CTC 14

2d Lt Marvin Newlin

CSCE 525

26 Nov 18

Two principles that can help the cyber community become more secure are fail securely and don’t trust services. As the cyber community moves towards centralizing systems, the principle of failing securely is a must. With all the legacy code that exists in Air Force systems, ensuring that systems, when they fail (and they will) do not allow users to access things they shouldn’t. Failing securely is important because if a system fails or throws an exception, then we need to be able to ensure that the system doesn’t allow any access during that failing period (“Security by Design Principles - OWASP” 2016).

As we move toward enterprise IT as a service, the principle of not trusting services becomes paramount. Not trusting services is important because we aren’t necessarily able to peek behind the curtain and see what is coming in with the data from our service. This makes it important to not implicitly trust that what is coming in is perfectly okay because if an outside service gets compromised and we use it in a way that doesn’t verify it, then we can get burned by not verifying that it is what it says it is (“Security Principles” n.d.). An example of this is utilizing the Amazon Web Services cloud. If something in Amazon gets breached then as long as we aren’t implicitly trusting the data coming from the AWS cloud and we verify it first, then we can insulate ourselves from the breach.

References

“Security by Design Principles - OWASP.” 2016. 2016. https://www.owasp.org/index.php/Security\_by\_Design\_Principles.

“Security Principles.” n.d. Accessed November 26, 2018. http://www.cs.ucsb.edu/~kemm/courses/cs177/principles.pdf.