1. Course number and name
   CptS 427: Computer Security

2. Credits and contact hours
   3 credits, 3 lecture hours

3. Instructor’s or course coordinator’s name
   Adam Hahn

4. Textbook, title, author, and year
   Other supplemental materials
   Instructor notes/slides and various papers/websites will be provided for some topics.

5. Specific course information
   a. Catalog description: Examines cyber vulnerabilities and attacks against computer
      systems and networks; includes security protection mechanisms, cryptography,
      secure communication protocols, information flow enforcement, network
      monitoring, and anonymity techniques.
   b. Prerequisites or corequisites: CPT S 360 with a C or better or CPT S 370 with a
      C or better; MATH 216 with a C or better; certified major in Computer Science,
      Computer Engineering, Electrical Engineering, or Software Engineering.

6. Specific goals for the course
   By the end of the course, students will be able to
   - Demonstrate an understanding of the principles of computer/network security,
     including basic threats and attacks to modern computer systems and networks (1a,
     1b, 1c, 1d, 2a, 2b).
   - Utilize threat modeling methodologies to identify potential threats and necessary
     protection for systems (1a, 1b, 1c, 1d, 2a, 2d).
   - Implement access control mechanisms and identify weaknesses within the
     approaches (1a, 1b, 1c, 1d).
   - Identify software vulnerabilities, develop exploits for them, and implement
     mitigations (1a, 1b, 1c, 1d).
   - Utilize basic cryptographic operations to protect communications and data stored
     on a system (1a, 1b, 1c, 1d).
   - Identify privacy and anonymity threats within current systems and appropriate
     protection techniques (2b, 2c, 4a).
   - Related current events related to cybersecurity to the techniques and principles
     discussed in class (4a, 4f, 7d, 7g).
7. **Brief list of topics to be covered**
   - Basic security principles (CIA, Design Principles)
   - Threat modeling techniques
   - Access control mechanisms (DAC, MAC, HMAC)
   - Hash algorithms (SHA, DES)
   - Symmetric key algorithms (AES, DES)
   - Asymmetric key algorithms (RSA, Diffie-Hellman)
   - Pseudorandom number generation (PRNG)
   - Transport Layer Security (TLS)
   - Software vulnerabilities and protections
   - Web vulnerabilities and protections