Security Analysis and Recommendations for a LoRa Relay Based Detonation System in Underground Mining

Pulkit Pannu
Student ID: 104093910
Swinburne University of Technology
Melbourne, Australia
104093910@student.swin.edu.au

***Abstract*— The deployment of a LoRa-based detonation system in underground mines has the potential to enhance both efficiency and safety by enabling a remote blasting system. However, these benefits come with huge security risks that needs be managed carefully. This report thoroughly identifies critical assets associated with the blasting system that could be impacted, such as mine workers, mine equipment, the detonation system itself, and the underground WiFi network of the mine. Utilizing a modified Delphi approach, the risks associated with each asset are calculated and evaluated. Based on this assessment, appropriate security policies are recommended for development, which include implementing strong authentication measures for all system communications, conducting frequent employee training and awareness drills and employing robust encryption techniques. By adopting this multi-faceted security approach, the mining operation can effectively address the identified risks and significantly improve its overall security stance.**

I. Introduction

LoRa, or Long Range, is a physical patented radio communication technique based on spread spectrum modulation techniques. It was developed by a French company named Cycleo, now Semtech, and was patented in 2014 [1]. LoRaWAN defines the communication protocol and system architecture which is now an official standard of the International Telecommunication Union (ITU) [1]. In the 2020 paper by P. Branch and T. Cricenti [2], their research and suggestion of using LoRa relay based detonating system in underground mines was reasonable due to the fact that LoRa and LoRaWAN together defines a low-power, wide-area networking protocol which can be used to wirelessly connect battery operated devices to the internet in the underground mines and establish bi-directional communication between different relays and IOT devices [1]. With this implementation of LoRa relays in underground mines, the threat and danger to individual miners can be decreased substantially as the distance between the explosive and the person initiating the detonation can be increased by enabling remote control of blasting processes.

However, the incorporation of such a system to the mining environment makes it vulnerable to threats and necessitates a thorough security assessment to prevent potential catastrophic failures, both accidental and malicious. As stated in the paper, the current system incorporates a PIN and simple streaming cipher as its only security features, which is inadequate for such an imperative system. Moreover, with the interest of connecting the system to the underground WiFi and initiating the blasts from the surface can pose more security threats and needs to be dealt with in a coherent manner.

This report aims to provide a detailed risk analysis by identifying key assets in the system and the risk associated with them, formulation of the security policy and the implementation of the security programme. The section II of this report looks at risk analysis, section III looks at policy formulation and section IV looks at the implementation of the security policy

II. Risk Analysis

Risk is a multi-factor measure. Information security is about risk management and managing the trade-off between security, functionality and cost. Meaning, the level of information security should be appropriate to the value of the information or loss its compromise might cause. Risk needs to be normalised by their likelihood and damage to the organisational assets.

Risk assessment is done by identifying the key assets associated with the organisation and their vulnerabilities.

A. Key Assets

1. PERSONNEL

In every mining industry, the safety of the miners is the first priority in any situation. Any malfunction in the detonating system could lead to catastrophe, resulting in sever injury and loss of life.

Hence, ensuring the safety of personnel is imperative to maintain the mining operations running and avoiding legal and financial ramifications.

2. UNDERGROUND EQUIPMENT

Reliable mining equipment are vital in any mining project to ensure the safety of the workers and reduce hazards. These equipment are very expensive and it is very critical to protect them from unintended damage from detonation system failures as the use of faulty equipment can lead to hazardous situations.

The number and rate of occupational mining fatalities [3] have significantly decreased due to the use of reliable mining equipment. Hence, keeping the underground equipment safe is important to prevent operational downtime and financial losses.

3. DETONATION SYSTEM

The blasting system, or the detonation system, in itself should be secure from physical and software damage. This is because if the blasting system is compromised, in one way or another, then it could lead to unauthorised or unintended detonations, risking the lives of personnel and equipment underground.

Hence, keeping the detonation system secure and reliable is very critical in the operational effectiveness of any mining project.

4. WIFI NETWORK

The proposal of connecting the system to an underground WiFi network to initialize blasts from the surface introduces additional security risks such as unauthorised access, data interception, message collisions, etc.

Wireless networks in underground mines also provide connectivity and improves communication between miners, ensuring worker's safety and equipment's efficient operation [4]. Therefore, securing the WiFi network from being compromised is a vital factor in the smooth undertakings of mining projects.

B. Associated Risk

To calculate the estimated risk associated with each asset we use the qualitative risk assessment method named the "Delphi Technique" [5]. Following is the risk assessment matrix considering the impact and likelihood of each risk.

1. RISK TO PERSONNEL

- **Risk:** System failure causing unscheduled detonations puts the health and safety of mine personnel in severe danger.
- **Impact:** 5/5 (Catastrophic) – Potential loss of life.
- **Likelihood:** 3/5 (Moderate) – Weak security policies, such as PIN and a stream cipher, increases the chance of system failure.
- **Total Risk:** 15

2. RISK TO UNDERGROUND EQUIPMENT

- **Risk:** Equipment damage due to unexpected detonation, rendering the equipment useless and costing large amount of money.
- **Impact:** 4/5 (Severe) – High cost of replacing expensive equipment because using defected equipment increases the risk of unfortunate incidents.
- **Likelihood:** 3/5 (Moderate) – Existing security measures are weak.
- **Total Score:** 12

3. RISK TO THE DETONATION SYSTEM

- **Risk:** Unauthorised access to the detonation system due to weak security measures.
- **Impact:** 4/5 (Severe) – Easily breakable PINs and stream ciphers can be vulnerable to an attacker with malicious intent.
- **Likelihood:** 4/5 (High) – Insufficient security protocols present in the current system which can be exploited readily.
- **Total Score:** 16

4. RISK TO THE WIFI NETWORK

- **Risk:** If the network is breached then the whole blasting system could be compromised and can be used to intercept data and potentially initialize unscheduled blasts.
- **Impact:** 4/5 (Severe) – The mining operations can be disrupted and can cause risk to the mine personnel's health and safety.
- **Likelihood:** 5/5 (Very High) – This is because wireless networks are inherently insecure and vulnerable to external threats.
- **Total Score:** 20

III. Policy Formulation

To address the risk associated with the key assets of the underground mining industry, we implement the following security policies.

1. ACCESS CONTROL

Policy: Any information available to a user is based on Role-Based Access control (RBAC) [6].

Justification: Restricting access of the system by setting permissions and privileges to enable access of particular information to particular authorised users can reduce the risk of unauthorised access of critical information and potential misuse.

2. AUTHENTICATION

Policy: High levels of multi-factor authentication (MFA) are associated with all the communications involving the detonation system.

Justification: The use of a blasting system is a critical task that requires the utmost precision and care, and should only be carried out by authorized personnel who have received proper training and are operating under strict guidelines. MFA adds an extra layer of security and reduces the risk of unauthorised access or an unintentional use of the blasting system.

3. ENCRYPTION

Policy: All communications should be encrypted by a standard encryption algorithm.

Justification: If the communications are not encrypted then an outsider listening on the network can seek to cause damage to the organisation by extracting all the sensitive information and using it against them.

4. PHYSICAL SECURITY

Policy: All the vital infrastructure of the blasting system is to be kept secure in tamper resistant enclosures.

Justification: Protecting the physical infrastructure of the blasting system with the control centre and the communication equipment is crucial to prevent physical damage by attackers.

5. INCIDENT RESPONSE

Policy: Every incident needs to be documented in a well developed Incident Response Plan (IRP)

Justification: Having a clear and comprehensive incident response plan in place allows the company to react swiftly and efficiently when security breaches occur, thereby reducing the potential damage and enabling a fast return to normal operations.

6. EMPLOYEE AWARENESS AND TRAINING

Policy: Regular security and risk awareness training will be undertaken by every employee.

Justification: By providing training to staff members on recommended security measures and common vulnerabilities, companies can equip their workforce with the knowledge and skills needed to identify and handle security issues properly, minimizing the chances of mistakes caused by human factors.

IV. Implementation of Security Policy

Security policies can be implemented in various different ways. In this section we take a look at the different ways of implementing the security policy mentioned in section III.

1. IMPLEMENTING ACCESS CONTROL

- Identifying and defining roles in the organisation and different privilege levels.
- Assign the permissions and access of the required information to each user on the basis of the Least Privilege Principle [7].
- Deploying an Identity and Access Management System (IAM) [8] to enforce RBAC. Solutions like AWS, Microsoft Azure AD or Okta can be used.
- Configuring IAM system for granting and revoking access based on role and employee status.

2. IMPLEMENTING AUTHENTICATION

- MFA is done using at least two factors from the following – hash based passwords, OTP, biometrics or mobile apps [9].
- For users with higher privileges, MFA from biometrics and passwords are recommended.
- To enforce MFA, technologies such as Google Authenticator, Duo Security or RSA SecureID Access can be used.
- For enabling seamless authentication for all applications and systems related to the detonation process, we can integrate MFA with the existing IAM system.

3. IMPLEMENTING ENCRYPTION

- AES-256 [10], which is a block cipher using SHA-256 hash algorithm, is used for the encryption of all communications.
- To ensure that the setup of individual AES session keys are encrypted, Elliptic-Curve Diffie-Hellman Key Exchange [11] is to be used.
- To manage all the session keys securely, we can deploy a secure key management system like AWS KMS or Azure Key Vault.

4. IMPLEMENTING PHYSICAL SECURITY

- Use of physical access control systems (PACS) [12] at critical entry points.
- 24/7 surveillance cameras can be used to monitor critical areas.
- Tamper detections systems technologies [13] can be used to keep enclosures with critical equipment safe and secure from physical harm.

5. IMPLEMENTING INCIDENT RESPONSE

- For handling security incidents, an incident response team with clearly defined roles must be formed.
- Development of a comprehensive IRP which states procedures and guidelines for detecting, analysing, removing and recovering from any incident.
- This IRP consists of all the communication plans, escalation processes and the contact information of all the stakeholders.
- Regular training sessions for incident response drills and updating the IRP based on the lessons learned.

6. IMPLEMENTING EMPLOYEE AWARENESS AND TRAINING

- Detailed training programs for staff members to educate them on topics such as phishing, social engineering, password security and incident reporting.
- Educating employees about e-learning platforms and security threats.
- Conducting phishing and social engineering attacks to test the awareness and readiness of the employee.

V. Summary

To summarise, the introduction of LoRa relay based detonation system in underground mining brought a lot of promise for an improved and secure way of performing underground blasting but it also brought forward the security threats associated with it. In this report we looked at

- Why the LoRa relay system was insecure,
- Risk analysis by identifying key assets associated with the blasting system,
- The Delphi technique to rank the associated risk with each asset,

- Forming policies based on the risk assessment and
- Implementing those policies through different techniques and technologies.

VI. References

[1] "LoRa", Wikipedia, (accessed Jun 05, 2024), [Online]. Available: https://en.wikipedia.org/wiki/LoRa

[2] Philip Branch, Tony Cricenti, "A LoRa Relay Based System for Detonating Explosives in Underground Mines", Swinburne University of Technology, 2020.

[3] "Number and rate of occupational mining fatalities by year, 1983 – 2022", NIOSH Mining. [Online]. Available: https://wwwn.cdc.gov/NIOSH-Mining/MMWC/Fatality/NumberAndRate

[4] GroundHog, "The advantages of having Wi-Fi in an underground mine", LinkedIn, 2023. [Online]. Available: https://www.linkedin.com/pulse/advantages-having-wi-fi-underground-mine-groundhogapps#:~:text=In%20an%20underground%20mine%2C%20communication,each%20other%20and%20the%20surface.

[5] "Delphi Method", Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Delphi_method

[6] "Role-Based Access Control (RBAC)", Imperva. [Online]. Available: https://www.imperva.com/learn/data-security/role-based-access-control-rbac/#:~:text=and%20Access%20Control-,What%20is%20RBAC,enable%20access%20to%20authorized%20users.

[7] "Principle of Least Privilege", Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Principle_of_least_privilege

[8] "What is identity and access management (IAM)?", Microsoft. [Online]. Available: https://www.microsoft.com/en-gb/security/business/security-101/what-is-identity-access-management-iam

[9] "Implementing Multi-Factor Authentication", Australian Government, 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

[10] "Advanced Encryption Standard", Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[11] "Elliptic-curve Diffie-Hellman", Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Elliptic-curve_Diffie–Hellman

[12] "Why physical access control systems are important for any security strategy", Avigilon. [Online]. Available: https://www.avigilon.com/blog/physical-access-control#:~:text=Also%20known%20as%20PACS%2C%20physical,you're%20protected%20from%20intruders.

[13] "Understanding Tamper Detection Sensors", Texas Instruments. [Online]. Available: https://www.ti.com/document-viewer/lit/html/SSZT372