TÉCNICO LISBOA

Workshop – Grupo 6

Secure Grades System

66047 – João Pinho | 68147 – Frederico Mendes | 68158 – João Sousa

Problem!

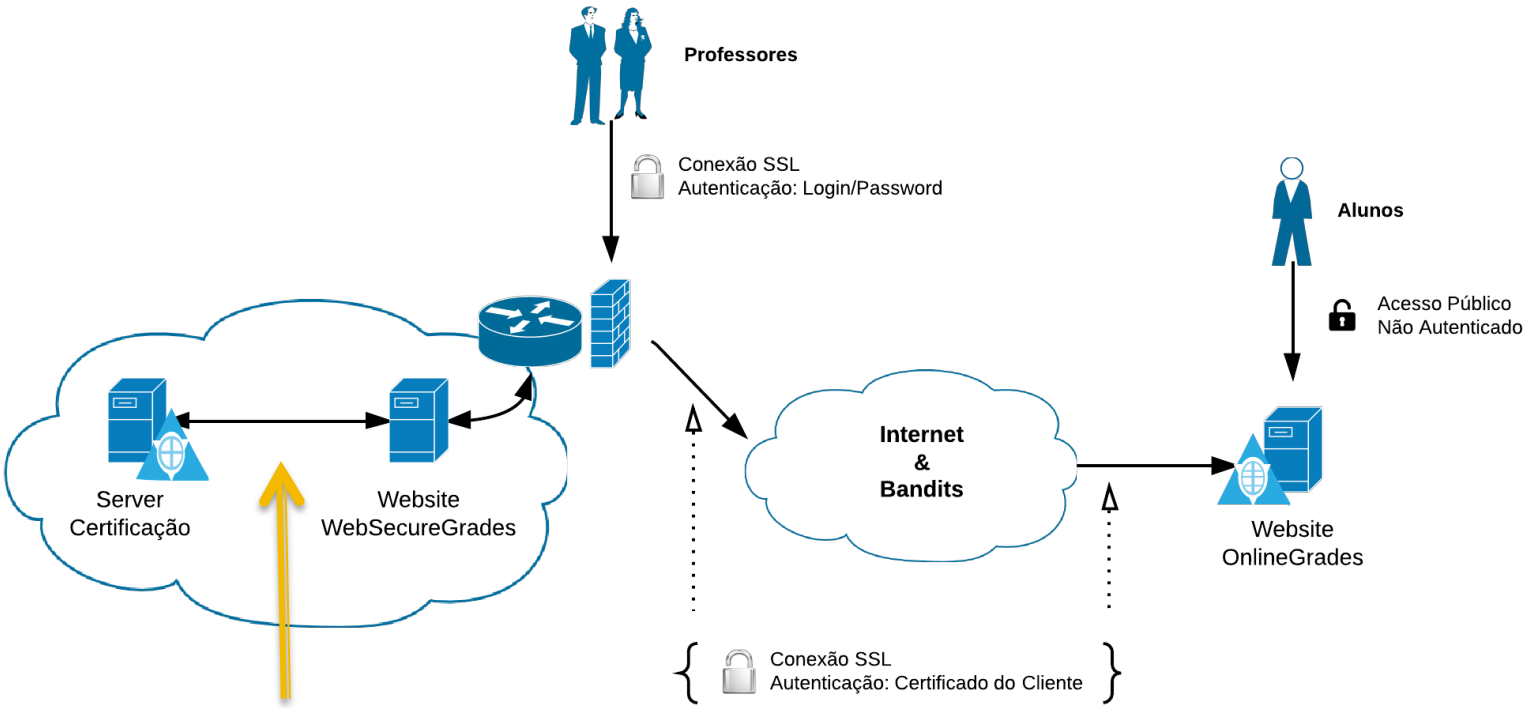
- The work aims to implement the secure submission and correction of students' grades in the Fenix system. It is suggested the development of a system to digitally sign documents with the student evaluations.

- The documents to be signed must be converted to a standard XML format. It should be studied the infrastructure that allows the update notes for teachers.

Security Considerations

- To implement a secure system the following considerations were taken into account:
  - An HTTP connectio to the WebSecureGrades Website over SSL, with Login authentication (username and password);
  - The grades uploaded into the WebSecureGrades are signed in a Certification Server, before they get sent to the Online Grades (the publishing system);
  - The connection between the WebSecureGrades and the OnlineGrades is done over HTTPS with authentication of both parties done by their respective certificates.

Solution Architecture



Pressupostos!

WebSecureGrades

- Website System that allows professors to sign-in and submit students grades to an external publishing system, securely!
  - Login
    - Password and Salt generated via CSPRNG are stored in the database;
    - Validation process verifies SHA1(Pass)+Salt = SHA1(DbPass) + Salt, if equal, login succeds!

Grades Certifier WebService

- The Certification Server, it's a machine were it's installed a WebService responsible for signing student grades data.
- It signs the binary representation of the data in XML.
- To assure all parties are in sync they must all speak the same language, because of that a XSD schema was created to assure the signatures on both ends have a valid match when the data is actually valid!
- Signature Process:
  - signature = rsa.SignData(SHA1(Data), "SHA-512)
- WebService Response is Base64(signature)

OnlineSecureGrades

- **Grades Publishing WebService**
  - This WebService receives the students grades along with the data signature;
  - The students grades are published only if:
    - The connection is secure: SSL (HTTP accesses to the WS are automatically refused!)
    - The Client Certificate is of the OnlineSecure Grades System trust, this is, a match is done with the ClientCertificateHashString and the ServerClientKnownPublicCertificate;
    - The data being sent is signed with the WebSecureGrades System Private Key.
  - Fulcral Properties Assured: Non Repudiation, Confidentiality, Integrity!

Conclusions

- We consider the solution robust, simple and secure! Do you? Questions?

- Our shared definition of secure: “It’s secure if the **cost** of the attacker in terms of resources, effort and time to break the overall system security is a considerably higher than the value of what we intent to keep secure”.