Encryption

- Symmetric cryptography
  - Both ends have the same key
- Asymmetric cryptography
  - Two keys coexists: public key and private key.
  - Only publish public key.
    - Data encoded with the public key can be decoded only with the private key;
    - Data encoded with the private key can be decoded only with the public key.

Encryption

- Use public key and private key
  - A client user encrypts the information (a secret key) with the other users' publish key
  - Only the holder of the private key that matches the public key can decrypt and view the message.
  - Or vise versa
- public key encryption systems are common used for authentication and securely passing a symmetric encryption key.
  - Algorithm is complex
  - Slow
  - CPU intensive

Encryption

- In practice, Symmetric keys will be used to encrypt data.
- What is certificate used by SSL?
  - Digital packages that contain the public half of a key pair belonging to an SSL web server
  - SSL certificates are issued by Organization known as root certification authorities (CAs).
  - Web Browsers come prepackaged with a long list of CAs from which they accept certificate of authenticity.
    - Check out tools->Internet Options->Content-> certificate, and then select Trusted Root Certification Authorities tab.

SSL certificate authentication scheme

1. Web Site A send certificate requests to CA. The request contains the public key.
2. CA issue the certificate that it encrypts with its private key.
3. Web Site A installs the certificate.
4. When client connect to Web Site A, this certificate is send to the client
5. The client validates the certificate with the trusted CA's public key – which ensures that the certificate was signed by that CA with its private key.

SSL certificate authentication scheme

6. Having validate the certificate, the client now open it and extract the web servers' public key.
7. The client generates a symmetric session key and encrypts that key with the Web Site A's public key.
8. For the rest of the SSL session, the client and the server use this shared symmetric key to encrypt all traffic.

Notes: The whole process is more complex than the above.

Creating a Secure Server with SSL

- Build a encrypted communication channel
- Security-Related Packages
  - open_ssl
  - mod_ssl
- OpenSSL
  - SSL/TLS library contains functions that implement the Secure Sockets Layer and Transport Layer Security protocols.
  - Crypto library contains a huge number of functions that implement a wide array of cryptographic (mathematical) algorithms.

Creating a Secure Server with SSL

- OpenSSL
  - On Linux, it is basically installed as two system libraries
    - libcrypto.a and libssl.a
      - Also libcrypto.so and libssl.so
  - An extensive command-line utility /usr/bin/openssl
    - Check if openssl is installed with RPM

      #rpm –q openssl
    - Check your version of openssl

      #openssl version

Installing and Using mod_ssl

- Five steps
  - Compile mod_ssl into apache if not already
  - Create a server key
  - Use your server key to create a certificate signing request (CSR)
  - Submit CSR to a commercial certificate authority for signing, or, as an alternative, create your own CS for certificate signing.
  - Configure Apache to use your signed SSL certificate(s).

Certificates and Security

- Certificates

  Secure Web Server uses a certificate to identify itself to web browsers.

  - from a Certificate Authority (CA)
    - Which CA to pick? Up to you.
    - Pick on that is widely accepted by all common browser software.
    - List of CAs that your Web browser will accept certificates.
      - On mozilla, edit->preferences->Privacy&Security->certificates->manage certificates->Authorities
        - » VeriSign
  - Self-signed certificates
    - Not be automatically accepted by users' browser, that is the user will be asked by the browser if he or she wants to accept the certificate and create the secure connection.

Steps

- See http://httpd.apache.org/docs/2.0/ssl/ssl_faq.html
  - How do I create a real SSL Certificate?

Configuring Apache to use SSL

- Added commands to load and enable the SSL module to the apache httpd.conf wrapped in <IFDefine SSL>

```
<IFDefine SSL>
LoadModule ssl_module modules/mod_ssl.so
</IfDefine>
```

- In the conf, there is a file named ssl-conf.
  - Contains the directives necessary to configure Apache for SSL, and also sets up a virtual host to listen on port 443.

```
<IfModule mod_ssl.c>
    Include conf/ssl.conf
</IfModule>
```

  - Where you can change certificate related location and file name directives.

5: Configuring Apache to use SSL

- Virtual host
  - To listen on 443

Self-signed certificate

- **$ openssl req -new -x509 -nodes -out server.crt -keyout server.key**
  These can be used as follows in your httpd.conf file:
  - SSLCertificateFile /path/to/this/server.crt
  - SSLCertificateKeyFile /path/to/this/server.key

Accessing secure server

- Use URL https://your_domain
- Secure web communication port 443
- Standard port for nonsecure Web communications is port 80.

Managing your webserver

- Monitor the log
  - History info
- For real time monitoring, enable the Apache server-status monitor
  - Load the mod_status module
  - Uncomment the location /server-status and set the allow directive

Summary

- Web servers are essential part of today's business
- Apache is a good choice
  - Deamon httpd and config file httpd.conf
- Performance
  - Directives, Cache, proxy servers
- Security
  - Permission
  - Secure web server SSL
- Monitoring