Keeping SCADA Networks Open and Secure

DNP3 Security

June 2008

DNP3 Protocol

DNP3 protocol has become widely accepted within water and electrical utilities worldwide for SCADA communications with field equipment. One of the reasons for its acceptance is because it is an open protocol. This allows manufacturers to supply equipment to utilities which can be easily integrated into their SCADA systems.

However, DNP3 was never designed with security in mind. Since it is an open design, anyone familiar with the protocol could launch an attack on a SCADA system. This is especially true when the protocol is used over radio networks where packets can be intercepted with a scanner.

In recent years, regulatory bodies have taken an increasing interest in the security of public infrastructure. The threat of terrorism attacks are taken particularly seriously. SCADA communications networks are of particular concern since they often control essential services such as sewerage, water and electrical supplies to the community.

The DNP3 community has recognized the need for secure SCADA communications and have developed a security model for the protocol with the following goals:

- Provide both authentication and message integrity
- Low overhead
- Supports remote key management
- Built into DNP3 at the application layer
- Compatibility with all DNP3 supported communications links

The security protocol specification is currently being finalised and is expected to be submitted to the DNP3 Users Group for review in the second quarter of 2008. It is expected to be approved and released shortly thereafter.

Implementations of secure DNP3 are already becoming available, and MultiTrode is at the forefront of this push. The MultiSmart Pump Station Manager includes secure DNP3.

MultiTrode has chosen to implement the new standard as early as possible because water and wastewater utilities are already demanding security within communications networks.

Figure 1 – MultiSmart Pump Station Manager

Proprietary Protocols vs. DNP3 Security

A common perception is that proprietary protocols are inherently secure because their design is not open. Unfortunately this assumes the protocol is not easily reverse engineered. Security measures that may exist in proprietary protocols cannot be independently verified for their robustness. Assuming a proprietary protocol is secure to the level required is therefore a leap of faith.

DNP3 Security is implemented within the protocol itself. Proven industry standard authentication methodologies are employed which can be investigated and verified independently. This approach is to be preferred when placing the security needs of civil infrastructure in a particular protocol.

How Secure DNP3 Works

Secure DNP3 is designed to eliminate the risk of messages being either falsified, or intercepted and repeated by a third party. Both scenarios could result in extensive damage to equipment and disruption of services if carried out correctly.

According to the draft specification, the following security threats are addressed by the protocol:

- Spoofing
- Modification
- Replay
- Eavesdropping - on exchanges of cryptographic keys only, not on other data.
- Non-repudiation – to the extent of identifying individual users of the system

Secure DNP3 secures against these threats by providing both authentication and message integrity. It does not encrypt the messages, but does use key encryption to keep session keys secure.

Secure DNP3 uses a “Challenge – Response” method to verify the message is originating from a valid source. The implementation is based on the proven “Challenge-Handshake Authentication Protocol (RFC 1994)”.

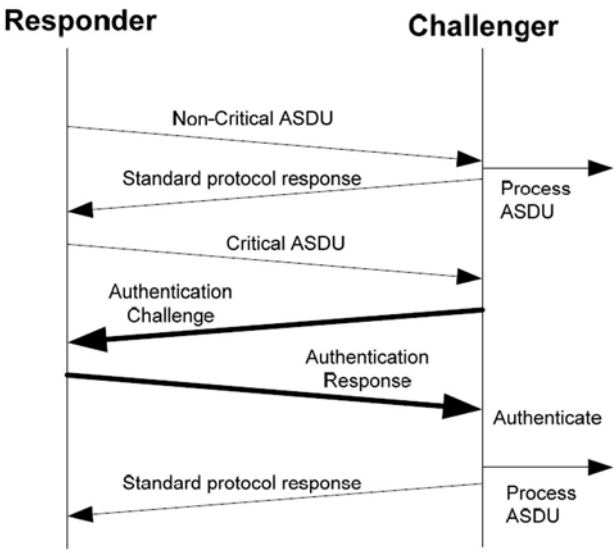

Figure 2 – Challenge Response Process

Either side of the link can initiate an authentication challenge. This can be at initialisation, periodically or when a critical function is received. An authentication response is then sent.

The authentication challenge contains some pseudo-random data, a sequence number and the required algorithm. The response contains a hash value generated from the challenge data and the key. The sequence number is also returned.

If the authentication response is valid then the challenger will respond to the original DNP3 message with a standard protocol response.

The Challenge-Response method above adds to the required communications bandwidth. If bandwidth is at a premium, a simpler authentication method can be used instead. "Aggressive Mode" reduces the required bandwidth by eliminating the normal challenge and response messages. The authentication data can also be included at the end of the DNP message. This mode is slightly less secure.

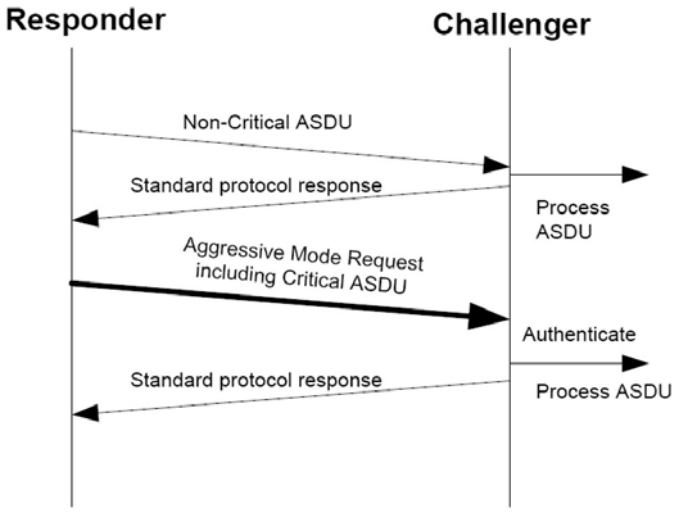

Figure 3 – Aggressive Mode

Key Management

Secure DNP3 uses minimum 128 bit AES encryption to keep keys secure. There are two types of keys - temporary session keys and update keys.

Session keys are initialised at start-up and then changed regularly approximately every 10 minutes.

Update keys are used to encrypt the session keys. These are pre-shared at either end of the link so they never need to be transmitted.

Summary

The addition of security measures to the DNP3 protocol is important for SCADA communications networks operating over easily intercepted mediums such as radio. Threats such as message interception and repeating are effectively handled by implementing secure authentication within the application layer of the protocol itself.

Using DNP3 Security allows an organisation to benefit from using an open, accepted, protocol without the need to use proprietary protocols from one vendor.

For more information on MultiTrode's range of products, visit their website at www.multitrode.com

References

DNP3 Specification, Volume 2, Supplement 1, Secure Authentication. Version 1.00, 3rd February 2007.