IA 315: Information Security Auditing and Assurance

- **Name:** Dr. Jabhera Matogoro
- **Office #:** B13, CIVE Admin Building
- **Course Aim:**
  - The course aims at enabling students to get knowledge, tools and skills to conduct security audit on organization's network, wireless network, applications, database, software, web server and email security.
  - Also enable student to write security auditing report.

IA 315: Information Security Auditing and Assurance

- **Course Objectives**
  - Students will understand security of different access points,
  - Students will understand and acquire knowledge and skills for analyzing and managing vulnerability
  - Students will be imparted with the knowledge of how exactly to go about auditing the security of an enterprise
  - Students will be able to acquire skills and ability to analyze practical development processes in terms of their prospects and problems.

Key Management

- Cryptography is used to secure communications over networks, to protect information stored in databases, and for many other critical applications.
- Cryptographic keys play an important part in the operation of cryptography.
- These keys are analogous to the combination of a safe.
- If a safe combination is known to an adversary, the strongest safe provides no security against penetration.

Why Key Management Matters?

- The proper management of cryptographic keys is essential to the effective use of cryptography for security.
- Poor key management may easily compromise strong algorithms.
- This Recommendation provides guidance on the management of a cryptographic key throughout its lifecycle, including its secure generation, storage, distribution, use, and destruction.

Why the Strength of the Keys Matter?

- Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of cryptographic mechanisms and protocols associated with the keys, and the protection provided to the keys.
- Secret and private keys need to be protected against unauthorized disclosure, and all keys need to be protected against modification.

Applications of Cryptographic Keys

- Cryptographic keys are used across a broad range of systems and applications in enterprises, many of which are managed by individuals who may not have expertise in key management.
- Consequently, organizations must ensure that clear guidance and oversight is provided for the proper management of keys, as well as controls to ensure that the guidance is being properly followed and implemented.

Choices in the use of Cryptographic Mechanisms

- Organizations and developers are presented with many choices in their use of cryptographic mechanisms.
- Inappropriate choices may result in an illusion of security but little or no real security for the protocol or application.
- This Recommendation (i.e., Special Publication (SP) 800-57) provides background information and establishes frameworks to support appropriate decisions when selecting and using cryptographic mechanisms

Cryptographic Modules

- Cryptographic modules are used to perform cryptographic operations using these keys.
- This Recommendation does not address the implementation details for cryptographic modules that may be used to achieve the security requirements identified herein.
- These details are addressed in Federal Information Processing Standard (FIPS) 140 [FIPS 140] and its associated implementation guidance and derived test requirements (available at https://csrc.nist.gov/projects/cmvp/).

Cryptographic Modules

- The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.
- Read:
  - Government Information Technology Management: Past and Future Issues - Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act) (everycrsreport.com)
  - Information Technology Laws: Handbook-Laws (cio.gov)

Resource Public Key Infrastructure (RPKI)

- RPKI facilitates the validation of routing information by other network operators on a global scale and forms one of the fundamental building blocks of routing security on the Internet.
- As a network operator, creating RPKI a Route Origin Authorisation (ROA) object(s) that cover all the prefixes you advertise to your BGP peers is the best common operational practice.
- It is also one of the Mutually Agreed Norms for Routing Security (MANRS') actions that a network operator can implement to demonstrate a commitment to running a safe and resilient Internet.