action.

(8) Recently I also wrote an invited chapter on "Nature-inspired malware anomaly detection in android-based systems" for the forthcoming book "Advances in Nature-inspired Cyber Security and Resilience" which is accepted for publication by Springer and is under the final stretch of publication. During this time, I learned how to organise vast information under a given word limit. This was also my first single-author academic publication, which was a great opportunity to put everything that I've observed so far into action.
My existing experience in academic research presentation and the one I will gain during my time in the program will make it easier for us to complete our objective of compiling a well-structured Thesis by the end of the program.

. Some of my major works are:

- **Papers:**

(1) AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis[16]
(2) Nature-inspired malware anomaly detection in android-based systems (Chapter Accepted, in pre-publication)
(3) PACE: Platform for Android Malware Classification and Performance Evaluation[17]
(4) PACER: Platform for Android Malware Classification, Performance Evaluation and Threat Reporting[18]
(5) Modified Firefly Optimization Algorithm-based IDS for Nature-Inspired Cybersecurity (Under Review)

- **Patents:**

(1) A scanning device, a system and a method for characterization of external devices.[19]
(2) Nature inspired adaptive Defense system for early intrusion detection (in processing) [11]

- **Copyrights:**

(1) NICS-based Network Testbed for Adaptive Defense Analysis[12]
(2) PAMC: Platform for Android Malware Classification

[11] Patent Number: 20211006268
[12] 23470/2021-CO/SW

5 PROPOSED TIMELINE

After understanding the expectations of both universities from their potential candidate in this cotutelle program and the premise of this association, I can visualise my contribution as follows-

5.1 Objective-wise work plan for 3.5 years

The total program time of three and half years can be divided into a set of 7 terms of 6 months each (half a year). Given below is my visualisation of the terms based on the objectives discussed above.[13]

5.1.1 ***Understanding current state of RFID security and model-based security concepts.***

Initially, we would need to understand the latest advancements in RFID security and recently proposed model-based security concepts. This can be performed by using attack trees and process algebra.

Expected Outcomes:

- A comprehensive and comparative review paper of existing models and concepts.
- Potential Improved security model

5.1.2 ***Exploration of test input domain, test case generation and coverage analysis***.

This endeavour is more practical in nature, after identifying and understanding the use-case of RFID, we can use our recent models to explore edge cases.

Expected Outcomes:

- 1. Possible Poster
- 2. Research data/results.

5.1.3 ***Analysis of an RFID use case in the context of automotive manufacturing.***

In this, we can take case studies and yearly reports from automotive companies to understand their needs and pitfalls. We can also conduct an industry level survey to better understand the implementation of RFID in manufacturing. Then we can choose the most optimal/common "use case" and analyse it for all established and well-known manufacturers.

Expected Outcomes:

- A presentation at DefCon (CHV)
- Conference Paper"

5.1.4 ***Development of a tailor-made novel testbed for accelerated prototyping and testing.***

[redacted]

[13]

Expected Outcomes:

- A paper on Testbed proposal and design
- A paper on Testbed's experiments
- The testbed

5.1.5 ***Development of a model-based security testing framework for RFID.***.

The development of a security testing framework for RFID will also start along with the testbed, enabling us to share the codebase whenever possible.

Expected Outcomes:

- A paper on Framework's proposal
- A paper on our results and comparison
- Talks and Presentations

5.1.6 ***Assessment of a combination of software and network attack vectors.***

As per Deakin's proposal, the emphasis would be on the software-driven security evaluation, and eventually, we would also cover network-based attack vectors.

Expected Outcomes:

- An article on current RFID attack vectors and surface w.r.t automotive industry

5.1.7 [redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

THE EXPECTED TIMELINE FOR THE PROGRAM

The total program time of 3 ½ years can be divided into a set of 7 terms of 6 months each.

Given below is my visualisation of the terms assuming the program will start from June 2022. The start date can be shifted to the actual start date while following the same six-months, seven-term structure.

(First year at Deakin)

[redacted]

(Final ½ year at Deakin)

JUN 2025 - NOV 2025

COMPLETION AND DEFENCE OF FINAL THESIS

Expected Output-

1. Thesis.
2. Dissertation defence.

6 WHY COVENTRY UNIVERSITY?

While searching for opportunities for a graduate research degree program in the domain of cybersecurity, I came across two interesting projects:

- Model-based Security Testing for RFIDs in Automotive[14]
- Model-based security testing for Automotive Systems[15]

They sound like a great chance for me to explore more in the domain of cybersecurity with a practical approach and learning more about two of the most interesting topics- vehicular communication and the future of RFID's security and privacy. Given Coventry's reputation in research and its industry ties, it looks like an excellent place to get exposure to significant academic research and see its implementation in the industry in real-time.

Apart from academic interests, I want to experience life in major cities out of India and meet like-minded people around the world, Coventry is just that.

Coventry's campuses' proximity to cities like London and Birmingham is exactly where I see myself in near future.

7 KEY PUBLICATIONS

Some significant journals and conferences in the field.

(1) Future Intelligent Vehicular Technologies[20]
(2) Security Assessment in Vehicular Networks[21]
(3) [redacted] (IF: 7) [22]
(4) Vehicular Communications (IF: 7) [23]
(5) [redacted]
(6) [redacted]
(7) [redacted]
(8) [redacted]
(9) CAR HACKING VILLAGE DefCon [28]

[redacted]

REFERENCES

[redacted]