

# Assignment 2: Smart Grid Security and Privacy

---

Instructor: Professor Deepa Kundur

Semester: Fall 2015

DEADLINE: Monday, November 2, 2015, 11:59 pm ET.

## Objectives of this assignment

- To provide students with an opportunity to apply the cyber security definitions introduced in the lectures to a power grid application.
- To distinguish between the notions of privacy, security and confidentiality.

Please note that this is an *individual* project and each person can talk to others, but must ultimately do their own paper selection, reading and write their own assignment report.

## Questions

1. For the first part of this assignment you must select a recent paper (within the last five years) on the topic of cyber security of the smart grid. There are many articles you can find. For example, the following recent special issues have a variety of papers on the topic:

*IEEE Power and Energy Magazine* Special Issue on Cybersecurity for Electric Systems, vol. 10, no. 1, Jan.-Feb. 2012.

*Proceedings of the IEEE*, Special Issue on Cyber-Physical Systems, vol. 100, no. 1, January 2012.

- In the lectures, we defined vulnerability, cyber attack, threat and countermeasure. Based on the paper you have read, please specify (in detail) a scenario of attack that you think may be possible to apply to some component of the smart grid. In your discussion you must specify (i) a **vulnerability**, (ii) a **cyber attack**, (iii) a **threat**, and (iv) a **possible countermeasure**. Be creative. This question is trying to get you thinking in terms of “security”.
2. Using the same paper, discuss and justify which security objectives within the C-I-A framework are being addressed. It may be more than one.
  3. In class we discussed concepts of security, confidentiality and privacy. Please discuss the relationship between privacy, security and confidentiality. Specifically, you should discuss what is different between security and privacy and what is different between privacy and confidentiality. You should also discuss how security and confidentiality approaches could be leveraged to achieve privacy and what shortcomings there may be. Please also provide a smart grid application where privacy is of concern and discuss methods (technical, legal, policy-based, or social) that can help achieve privacy. You will need to do research, so please make sure your final report has references to reflect your contributions.

## Report Format and Grading

Your report should be approximately 4-6 pages (including figures and the reference list which should include your selected paper in Question 1). Please list your name and student number on the top of the report. For Question 1 your report should provide an introduction summarizing the security issue(s) being considered in the paper along with any proposed solutions. Please then provide answers to Questions 1 and 2. For Question 3 please answer the associated questions in discussion style with section headings and paragraphs as relevant.

The overall report should be in complete sentences, *in your own words*, and in paragraph form. Use section headings if you like. Any diagrams should be original (not copied for the paper). You will be graded on the correctness, preciseness and comprehensiveness of your answers and quality of your presentation. You will also be graded on your ability to follow the specific submission instructions below: