Encryption and Its Importance to Device Networking

Lantronix, Inc.
15353 Barranca Parkway
Irvine, CA 92618
Tel: +1 (800) 422-7055
Fax: +1 (949) 450-7232
www.lantronix.com

Contents

Introduction

The role of computers and networks in our everyday lives has made protecting data and adding security an important issue. Most data transmitted over a network is sent in clear text making it easy for unwanted persons to capture and read sensitive information. Encryption algorithms protect data from intruders and make sure that only the intended recipient can decode and read the information.

Encryption is simply the translation of data into a secret code, and it is considered the most effective way to ensure data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Modern encryption is achieved using algorithms with a “key” to encrypt text or other data into digital nonsense and then decrypting it by restoring it to its original form.

Until 1996, the U.S. government considered anything stronger than 40-bit encryption a “munition” and its export, therefore, was illegal. Most government restrictions have now been lifted with 128-bit cryptography emerging as the new digital standard.

What is Encryption?

Encryption is a formula used to turn data into a secret code. Each algorithm uses a string of bits known as a “key” to perform the calculations. The larger a key is (the more bits in the key), the greater the number of potential combinations that can be created, thus making it harder to break the code and unscramble the contents.

Cryptography

Cryptography is the practice of encoding data so that it can only be decoded by specific individuals. A system for encrypting and decrypting data is a cryptosystem. These usually involve an algorithm for combining the original data ("plaintext") with one or more “keys” - numbers or strings of characters known only to the sender and/or recipient. The resulting output is known as “ciphertext”.

The security of a cryptosystem usually relies on the secrecy of the keys rather than the supposed secrecy of the algorithm. A strong cryptosystem has a large range of possible keys so that it is not possible to just try all possible keys. A strong cryptosystem will produce ciphertext which appears random to all standard statistical tests and can resist all known methods for breaking codes.

Keys

A key allows the encrypted secret code to be decrypted or allows plaintext (data that can be read by anyone) to be encrypted. There are typically two types used with data encryption--secret keys and public keys.

Common Types of Encryption

There are two main types of encryption: asymmetric encryption (also known as public-key encryption) and symmetric encryption. There are many algorithms for encrypting data based on these types. Some of the most common are listed below:

- Skipjack – uses an 80-bit key and was designed to run on "tamper-proof" hardware.
- Data Encryption Standard (DES) – uses a 56-bit key to encrypt the data. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours.
- Triple-DES – uses three successive DES operations to provide stronger encryption than DES. The algorithm is believed to be practically secure, although it is theoretically susceptible to some attacks. In recent years, Triple-DES has been superseded by the Advanced Encryption Standard (AES).
- Advanced Encryption Standard (AES) – also known as Rijndael, it can use 128, 192 or 256-bits to encrypt and decrypt data in blocks of 128-bits. As of 2004, there have been no successful attacks against AES.

Secret Key (Symmetric) Encryption

Using the same secret key to encrypt and decrypt messages. The problem with this method is transmitting the secret key to a legitimate person that needs it. Examples of systems that use this technique include:

- **Data Encryption Standard (DES)** - an encryption algorithm that operates on 64-bit blocks with a 56-bit key.
- **International Data Encryption Algorithm (IDEA)** - an encryption algorithm that operates on 64-bit blocks with a 128-bit key.

Public Key (Asymmetric) Encryption

This encryption type gives each person a pair of keys (a public key and a private key). Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his private key. This method eliminates the need for the sender and the receiver to share secret information (keys) with a secure channel. All communications use only public keys, and no private key is ever transmitted or shared. Examples of systems that use this type of technique include:

- **RSA** - used for both encryption and authentication.
- **Pretty Good Privacy (PGP)** - mainly used to secure email.

The longer the "key", the more computing required to crack the code. For example, using the now industry standard 128-bit encryption key, it would be 4.7 sextillion (4,700,000,000,000,000,000,000) times more difficult than cracking a 56-bit encryption key. Given the current power of computers, a 56-bit key is no longer considered secure whereas a 128-bit key is.

To implement public-key encryption on a large scale, such as a secure Web server might need, a digital certificate is required. A digital certificate is basically a bit of information that says that the Web server is trusted by an independent source known as a certificate authority. The certificate authority acts as a middleman that both computers trust, and confirms that each computer is in fact who it says it is, and then provides the public keys of each computer to the other.

WEP

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs) which are defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN, however LANs provide more security by their inherent physical structure that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the data link and physical layers of the OSI model and does not offer end-to-end security.

WPA

Supported by many newer devices, Wi-Fi Protected Access (WPA) is a Wi-Fi standard that was designed to improve upon the security features of WEP. WPA technology works with existing Wi-Fi products that have been enabled with WEP, but WPA includes two improvements over WEP. The first is improved data encryption via the temporal key integrity protocol (TKIP), which scrambles keys using a hashing algorithm and adds an integrity-checking feature to ensure that keys haven't been tampered with. The second is user authentication through the extensible authentication protocol (EAP). EAP is built on a secure public-key encryption system, ensuring that only authorized network users have access. EAP is generally missing from WEP, which regulates access to a wireless network based on the computer's hardware-specific MAC Address. Since this information can be easily stolen, there is an inherent security risk in relying on WEP encryption alone.

IPsec

IP Security (IPsec) is a set of protocols developed by the Internet Engineering Task Force (IETF) for the secure exchange of data packets at the IP layer and is widely used to implement Virtual Private Networks (VPNs).

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion of each packet, and leaves the header untouched. The Tunnel mode is more secure in that it encrypts both the data and header. On the receiving side, an IPSec-compliant device decrypts each packet. Through the Internet Security Associate and Key Management Protocol/Oakley (ISAKMP/Oakley), both the sending and receiving device share a public key.

The Importance of Encryption

It would be careless to underestimate the role that encryption technology plays in safeguarding our public and private networks. It is important because it protects things such as e-mail, medical records, confidential corporate information, data on personal buying habits, legal documents, credit histories and transactions, and

government and regulatory agency databases. Securing this data is critical to peace of mind in communicating business and personal information.

The U.S. government has made it compulsory that all its organizations have certified systems in place to protect data transmissions. Government technology integrators and contractors are now pursuing NIST certification for that extra edge to be included in any government IT purchases. Starting in 2005, the federal government will begin to retrofit previously installed IT systems with NIST-certified AES equipment, providing tremendous opportunities for government VARs.

In addition to the government market, demand for AES-certified products is expected to increase in commercial markets that require the highest level of secure data encryption and privacy, such as financial, banking and medical information applications.

What is NIST?

NIST is the National Institute of Standards and Technology created by the U.S. Commerce Department's Technology Administration in 1901. It is a non-regulatory federal agency created to develop and promote measurement, standards, and technology to enhance productivity and facilitate trade.

FIPS

The Federal Information Processing Standards (FIPS) are Secretary of Commerce approved standards and guidelines that are developed by NIST for federal computer systems. These rigorous IT security standards were developed because there were no federal government requirements, acceptable industry standards or solutions. The FIPS program is supervised by the National Security Agency (NSA), which employs the best cryptographers and code-breakers in the world who are experts in securing U.S. secrets while deciphering those of other countries. It is with the oversight of the NSA, that the FIPS themselves are presumed to specify the strongest unclassified encryption technologies available.

There have been numerous FIPS issued since they were first published in 1974, but only some FIPS publications are of significance. The most important to remember are:

- FIPS 46 (Revisions 1, 3, and 3) -- the Data Encryption Standard (DES) used by the federal government and private industry to secure sensitive data.
- FIPS 140 (Revisions 1 and 2) -- the detailed security requirements for encryption software that is required for software using encryption used within the federal government.
- FIPS 180 (Revisions 1 and 2) -- the Secure Hash Standard for digital signature systems that is used by government and industry to ensure data integrity.
- FIPS 186 (Revisions 1 and 2) -- the Digital Signature Standard which is an algorithm used for digital signatures within the government as well as other industries.
- FIPS 197 -- the Advanced Encryption Standard (AES) which superseded the DES as the standard encryption algorithm for government data.

FIPS 140 specifies comprehensive implementation and certification requirements for any system which provides encryption. By law, Federal agencies cannot process

sensitive information without using an encryption product which has been certified to FIPS 140 (when companies claim their products are “FIPS certified”, they typically mean certified to meet the requirements of FIPS 140). In effect, anything that is worth encrypting must be encrypted using software certified under FIPS 140.

FIPS 140 certification is particularly valuable for embedded devices which are increasingly network-oriented and frequently lag behind desktop systems in their security offerings. With FIPS 140 certification, networked embedded products such as medical devices, monitoring systems, alarm and surveillance systems can immediately differentiate themselves and have access to the substantial federal government market, as well as private contractors developing federal systems.

Unlike other FIPS, which describe algorithms for encryption or hashing or digital signatures, FIPS 140 specifies how any encryption product must be designed, implemented and tested. Therefore, FIPS 140 is a more systematic, broad standard, whereas other FIPS are narrowly focused on a particular encryption algorithm.

It is a requirement of FIPS 140 that cryptographic modules must implement at least one FIPS-certified algorithm. This means that in order to be compliant with FIPS 140, a module must first receive FIPS certification for one or more encryption algorithms, such as DES (FIPS 46-3) or AES (FIPS 197). Therefore, it is not possible to receive FIPS 140 certification without at least one other FIPS certification, and typically more than one for a useful product.

Why is AES important?

The Advanced Encryption Standard (AES) supports key sizes of 128 bits, 192 bits and 256 bits and serves as a replacement for the Data Encryption Standard (DES), which has a key size of 56 bits. DES had been cracked and declared no longer suitable for securing sensitive data. In 1997, NIST started its effort to develop the AES. It brought together researchers from 12 countries who submitted encryption algorithms. Fifteen different formulas were “attacked” for vulnerabilities and evaluated by the worldwide cryptographic community. Eventually the winning algorithm was selected in October 2000. It incorporates the Rijndael encryption formula that was developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who have agreed that it may be used without royalty fees. The final standard was published in December 2001.

In an article in Network World Fusion it is estimated that it would take a computer typing 255 keys per second approximately 149 trillion years to crack the AES code. In addition to the increased security that comes with larger key sizes, AES can encrypt data much faster than Triple-DES, a DES enhancement that which essentially encrypts a message or document three times.

On May 26, 2002, AES replaced the DES as the algorithm of choice for the government. AES is described by the standard known as FIPS-197. This new standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used to protect sensitive information.

Products that support AES may be validated against the standard to demonstrate that they properly implement the algorithm. A validation certificate issued to the

product's vendor which states that the implementation has been tested. In addition, the product is then listed on the NIST website:

http://csrc.nist.gov/cryptval/aes/aesval.html

Rijndael Algorithm

Rijndael is the name for a symmetric block cipher that can encrypt and decrypt information that may be implemented in software, firmware, hardware, or any combination thereof, and is part of AES.

Secure Shell

Secure Shell (SSH) is a program that provides strong authentication and secure communications over unsecured channels. It is used as a replacement for Telnet, rlogin, rsh, and rcp, to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

The Relationship Between AES and SSH

AES is one of the many encryption algorithms supported by SSH. Once a session key is established SSH uses AES to protect data in transit.

Both SSH and AES are extremely important to overall network security by maintaining strict authentication for protection against intruders as well as symmetric encryption to protect transmission of dangerous packets. AES certification is reliable and can be trusted to handle the highest network security issues.

Importance of Encryption in Device Networking

It seems as though access and security are at opposite ends of the spectrum – the more access you give, the less security you have. Organizations have a need to protect personal or sensitive data from computer hackers or careless users. Often device servers are connected through the Internet, which exposes the serial device data stream to security risks. To keep data secure, it is important to use data encryption as a means of data translation into another format, or alternate language, which provides the highest level of security protection.

In the simplest connection scheme where two device servers are set up as a serial tunnel, no encryption application programming is required since both device servers can perform the encryption automatically. However, in the case where a host-based application is interacting with the serial device through its own network connection, modification of the application is required to support data encryption or by adding Secure Com Port Redirector™ (SCPR). SCPR is a Windows® application which creates a secure communications path over a network between the computer and electronic serial-based devices that are traditionally controlled via a COM Port. Utilizing SCPR eliminates the need to change the design.

Device Server Security

With NIST-certified AES encryption, a device server's security is insured preventing an intruder from reconfiguring the device or getting access to the serial stream.

A device server can be "locked down" in the following ways:

- Configure device servers to shut down unwanted access from the network
- UDP configuration ports helpful in manufacturing may be disabled
- Web browser access for interactive setup can be prevented
- Telnet access can be password protected or disabled all together to prevent network reconfiguration.
- Closing of the TFTP port to prevent the network download of new or possibly harmful firmware.
- For the even tougher environment, SNMP can be disabled preventing the Device server from responding to even benign network queries.

Once a device server is "locked down", the only way to reconfigure it is through the serial port. Getting access to the serial port is a "physical" security issue that needs to be addressed during the actual manufacturing and installation of the device server.

Data encryption of networked devices is seen as the best way to cut the risks associated with misplaced, lost or stolen data. Encryption also helps with the legal liability over information found on misplaced machines, and the growing threat of virus attacks.

How a Device is Certified

To become certified, a device must undergo a series of tests outlined in the Advanced Encryption Standard Validation Suite (AESAVS). The AES algorithm may be implemented in software, hardware, firmware or any combination thereof, and must be used in conjunction with a FIPS-approved or a NIST-recommended mode of operation. The correct implementation of AES is tested by one, of a list of National Voluntary Accreditation Program laboratories. The process of working with the lab can be very costly, but it is the only way to perform conformance tests on the device implementation. All noncompliance issues must be corrected prior to certification. When a device receives its certified compliance, NIST will issue a certificate for the implementation, and publish the FIPS certificate number on its website.

NIST formally re-evaluates the standard every five years and continually analyzes the AES algorithm for any breakthrough in technology, mathematical weakness or other possible threats that could reduce the security of the standard.

It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list. A validation certificate issued to each vendor will show the laboratory that tested the implementation, and the operating environment (software or firmware) used to test the implementation. Any implementation which has received FIPS certification will be listed on NIST list of validated implementations. If a vendor cannot provide a certification number for the appropriate FIPS, it is not certified.

In order to remain certified, an implementation must update its certification with each new version, which results in an updated certified reflecting the new version information. Therefore, if the certificate number is valid, but it doesn't specify the version provided by the vendor, the certification is not valid to the product. For example, if a vendor asserts that its 5.0 product is FIPS 140 certified with a particular certificate number, then it must provide another certificate number for its 5.1 version or it is not certified.

Additionally, customers need to be aware that if they purchase a NIST certified product from a supplier and they want to load their company's own firmware onto the device, the device may need to be re-certified. This depends on the firmware change. If the customer completely changed the firmware with the AES encryption, then they would need to go through the costly and lengthy process to re-certify. If they modified or customized the firmware but did not change anything regarding the AES library within the product, then the product would retain its NIST certification.

FIPS 140 Certification

When a device has obtained at least one algorithm certification, the company may now begin the process of FIPS 140 certification. This long process requires reading and understanding the FIPS 140 standard document, the FIPS 140 Derived Test Requirements (DTR) document and the FIPS 140 implementation guidelines document. After implementing all of the requirements prescribed into the encryption module, the next step is to contract with the certification lab. The company will need to compose a FIPS 140 certification evidence document which outlines each relevant assertion in the FIPS 140 DTR. The lab will perform exhaustive testing of the module, and may ask that the company itself perform certain tests and send to the lab for validation.

Another requirement of FIPS 140 certification is the creation of a security policy document, which describes the module's security policy. The lab will then affirm the module's compliance to NIST, and forward all relevant documentation to NIST personnel. The application will then enter a queue, through which it will move as NIST personnel review the evidence and respond to the lab with requests for clarification or correction. If everything is in compliance, a FIPS 140 certificate, and a verifiable certificate number which will be published on the NIST website listing of FIPS 140-certified modules.

This process can cost up to $75,000 in lab fees, not to mention the many months of developer and technical writer time, plus the three to 12 months for the actual certification. If any compliance issues or errors are present in the module, these costs could go higher.

An easier solution would be to license a FIPS 140-certified module from a third-party. As long as the vendor maintains the module's certification, it qualifies as a FIPS certified product for use within the federal government. Given the substantial cost and time investment for FIPS 140 certification, licensing from a third party is a viable alternative.

Security Solutions from Lantronix

AES is the highest level of encryption available to the public and Lantronix is a leader in developing AES-compliant products. Lantronix SecureBox™, SCS and SLC products include the industry's first NIST-certified implementation of AES as specified by the FIPS-197 standard. The company is committed to serving U.S. governmental agencies and other customers who work closely with these agencies knowing that compliance with the AES standard is mandatory.

Saving its customer's time, money and the trouble of adding encryption, Lantronix is the first and only company to offer a full range of secure devices that address both IT and non-IT, or "edge" products that include bar code scanners, thermostats, factory machines, scales, blood analyzers and security systems. With the company's extensive networking experience, customers are assured that all issues associated with adding encryption are solved with no impact to performance or the system processor. Utilizing Lantronix's NIST-certified products provides the peace-of-mind of the highest level of device server security available on the market.

Five of the company's products are the first of their kind in both the console management and device networking markets to offer a NIST-certified implementation of AES as specified by the Federal Information Processing Standard (FIPS) 197. Lantronix products are listed under certificate numbers 162, 157 and 120. Specifically for its CoBOS-based family of products such as XPort®, WiPort™, UDS, etc., the certificate covers both Cipher Block Chaining (CBC) mode and 128-bit Cipher Feedback mode with 128, 192 and 256-bit encryption key sizes.

Lantronix NIST-certified AES products include:

- XPor®
- WiPort™
- WiBox™
- SecureLinx™ SLC Console Manager
- ActiveLinx™ Secure Console Servers
- SecureBox™ Device Servers

Note:
For Lantronix AES-encrypted device servers to provide the highest level of security, they require that:

- the wireless (WEP/WPA) and AES data encryption be enabled and properly configured
- the device server be properly configured to disable all other communication methods

Lantronix Embedded Servers

For secure communications, XPort offers 256-bit AES encryption while providing the ability to Internet-enable just about any electronic device so it can be monitored and controlled remotely. The XPort is a complete network enabling solution in a small RJ45 package. Providing an instantaneous "plug and play" solution, the XPort removes the complexity by including all the required hardware and software inside a single embedded device. In addition to the AES algorithm, it features all the essential networking specifications including a 10Base-T/100Base-TX Ethernet connection, a

proven operating system, an embedded Web server, e-mail alerts and a full TCP/IP protocol stack.

With 128-bit WEP and WPA and end-to-end 256-bit AES encryption, WiPort is the most compact, integrated solution available to add 802.11b secure wireless networking to any edge device with a serial interface. Within a single compact package, WiPort features a 10/100 Ethernet transceiver, a reliable and proven operating system stored in flash memory, an embedded Web server and a full TCP/IP protocol stack.

Lantronix Console Servers

Lantronix console servers are the first to provide secure access to a wide variety of IT and data center equipment, including Linux, Unix or Windows® 2003 servers, routers, switches, firewalls, PBXs, UPSs and building-access devices. IT professionals can manage a broad range of equipment either locally or remotely with centralized, secure local and remote access quickly, efficiently and cost effectively. Console servers from Lantronix provide the ability to monitor, manage and troubleshoot nearly anything in the data center rack, from anywhere, at any time -- even when servers or networks are down.

IT managers who are looking to take advantage of the benefits of remote management also need to address data privacy and network security concerns. The SCS and SLC console management products meet both remote management and security needs. The SecureLinx SLC provides integrated security features to help safely manage and access assets. The SLC supports SSL and SSH for data encryption, and also supports remote authentication for integration with other systems already in place in the data center.

Lantronix ActiveLinx products safeguard remote equipment with several layers of security. ActiveLinx uses authentication to limit access to authorized users by utilizing LDAP, NIS, RADIUS, or local usernames and passwords. It also restricts access to attached equipment with port-based user permissions, and when used with NIS, port permissions can be centrally managed. Strong encryption authentication is provided via SSH v2 for security over insecure channels. Plus a built-in firewall allows unused services to be disabled, and inbound connections can be denied to minimize visibility of the unit to port scanning.

Lantronix Device Servers

Lantronix SecureBox device servers enable devices with a serial port (RS-232, RS-422/485) to connect to Ethernet networks and offer advanced encryption for maximum security. SecureBox gives companies a scalable method to connect equipment without the need for a server or gateway or additional software or configuration changes. Devices such as barcode scanners, message displays, scales, factory floor automation equipment, laboratory equipment, security systems and HVAC systems can all be connected to provide centralized secure access and control.

WiBox combines power and security with the ability to connect serial devices to 802.11b wireless networks quickly and easily. WiBox offers serial RS-232/422/485

flexibility, WEP and WPA security, robust data handling capabilities and high serial speeds.

Lantronix Secure Com Port Redirector

Lantronix Secure Com Port Director (SCPR) enables users to extend the functionality of COM port-based Windows applications. Virtual COM ports can be mapped to Lantronix device servers and encrypted at both ends of the communication, enabling users to transport sensitive information to and from remote device servers over the network or the Internet with the highest level of security. Securely encrypted serial-based communications can be achieved over up to 64 secure channels.

Lantronix SCPR can also be used to create secure COM port-based connections between PCs over Ethernet. With SCPR installed at each machine, PCs that were formerly hard wired by serial cabling for security purposes or to accommodate applications that only understood serial data, can instead communicate over an Ethernet network or the Internet.