Security Role Based Data Encryption for J2EE Web Applications

Heesun “Al” Park, PhD
SAS Institute, Inc
April 23, 2009

SSTC 2009

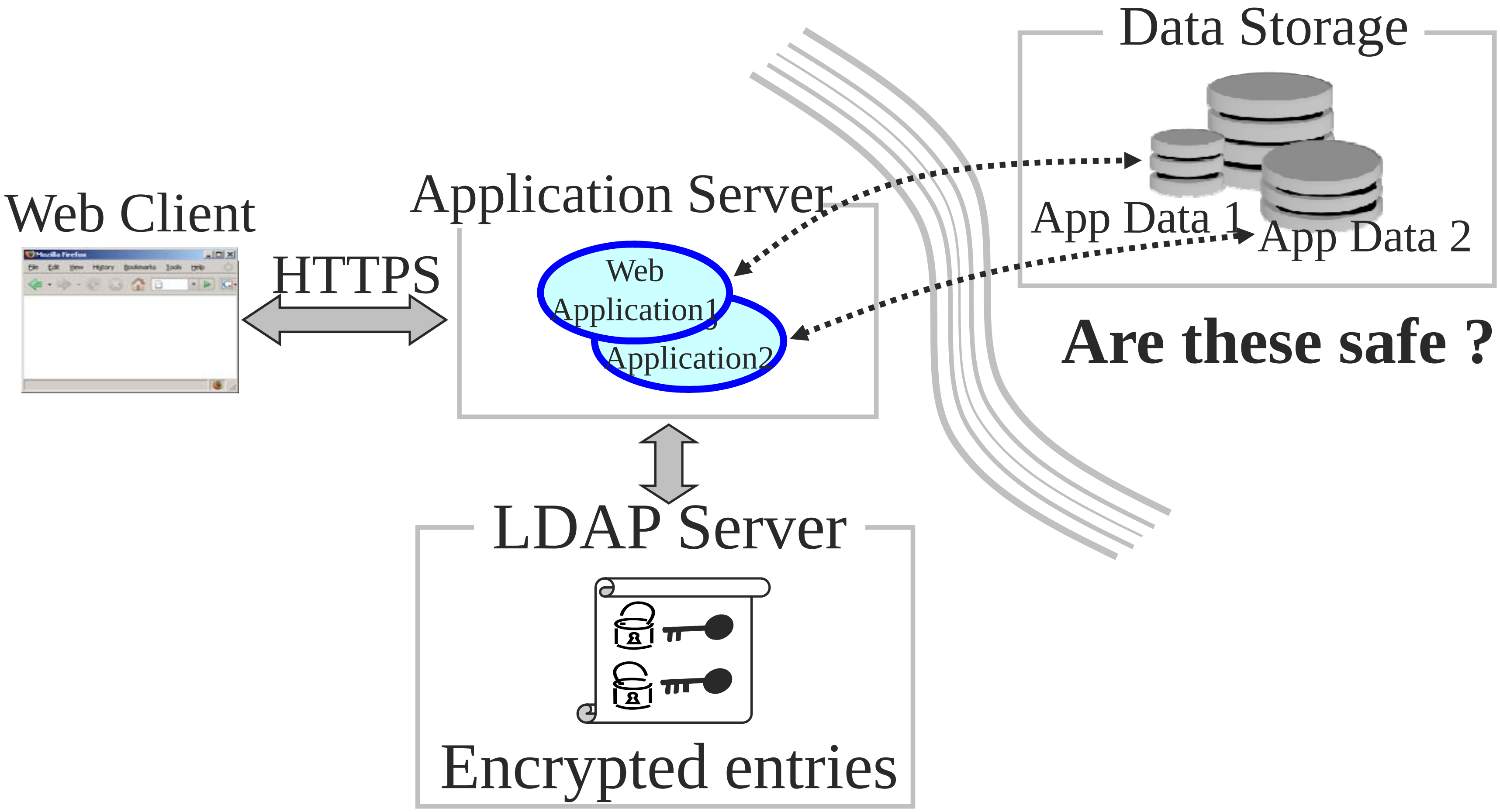
Topics

- End-to-End Web Application Security
- Security Role Mapping for Web Applications
- Data Encryption from Web Application
- Role to Encryption Mapping Table (REMT)
- Security Role Based Encryption Module (SREM)
- Application Data Encryption in PKI environment
- Impact on Performance
- Conclusion

Basics of Encryption Technology

- Public Key Cryptography (PKC)
- X.509 Certificate
- Public Key Infrastructure (PKI)
- Secure Socket Layer (SSL)
- SSL Handshake
- FIPS 140-2
- Quality of Encryption (Algorithm and Strength)
- LDAPS
- Java Cryptography Extension (JCE)

End-to-End Web Application Security



Are these safe ?

Figure 1: End-to-End Application Data Security

Security Role Mapping for Web Applications

- Fine grain web application protection mechanism
- Two phase process
- Logical group name (role-name) is defined in the deployment descriptor (web.xml) of the web application.
- Application server delivers the physical users to the logical group name during or after the web application deployment.
- Only users that belong to the logical group can access the web application.

Security Role Mapping (web.xml)

```
 <security-constraint>
   <web-resource-collection>
   <web-resource-name>MyWebApp
   </web-resource- name>
    <url-pattern>/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
   </web-resource-collection>
  <auth-constraint>
   <role-name>marketingRole</role-name>
  </auth-constraint>
 </security-constraint>

 <login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>My Realm</realm-name>
 </login-config>

<security-role>
  <role-name> marketingRole </role-name>
</security-role>
```

Data Encryption from Web Application

- Report or file generated by the web application (We are NOT talking about raw data used for report or file generation)
- Typically they are stored in WebDAV location.
- It may or may not contain “raw” data.
- In most cases, they are not encrypted
- Great security risk if exposed
- Security Role based encryption through Java Cryptography Extension (JCE)

Security Role based Encryption

- Associate encryption algorithm to the security role and use it when store or retrieve web application generated file (or report).
- This way, only the ones that belong to the security role can access the file (or report).
- Security risk is minimal even if it is exposed or stolen
- Use of Role to Encryption Mapping Table (REMT)

Role to Encryption Mapping Table (REMT) -1

- Central and key piece for the application data encryption.
- Constructed and maintained by security administrator.
- Contains entries that have role-name and encryption properties
- Mnemonic values can be used. Implementation code converts to actual encryption properties.
- Admin should be able to use any encryption algorithm by updating the entry for recovery, etc.

Role to Encryption Mapping Table (REMT) -2

- Encryption admin maintains the table with separate interface or GUI.
- Access should be strictly controlled
- REMT itself can be encrypted

Sample Role to Encryption Mapping Table (REMT) – Plain

Security Role-name	Encryption Algorithm	Encryption Key Data
marketingRole	DES	desKey
salesRole	RC4	Rc4Key
adminRole	DES	desKey

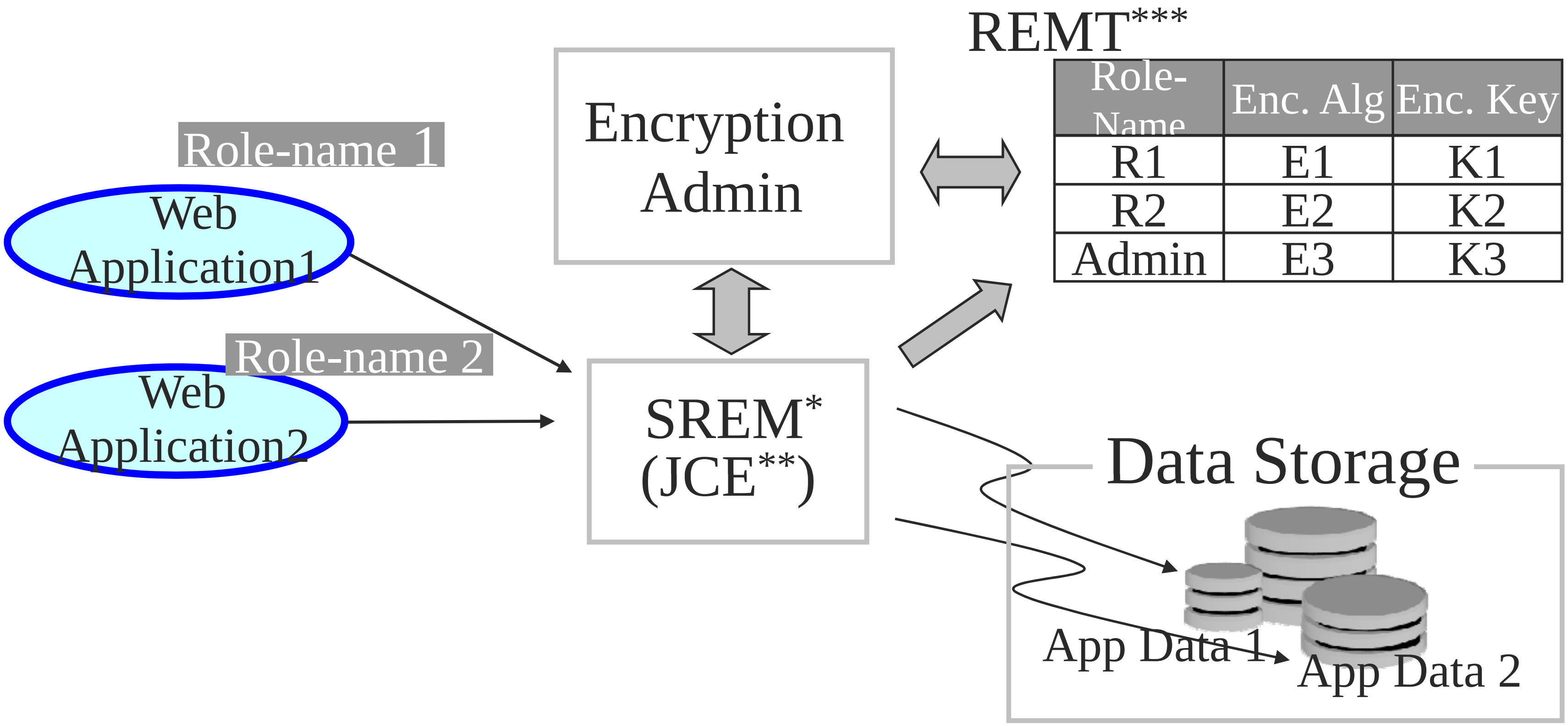
Sample Role to Encryption Mapping Table (REMT) – Cryptic

Security Role-name	Encryption Algorithm	Encryption Key Data
marketingRole	E1	K1
salesRole	E2	K2
adminRole	E1	K1

Security Role based Encryption Module (SREM)

- Application data protection based on security role.
- Common module implementation for multiple web applications.
- Use of Role to Encryption Mapping Table (REMT) to find encryption algorithm and encryption key data.

SREM



Role-Name	Enc. Alg	Enc. Key
R1	E1	K1
R2	E2	K2
Admin	E3	K3

*SREM : Security Role based Encryption Module

**JCE : Java Cryptography Extension

***REMT : Role-name Encryption Mapping Table

Figure 2: Role-name based Application Data Encryption

SREM code – key generation

```
// Retrieve encryption properties for the role from
// the REMT – determine the encryption algorithm
// and the encryption key to use …..
rolename = “marketingRole”; encalg = “DES”;

// make up the encryption key from “desKey”
enckeydata = “Life_Is_Good”;

// Generate encryption key/spec
KeyGenerator keygen = KeyGenerator.getInstance(encalg);

byte[] roleKeyData = enckeydata.getBytes();

DESKeySpec desKeySpec = new
DESKeySpec(roleKeyData);
```

SREM code – Encryption through JCE

```
// set IBMJCE provider Provider
 ibmJce = new IBMJCE();
SecretKeyFactory keyFactory =
SecretKeyFactory.getInstance(encalg,ibmJce);
SecretKey rolenameKey =
keyFactory.generateSecret(desKeySpec);
// Create a cipher instance and initialize it
 Cipher desCipher;
desCipher = Cipher.getInstance(encalg);
desCipher.init(Cipher.ENCRYPT_MODE, rolenameKey);
 // Prepare for target data and do the encryption
 origtext = “The data to be encrypted” ;
byte[] cleartext = origtext.getBytes();
byte[] ciphertext = desCipher.doFinal(cleartext);
 // Save the encrypted content to the file system
```

Application Data Encryption in PKI environment

- PKI is based on PKC / x.509 certificate
- PKI provides Encrypting File System (EFS)
- Assume that web application stores and retrieves file through EFS.
- Each user gets its own user certificate
- Set EFS file permission to users based on web application security role

Impact on Performance

- Security role based data encryption is NOT for general server side data encryption. It only applies to web application generated files.
- Performance gets affected by the size of the file, encryption algorithm and strength of encryption key.
- But the performance impact is relatively small compared to that of SSL or encrypted data I/O.

Conclusion

- Security role based encryption for web application provides extra protection for web application generated files and reports.
- Role to Encryption Mapping Table (REMT) approach allows common encryption module (SREM) for multiple web application.
- Encryption administrator maintains REMT and provides extra services.

Questions?