Boston University **Spring 2024**
ECE Department

Advances in Cyber and IoT Security (EC700 A3)

Syllabus

Synopsis: This course covers new developments in cybersecurity, with an emphasis on networking and communications aspects and the Internet of Things (IoT). Selected topics may include threat modeling, game theory for cybersecurity, blockchains, side-channel analysis, network infrastructure security, and security for connected vehicles. The course blends theory and practice and culminates with a research project, building on recent results from the literature.

List of topics for current course offering:

- **Game theory foundations:** Nash equilibrium, price of anarchy (PoA), Stackelberg games.
- **Game theory applications:** Stackelberg security games (SSG), security games in wireless networks.
- **Algorithmic foundations**: Algorithmic game theory (mechanism design), Byzantine fault tolerance (BFT).
- **Crypto foundations:** Hash functions, Merkle trees, digital signatures, elliptic curves, public-key infrastructure (PKI), zk-Snarks.
- **Blockchains**: Bitcoin P2P network, Nakamoto consensus, incentives and proof-of-work, mining, scripts, Layer 2 solutions.
- **Dapps and DeFi**: Ethereum P2P network, decentralized applications, (DApps), decentralized finance (DeFi).

References:

1. S. Tadelis, *Game Theory: An Introduction*, Princeton University Press, 2013.
2. T. Roughgarden, *Twenty lectures on algorithmic game theory*. Cambridge University Press, 2016.
3. A. Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016.
4. A. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd edition, O'Reilly, 2018.
5. A. Antonopoulos and G. Wood, *Mastering Ethereum*, O'Reilly, 2018.