ELECTION FRAUD

PRIMARY DOCUMENTS

Election Fraud – Election Hardware of the Ballot Sorter

Benjamin Wilkerson

Synopsis for "Election Fraud
Election Hardware of the Ballot Sorter"

Numerous subject matter experts have investigated the issue of the ballot sorting machines that were used for the April 15th South Korean general election, and some of them have concluded that there were vulnerabilities and irregularities with the ballot sorters. Notably, the experts have not been allowed to conduct detailed or forensic examinations of the ballot sorting machines. This lack of transparency on the part of electoral officials has raised suspicions regarding the results of South Korea's 21st general election.

Mr. Benjamin Wilkerson is one of the aforementioned experts. He was able to examine a ballot machine in enough detail to raise concerns over the capabilities of the ballot sorting machines.

Mr. Wilkerson's detailed report describes three major issues with the ballot sorters used in the April 15th election: First, Article 5 of the Supplementary Provision of the Public Official Election Law states that the ballot sorter should be a simple sorter and operate as a stand-alone without being connected to any other external devices. However, the ballot sorter used has five built-in USB ports which make it possible to send the internal data to the outside and to receive and store/implement firmware or data from the outside.

Second, the Field Programmable Gate Array (FPGA) was used as a H/W component, and this means that the firmware can be changed at any time to perform certain tasks.

Third, QR codes were used in violation of the existing election law, which states that only barcodes can be used on the ballot paper. Furthermore, the ballot sorter was designed to read and decipher even confidential information that may not be read by an ordinary QR code reader.

The technical issues discovered with the ballot sorting machines used in the general election are problematic, according to Mr. Wilkerson. As configured, tampering and manipulation of the machines was possible. And the suspicions of such activity alone call into question the integrity of the entire 21st South Korean general election.

Introduction

Many subject matter experts in South Korea have investigated the hardware of the ballot sorting machines (hereinafter referred to as 'ballot sorter') and concluded that there were three major and critical problems with the ballot sorter which would invalidate the outcome of South Korea's 21st General Election held on April 15, 2020.

Benjamin Wilkerson, former Technical System Engineer of IBM's semiconductor design, released a picture of a printed circuit board (PCB) in the ballot counting machine. His picture of the motherboard clearly shows 2 built-in CPUs, so that the ballot counting machines function as a powerful computer. Benjamin Wilkerson explained, "This is a supercomputer specification higher than a normal laptop specification. Due to the nature of a simple counting system, such a high-performance system is not required." Huawei communications devices were also discovered in system hardware and other devices of the National Election Commission (NEC) platform.

<Figure 1> Circuit board of the ballot sorter

This report discusses the three major problems with the hardware of the ballot sorter, investigated and concluded by many subject matter experts in South Korea.

Please be advised that most investigation and analysis were done based on a few available photos and recollection of what has been seen since the NEC of South Korea has decided not to release the specifications of the hardware and software source code and has refused to preserve the evidence related to the ballot sorters and laptop computers used in the election.

Three major problems with the ballot sorters used in this election

First, Article 5 of the Supplementary Provision of the Public Official Election Law states that the ballot sorter should be a simple sorter and operate standalone without being connected to any other external devices. However, as you can see in the picture shown below, the ballot sorter has 5 built-in USB ports which makes it possible to send the internal data to the outside and to receive and store/implement firmware or data from the outside. And, if you look at the mainboard inside the ballot sorter as shown below, there is a reset button and a boot button which infer that there is an operating system. In short, the ballot sorter is a high-performance computer system. Furthermore, the problem is that it has a backdoor that can be connected to an external device to perform necessary operations to manipulate the counting process.

<Figure 2> USB ports in the ballot sorter

Second, the Field Programmable Gate Array (FPGA) was used as a hardware component, and this means that the firmware can be changed at any time to perform certain tasks.

Third, QR codes were used in violation of Article 151, Paragraph 6 of the Public Official Election Law, which states that only barcodes can be used on the ballot paper. Furthermore, the ballot sorter was designed to read and decipher even confidential information which may not be read by an ordinary QR code reader.

<Figure 3> QR code on ballot

Details

The laptop (LG Gram) used in connection with a sorter is known to have a Wi-Fi module mounted directly on the PCB and cannot be removed by a user. Looking at the hardware configuration of the sorter, they are the main CPU (STM3 chip from ST Micro) and FPGA (SPARTAN3 family chip from XILINX). Nevertheless, considering that all functions of the ballot sorter are performed only when connected to the controlling laptop, it seems that the controlling laptop acts as a master and the ballot sorter plays the role of slave. As discussed here, the controlling laptop playing the role of master means the operations of the ballot sorter can be arbitrarily controlled through the laptop. This is in violation of the definition of a ballot sorter as a simple sorting machine which must operate independently as stipulated by law.
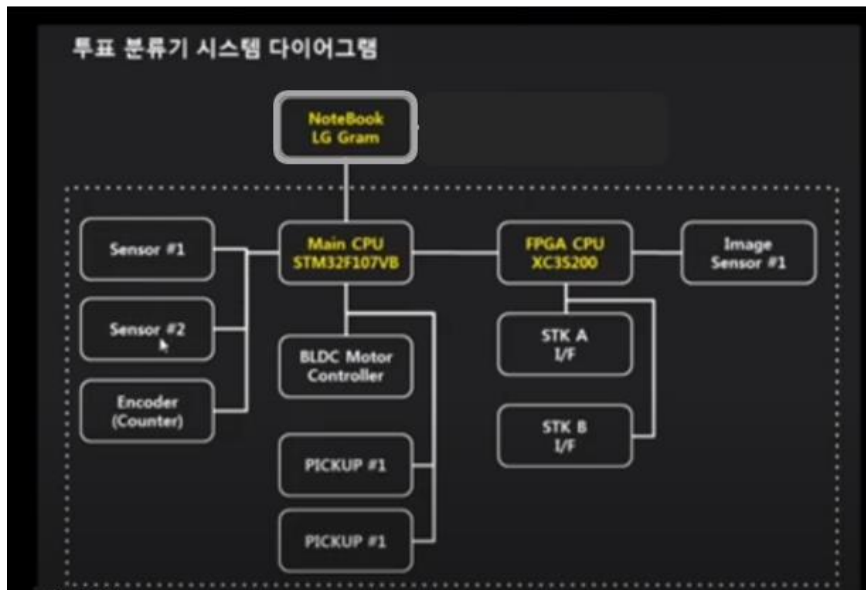
<Figure 4> System diagram of the ballot sorter

Through an incident that occurred in a local electoral district (Buyeo district), it was confirmed that there was a built-in wireless LAN card in a laptop (LG Gram) connected to the ballot sorter, and an unidentified entity/person downloaded certain codes (an indication of possible manipulation) for different electoral districts after being connected to the central server once the laptop was booted. In addition, the ballot sorter printed out the counting status which included the number of electors, number of distributed ballots, number of voters and number of votes for different candidates, and this was impossible without having some type of communication capabilities. Furthermore, the circuit diagram of the ballot sorter submitted for patent shows the term, 'communication unit'. These findings led many experts to believe that the ballot sorter used in this election was more than a mere sorter as required by law. As a matter of fact, it is highly suspected that the sorter had functions of a computer which could communicate with external devices/entities.

The following briefly describes what had happened in the electoral district. One of the official observers, a member of the opposition party, complained about the frequent malfunction of a ballot sorter on site, and a member of the National Election Commission reluctantly restarted the

ballot sorter by pressing the reset button. Once reset, the ballot sorter started working fine and very interestingly, a candidate from the opposition party ended up winning the district. This led the experts to suspect that there might have been an effort to modify software, firmware and/or coefficients in order for someone or an entity to manipulate the ballot sorting process using the controlling laptop or an external device connected to the ballot sorter through one of the USB ports.

The ballot sorter used in this election is intentionally designed as a high-performance computer system to remotely control the process on the network. In addition, there is a 'Good Software 1st Grade' certification mark on the ballot sorter. This means the ballot sorter has a built-in software and is capable of executing various manipulations. This also proves that the ballot sorter used in the election was not a mere sorter as claimed by the NEC, but rather a computer-like device equipped with a CPU and communication functions which is a violation of Article 5 of the Supplementary Provision of the Public Official Election Act (Act No. 4793).

The ballot sorter used in this election was a complete joke with absolutely no security and 100% possibility of manipulation. This ballot sorter should have not been used at all.

Initially, the observers thought that the laptop was there simply to upgrade the firmware of the embedded system and to conduct simple 'monitoring'. The observers had been fooled when the NEC said that the ballot sorter was a mere sorting device. The observers somehow came to the conclusion that the laptop would enhance security.

Many experts, however, concluded that the laptop played a role of master by processing images and transmitting the 'sorting' command. The laptop also had a function to display all the processes on the screen. Based on these findings, the experts claim that the ballot sorter's real job was to confirm and assure that the ballots that were cast are carefully manipulated, so as to satisfy the predetermined ballot count.

The ballot sorter must have counted the number of ballots cast and then sent the results to a manipulator(s) in advance, and intentionally readjust the ballot count to favor a pre-selected candidate(s). To manipulate the ballot itself, a massive number of fake ballots were placed in the early voting boxes. The reason for this scheme is that the electronic list of voters was used for the early voting and each voter was not manually counted. During early voting, the ballot count was manipulated in real-time, and the fake ballots were entered in the box(es) to satisfy the manipulated number. The massive number of fake ballots were used for this purpose.

These fake ballots were generated in the names of individuals considered as non-voters according to the electronic list of voters and confirmed by the QR code. Through this, the fake ballots were counted as valid ballots. When compared with the electronic list of voters, the fake ballots would be confirmed as valid ballots.

Conclusion

As briefly shown above, a great number of subject matter experts believe that the ballot sorters used in the 21st General Election held on April 15, 2020 were in violation of the Public Official Election Act in three main areas. Each ballot sorter was designed to act as a computer, had gate array components which could be connected to an external central server, and was equipped with a QR code reader. The experts concluded that their assessments led to the conclusion that the ballot sorter was designed and manufactured to do only one job: manipulation.