Chapter 7

Securities Perspective in ESB-Like XML-Based Attacks: Interface Abstraction, Data Privacy, and Integrity

Ayush Gupta
SISA, India

Ravinder Verma
Protiviti, India

ABSTRACT

In today's world where technology drastically changing and we supposed to believe that layer 7 protocol HTTP(s) is sufficient from the security perspective. But it’s not, malicious user or hackers are so prudent in their attacks that most of the breaches occurs at layer 7 i.e. HTTP/HTTPS. And XML based attacks either of XML parser attack, XML generator attack or XXE Denial of service attack etc. are all comes in the first place of OWASP TOP 10 vulnerability. HTTPS connection is not sufficient enough to stop masqueraders or attackers, as XML injection or XSS attack doesn’t care about the encryption of data as it deals with the scripts mainly. ESB where considered as pluggable device where all the existing systems or IT infrastructure devices can be exposed to new applications and cut the time and cost by implementing this. But data travels on the bus is always be preferred on XML and here it’s all security & privacy issues comes into picture and the same has been highlighted in this chapter throughout.

INTRODUCTION

ESB where considered as a service oriented infrastructure component which actually helps services to interact via messages and events. But now a days’ paradigm has been changed and the SOA which helps in providing B2B services and cutting cost effectively is no more reliable with traditional ESB. Because XML attacks/injection is not only a factor while using ESB but data privacy & integration is also a major concern. Protection of internal applications is one of them while interfaces are exposed to external parties.

DOI: 10.4018/978-1-5225-2157-0.ch007
in B2B/server to server communication and henceforth data privacy & integrity can’t be maintained most of the times. Interface abstraction was not as powerful to encapsulate the message among layers due to the emerging XML based attacks where you IP based firewalling is not enough instead the application interaction using the service interfaces like XML, JSON, SOAP and REST API etc.

One of the best solution is to use SOA Gateways instead of traditional ESB where not only it protects from new threats like XML based but also provides endpoint abstraction plus message and field level data integrity and privacy as well. The only thing while deploying the SOA gateways is vendor implementations for example custom code shall not be allowed to add to your XML gateway just like we don’t add any custom code at network packet firewall. And the only IBM DataPower (2016) and Forum Sentry are the products who don’t permit code to be injected or dropped at XML gateways while CISCO ACE Gateway (Cisco, n.d.) does. So choosing the appropriate protocol with appropriate format to deliver the message to the target destination is one of the crux to keep in mind for SOA Gateway Vendor implementations (SOA Expressways, n.d.). But it doesn’t mean that we exclude the idiosyncrasies or security features of SOA gateway which ultimately once configured correctly will guarantee the best security in the environment. There is believe that SOA gateway can be worked and considered as half of Web Application Firewall as it allows to configure the policies and ACL.

So this is not just limited with the limitations and security aspect in ESB. There is much more detailed and descriptive information has been required to depth look into to actually know how the new threats actually like XML attacks intercept the request and response and do the malicious tasks as per they like. XXE based attack, Injection & generator attack are just one of the kind. How in depth privacy comes into the picture and how actually it evades at deep web network? How & what kind of privacy laws and security certifications (ex. FIPS 140-2 gold standard) can provide security assessment? Why traditional approach of ESB was not sufficient enough to protect the data in message? What kind of OWASP TOP 10 vulnerabilities comes into the play, what are their severity score to hamper the business and what could be the mitigations? What Keys, Encryption/Signature policies can be utilized to secure at XML gateway?

Related Work

As of now every organization is focused on implementing the ESB architecture and publishing new applications over it to make their business continue. And XML is one of the facility which not only transports data but also provide security also. And it was observed that now a days so many XML attacks has been come which can steal confidential information and even put the company’s reputation into the matter of concern. Till now OWASP top 10 specifies such attacks and their mitigation. But author has also noted that not only security researchers had devoted their time and provide a framework of OWASP which take care of web application security but instead big organization are also active in the market and coming up with the product security where manual intervention is required at least as possible. And authors reviewed that industry leaders (Cisco, n.d.; IBM, 2016; Ca technologies, 2014) are such who came up with CISCO Ace gateway (Cisco, n.d.), IBM DataPower (2016) and Forum Sentry. But they do have their own limitations with respect to privacy which can only be implemented by both entities who are sharing the information over the web and it could be between B2B or between users to companies. The author tries to provide security issues in ESB and what are the possible solutions in the market in either form or product and high lightened the privacy issues to be take care.

Some of the prevalent attacks in the present industry & some privacy issues which will become more frequent: