AN UPDATE ON NETWORK-BASED SECURITY TECHNOLOGIES APPLICABLE TO TELEMETRY POST-PROCESSING AND ANALYSIS ACTIVITIES

Jeff Kalibjian
Hewlett-Packard Corporation

ABSTRACT

Networked based technologies (i.e. TCP/IP) have come to play an important role in the evolution of telemetry post processing services. A paramount issue when using networking to access/move telemetry data is security. In past years papers have focused on individual security technologies and how they could be used to secure telemetry data. This paper will review currently available network based security technologies, update readers on enhancements, and discuss their appropriate uses in the various phases of telemetry post-processing and analysis activities.

KEYWORDS

Network based computing, data security, security protocols, key management, telemetry post processing, cryptography, identity services.

INTRODUCTION

Securing data flowing over TCP/IP networks has been a critical issue. Today there are five security protocols most commonly used to protect data flowing over TCP/IP networks. Specifically:

- Transport Layer Security (TLS) – Formally known as Secure Sockets Layer (SSL) this is probably the most commonly used security protocol. The protocol runs on top of the TCP/IP protocol. It can facilitate secured and authenticated client/server interactions.

- Secure Internet Protocol (IPSec) – IPSec operates at the TCP/IP level, it facilitates secure network entity (packet) communication. Because it only operates at the packet level, application level data is typically not protected.

- Secure Multi-Purpose E-mail Extensions (S/MIME) – S/MIME is most often used to protect e-mail transactions. The protocol provides for data encryption and authentication. It can also be used outside of e-mail applications to secure data.

- Wireless Security (802.11x) - This has received a lot of attention in recent years because original implementations were done insecurely (Wired Equivalent Privacy, WEP) and had many vulnerabilities. Later versions (Wired Protected Access, WPA, WPA2) have been implemented more robustly. It facilitates data privacy and authentication over wireless networks.

- Web Services Security – The popularity of the web spawned a new set of protocols specifically oriented to securing transaction data being encapsulated utilizing XML schemas (more specifically the Simple Object Access Protocol, SOAP), Two security standards have been defined to protect XML based transactions; namely, XML Digital Signature and XML Encryption

BACKGROUND

Computer security is accomplished with a set of mathematical operations from a field known as cryptography [1]. Cryptographic keys are used with computational algorithms (known as ciphers) to encrypt (disguise) and decrypt (un-disguise) data. A key which is used to both encrypt and decrypt data is known as a symmetric key and they are used with symmetric ciphers (e.g. DES). There are also dual asymmetric key algorithms in which key pairs can be generated with the following property: one key can be used to encrypt data, and only the other corresponding key can be used to decrypt the data. One of these keys is typically known as a public key, the other as a private key. The most famous dual asymmetric key algorithm is known as the RSA algorithm [2]. RSA are the initials of the last names of the people who invented the algorithm. (Rivest, Shamir, and Adleman). A hash function (e.g. SHA-1) is a mathematical function that returns a unique set of bits given an input. A digital signature involves hashing a value and encrypting it with a private key. The public key can then be used to decrypt the hash value---demonstrating that the person with the private key was the one who originally encrypted the hash. Validating a digital signature is known as an authentication operation.

IDENTITY

Authentication is an important issue when interacting with remote entities that one cannot see. On the Internet identity is most often established and validated using what is known as an X.509 v3 [3] certificate. The certificate is simply a collection of information identifying someone or something. So it would contain data like name, e-mail address, etc. To make sure the certificate cannot be altered it is digitally signed by what is known as a Certificate Authority (CA). The CA uses dual asymmetric keys in its business operation. It creates a certificate (after using "out of band" means to confirm the identity of the certificate requestor), then it uses its private key to sign the certificate. When a third party encounters the certificate (for example when it is used in TLS or S/MIME) it can use the CA's public key to verify the certificate. Assuring that there is sufficient infrastructure for all recognized CAs to have their public keys readily available has always been an issue in the use of dual asymmetric keys to establish identity. The most famous CA today is VeriSign. There are also smaller companies which provide similar services

KEY MANAGEMENT

The most important aspect of cryptographic services is cryptographic key management-----whether the key is a symmetric key or a dual asymmetric key. Key management implies protecting the key so that it cannot be used in an unauthorized manner. Since cryptographic keys protect important information (identity data, financial transactions, national security secrets) this is an important aspect of security. In its most robust form, key management implies ensuring that the bits that make up the cryptographic key cannot be observed by third party entities (processes, people, etc) in any way. This usually restricts the key use to computing environments that have very rigorous security certifications (e.g.NIST FIPS 140-2 Level 1-4 [4]). These environments essentially make it very difficult for key material to "leak" outside the process space using the key. Cryptographic keys should never be stored in the clear. They are usually stored encrypted by other cryptographic keys. In their simplest form, the other cryptographic keys can be derived by hashing pass-phrases. In more robust environments it may take several people (each with a portion of the encrypting key bits) to derive a key encryption key.

TLS

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) is probably the most commonly used security protocol. On the OSI stack TLS operates at layer 4. SSL 1.0 was originally proposed and implemented by Netscape. More robust versions were deployed (SSL 2.0, SSL 3.0) in later years. SSL 3.0 and TLS 1.1 [5] are fairly similar, TLS is an officially adopted IETF open standard. TLS enables TCP/IP connected applications to not only communicate in a secure fashion (data is encrypted between client and server), but also enables client and server entities to authenticate one another. After client/server entity authentication, the rest of the protocol centers on exchange of keying material that enables client and server entities to derive the same bulk encryption key.

Important aspects of the protocol are that encryption is generally done using symmetric ciphers; dual asymmetric cipher use is only done at the beginning of the protocol to exchange keying material. There are five important steps in TLS key derivation:

1. Client contacts server, indicates TLS version it supports, suggests ciphers, asks for server identification (X.509 certificate).
2. Server responds with certificate, ciphers that will be used, and might ask for the client certificate.
3. Client uses server dual asymmetric public key to encrypt random data, server decrypts that data with its private dual asymmetric key.
4. Server then sends some random data to client (doesn't have t be encrypted).
5. Client and server use the same hash functions on the random data to generate the same symmetric session key

Thus, client and server entities can use TLS to both authenticate one another and also insure confidentiality in their data communications.

IPSec

Secure Internet Protocol or IPSec [6] operates at Layer 3 in the OSI stack model. It uses the same cryptographic elements as TLS, but in a slightly different fashion to delivery a transport security product. IPSec is mandatory for IPv6 an optional for IPv4. Most IPSec implementations today are done under IPv4. IPSec has two modes of operation. In transport mode only the payload of the packet is encrypted. The IP header is not touched. In Tunnel Mode, the entire packed is encrypted and so the encrypted packet must be encapsulated into a new IP packet in order to facilitate proper routing. Either mode can create a Virtual Private Network (VPN) and this is the most typical use of IPSec. The modes of operation will not work unless there is agreement on types of cryptographic algorithms and keys used. This is achieved via the so called *security association*. A security association can be thought of as simply an agreement of algorithms and keys to be used in a particular path. Each packet will then have a related security association based on its destination address. Key exchange is actually carried out in user space via the IKE/ISAKMP protocols/

Two new headers (operating directly on top of IP) have been created to deliver the security functionality. The first header known as the Authentication Header (AH) offers connectionless integrity and data origin authentication. It can also guard against replay attack by utilizing a technique known as sliding window. The second header, known as the Encapsulation Security Payload (ESP) offers integrity, authenticity, and confidentiality with encryption only and authentication only modes also available. So, IPSec can be used to insure packet traffic payloads are not modified in transit (integrity), payload content is not revealed in transit (privacy), packet data is not being replayed, and networking nodes are authenticated.

S/MIME

Secure Multi-Purpose E-mail Extensions was originally developed by RSA Data Security Inc., but has since been handed over to the IETF and is now part of their Cryptographic Message Syntax protocol [7]. S/MIME originally brought together a secure data encapsulation standard known as PKCS-7 [8] and an IETF standard for sending typed data in e-mail (MIME [9]) PKCS-7 is basically a format specifying how data may be protected in a self contained package (data blob). The format specifies encryption and authentication. That is, one is able to authenticate who actually created the data blob as well as protect the data inside it. The details of the format are beyond the scope of this paper. However, it is important to note that S/MIME is an example of a security protocol that operates at higher application layer. In the OSI model that is layers 5-7. Not surprisingly (because of the MIME involvement), the most common use of S/MIME today is in e-mail. Many e-mail applications today support S/MIME (e.g. Microsoft Outlook, etc.). However S/MIME is not limited in use to e-mail applications. It can be used by applications needing to transport sensitive data in a self contained manner. The advantage over TLS is that the data is actually protected in the application layer. When TLS is used by an application, by the time data gets to the application layer it is already decrypted and in the clear.

WS-Security

A “web service” is defined to be computer-to-computer application interactions within or between enterprises utilizing platform independence and programming language neutrality concepts. The web service model uses XML, HTTP and SOAP to link applications together. A key requirement of web services is that they be secure. There are seven proposed Web Service specifications to achieve this. WS-Security [10] specifies how XML signatures [11] and XML encryption [12] maybe used to secure web services.

The XML digital signature can be applied to an entire XML document, multiple XML documents, non-XML documents, specific elements in an XML document or element content portions of an XML document. XML signatures can even contain other XML signatures. The XML signature itself maybe stored separate from the data the signature is over (detached signature), or in the same XML file (enveloped signature). The primary signature elements include

- <Signature> -- The XML signature element.

- <SignatureValue> -- The cryptographic signature.

- <SignedInfo> -- The data that was signed. Will typically contain <Reference> elements that contain a digest of the data, digest algorithm and a URI to where the data can be found. URI’s may refer to non-XML content. Reference elements may also specify transforms to be performed on data before they are digested. Canonicalization transforms exist that insure simple variations in syntax (e.g.whitespace) will not prevent “identical” texts from “digesting” differently.

The XML encryption facility, like the signature capability, can also be applied to an entire XML document, multiple XML documents, non-XML documents, specific elements in an XML document or element content portions. The primary encryption element is the <EncryptedData> element. This element will replace an element that is encrypted. The <EncryptedData> element may include a type attribute that describes the MIME type of the element or element content that was encrypted. The <EncryptedData> element also defines the algorithm that is used for encryption. User defined properties may also be associated with an encrypted element. Other encryption elements include

- <CipherData> -- Stores result of encryption operation.

- <CipherValue> -- Contains actual encrypted data.

- <CipherReference> --- URI reference to encrypted data stored at another location.

It should be noted that XML encryption and XML signature standards make use of lower level PKCS-7 constructs.

WIRELESS SECURITY

The 802.11x [13] standard implies two modes of operation. The first is peer to peer mode (also known as “ad hoc” mode) in which wireless nodes directly communicate. The second, requires two pieces of equipment to operate: the wireless node and an Access Point (AP) which acts like a hub between the wireless systems and a wired network (Figure 1). This mode of operation (also known as “infrastructure” mode) is the more familiar client/server infrastructure where the hub acts as bridge to the wired network.

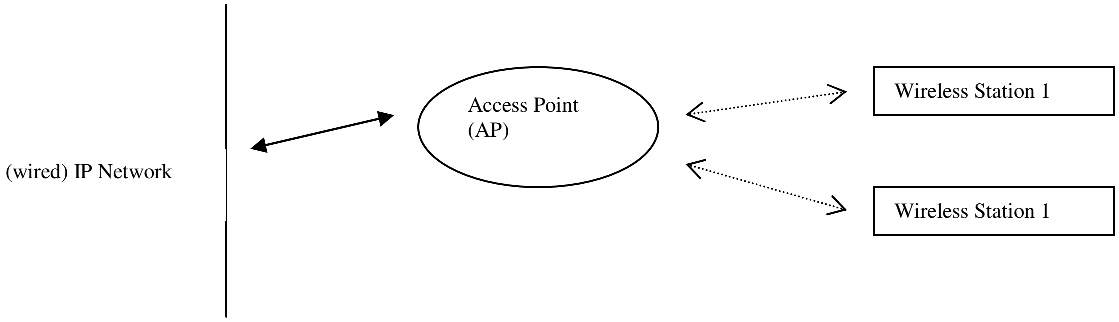

Figure 1. A simple 802.11x network architecture

802.11x SECURITY ISSUES

Before utilizing the AP, the wireless client and the AP must establish a relationship known as an association. This is actually a process in which the client goes through three phases with respect to the AP:

- Unauthenticated and unassociated – not connected.

- Authenticated and unassociated – A client can listen to identify access points within range or actually send out specific requests to find an access point. Information is exchanged (known as management frames). There are two types of authentication open system authentication in which anyone is authenticated, or Shared Key authentication, which uses a classic challenge/response paradigm.

- Authenticated and associated – After being authenticated the client sends an association request frame; then after receiving the association response frame the client is on the wireless network.

In its initial form, privacy was achieved by use of Wired Equivalent Privacy (WEP) [14]. This had many vulnerabilities including the use of the RC4 cipher. Keys could be deduced by hackers employing known techniques. In addition WEP used a CRC for integrity that was insecure (one could actually alter a payload and update the CRC without having to know the RC4 key). The introduction of Wired Protected Access (WPA) by the Wi-Fi Alliance began to make things better. They introduced a Message Integrity Code (MIC) algorithm named “Michael” that would protect the payload from alteration. The MIC also used a frame counter to prevent replay attacks.

In addition a new key management algorithm known as the Temporal Key Integrity Protocol (TKIP) which dynamically changed keys in the system was also introduced. Later WPA2 [15] was deployed which implements the mandatory elements of the 802.11i standard including use of a new AES based cipher algorithm known as CCMP. CCMP is considered fully secure by most crypto-analysts.

TELEMETRY APPLICATION AREAS

Each of the security protocols discussed has application to telemetry post processing and analysis network environments. In environments where an organization does not want to burden users with key management and client authentication issues, IPSec can be utilized to secure network segments that are utilized for telemetry reduction and analysis activities.

Table 1 Security Protocol Use for Telemetry Post Processing Applications

Security Protocol	**Potential Telemetry Post Processing Use**
TLS	Secure data links and also concerned about authenticating clients
IPSec	Secure data links, not too concerned about access control of data
S/MIME	Concerned about privacy of data ad access of data on client workstation
WS-Security	Concerned about privacy of data and access of data on client workstations or by other WS-Security sensible applications
WEP/EAP	Concerned about securing wireless network link.

Data will be secured as it moves point to point in the network infrastructure; however, on the actual machine the data ends up on the data will not be secured as it is processed by the analysis applications on those machines. If data access control is a concern and reduced data is housed on a centralized server, an organization might want to use TLS. Client authentication could be enabled requiring analysts to present their X.509 certificates before they could access data. Of course, when the data was actually moved to the analyst's client workstation it would also be encrypted in transit. But, again, once data reached the client workstation it would remain unencrypted. If data security at the client workstation was an issue, S/MIME or WS Security technologies could be utilized to insure that data remained encrypted at rest (in a PKCS-7 "blob") on the analyst's client workstation. Since both S/MIME and WS Security have authentication notions, client authentication could also be supported utilizing these standards.

Additionally S/MIME and WS-Security lend themselves to be utilized by other post processing applications that may need to handle and access secured telemetry data. Finally, in circumstances where wired networks are not practical 802.11.x could be utilized to set up wireless networks in areas where data analysis might need to take place (perhaps at a field test location). If there is concern about the underlying wireless security protocol being used (WEP, EAP), one could use a higher level protocol (e.g. TLS) on-top of the wireless security protocol to make data security more robust. Table 1 summarizes the discussed uses of the security protocols.

SUMMARY

Five security protocols have emerged as the security protocols of choice to use in a networked computer environment: TLS, IPSec, S/MIME, WS-Security, and WEP/EAP). Each has application use in telemetry post processing and analysis environments. All protocols are capable of utilizing cryptographic techniques that have proven to be very robust. A key differentiating factor between the protocols is the OSI layer they operate at. Some operate at a link layers (e.g. IPSec) others work at an application level (S/MIME) and one needs to be aware that if data needs to be secured on the client workstation accessing data, then a protocol like S/MIME should be considered. It is important to use these security protocols inside the company firewalls because studies still show that up to 80 percent of all data breaches occur from sources inside the organization.

References

[1] Schneier, Bruce, *Applied Cryptography*, John Wiley and Sons, Second Edition.

[2] Rivest, R, Shamir, A, Adelman, L, *A Method for Obtaining Digital Signatures and Public-Key Crypto Systems*, http://people.csail.mit.edu/rivest/Rsapaper.pdf

[3] IETF, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, http://www.ietf.org/rfc/rfc3280.txt

[4] NIST, *Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] IETF, *The Transport Layer Security (TLS) Protocol, Version 1.1*, http://www.ietf.org/rfc/rfc4346.txt

[6] IETF, IP *Security Protocol (IPSEC)*, http://www.ietf.org/html.charters/OLD/ipsec-charter.html

[7] IETF Network Working Group, *S/MIME Version 2 Message Specification*, http://www.rfc-editor.org/rfc/rfc2311.txt

[8] RSA Laboratories, PKCS *#7: Cryptographic Message Syntax Standard*, http://www.rsa.com/rsalabs/node.asp?id=2129

[9] IETF, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*, http://www.ietf.org/rfc/rfc2045.txt

[10] OASIS**,** *OASIS Web Services Security (WSS) TC*, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[11] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/

[12] W3C, *XML Encryption Syntax and Processing***, http://www.w3.org/TR/xmlenc-core/**

[13] IEEE, *802.11 Document System*, http://www.ieee802.org/11/

[14] EZLAN.NET, Wireless Encryption - WEP, WPA, and WPA2, http://www.ezlan.net/wpa_wep.html

[15] Wi-Fi Alliance, WPA2 (Wi-Fi Protected Access 2), http://www.wi-fi.org/knowledge_center/wpa2