Computer Security Endterm Assignment

Bianca Caissotti di Chiusano

Assume the following scenario: You are about to implement a Bulletin Board for Top Secret Information Exchange. Implement a sketch of your system considering the following points:

1. Which software components do you need to achieve this? (Webserver, Database server, ...)

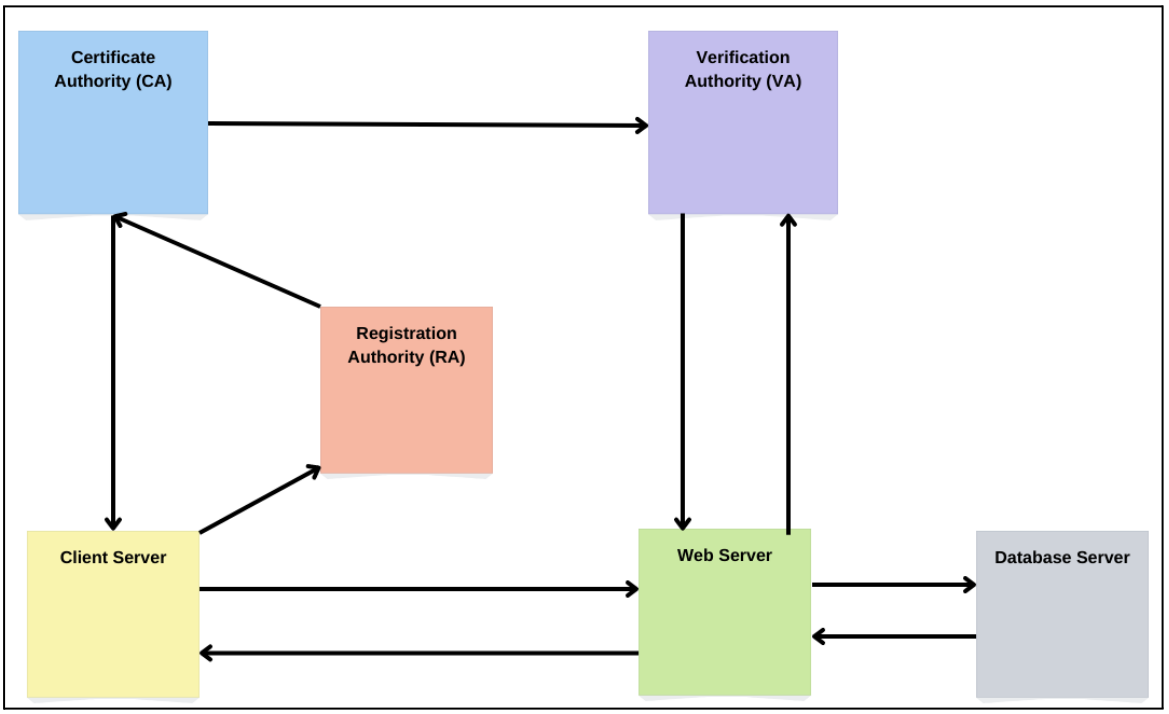
2. Do these components run on the same physical server? Give reasons for your decision.

3. How do the components communicate? (How is a connection established? Is there a need for encryption?, ...)

4. What security issues that we have discussed in the lecture about the OWASP Top Ten list can occur in your set up? For the others: Why can't they occur?

5. What can you do in order to prevent the previously identified vulnerabilities in your application?

Sketch of the System:



Components:

The task is to implement a Bulletin Board for top-secret information exchange. As this implies a medium where electronic communication occurs, we are going to use a Public Key Infrastructure (PKI) to ensure secure communication. PKI is used for authenticating users and

devices. As can be observed in the diagram, there are three servers embedded within this infrastructure. The client, web and database servers. The web server will allow the users/clients to connect to the system, or in general, display HTML content to a client (registered and authenticated through PKI) who is requesting it, hence the two arrows between client and web server. A database server stores the data, such as the Bulletin Board information. These components do not run on the same physical server, as we need to ensure that if the web server goes down, the data is still saved in the database server.

Communication between servers

An example of how these servers work together may be the following: Alice types the address of the bulletin board, which will be received as an HTTP request by the web server and will give back to Alice an HTML page displaying the bulletin board system. If Alice wants to read or write on the bulletin, the web server will access the database server using for example MySQL, which will in turn retrieve or deliver the content from or to the web server. As we want secure communication and information exchange, more authentication and security take place.

PKI components

The other components of PKI are the Certificate Authority (CA), Register Authority (RA) and Verification Authority (VA). This system is preferred to the Web of Trust as it is less vulnerable when scaling. With PKI the trust is given to the CAs, which are professional Third Parties that store, issue and sign digital certificates. These digital certificates are the public key and the identity of the client bound together. When requesting a certificate, the identity of the client has to first be verified by the RA. Once the identity is verified and the digital certificate is issued (and public key signed), this is sent back to the client. However, the CA will also send the VA a list of all certificates that were officially cancelled. The VA is publicly reachable, thus when a client wants to access the Bulletin board, the web server will verify their authenticity by checking through the VA.

Information Exchange:

The information exchange within the bulletin board may work like this: Alice and Bob want to exchange top-secret information. Alice retrieves Bob's public key from PKI and sends a message encrypted with his public key. Bob receives the message and decrypts it using his private key. Bob does the same as Alice did and they prove their identities. At this point, Alice can create a symmetric session key to start a symmetrically encrypted communication. This symmetric key is encrypted using Bob's public key and is sent to Bob. If a new member wants

to participate in the information exchange, their identity has to be verified by both Alice and Bob. And every time this group expands, every new member has to be verified by each already existing participant in the group. Everyone has to trust everyone. As Alice started this communication, she is in charge of sending the symmetric session key to whoever joined the group.

Security Issues and Preventions:

As the bulletin board may be hosted on a webpage and may have a mailing list for trusted clients, it is vulnerable to Cross-site scripting (XSS) attacks. XSS is a type of injection that sends malicious scripts to a user, which when executed can steal the user's session, sensitive data and even rewrite the webpage. A typical example of an XSS attack is a phishing email. Part of the prevention of XSS attacks is Output Encoding, so user input can only be interpreted as text and not as code (for example when new information is posted on the bulletin board).

Because we are using a database, another type of injection that can occur with our Bulletin Board setup is an SQL Injection. These can be used for spying/manipulating data and even taking over the system. We should ensure that the database can distinguish between code and data, no matter the supplied user input. This can be done through the use of prepared statements with parameterized queries.

Connecting to what was just discussed, Broken Access Control is another OWASP security issue that can occur in this system. This is when users act outside of their permissions, like modification or destruction of existing data. For our specific example, to prevent this issue, access should be denied by default, except for public resources. Moreover, there should be enforced record ownership to prevent users from just being able to access any record. Lastly, disable the web server directory listing.

Looking at other OWASP security issues, the authentication, such as "*Broken Authentication*" issues should not occur because we are using the PKI infrastructure, thus there is no user and password input, but authentication occurs through the verification of the client's digital certificates, and public/private key usage. The issue that could occur is if an attacker manages to find a trusted/verified client's private key.

However, with the PKI infrastructure, there can be other security issues outside of the OWASP Top Ten. An issue is if there is a loss of trust in the CA, such as if certificates are issued so an unintended party or if there is a failure in renewing or revoking them.