Software Architecture Series

Microservices Security

Check List

When designing a secure microservices architecture, use this checklist to make sure your microservices architecture is as secure as possible.

Topic	Description	Notes
Map external and internal services	Check which of the services are external (=allow external access) and which are internal (=allow access only from other services). Work with the security team of the organization to decide the security policy of each type of services. For example, you might decide that external services require TLS communication while internal do not.	- If there isn't a security team in the organization, make these decisions by yourself and try to make educated decisions based on the type of systems and

	Or – that external services require end user authentication while internal service require service identity.	data the organization works with.
Encrypt communication	Make sure all communication to services (or external services) is encrypted. Make sure the encryption protocol is up to date. As of writing this document, you should use only TLS versions 1.2 and up.	
Encrypt data	Make sure all data in the system is encrypted. Note that all modern databases offer built-in support for data encryption, use it.	
Decide on type of authentication required	Decide (with the organization’s security team) on the type of authentication required in the system. Mainly – service identity vs end user identity.	As mentioned above, sometimes the decision will be to go with both.
Implement authentication	If using service identity – decide on API key vs access token. Note that for access token you’ll need external authentication engine.	

	If using end user authentication – implement OAuth2 flow.	
Implement authorization	Authorization should be implemented in the service's code. Check the roles of the user / service, and limit access to the allowed functionality only.	
Implement logging	Log every security related event. Even if you're not sure whether an event is security related (for example – unauthorized access), assume it is and log it as such.	
Connect to SIEM tool	If the organization has a SIEM tool in place, make sure your security logs are connected to it, to enable the organization to have a holistic view of the information security state.	

I Hope you enjoyed the course, and that it made you a microservices security expert. I'm sure you'll now be able to design secure microservices systems, and that it made you a better Architect!

For any question or comment contact me at:

memi@memilavi.com

Thanks,

Memi