18-732: Secure Software Systems

Lecture 1

A Taxonomy of Vulnerabilities Against Differential GPS

David Brumley
Scribed by: Brady Tello, Evan Tobac, Chase Midler

November 23, 2011

1 Introduction

2 Differential GPS

3 RTCM and Ntrip

The Radio Technical Commission for Maritime Services (RTCM) is a non-profit organization comprised of both government and non-government bodies that is heavily involved in publishing standards related to several topics including differential GNSS. RTCMs Special Committee 104 publishes two standards which we focused on in our research.

First we will discuss the RTCM 10403.1 standard (Differential GNSS Services Version 3). The 10403.1 standard defines a set of messages which contain the data required by Differential GNSS capable receivers. The data defined by this standard is commonly referred to as just RTCM, RTCM-104, or RTCMv3. From this point on, we will refer to the data standard as RTCM unless it would be ambiguous in which case we will refer the the standard by its full name.

// TODO Put a table here that shows an example of an RTCM message and a blurb pointing to it in the previous paragraph

The second standard of interest is known as Ntrip (Networked Transport of RTCM over Internet Protocol) which is also published by the RTCM Special Committee 104. Ntrip is an application layer networking protocol designed to stream RTCM correction data over the Internet. A feature of Ntrip that seems to be popular is that it can transmit corrections over cellular data networks such as GPRS and EDGE, thus allowing corrections to be downloaded in very remote locations. After conducting a survey of commercial GNSS devices and conducting brief interviews with sources close to the development of Ntrip we have come to the conclusion that most commercial GNSS reference stations are equipped with the capability to transmit RTCM correction data over Ntrip. Furthermore, it has a wide variety of use cases which will be discussed in // TODO SECTION NUMBER. The technical details of the protocol are contained in the following paragraphs.

The primary objective of the Ntrip protocol is to transmit correction data from reference stations to receivers over the Internet. Its architecture is similar to that of a streaming Internet radio

service. When a GNSS receiver wants to listen to a correction stream from a reference station, it requests the stream from a broadcast source which delivers the stream to the receiver in real time. In Ntrip terminology a reference station is known as an Ntrip Source, a receiver is known as an Ntrip Client ,and a broadcaster is known as an Ntrip Caster. An additional component known as an Ntrip server acts as a middle man between sources and casters. The server aggregates data streams coming from sources and delivers them to casters which in turn aggregate several servers.

// TODO Insert picture of the Ntrip architecture here. Its saved in your dropbox

The standard is relatively abstract in its definitions of these components so it is helpful to understand how these components might be implemented in a real Ntrip network. Ntrip sources are implemented in GNSS reference stations such as the Trimble NetRS. The device generates RTCM data and is uploaded to a server using one of several communications interfaces such as serial, TCP/IP, or various others (the Ntrip standard actually doesnt define a communication interface between sources and servers). An Ntrip server and an Ntrip caster would be a traditional software package installed on one or more desktop/laptop computer(s). Although they are defined as two logically separate entities, the server and caster program can be implemented as part of the same program and still conform to the specification [Brady2]. A client is a piece of software at the receiver which is trying to correct its position. The Ntrip client downloads corrections and hands them off to the GNSS software which then applies them to an uncorrected position calculation in order to get a corrected position.

The reason we have decided to focus our efforts on Ntrip and RTCM is because of their non-proprietary nature. The two are not the only protocols available for encoding and disseminating differential correction data but they are certainly widely implemented and open to public use (for a small fee). Knowing that all differential GNSS packages adhere to the same physical principles, we assume that they would be vulnerable in similar ways but this question is left for future work.

4 Applications

NDGPS Assessment report has tons of applications [Brady4]

5 Attack Taxonomy

- Attacks on Casters (man in the middle) Casters are the backbone of the Ntrip network. Worldwide, there are about 140 documented NTCasters[Brady3]. We have reason to believe that the number is actually much greater than that since we were able to find two more private casters with a couple of user interviews.

- Man in the Middle with GPRS, EDGE Rogue Base Station - Location Privacy Concerns for the clients. Read Section 2.1.3 of the Ntrip 2 standard - Cracking authentication. Look at the Digest Authentication and caster management sections of the Ntrip 2 standard

6 An Attack on a Real Time Kinematics Engine

7 Scope of Impact

8 Future Work

Investigate how networks average error Investigate other DGPS protocols Run our attack on a real RTK receiver (not rtklib) and see if we get similar results

9 Thanks

Dr. Georg Weber for providing helpful links and commentary on the adoption of Ntrip in geodetic equipment. Jeff Jalbrzikowski for providing valuable guidance regarding real life applications of Differential GPS and GNSS in the context of Surveying. Tyler Nyswander for sharing his efforts in gaining root access to the NetRS device.