INFOF405: Computer Security
Project1 – Threat Modeling

21 novembre 2013

1 Modeling and Gathering Information

1.1 Use Scenarios

1. SSL connexion via OpenSSL between AS and WS1 and between AS and WS2.
2. The client is written in Java 1.7.
3. The communication between the client and AS is crypted with RSA.
4. The administrator access AS via an interface written in PHP 5.4.16.
5. Each server rests behind a firewall.
6. The servers will run on Apache 2.4.4.
7. The databases run on Mysql 5.6.12.

IF ENOUGH TIME Log the connection attempt().

8. The user cannot try more than three passwords per minute.

1.2 External Dependicies

1. Random number generator ?
2. The generated keys depend on OpenSSL.
3. The security of the access to AS depends on PHP.
4. The security of the the request depends on the firewall.

1.3 Implementation Assumptions

TO COMPLETE Encryptions respect the standards.

1.4 External Security Notes

1. The identification of the administrator is made with a password. Although special characters are required, the user is responsible for the password strength.

1.5 Internal Security Notes

1. ?

1.6 Levels of Trust

1. **Registered User** This identity gives access to the WS.
2. **Non-registered User** Can communicate with AS (which will refuse him).
3. **Administrator** Can connect through https to AS. He can registrate users, manage access control list (?), distribute RSA keys to clients, can create and distribute RSA keys to servers, can revoke keys.
4. **Web Server** Communicates with AS and te databases.

1.7 Entry Points

1. Login page for the client

1.8 The Assets

1. User info
2. Private keys
3. Stored password on the WS.

2 Analysis of the Model

2.1 Data Flow Diagram