RoweBots Limited

Software Data Sheet

Unison RTOS version 5.3

Ultra tiny embedded Linux™ or POSIX™ compatible RTOS

Unison and

System Security

www.rowebots.com

Secure Systems

Secure systems are paramount in modern societies and small systems are no less vulnerable than larger systems. The security approaches taken within Unison are as follow:

- Encrypted passwords using approved algorithms.
- SSL/TLS 1.2 to secure data transfers at a session level.
- IPSec to build virtual secure networks.
- SSH server support for secure system access and file transfer.
- SFTP secure file transfer.
- Radius client.
- Power on self test with flash trip wire checking (secure boot).
- Over the internet upgrades with integrity checking.
- SNMP v3 to protect data through encryption either locally or as it is about to be transferred to another machine.
- SMTP
- HTTPS
- Encrypted file system
- IP filtering

Each of these areas will be discussed in turn.

Encrypted Passwords

First, Unison encrypts all passwords using standard security algorithms. As a first line of defense, to ensure a safe system, users can be sure that passwords measure up to high quality standards.

SSL/TLS 1.2

By adding session level encryption on data sent over sockets, users can rest assured that their critical data is protected using strong, industry standard encryption. The typical encryption algorithms used include the following:

Symmetric Key Algorithms for Large Data Encryption
- AES
- 3-DES
- RC4

Asymmetric Key Algorithms for Public Key Private Key Encryption
- RSA

Hash Algorithms for data checking
- MD5
- SHA-1

SSL/TLS uses public key encryption to authenticate the server to the client, and optionally the client to the server. Public key cryptography is also used to establish a session key. The session key is used in symmetric algorithms to encrypt the bulk of the data. This combines the benefit of asymmetric encryption for authentication with the faster, less processor-intensive symmetric key encryption for the bulk data. This is ideally suited to smallermicrocontroller (MCU) usage.

SSL uses a MAC or hash function in early versions while the converged SSL/TLS used an HMAC. Today, these two approaches have converged. The HMAC approach adds a secret key to the message which is then hashed, which adds additional security.

Hardware accelerators are sometimes available within the MCU hardware. When available, the on board security hardware is utilized.

Other protocol layers are used on top of SSL/TLS to provide other services as shown in the figure. SSL/TLS only supports TCP and does not support UDP.

SSL/TLS is a layered protocol on top of TCP/IP and runs at the session layer. The handshake layer ensures server and optionally client authentication using X509, the cypher spec allows selection of bulk transfer algorithms with shared keys and the record layer transfers bulk encrypted data. Alerts indicate status or error conditions.

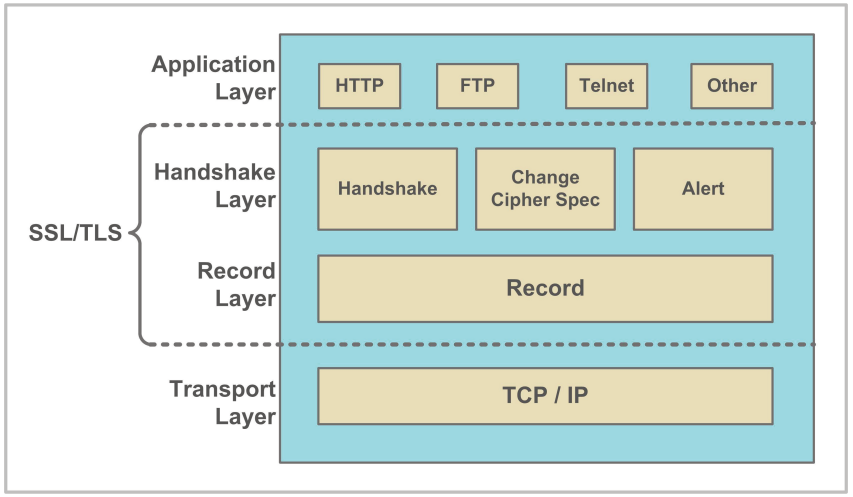

Figure 1: SSL / TLS Layers

IPSec Tunneling Protocol

As an integral part of the mixed IPv4 and IPv6 protocol stack for Unison, IPsec support is offered to allow users to build virtual private networks with strong encryption. It is embedded in the stack providing encryption on all data going over the link.

IPSec used the same approach as SSL/TLS although it may have a preshared key. Typically systems rely upon SSL/TLS because it is simpler to setup and maintain. For long term use of a broad set of applications, a VPN is superior though. Here is a simple comparison table.

Function	IPSec	SSL/TLS 1.2
Configuration	Hard	Easy
Client Authentication	Must	Optional
Pre-shared Key	Yes	No
Interoperability Problems	Yes	No
TCP Application Support	All	Some
UDP Support	Yes	No
Throughput	High	High
Handshake Time	Slow	Fast

SSH (Secure Shell)

SSH is a secure shell utility program which comes as a host component and a server component. Users interact with the host component and the server side provides results. It allows users to talk to remote systems using strong encryption without concerns about being hacked.

SFTP - Secure File Transfer Protocol

SFTP is a protocol which provides secure file transfer. Program such as FTP pass data and passwords in the clear. SFTP is completely secure but does require SFTP support at both ends.

Radius Client

A Radius client is available to support authentication using a Radius server. No Radius server capabilities are available in Unison. The Radius client is a minimal size and has a minimal feature set.

Power On Self Test (POST)

Power on self test solutions are used to ensure that the processor is working properly and the memory is good before the system is started. By adding checks on the flash contents which are masked in the flash image before starting, additional protection related to overloading of unsafe programs is added. Digital signatures could be added if very strong protection is required.

Remedy Bootloader Upgrades

Hand in hand with the POST checking, checks on updated images over the internet can be performed. Standard checks are currently used but upgrade checks including complete digital signatures are easily added and utilized.

Subsequent to file transfer, a public key can be used to decrypt the digital signature and check the integrity of the downloaded S-record or Hex file. With this approach, new downloads are ensured correct before files are programmed into the flash.

SMTP

SMTP - simple mail transfer protocol security is often enhanced using secure transmission using TLS or a VPN to the mail server. This is sufficient if the data is not sensitive; however, if the data is very sensitive, this is insufficient because the information is in the clear on the mail server. Using a separate encryption scheme with a shared key or a public key / private key crypto system for both signatures and decryption will ensure that messages can be authenticated and kept secret.

HTTPS

HTTPS is the secure version of the HTTP protocol. It is based on TLS encryption and ensures that the channel over which data is sent is encrypted. This is a typical method used to secure web financial transactions.

Encrypted File System

Encrypted file systems are required to secure information to prevent lose when physical access is possible and other methods of securing the data fail in some way. By ensuring that the file system encrypts the data on and off the media, the data can be protected even if the device is stolen or lost or other protection systems fail.

IP Filtering

Most important of all means to protect most devices is the ability to have a firewall or to do IP filtering. By rejecting all packets that not part of the normal operation of the system, many problems can be eliminated before they start. This is the first line of defense to stop intruders.

The Unison OS offers a comprehensive security system. From the above list, the interdependence of these features and how they work together to ensure the system is secure is paramount. Security cannot be an after thought - it must be designed in and all bases must be covered.

Software Version

- Unison 5.3

Availability

- Encrypted Password
- SSL/TLS
- IPSpec
- SSH
- Radius Client - Beta
- Remedy Bootloader
- Remedy POST
- SMTP
- HTTPS
- Encrypted File System
- IP Filtering

Additional Information

Other seperately available RoweBots files for Unison OS:

- File Systems
- Remedytools
- Wireless
- USB
- IoT or M2M Communication
- Internet Protocols
- Unison for Specific Processor Families

Contact: sales@rowebots.com
+1 519 279 46 00

RoweBots Limited