Network Security Research Proposal

Will Laurance

October 2, 2011

Contents

1 Problems Addressed

This paper will address the security issues associated with NFC, near field communication. Problems include but not limited to eaves dropping, man in the middle attacks, data modification, relay attacks, and physical loss of NFC devices.

2 Motivation

The motivation behind this research is to design a secure protocol for NFC devices and their receiver counterparts. The secure channel will need to satisfy PCI standards to provide secure financial transactions. Limitations of hardware will factor into the design of this protocol.

3 Related Work

Related work includes but not limited an implementation of said secure protocol.

4 Methodology

1. Testing environment will simulate payment transactions using NFC sender and reciever devices. Record wireless traffic with a sniffer tag.
2. Attempt to jam signal between sender and receiver with RFID jammer.
3. Use software tools from Mulliner's Python library to send, receive, and analysis traffic.

5 Resources

1. NFC Device
2. NFC Receiver
3. Linux Box
4. RFID Jammer
5. RF sniffer
6. Collin Mulliner's Python NDEF library and tools.

6 Milestones

1. Research current works concerning NFC.
2. Testing Environment setup - to include setup of RF sniffer, NFC devices (receiver and sender).
3. Analyze current transmissions and study for vulnerabilities.

4. Attempt various attacks on NFC transmissions.
5. Design protocol to prevent against attacks
6. Implement protocol
   (a) Fully documented code
   (b) Test Suite
   (c) API Java and Python Implementations
7. Test implementation against attacks
   (a) Run test suite against implementation
   (b) Adjust implementation appropriately
8. Conclusion - Identify the strengths and weaknesses of protocol and indicate areas that require improvement.

7 Schedule

1. **October 17, 2011**. Complete current research study. Have all materials necessary to setup testing environment.
2. **October 28, 2011**. Complete testing environment setup and have preliminary analysis started.
3. **November 16, 2011**. Study vulnerabilities and attempt various attacks. Brainstorm techniques to combat these attacks using my knowledge of cryptology, hardware, and software. Begin outline of final report.
4. Complete protocol design
   (a) **November 20, 2011**. Identify all sections of outline and begin adding details.
   (b) **November 25, 2011**. Add more details to outline.
   (c) **November 30, 2011**. Complete documentation of protocol.

8 Future Work

1. If time does not allow, implement protocol at a later date.
2. Continue research of NFC devices, related hardware, algorithms, and cryptology related to NFC.
3. Prospect the economics, business, and social aspects of NFC.