ANALYSIS OF SDR TO DETECT LONG RANGE RFID BADGE CLONERS

A Thesis
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Brett Knecht

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Computer Science
Option: Cybersecurity

July 2020

Fargo, North Dakota

North Dakota State University
Graduate School

Title

ANALYSIS OF SDR TO DETECT LONG RANGE RFID BADGE CLONERS

By

Brett Knecht

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Jeremy Straub
Chair

Kendall Nygard

Benjamin Braaten

Approved:

July 30, 2020
Date

Kendall Nygard
Department Chair

ABSTRACT

This thesis proposes a way of detecting when radio frequency identification (RFID) badge credentials are being captured through the use of software defined radio (SDR). A method for using SDR to detect when badge cloning technologies are in use on the premises is presented, tested, and analyzed. This Thesis presents an overview of the problem with badge systems and a background literature review. Next, the proposed method of detection and its workings are presented. Then, the strategy for evaluating the methods performance. This is discussed by discussion and evaluation of the results. Finally, the thesis concludes with a discussion of the method's potential benefits and proposed future work.

ACKNOWLEDGEMENTS

I would like to thank Tim Jensen, a Senior Penetration Tester who works for BSI, a large multinational cybersecurity company, for all his help with idea formation for this thesis as well as providing a long-range badge cloning device to test with. I would also like to thank Dr. Jeremy Straub, my advisor and professor at North Dakota State University, for his help through the writing process and for providing the SDR equipment to conduct this testing with.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

1. INTRODUCTION

Many businesses and other organizations use radio frequency identification (RFID) systems, such as proximity cards and fobs, to control access to areas of their facilities. Others use small tags to track products in their supply chains. In some cases, RFID is used by employees to punch in and out for their shifts. The important information and permissions that these RFID badges grant make them valuable targets for those trying to gain unauthorized access [1]–[3].

One way that unauthorized people make their way into restricted areas is by cloning an authorized badge and passing it off as their own. They obtain the information needed to make a cloned badge through the use of a long-range badge cloner [1], [4]. Long-range badge cloners are devices that get the information from another badge without having to physically contact the badge, making them very difficult to notice.

An example illustrates the problem. One scenario when a long-range RFID badge cloner could be used to gain unauthorized access to a building of a competitor with the intent of stealing a technical breakthrough. This scenario is based on an attack scenario that physical security testing companies commonly present to their clients [5].

A company has recently made a major breakthrough on one of its projects. A competing company is desperate to get their hands on this discovery and hires someone to steal the information from their competitor. This individual must get into a facility secured with access control badges to get the information they are after.

The soon-to-be-thief packs his long-range RFID badge cloner into a backpack or carrying bag and hangs out around the facility that he is trying to gain access to. He might hang out near an entrance door, pretending to be on a break or distracted on his phone, while people pass by to go inside. All the while, the cloner in his backpack is capturing badge information from people

passing by. The thief might also approach an on-site security guard while holding a map and ask for directions as an excuse to get close enough to capture their badge information also.

With this captured information, the thief can create copies of multiple badges. Now all the thief has to do is dress like one of the employees of the company and use one of the cloned badges to walk in and gain access to the technology and steal it without setting off any alarms and possibly without raising any suspicions from employees of the company.

In this scenario, none of the people who had their badge information stolen would have any idea the act was occurring. This type of attack could result in the targeted company loosing large amounts of money, as its competitor can now produce a similar product without similar development time and costs.

An alternate scenario shows how badge cloning could have a major impact on a business in their supply chain integrity. In the commercial fishing industry, for example, shipments of valuable fish are tracked with RFID tags, either in the containers or attached to the fish individually for larger fish [6].

In this scenario, the supply chain procedures of fish markets are the focus. When a shipment of fish is sent to a market, the valuable fish (like tuna) are tagged and tracked through the shipping process [7], [8]. A badge cloning device could be used to clone the tags of these valuable fish and tag less valuable fish with them. The valuable fish could then be stolen, without being noticed, during the shipping process. The theft may not be noticed until the shipment arrives at its final destination, because all of the tags for the shipment are still present.

In this scenario, both the supplier and the market that ordered the fish lose money. The supplier loses money due to the theft and will have to adjust its billing when the market reports

that the shipment is incorrect. The market would lose sales because they lack goods to sell and they will have to wait for the next shipment to get more.

There are many more scenarios under which a badge cloner could be used for nefarious purposes. These uses result in problems ranging from security issues for a facility to even causing a financial crisis.

The purpose of this research is to determine if long range badge cloning devices can be detected through the use of software defined radio (SDR). An SDR is a device used to tune into a radio frequency through the use of software to filter and monitor activity occurring on the frequency [9]–[12].

This thesis begins by presenting information about RFID badge systems, SDR, and long-range RFID badge cloners. This is followed by a proposed method for detecting long-range RFID badge cloning systems. Finally, from using the proposed detection method is presented and analyzed for two test cases. This thesis concludes with a discussion of areas of future work and possible system improvements.

2. BACKGROUND

This thesis is based on three major types of existing systems and how they interact. These systems are the following: RFID badge systems, long range RFID badge cloners, and software defined radio. Understanding how RFID badge systems and RFID badge cloners work is key to understand how SDR can be used to detect long range RFID badge cloners. All of these systems rely on the use of radio waves to conduct their functions. Each of these three technologies is now discussed, followed by a discussion of SDR.

2.1. The Beginning and Evolution of RFID

The RFID technologies used in products today exist in many forms and are a result of decades of development of the technology. The origin of RFID technologies can be traced back to scientific discoveries and advancements regarding the understanding of electromagnetic energy and magnetism in the 1600's through 1800's [13].

There are many milestones in the evolution of RFID technologies, on the way to modern RFID. One of the first came in 1896 when Guglielmo Marconi was the first to transmit radiotelegraphy across the Atlantic Ocean successfully [13]. Other milestones include the development of modern radio communication by Ernst F.W. Alexanderson in 1906, when he developed the first continuous wave radio, which would lead to the development of radar during World War II [13]–[15].

It wasn't until 1948 that RFID, as it is now, was first theorized by Harry Stockman who published a paper entitled "Communication by Means of Reflected Power." In this paper Stockman presented the foundations that would become today's RFID [16]. At the time, RFID was not possible due to the limitations of current technologies. Stockman concluded his paper by saying, "evidently considerable research and development work has to be done before the

remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored" [13], [16].

The 1950s through the 1970s were filled with technological advancements that explored RFID concepts and made steps towards bringing Stockman's theories to fruition. There were continued advancements in radar and the development of aircraft identification systems, and inventors began utilizing concepts of RFID to develop new products [14], [15]. In the 1960s the first use of the RFID tag concept was used commercially as an anti-theft device. These tags were called electronic article surveillance (EAS) and held only 1 bit of data, which is much less than the capabilities of modern RFID tags [13]. Research into RFID continued through the 1970s for various purposes such as animal tracking, vehicle tracking, and factory automation.

In the 1980s and 1990s, RFID really started to become what it is today. RFID tags went through rapid improvements in circuitry and size reductions, which allowed for cheaper production and large-scale manufacturing. RFID technologies were introduced for more purposes, like toll road fee collection and train cargo tracking. This trend of rapid improvements to RFID capabilities has continued until today, where the biggest current limitation of RFID is the size of the antenna required to operate the circuit [14], [17], [18].

2.2. RFID Badge Systems

A common system for controlling access to and logging attendance at a facility is the use of RFID badge systems. These systems are commonly used to track who is entering and leaving a facility, as well as granting access to only those that are permitted to enter. Another use for RFID systems is the use of RFID tags for inventory and supply chain tracking [4], [13].

RFID badge systems are comprised of two primary components, a badge or token that personnel carry and a reader that is usually affixed to the facility. These systems work through

the use of radio frequencies to both power the badge or token and pass information back to the reader.

The readers for these systems contain an antenna which is usually comprised of a coil of copper wire that constantly broadcasts at one frequency, creating an electric near field. A near field is an area of electromagnetic energy that rapidly decreases in strength as distance increases from the source. This near field is what is used to power the badges or token fobs, as they do not have any batteries or power sources of their own. Additionally, the reader waits listening for data from a responding badge or token fob to be validated. When the signal from the RFID device is received by the reader, it is translated into data a computer can understand. After conversion the data is sent to a host computer to be entered into or compared against a database, and a decision of granting or denying access is made.

Both badges and token fobs consist of the same few components. The main difference is their form factor. These devices both contain an antenna that collects energy produced by the reader's near field, when they are brought within range. When held in the field long enough, the badge will collect enough energy to power the microchip contained within it. This microchip sends its stored data back to the reader, using its antenna, expending the energy collected. This process of charging and sending data will repeat continuously while the badge is held within range.

Once enough charge has been collected and data is sent, if the reader is within range and receives it, it will attempt to validate the data. How validation is performed is dependent on how the system is implemented. In more secure implementations, the reader validates the data against a database. In other cases, validation is performed right at the reader against its cached history of known authorized badges.

The frequencies at which a RFID system operates depends on its type. There are three general categories of RFID systems: low frequency, high frequency, and ultra-high frequency. Each of these categories has a unique set of properties. The most common low frequency used is 125 kHz, but low frequency devices can range from 120-140 kHz. They typically have a passive read distance of 10cm to 20cm [4], [19], [20]. High frequency devices use a frequency of 13.56 MHz and have a passive read distance of 10cm to 20cm [3]. Ultra-high devices use frequencies ranging from 868 MHz to 928 MHz and have a passive read distance of over 15 meters [21].

2.3. Long Range RFID Badge Cloners

Long range RFID badge cloners are a threat to RFID badge systems. These cloners give their user the ability to steal a badge or token's information and can make a copy of it without having to physically access the item. These long-range cloners work in a similar way to how the readers of RFID badge systems function. In some cases, a repurposed reader can even be transformed into a long-range cloner. The cloner has an antenna, usually a coil of copper wire, that generates a near field like a normal reader does. These cloners can generate a slightly larger field than a standard reader, through the use of a larger antenna, by supplying additional power.

The biggest difference between a long-range RFID badge cloner and a reader is that when the long-range RFID badge cloner has a badge pass through its field and is sent data, the cloner does not try to validate the data. The data is instead stored to be used later in a replay attack or saved to be used in the production of phony badges. These cloned badges can then be used at any time to gain access to the targeted facility for as long as the original badge has access to it. A replay attack is a technique used where the attacker intercepts information needed to gain access, then re transmits it to gain access.

Unlike readers, cloners are usually not mounted on a wall by a door and powered with a wired connection. These cloners are powered by battery packs, allowing them to be concealed and hidden in things like backpacks or briefcases. By concealing a long-range cloner, a would-be thief can walk by his target without tipping them off that they've had their information stolen. This is a big part of why cloners can be hard to catch and what makes them a major threat to secured facilities.

Although this device has the word cloner in its name, it does not actually conduct the actual cloning. A long range badge cloner only captures the information from the credentials that pass through its field. If a badge or fob is in the cloner's field long enough the cloner may gather enough data from it to allow the attacker to make a cloned badge. This information needs to be ported to a software and hardware system, where the information could then be written to a blank card, in the hope that it will be passable as the real thing.

2.4. Software Defined Radio

Both RFID badge systems and long-range badge cloners operate by sending and receiving radio frequency data. This supports the key premise that SDR can be used to detect badge cloner activity.

Software defined radio leverages computers' flexibility and is a very powerful tool for radio transmission receiving and broadcasting. Many of the components of a standard radio, that are traditionally hardware based, are implemented in software in SDR. This gives SDR its wide range of capabilities [9]–[11], [21], [22]. Functions that typically were hardware based but are now implemented in software in SDR systems include components like mixers, filters, amplifiers, modulators, demodulators, and detectors [12], [21]. Because so much of the functionality of SDR is based in software it can be adjusted for different uses quickly and

inexpensively. This is a big part of the appeal of SDR and why some modern radio systems use it.

There are two primary components to an SDR system. The first part is the hardware portion; a dedicated receiver paired with an antenna. These antennas are typically detachable and swappable allowing a user to select an antenna that is suited to the frequency used. General purpose antennas can be good for beginning users of SDR, but an antenna built for a specific frequency gives a user better control over the data they collect.

The second major component of an SDR system is the software used to control the hardware. There are many different software suites for SDR. Each has its own capabilities. Some software focuses on circuit level design and allow the user to tune their SDR through designing circuits necessary to interpret the received signals. Others focus on visualizing the spectrum, allowing the user to tune their radio by looking at the visualized wavelengths and intensity.

Both parts, the hardware and software components, are required to build a functional SDR system. Choosing the set of components for a project is a key design decision. There are a large number of available options.

3. SYSTEM DESIGN

This section discusses test environment that was used. This environment consists of components for both the simulated attacking device and the proposed defensive system. The HackRF One was the SDR device chosen for use, due to its open-source nature and impressive capabilities. This SDR is paired with an ANT500 antenna and SDR# (SDR Sharp) tuning software, which is used to observe the desired frequency needed for testing. The adversarial long-range cloner being tested against is comprised of a proximity reader connected to a Raspberry Pi 3b+ running the Wiegotcha operating system. A generic RFID badge for the 125 kHz frequency was used to simulate a credential being stolen by the long-range cloner.

3.1. HackRF One paired with ANT500

The HackRF One was designed by Great Scott Gadgets. It is an open-source hardware platform that operates as a USB device or a programable standalone device. It is capable of both transmission and reception of radio signals [23]. This SDR boasts several features that were helpful for testing. These include an operating frequency range of 1 MHz to 6GHz and a sample rate of up to 20 million samples per second [24]. The HackRF One is compatible with a variety of different tuning software applications, due to its open-source nature. It is also powered over a USB connection. This makes it easy to set up and use with any device with the capabilities to run software that can control it and which is equipped with a USB port. Other useful features of the device are the SMA female antenna connector that allows for quick and easy changing of antennas, and software-configurable RX and TX gain and baseband filtering to help filter out static and achieve a clearer picture of the data that is sought.

Although this device advertises its range as being 1 MHz to 6 GHz, it works in ranges outside of this when paired with a proper antenna and capable tuning software. The sample rate

of this device is important for the collection of data for this experiment. With a high sample rate, it is less likely that important data will be missed.

The HackRF One was paired with an ANT500 antenna for the testing done for this thesis. The ANT500 is a 50-ohm general purpose antenna with telescopic capabilities from 20cm to 88cm. It is rated for 75MHz to 1 GHz use [25]. This antenna was chosen because it was the one with the closest frequency range to the one being observed that could be found.

Using this of antenna and software, the 125 kHz range is observable. This allows for the collection of data for this experiment. The configured HackRF One is shown in Figure 1.

Figure 1. SDR: HackRF One with attached ANT500 antenna.

3.2. SDR#

The tuning software chosen to control the HackRF One for this project was SDR# (SDR Sharp). This is a free SDR tuning application created by Youssef Touil [23]. SDR# provides full configurability of SDR devices and a user-friendly interface. It is shown in Figure 2. SDR# has support for plugins, allowing for the customization of the platform to fit a user's needs. With this

platform, users can visually tune their radio and make adjustments as needed while it is running in real time.

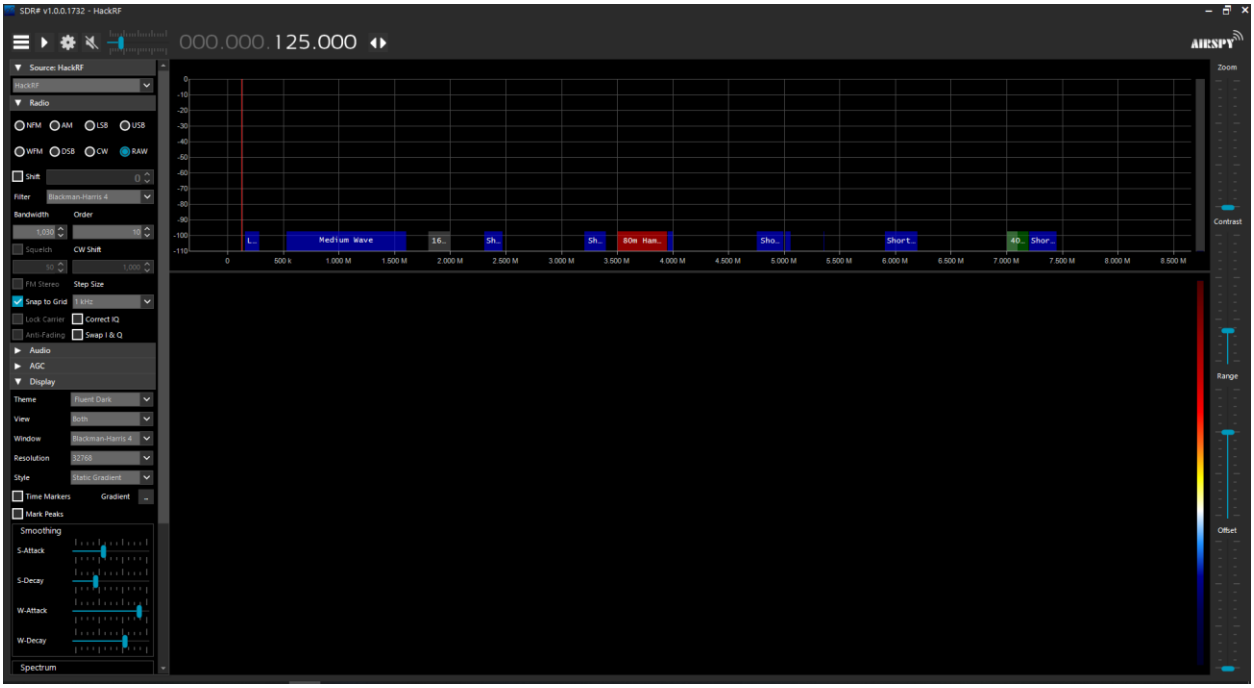

Figure 2. SDR# User Interface.

3.3. Long Range RFID Badge Cloner System

The long-range cloning system is comprised of several components. The first piece of the system is a large HID MaxiProx badge reader. This device measures 11.75’’ x 11.75’’ x 1’’ and is shown in Figure 3. These readers are commonly used for drive up access control security for parking lots and parking ramps with restricted access. They are intended to be able to read a badge or token fob from a user’s car as they drive up. In order to do so, they are a larger than a standard door access reader and generate a larger near field to fulfill this requirement. Because of this increase in reading range, they make for a good long-range RFID badge cloner when adapted.

Figure 3. HID MaxiProx Badge Reader.

Within the readers housing are the factory standard components plus a Raspberry Pi 3b+, as shown in Figure 4. The Raspberry Pi is used in place of the system a badge reader would normally communicate with. This Raspberry Pi runs a special operating system, Wiegotcha, which was made by the user lixmk on GitHub [26]. The Raspberry Pi 3b+ is equipped with a Wi-Fi module and allows for real time monitoring of credentials being grabbed by the cloner when connected to a phone or tablet. Additionally, the cloning system is equipped with a quick connect

power adapter, allowing it to be run from battery or a wired connection. For testing a wired connection was used for reliability and consistency between tests.

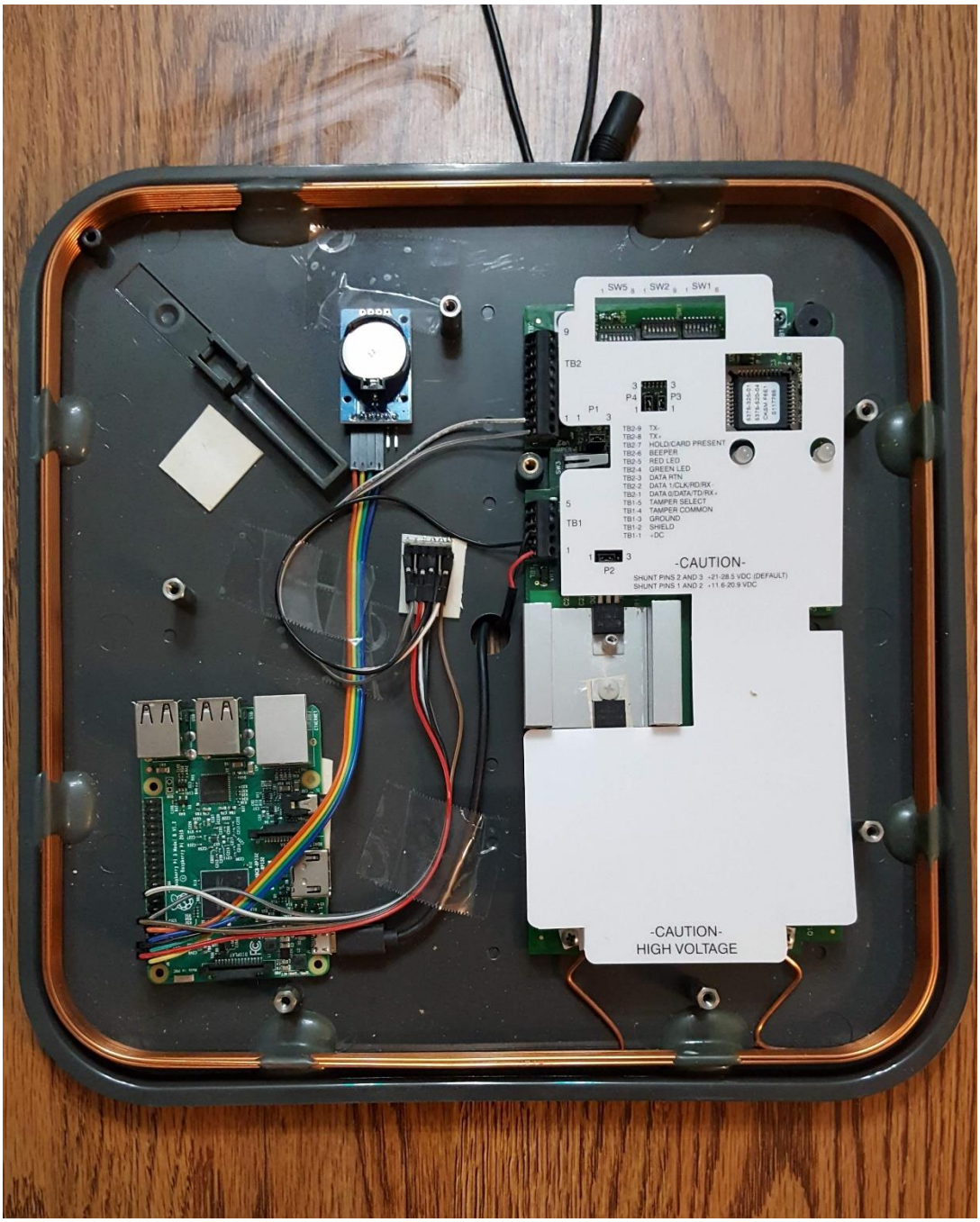

Figure 4. HID MaxiProx Badge Reader Modified Internal Components.
Note: This is an example of how an attacker may turn a system into a weapon by adding in components and making modifications to standard hardware.

4. DATA PRESENTATION AND ANALYSIS

In this section, details about how the experiments for two test cases were conducted are presented. The data that was collected is presented and the process used for its' collection is explained. In addition, an analysis of the data is offered for both test cases.

4.1. Experimental Methodology

First, the utility of the experimental configuration, described in the previous section, for detecting cloning was demonstrated. Then, tests were conducted and measurements for the maximum range of detection were completed for two test case scenarios.

- **Test Case One:** The maximum range at which an active long-range RFID badge cloner can be detected through the use of SDR was assessed.
- **Test Case Two:** The maximum range at which an active long-range RFID badge cloner, which is actively stealing credentials, can be detected through the use of SDR was assessed.

For both test cases, the SDR was initially positioned near the long-range RFID badge cloner and is incrementally moved farther away until the cloner's activity is no longer perceivable. The SDR is moved in increments of 2 feet until detection is no longer discernible. When no activity is discernable, the SDR is moved closer until the cloner's activity is faintly visible. This point is considered the maximum detectible range. Each test case was conducted eight separate times.

4.2. Experiment Data

Detection of cloning is done by observing the frequency that a cloning device would have to be using in order to steal credentials. By monitoring the frequency required to steal credentials, any activity by a cloning device is observable.

4.2.1. Data for Test Case One

Test case one is to determine the maximum detectable distance of an active long-range RFID badge cloner through the use of SDR, while there is no badge within range of the cloner. Figure 5 shows how the experiment for test case one was conducted.

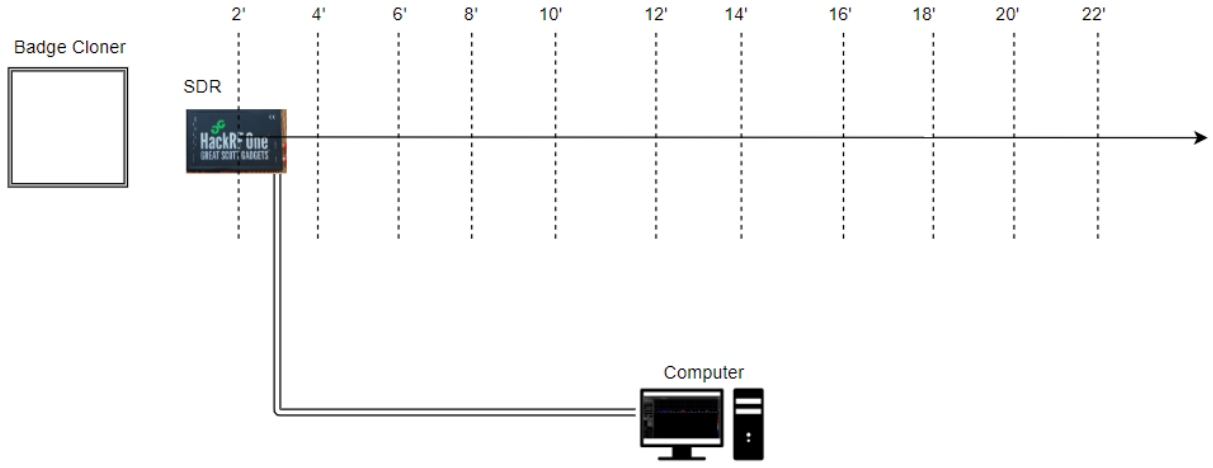

Figure 5. Test Case One Experiment Setup.
Note: This diagram shows how the experiment was conducted with a stationary badge cloner and the SDR moving incrementally away from the badge cloner.

The SDR starts two feet from the long-range RFID badge cloner and is moved away in two-foot increments. Visual data is recorded at each step for a minimum of 20 seconds before moving to the next. When a distance where activity is no longer visible is found, the SDR is slowly moved back towards the long-range RFID badge cloner until activity is faintly visible. This is the distance that is considered the maximum detectable distance.

The long-range RFID badge cloner's activity is represented by the brighter portion of each image which is concentrated near each image's middle vertical area. Each image shows the long-range RFID badge cloner's activity over a time period of 20 seconds. Activity is shown starting at Time 0 seconds (near the top of the image) until time is 20 seconds (at the bottom of

the image). The very top of each image shows the current activity at time 0 seconds before it is pushed down to be recorded in the area below and the next second is displayed.

Figures 6 to 10 present visual data for 2', 4', 6', 8', 10', 12', 14', 16', 18', 20', 22', 24', 26', and 27'. Each image is 20 consecutive seconds of data at each noted distance.

Figure 6 shows visual data for 2', 4', and 6'. At these distances, the long-range RFID badge cloner appears clearly for the full duration of the capture and has a clear repeatable pattern. At 2' and 4', activity is very bright and distinguishable from any background static. At 6' the brightness starts to fade slightly.

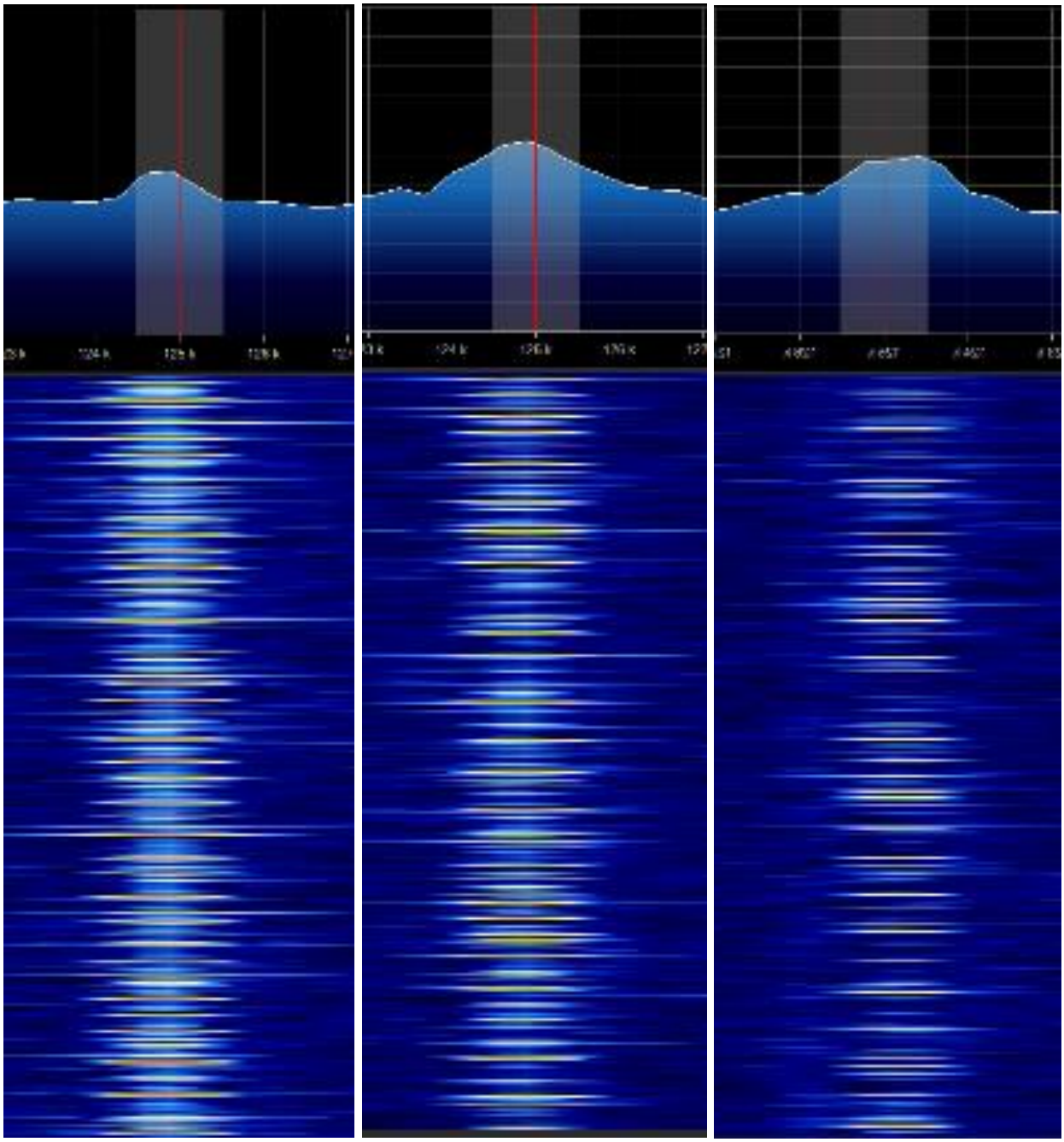

Figure 6. Visual data for 2',4', and 6' with no badge in range.
Note: Visual data for the SDR being 2', 4', and 6' from the long-range RFID badge cloner show identical activity over the period of 20 seconds shown for each distance.

In Figure 7, the long-range RFID badge cloner begins to show up less vividly, but it is still clearly visible through 8', 10', and 12' and its pattern is still clearly visible. At these

distances the image becomes less cluttered as the less intense portions of the long-range RFID badge cloner's activity begins blend into the background noise and is filtered out.

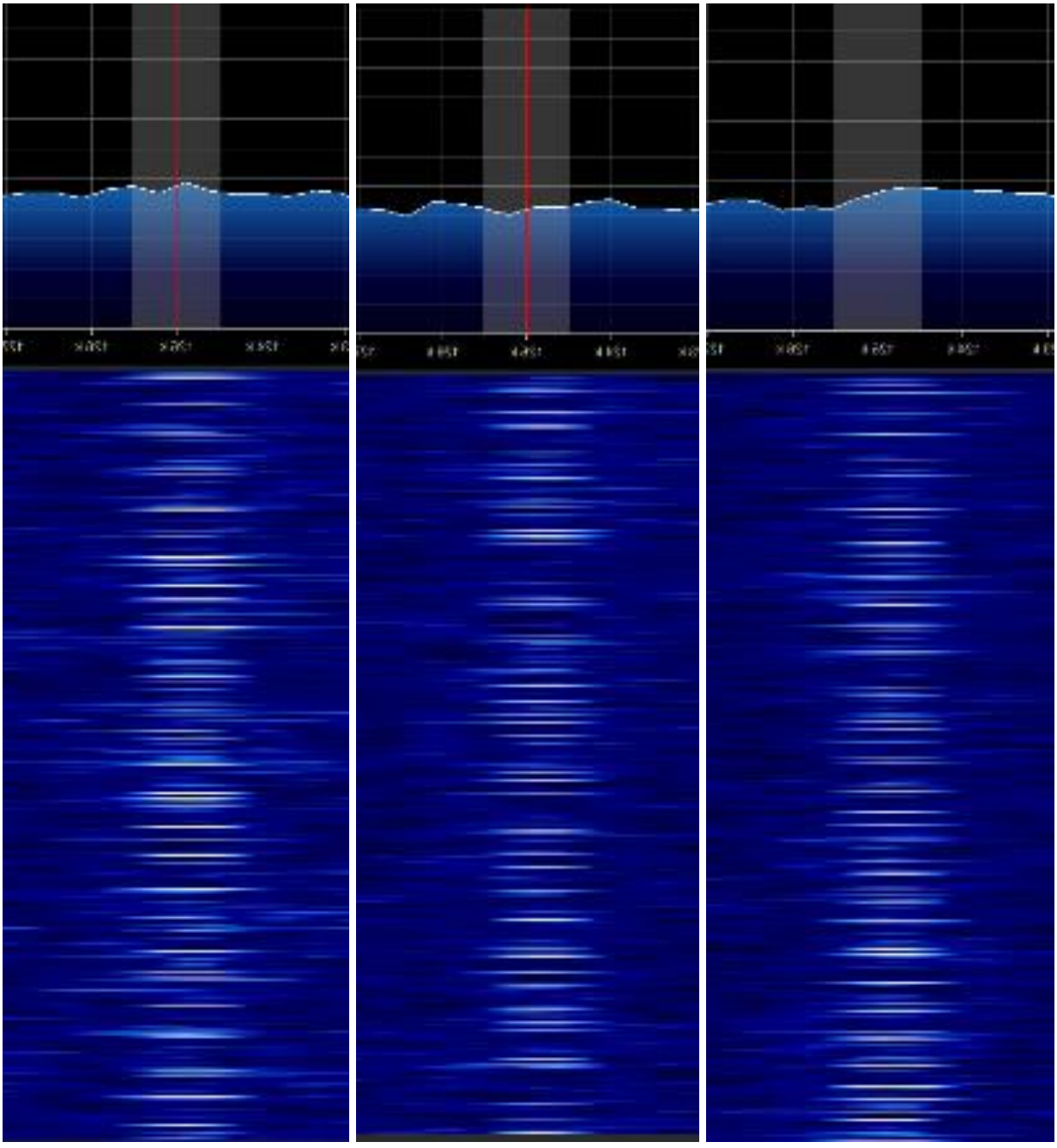

Figure 7. Visual data for 8', 10', and 12' with no badge in range.
Note: Visual data for the SDR being 8', 10', and 12' from the long-range RFID badge cloner show identical activity over the period of 20 seconds shown for each distance.

Beyond 12', the long-range RFID badge cloner continues to be visible at a similar vividness. At 14', 16', and 18' the SDR can still detect the cloner's activity, as shown in Figure 8. Activity on the outside edges continues to fall off as distance is increased resulting in a concise repeating pattern over the captured 20 seconds.

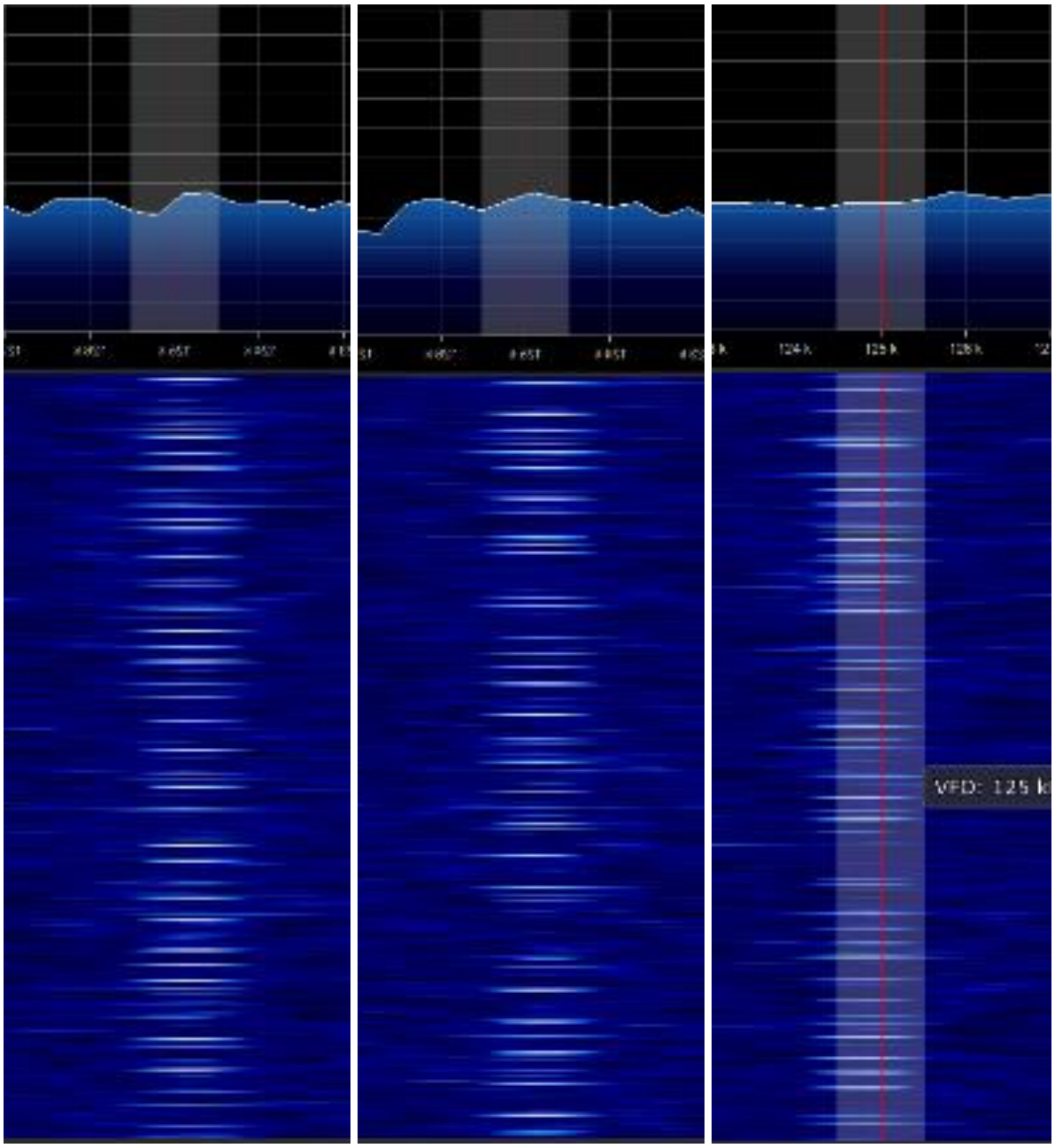

Figure 8. Visual data for 14', 16', and 18' with no badge in range.
Note: Visual data for the SDR being 14', 16', and 18' from the long-range RFID badge cloner show identical activity over the period of 20 seconds shown for each distance.

Figure 9 shows the visual data for when the SDR setup used in this experiment begins to reach its limit of detecting the long-range RFID badge cloner, at 20', 22', and 24'. At 24' there is a significant reduction in sharpness for the visual data captured. However, in an otherwise noise free environment this pattern might be suggestive of cloner use.

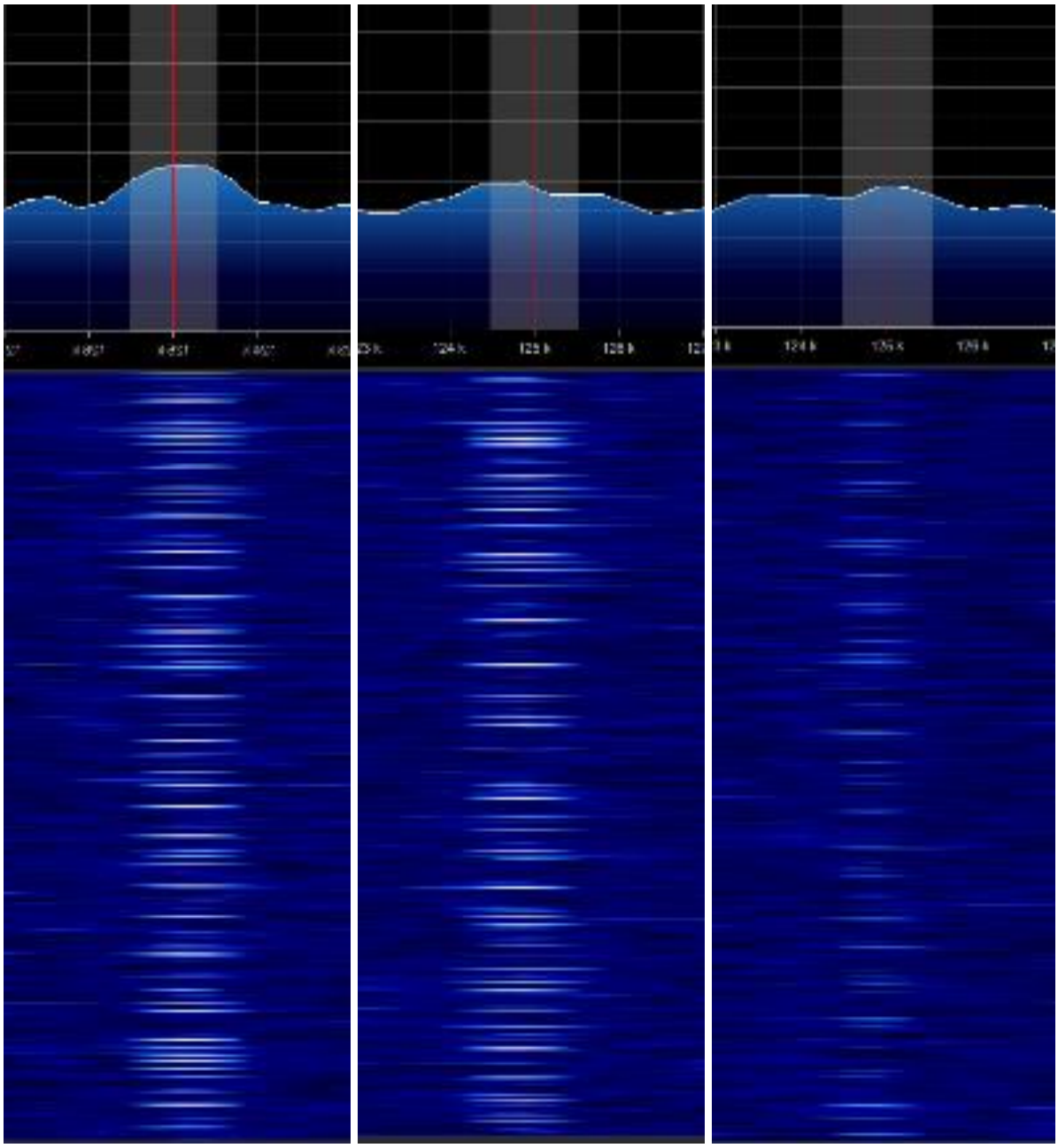

Figure 9. Visual data for 20', 22', and 24' with no badge in range.
Note: Visual data for the SDR being 20', 22', and 24' from the long-range RFID badge cloner show visible activity over the period of 20 seconds shown for each distance.

After 24’ it becomes very difficult to discern the cloner’s activity from and background static. Figure 10 shows visual data for 26’ and 27’. Portions of the cloner’s activity can be seen at 26’ (though the pattern is not readily discernable) while at 27’ almost nothing appears.

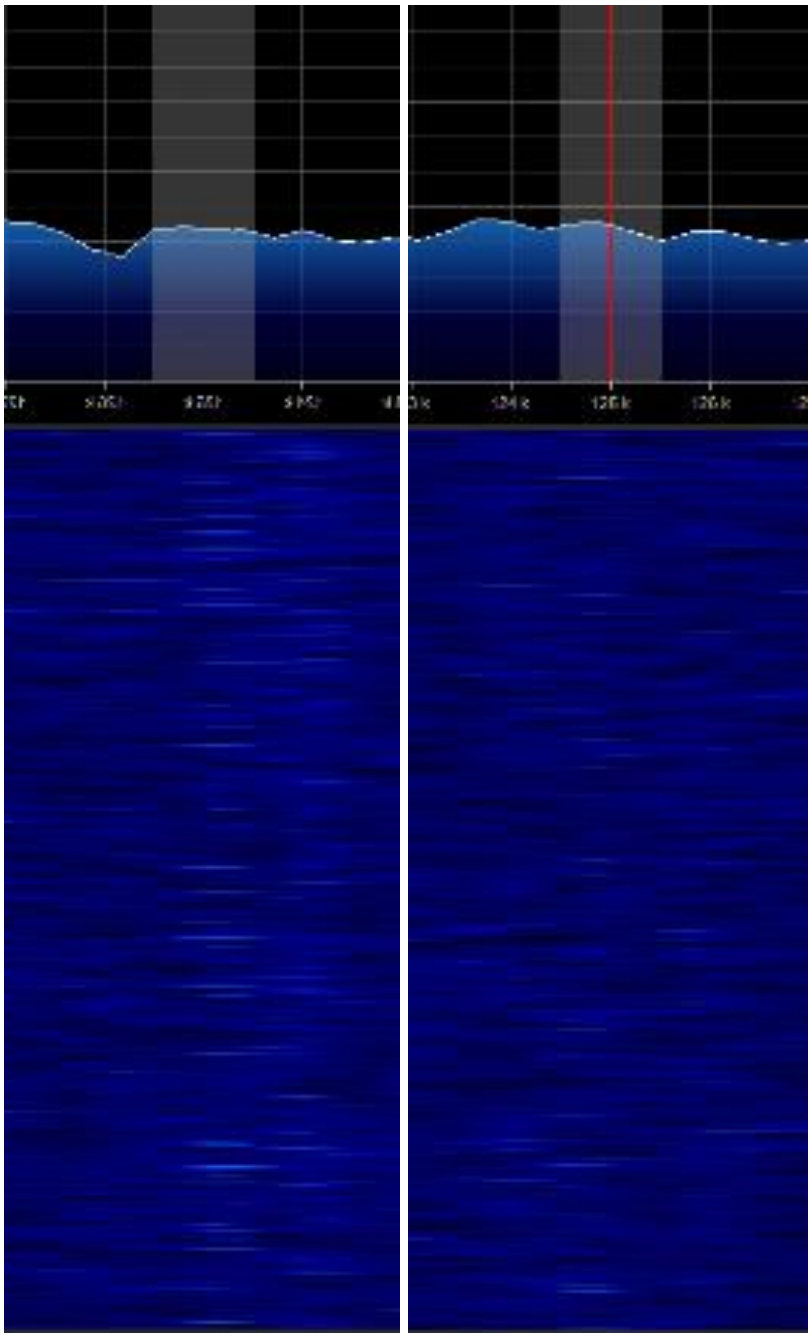

Figure 10. Visual data for 26’ and 27’ with no badge in range.
Note: Visual data for the SDR being 26’ and 27’ from the long-range RFID badge cloner show faintly visible activity over the period of 20 seconds shown for 26’ and nearly no activity at 27’.

4.2.2. Data for Test Case Two

Test case two seeks to determine the maximum detectable distance of an active long-range RFID badge cloner, through the use of SDR, while there is a badge within range of the cloner. Figure 11 shows how the experiment for test case two was conducted.

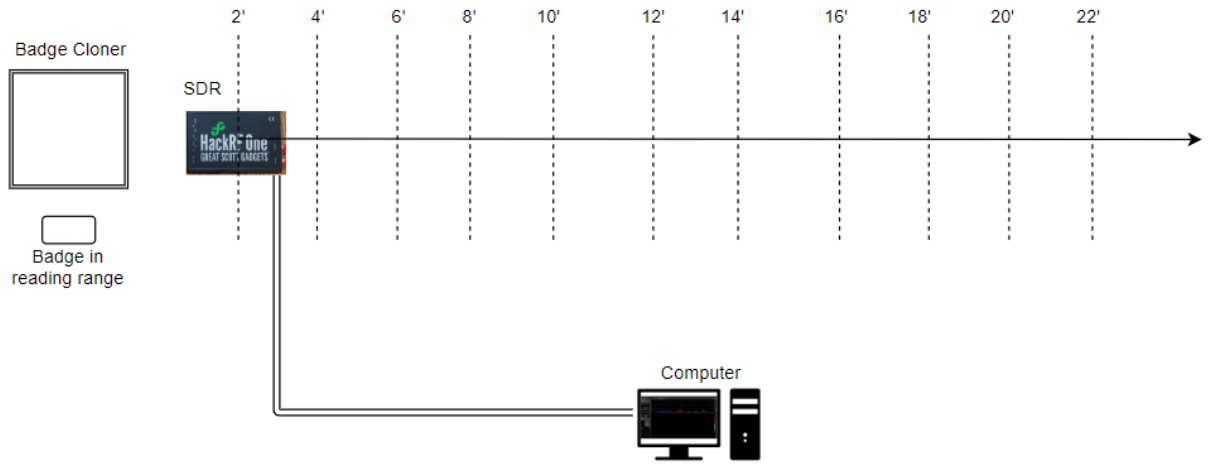

Figure 11. Test Case Two Experiment Setup.
Note: This diagram shows how the experiment was conducted with a stationary badge cloner and the SDR moving incrementally away from the badge cloner while a badge was within reading distance of the cloner.

Like with case 1, the SDR starts two feet from the long-range RFID badge cloner and is moved away in two-foot increments. Visual data is recorded at each step for a minimum of 20 seconds before moving to the next. When a distance where activity is no longer visible is found, the SDR is slowly moved back towards the long-range RFID badge cloner until activity is faintly visible. This is the distance that is considered the maximum detectable distance.

The long-range RFID badge cloner's activity is represented by the brighter portion of each image concentrated near central vertical area of the image. Each image shows the long-range RFID badge cloners' activity over a time period of 20 seconds. Activity is shown starting at Time 0 seconds near the top of the image until time is 20 seconds at the bottom of the image.

The very top of each image shows the current activity at time 0 seconds before it is pushed down to be recorded in the area below and the next second is displayed.

Figures 12 to 16 present visual data for 2', 4', 6', 8', 10', 12', 14', 16', 18', 20', 22', 22.5', 23', and 24'. Each image depicts 20 consecutive seconds of data collection at each noted distance.

Figure 12 shows visual data for 2', 4', and 6', from the long-range RFID badge cloner. Activity appears vividly and a clearly repeating pattern over the duration captured is present. At 6', the sharpness of the captured activity decreased considerably.

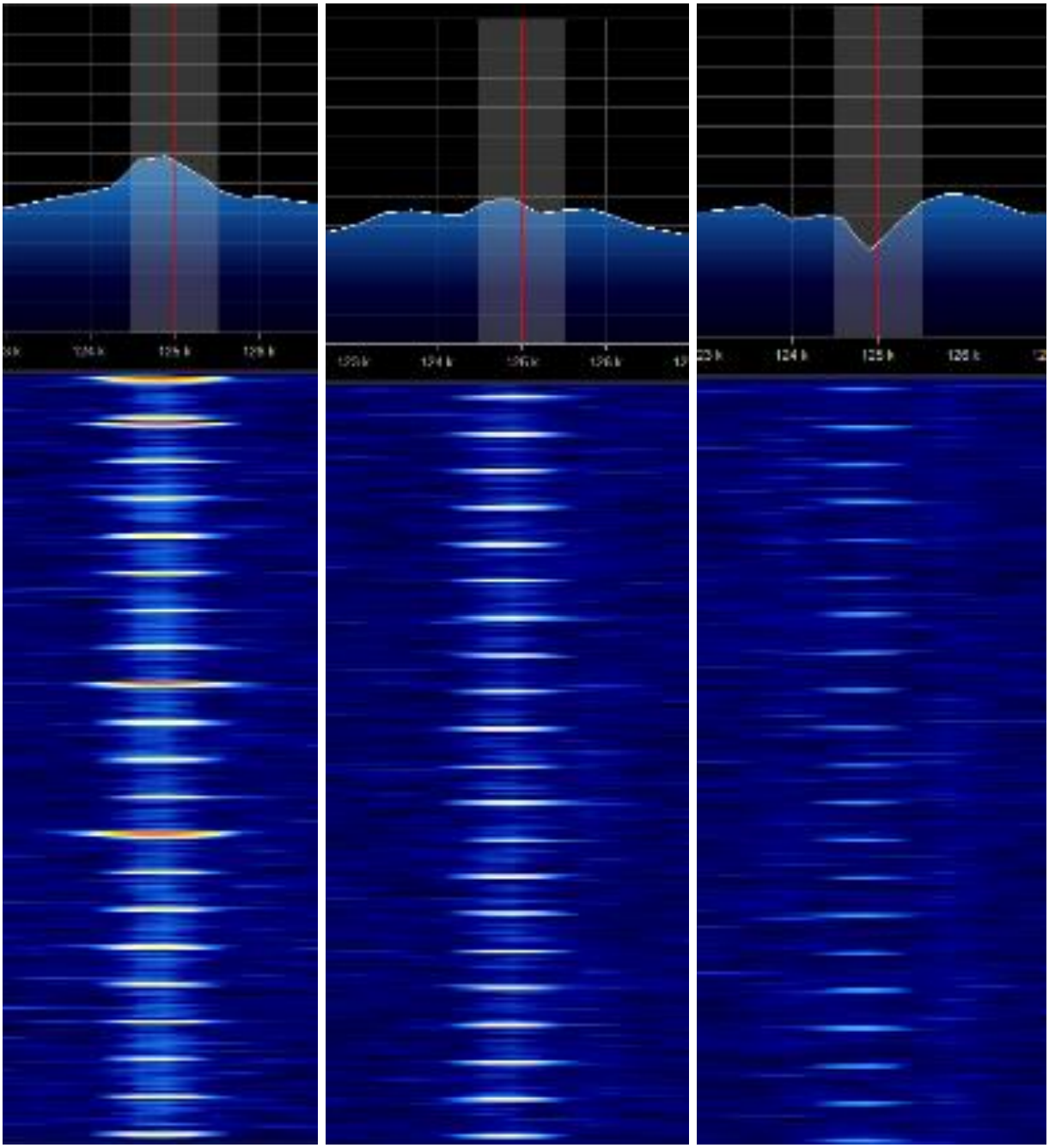

Figure 12. Visual data for 2’, 4’, and 6’ with a badge in range of cloner.
Note: Visual data for the SDR being 2’, 4’, and 6’ from the long-range RFID badge cloner show strong and identical activity over the period of 20 seconds shown for each distance.

At 8’, 10’, and 12’ the long-range badge cloner is still visible to the SDR system, but it has quickly faded in sharpness, as shown in Figure 13. The consistent pattern is still visible at these distances, but it is significantly less pronounced than at closer distances.

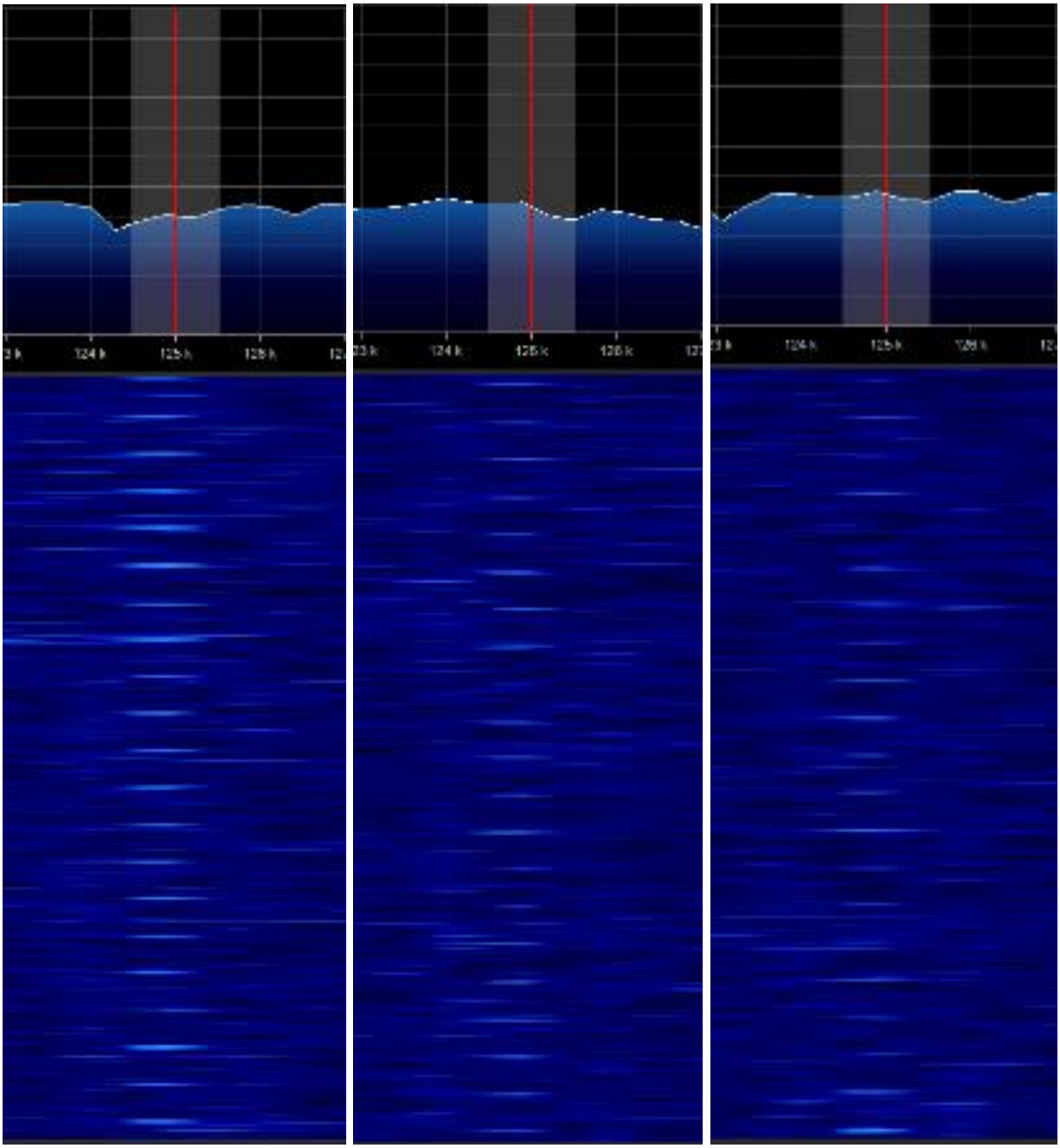

Figure 13. Visual data for 8’, 10’, and 12’ with a badge in range of cloner.
Note: Visual data for the SDR being 8’, 10’, and 12’ from the long-range RFID badge cloner show identical but more faint activity over the period of 20 seconds shown for each distance.

Figure 14 shows visual data for distances of 14’, 16’, and 18’ away from the long-range badge cloner, while a badge is within range of it. Activity is still visible at these distances but

continues to become fainter and the pattern becomes harder to discern. Some points in time appear lighter than others at the same distance.

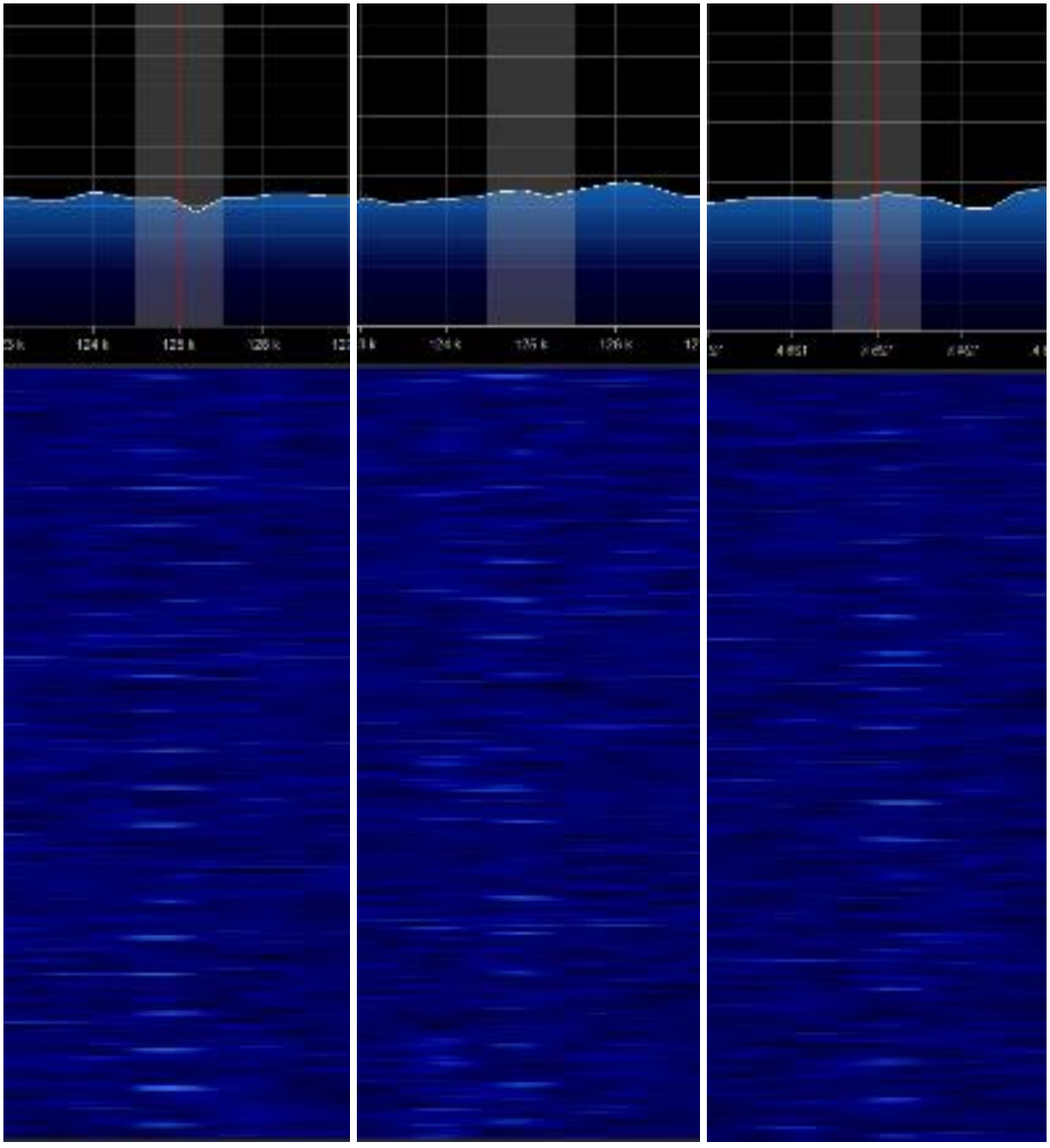

Figure 14. Visual data for 14', 16', and 18' with a badge in range of cloner.
Note: Visual data for the SDR being 14', 16', and 18' from the long-range RFID badge cloner show identical but more faint activity over the period of 20 seconds shown for each distance.

Visual data in Figure 15 shows the long-range RFID badge cloner is visible at 20’ and 22’ but at 22.5’ it becomes extremely difficult to discern any activity. At these distances the pattern is not fully visible in some points in time. By 22.5’ about half of the time activity from the long-range RFID badge cloner is not noticeable and the pattern is not clearly present.

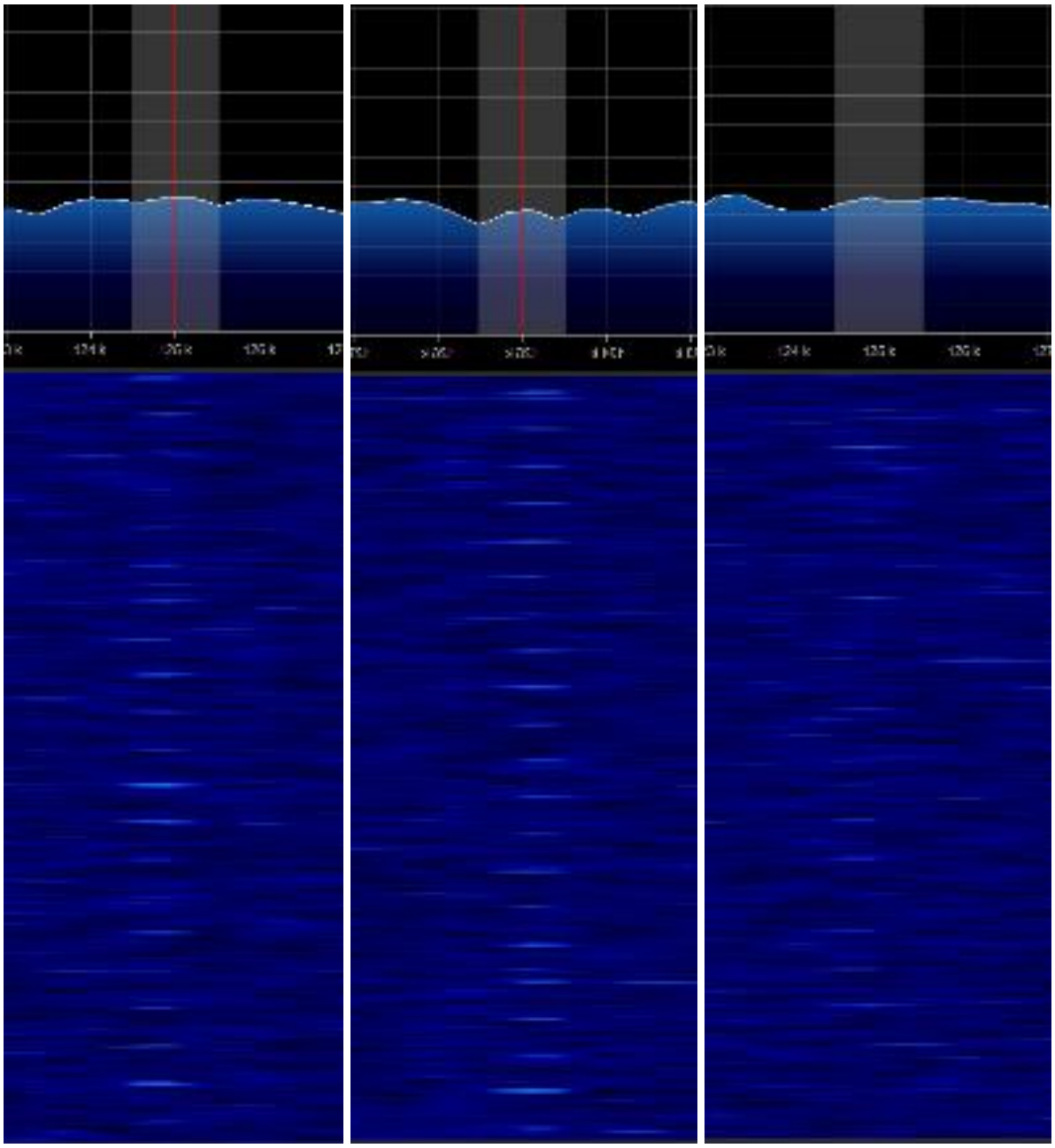

Figure 15. Visual data for 20’, 22’, and 22.5’ with a badge in range of cloner.
Note: Visual data for the SDR being 20’, 22’, and 22.5’ from the long-range RFID badge cloner show identical but more faint activity over the period of 20 seconds shown for each distance.

Figure 16 shows no easily discernible activity from the long-range RFID badge cloner when the SDR is placed at 23’ and 24’ from it. At these distances, not enough of the cloner’s activity comes through to be seen through filtering or background static.

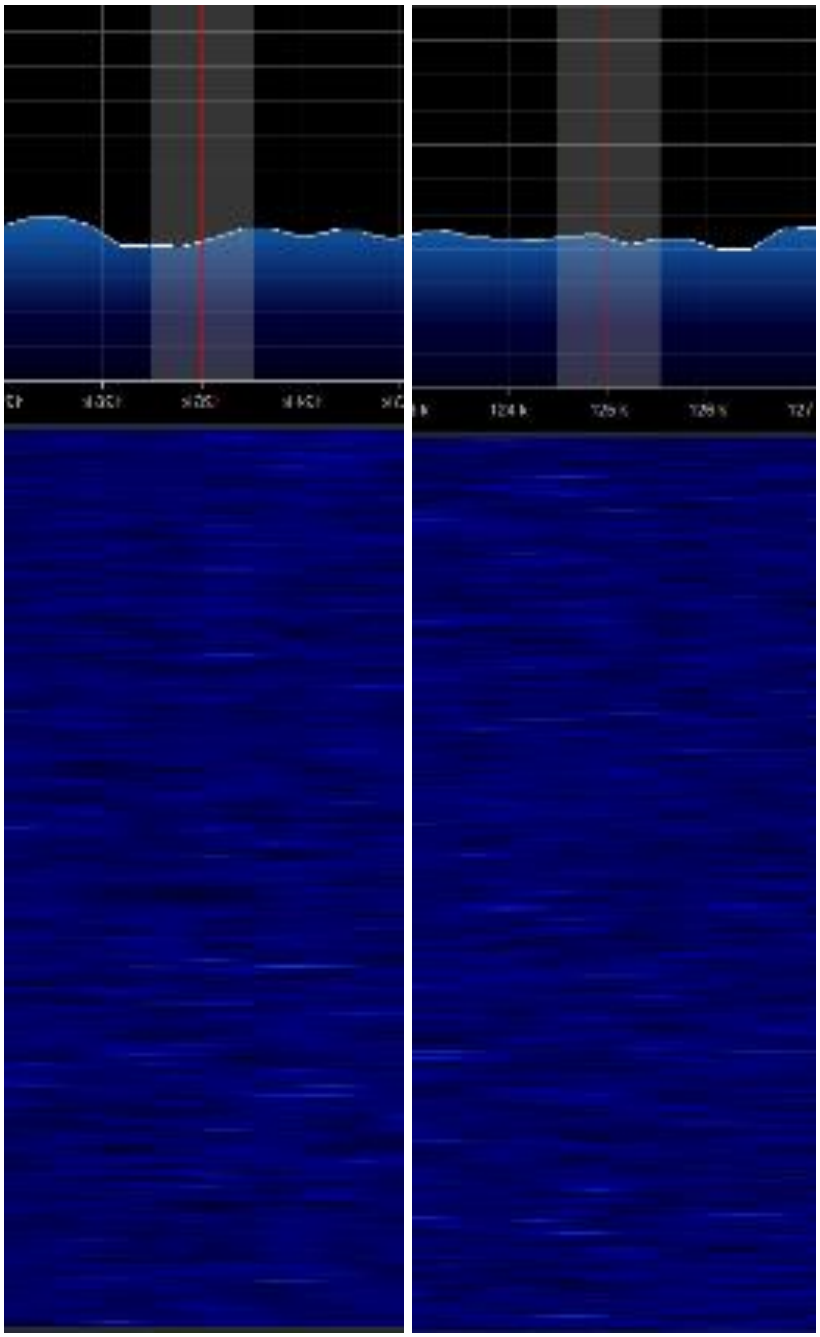

Figure 16. Visual data for 23’ and 24’ with a badge in range of cloner.
Note: Visual data for the SDR being 23’ and 24’ from the long-range RFID badge cloner show no easily identifiable activity over the period of 20 seconds shown for each distance.

4.3. System Evaluation

4.3.1. Analysis of Test Case One

Each capture taken from a progressively further distance shows an increasingly weaker signal. The farther away from the long-range RFID badge cloner the SDR was placed the weaker the detectable signal got. The signal appears to very gradually decrease until between 22’ and 24’. The signal strength becomes significantly weaker at a faster rate beyond 22’.

The long-range RFID badge cloner is visually detectable easily with the current SDR setup up to 24’. Beyond that it is still visible but far harder to see at first look. This supports that SDR can reliably detect long range RFID Badge cloners and up to a distance of 24’ with this implementation.

4.3.2. Analysis of Test Case Two

Each capture shows a progressively weaker signal as the SDR moved further away from the badge cloner. Each bright blip represents when the RFID badge within range sends its information to the cloner. This activity is easy to see up until around 8’ away. Beyond 8’ it is observable but more difficult. It remains similarly difficult to observe throughout the 10’ to 22’ ranges. Beyond 22’ it is difficult to distinguish the cloner’s activity amongst the background.

The long-range RFID badge cloner is visually detectable while gathering credentials up to 22’ by use of the SDR system. This data supports that SDR can reliably detect a long-range RFID badge cloner up to 22’.

4.3.3. Test Case Comparison

Both test cases show the plausibility of detecting long range RFID badge cloners with the use of SDR. A cloner that is active but not in the process of stealing a credential is visually

louder all the way up until its drop off detection distance than a cloner in the process of stealing a credential. Both test cases were able to detect activity beyond 20’.

Based on the data from these two test cases, a few things can be determined. It is better to look for cloners in a pre-capture state, as they are easier to see while not actively capturing a credential. A change in signal could indicate a start of a cloner begging to capture credentials. The signal used by a cloner is readily discernible by software as part of an intrusion detection system. Based on the limited range of detection, for the purpose of intrusion detection multiple units would be needed to cover a larger area.

5. CONCLUSION

Identifying a method to detect long range RFID badge cloners is an important step towards improving security of businesses and other organizations that rely on RFID badges and tags for access control and supply chain tracking. Currently there are no available systems for detecting these long-range cloners and preventing their users from gaining access to places they are not authorized to be.

This thesis presented information about RFID badge systems, SDR, and long-range RFID badge cloners. A method was proposed for detecting long range RFID badge cloning systems and experiment data was presented and analyzed for two test cases. It showed that long range RFID badge cloners are detectable by way of an SDR system. They are demonstrably detectable up to 22’ away while stealing credentials and up to 24’ away while not in the process of capturing.

There is potential for improvement to the detection system by developing a more specialized antenna specifically for monitoring the 125 kHz frequency band, as there are not currently antennas on the market usable with an SDR for this purpose. Having an antenna better suited for observing this frequency may result in a longer detection range and improve efficiency of the system.

Additional detection range might also be obtainable through the development of a plugin to automatically analyze the data in real time and better filter out background noise and make activity clearer and easier to recognize. A plugin could automate the process by turning the information into a quantifiable metric that could more easily be used.

Other future work could consider using the basis of this proposed system to create an intrusion detection system using multiple antennas placed all around a facility to simultaneously

monitor a larger area. This could be supported by developing software that could be used to triangulate where exactly a long-range RFID cloner is on the premises by making use of many antennas around a facility. This could allow for more efficient deployment of security teams to apprehend a would-be credential thief and prevent a potential breach.

The information learned from these experiments could be beneficial to those in adversarial roles as well. A penetration tester, for example, evaluating a business that has implemented a system like the one proposed could use this information to try and avoid being detected and bypass the system.

A penetration tester could implement a system to turn off their long-range badge cloner while not near anyone and turn it back on when they are near someone they suspect may have a credential they want to grab. Because detection range is slightly reduced and significantly harder to spot while a cloner is actively grabbing a credential, a penetration tester could do this in an attempt to hide themselves from a system like the one proposed in this thesis.

Another tactic that might be employed by a penetration tester, if they know their target facility has a detection system for long-range cloners implemented, would be to avoid bringing the cloner on site. They might follow employees they decide are of interest to other places like restaurants or coffee shops that they frequent and try to capture their credentials there. They could try to intercept people on the outskirts of the facility, that may be walking from their cars to work. These situations would completely circumvent the detection system all together.

REFERENCES

[1] S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security and Privacy*, vol. 3, no. 3. pp. 34–43, May-2005, doi: 10.1109/MSP.2005.78.

[2] M.-S. Jian and J.-S. Wu, "RFID Applications and Challenges," in *Radio Frequency Identification from System to Applications*, 2013.

[3] "RFID Cards | Radio-Frequency Identification Cards & Badges - IdentiSys." [Online]. Available: https://www.identisys.com/about-identisys/learning-center/id-and-tracking-glossary/rfid-card. [Accessed: 04-Feb-2020].

[4] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2. pp. 381–394, Feb-2006, doi: 10.1109/JSAC.2005.861395.

[5] "RFID Under Attack Again." [Online]. Available: https://www.darkreading.com/risk/rfid-under-attack-again/d/d-id/1128708. [Accessed: 21-Jul-2020].

[6] E. Abad *et al.*, "RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain," *Journal of Food Engineering*, vol. 93, no. 4, pp. 394–399, 2009, doi: 10.1016/j.jfoodeng.2009.02.004.

[7] Y. C. Hsu, A. P. Chen, and C. H. Wang, "A RFID-enabled traceability system for the supply chain of live fish," in *Proceedings of the IEEE International Conference on Automation and Logistics, ICAL 2008*, 2008, pp. 81–86, doi: 10.1109/ICAL.2008.4636124.

[8] "The Fishy Side of RFID Technology." [Online]. Available: https://www.advancedmobilegroup.com/blog/the-fishy-side-of-rfid-technology. [Accessed: 21-Jul-2020].

[9] R. H. Hosking, *Software Defined Radio Handbook*. 2016.

[10] Wireless Innovation Forum, "What is Software Defined Radio," *Forum American Bar Association*, p. 6, 2011.

[11] E. Grayver and E. Grayver, "What Is a Software-Defined Radio?," in *Implementing Software Defined Radio*, 2013, pp. 5–8.

[12] D. Rouffet and W. König, "Software defined radio," *Alcatel Telecommunications Review*, no. 3. pp. 203–204, Sep-2003, doi: 10.1007/978-3-319-15657-6_14.

[13] J. Landt, "The history of RFID," *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, Oct. 2005, doi: 10.1109/MP.2005.1549751.

[14] R. J. James, “A history of radar,” *IEE Review*, vol. 35, no. 9, p. 343, 1989, doi: 10.1049/ir:19890152.

[15] M. Guarnieri, “The early history of radar,” in *IEEE Industrial Electronics Magazine*, 2010, vol. 4, no. 3, doi: 10.1109/MIE.2010.937936.

[16] H. Stockman, “Communication by Means of Reflected Power,” *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, 1948, doi: 10.1109/JRPROC.1948.226245.

[17] A. Galehdar, D. v. Thiel, and S. G. O’Keefe, “Antenna efficiency calculations for electrically small, RFID antennas,” *IEEE Antennas and Wireless Propagation Letters*, vol. 6, pp. 156–159, 2007, doi: 10.1109/LAWP.2007.891960.

[18] D. Lourdes, R. Murcia, and M. E. N. Epidemiologia, “ANTENNA DESIGN FOR PASSIVE RFID TAGS,” vol. 16, no. 2, p. 176, 2005.

[19] J. Kim *et al.*, “The Beginner’s Guide To RFID Systems,” *Holtek Semiconductor Inc*, vol. 5, no. 3, p. 16, 2017, doi: 10.5281/zenodo.1133846.

[20] “What is RFID? | The Beginner’s Guide to RFID Systems.” [Online]. Available: https://www.atlasrfidstore.com/rfid-beginners-guide/. [Accessed: 04-Feb-2020].

[21] “What is Software Defined Radio Software Defined Radio-Defined.”

[22] E. Grayver, *Implementing software defined radio*, vol. 9781441993. 2013.

[23] “Airspy SDR - High Quality Software-Defined Radio.” [Online]. Available: https://airspy.com/. [Accessed: 04-Feb-2020].

[24] “HackRF One - Great Scott Gadgets.” [Online]. Available: https://greatscottgadgets.com/hackrf/one/. [Accessed: 04-Feb-2020].

[25] “Amazon.com: ANT500 - The Telescopic Antenna for HackRF One or Yard Stick One: Computers & Accessories.” [Online]. Available: https://www.amazon.com/ANT500-Telescopic-Antenna-HackRF-Stick/dp/B01CQYZJV2. [Accessed: 29-Feb-2020].

[26] “GitHub - lixmk/Wiegotcha: Wiegotcha: Long Range RFID Thief.” [Online]. Available: https://github.com/lixmk/Wiegotcha. [Accessed: 05-Feb-2020].