1 PPIDR: Privacy Preserving Intrusion Detection and Response

The use of wireless communications has had tremendous expansion in recent years, mainly due to the evolution of mobile wireless networking and computing devices. Wireless communication technologies such as wireless ad hoc networks, WSN (Wireless Sensor Networks) and RFID (Radio Frequency Identification) systems are increasingly deployed in supply chain management, environmental monitoring, smart home appliances, military surveillance as well as medicine and healthcare applications. Nevertheless, this cascade of wireless communications comes with both impressive advantages and serious threats. The poor physical protection, dynamic deployment, as well as the power and communication constraints of such systems, make them vulnerable to a broad range of attacks and threats against privacy. For this reason the development of efficient safeguarding mechanisms that guarantee the reliability and quality of service in information and communication networks is of utmost importance.

The main goal of the PPIDR (Privacy Preserving Intrusion Detection and Response in Wireless Communications) was the development of intrusion detection and response (IDR) techniques that strike an optimal balance between the promptness of warnings, the reliability of detection and the network performance.

I have investigated how to properly use classification methods in intrusion detection for wireless mobile networks (i.e. Manets). In order to do so I investigated: (i)Firstly, how simple classification versus cost-sensitive classification affects performance, both in terms of classification error (CE) and in terms of weighted error (expected cost) (WCE). (ii) Additionally, I investigated how hyper-parameter tuning affects performance when new unknown attacks are included in the test dataset.

I have also investigated thoroughly the problem of RFID authentication which is very closely related to the intrusion detection and response problem since both of them are decision making problems. More precisely, in the intrusion detection and response problem often we are not sure if nodes that participate in a network are malicious or honest and we need to take a decision about the optimal response that strikes an optimal balance between reducing the cost of potential threats and maximising the network performance. Similarly, authentication is an important decision making problem where we need to decide whether we need to accept the credentials of an identity-carrying entity.

For instance, recent cars have embedded RFID readers and car keys have embedded RFID chips (tags). In such a scenario, the car key has to be close enough to the car in order to unlock it. However, an attacker can perform a type of attack, called *relay*, and unlock the car even if the car key is very far away. These attacks have also been launched against bankcards. The main countermeasure against these attacks is a special type of authentication protocols called *distance bounding* protocols.

I have analysed the security of existing distance bounding protocols, described attacks that can be launched against them and proposed new ones that do not suffer from the identified vulnerabilities. Additionally, I investigated how it is possible to formalise and analyse distance bounding protocols in the context of provable security, something that has not been done before.

An important problem is keeping the location of a prover (i.e. someone carrying an RFID tag) that participates in a distance bounding protocol *private*. I proved that it is theoretically impossible to achieve location privacy for powerful adversaries. However, I showed that for limited adversaries carefully chosen parameters allow computationally provable secure location privacy.

Additionally, I have investigated the weaknesses of an existing Gen-2 authentication protocol and the vulnerability of a class of RFID authentication protocols in traceability attacks.

Authentication can be seen as a decision making problem where we need to decide, whether to authenticate someone or not. In some authentication protocols this decision is harder since they are performed under noisy conditions. This means that not only an attacker but also a legitimate user may give erroneous responses to the received challenges due to the noise. For this class of protocols I have performed an analysis of the expected loss when authenticating an attacker and the expected loss when legitimate users are not authenticated.

Another important decision making problem is how to respond if an attack is detected. Often we are not sure if a suspicious node (i.e. computer or wireless device) of a network is malicious or honest. Thus, we need to decide either to remove the node right away or keep it in the network in order to gather more information and reduce our uncertainty. I proposed a decision-theoretic intrusion response algorithm that has near optimal performance.

1.1 Impact of the research project

The PPIDR is highly connected with maintaining and guaranteeing the quality of communication in RFID systems and WSNs taking into consideration that it is important not to violate the privacy rights of the

involved parties (such as their location). Thus, the conduction of this research can definitely contribute to the European excellence and competitiveness in the following sectors:

- **Information and Communication Technologies (ICTs):** WSN and RFID systems are part of the ICTs. Our research aims to detect and prevent possible attacks and take decisions regarding the appropriate response to these attacks, in order to guarantee the quality of service and performance of the network. Thus, our research will contribute substantially in safeguarding the stability and security of the network as well as the reliability of the involved systems. Our goals perfectly fit with the priorities identified by the European Commission (EC) as key research areas for ICTs.
- **Health:** WSN and RFIDs are already used in healthcare applications either for monitoring the condition of patients (i.e. blood pressure, glucose, levels, cardiac distress, etc.) or for collecting data that can be used to help diagnosis or by improving elderly healthcare. Conducting research in possible methodologies that safeguard and guarantee the reliability of WSN and RFID communication, can only have a positive impact in healthcare applications based on these technologies.
- **Transport:** RFID systems are extensively used in public transport systems (i.e. OV-chipkaart (Nether- lands), Oyster card (UK)). Recent attacks against the OV-chipkaart have created great concerns about the Dutch transport system. Preventing relay attacks (one of the most serious threats against these systems), detecting and responding against possible attacks in these systems is a significant step towards the EC's vision for secure and reliable transport systems.
- **Industry:** WSNs and RFID systems are extensively being used in supply chain management and industry for inventory control, product and asset monitoring. Their application in industry has contributed considerably in improving services, reducing labour cost, increasing productivity, maintaining quality of standards and thwarting product counterfeiting. Our proposal focuses on improving the reliability of these technologies. Such a research can only have a positive impact in industry related applications of WSNs and RFIDs.
- **Other sectors:** WSNs and RFID have a broad range of critical applications including, e-passports, highway toll collection, monitoring the condition of perishable products, traffic, border, space and environmental monitoring. All of these applications are strongly connected with enhancing European security, improving the food and agriculture sector, monitoring the environmental changes and advancing space-observation tools. Guaranteeing the reliability of technologies used in such critical applications is of high importance.
- **Privacy-preservation:** Ubiquitous computing technologies have a lot of advantages, as well as deleterious side-effects. The latter includes the newly created ability to collect private information pervasively, silently and cheaply. Thus, all proposed mechanisms that focus on safeguarding the reliability of these technologies should also provide privacy guarantees. One of the main goals of our research is to achieve efficient and reliable communication in wireless technologies, while protecting the privacy rights of the involved parties.

The url address of the project is: `http://lasecwww.epfl.ch/~katerina/ppidr.html`
Contact details: Dr. Aikaterini Mitrokotsa (`mitrokatkm@gmail.com`)