**From Distributed Computing to Microarchitectures – Activity**

Vulnerabilities at the business processes layer are listed below. **Are you able to provide a description of each?**

- Business Process Execution Language (BPEL) scanning.
- Metadata spoofing.
- BPEL state deviation.
- Instantiation flooding.
- WS-Addressing spoofing.
- Workflow engine hijacking.

**Feel free to discuss your responses with your tutor/team.**

1. **Business Process Execution Language (BPEL) scanning.**

Business Process Execution Language (BPEL) is a powerful, executable language that facilitates interactions with web services, enabling transactions and human engagement. Its primary function is to compose synchronous and asynchronous services, integrating them into seamless process flows (Oracle, N.D.).

Therefore, Wright (N.D.) explains that BPEL, an XML-based language, facilitates communication and data sharing between web services, APIs, and human procedures in a service-oriented architecture (SOA) for business workflow.

2. **Metadata spoofing.**

A Metadata Spoofing attack is a cyber-attack that aims to deceive victims into thinking that the malicious resource they are accessing is actually from a trustworthy source. The main objective of this type of attack is to trick users into using the malicious resource, which could cause a range of negative technical consequences. This kind of attack can be carried out by manipulating metadata, which includes information about the file, such as its type, size, and author, among other things. The attacker can modify the metadata so that the malicious resource appears legitimate, making it more likely that the victim will be fooled into using it. Once the victim uses the malicious resource, it can result in various adverse consequences, such as data theft, system compromise, or other forms of cyber-attacks (Kaspersky, 2021).

3. **BPEL state deviation.**

Web Services Business Process Execution Language (WS-BPEL), also known as Business Process Execution Language (BPEL), is an OASIS standard used for external communication partners. An engine that supports BPEL provides Web Service endpoints that accept all incoming messages, thus resulting in potential vulnerabilities such as BPEL Correlation Invalidation and BPEL State Invalidation (Masood, N.D.).

4. **Instantiation flooding.**

Instantiation flooding is a cyber-attack in which many instantiations are sent to a system to overwhelm it. This attack can cause the system to crash or become unresponsive, leading to significant disruptions in operations. Organisations must be aware of this attack and take measures to prevent it (Gunestas & Wijesekera, N.D.).

5. **WS-Addressing spoofing.**

WS-address offers supplementary routing details within the SOAP header to facilitate asynchronous communication. However, in a WS-address spoofing assault, the perpetrator dispatches a SOAP message with counterfeit WS-address data to the server. The <ReplyTo> header then comprises the endpoint address designated by the perpetrator rather than the web service client's address.

6. **Workflow engine hijacking.**

Workflow engine hijacking refers to malicious actors who exploit how applications are executed in operating systems, allowing them to manipulate the system's behaviour and run harmful payloads for an extended period. This can be achieved through different methods, such as tampering with program and library locations or contaminating file directories with malware. It is crucial to be aware of this threat and take necessary precautions to protect against such attacks (ATT&CK).

**References:**


Oracle (N.D.). *Business Process Execution Language (BPEL)*. [online] Available at: https://docs.oracle.com/cd/E16764_01/admin.1111/e12782/c08_bpel002.htm [Accessed 17 Oct. 2023].

Wright, G. (N.D.). *What is BPEL (Business Process Execution Language)?* [online] Available at: https://www.techtarget.com/searchapparchitecture/definition/BPEL-Business-Process-Execution-Language.

Kaspersky (2021). *What is Spoofing?* [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/spoofing.

Masood, A. (N.D.). *Cyber security for service oriented architectures in a Web 2.0 world: An overview of SOA vulnerabilities in financial services*. [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6698966.

Masood, A. (N.D.). *Cyber security for service oriented architectures in a Web 2.0 world: An overview of SOA vulnerabilities in financial services*. [online] Available at: https://ieeexplore.ieee.org/document/6698966.

Gunestas, M. & Wijesekera, D. (N.D.). *Online detection of web choreography misuses*. [online] Available at: https://ieeexplore.ieee.org/document/5363416 [Accessed 30 Oct. 2023].

Examtopics (N.D.). *Exam 312-50v11 topic 1 question 364 discussion - ExamTopics*. [online] Available at: https://www.examtopics.com/discussions/eccouncil/view/63044-exam-312-50v11-topic-1-question-364-discussion/ [Accessed 30 Oct. 2023].

ATT&CK (N.D.). *Hijack Execution Flow, Technique T1625 - Mobile | MITRE ATT&CK®*. [online] Available at: https://attack.mitre.org/techniques/T1625/ [Accessed 30 Oct. 2023].