|  |  |  |
| --- | --- | --- |
| **1. Course title/number, number of credit hours** | | |
| Distributed systems security CIS6375 | | # of credit hours  3 |
| **2. Course prerequisites, corequisites, and where the course fits in the program of study** | | |
| An introductory course on Computer Security. Background on web-based systems. Knowledge of UML is useful. | | |
| **3. Course logistics** | | |
| *Term*: Fall 2018  This is a classroom lecture course  *Class location and time*  FL 404 TR 11:00-12:20  This course has a significant amount of design content (project). | | |
| **4. Instructor contact information** | | |
| *Instructor’s name*  *Office address*  *Office Hours*  *Contact telephone number*  *Email address* | Dr. Eduardo B. Fernandez (see bio at the end)  EE417  TR 1:00-3:00 or by appointment  561-297-3466  fernande@fau.edu | |
| **5. TA contact information** | | |
| *TA’s name*  *Office address*  *Office Hours*  *Contact telephone number*  *Email address* | None | |
| **6. Course 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. | | |
| **7. Course objectives/student learning outcomes/program outcomes** | | | |
| *Course objectives* | Analyze current topics on distributed system security, including new architectures.  Understand the modus operandi of attacks to distributed systems 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 | | |
| *Student learning outcomes*  *& relationship to ABET a-k objectives* | This is a graduate course | | |
| **8. Course evaluation method** | | | |
| Research Project - 70 %  Homework Assignments (2)- 30 % | | *Note*: The minimum grade required to pass the course is B. | |
| **9. Course grading scale** | | | |
| Relative grading, no curves or ranges. | | | |
| **10. Policy on makeup tests, late work, and incompletes** | | | |
| Decided on a case by case. | | | |
| **11. Special course requirements** | | | |
| None | | | |
| **12. Classroom etiquette policy** | | | |
| University policy requires that in order to enhance and maintain a productive atmosphere for education, personal communication devices, such as cellular phones and laptops, are to be disabled in class sessions. | | | |
| **13. Disability policy statement** | | | |
| In compliance with the Americans with Disabilities Act (ADA), students who require special accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) located in Boca Raton campus, SU 133 (561) 297-3880 and follow all OSD procedures. | | | |
| **14. Honor code policy** | | | |
| Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and place high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. See University Regulation 4.001 at  [www.fau.edu/regulations/chapter4/4.001\_Code\_of\_Academic\_Integrity.pdf](http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf) | | | |
| **15. Required texts/reading** | | | |
| Class notes and selected papers posted in Canvas | | | |
| **16. Supplementary/recommended readings** | | | |
| E.B.Fernandez, “*Security patterns in practice: Building secure architectures using software patterns*”, Wiley Series on Software Design Patterns, 2013. Parts posted on Canvas.  E.B. Fernandez, “Cloud and IoT security using patterns”, book in progress, posted in Canvas  List of selected references for each chapter. | | | |
| **17. Course topical outline, including dates for exams/quizzes, papers, completion of reading** | | | |
| 1. **Motivation and overview**. Distributed systems and security. Threats. Review of basic aspects of security.                 2. **Security patterns**. Other types of patterns. Reference architectures. Review  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. ASE. 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 network threats and defenses.  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. | | | |

Eduardo B. Fernandez (Eduardo Fernandez-Buglioni) is a professor in the Department of Computer Science and Engineering at Florida Atlantic University in Boca Raton, Florida, USA. He has published numerous papers on authorization models, object-oriented analysis and design, cloud computing, and security patterns. He has written four books on these subjects, the most recent being a book on security patterns; he is working now on a book on Cloud and IoT security patterns. He has lectured all over the world at both academic and industrial meetings. He has created and taught several graduate and undergraduate courses and industrial tutorials. His current interests include security patterns, cloud computing security, and cyber-physical systems security and safety, including IoT. He holds a MS degree in Electrical Engineering from Purdue University and a Ph.D. in Computer Science from UCLA. He is a Senior Member of the IEEE, and a Member of ACM. He is an active consultant for industry, including assignments with IBM, Allied Signal, Panasonic, Motorola, Lucent, Huawei, and others. Since 2007 he goes every year for two-three weeks to Japan to work with a group at their National Institute of Informatics.

Since 2014 he teaches a short course every year in Chile.