The 2015 Ukraine Blackout: Implications for False Data Injection Attacks

Gaoqi Liang, *Student Member, IEEE,* Steven R. Weller, *Member, IEEE,* Junhua Zhao, *Member, IEEE,* Fengji Luo, *Member, IEEE, and* Zhao Yang Dong, *Senior Member, IEEE*

***Abstract*— In a false data injection attack (FDIA), an adversary stealthily compromises measurements from electricity grid sensors in a coordinated fashion, with a view to evading detection by the power system bad data detection module. A successful FDIA can cause the system operator to perform control actions which compromise either the physical or economic operation of the power system. In this letter, we consider some implications for FDIAs arising from the late 2015 Ukraine Blackout event.**

***Index Terms*— Cyber-attacks, Ukraine Blackout, False Data Injection Attacks**

I. Background on the 2015 Ukraine Blackout

On 23 December 2015, a synchronized and coordinated cyber-attack compromised three Ukrainian regional electric power distribution companies, resulting in power outages affecting approximately 225,000 customers for several hours [1]. This cyber-attack entailed several technical components, probably requiring extensive reconnaissance of the victim networks by adversaries [2]: variants of the BlackEnergy 3 malware were reportedly delivered via spear phishing emails and may have been used as an initial access vector for the theft of authorized users' virtual private network (VPN) credentials; a telephonic denial-of-service attack was executed to frustrate reports of outages to call centers; and a modified KillDisk firmware attack erased master boot records on workstations, thereby delaying restoration efforts.

These security compromises enabled the primary attack, namely a hijack of the Supervisory Control and Data Acquisition (SCADA) network, including the targeting of field devices with malicious firmware, thereby facilitating the remote opening of substation breakers. Manual operations were ultimately required to restore electrical service to customers [2].

G. Liang is with the Center for Intelligent Electricity Networks (CIEN), University of Newcastle, Callaghan, NSW, 2308, Australia (e-mail: gaoqi.liang@uon.edu.au).

S.R. Weller is with the School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW, 2308, Australia (e-mail: steven.weller@newcastle.edu.au).

J. Zhao is with Chinese University of Hong Kong (Shenzhen), Shenzhen, Guangdong, China (e-mail: junhua.zhao@outlook.com).

F. Luo is with the School of Civil Engineering, The University of Sydney, Australia, Sydney, NSW, 2006, Australia (e-mail: fengji.luo@sydney.edu.au).

Z.Y. Dong is with the School of Electrical and Information Engineering, the University of Sydney, Sydney, NSW, 2006, Australia (e-mail: joe.dong@sydney.edu.au).

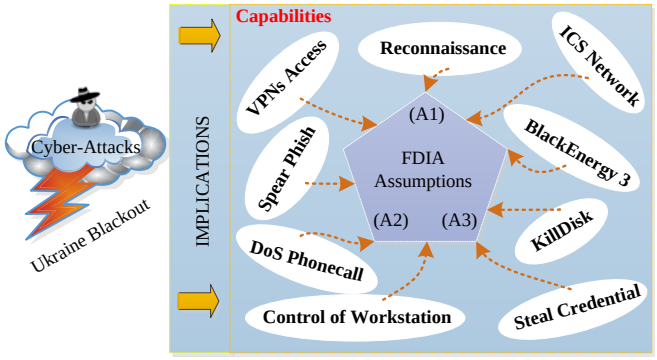

Fig. 1. Cyber-attackers' Capabilities towards Power Systems

II. Implications

A. Assumptions for FDIAs

The FDIA, first proposed by Liu *et al.* [3], is a cyber-attack in which power system state estimation outputs are corrupted by injecting false data into meter measurements in a carefully coordinated fashion. The defining feature of a successful FDIA is that the state estimation residual falls below a hypothesis test threshold despite the presence of corrupted measurements, the attack thereby evading detection.

Research on FDIAs has been extensive [3]–[7], typically relying on three key assumptions [3][4], namely that the attackers:

(A1) have knowledge of power system operations and features of the target system;

(A2) are capable of manipulating meter measurements; and

(A3) have knowledge of important control and operation information, such as the network topology, system electrical parameters, specifics of the SCADA network devices and bad data detection scheme, etc.

Considered jointly, (A1)–(A3) are strong assumptions, potentially calling into question the practical feasibility of mounting a successful FDIA. Nevertheless, we contend that the Ukraine blackout underscores the plausibility of assumptions (A1)–(A3), shown in Fig. 1, and that the "strongest capability of the [Ukraine blackout] attackers was […] their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack" [2].

B. Aspects Contributing to Feasibility of FDIAs

1) Ready Access to Information Sources

In the Ukraine blackout, adversaries showed expertise. Besides the intrusion of the Information Technology (IT) networks, they could even wrest control from substation control centers and operate the Human Machine Interface (HMI) in the supervisory control system to switch on breakers remotely.

The Internet provides potential adversaries with ready access to substantial quantities of high-quality, power system and vendor specific information: textbooks introduce the foundations of generation, transmission, and distribution systems; research publications update scholars' knowledge and power system innovations; industrial control system (ICS) vendors readily share basic functionality and system architectures on web portals; and industrial control standards and network protocols are freely distributed on the Internet. Collectively, these resources provide determined adversaries with considerable knowledgebase with which to inform a cyber-attack.

2) Utilization of Vulnerabilities

Vulnerabilities in firewall, network protocols, encryption, and VPN connections serve as "half-open-doors" to informed adversaries. There are three approaches to manipulating meter measurements for FDIAs: (i) compromising meters locally; (ii) intercepting and forging data packets when transferring to the control center; and (iii) modifying control center database [4].

In the Ukraine blackout, adversaries loaded malicious firmware into SCADA network field gateway devices to ensure that even when operator workstations were recovered, remote commands could not be issued to bring the substations back online [2]. Based on this, it can be foreseen that there would be high probabilistic for the adversaries to locally manipulate device parameters and gathered measurements by building direct access to field devices.

Furthermore, intercepting and forging communication messages is easy to achieve, since the SCADA layer communication network architecture has no cryptographically secure communication protocol.

In the Ukraine blackout, password-protected access to substation control center workstations was likely gained by adversaries via keystroke loggers [2]. The adversaries could exploit stolen credentials via VPNs to enter ICS network. Information stored on SCADA servers can be then readily stolen. Database manipulation is therefore possible after successfully gaining credentialed access.

3) Reconnaissance

The Ukraine cyber-attack likely followed long-term power system reconnaissance over six months or more without being noticed [2]. According to E-ISAC and SANS, long-term reconnaissance is considered as the strongest capability of the attackers to launch this highly synchronized, multistage, multisite cyber-attack.

For FDIAs, identifying network topology and parameters can not only be gained via on-off observation of components, but also estimated from market data or measured power flows over extended periods. Additionally, working staffs may also be proactively or passively tracked, decoyed, and deceived to tattle important configuration or operation information to adversaries. Moreover, existing researches on FDIAs based on incomplete topology information and limited meter manipulation capability have been demonstrated to be valid. Therefore, assumption (A2) and (A3) are flexible for attackers as long as necessary information and competence for launching FDIAs are collected and gained during reconnaissance.

It is also clearly seen from the Ukrainian blackout that the adversaries hold the initiative to pose themselves as scheduled. Before launching this attack, they concealed their motivations for a long time. While, it is also a feasible motivation for attackers to launch successful FDIAs for the purpose of gaining economic profits by concealing themselves over an extended period.

C. Recommendations

Both ICS-CERT [1] and SANS [2] have provided recommendations and defense strategies regarding the Ukraine blackout incident. We further recommend that regular staff cyber-security training should be regarded as fundamental to power system security. Such training would strengthen defenses against FDIAs and coordinated cyber-attacks alike. Moreover, we recommend that components such as remote terminal units (RTUs), switches, breakers etc. should support both automatic and manual modes, in the event of failures in automatic restoration.

III. Conclusions

The Ukraine blackout is the first publicly acknowledged incident which is caused by cyber-attacks. This event highlights the vulnerability of highly automated, cyber information-based smart grid environments to coordinated cyber-attacks. In particular, this letter argues that the circumstances of the Ukraine blackout underscores the plausibility of common assumptions regarding the knowledge and capabilities required by an adversary in order to mount a successful false data injection attack on a power system.

References

[1] NCCIC/ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," released 25 February 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed: 20 June 2016].

[2] E-ISAC and SANS, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," released 18 March 2016. [Online]. Available: https://ics.sans.org/duc5 [Accessed: 20 June 2016].

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security (TISSEC), vol. 14, no.1, May. 2011.

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Dong, "A review of false data injection attacks against modern power systems," IEEE Trans. Smart Grid, 2016, in press.

[5] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," IEEE Trans. Smart Grid, vol. 2, no.2, pp. 382–390, Jun. 2011.

[6] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," IEEE Trans. Smart Grid, vol. 6, no.4, pp. 1686–1696, July. 2015.

[7] L. Jia, J. Kim, R.J. Thomas and L. Tong, "Impact of data quality on real-time locational marginal price," IEEE Trans. Power Syst., vol. 29, no. 2, pp. 627–636, Mar. 2014.