CIS 6375 Distributed Systems Security

Credits: 3 credits

Textbook, title, author, and year: Class notes and selected papers posted in Canvas

Reference Materials: E.B.Fernandez, "*Security patterns in practice: Building secure architectures using software patterns*", Wiley Series on Software Design Patterns, 2013.

E.B. Fernandez, "Cloud and IoT security using patterns", book in progress, posted in Canvas.

Specific Course Information

Catalog Description: Most practical information systems are distributed systems. This comes from the ubiquitous use of the Internet, the need to provide access to corporate information for distributed employees and customers, and to adapt to application needs. This course considers the security issues of such systems together with possible solutions. We use UML and patterns to describe architectures. We discuss security in new types of systems such as web services, cloud computing, IoT, blockchain, wireless, and cyber-physical systems. We present a systematic methodology to build secure distributed systems.

Prerequisites: An introductory course on Computer Security. Background on web-based systems. Knowledge of UML is useful.

Specific goals for the course: Analyze current topics on distributed system security, including new architectures.

Understand the modus operandi of attacks and their countermeasures. Understand the importance of system architecture on security.

Learn to use patterns and apply a methodology to build secure systems
Learn how to write papers and theses.

Brief list of topics to be covered:

1. **Motivation and overview**. Distributed systems and security. Threats.
2. **Security patterns**. Other types of patterns. Reference architectures. Overview of UML. Security principles: sandboxing, isolation methods.
3. **Threat analysis**. Misuse patterns. Defenses. Authentication: OAuth, Shibboleth. Authorization: PEP and PDP. Active defenses. AI and threat detection.
4. **Methodologies for building secure distributed applications.** Secure Solution Frames. UMLSec, SecUML, Secure Tropos. **Assignment 1**
5. **Distributed architectures**. Secure versions of patterns: Broker, MVC, Publish/Subscribe Agents. P2P systems. Middleware.
6. **SOA and Web services**: architectures, attacks, and standards. Web services patterns. Identity. Security standards: SAML, XACML. Misuse patterns. REST security
7. **Security in cloud computing**. Threats and defenses. Patterns and misuse patterns. Access Control, Infrastructure security. OpenStack security. Container security. Virtualization security. NFV. Cloud ecosystems. **Assignment 2.**
8. **Cyber-physical systems**. Threat modeling. Stuxnet. Security in smart grid, vehicles, cargo ports, oil and gas pipelines, smart buildings. The Internet of Things. Fog computing.
9. **Wireless systems**. Operating system architectures, application security. Sensor network security. Wireless clouds. Vehicular networks threats.
10. **Specialized architectures**. Security in Blockchain architectures. Big Data architectures. Robotics. AI and security**. Assignment 3.**
11. **Software development for clouds and IoT.** DevOps, SecOps, secure microservices.
12. **Security evaluation**. Use of patterns and arguments. Common Criteria.