Information Sheet – Security – UK Government Code of Practice

Security can take many forms, but with the Internet of Things (IoT), concern exists for the accessibility of systems to outside influences. Whilst there are items with specific functions – such as Cameras, TVs, Wearable health trackers, there are also systems which provide a generic backbone to provide a variety of uses. The UK Government 2018 Code of Practice for Consumer IoT Security details guidelines covering:

1. No default passwords
2. Vulnerability Disclosure policy
3. Software Updates
4. Secure Storage of credentials and security sensitive data
5. Communicate Securely
6. Minimise exposed attack surfaces
7. Ensure Software Integrity
8. Ensure Personal Data is protected
9. Make systems resilient to outages
10. Monitor System Telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate Input Data

Whilst the Rayzig System is designed to work within the Light Industrial / Commercial sectors, it is possible it could be used in large domestic settings, so the guidelines have been considered in relation to Rayzig development.

The guidelines indicate principle concern exists for the first 3 items on the list. Rayzig has tried to ensure consideration for all aspects of the Code of Practice:

1. Within the Raymon software, which is used to setup and configure the network, each system will require Passwords to be set for specific user levels. These relate to the site, and whilst a recovery password is provided it is applicable to the specific system and not as a generic password. Within the Rayweb it is possible to define users and allocate specific limitations. These users can have passwords set, and are these are unique to that site.

   In the event of Utility Site Management facilities being setup, a specific Utility User and Password are set up between the Utility and Client. The password and access is controlled by the client.

   As some information is stored on an inbuilt Web-Server, it is essential that standard ports to access applications, and standard Ids are changed to prevent unwelcome access on the single board computer that is used.

These should include, but are not limited to:

Application	Port
MySQL	3306
HTTP	80
FTP	21/22
SSH	..

2. Vulnerability Disclosure Policy

   The draft Vulnerability Disclosure Policy is shown at the end of this Information sheet, along with details of the public PGP Key to allow secure notification to the email security@rayzig.com.

3. Software Updates

   The Software for the Rayzig system is developed in a number of sections, relating to the module and the micro processor being used. The general operational software is

   Raymon

   or

   Rayweb

   whereas there are a number of elements of firmware that may, from time to time, require update. These are:

   Rayzig

   Raxmega

   Raydal

   WBxMega

   TFT Display Flash.

   Raymon and Rayweb are the most likely to change. A Raymon update can be undertaken from within the Raymon software on the client site and this connects with an update server. The Rayweb software will be distributed to the client by secure email, or where agreed, a direct update from Rayzig to the Clients' web-server.

4. Secure Storage of credentials and security sensitive data

   Some data is stored on the Rayzig Gateway, and any transmissions are encrypted with a dynamically changing security key. A number of checksums are embedded within the data, and these are

encrypted as well. This will limit the possibility of spoofing data to gain access to the system, as well as making it highly unlikely to gain access to the system through brute-force or dictionary attacks as the key changes with every access to the system. It also varies from site to site and from user to user.

Within Rayweb, which is a Server Client based system minimal data is transferred to the client, with any sensitive data being held on the server. Cookies are not knowingly used and session variables are destroyed on ending a session.

5. Communicate Securely

Within the Raymon System all data transmission are encrypted, so that exposure of any data is minimised. However, communication to / from the system, if carried out over the internet, rather than an intranet, could carry some risk. Where possible the transmission of system sensitive data is minimised, and data is normally only available for the session of the user.

Some data is held with an embedded single board computer, which allows use of a web-server and mysql database. These secured at installation time, and the client should ensure that security is not compromised by releasing the details to authorised personnel only.

Normal recommendations for the system are such that appropriate firewalls and DMZ's are utilised to minimise exposure.

6. Minimise exposed attack surfaces

The Rayzig System, once installed, can operate within a closed environment, namely no external connection is needed. The principle security data is held within device in a number of elements, which are only assembled when used and some aspects are dynamically changed to ensure secure transmissions. The communication between the Rayzig System and the embedded single board computer is using I2C. The use of Raymon is via an Ethernet connection, which could be direct.

When using the Rayzig Site System, or the Rayweb Web-Server software, the Rayzig system is open to external connection, namely the system is connected to a WAN or LAN with external connectivity, the system is open to normal network security issues – such as open ports, un-used application, etc.

Recommendations as to system security and the potential exposure will be discussed with Associates, Clients and Customers.

7. Ensure Software Integrity

Distribution of any software should be accompanied by a CRC32, SHA1 or HASH5 to ensure the correct software is both distributed and received as part of any system update. The website contains details of the appropriate hash for the version concerned.

8. Ensure Personal Data is protected

   The Rayzig System does not specifically hold personal data. A Name can be entered into the User fields, whether this is an actual name or not, as long as it is unique, it is acceptable.

9. Make systems resilient to outage

   As Rayzig is designed to control electrical power, when there is no power the system can not operate. In the event of a power return, whether full or partial, the system will resume operations to a pre-set state – set by the user, for when power is restored.

10. Monitor System Telemetry Data

    All power output modules within the Rayzig System record details of activity (with up to 8K events being recorded), whether this is a power on, a command action, or a repower. These events can be checked from the Gateway and used to provide necessary data.

    It is not possible to check all telemetry data within the mesh, as at a low level, the modules are checking to see where the strongest signal may be before transmission, or finding a route around the system. The system also regularly checks to see if updates are available, and will ensure that any battery nodes have at least a designated power level. To record and report all telemetry would result in any data analysis being cumbersome, and in some instances pertinent data could be overwritten.

11. Make it easy for consumers to delete personal data

    As detailed in 8 above, no personal data need be held on the system. It is also an easy task for a designated person to delete any User or Password from the system, thereby stopping any activity with that Id and Password.

    System relevant data, which is seen as affecting the operation of the overall system can only be changed at the highest level of User. It is not available for a change by Administrator or User level personnel.

12. Make installation and maintenance of devices easy

    Any system which is dealing with mains electricity should only be installed and maintained by qualified personnel. It is recommended that this applies to Rayzig Mains modules. Other modules which are controlled by battery or 12v DC supply can be installed by a non-qualified user.

    The Rayzig Manual contains detailed descriptions of how to setup, install and maintain all modules. Some video ‘how to’ are available on the Rayzig website.

13. Validate Input Data

Where practicable, Rayzig configuration requiring user input is verified at point of entry, however, in certain instances putting a valid, but wrong, entry would result in a potential issue. This is a matter of 'finger trouble' which can not be validated to ensure no errors occur.

For more information, check out the Rayzig Website – Rayzig.com, where details of any vulnerabilities dealt with, current version numbers, hash values and other general information can be found.

For more information please contact:

Rayzig Limited
Ballalough House
Smeale Road
Andreas
Isle of Man
IM7 4JA

Email : Sales@Rayzig.com

Vulnerability disclosure policy

Protecting our systems, and data entrusted to us by our associates, clients and customers is integral to what we do.

We value the work done by security researchers in making the Internet a safer and more secure space, and have developed this policy using guidance from ISO 29147:2018

If you have identified a security vulnerability in our products, services or systems we would like to work with you to improve our systems. Please review this policy before attempting to test or report a vulnerability.

A security vulnerability is a weakness in a product, service or system that could allow an attacker to compromise the integrity, availability, or confidentiality of that product, service or system.

Reporting vulnerabilities

You can report **any** vulnerability you discover in our systems by e-mailing security@rayzig.com. More details on how to contact us, including how to secure your communications, are provided later in this policy.

In all cases, you **must**:

- **Respect our associates', clients' and customer' privacy.** Contact us immediately if you access anyone else's data, personal or otherwise. This includes usernames, passwords and other credentials. You must not save, store or transmit this information
- **Act in good faith.** You should report the vulnerability to us with no conditions attached
- **Work with us.** Promptly report any findings to us, stopping after you find the first vulnerability and requesting permission to continue testing. Allow us a reasonable amount of time to resolve the vulnerability before publicly disclosing it

And you **must not**:

-
- Exfiltrate data. Instead use a proof of concept to demonstrate a vulnerability
- Use a vulnerability to disable further security controls
- Perform social engineering
- Perform any testing of physical security
- Break the law, or any agreements you may have with Rayzig or third parties

Testing for vulnerabilities

If you want to actively test our systems for vulnerabilities, you **must**:

- Only test systems that are in scope of this policy. These are listed further down in this policy
- Use a test, or other non-production, environment if it is available to you
- Only test vulnerabilities using your own accounts, or accounts that you have permission to test with

And you **must not**:

- Perform testing likely to provide you with access to someone else's data
- Perform testing likely to delete, destroy or corrupt anyone else's data
- Perform testing likely to affect other users e.g. denial of service and brute-force attacks, spamming
- Use automated scanners/fuzzers
- Test systems not-in-scope of this policy

You can help us by:

-
- Providing the IP address from which you performed the testing so that we can view logs related to your testing.
- Clearly identifying your traffic, for example by including a unique custom HTTP header such as **X-Rayzig-CVD:<youremail@address>**
- Providing us with detailed information about the vulnerability to help us confirm it eg:
    - The URL of the product, service or system
    - If the vulnerability is in code that Rayzig distributes, the code element name and version number
    - A description of the vulnerability
    - The steps needed to reproduce the vulnerability, any proof-of-concept code
    - Any screenshots Details of the browser and OS used during testing
    - How you prefer to be contacted
    - Any current plans you have to disclose the vulnerability

What we'll do

Rayzig will:

- Respond to and acknowledge your report within seven calendar days
- Ask for any additional information we need to investigate your report
- Work with you to confirm the vulnerability, the extent to which it affects us, and let you know how long we think the vulnerability will take to fix. Our aim is to fix vulnerabilities within 90 days of confirmation
- Notify you when the vulnerability has been fixed
- Where appropriate, release information about the issue to our associates, customers, and clients, or the public to help others determine if they are affected by the vulnerability, and if so, what they need to do
- Review what went wrong and update our practices and processes to improve our products and services
- If you wish, acknowledge your assistance to Rayzig on this page

- Promise not to take legal action against you for accessing (or attempting to access) our systems as long as this policy is followed and you do not cause foreseeable harm
- Treat your report as confidential, treat your data according to our privacy policy, and not pass your personal data onto any third parties without your permission

There are some issues that we may not consider to be security vulnerabilities, but you can still report them to us. We will respond and inform you why we do not consider it to be a security vulnerability. These are largely non-exploitable vulnerabilities or configuration issues, eg:

- Missing security headers that may be best-practice but do not impact on the security of the system in this instance
- Support for older, but non-exploitable, protocols and cipher suites such as TLS 1.1.
- Fingerprinting/version detection
- Out of date software, with no exploitable vulnerability

Communicating with Rayzig

If you are worried about the confidentiality of information sent to Rayzig as part of this process, we recommend you send the information using PGP/GPG. Details of Rayzig's Public PGP key can be found here.

You may wish to report something to us entirely anonymously. We are happy for you to do this, but it may make it difficult for us confirm the vulnerability and acknowledge your efforts if we are unable to contact you. We may also fail to identify activity if you are anonymous, for example, if you do not wish to provide us the IP address used to test our systems.

Scope of the policy

This policy is under active development. We are using a limited scope to help us explore what works well and what does not. The scope of the policy will change over time.

Systems in scope

The fully qualified domain names of the systems within scope are listed below. Subdomains not explicitly listed are not in-scope. All systems within scope can be identified by the presence of security.txt within their web root, for example
https://rayzig.com/security.txt.

- Rayzig.com
- Test.rayzig.com

Systems not in scope

- All systems not explicitly mentioned as in-scope

If you are unsure as to whether a system is in scope, please contact us first**.**

Rayzig employees and contractors

If you are a Rayzg employee or contractor, use the internal process for reporting incidents, not this external process.

We would like to encourage you to work on security problems that cannot be addressed externally and ensure that your efforts are recognised by our performance management system. For more information contact the information security team.

Hall of fame

Rayzig would like to thank the following people for helping improve the security of our products, services, and systems:

..

..

..

PGP Public Key Block

----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEXjA+ZhYJKwYBBAHaRw8BAQdAz7g0ES1pOBuL359KG/5pQrD1d6iSSK0P8IWJ
2s7hH3+0HlNlY3VyaXR5IDxzZWN1cml0eUByYXl6aWcuY29tPoiWBBMWCAA+FiEE
cbZq6DBm6VuPzHdoZ9jQ96B7sfAFAl4wPmYCGwMFCQlmAYAFCwkIBwIGFQoJCAsC
BBYCAwECHgECF4AACgkQZ9jQ96B7sfBF2QD/XA4qN8BmMDTN0j7UgkS64KWLgeIt
mm6m979Rd7161tcBAKNkdIX6hNNpxG1PhVlTMeZIo7afJSERxlZpb+++GbUNuDgE
XjA+ZhIKKwYBBAGXVQEFAQEHQIozGUxFlal3XxG4aeOYXJClaoDWYwOQmMi/Qv3q
wUAPAwEIB4h+BBgWCAAmFiEEcbZq6DBm6VuPzHdoZ9jQ96B7sfAFAl4wPmYCGwwF
CQlmAYAACgkQZ9jQ96B7sfA7YAEAusN74Px8X0Lu2S24VvOm4Zswz/9pHeAeRA/l
Jw0EMU8BAO8LD/RW8/fHEFWlbRK62DCHTf4F/Wkz6q1ytvtKRgkL
=x8O5
-----END PGP PUBLIC KEY BLOCK-----