University of Amsterdam

Research Project I proposal

Protecting against relay attacks

Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

January 7, 2015

Contents

1 Introduction

As technology progresses, many traditional devices are improved with wireless features, aimed to improve user's comfort. Examples of these improvements can be found in access control (car keys, company IDs, public transportation cards) or credit card payment systems, among others.

Most of these systems are vulnerable to relay attacks, in which an attacker simply forwards messages between parties. These are specially dangerous in some cases, as they can provide unauthorized access even if the communication is fully encrypted and protected. A typical and well-documented example of this kind of attack are cars with PKES, in which an attacker can get into a victim's car by relaying the transmission between the car and the key at a longer distance than it is supposed to work. Some non-wireless platforms and services are also vulnerable to this kind of attacks, although they tend to be more difficult to perform.

This project will attempt to provide recommendations on how to make those systems more secure, either by making the systems less predictable or by proposing features that can block partially or totally some of the attacks.

2 Related Work

There are many research project studying relay attacks on different services and applications, such as [1, 2]. There is large number of systems vulnerable to these attacks, and due the limited time available for this project we will have to focus on some of them, aiming for the most relevant and/or commonly used.

Another interesting source of information will be available studies on how location systems can be secured, as in [3]. Using this as an starting point we will attempt to provide practical solutions to the presented problems.

3 Project Scope and Approach

As stated in the Related Work section, there are a lot of real world utilities that are vulnerable to relay attacks. There are extreme variations on the limitations and conditions of these systems, meaning that a single solution will most probably not fit all of them. The scope of the project might vary depending on the time restrictions and how fast the progression is.

This project will be a theoretical approach on how to fix these issues. Although practical experiments would definitely be useful, time is the heaviest constrain and it is infeasible to acquire or develop the platforms to test the proposed solutions on the field. However, this would surely be an interesting future work.

4 Research Questions

The basic question this project aims to answer is:

Can vulnerable applications be successfully secured against relay attacks?

This question will most likely not have a binary answer. We expect that some systems will be easier to secure than others. Some might have conditions that enable perfect solution against relay attacks. However, we expect that most of them will only achieve a higher degree of security, but will still not be completely secure.

We will select one -or various- of the most interesting study cases and try to answer that question for each specific case.

5 Planning

This project will run over the course of five weeks. First week is intended to be dedicated to researching previous related work and defining the project scope. Second and third week are designated for the project development. Fourth week will be used to write the documentation and prepare the presentation. Lastly, the presentation and project defence will be done on the fifth week.

6 Expected results

The project will start providing a brief explanation of what kind of platforms we want to study. From that list we will select those we consider to be the most relevant study cases, and attempt to provide an insight on how their security against relay attacks could be improved.

7 Ethical considerations

The project will be a theoretical study that will not be using any kind of user data, and solutions provided will be based upon theoretical models. This means we will not be running into any kind of ethical issues.

References

[1] A. Francillon, B. Danev, S. Capkun, *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*

[2] J. van den Breekel, *A Security Evaluation and Proof-of-Concept Relay Attack on Dutch EMV Contactless Transactions*, October 2014

[3] S. Capkun, J. Hubaux, *Secure Positioning in Wireless Networks*