Investigation and Creative Ideas for Securing Public Transportation System

Yi Wei, Yichen Feng, Yuhan Weng
Nanyang Girls' High School (As of 2015),
in collaboration with A*STAR Singapore

***Abstract*—Public transportation system has been highly appreciated for its convenience and fastness. With the fast development of Information Technology and more high-tech cybercrimes happening, the cybersecurity of the public transportation system is critical. In this paper, we aim to identify and assess security vulnerabilities of current communication and signalling systems and propose methods to effectively prevent them. There would be a possible scenario in which an insider attacker who has direct access to a certain computer and network of the public transportation system intends to disrupt the signalling system or send malicious command to disturb the vehicle's operation. Under this hypothesis, we tested the possibilities of insider attack using ARP (Address Resolution Protocol) Poisoning technology and suggested possible solutions.**

Keywords-public transportation system, cyber security, signalling system, ARP Poisoning

I. Background and Purpose of Research Area

The city state has invested vast amounts of monetary and human resources in order to provide fast and effective means of transport to commute to work. However, the occurrence of frequent breakdown incidents has not only resulted in the compromise of convenience, but also in systematic reviews that have identified the need to discover space for potential improvement of the system.

During our pre-experimental survey, the causes of vehicle breakdown in recent years are shown in Figure 1. From Figure 1, there are four major faults, namely track fault, power system fault, train fault and signal fault. Since track fault, power system fault, and train fault maybe belong to the areas of mechanical, electrical or electronic parts, we focused on signal fault (15%) and identified as one of the main causes of train breakdown and needed to pay more attention. Therefore, we decided to explore some related security issues with potential signaling attacks. In order to specialise our research, we then listed all the pathways involved in the transfer of signals. Through communication with experts, we were acknowledged the act of a potential insider attack. As a result, we planned to test on the possibility of this act and by doing so, we hope to raise the awareness of the importance of improving cyber security.

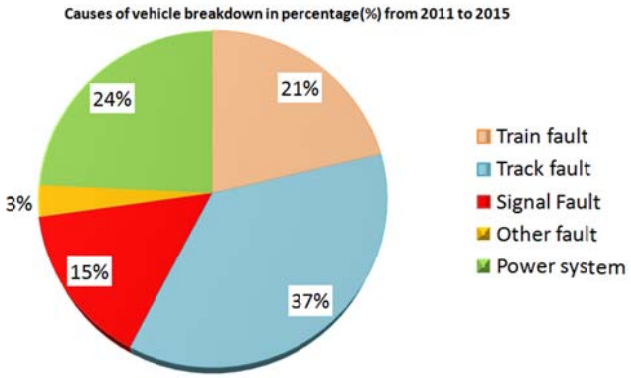

Figure 1. Causes of vehicle breakdown in recent years.

As shown in Figure 2, Communications-Based Train Control (CBTC) is a railway signaling system that makes use of the communications between the train and track equipment for the traffic management and infrastructure control [1].

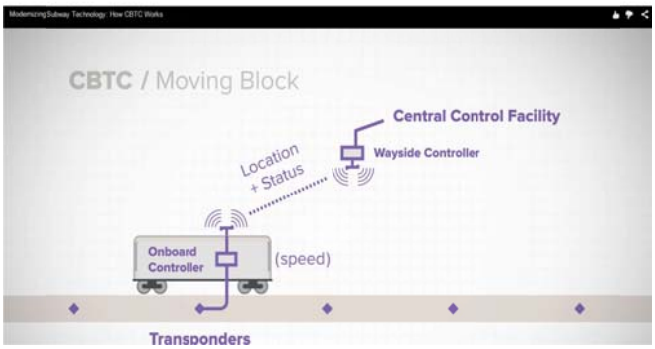

Figure 2. CBTC Railway signaling system.

II. HYPOTHESIS OF THE RESEARCH

Commands sent from the controlling system are the kernel of the vehicle's operation. Admittedly, the controlling system is already very secure since the communication network is isolated from the public Internet network and every pass and access needs a password which is only known to the insiders. However, there is still a chance that an insider attacker, who may be a depressed employee or be an undercover, can disrupt the system and send malicious command to disturb the vehicle's operation. Hence, we simulated the process of a possible insider attack to understand how an insider can break into the system.

III. RESEARCH METHOD AND MATERIALS

We created a scenario in which an insider attacker who has direct access to a certain computer and network in the control rooms of Operation Control Centre or Train Stations intends to disrupt the signalling system or send malicious command to disturb the vehicle's operation. Under this hypothesis, we tested the possibilities of insider attack using ARP (Address Resolution Protocol) Poisoning technology and suggested possible solutions.

A. STUDY, SURVEY AND COLLECT INFORMATION

1) Communication Based Train Control System

Tracks divided into blocks with each 100 feet long. Signal colours include green, yellow and red. Green indicates trains travelling normally down the track while yellow represents caution and trains travelling slowly. Red means occupied (*tracks are considered occupied even if only a small part of the train is on it) and trains must stop (*if they don't stop, safety devices will trigger the breaks of the trains). Buffers are added to ensure trains do not run too close to each other.

2) Structure of Signalling System

Signalling system is defined as the network of transmission of signals between the train and Operation Control Centre (OCC). The system consists of central ATS at OCC, local ATS, trackside ATC and CBI (Computer-based interlocking) at Main Signalling Stations (MSSs). MSSs are spread out across the line for every 2-3 stations and take charge of signalling for neighbouring secondary stations, which is used to safely direct railway traffic.

3) Address Resolution Protocol(ARP) Poisoning

ARP Poisoning technology is a type of attack in which a malicious attacker sends falsified ARP messages over a local area network and steals information by associating itself with the IP address of a legitimate computer or server on the network. By using ARP Poisoning, the insider attacker can easily fool the network by associating other operationally significant IP address to the insider attacker's own MAC address. The insider attacker can exploit ARP Poisoning to intercept network traffic between two devices in the network, for example, one of the computers in control station and the router, and sniff clear text passwords by sending a malicious ARP reply to the computer.

B. ANALYSIS OF POSSIBLE SCENARIO

As the attacker is an insider, he has access to the control room and his identity allows him to manipulate the computer and the network without being suspected. After the attacker breaks into any one connection between two devices A and B, he can disguise himself as A to send message to B, and as B to A (Figure 3). Thus, both A and B will recognise the attacker's wrong command as being given by the system and continue to pass it down without arising suspicion.

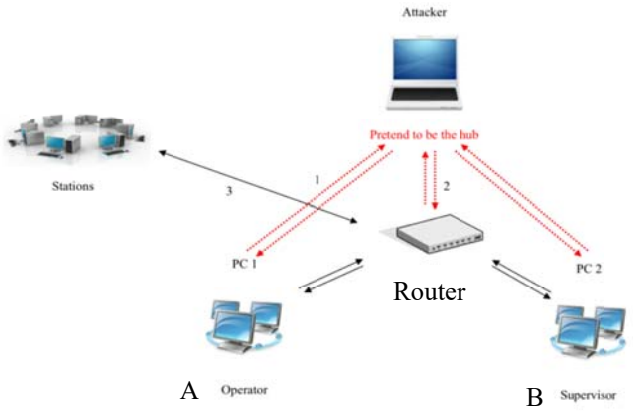

Figure 3. Analysis of Possible Insider Attack.

C. EXPERIMENT

Before the experiment, we randomly select two of the devices to relatively be the command sender and receiver and connect to a router which could be involved in signal transferring. We follow the steps as follows:

a. Connect the selected devices to the router.
b. Launch the attacking software Ettercap and Wireshark on the attacking device to enable the attack.
c. Start the sniffing function on the attacking device.
d. Wait and sniff when the commander sends the command to the receiver.
e. Search the information to attain the command according to the known IP address of the commander.
f. The command is obtained by the attacker and then the attacker may launch the replay attacks.

Or the attacker can edit the command and then send it to the receiver for malicious purposes.

IV. Proposed Solutions

During the period of experimentation, possibilities of preventing ARP Poisoning emerged. One possible solution is to encrypt all the commands. However, this way also cannot completely avoid the insider attacks as the insider may also know the encryption/decryption key(s). The other possible solution we came up with is to design a program which directs a command to a random PC so that each command cannot not be sent without being verified by another officer.

V. Conclusion

In this research work, we created a scenario of cyber attack on the metro system and explored the possibility of using ARP Poisoning. During the experiment, we have successfully attacked the command sender and stolen all the information which were sent through the network. In other words, with direct access to the computer and network, an insider attacker can easily attack the metro system, causing the subways to the stop and setting off a panic in many ways. Firstly, the insider attacker can easily fool the network by associating other operationally significant IP address to the insider attacker′s MAC address. Secondly, the insider attacker can exploit ARP Poisoning to intercept network traffic between two devices in the network, for example, one of the computers in control station and the router, and sniff the passwords by sending a malicious ARP reply to the computer.

One possible solution is to encrypt all the commands if the insider attacker does not know the encryption/decryption key(s). The other possible solution is to design a program with the two-tier approval system.

Acknowledgment

We would like to thank the Institute for Infocomm Research, A*STAR for giving us this opportunity to participate in this program. We would also like to show our appreciation to our teacher advisor, Mr. Benny Koh and our mentor Dr. Huaqun Guo for all the patient guidance and constant support along the way.

References

[1]. Communications-based train control. https://en.wikipedia.org/wiki/Communications-based_train_control

[2]. Modernising Subway Technology: How CBTC Works. https://youtu.be/x8Y237PcuzY

[3]. Regional Plan Association. Accelerating the Transition to Communications-Based Train Control for New York City's Subways. http://library.rpa.org/pdf/RPA-Moving-Forward.pdf

[4]. Thales SelTrac. https://youtu.be/ziVYm0BJNXI

[5]. Singapore power. Singapore Power ElectricityCable Tunnel Project. http://www.singaporepower.com.sg/irj/go/km/docs/wpccontent/Sites/CableTunnel/Site%20Content/index.html