Breaking out of Prison is easier than you think

Allen L, Kabello

New Horizons

Author Note

Allen L. Kabello, Information Security, New Horizons

Allen.kabello01@yahoo.com

Contents

Abstract

This paper explores three published online sources about vulnerabilities in Access Control Points (ACP) with prisons. While there are many different forms of Access Control Point (ACP), the main security system used in our prisons today is a basic Programmable Logic Controller (PLC). This paper refers to many incidents that have happened in prisons across the United States. Which have been only increasing over the years. It will also cover how an attacker on the outside can gain access to any high risk or high violent inmate that can lead to bodily harm to inmates, guards, and civilians which can lead to death. It will also review some of the preventative measures that can be used to limit or remove these incidents from recurring. This paper examines the use of a honeypot system and how to implement an Intrusion Detection System (IDS). It also covers how the physical security should not be solely replaced by machines.

Keywords: Programmable Logic Controller, Access Control Point

Introduction

Why are prisons so vulnerable to cyber-attacks? Cyber-attacks in prisons have been an issue for years and-one thing that is often over looked is the security systems of our prisons. We need to hold the manufacturers accountable for their security systems that are implemented in our prisons today. Attackers have many ways to attack innocent people without physically harming them, but when working with some of the most violent criminals this changes everything. There have been multiple reports in the United States of prisons receiving a power surge or a glitch which have opened multiple prison cells at once (Inmates Have Tried Many Ways To Break Out Of Prison: Chip Away At Concrete, Overpower Guards, Tie, n.d.). We can take steps to limit this from happening by implementing a stronger system to keep prisoners locked down.

Accountability

The manufacturers should be held accountable for some of the issues that are present in these systems. They should be required to maintain an updated version of the software for their customers. If there are known issues with these systems, they should be addressed immediately. If they are not, it can put more than just the inmates in danger. Guards are just as much at fault for any of the issues as the manufacturers. The same computer systems that are used to access control points are being used to check personal email or view social media websites (Zetter, 2011). The Programmable Logic Controller (PLC) is used in many prisons around the United States. This is a simple input/output system, which is controlled by four basic steps. These steps are input scan, program scan, output scan, and housekeeping. The same PLC systems that are used for vending machines and assembly lines are used for the design of cell doors (Zetter, 2011).

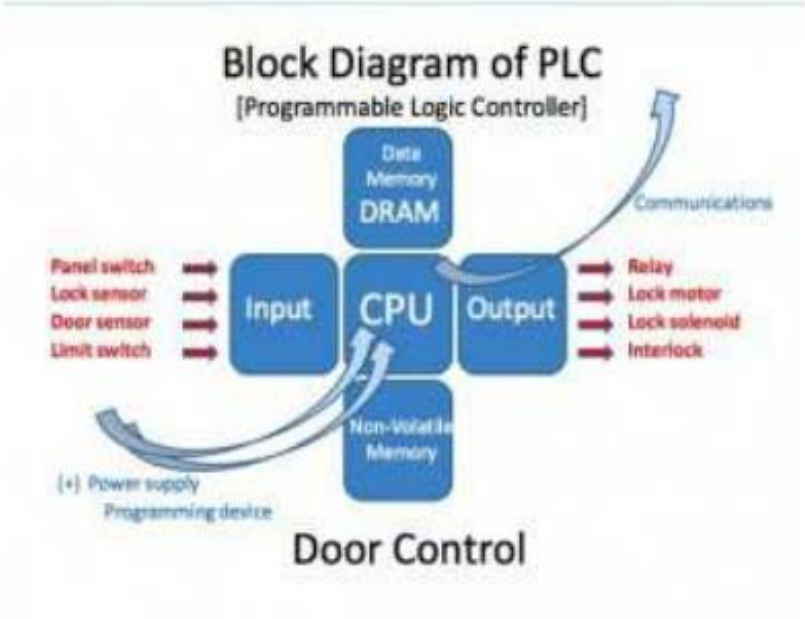

Figure 1. (Inmates Have Tried Many Ways To Break Out Of Prison: Chip Away At Concrete, Overpower Guards, Tie, n.d.)

Vulnerabilities

Public safety becomes an issue if outsider gain access to control the environment as inmates could easily find a way to escape. In California, a computer glitch released over 450 prisoners with high violence crimes (Inmates Have Tried Many Ways to Break out Of Prison: Chip Away at Concrete, Overpower Guards, Tie, n.d.). If an outsider assisted a group or wing of inmates, they would be able to gain control over the guards. If all of the inmates are released and the attacker opens the door to the guard headquarters, then the inmates would have no issues physically overpowering a group of guards. After the inmates gain access to the guard headquarter, they would then have physical access to all of the computers that control the prison. They would be able to release additional prisoners if they have not already done so. Once the prison is overrun, what would stop them from leaving the area with rifles and possibly shooting

innocent civilians? There have been multiple tests at DEFCON which show how vulnerable these systems are. In fact, a prison in Colorado allowed a group of prisoners to break the system in 2010. They called this the beta test, using nonviolent prisoners as a security liability and asset to empower the security systems (Luallen, 2011).

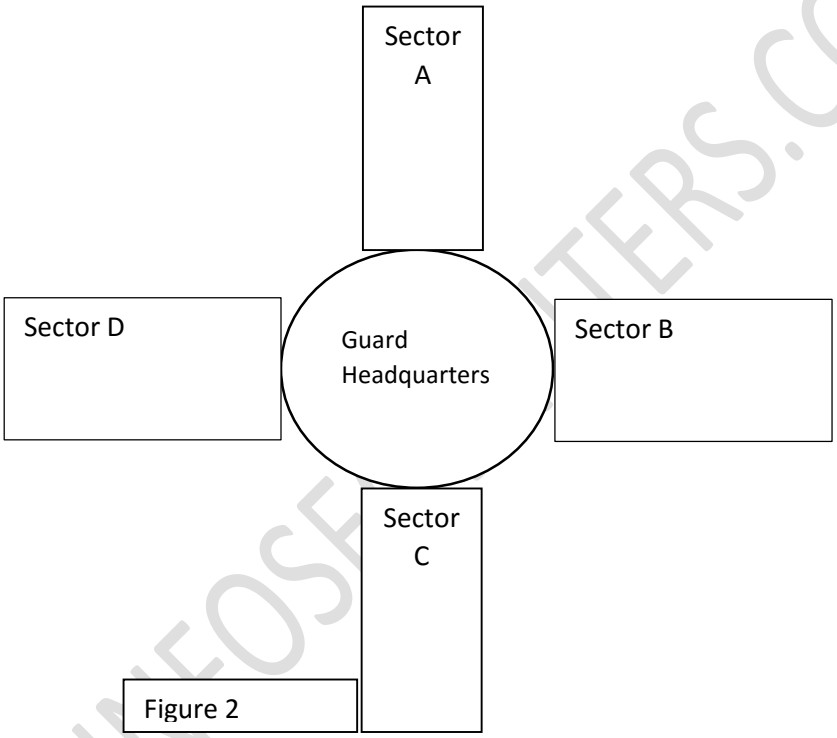

Figure 2

Honeypot and intrusion detection systems

One way we can prevent these issues would be by upgrading hardware and implementing high-interaction Honeypots. What this would do is provide a trap which would imitate the activities of the Access control point. This will allow the attacker to use a lot of the services on a virtual machine which is redirected to false locations. So this will give the attacker a false location to run commands and attempt to cause damage to the security system without actually having physical change to the prison. Even if the honey pot does fully get compromised it is on a

virtual side and can be recovered easily. We can implement more security from the cyber side with Intrusion Detection System (IDS), which allows the systems to detect and block any incoming attacks.

Summary

To keep up with the technology today, we need to keep upgrading the security systems. With how society is moving, cyber-attacks are becoming more frequent. Implementing a no-fault system would benefit the safety of prison personnel. This will lower issues when power surges happen or unauthorized commands are entered in the system. Also an increase in hardware technology can help implement a system that requires 2 guards to unlock a door via palm print that would be the safest way. We should not only rely on computers to do the work for us. There should be an emergency set of keys for each block to physically unlock the cell doors.

Conclusion

Security systems in our prisons have been over looked especially to cyber-security attacks. Being able to prevent these attacks can prevent more damage from happening. Knowledge on how these attacks work will help prevent them from the guard level. Focusing on the vulnerabilities of the security systems will allow manufactures to reduce the accessibility for the attacker, also we can not only rely on the manufacturers to fix all of the issues. This is where adding the honeypot detection system is just another line of defense to fight them. These are some of the most common reasons on why prisons are so vulnerable to Cyber-Security attacks.

References

Luallen, M. E. (2011, November). Critical Control System Vulnerabilities Demonstrated - And What to Do About Them. Retrieved November 11, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/critical-control-system-vulnerabilities-demonstrated-about-35110

Zetter, K. (2011, July 29). Researchers Say Vulnerabilities Could Let Hackers Spring Prisoners From Cells. Retrieved November 11, 2015, from http://www.wired.com/2011/07/prison-plc-vulnerabilities/

Inmates Have Tried Many Ways To Break Out Of Prison: Chip Away At Concrete, Overpower Guards, Tie. (n.d.). SCADA Hack Could Help Prisoners Escape. *SCADA Hack Could Help Prisoners Escape*. Retrieved November 11, 2015, fromhttp://rageuniversity.com/PRISONESCAPE/PRISON%20LOCKS%20AND%20KEYS/SCADA%20Hack%20Could%20Help%20Prisoners%20Escape.pdf