SENA

Network security for device servers

Kumar Nandi
Marketing Manager
Sena Technologies
(408) 262-6762

Device servers deliver the appropriate network connection and physical interface for industrial device applications. Providing this function in a secure fashion is becoming a major concern for industrial IT managers as burgeoning numbers of industrial devices receive a real or proxy Ethernet connections. Security-related features have become one of the main factors in device server selection.

The ability to manage industrial and manufacturing equipment remotely is a top priority and information security has become a major concern. The security process requires that a number of attributes should be applied to information in transit and storage.

The first of these is confidentiality: Information should not be understood by anyone for whom it was unintended. Integrity: Information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected. Non-repudiation: The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information; Authentication: The sender and receiver can confirm each other's identity and the origin/destination of the information.

Maintaining strong security requires a suitable architecture for the security system, and to make and enforce strict operational rules for all personnel in using or administering the system. In real-world applications, no rule, mechanism or device alone can maintain information security. User authentication, data encryption, network packet filtering, physical access control, system logging, and quick alarm notification are some of the mechanisms available to preserve information security. Every mechanism has a very specific area of protection which is really only effective when taken in combination with other measures. We need to apply all of these in a layered manner:

* Only authorized personnel should manage system administration;
* The data stream should only be visible where it is required to be so;
* Only the host from the proper address should have a right to access the system;
* All activity should be logged for future analysis/prevention purposes;
* Abnormal activity should be notified quickly to the appropriate administrator.

Intensive introduction of the network technologies in the industrial world makes the information security more important than ever. The security of the factory floor is more

significant in that damage to one device may affect other devices or the system connected to the network cluster.

While most security measures envisage protection against malicious activity – hacking, virus attacks, data theft and similar things – problems more often occur when unauthorized, untrained or unfamiliar plant personnel attempt access on the system for apparently legitimate reasons. The system should only allow access on terms appropriate to the personnel involved.

Device server security support

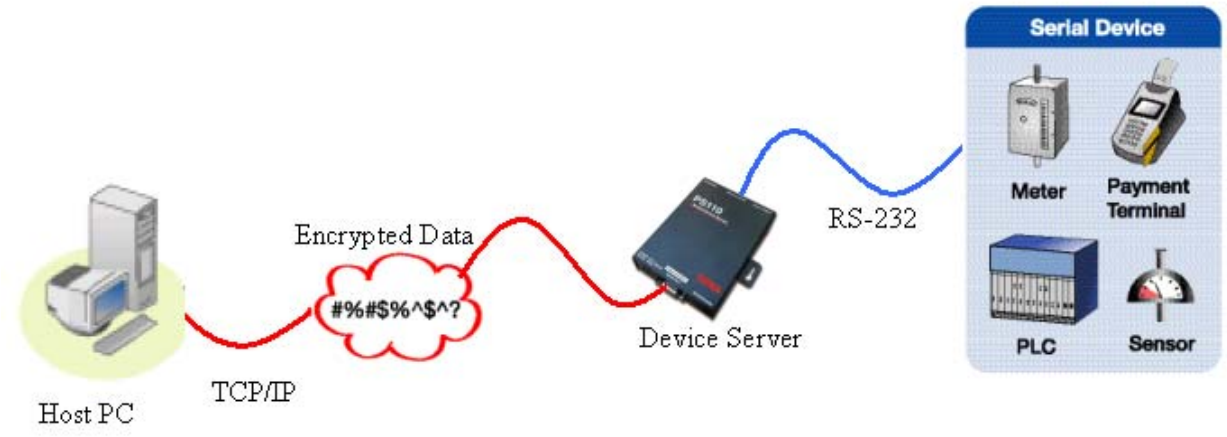
Device and terminal servers frequently connect through the Internet exposing serial device data to security risks. To keep data streams secure, it is important to use data encryption to achieve the highest level of security.

Device servers should support user authentication, i.e., the positive verification of the identity of a user or device in a system, often as a prerequisite to allowing access to system resources.

Device servers should also provide an IP address filtering function to deny inappropriate data streams forward transmission over the network. Most network traffic is based on TCP/IP for both the Internet and corporate intranets. However, the original Internet Protocol (IP) failed to define any structures for security, so application layer implementations, such as Secure Sockets Layer (SSL) and Secure Hypertext Transfer Protocol (S-HTTP) have been used to provide data security over the Internet.

Device servers can support encryption protocols such as SSL for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is to be transferred over the SSL connection.

Additionally, HTTPS provides for secure data transfer over the web, SCP for secure file transfer, while IP filtering controls access to serial devices.



Basic application showing transport of encrypted serial device data over a plain view network by using a secure device server

Secure tunneling:

==========

Serial tunneling occurs when two secure device servers are configured to work together to share or communicate their respective serial device data. The serial tunnel is established by connecting one device server configured for Server/Client mode to a device collecting data, and the other device server is configured for Server/Client mode to the field device sending data. This allows two previously non-networked and isolated devices to communicate information over a network rather than achieving the same thing by using a long serial cable.

Secure modem emulation:

==========

Modem emulation technology enables a networked device server to act as a modem to send and receive data over an IP network instead of using the public telephone network. If you then add the SSL encryption capabilities of high-end device servers this feature can provide secure serial modem emulation – including the use of AT commands – in an encrypted format to connect and communicate with serial devices. In short, modem emulation enables a networked device server to act as a modem to send and receive data in an encrypted format over an IP network instead of via PSTN.

Secure port data logging:

==========

Port Logging feature of device servers allow user to keep serial and TCP data safely in data storage locations such as NFS Server, Syslog server, internal memory and PC card Flash memory.

Future developments:

==========

Changes in the office-computing environment seem to spread rapidly into the various industrial sectors – and the measures developed for information security are no exception. Administrators should make a decision as to whether they really need a secure communication system taking into account the extra cost. The correct thing to do may be to establish security based turning the whole network infrastructure over to a secure VPN. Alternatively they might zone the system selectively by adding security to the device servers on the front-end of the devices.

The most important thing that administrators should keep in mind is that defensive strategy works, prevention works as do in-time alarms. All of these should be harmonized to design and manage a security system. However, it is not only the key components of the system that matter, but also the management process behind the running of the system.