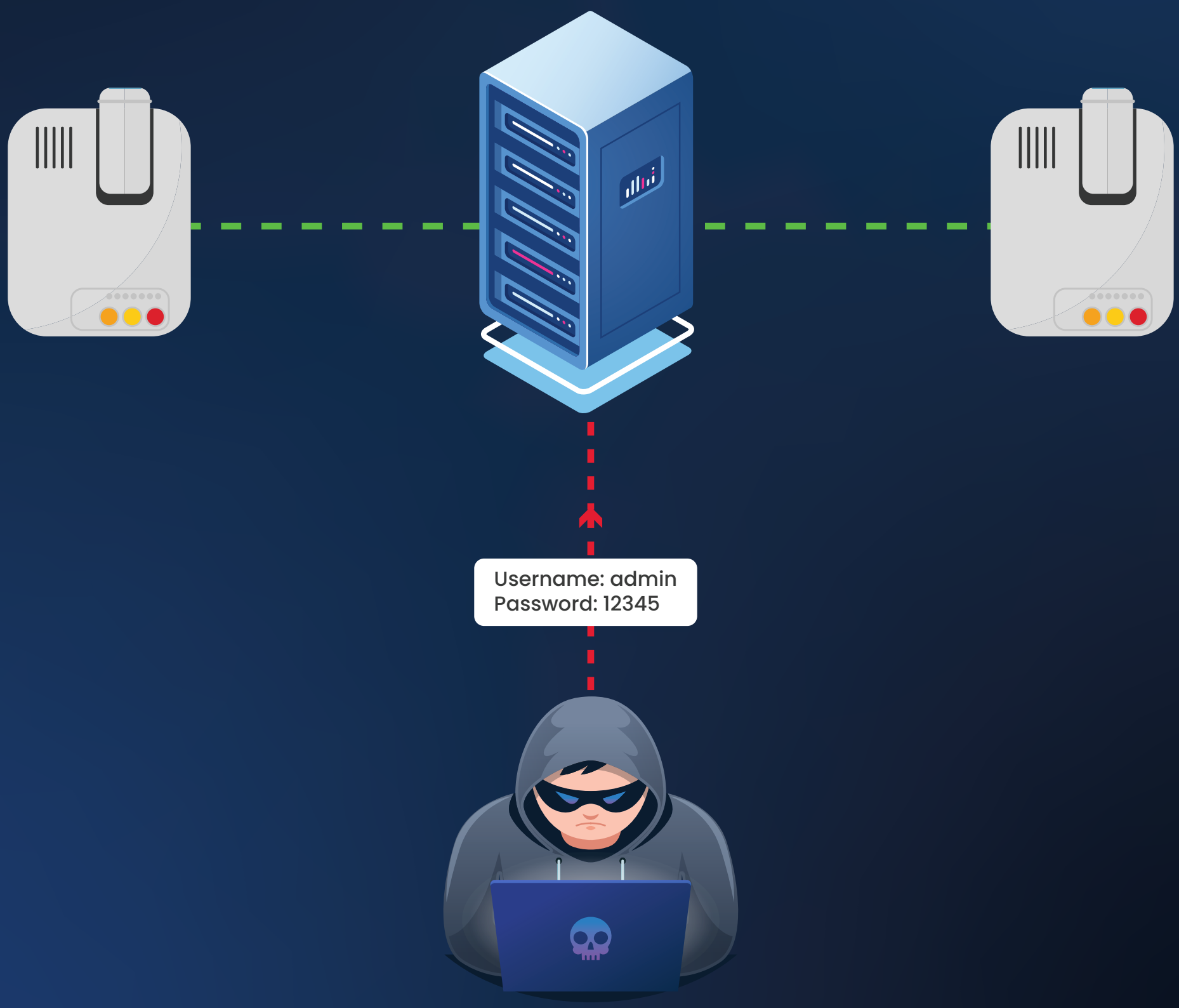
SECURITYBOAT
Frontline Of Your Business

MQTT DICTIONARY ATTACK

HANDBOOK



www.securityboat.net

SECURITYBOAT
Frontline Of Your Business

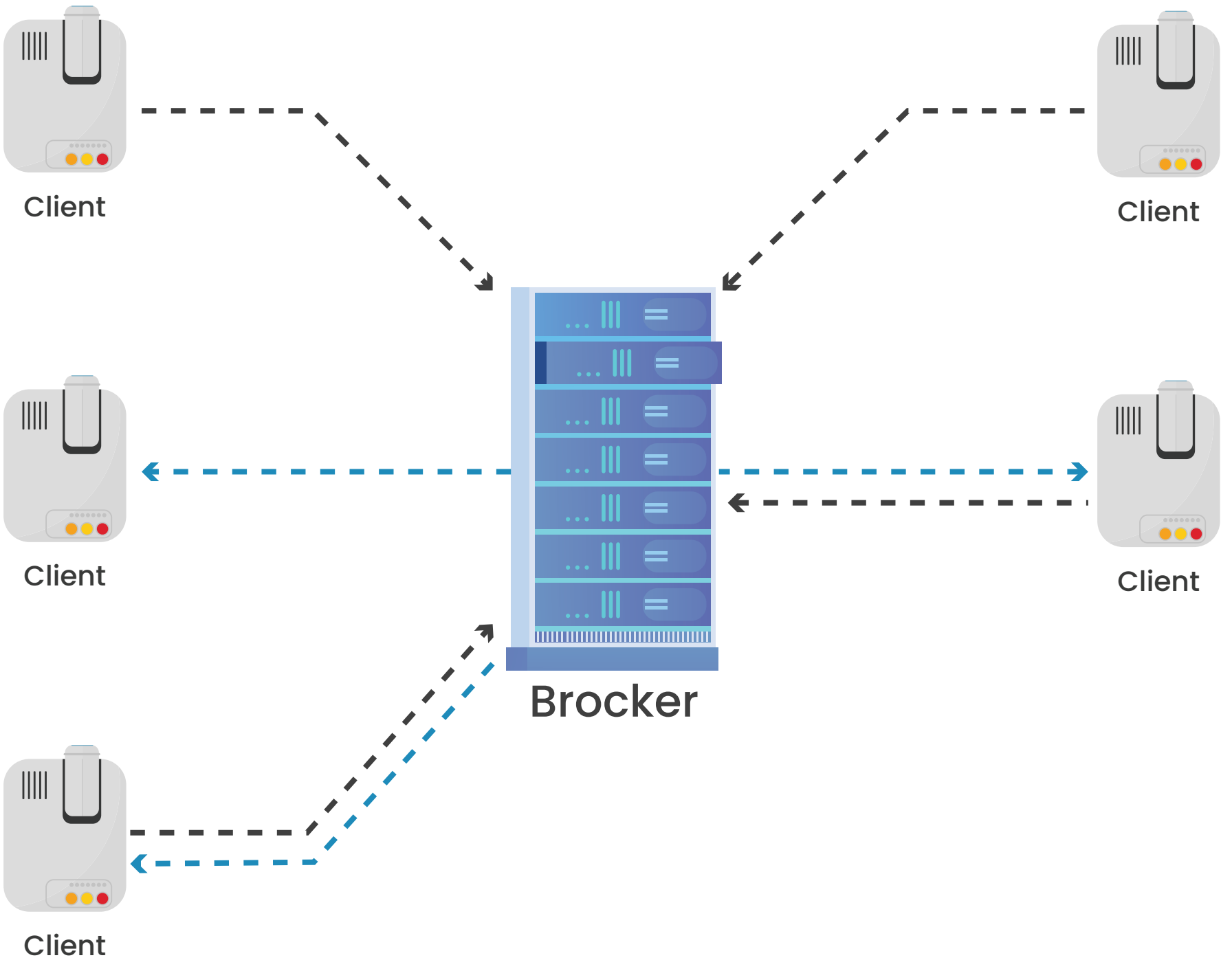
Table of Contents

1. What is MQTT? 01
2. What is MQTT Dictionar Dttack? 02
   2.1 Stages of MQTT Dictionary Attack 02
      2.1.1 Prepare Dictionary 02
      2.1.2 Connect to Broker 03
      2.1.3 Attempt Login with Each Combination 03
      2.1.4 Successful Login 03
      2.1.5 Exploit Access 03
3. Types of Dictionary Attack 04
   3.1 Brute Force Attack 04
   3.2 Wordlist Attack 04
4. Tools 05
   4.1 MQTT Pwn 05
   4.2 MQTTSA 05
   4.3 Hydra 05
5. Impacts 05
   5.1 Unauthorized Access 05
   5.2 Data Breaches 05
   5.3 Service Disruption 05
   5.4 Operational Downtime 05
6. Preventions 06
   6.1 Strong Password Policies 06
   6.2 Multi-Factor Authentication (MFA) 06
   6.3 Account Lockout Mechanisms 06
   6.4 Regular Expressions (Regex) 06
   6.5 Adaptive Authentication 06
7. QR Code 07

1. What is MQTT?

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol designed for small sensors and mobile devices. It is commonly used in Internet of Things (IoT) applications. This protocol allows devices to communicate by sending (publishing) and receiving (subscribing to) messages through a central server called a broker. Because MQTT uses minimal network bandwidth, it is perfect for devices with limited resources or for networks with low bandwidth.

MQTT operates over TCP/IP and uses a publish-subscribe model. In this model, clients connect to the broker, which handles the distribution of messages. Clients can publish messages to specific topics and subscribe to topics to receive messages that interest them. The broker manages these connections and ensures messages are routed to the appropriate clients.



2. What is MQTT Dictionary Attack?

An MQTT dictionary attack is a method where attackers try to gain unauthorized access to an MQTT broker, which is a server managing communication between devices. Attackers use a list of common usernames and passwords (a dictionary) to repeatedly attempt logging in. If the broker has weak security, the attacker might find a valid combination, allowing them to intercept, publish, or manipulate messages within the network.

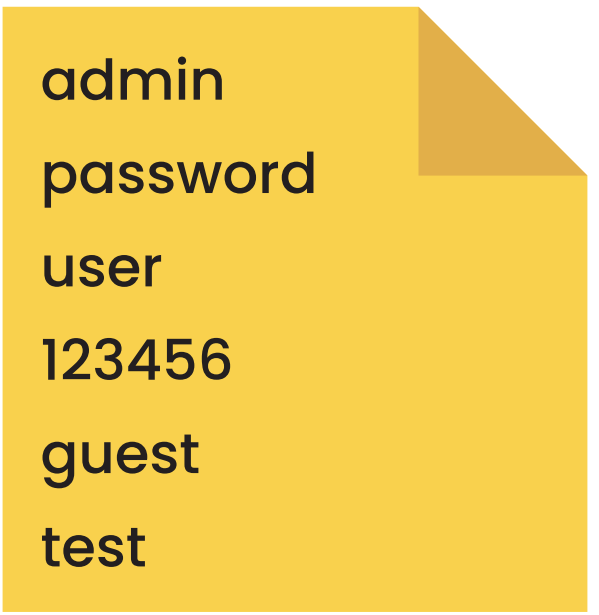
This attack involves automated tools that systematically try various username and password pairs from a precompiled list against the MQTT broker's login interface. These tools use brute force techniques to attempt each combination rapidly. Once valid credentials are found, the attacker can subscribe to or publish messages on the broker, potentially causing data breaches or disrupting the network. This type of attack exploits weak or default credentials, highlighting the importance of strong, unique passwords and additional security measures like account lockouts and two-factor authentication.

2.1 Stages of MQTT Dictionary Attack

Here is how the workflow of dictionary attack looks

2.1.1 Prepare Dictionary

The attacker prepares a list of common usernames and passwords, known as a dictionary.



Dictionary File

2.1.2 Connect to Broker

Using an automated tool, the attacker connects to the target MQTT broker.

```
$ mosquitto_sub -h broker.example.com -p 1883 -u user -P password -t "example/topic"
$ mosquitto_pub -h broker.example.com -p 1883 -u user -P password -t "example/topic" -m "Hello, MQTT!"
```

2.1.3 Attempt Login with Each Combination

The tool methodically tries each username and password pair from the dictionary.

```
[+] Starting brute force!
[+] Found valid credentials: root:123456
[+] Found valid credentials: admin:password
[+] Found valid credentials: dev:12345678
[+] Found valid credentials: user:1234
^C
[-] Brute force has stopped...
```

2.1.4 Successful Login

If the tool finds a valid combination, the attacker gains access to the broker.

```
mqtt-pwn >> connect -h broker.example.com -p 1883
broker.example.com:1883 >>
```

2.1.5 Exploit Access

Once inside, the attacker can subscribe to sensitive topics, publish malicious messages, or intercept communication.

```
>  mosquitto_sub -h broker.example.com -p 1883 -u attacker -P attacker_password -t "sensitive/data"
```

3. Types of Dictionary Attack

3.1 Brute Force Attack

In a brute force attack, the attacker systematically tries every possible combination of usernames and passwords to gain access to an MQTT broker. This method starts with simple combinations and progresses to more complex ones, using automated tools to speed up the process. Brute force attacks are resource-intensive but can be effective if the target has weak credentials or lacks security measures like account lockout after multiple failed attempts.

Example: Starting with simple combinations like "admin/password" and progressing to more complex ones like "admin/#$!@#$%". This approach continues until the correct credentials are discovered, allowing the attacker to gain unauthorized access to the MQTT broker.

```
[+] Starting brute force!
[+] Found valid credentials: root:1234
[+] Found valid credentials: root:123456
[+] Found valid credentials: root:12345678
[+] Found valid credentials: root:123456789
^C
[-] Brute force has stopped...
```

3.2 Wordlist Attack

A wordlist attack involves using a predefined list of commonly used usernames and passwords, known as a wordlist or dictionary. This method is more efficient than brute force because it focuses on trying likely combinations first. Attackers utilize automated tools to iterate through the wordlist, attempting each username-password pair against the MQTT broker. Wordlist attacks are effective against users who choose weak or easily guessable passwords.

Example: An attacker uses a list of common usernames and passwords (e.g., "admin" with "password") to systematically attempt unauthorized access to the MQTT broker.

```
[+] Starting brute force!
[+] Found valid credentials: root:123456
[+] Found valid credentials: user:98765
[+] Found valid credentials: dev:admin123
[+] Found valid credentials: admin:password
^C
[-] Brute force has stopped...
```

4. Tools

4.1 MQTT Pwn

A tool specifically designed for security testing of MQTT brokers, including dictionary attacks.
https://github.com/akamai-threat-research/mqtt-pwn

4.2 MQTTSA

Automatically detect misconfigurations in MQTT brokers, support dictionary attacks & provide reports in PDF format.
https://github.com/stfbk/mqttsa

5. Impacts

5.1 Unauthorized Access

Unauthorized access occurs when attackers successfully guess or crack passwords to enter systems or accounts. This can lead to them accessing sensitive information or performing actions they're not authorized to do, potentially compromising security.

5.2 Data Breaches

Data breaches happen when attackers gain access to and expose confidential or personal information stored on systems. This can include financial data, personal details, or intellectual property, causing significant harm to individuals and organizations.

5.3 Service Disruption

Service disruption occurs when attackers flood systems with multiple login attempts, overwhelming them and causing slowdowns or complete denial of service. This disrupts normal operations, affecting users' ability to access services or perform tasks.

5.4 Operational Downtime

Operational downtime results from compromised systems or services being unavailable due to successful attacks. This downtime can lead to lost productivity, revenue, and customer trust, impacting overall business continuity.

6. Preventions

6.1 Strong Password Policies

Implement strong password policies that require users to create complex passwords containing a mix of letters, numbers, and special characters. Regularly educate users on the importance of choosing unique passwords and avoid using easily guessable information like names or birthdays.

6.2 Multi-Factor Authentication (MFA)

Enable MFA to add an extra layer of security beyond passwords. With MFA, users must verify their identity using a second method, such as a code sent to their phone or email, in addition to entering their password. This greatly reduces the risk of unauthorized access even if passwords are compromised.

6.3 Account Lockout Mechanisms

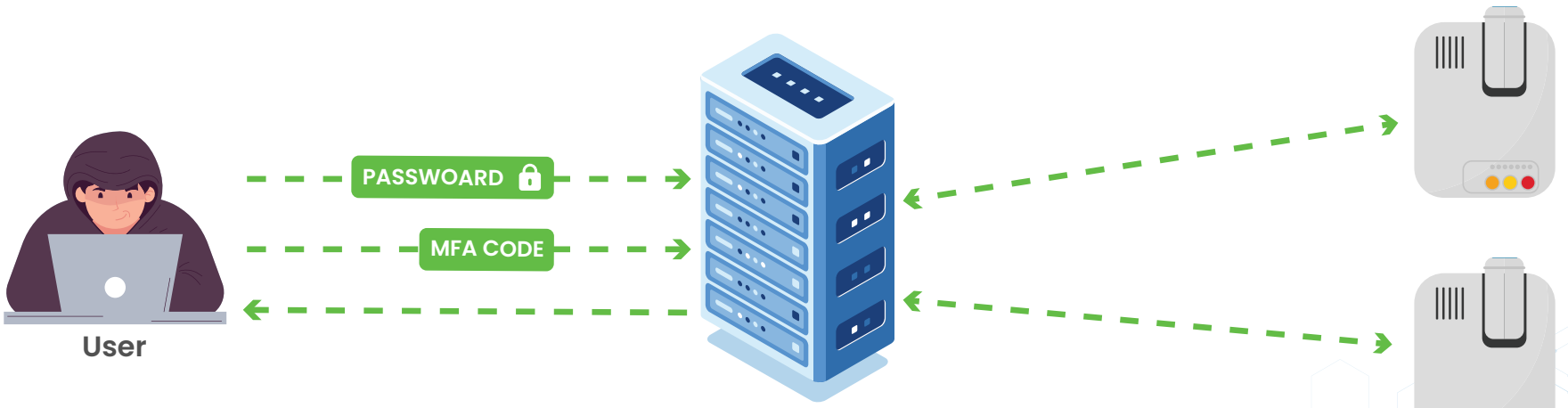
Implement account lockout mechanisms that temporarily lock user accounts after multiple failed login attempts. This prevents attackers from continuously guessing passwords and reduces the effectiveness of brute force or dictionary attacks.

6.4 Regular Expressions (Regex)

Utilize regex patterns to enforce strong password policies. This can include requiring passwords to meet specific criteria such as minimum length, inclusion of special characters, and avoidance of common dictionary words or predictable sequences.

6.5 Adaptive Authentication

Employ adaptive authentication mechanisms that dynamically adjust security measures based on risk factors such as login location, device type, and time of access. This ensures stronger authentication for higher-risk scenarios while minimizing friction for legitimate users.



SECURITYBOAT

Frontline Of Your Business

MQTT DICTIONARY ATTACK HANDBOOK

Scan QR Code to Download Handbook

www.securityboat.net