

14 November 2019

Wireless and Mobile Softwarization: Security and Privacy Pandora's Box? (1:00 – 1:50pm EST)

AND

Building Secure Software Systems Using Security (2:00 - 2:40 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. Capitol Technology University (CTU) hosts the presentations using Adobe Connect which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Topic: Wireless and Mobile Softwarization: Security and Privacy Pandora's Box?

Time: 1:00pm – 1:50pm EST

Location: <https://captechu.zoom.us/j/664120328>

Just log in as "Guest" and enter your name. No password required.

Presenter(s): Guevara Norrd12 2 Tm0T.e.70.0000092 0 612 2 reN3(r calertheaW*nt/F2r)11(UnW*ñBTrs(d)3(t(ms)-4(U)

CAE Tech Talks are recorded; view them here: <https://www.caecommunity.org/content/cae-tech-talk-resources>

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov

limitations. The talk points are illustrated using our recent research, spanning a variety of application areas, such as demonstrating mobile apps tracking without requiring any permissions, Apple AWDL design and implementation vulnerabilities permitting tracking and man-in-the-middle attacks, covert channels for exfiltrating sensitive personal and business data through wireless and mobile devices, and air traffic attacks on the Instrument Landing Systems (ILS), or Automatic Dependent Surveillance – Broadcast (ADS-B) system.

AND

Topic: Building Secure Software Systems Using Security

Time: 2:00pm – 2:40pm EST

Location: <https://captechu.zoom.us/j/664120328>

Just log in as “Guest” and enter your name. No password required.

Presenter(s): Eduardo Fernandez, Florida Atlantic University

Description:

Patterns combine experience and good practices to develop basic models that can be used to build new systems and to evaluate existing systems. Security patterns join the extensive knowledge accumulated about security with the structure provided by patterns to provide guidelines for secure system requirements, design, and evaluation. We consider the structure and purpose of security patterns, show a variety of security patterns, and illustrate their use in the construction of secure systems. These patterns include among others Authentication, Authorization/Access Control, Firewalls, Secure Broker, Web Services Security, and Cloud Security. We have built a catalog of over 100 security patterns. The use of patterns can provide a holistic view of security, which is a fundamental principle to build secure systems. Patterns can be applied throughout the software lifecycle and provide a good communication tool for the builders of the system. The patterns are shown using UML models and examples are taken from my two books on security patterns as well as from my recent publications.

CAE Tech Talks are recorded; view them here: <https://www.caecommunity.org/content/cae-tech-talk-resources>

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov