Smart Grid Security—Attack and Defense Strategems

Wasfi Momen   
CSC 6222  
Department of Computer Science – Georgia State UniversityAtlanta, Georgia   
[wmomen1@student.gsu.edu](mailto:wmomen1@student.gsu.edu)

*Abstract*—This electronic document is a “live” template and already defines the components of your paper [title, text, heads, etc.] in its style sheet. *\*CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract*. (*Abstract*)

# Introduction (*Heading 1*)

# Smart Grid Attacks

## False Data Injection

In our first attack, we look both conceptual research and current impacts in violations of integrity. Integrity is defined as the manipulation of data either by a malicious adversary or an error-producing source that compromises the authenticity of information that can be gained from the data. In networks protocol design, some protocols use checksums or error correction codes in order to prevent or fix integrity violations. Unfortunately, only one power substation protocol, DNP3, gives any kind of integrity checking with checksums [DNP3 Primer], but DNP3 is not as widespread as other, more insecure protocols like BACnet or Modbus. Today, most power substation setups utilize these insecure protocols as minimal as possible and only in machine-to-machine networks.

However, the Smart Grid aims to ubiquitous and secure across its realms. Therefore, new problems arise while implementing past-day solutions. An adversary might not have access to all parts of the Smart Grid, he or she can attack either at the top at the power generation realm or at the bottom at the distribution, end user, or service provider. Therefore, making use of either the top or bottom might compromise the other. By injecting integrity violations, the adversary can push incorrect data that will affect operations and lead to issues in power delivery service.

### Integrity violation via calculations

With respect to integrity violations, Mrabet et al. [Mrabet] describe the *false data injection attack*. In the scope of the Smart Grid, false data injection is typically implemented at the bottom realms of power distribution, end user networks, and the service provider. By influencing the calculations on the metrics of power consumption, an adversary violates the integrity of the data and ensures a false result once the metrics reach to the SCADA core. Specifically, Liu et al. [Liu et al.] give the calculation of state estimation as describe by the linear regression model:

By impacting values in z to find an attack vector, the estimation function H can be altered and produce a false result of the estimate. Liu et al. also debunk previously stated beliefs that an attacker would need a substantial probability to find an attack vector to compromise the network. In the experimental evaluation, the attacker only needs a 20 percent chance of random false data injections before the attack vector is found. A sample setup of this attack can be modeled by an attacker having access to a variety of RTUs or parts of the AMI such as a smart meter for a house. The formation of the state estimation for Smart Grids is primarily used as the basis for modeling an Intrusion-Based Detection System (IDS).

### Integrity violation via hardware

Along with the manipulation of data via software inferred calculation, an integrity violation with easy accessibility to the attacker is found in the smart meter devices themselves as a part of the Smart Grid. An article written by reporter Brian Krebs informs of widespread hacking of smart meter devices in Puerto Rico [Krebs]. Puerto Rico is among one of many locations around the world that have implemented smart meter infrastructure due to natural disasters destroying the infrastructure. In Puerto Rico, some citizens have modified their smart meters to cut off metrics being sent back to the public power utility, PREPA. As a result, the FBI claims 400 million US dollars will be lost in the long term.

Halim et al. [Halim] give a review of various hardware hacks that can implemented on smart meters [Halim]. Smart meter infrastructure, just like the rest of Smart Grid components, are still early in their development and deployment, but still ship with hardware vulnerabilities. First off, smart meters come without any encrypted or obfuscation of memory locations. Therefore, it is easy to get memory readouts via the pins connecting the devices and inject data to cause integrity violations. Another method is simply unplugging the meter’s metric connection or placing a strong magnet on the meter—the technique used in Puerto Rico. No data at all still means disruptions of power consumption. Whole communities within the end user realm could use these techniques which are highly incentivized by the financial gain and highly accessible due to rise of a technology-savvy generation.

### Preventing false data injections

By the Smart Grid’s own interconnectedness, false data injection can cause widespread disruption in the network. As mentioned before, the calculation for state estimation is typically used for modeling an IDS. The solution proposed by current research involves various algorithms that try to decrease the number of false positives while maintaining true negative accuracy. Chen et al. [Chen et al.] tries a machine learning approach that differs in the traditional statistical-based IDS. The authors formulate a consistent-inconsistent region to measure how much of a grid is reliable or not. Then, each state and its neighbor in a set is compared by trust-based voting to see if their state estimations are reliable. Finally, elements are targeted as “Good”, “Abnormal”, and “Unknown” if they fall into the consistency region or not.

In experimental evaluation, this method proved to produce false-positive rates two-thirds lower than the next best algorithm. It also provides configurable regions to let end users decide on­ how reliable they want the algorithm to perform. Various improvements can be made by strictly checking the “Unknown” components. According to the solution, “Unknown” components are caused when there is not enough data on state estimations to say a neighbor is reliable or not. Data-sparse regions in the Smart Grid are plentiful in more rural areas or places with poor data connection. If the solution is to be made for real-time correlation, some development in data-sparse areas should be considered, perhaps even utilizing data from the previous statistical-based models if applicable.

For the issue of hardware violations, it is representative of the more “security through obscurity” problem largely present in the current power generation grid. Mandatory requirement for future standard IEC 62056-21 should be implemented across the Smart Grid which includes simple passwords, encrypted passwords, and handshaking to smart meters. Future specifications of the standard should include higher cryptographic protocols. The meters themselves should be secured based on a minimal set of requirements to delay tampering or notifying the end user or power company.

## Popping the HMI

Mrabet acknowledge the HMI or *Human Machine Interface* in the paper as part of the exploitation an attacker can use to gain access to critical systems in the Smart Grid. The HMI is defined as the mechanism for human interaction to the SCADA interface. In the past, this used to relate to buttons and knobs of generation one SCADA via mechanical switches. However, today’s generation and the future will utilize web browsers as the main HMI since they are well-supported and tested through everyday use.

Mrabet brings up the point that exploiting HMI vulnerabilities “does not require advanced networking skills or significant experience in security and industrial control system to perform” and puts the attack as a high severity, but then puts it as low probability for implementation which seems contradictory. HMI attacks high severity due to their ability to compromise confidentiality, integrity, and accessibility throughout the Smart Grid. However, the research for HMI attacks in SCADA and other components of Smart Grid systems only count to a few studies and therefore represent a blind spot for security.

*Popping the HMI* is a term used to relate attacks on the HMI interface. Any attacks on web browsers apply to the HMI of the smart grid system at all levels. Normally, attacks are part of an implementation of a library or system that the HMI requires. For example, most web browsers use OpenGL as the main shading language for users and files to gain access to the GPU functions to render content. While thoroughly developed and optimized, there are still some problems outside of actual software vulnerabilities. GPU operations have regularly timed I/O operations that can be captured and analyzed to see what the user was doing at the time. This timing aspect is what makes up one of the greatest threats to the Smart Grid.

### Timing attacks on the HMI

While there are many different vectors of attack on the HMI, ranging from cross-site scripting to library substitution, we focus on timing attacks on the HMI that reveal what the system was doing at the time. The attacker’s goal is reconnaissance of the target network topology in the Smart Grid. Specifically, the attacker wants to know which devices that are Type 1A/P2 that need a critical time delay of 3 milliseconds to conduct operations—these devices will be highly targeted areas of the network [Wang et al]. Over a large sample of requests, the attack will either divulge the target devices or give enough information to conduct additional attacks.

The procedure of the attack is nothing new to vulnerabilities of web browser development. Javascript and the loading of HTML and CSS at particular times by Content Delivery Networks give enough information to determine which web site a user is browsing, and since a user-agent string is sent via Content headers in HTTP the attack space narrows to specific browsers. The attacker uses a time statistic to base their measurements, sends some code to the target machine, and then sees how long the process takes.

Since HMIs are sold along with the machines that make up components of the SCADA core, fingerprinting browser can go down to the application level and development stacks of the power substation setup. For example, the Siemens WinCC HMI had a CVE (Common Vulnerability and Execution) that came from its Windows Server Version that required an update. Since Siemens HMI will be perform and execute at consistent times with caching and perform at different times relevant to other popular HMIs, the attacker has learned crucial and valuable information that can be now shifted into other aspects of the Siemens SCADA system.

### Defense with Deterministic Browsers

Due to the potential of attacks, browsers built for security tend to reduce their fingerprinting as far as possible. The Tor browser, built on top of the Tor networking protocol, tells its users to always keep a low profile by keeping every aspect of the modern web browser in check. Tor has options to reduce screen resolution to keep with the most popular formats, disabling Javascript entirely, and, according to Wang et al. [Wang et al.], even prevents timing attacks by adding “jitters to the browser clock”.

However, mitigating attacks on the timing of web browsers has proven difficult with options becoming more distinct over time with the different hardware and software provided in the modern day. As mentioned before, SCADA systems will use the most supported web browser, but the Smart Grid SCADA core requires even more security. The *deterministic browser* provides a possible defense against timing attacks for web browsers of the Smart Grid.

Wang described the process of developing deterministic browser to defeat timing attacks. The deterministic browser produces a time based on the attacker’s input so the attacker will get a different time than the actual time the process took to complete. The browser is constantly ticking time on the clock even if there are no process tasks to be done. The actual time the process takes is slotted inside a constant time window that is resistant to timing attacks. Currently, Wang has built a custom build of Firefox named Deterfox that defends against timing attacks. Even over a large sample of devices, files, times, and popular websites, there was no useful information gained from conducting performance metrics. All operations seem to complete in constant time as seen by the adversary.

If adopted as a primary browser for the Smart Grid and researched further, the deterministic browser can become a new defense against a difficult attack. However, it should be noted that the Smart Grid should adopt other secure methods of HMI web browser interaction such as private VPN tunneling, secure HTTPS, and firewall configurations to not divulge information about target machines in plaintext.

The issues for the deterministic browser is the Javascript time execution. All operations conducted through Javascript calls have to be considered to predict the time the process will take and the resultant confusion for the attacker. Javascript and its now popular superscript Typescript will introduce new synchronous and asynchronous functions that will break compatibility with this deterministic browser. Also, any calls to the performance API in Javascript will break compatibility with the deterministic browser and revert back to regular true system time. Many HMIs might require access to these APIs and functions.

# Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

## Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

## Units

* Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive”.
* Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
* Do not mix complete spellings and abbreviations of units: “Wb/m2” or “webers per square meter”, not “webers/m2”. Spell out units when they appear in text: “. . . a few henries”, not “. . . a few H”.
* Use a zero before decimal points: “0.25”, not “.25”. Use “cm3”, not “cc”. (*bullet list*)

## Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

*a**b* 

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(1)”, not “Eq. (1)” or “equation (1)”, except at the beginning of a sentence: “Equation (1) is . . .”

## Some Common Mistakes

* The word “data” is plural, not singular.
* The subscript for the permeability of vacuum **0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter “o”.
* In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
* A graph within a graph is an “inset”, not an “insert”. The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
* Do not use the word “essentially” to mean “approximately” or “effectively”.
* In your paper title, if the words “that uses” can accurately replace the word “using”, capitalize the “u”; if not, keep using lower-cased.
* Be aware of the different meanings of the homophones “affect” and “effect”, “complement” and “compliment”, “discreet” and “discrete”, “principal” and “principle”.
* Do not confuse “imply” and “infer”.

# Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## Authors and Affiliations

**The template is designed for, but not limited to, six authors.** A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

### For papers with more than six authors: Add author names horizontally, moving to a third row if needed for more than 8 authors.

### For papers with less than six authors: To change the default, adjust the template as follows.

#### Selection: Highlight all author and affiliation lines.

#### Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select the correct number of columns from the selection palette.

#### Deletion: Delete the author and affiliation lines for the extra authors.

## Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is “Heading 5”. Use “figure caption” for your Figure captions, and “table head” for your table title. Run-in heads, such as “Abstract”, will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named “Heading 1”, “Heading 2”, “Heading 3”, and “Heading 4” are prescribed.

## Figures and Tables

#### Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 1”, even at the beginning of a sentence.

1. Table Type Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
| Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

1. Sample of a Table footnote. (*Table footnote*)
2. Example of a figure caption. (*figure caption*)

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization”, or “Magnetization, M”, not just “M”. If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization {A[m(1)]}”, not just “A/m”. Do not label axes with a ratio of quantities and units. For example, write “Temperature (K)”, not “Temperature/K”.

##### Acknowledgment *(Heading 5)*

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

##### References

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first ...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord “Format” pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

1. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
3. K. Elissa, “Title of paper if known,” unpublished.
4. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
5. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
6. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.**