Student Response System Security Analysis

3 December 2017

Terrence Lim, HaeIn Oh

Advanced Computer Security: CINS 548

Final Project Research Paper

I.Introduction

iClicker is one of the most widely used Student Response Systems (SRS) in classrooms for the instructors to get instant responses from the students. Each base has its own unique channels from *'AA'* to *'DD'*. Students register device ID on the course blackboard. Then, instructors use base system to open and close sessions to receive students' responses from the iClicker keypad. According to the manufacturer, *the base can cover maximum of 300 feet and able to accept 750 responses per second in multiple choice mode, 600 responses per second in numeric mode, and 440 responses per second in alphanumeric mode*. [1] The purpose of this paper is to find out the possible vulnerabilities of iClicker and how much information can be revealed from the aggregated data.

II. Target

The targets of this project are the base systems installed around the California State University, Chico classrooms and the iClicker keypads. California State University, Chico has 113 bases installed in 15 buildings (Table 1). CSU, Chico is using 15 channels out of 16 channels leaving the 'AA' default channel, which is not being used by the campus (Table 2). The range of the frequency is from 905.0 MHz to 923.11 MHz. The keypad has a function to alter its frequency channel if it is presented within the range of certain frequency.

Channel	Frequency	Channel	Frequency
AA	Default	CA	922.46 MHz
AB	913.5 MHz	CB	923.11 MHz
AC	914.136 MHz	CC	907.2 MHz
AD	915.527 MHz	CD	908.3 MHz
BA	916.3 MHz	DA	905.0 MHz
BB	919.11 MHz	DB	909.811 MHz
BC	920.0 MHz	DC	911.25 MHz
BD	921.6 MHz	DD	909.9 MHz

(Table 2 Frequency list table)

III. Procedure

We used a program called CubicSDR and i> clicker2 to find out what frequency has the base channel from AB to DD. We first installed CubicSDR on Linux[2]. After the installation, we tested the functionality of mini SDR and CubicSDR by capturing local radio frequencies. The author of the *Security Analysis of the i>clicker Audience Response System* found the base frequencies by conducting a reverse engineering method on the clicker keypads.[3] However, since this the main objective of our research is purely based on the frequency level, we avoided to disassemble the device, rather capture frequencies directly from the iClicker bases and record the actual frequencies that these bases are operating on. After organizing the list of installed iClicker bases on the campus [4], we visited each base stations and measured the frequencies to compile our own specific frequency table. While we were measuring the frequencies, we referenced the paper [3], which they obtained the frequency range by reverse engineer. However, some of the frequencies were somewhat different or slightly off from the referenced table, so we recorded the frequency of what we found to compile the list table (Table 2).

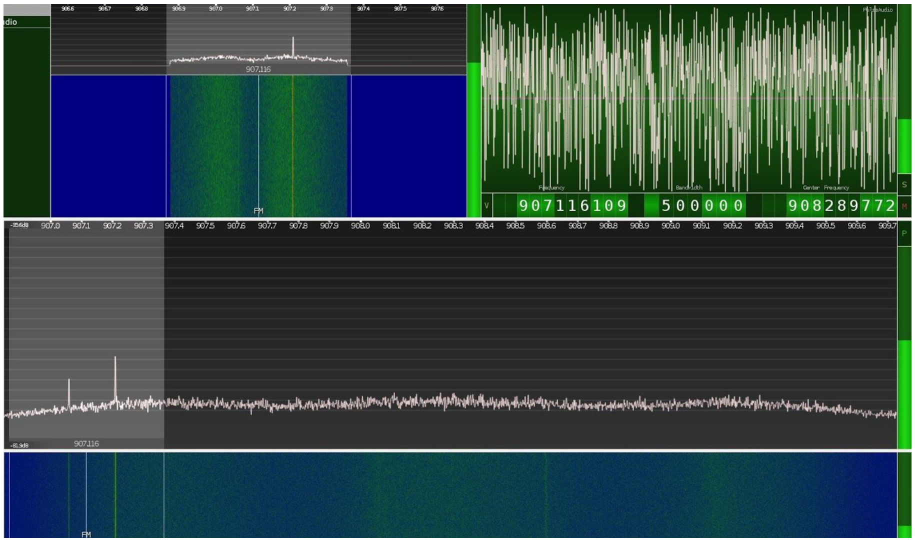
IV. Security Issues

a. Authentication

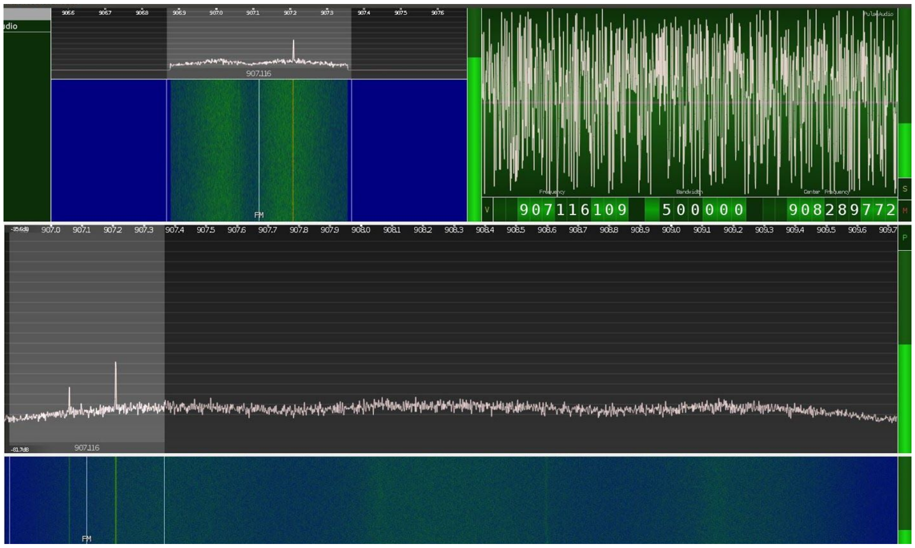
When the keypad starts to send signals within the range of bases, the base collects all signals in the air only that hold same channel frequency. For example, if keypads send signal after setting the channel frequency to AB, then any bases with the channel AB will capture the signal and store it. This demonstrates that the interaction between the base and keypad does not require authentication to exchange the data only with the certain devices because the their communication method is frequency-to-frequency rather than device-to-device. In fact, during the field research, we were able to set the iClicker's channel to the nearest base and send signals successfully even without registering the iClicker id on the course blackboard. Hence, there is a possibility to interfere and send malicious signals over the frequencies to the base if the source of the device sets the frequency channel same to the target base, but it is difficult to track down the source of device.

b. Frequency Range

Theoretically, the base can cover upto 300 ft range of area with its frequency. Frequencies were detectable from approximately 10 meters from the base using the mini SDR (R820T SDR & DVB-T) to detect frequencies. This includes in front (Fig. 1) and one floor above/below (Fig. 2) the room where the base is installed. Based on the theory, 300ft covers nearly entire floor or the building, but considering the concrete walls blocking the frequencies resulting to weakening them, finding out the validity of 300ft was not possible during the research. However, in order to prevent the frequency interference, the bases with the same channel were installed at least few rooms away from each other.

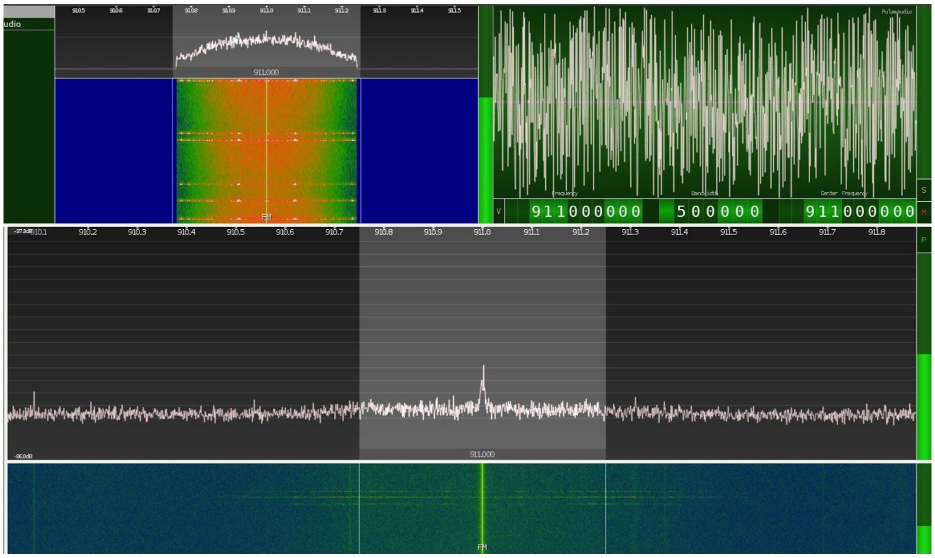


(Fig. 1 Channel CC - Frequency 907.2 MHz in front of Glenn Hall 216)



(Fig. 2 Channel CC - Frequency 907.2 MHz at the floor below of Glenn Hall 216)

The frequency range applies to the mobile keypads as well. Once the devices are set to the specific frequency, which is same as the nearest base, the SDR can detect its activity by drawing multiple vertical lines within the base's frequency range (Fig. 1). There were no differences in the strengths or performances among each keys, A to E.



Frequency 911000000
Bandwidth 500000
Center Frequency 911000000

(Fig. 3 Channel DC - Frequency 911.25 MHz. Multiple lines drawn when key ‘A’ was pressed)

V. Further Research

Currently, this research had a progress only upto finding out that the frequency exchange between the base and mobile keypads has no authentication process to recognize and authorize data, rather any devices with the same frequency channel can receive and send data to the base. Therefore, based on the current findings, we will conduct a further research to find the encryption status of data. The hypothesis of the further research is that since the manufacturer omitted the authentication function in the devices, the data should’ve been encrypted before send out to the air. The research will begin with writing a program to store captured data in the frequency, then analyze it. If the data can be simply translated without any decryption process, we want to see what kind information can be exploited. However, if the data is encrypted, the research objective will be to find out the encryption method and anymore existing vulnerabilities.

VI. Conclusion

The initial purpose of the research was to find the vulnerabilities of the student response system, iClicker, by using the frequencies. The main vulnerability found through this research was the authentication problem between the base and keypads when communicating to each other, and the unprotected frequency that any devices within the range can detect and capture their activities. However, there are more factors need to be further studied to come to the final conclusion where these captured frequencies can be translated into human readable data.

Building	Room #	Channel	Building	Room #	Channel	Building	Room #	Channel
ARTS (6)	105	CA	**LANG** (7)	300	AC	**GLNN** (18)	102	BA
	106	BB		303	AB		112	AC
	107	CD		302	AD		123	DB
	111	BA		104	CB		125	AD
	112	BD		105	CC		202	AC
	306B	AB		106	CD		212	AB
AYRS (3)	106	AC		107	BB		214	DD
	120	CD	**MODC** (8)	114	AC		216	CC
	201	BB		118	CA		223	CA
BUTE (15)	101	BD		120	CC		225	BC
	103	AC		123	BB		302	BC
	104	CD		217	AB		304	AD
	109	BC		220	CD		306	BD
	113	DC		221	BC		308	CB
	205	CC		222	BA		310	DA
	219	CD	**OCNL** (7)	120	AB		312	BB
	221	CA		121	AD		314	DC
	227	AD		123	AC		327	BA
	229	AB		124	CC	**HOLT** (14)	111	CA
	307	DD		237	BB		113	DB
	319	DB		239	BA		170	AB
	323	BB		254	CD		173	CD
	327	BA	**PAC** (4)	134	CD		185	BB
	505	BC		144	AB		187	BD
THMA (11)	106	AC		206	AC		189	CB
	107	DD		210	BB		266	CC
	108	CD	**PHSC** (7)	104	CA		268	AD
	113	BB		105	BA		277	BC
	115	BC		106	DB		350	BA
	116	AC		108	BD		352	DA
	117	BA		109	CD		357	AC
	121	AD		202	DD		363	DC
	130	AB		301	AC			
	134	CC	**PLMS** (8)	102	AC			
	210	BD		106	AB			
YOLO (5)	143	AC		201	BB			
	117	BC		205	CD			
	171	CD		301	BC			
	217	BA		303	BD			
	218	CC		312	AD			
SSKU (1)	120	CD		329	DA			

(Table 1 California State University, Chico iClicker base installed status)

VII. References

[1] Community.macmillan.com. (2017). FAQ: iClicker Base | The Macmillan Community. [online] Available at: https://community.macmillan.com/docs/DOC-7364-faq-iclicker-base [Accessed 27 Nov. 2017].

[2] GitHub. (2016). cjcliffe/CubicSDR. [online] Available at: https://github.com/cjcliffe/CubicSDR/releases/tag/0.2.0 [Accessed 20 Nov. 2017].

[3] Security Analysis of the i>clicker Audience Response System. (2010). [pdf] Derek Gourlay, Yik Lam Sit, Yuan Sunarto, Tim Wang. Available at: https://courses.ece.ubc.ca/cpen442/term_project/reports/2010/iclicker.pdf [Accessed 15 Nov. 2017].

[4] Csuchico.edu. (2017). Clicker Channel Assignments - Classroom Technologies - CSU, Chico. [online] Available at: http://www.csuchico.edu/classrooms/classrooms/clicker-channels.shtml [Accessed 27 Nov. 2017].