**LM 2. Information Security Essentials**

1. **LM2. Student Learning Outcomes**

After completing this module, a student will be able to:

* Define Information Security and Wireless Security
* Describe the five principles Information security: CIA triad, Non-repudiation and Accountability.
* Explain the difference between symmetric key cryptography (SKC) and public key cryptography (PKC).
* Describe how integrity is achieved through hash function.
* Describe how digital signature works
* Define the AAA of information security
* Discuss the threats category to wireless network/device
* Describe the five pillars of information security.
* Discuss defense in depth in information security
* Discuss information security standards and regulatory compliances.

1. **LM2. Learning Material & Study Guide**

Note: this module covers important concepts related to information security. Many of the concepts you already learned from previous class. We will discuss the threats and vulnerabilities specific to wireless and mobile network and corresponding mitigation strategies in future modules.

* Define Information Security and Wireless Security

<https://en.wikipedia.org/wiki/Information_security>

<https://en.wikipedia.org/wiki/Wireless_security>

* Describe the five pillars of information security.

<http://cf.rims.org/Magazine/PrintTemplate.cfm?AID=2409>

* Discuss defense in depth in information security

<https://en.wikipedia.org/wiki/Defense_in_depth_(computing)>

* Multiple layers of security control from physical controls, to technical controls and administrative controls
* Define the AAA of information security

<http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting>

-Define authentication, authorization, and accounting

* Describe the five principles Information security: CIA triad, Non-repudiation and Accountability.

<https://www.usna.edu/CyberDept/sy110/lec/pillarsCybSec/lec.html>

-What are confidentiality, integrity, availability, accountability, Non-repudiation and Authentication? What are the ways to achieve those principles? Confidentiality – encryption; integrity – hash algorithm; availability – prevent denial of service attack; accountability – authentication; Non-repudiation – digital signature and Authentication

* Explain the difference between symmetric key cryptography (SKC) and public key cryptography (PKC).

SKC:<http://www.webopedia.com/TERM/S/symmetric_key_cryptography.html>

AKC: <https://en.wikipedia.org/wiki/Public-key_cryptography>

Hybrid cryptograph: <https://en.wikipedia.org/wiki/Hybrid_cryptosystem>

-confidentiality is achieved through encryption; hybrid cryptograph combines the strength of both SKC & AKC

* Describe how digital signature works
* <https://en.wikipedia.org/wiki/Digital_signature>

-Digital signature can be generated using the private key of AKC system. It’s used to authenticate the sender, ensure the non-repudiation, and integrity of the message.

* Describe how integrity is achieved through hash function.

<https://www.tutorialspoint.com/cryptography/data_integrity_in_cryptography.htm>

* Discuss the threats category to wireless network/device

-there are generally three types of threats: system access, device control, and data theft.

* Discuss information security standards and regulatory compliances.

<https://en.wikipedia.org/wiki/Cyber_security_standards>

<https://www.tcdi.com/information-security-compliance-which-regulations/>

* For cyber security standards, focus on ISO/IEC 27001: 2013, ISO/IEC 27002: 2013, NIST SP 800-53. For Regulatory compliance, focus on Sarbanes-Oxley Act, GLBA, HIPPA, PCI-DSS.