

Certificate Management

William I Tabor

Vice President

Research and Development

Protexx, Inc

Why

- WASHINGTON – President Barack Obama has created the new Office of Cybersecurity Coordinator and laid out the administration's plans for bolstering cybersecurity.
- Where does this lead us?

PKI

The government is pushing us to use PKI (Public/Private Key Infrastructure).

Credentials are already on CAC and TWIC cards.

The Federation for Identity and Cross-Credentialing Systems (FiXs) card is coming.

Government PKI

Structure has already been put in place.

To deal with various Federal entities today, via email or web, you must have

ECA (External Certificate Authority)
certificate.

Areas covered in this talk

- 1) How PKI works
- 2) How to set up a secure web server
 - A) Server credentials and crl
 - B) Client credentials
- 3) How to use your client certificate to sign documents and email
- 4) Using LDAP to store user credentials

How PKI Works

Three Way authentication

Entity one is Valid to the CA

Entity two is Valid to the CA

Either entity can check the other entity
with the CA

Problem SSL Connections

- One sided authentication
- Subject to man in the middle attack

Solution

- Two authentication
- Server certificate
- Client certificate
- Handshake takes place on two sided RSA
Encryption

Setting up SSL in Apache

```
<IfDefine SSL>
<IfDefine !NOSSL>
<VirtualHost certs.protexxinc.com:444>
    # General setup for the virtual host
    DocumentRoot "/srv/www/certs"
    ServerName certs.protexxinc.com
    ServerAdmin tabor@protexx.com
    ErrorLog /var/log/apache2/certs_error_log
    TransferLog /var/log/apache2/certs_access_log
<Directory "/srv/www/certs">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/certs/certs.protexxinc.com.crt
    SSLCertificateKeyFile /etc/apache2/certs/certs.protexxinc.com.key
    SSLCACertificateFile /etc/apache2/certs/ProtexxCERTSCA.crt
    SSLCARRevocationFile /etc/apache2/certs/ProtexxCERTS.crl
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
<Directory "/srv/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
    SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
    CustomLog /var/log/apache2/ssl_request_log ssl_combined
</VirtualHost>
</IfDefine>
</IfDefine>
```

Adding Client Authorization

```
<IfDefine SSL>
<IfDefine !NOSSL>
<VirtualHost certs.protexxinc.com:444>
    # General setup for the virtual host
    DocumentRoot "/srv/www/certs"
    ServerName certs.protexxinc.com
    ServerAdmin tabor@protexx.com
    ErrorLog /var/log/apache2/certs_error_log
    TransferLog /var/log/apache2/certs_access_log
<Directory "/srv/www/certs">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/certs/certs.protexxinc.com.crt
    SSLCertificateKeyFile /etc/apache2/certs/certs.protexxinc.com.key
    SSLCACertificateFile /etc/apache2/certs/ProtexxCERTSCA.crt
    SSLCAREvocationFile /etc/apache2/certs/ProtexxCERTS.crl

    SSLVerifyClient require                !!!!!!!
    SSLVerifyDepth 2
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
<Directory "/srv/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
    SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
    CustomLog /var/log/apache2/ssl_request_log ssl_combined
</VirtualHost>
</IfDefine>
</IfDefine>
```

Signing Email

- Why?
- Validate who sent it.
- Make sure it has not be changed.

Encrypting Email

- Uses the receiver's private key
- Ensures that only the receiver can read the email.
- The email is signed to ensure that the email has not changed.

Other uses

- Future enhancements to the PKI infrastructure will include a new type of certificate known as NPE (non-personal entity)
- This feature will be used but not limited to allow a machine access to the network before authentication of the user.

Demo

Questions?