Tutorial T-06: Denial of Service Attacks on the Smart Grid: Classification, Solutions, and Challenges

Presenters: Kemal Bicakci (TOBB University of Economics and Technology)
Suleyman Uludag (University of Michigan - Flint)

Tutorial Overview

The overarching goal of this tutorial is to present the emerging Denial-of-Service (DoS) vulnerabilities, attacks taxonomy, challenges, and solutions in the Smart Grid.

Unprecedented initiatives have recently been instituted around the world to ameliorate the electric grid with the Smart Grid (SG). The conception of the Smart Grid (SG) paradigm is to offer many benefits to the transmission, distribution, and consumption of energy. With the new paradigm, a Pandora's box of cybersecurity related issues comes to the forefront to develop techniques for.

According to NIST Guidelines for Cybersecurity, availability, the main target of DoS attacks, is the most important security objective for power system reliability. DoS attacks disrupting the Internet traffic have already cost billions of dollars world-wide. With the increasing connectedness of power grid systems, a DoS attack to the grid infrastructure causing a major power failure becomes quite possible and could be undoubtedly more harmful and costly. This is because in modern society electricity is a utility we depend mightily not only for communication but also for many other life-critical purposes.

It is in this framework that we are proposing to present a structured, methodical, holistic, and comprehensive view of the *availability* dimension of the Smart Grid cybersecurity issues, threat models, existing solutions, and remaining challenges and research problems.

The detailed *tentative* outline of the sections is given below:

1. Power Grid Fundamentals and the Smart Grid Paradigm
   (a) Power Grid history, structure, topologies and operating states
   (b) Power Grid communications infrastructure
   (c) Deficiencies
   (d) Advanced Metering Infrastructure (AMI), Demand Response and Microgrids
   (e) Automated Control Systems, Network Management and Microgrids
2. Classification of DoS attacks on the Smart Grid
3. Solutions
   (a) Filtering / Firewalls
   (b) Rate Limiting (client-puzzles, CAPTCHAs)
   (c) Intrusion Detection (signature-based, anomaly-based, specification-based)
   (d) Attack Reaction (source identification, resource management)
   (e) Cryptographic Authentication (user authentication, scalable cryptographic infrastructure)
   (f) Protocol Solutions (secure routing, broadcasting/multicasting, aggregation, etc. protocols)
   (g) Architecture Solutions (resiliency of network topology and architecture, reconfiguration, honeypots / honeynets)
   (h) Host-based (Device) Solutions (trusted computing, secure bootstrapping, secure patching, attestation, diversity)
   (i) Wireless Solutions (signal-based/packet-based detection, jamming-resilient schemes)
   (j) System-theoretic Solutions (Cyber-Physical Security of Smart Grids)

(k) Recommendations for a holistic solution

4. Challenges, Open Issues, and Questions

   (a) DoS-resistant backward-compatible networking protocol?
   (b) Impact analysis and risk assessment
   (c) Testbeds, simulation, emulation
   (d) Attack-resilient architectures
   (e) Physical consequences of compromises

Learning objectives:
From the Blooms Taxonomy of Objectives for the Cognitive Domain, the learning objectives of the tutorial can be attributed to *Knowledge* and *Comprehension* levels to facilitate *Application*, *Analysis* and *Synthesis* levels as a result. More concretely, by the time the presentation of the tutorial is finished, the audience should be able to

- State current power grid structure as well as the new Smart Grid paradigm,
- Describe the need for research efforts for the the availability dimension of the Smart Grid, especially the DoS attacks,
- Explain the major DoS attack types on Smart Grid,
- Explain some major defense mechanisms against DoS attacks on the Smart Grid,
- Identify the general areas of open research issues and areas in Smart Grid DoS attacks.

Presenter Biographies

Kemal Bicakci is currently a professor of Computer Engineering at TOBB University of Economics and Technology, Ankara, Turkey. He has been teaching graduate and undergraduate level courses in Information Security, Cryptography and Computer Networks for more than ten years. He developed and co-taught a 10-day hands-on cyber defense training course series funded by the NATO Science for Peace and Security (SPS) Programme and participated by network/system administrators from several NATO partner countries in the period of 2012-2015 (see *http : //www.nato.int/cps/en/natolive/news_*99718*.htm*). In the Avicenna project (Network of universities for open distance learning) funded by UNESCO, he was responsible for producing an online computer security and cryptography course. Prof. Bicakci was the thesis supervisor of Yusuf Uzunay, Middle East Technical University Best Thesis Award Winner. His survey paper on DoS attacks and countermeasures in IEEE 802.11 networks is highly cited.

Suleyman Uludag received his Ph.D. from DePaul University, Chicago in 2007. He is an associate professor of computer science at the University of Michigan - Flint. The general areas of his research include security, privacy, and optimization in the smart grid, network quality of service, routing in wireless and wired networks. He has been awarded the Lois Matz Rosen Junior Faculty **Excellence in Teaching Award** in September 2010 at the University of Michigan - Flint. He has been a **Fulbright Scholar** (Core Program) at TOBB University of Economics and Technology in Ankara, Turkey during the 2012-2013 academic year. He was a visiting scholar at the TCIPG (Trustworthy Cyber Infrastructure for the Power Grid) at the University of Illinois at Urbana-Champaign and the MONET research group of Professor Klara Nahrstedt at UIUC from August of 2013 to August of 2014. TCIPG is the preeminent research center on power grid cybersecurity.