An Internet Security Protocols for Embedded System

Neha Kulkarni
Dept. of Computer Science & Engineering, Dept of Biomedical Engineering
S.G.S.I.T.S Indore India

VinayManurkar
Dept. of Computer Science & Engineering, Dept of Biomedical Engineering
S.G.S.I.T.S Indore India

Varun Pathak
Dept. of Computer Science & Engineering, Dept of Biomedical Engineering
S.G.S.I.T.S Indore India

Abstract - Security can mean resistance to casual attacks like most viruses and security can also mean resistance to DOS attacks. But in this paper, security will mean the embedded devices' ability to contain sensitive information and to hold down its end of a secure communication. In this paper we also are studying about various types of protocols which are used in networks security. These are TCP/IP, IPSec and SSL which are used in those networks which are also using embedded devices. Security protocols, such as IPSec and SSL are being increasingly deployed in the context of networked embedded systems. The resource-constrained nature of embedded systems and in particular, the modest capabilities of embedded processors makes it challenging to achieve satisfactory performance while executing security protocols.

I. INTRODUCTION

Embedded Systems are computers (Microprocessors) that are enclosed (embedded) in customized hardware. Examples of embedded control systems would be portable medical equipment, cellular phones, police, fire, emergency communications equipment, laboratory test equipment, robotic equipment and manufacturing monitoring of assembly lines. Embedded systems are designed under a wide range of constraints, including cost, Performance and power consumption. Security has traditionally been an important consideration in the design of specific embedded systems, such as smart cards. As embedded systems are used in increasingly diverse applications to perform critical functions and access sensitive information, security has become a widespread concern in their design. Due to the networked nature of many modern embedded systems, they are exposed to the myriad security threats that we have experienced with personal computers (PCs) and the Internet.

Currently, embedded system is becoming a main solution to most specific tasks because of its high stability, economic power consumption, portability and numerous useful. As a result, embedded system was used as a tiny computer to process many applications. Nowadays, many new applications are developed using web- based technologies, which users can access from anywhere through the Internet. However, data communicated between users and web-based applications may be revealed by anyone in the Internet, so secured communication is needed for web-based applications.

There are lot of different operating system, technologies and different development tools are also available which are

A. Embedded Technologies

x86 · 68k/ColdFire , PowerPC , ARM , MIPS , DSPs, Ubicom, 8051 , PICs , Z80, SPARC

B. Embedded OS's

Windows CE, VxWorks, pSOS+, QNX,

being lowered, and increasing numbers of embedded products are adopting this technology. Adoption is being made possible by hardware acceleration techniques that give low-powered processors the ability to perform cryptography algorithms quickly, and

Embedded Linux, BSD Unix

C. Embedded Development tools

single board computer SDKs, SDCC, KEIL C/C++ , Java , assembler Circuit the availability of software protocols designed for embedded systems. Secure Shell (SSH), Secure Socket Layer (SSL, also known as Transport.

As internet get a fast growth these all faced various type of attack, according to there attack these access risk will be classified in to three major group, Risk is determined by what the effect of penetration would be. For US Government operations, the following terms1 are used:

- TOP SECRET-unauthorized disclosure could cause exceptionally grave damage to national security.
- SECRET-unauthorized disclosure could cause serious damage to national security
- CLASSIFIED-unauthorized disclosure could cause damage to national security

NETWORK SECURITY FOR EMBEDDED APPLICATIONS

With an increasing number of network-

Connected embedded devices and an increasing amount of transactions occurring over the Internet, the corresponding rise in electronic threats are producing a growing need for network security. The traditional barriers to adding network security technology to embedded systems have been performance bottlenecks due to computationally-intensive cryptography algorithms and significant memory requirements. These barriers are now Provide excellent security; authentication, encryption, integrity and replay protection.

The main difference between the protocols is that the security is applied at different levels in the system structure. SSL resides within the application, while IPSec resides within the TCP/IP stack. SSH is an application of its own, providing a secure connection to a remote host.

2.1 TCP/IP security technology

Protocol like TCP/IP provide the

syntactic and semantic rules for communication.It is the basic technology which has survived nearly two decades of exponential growth and the associated increases in traffic.

The three major security needs in network communication are authentication, confidentiality, and integrity. Authentication means that the senders of the communication are actually the person's the recipient believes them to be. Confidentiality means that no one can read the communication except sender and recipient. Integrity means that the communication received has not been modified during transmission. Although TCP/IP networks have been widely adopted, they are vulnerable to security

risks for the same reasons that contributed to their success. First, they are public, which means that complete confidentiality is difficult. Second, in order to handle an ever-expanding network owned by multiple entities, IP packet routing was designed to be simple. Consequently, packets routed over the Internet can be picked up, copied, or routed to another destination by almost anyone who has Internet access, making authentication and integrity difficult. These problems limit the use of large IP networks for sensitive communications.

2.2 IPSec and SSL

Several protocols address the security vulnerabilities of TCP/IP. The two most common are IP Security (IPSec) and Secure Socket Layer (SSL). These protocols use complex algorithms for encryption and authentication, including Data Encryption Standard (DES), Advanced Encryption Standard (AES), Message Digest (MD5) and Secure Hashing Algorithm (SHA).

SSL resides between the TCP/IP stack and the application. When an SSL connection is set up a handshake procedure is first performed. During the handshake, authentication is performed and encryption keys are exchanged in a secure way. The algorithms to use for encryption, integrity and replay replay detection are also negotiated. All the Information negotiated during the handshake is stored in an SSL session. SSL sessions can be re-used for later connections, which will allow subsequent connections to be established with minimal overhead. This is a big advantage, particularly in real-time embedded systems where a full handshake may take too long in certain situations. Once an SSL connection is

established, all data is encrypted on the sending side and decrypted on the receiving side. Furthermore, the sender provides information that makes it possible for the receiver to verify that the message is from the expected sender, that it has not been modified and is not replayed. On other hand IPSec applies authentication, encryption,

integrity checks and replay detection at the network layer. SSL operates at the transport layer of a TCP/IP stack, above the TCP and UDP layers, and just below the application layer. IPSec operates at a much lower part of the stack in the network layer. IPSec is used for configurable and highly controlled secure access to a private network. It can work with any TCP/IP application above the IP layer, including web, e-mail, and file transfer applications, as well as terminal services, IP telephony, and other client-server applications. SSL, on the other hand, is used for secure web access to a publicly available website. Because it operates at the transport layer, a limited number of applications can be used with SSL, mainly web, e-mail, and file-transfer applications. Other applications that use SSL are often accessed with a customized web browser-based front-end. Currently, only IPSec supports User Datagram Protocol (UDP)-based applications, such as audio and video streaming. There is no standard method for securing UDP communication with SSL. SSL and IPSec offer similar types of encryption and authentication. In terms of overall security, IPSec can be considered more secure than SSL for a number of reasons. Because IPSec requires specially- configured software on both h the client and server side, it offers more security than an SSL solution, which could permit access from unknown users using
only a standard web browser. IPSec can also be used to secure more information than SSL. Whereas SSL secures only the data portion of TCP information, IPSec uses techniques such as tunneling, which can completely hide the identity of the information's sender and receiver.

III. IPSEC AND SSL IN EMBEDDED SYSTEMS

Because of performance and memory issues caused by their computationally- intensive algorithms, developers have rarely used IPSec and SSL in embedded applications. These protocols can seriously impact the performance of an application running on power-sensitive embedded microprocessors. In addition, their implementations often require a significant amount of memory. Therefore, implementations are needed which have been specifically designed for low-power, memory-constrained, embedded devices. In embedded systems, SSL is most often used to implement a server-side application, such as a secure web server. This makes this protocol relatively easy to deploy in an application, and makes the embedded device easy to access securely by non- technical users using standard web browsers. This standard client interface also creates an environment in which it is easy to add more client users to the system. However, because SSL-based applications must be integrated with the SSL socket layer, adding new applications requires a moderate amount of work from the developer. IPSec tends to be used in a client situation to allow an embedded device to connect to a virtual private network (VPN). In order to deploy this type of solution there is no standard, widely used means of access, such as a web browser. IPSec does allow easy deployment of new applications because nothing needs to change at the socket layer. New applications will function over IPSec-secured networks with little or no modifications to the application or
to the IPSec security configuration.

REFERENCES

[1] Douglas E.Comer, “Internetworking with TCP/IP: Principles, Protocols and Architectures” Fourth Edition. Person Education, 2003

[2] W. Stallings, “Cryptography and Network Security: Principles and Practice” Prentice Hall, 1998.

[3] Chanin Maharak and Boonchai Sowanwanichakul “Security Methods For Webbased Applications On Embedded System ,2004IEEE

[4] Lawrence Ricci, Larry McGinnes, “Embedded System Security”.

[5] Dr. Ulrich Topp,Peter Müller, “Web based service for embedded devices”, ABB Corporate Research

[6] Nachiketh R. Potlapally†, Srivaths Ravi‡, Anand Raghunathan‡, Ruby B. Lee†,and Niraj K. Jha, “Impact of Configurability and Extensibility on IPSec Protocol Execution on Embedded Processors,” Proceedings of the 19th International Conference on VLSI Design (VLSID’06),IEEE