Math 135: The Art of Secret Writing (Summer 2006)
Basic Internet Security

Internet Protocol Suite

The Internet protocol suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It is sometimes called the TCP/IP protocol suite, after the two most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

The Internet protocol suite can be viewed as a set of layers, each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers. Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that can eventually be physically transmitted.

- **Application Layer**: Protocols include FTP, HTTP, DNS, IMAP, POP3, SMTP, TELNET, BitTorrent.
- **Transport Layer**: Protocols include TCP.
- **Network Layer**: Protocols include IP.
- **(Data) Link Layer**: Protocols include Ethernet, Wi-Fi, PPP.

Internet Protocol (IP)

The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched internetwork. IP provides the service of communicable unique global addressing amongst computers. (Each computer on the Internet has a unique IP address.)

Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is also one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange data in packets.

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is a method used to transfer information on the World Wide Web. HTTP is a request/response protocol between clients and servers. The originating client, such as a Web browser, is referred to as the user agent. The destination server, which stores resources such as HTML files and images, is called the origin server. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels.

An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

Upon receiving the request, the server sends back a status line, such as “HTTP/1.1 200 OK”, and a message of its own, the body of which is perhaps the requested file, an error message, or some other information.

Resources to be accessed by HTTP are identified using Uniform Resource Locators (URLs) using the `http://` or `https://` schemes.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, are cryptographic protocols which provide secure communications on the Internet. SSL provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; mutual authentication requires public key infrastructure (PKI) deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. SSL involves three basic phases:

- peer negotiation for algorithm support;
- public key encryption-based key exchange and certificate-based authentication; and
- symmetric cipher-based traffic encryption.

During the first phase, the client and server negotiation uses cryptographic algorithms. Current implementations support the following choices:

- for public-key cryptography: RSA, Diffie-Hellman, DSA, or Fortezza;
- for symmetric ciphers: RC2, RC4, IDEA, DES, Triple DES, or AES;

SSL runs on layers beneath application protocols such as HTTP, and above the TCP transport protocol. SSL can add security to any protocol that uses reliable connections, but is most commonly used with HTTP to form HTTPS.

Secure Hypertext Transfer Protocol (HTTPS)

HTTPS is used to secure World Wide Web pages for applications such as electronic commerce by employing public key certificates to verify the identity of endpoints.

`https://` is a URL scheme which is syntactically identical to the `http://` scheme normally used for accessing resources using HTTP. Using an `https://` URL indicates that HTTP is to be used, but with a different default port and an additional encryption/authentication layer (usually Secure Socket Layer or SSL) between HTTP (on the application layer) and TCP (on the transport layer). This system was invented by Netscape to provide authentication and encrypted communication, and is widely used on the World Wide Web for security-sensitive communication, such as payment transactions and e-commerce.

The level of protection depends on the correctness of the implementation by the Web browser and the server software and the actual cryptographic algorithms supported. A common misconception among credit card users on the Web is that `https://` fully protects their card number from thieves. In reality, an encrypted connection to the Web server only protects the credit card number in transit between the user's computer and the server itself. It does not guarantee that the server itself is secure, or even that it has not already been compromised by an attacker.

Attacks on the Web sites that store customer data are both easier and more common than attempts to intercept data in transit. Merchant sites are supposed to immediately forward incoming transactions to a financial gateway and retain only a transaction number, but they often save card numbers in a database. It is that server and database that is usually attacked and compromised by unauthorized users.

The Difference Between Authentication and Encryption

Authentication is vital for secure e-commerce transactions in which you send private and confidential information over the Internet and first want to verify the receiving server's identity. Server authentication allows you to confirm a Web server's identity. Your browser can automatically check that a server's certificate and public key are valid and have been issued by a certificate authority (CA), such as VeriSign.

An encrypted connection requires all information sent between your computer and someone else's server to be encrypted by the sender and decrypted by the receiver. This protects private information from being intercepted over the Internet. This means that you can share personal data (such as your account information) trusting that it will remain private and confidential.

VeriSign and SSL Certificates

VeriSign is the leading Secure Sockets Layer (SSL) certificate authority enabling secure e-commerce and communications for Web sites, intranets, and extranets.

An SSL certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server and the client and establishes an encryption method and a unique session key. They can begin a secure session that guarantees message privacy and message integrity.

Without SSL encryption, packets of information travel networks in full view. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. Without third-party verification, how do you know a Web site is an authentic representative of a business you trust? Every SSL certificate is created for a particular server in a specific domain for a verified business entity. Like a passport or a drivers license, an SSL certificate is issued by a trusted authority. When the SSL handshake occurs, the browser requires authentication from the server. If the information does not match or the certificate has expired, the browser displays an error message.

An online retailer (or anyone, in fact, that wants to serve secure Web sites) purchases an SSL certificate from VeriSign who then complete a business authentication process to ensure the identity of the purchaser.

Web Browsers

The newest Web browsers, including Internet Explorer 5.5 and Netscape 4.72, are capable of providing 128-bit encrypted sessions for SSL certificates (provided that the operating system allows it). The Web browser reads the public key certificate which uses a digital signature to bind together a public key with an identity, such as the name of a person or organzation. (See Section 4.6 of the textbook.) In a typical public key infrastructure scheme, the digital signature will be of a certificate authority (CA). The certificate is then used to verify that the public key belongs to the named individual.

The following information is from the Web site of the newly released Web browser, Opera.

Opera is designed with the most advanced and widespread security measures available, making on-line purchasing simple. When you enter your credit card number on a page where Opera's icon displays *Secure*, Opera and the Web site use public keys to agree on a secret one-time key before sending the number. This is called a handshake. The key encrypts all the information sent and is used for this session only. The level of encryption depends on the available key space, which means the number of possibilities when generating keys. The more possible keys, the higher the security. For session keys, the most powerful form of encryption available in browsers today is 128-bit encryption. Although Opera supports as much as 3072-bit encryption when generating key pairs (a public key and a private key), some secure sites may not support this level of encryption. Opera's default setting of 1024-bit encryption should work with most secure sites. The number on the padlock icon signals the level of encryption. Three dots means that the Web site has a high level of security. When rating the security level of a secure document, Opera takes into consideration the following:

- everything loaded with the page, including images, frames, and redirects;
  - Insecure images will automatically result in a level one rating.
  - Other insecure content (such as scripting) will result in level zero.
- the size of the symmetric key; and
- the server's public key size.

Only documents using the most secure methods, 3-DES or 128-bit C4 and public keys larger than approximately 900 bits, get a level three rating. Reputable on-line merchants have their public keys signed by trusted authorities (such as VerisSign) which issue digital certificates that contain the public key, and are signed in a way that can be automatically proven. To display your current list of authorities, click "Manage Certificates." Opera, like all secure browsers, comes with a set of certificates. Most of the time, certificates are fully valid, and if there is something questionable about a certificate, a warning dialog will be displayed. You may choose to proceed, but full security cannot be guaranteed at this point.

128-bit Encryption

The phrase 128-bit encryption is commonly used to refer to the Advanced Encryption Standard (AES) (inaccurately used synonymously with Rijndael) which is a block cipher adopted as an encryption standard by the US government. (Read pages 30–32 in the textbook again.) AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. (Strictly speaking, Rijndael allows for variable block and key sizes.) For a thorough description of Rijndael, consult

`http://en.wikipedia.org/wiki/Rijndael`

The choice of Rijndael as the de-facto Advanced Encryption Standard was made by the National Institute of Standards and Technology (NIST) after an extensive competition. Furthermore, the National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for US Government non-classified data. In June 2003, the US Government announced that AES may be used for classified information. This marks the first time that the public has had access to a cipher approved by NSA for TOP SECRET information. It is interesting to note that many public products use 128-bit secret keys by default; it is possible that NSA suspects a fundamental weakness in keys this short, or they may simply prefer a safety margin for top secret documents (which may require security decades into the future).