**COMP-530 Cryptographic Systems Security**
***Requires Programming Background**

**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 | Ghassan Karame |
| **Mode of Delivery** | **Work Placement** | **Co-requisites** |
| Distance Learning | N/A | None |

**Objectives of the Course:**

Overview of existing digital currencies, theoretically and operationally.

1. Basic security and privacy provisions of existing popular currencies, and will be exposed to the state-of the-art attacks and threats reported against existing systems/deployments.
2. The effectiveness of combining network-level security primitives, with novel cryptographic primitives to deter attacks on payment systems

**Learning Outcomes:**

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

1. Reason about the security and privacy definitions of open payment systems.
2. Explain the security of Bitcoin and Ripple in light of the state of the art reported attacks.
3. Reason about possible network security and cryptographic countermeasures to deter attacks on existing implementations of Bitcoin and Ripple.
4. Explain best security/privacy practices to strengthen the security of existing digital currencies, and extract relevant lessons for the design of secure future digital currencies.
5. Appreciate the need for thorough and formal security and privacy assessments for existing digital currencies.

**Course Contents:**

1) Introduction into Digital Currencies: here, we establish security and privacy definitions for digital currencies. We also briefly recap the basic operations of the Bitcoin system.
2) Bitcoin security: Selfish mining, new attacks, and countermeasures. In this session, we go deeper in the security of Bitcoin, We will first start with an overview of the widely-known security assumptions about Bitcoin, and then delve into a number of recently reported attacks on the system.
3) Fast payments in Bitcoin: Insecurity of fast payments in Bitcoin and countermeasure. We will study one of the widely used form of payments in Bitcoin. These are zero-confirmation transactions. We will show that this form of payment is inherently insecure and we discuss means to enhance the security of fast payments in Bitcoin.
4) Anonymity and Privacy in Bitcoin: To which extent does Bitcoin protect the privacy of its users? We will learn how to define, and quantify privacy in digital currencies, such as Bitcoin.
5) Lightweight clients: security and privacy provisions due to the use of Bloom filters. Current lightweight clients employ Simple Payment Verification protocols to minimize bandwidth and energy consumption. We will discuss the lack of privacy offered by existing implementations.
6) Security of Bitcoin wallets. Besides existing approaches, we will learn about multi-sig transactions, and reason about a possible secure and robust solution where Bitcoin private keys can be stored.
7) Is Bitcoin a de-centralized currency? Who controls Bitcoin? We discuss how the vital operations and decisions that Bitcoin is currently undertaking are not decentralized.
8) Increasing user privacy in Bitcoin. We will study a number of existing proposals for enhancing user privacy in Bitcoin.
9) The Ripple payment system. We will analyze the Ripple protocol and discuss the consensus protocol of Ripple.
10) Security and Privacy of the Ripple system. We analyze the security of the Ripple protocol, and the current usage patterns and trade dynamics in Ripple.
11) Comparison between Bitcoin and Ripple. We compare the security and privacy of Ripple to the provisions of the Bitcoin system. Other block-based currencies and alternative uses of the Bitcoin block chain. We will explore the current envisioned applications of Bitcoin and of the blockchain. We will also go over Bitcoin2.0 and Ethereum

**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-cryptoanarchistsanswer-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-toknow-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.