University of Nicosia, Cyprus

Course Code	**Course Title**	**ECTS Credits**
COMP-530	Cryptographic Systems Security	10
Department	**Semester**	**Prerequisites**
Computer Science	Fall/Spring/Summer	DFIN-511
Type of Course	**Field**	**Language of Instruction**
Elective	Computer Science	English
Level of Course	**Year of Study**	**Lecturer(s)**
2nd Cycle	2nd	Dr Ioanna Dionysiou
Mode of Delivery	**Work Placement**	**Co-requisites**
Distance Learning	N/A	None

Objectives of the Course:

The main objectives of the course are to:

- appreciate the need for computer and network security practices as well as information protection in digital currencies frameworks.
- provide students with knowledge on various concepts of classical computer and network security paradigms and their application/utilization by digital currency applications.
- expose students to techniques to manage security threats in digital currency frameworks by means of contemporary host-based and network-based intrusion detection/prevention tools, physical security measures, auditing, logging.
- expose students to best practices that enhance security in digital currency frameworks.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. explain the use of cryptography concepts such as symmetric/asymmetric encryption, digital signatures, and hash functions by various digital currency frameworks.
2. identify computer and network attacks (denial of service, flooding, sniffing and traffic redirection, inside attacks, etc.) and basic defense tools
3. assess the security framework of various digital currency applications and discuss its vulnerabilities that could be exploited by intentional and unintentional attacks
4. explain policies, procedures and best practices that strengthen the security framework of digital currency applications
5. appreciate the importance of ethics as a network security practitioner

Course Contents:

1. Motivation of security and introduction of basic security services
    a. Preliminary assessment of security in various digital currency

frameworks

2. Symmetric Ciphers – Classical Encryption techniques, Symmetric Encryption, Block Ciphers
    a. Applications of symmetric encryption in digital currency operations
3. Asymmetric Ciphers – Asymmetric Encryption, Public-Key cryptography, Key exchange protocols
    a. Applications of asymmetric encryption in digital currency operations
4. Cryptographic Hash Functions, Message Authentication Codes, Digital Signatures
    a. Utilization of hash functions (and/or MAC) in digital currency frameworks
5. Key Management and Distribution
    a. Key management procedures among digital currency framework entities (owners, miners, traders, etc.)
6. User authentication (password-based, token-based, biometric) techniques and authentication protocols (Kerberos, PKI)
    a. User identification and verification schemes in current digital currency frameworks
    b. Anonymity issues
7. IP Security and Web Security
    a. Security assessment of the communication framework of digital currencies
8. Computer and network threats and attacks
    a. Introduction of threats - Viruses, worms, denial of service attacks, flooding, sniffing and traffic redirection, exploit attacks.
    b. Threats to digital currency systems –wallet password sniffing, wallet contents corruption, mobile wallet vulnerabilities, denial of service for decentralized ledgers, exploiting vulnerabilities to destabilize the system, botnet attacks via malware infection, etc.
9. Contemporary network defence countermeasures
    a. Host-based and network-based intrusion systems (e.g. snort, and other open source tools), firewalls, anti-virus software to protect from and/or detect intrusions mentioned above.
10. Comprehensive Security Framework for Digital Currencies
    a. Revisit assessment of security in various digital currency frameworks
11. Determine policies, procedures, and best practices to secure digital currencies transactions, including transmission of digital currencies and storage of digital currencies
    a. Certification standards for protecting assets (ISO 27001 family) and their applicability to online wallets managed by third parties, cold storages and offline storages.
    b. Desktop wallets, mobile wallets, hardware wallets
12. Legal, ethical, and professional aspects of network security practices

Learning Activities and Teaching Methods:

Lectures and case studies

Assessment Methods:

Written and programming assignments, mid-term exam, final exam

Required Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
W. Stallings	Cryptography and Network Security: Principles and Practice, 6th Edition	Prentice Hall	2013	0133354695
W. Stallings	Network Security Essentials: Applications and Standards, 4th edition	Prentice Hall	2010	0136108059

Recommended Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
R. Anderson	Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition	John Willey and Sons	2008	0470068523

Recommended Articles / Reading List:

- S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to better – how to make bitcoin a better currency,” in Financial Cryptography 2012, vol. 7397 of LNCS, 2012, pp. 399–414.

- L. Garber, "News Briefs -Attacks Target Bitcoin Virtual Currency “ Computer, vol. 46, no. 5, pp. 19-21, May, 2013

- S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system, 2009,” 2012. [Online]. Available: http://www.bitcoin.org/ bitcoin.pdf

- Miers, C. Garman, M. Green, A. D. Rubin, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin”, in 2013 IEEE Symposium on Security and Privacy, San Francisco, CA, 2013, pp 397- 411.

- M. E. Peck, “Bitcoin: The Cryptoanarchists’ Answer to Cash “, IEEE Spectrum, June 2012. [Online]. Available: http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash

- M. E. Peck, “What You Need to Know About Mt. Gox and the Bitcoin Software Flaw “, IEEE Spectrum, February 2014 . [Online]. Available: http://spectrum.ieee.org/tech-talk/computing/networks/what-you-need-to-know-about-mt-gox-and-the-bitcoin-software-flaw

- F. Reid and M. Harrigan, “An analysis of anonymity in the Bitcoin system,” in Privacy, security, risk and trust (PASSAT), 2011 IEEE Third International Conference on Social Computing (SOCIALCOM). IEEE, 2011, pp. 1318–1326.