A STUDY OF SECURITY ISSUES IN WEB SYSTEMS

Solijonov Madaminbek Botirjonovich
Graduate student of the Nurafshan branch of the Tashkent University of Information Technologies named after Muhammad Al-Khorazmi

Annotation: *Web Services are a promising solution to an age-old need: fast and flexible information sharing among people and businesses. They represent the next phase of distributed computing, building on the shoulders of the previous distributed models. Web Services leverage the ubiquity of the Internet to link applications, systems, and resources within and among enterprises to enable exciting, new business processes and relationships with customers, partners, and suppliers around the world. Web Services are a promising solution to an age-old need: fast and flexible information sharing among people and businesses. They represent the next phase of distributed computing, building on the shoulders of the previous distributed models. Web Services leverage the ubiquity of the Internet to link applications, systems, and resources within and among enterprises to enable exciting, new business processes and relationships with customers, partners, and suppliers around the world. They enable access to data that has previously been locked within corporate networks and accessible only by using specialized software. Along with the benefits of Web Services comes a serious risk: sensitive and private data can be exposed to people who are not supposed to see it.*

Key words: *security, web services, distributed computing, link applications.*

Introduction Web Services (Neil, 2003) are loosely coupled self-contained, self-describing and modular applications that can be described, published, located and invoked over a network. Web services can be provided on any platform and may be written in any programming language. Web services are the newest incarnation of middleware for distributed computing and unlike all previous forms of middleware, it is a simpler, standards-based, and more loosely coupled technology for connecting data, systems, and organizations. Web Services essentially involve the three roles of Service Oriented Architecture (SOA): service provider, service requester and service broker. A service provider could be an industry, business or a company capable of providing service. A requester also could be a company or a business that is in need of the service, where as the broker is a place, entity or a system that helps both service provider and service requester to discover each other. Basically, four technologies form the basis of Web services: eXtensible Markup Language (XML); Simple Object Access Protocol (SOAP); Web Services Description Language (WSDL); and Universal Description, Discovery, and Integration (UDDI). XML: eXtensible Markup Language (XML) was created as a structured self-describing way to represent data that is totally independent of application, protocol, vocabulary, operating system, or even programming language. XML was initially developed to overcome the limitations of HTML, which is good at describing how things should be displayed but is poor at describing what data to be displayed. SOAP: Simple

Object Access Protocol (SOAP) is used for communication among different Web Services. SOAP was created as a way to transport XML from one computer to another via a number of standard transport protocols. HTTP is the most common and the most prevalent transport used by the Web itself. SOAP (Mcintosh and Austel, 2005) messages flow from originator to an ultimate receiver through a SOAP message path. A SOAP message consists of Soap Envelope which contains Soap Body element and an optional Soap Header element. The Soap Header element may contain a set of child elements that describe message processing that the sender expects a recipient to perform. Below is a typical SOAP listing.

01 ‹Soap: Envelope—-◊
02 ‹Soap: Header (optional)›
03 ‹Soap: Body› (mandatory)
04 ‹get Quote symbol = "——"/›
05 ‹/Soap: Body›
06 ‹/Soap: Envelope›

SOAP envelope is used to encapsulate the SOAP message. SOAP header is the optional part of the SOAP protocol. Header contains information for the SOAP node, the processor of the SOAP message, how to process the SOAP message. This may be authentication, routing etc. Soap body contains the targeted to the SOAP message receiver. Get Quote element is the child of SOAP body. WSDL: Web Service Description Language (WSDL) is used to describe the functionalities of the services. It is an XML language that defines what the input and output structure will be for a Web service, and what one expects to see in the payload XML message. WSDL is how one service tells another which way to interact with it, where the service resides, what the service can do, and how to invoke it. Once the requester receives the WSDL document for the candidate Web service, it must be validated. The simplest method of doing this is to provide a digital signature of the WSDL document for the requester to use. Requesters cannot connect to most providers without some form of authentication. The major problem with modern Web applications is that, they serve as key entry points for all kind of cybercrime which may be directed on entrepreneurs and business organizations over the internet. Web security breaches have become more common nowadays, due to the increased usage of Web-based applications. As a matter of fact, many big and small organizations around the world have reported incidents of Web application breaches that have dealt massive blows on their financial strengths and reputations. It is estimated that 75 percent of all major business organizations in the world have been victims of cybercrime at least once in the last 24 months. This intrusion has resulted into identity theft, breach of potential data, and defacement of brand, among other serious effects. This constant breach of Web applications is a clear indication that existing safety measures have failed to protect individuals and organizations against the dangers of insecure online environment. Following is a summary of some of the common Web application security issues observed in the current world.

Technical Web attacks This refers to the practice of interfering with Web applications in a technical manner by using hacking approaches such as cross-site scripting and SQL. Among various other hacking techniques, these two are believed to be the most common ones that are used by cybercriminals to execute online fraud on unsuspecting users. Cybercriminals are becoming more intelligent as the development in technological innovations continues to rise and this has tremendously accelerated the rate of Web attacks around the globe (Huang et al. 2003).

Business Logic Threats Apart from the technical Web attacks discussed above, cybercriminals have also been engaging in business logic fraud of late. As a matter of fact, hackers are spending many hours online perusing Websites for valuable information that will enable them exploit or mitigate users who might be of particular interest to them (Curphey & Arawo 2006). As it would be observed, hackers with the intention of carrying out this form of fraud are mainly equal opportunists who are in the look out for ways to compromise, wreck and tarnish the reputation of competitors in the market. Hackers conducting business logic threats could also be operating on behalf of business organizations against their rivals in the market. Once they make their way in the Web applications or databases of the targeted organizations, the hackers will be seeking to unveil valuable information that could be used to bring the targeted organizations down.

Conclusion Hackers have become more industrialized in their mission to steal users' personal data for fraudulent reasons. Internet fraud has emerged as the biggest security threat that has ever happened to Web applications nowadays. The bitter truth, however, is that modern security products such as IPS and firewalls have completely failed to provide desirable security levels against these growing threats. Web applications have found great use in the corporate world nowadays than at any other time in history. In this regard, there is a need for enterprises to utilize effective security programs that will play a key role in safeguarding their most important business data from cybercriminals. I suppose that the internet will be a safe environment to trend on in the future, with these measures having being put in place.

REFERENCES:

1. Cheswick, W, Bellovin, S & Rubin, A 2003, *Firewalls and Internet security: repelling the wily hacker*, Addison-Wesley Longman Publishing Co., Inc., Chicago, Illinois.

2. Curphey, M & Arawo, R 2006, 'Web application security assessment tools', *Security & Privacy, IEEE*, vol. 4, no. 4, pp. 32-41.

3. Huang, Y, Huang, S, Lin, T & Tsai, C 2003, 'Web application security assessment by fault injection and behavior monitoring', *In Proceedings of the 12th International Conference on World Wide Web*, vol. 17, no. 9, pp. 148-159.

4. Joshi, J, Aref, W, Ghafoor, A & Spafford, E 2001, 'Security models for web-based applications', *Communications of the ACM*, vol. 44, no. 2, pp. 38-44.

5. Pfleeger, C & Pfleeger, S 2007, *Security in computing*. Prentice Hall, Upper Saddle River, NJ.

6. Stuttard, D & Pinto, M 2008, *The web application hacker's handbook: discovering and exploiting security flaws*, John Wiley & Sons, Hoboken, NJ.