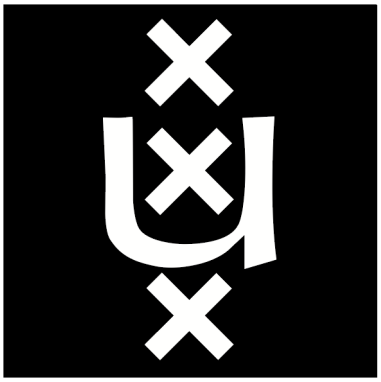
University of Amsterdam

Research Project I

Protecting against relay attacks forging increased distance reports



Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

January 22, 2015

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sed diam metus. Quisque velit urna, dictum vel eros eu, congue luctus augue. Nulla sit amet metus nec ipsum pretium vestibulum ut quis sem. Nullam malesuada risus ut rhoncus consequat. Fusce in hendrerit nibh. Morbi a magna nunc. In vel justo tincidunt, porttitor tellus in, porta lacus. Nulla posuere enim arcu, eget aliquet mauris dictum ornare. Morbi iaculis nec elit vitae rutrum. Nam posuere, risus sed semper finibus, augue lorem blandit ex, non tempor nunc tortor vel arcu. Cras non tortor ipsum. Suspendisse vestibulum molestie nibh, lacinia efficitur nunc luctus non. Phasellus sed nibh at est suscipit pulvinar. Cras eleifend ante et volutpat suscipit.

1 Introduction

Communications between machines face many challenges when the transmitted information needs to be protected. Most communications can prove to be valuable attack points for third parties that want to recover, modify, block or otherwise manipulate the original message sent for personal profit. Part of these attacks can be prevented by using end to end encryption and signature of the data. However relay attacks cannot be prevented just by using cryptographic algorithms.

Relay attacks consist on the mere reception and replay of information. Although at first this might seem harmless, many systems become vulnerable if that relaying of information is not noticed. One scenario that can be used as an example of the threat these attacks represent are access control systems, in which a device is used to prove that a user is within a certain distance from a validator through a challenge-response protocol. On unprotected implementations of these access control systems, an attacker can relay the challenge from the validator to a valid user who is not in range and relay its answer back to the validator, effectively bypassing distance validation. Practical attacks on this kind of systems have been demonstrated on various studies, as in [3, 4, 5, 9].

In this paper, we will first discuss the relay attacks used to forge fake location positions, focusing on the countermeasures against them. We will then focus on attacks forging increased distance reports, the feasibility of these attacks and propose solutions to them. In Section 2 we will discuss the available literature on this topic. We will present on Section 3 a more detailed explanation on the research questions this project aims to answer. Following on Section 4 we will explain the methodology used in this study. In Section 5 we will briefly present results and conclusions from our research in distance bounding protocols and GPS: Sections 6 and 7 will discuss the actual results from our research questions, after which we will provide conclusions about the results gathered in Section 7.

2 Related Work

Relay attacks have been for long, and continue to be, an extensive field of research, as technologies and devices are shifting to a more mobile-focused paradigm. Many old procedures are being enhanced with wireless features, such as credit cards and car keys.

There are many papers available presenting solutions to distance bounding problems, as [1, 11, 10]. All of these studies are used as a base for others in a constant iteration to improve the protocols. Practical studies in this field tend to test the vulnerabilities on real applications, such as [3, 4, 5, 9, 2]. Although all that research refers to forging decreased distance reports, it has been deeply useful to our research as an starting point and inspiration.

Later on, we will require to make some assumptions and justifications on our investigation based on the characteristics of GPS signals. Many studies focus on the feasibility of intentional attacks against GPS systems, as [12, 13,

7]. These studies conclude that, even though spoofing is hard with the solutions they propose, it is not impossible.

This study is closely related to the field of MANETs (Mobile Ad-hoc NETworks), and as such, literature available in this topic is of our interest. In particular, wormhole attacks ([6, 8]) are a specific type of relay attack that, while being different than the ones we will study in this document, provide insight to our investigation as they are closely related.

3 Research Questions

The initial proposal of this project was strongly related to relay attacks on contactless credit cards and automatic car key entry systems. Improving the proposed systems on the work done by Brands and Chaum on [1] and Rasmussen and Capkun on [10] seemed infeasible for a two week project. Automatic car key entry systems can already be solved by correctly implementing the protocols on these papers, while credit cards require additional hardware performing those operations to be secure.

Ultimately, this project aims to answer the following questions:

How feasible are forged increased distance report attacks?

How can we fight these attacks?

3.1 Feasibility of forged increased distance report attacks

Minimum distance bounding appeared to have many solutions on the current literature. However, we observed that distance bounding regarding upper limits on reported distances was not a subject of research. In this project, we will present some theoretical attacks that could be used on many real world scenarios, and propose variations on the current distance bounding protocols to solve them.

The proposed scenarios are diverse in both context and properties of the systems involved in the communications. We will focus the study from the point of view of systems involving communication between drones, although we will provide solutions that can be extrapolated to other systems as well, such as automatically driven cars.

In this research question, we ultimately aim to explain why these attacks can be dangerous and an interesting topic of research.

3.2 Fighting forged increased distance reports

The second research question will focus on providing solutions to the issues stated on the first. Unlike minimum distance bounding protocols, we won't be able to use the speed of light as a fact to develop responses that cannot be faked, which implies that we might not be able to develop a system that

completely protects against these increased distance reports. However, we do expect to provide solutions that suppose a meaningful security increase against these attacks.

4 Methodology

This project is a theoretical research on a proposed problem. Most of the work will be based on the research and exploration of the current literature on topics related to our research questions. By contrasting information on these sources, we will develop solutions based on modifications of the current systems and protocols.

There will be no practical exploration on the issues, as that kind of study is out of our research scope.

5 Distance bounding and GPS

Introduction to distance bounding. Explain available methods and why radiofrequency is the most reliable method. [at least 1 paragraph for each one. 2 or 3 for radiofrequency]

- Signal intensity
- Ultrasound
- Radiofrequency (extended explanation on this one as it is the focus of our research)

Explain why faking decreased distance reports is not feasible but faking increased reports is (on our study case). [1 paragraph]

Explain why increasing the reported distance between two parties can be a problem. [1-3 paragraphs]

Talk about other systems that are used for location (GPS, RADAR) and justify how we use them. [1 or 2 paragraphs for each one]

6 Feasibility of forged increased distance report attacks

Answer the first research question.

Explain the theoretical attack case. Introduce and notice its difficulties as a practical attack. [1-2 paragraphs]

Explain the assumptions made [1 paragraph] Feasibility of the jamming and relaying ...?

Present diverse attack scenarios. [at least 1 paragraph per case] Drones (multiple cases) Cooperative working Area surveillance Automatically driven cars Boats and harbours ...? For each case, state clearly the assumptions made and its limitations

7 Fighting forged increased distance reports

Present the solutions

Multiple antenas and shared knowledge [Various paragraphs (5+), this is the first solution]

8 Conclusions

Consider the theoretical assumptions of the project [1 paragraph]

Given the proposed solutions, introduce and explain the implications [2 or more paragraphs]

9 Future Work

Briefly talk about the need of a more practical study with real hardware [1 paragraph]

...?

10 Acknowledgements

[2 paragraphs max]

References

[1] Stefan Brands and David Chaum. "Distance-bounding protocols". In: *Advances in CryptologyEUROCRYPT93*. Springer. 1994, pp. 344–359.

[2] Jordi van den Breekel. "A Security Evaluation and Proof-of-Concept Relay Attack on Dutch EMV Contactless Transactions". In: (2014).

[3] Aurélien Francillon et al. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." In: *NDSS*. 2011.

[4] Lishoy Francis et al. "Practical NFC peer-to-peer relay attack using mobile phones". In: *Radio Frequency Identification: Security and Privacy Issues*. Springer, 2010, pp. 35–49.

[5] Gerhard P Hancke. "A practical relay attack on ISO 14443 proximity cards". In: *Technical report, University of Cambridge Computer Laboratory* (2005), pp. 1–13.

[6] Yih-Chun Hu, Adrian Perrig, and David B Johnson. "Wormhole attacks in wireless networks". In: *Selected Areas in Communications, IEEE Journal on* 24.2 (2006), pp. 370–380.

[7] Ali Jafarnia-Jahromi et al. "GPS vulnerability to spoofing threats and a review of antispoofing techniques". In: *International Journal of Navigation and Observation* 2012 (2012).

[8] Ritesh Maheshwari, Jie Gao, and Samir R Das. "Detecting wormhole attacks in wireless networks using connectivity information". In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE. 2007, pp. 107–115.

[9] Konstantinos Markantonakis. "Practical relay attack on contactless transactions by using nfc mobile phones". In: *Radio Frequency Identification System Security: RFIDsec* 12 (2012), p. 21.

[10] Kasper Bonne Rasmussen and Srdjan Capkun. "Realization of RF Distance Bounding." In: *USENIX Security Symposium*. 2010, pp. 389–402.

[11] Yu-Ju Tu and Selwyn Piramuthu. "RFID distance bounding protocols". In: *First International EURASIP Workshop on RFID Technology*. 2007, pp. 67–68.

[12] Jon S Warner and Roger G Johnston. "GPS spoofing countermeasures". In: *Homeland Security Journal* (2003).

[13] Hengqing Wen et al. "Countermeasures for GPS signal spoofing". In: *ION GNSS*. 2005, pp. 13–16.

** bibliography goes here **
** appendix goes here **