Annexure - III

CA 836 SECURITY ASPECTS OF CLOUD ARCHITECTURE

Introductory Topics: Domain of information security. Taxonomy of information security, Information as an asse Need for securing information in the contexts of individuals, organizations, business, and government. Impact o information security on ensuring security in a broader context. System security topics : Access Control - MAC DAC, RBAC. Security Models as basis for OS security - BLP, Biba, Chinese Wall and Clark Wilson. Introductio to DB Security. Software vulnerabilities - Buffer and stack overflow, Phishing. Malware - Viruses, Worms and Trojans. Topological worms. Internet propagation models for worms.

Cryptography Topics: Secret vs. Public, Secret Key - DES, Public Key - RSA, Cryptographic hash - SHA1, Discrete Log - Diffie Helman, Digital certificates and PKI. Evolution of cryptography – from Enigma to Elliptic Curve Cryptography. Interlinkings with number theory and other developments in mathematics. Development of cryptographic protocols. Concept of cryptocomplexity. Protocol topics: One way and two way authentication, Centralised Authentication, Needham-Schroeder protocol, Kerberos. Biometrics for authentication - methods and error types.

Information security in the context of Trust and Privacy. Models of trust and computational aspects. Difference between privacy and security. Relevance of privacy rights from individual and organizational viewpoints – links with information security. Security as a dynamic equilibrium between attacks and defenses. Modeling attack and defense mechanisms using game theoretic concepts.

Enterprise security - Policy, Standards, Guidelines and Procedures. The balance between operational security and compliance/legal requirements in specific domains – An example of financial (SOX) or health (HIPAA) may be adopted. International standardization – ISO 27000 series (1 to 6) – salient features.

Security in current applications Cases from any two of the three topics: Online banking or Credit Card Payment Systems, Web Services Security, RFIDs.

References

1. Bernard Menezes, Network security and Cryptography, Cengage Learning India, 2010.
2. Dieter Gollmann, Computer Security, 3rd edition, John Wiley and Sons Ltd., 2011.
3. Whitman and Mattord, Principles of Information Security, 4th edition,Cengage Learning, 2011.
4. Information Security Management Handbook, 6th Edition, Harold Tipton, Micki Krause (Editors) Auerbach / CRC Press, 2012.
5. Computer Security Handbook, 5th Edition. Seymour Bosworth, M E Kabay (Editors). John Wiley, 2009.
6. Furnell, Katsikas, Lopez, Patel. Securing Information and Communication Systems: Principles. Technologies and Applications,Artech House Inc., 2008.
7. Charles P Pfleeger, Shari Lawrence Pfleeger. Security in Computing, 4th edition, Prentice Hall,2007.
8. H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, Springer-Verlag.
9. Speed and Ellis, Internet Security, Elsevier Science.
10. Security Engineering with patterns: origins, theoretical model, and new applications. Markus Schumacher. LNCS 2754, Springer.
11. ISO Standards in information security. http://www.27000.org/.
12. J M Seigneur. Trust, Security and Privacy in Global Computing. Ph.D. Thesis, University of Dublin.

Mrs-RB
11/9/13

Mrs-V-V-C for Senate approval
11/9/13