Distance Formula for XML Signature

Electrical and Computer Engineering — **Washkewicz College of Engineering**

Minusha k
minusha46@gmail.com

Mansi Trivedi
mansi.joshi@outlook.com

Advisor : Dr.Abdul Razaque
arazaque@bridgeport.edu

Abstract

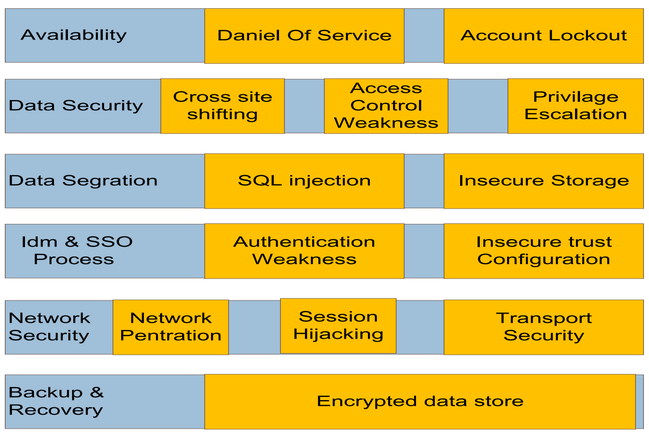
In this paper we present the vulnerabilities of SaaS architecture for security attacks and address the authentication attack among them. In our study we noticed that every attack is possible only when the attacker overcomes the obligations of authentication and once he gains the access then everything is in his hands. So this paper will go deep into the authentication attack, SaaS architecture weaknesses for it.

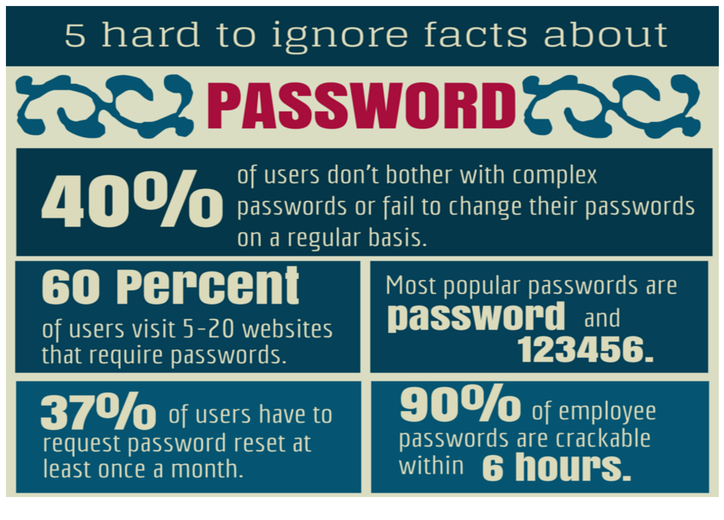
Introduction

Identity management [IDM] and sign-on process is for authentication purpose. It authenticates the clients to access the requested data. It stores the complete information of the users and their access accounts, id's, passwords, authorization rules etc. So if there is any data breaches found it 1st actually addresses authentication vulnerability. This is the part that should be secured first .

For providing this service, we did detailed analysis of how single sign on works. The Single Sign-On is greatly used to curtail the incidents which are mostly related to passwords. By considering this strategy, it makes the user to use more productive process of authentication and enhance the convenience . Single Sign-On is meant as by using this mechanism the user uses single action of authorization and authentication which allows the user to connect different types of computers.

Authentication Attack

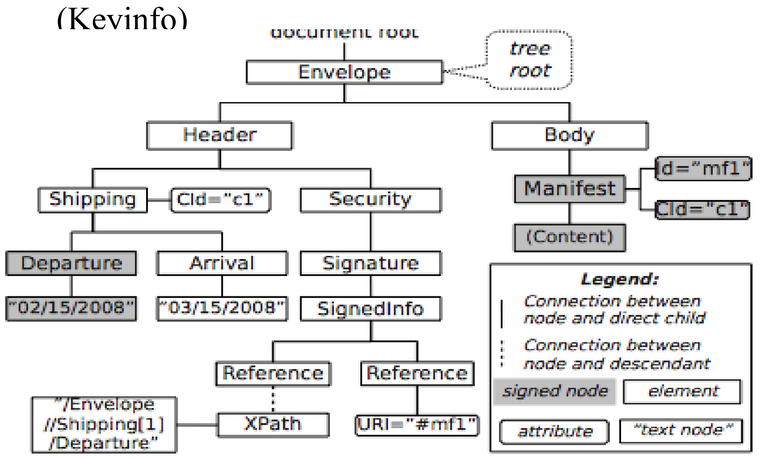




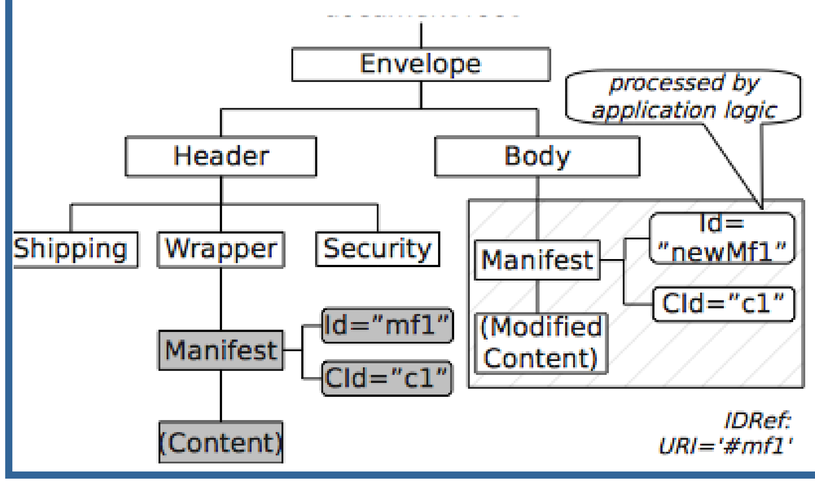
How XML Signature Works?

Structure of Xml signature:

```
<Signature>
  <Signedinfo>
    (colonization method)
      (signature method)
        (<Reference (URI=)?>
         (Transforms)?
          (Digest method)
            (Digest Value)
        </Reference)+
  </Signedinfo)
  (Keyinfo)
```



Wrapping Attack



Mathematical Calculations

a.)Message received & sent = [existing header] + [length of the message] + [size of the message] + [last modified timestamp of message] + [length of header and body]

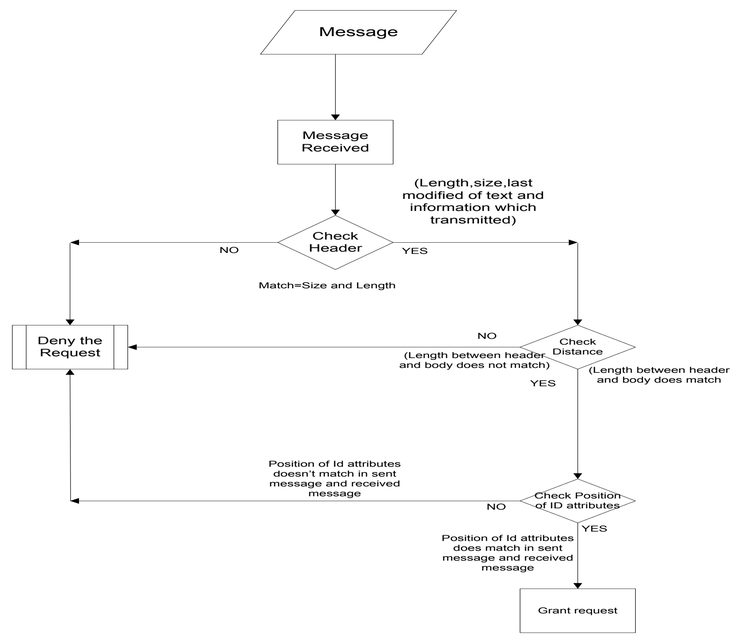
b.)Distance between header and body (ID) = [message length between header and ID in sent] – [message length between header and ID in received]

c.)Position of header and body (ID) = [difference in position of header and body (ID) in sent] – [difference in position of header and body (ID) in received]

Proposed Plan- Algorithm

1.Initialization of message M(sent from client to IDP for authentication)
2.Initialization of Parameter Lhs = Length of header and body at sender , Lbr= Length of header and body at receiver, Shs=size of header and body at sender, Sbs= size of header and body at receiver, Ths= Timestamp at sender , Thr = Time stamp at receiver, Dc-Da= Distance between header and Id attributes of body, Pc-Pa= Position of header and Id attributes of body.
3.C0= compare the length of the header, size of the header and time stamp between sender and receiver, C1= compare the distance between header and body attributes, C2= Compare the position of id attributes.
4.While message M received at C0- Length of header and body at sender and receiver Lhs, Lbr Size – Shs and Sbr and timestamp Ths and Thr
5.At C0
6.If Lhs=!Lhr, Shs=!Shr && Ths=!Thr then Message M is denied
7.Else if
8.At C1 9. If Dc-Da=!0 then Message M is denied 10.Else if 11.At C2
12.Pc-Pa =!0 then Message M is denied
13.Else Signature is verified
14.End if 15.End if 16.End if 17.End While.

Flow Chart



Conclusion

To successfully validate the step b and c, the value of the outcome after this calculation should be zero (0).By Using the proposed method which is discussed above will be helpful to close the wrapping attack with this we can close the vulnerabilities of SSO used in IDM. By closing all these we can close the authorization attack which can improve the architecture of SaaS model .With this the efficiency of SaaS improves reliable and less prone to attacks.