# DEPARTMENT OF THE AIR FORCE

**A I R U N I V E R S I T Y (A E T C)**

**GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT**

**Department of Electrical and Computer Engineering**

**CSCE 660 – Mobile, Wireless, and SCADA Device Security**

**Course Syllabus**

**Spring 2019**

|  |  |
| --- | --- |
| **Meeting Times** | Tu, Th 1300 – 1400 for lecture, Tu, Th 1400 – 1600 for lab |
| **Location** | Bldg 642, Rm 204 – the GECO Classroom |
| **Instructor** | Maj Rich Dill, PhD |
| **Office Location** | Bldg 642 Room 219F |
| **Office hours** | Wednesdays, 0900 – 1000 or By appointment |
| **Contact Information** | richard.dill@afit.edu |

**Course Description:**

This course provides instruction on the mobile and SCADA devices. Students learn about the communication network operation to include message/call routing and supporting hardware elements, as well as the mobile network’s evolution and development. Vulnerabilities of various devices (smart phones, tablets, SCADA, etc.) are discussed, providing opportunities for exploitation and implementation of security measures through lab exercises.

|  |  |
| --- | --- |
| **Credits** | 4 |
| **Prerequisites** | N/A |

# Student Learning Objectives:

|  |  |
| --- | --- |
| 1 | Identify and explain security weaknesses and mitigation steps in mobile application technologies |
| 2 | Evaluate the current state of mobile and SCADA security |
| 3 | Propose a methodology to integrate mobile and SCADA security technologies in support of existing research |
| 4 | Research and present a topic of interest that support research and integrates mobile / SCADA security concepts |

# Recommended Resource Materials (MLA Style):

Arnatovich, Yauhen Leanidavich, et al. "A Comparison of Android Reverse Engineering Tools via Program Behaviors Validation Based on Intermediate Languages Transformation." *IEEE Access* 6 (2018): 12382-12394.

Assante, Michael J., and Robert M. Lee. "The industrial control system cyber kill chain." SANS Institute InfoSec Reading Room 1 (2015).

# Elbez, Ghada, Hubert B. Keller, and Veit Hagenmeyer. "A New Classification of Attacks against the Cyber-Physical Security of Smart Grids." *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 2018.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." *White paper, Symantec Corp., Security Response* 5.6 (2011): 29.

Jaiswal, Mayank, Yasir Malik, and Fehmi Jaafar. "Android gaming malware detection using system call analysis." *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2018.

Mondal, Sarmistha, Anindita Sinha, and Jayati Routh. "A Survey on Evolution of Wireless Generations 0G to 7G." *International Journal of Advance Research in Science and Engineering-IJARSE* 1.2: 5-10.

Montenegro, José A., Mónica Pinto, and Lidia Fuentes. "What do software developers need to know to build secure energy-efficient Android applications?." *IEEE Access* 6 (2018): 1428-1450.

Mutchler, Patrick, et al. "A large-scale study of mobile web app security." *Proceedings of the Mobile Security Technologies Workshop (MoST)*. 2015.

# *N. Varol, A. F. Aydogan and A. Varol, "Cyber attacks targeting Android cellphones," 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, 2017, pp. 1-5.*

# Scoccia, Gian Luca, et al. "An investigation into Android run-time permissions from the end users' perspective." Proceedings of the 5th International Conference on Mobile Software Engineering and Systems. ACM, 2018.

Tan, Darell JJ, Tong-Wei Chua, and Vrizlynn LL Thing. "Securing android: a survey, taxonomy, and challenges." *ACM Computing Surveys (CSUR)* 47.4 (2015): 58.

Tam, Kimberly, et al. "The evolution of android malware and android analysis techniques." *ACM Computing Surveys (CSUR)* 49.4 (2017): 76.

Toorani, Mohsen, and A. Beheshti. "Solutions to the GSM security weaknesses." *2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies*. IEEE, 2008.

Xia, Xuwei, Chen Qian, and Bo Liu. "Android security overview: A systematic survey." *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2016.

# Grading Scheme/Policy:

|  |  |
| --- | --- |
| **Assignment** | **Grade %** |
| Participation | 10% |
| Labs | 40% |
| Interim Presentation | 10% |
| Draft Paper | 10% |
| Abstract | 5% |
| Peer Review | 5% |
| Final Paper ([SECURWARE 2019](http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=86034&copyownerid=83510)) | 20% |

|  |  |
| --- | --- |
| **Letter Grade** | **Numerical Grade** |
| A | 94-100 |
| A- | 90-93 |
| B+ | 87-89 |
| B | 84-86 |
| B- | 80-83 |
| C | 70-79 |
| D | 60-69 |
| F | < 60 |

**Grading Scheme/Policy:**

Email all assignments by 11:59PM EDT on the due date to both [richard.dill@afit.edu](mailto:richard.dill@afit.edu) and [prof.rich.dill@gmail.com](mailto:prof.rich.dill@gmail.com).

# Policies:

* 1. **Attendance:** Attendance at all class sessions and exams is mandatory for military and civilians assigned to AFIT as full-time students except for extenuating circumstances. Scheduled classes and exams are defined by the instructor and they are documented in the course schedule. Part-time students are expected to attend scheduled classes, and absences should be explained to the instructor. The student should provide advance notice, if possible. (References: Student Handbook, Graduate School Catalog)
  2. **Academic Integrity:** All students must adhere to the highest standards of academic integrity. Students are prohibited from engaging in plagiarism, cheating, misrepresentation, or any other act constituting a lack of academic integrity. Failure on the part of any individual to practice academic integrity is not condoned and will not be tolerated. Individuals who violate this policy are subject to adverse administrative action including disenrollment from school and disciplinary action. Individuals subject to the Uniform Code of Military Justice may be prosecuted under it. Violations by government civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. (References: Student Handbook, ENOI 36 – 107, *Academic Integrity*)
  3. **Academic Grievance:** AFIT and the Graduate School of Engineering and Management affirm the right of each student to resolve grievances with the Institution. Students are guaranteed the right of fair hearing and appeal in all matters of judgment of academic performance. Procedures are detailed in ENOI 36 – 138, *Student Academic Performance Appeals*.
  4. **Testing Policy: N/A**

|  |  |  |
| --- | --- | --- |
| **Date** | **Objective** | **Assignments** |
| Tu/26 Mar | Course Intro | Lab 0 (assigned) |
| Th/28 Mar | Critical Infrastructure Overview |  |
|  | **Read:** *NIST 800-82 Section 2* |  |
| Tu/2 Apr | PLC/Embedded system architecture – ICS Lab 1 handout | **Lab 0 (due)**  ICS Lab 1 (assigned) |
|  | **Read:** *Falliere* |  |
| Th/4 Apr | Mobile Risk Ecosystem |  |
|  | **Read***: Mondal, Toorani, N. Varol* |  |
| Tu/9 Apr | Android OS | **ICS Lab 1 (due)**  Mobile Lab 1a, 1b (assigned) |
|  | **Watch:** <https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/lecture-20-mobile-phone-security/>  **Read**: *Xia, Tan* |  |
| Th/11 Apr | Guest Lecture – Dr. Temple | **Student Topic (due)** |
|  | **Read:** TBD |  |
| Tu/16 Apr | App Analysis | **Mobile Lab 1a, 1b (due)**  Mobile Lab 2 (assigned) |
|  | **Read***: Mutchler, Scoccia,* [*https://usa.kaspersky.com/blog/android-8-permissions-guide/16300/*](https://usa.kaspersky.com/blog/android-8-permissions-guide/16300/) |  |
| Th/18 Apr | How to control a process – ICS Lab 2 handout | **Abstract (due)** |
|  | **Read:** TBD |  |
| Tu/23 Apr | ICS Network Protocols | **Mobile Lab 2 (due)**  ICS Lab 2 (assigned) |
|  | **Read***: TBD* |  |
| Th25 Apr | Static Analysis | **Draft Paper (due)** |
|  | **Read:** *Arnatovich, Darell* |  |
| Tu/30 Apr | Develop your first Application | **ICS Lab 2 (due)**  Mobile Lab 3 (assigned) |
|  | **Read:** *Montenegro,* [*https://developer.android.com/training/basics/firstapp/*](https://developer.android.com/training/basics/firstapp/) |  |
| Th/2 May | Dynamic Analysis | Peer Review (assigned)  Mobile Lab 4 (assigned) |
|  | **Read:** *Tam, Jaiswal* |  |
| Tu/7 May | Guest Lecture – Rob Lee, CEO Dragos Cyber Security | **Mobile Lab 3 (due)**  ICS Lab 3 (assigned) |
|  | **Read:** *Elbez* |  |
| Th/9 May | Attacking control systems - ICS Lab 3 handout | **Peer Review (due)**  **Mobile Lab 4 (due)** |
|  | **Read:** *Assante* |  |
| Tu/14 May | Defending control systems | **ICS Lab 3 (due)**  ICS Lab 4 (assigned) |
|  | **Read:** *TBD* |  |
| **Date** | **Objective** | **Assignments** |
| Th/16 May |  |  |
|  |  |  |
| Tu/21 May |  | **ICS Lab 4 (due)** |
|  |  |  |
| Th/23 May | Guest Lecture – TBD |  |
|  |  |  |
| Tu/28 May | Guest Lecture – TBD |  |
|  |  |  |
| Th30 May | Guest Lecture – TBD | **Final Paper (due)**  Student Presentations |

*The course syllabus is a general plan for the course; deviations announced to the class by the instructor may be necessary.*