Low-budget Energy Sector Cyberattacks via Open Source Exploitation

Anastasis Keliris
Tandon School of Engineering
New York University
Email: anastasis.keliris@nyu.edu

Charalambos Konstantinou
Center for Advanced Power Systems
Florida State University
Email: konstantinou@caps.fsu.edu

Marios Sazos, Michail Maniatakos
Center for Cyber Security
New York University Abu Dhabi
Email: {marios.sazos, michail.maniatakos}@nyu.edu

Abstract—**Modern cyber warfare involves penetration of a nation's computers and networks, aiming to cause extensive damage and/or disruption. Such actions are generally deemed feasible only by resource-wealthy nation state actors. In this work, we challenge this perception and introduce a methodology dubbed Open Source Exploitation (OSEXP), which leverages public infrastructure to execute an advanced cyber attack on critical infrastructure. In particular, we characterize and verify an effective and reusable OSEXP attack vector based on time spoofing of Global Positioning System (GPS) signals. Our GPS attack employs commercial devices and open source software, and manipulates the time synchronization of carefully selected power grid equipment in a manner that can lead to large scale blackouts. We experimentally verify the feasibility of our GPS OSEXP methodology, and demonstrate that an actor with limited budget has the ability to cause significant disruption to a nation.**

I. Introduction

The first public electric power systems were established in the 1880's for providing street lighting [1]. Since then, power systems have significantly evolved and grew to become essential in our everyday life. Today, electric power systems can be considered the "backbone" of critical infrastructure as several sectors, such as water treatment and desalination, heavy industry, and military defense systems, rely on electric power. The far-reaching effects of power outages (also known as *blackouts*), further demonstrate our strong dependence on uninterrupted supply of electricity. Typical causes of blackouts include extreme weather and natural phenomena, misoperation, human errors, equipment failures, and animals [2].

Over the past years, *cyberattacks* have been added to the list of potential threats against the stable and continuous operation of power systems. The Aurora Generator Test was one of the first demonstrations of how cyberattacks can damage physical power grid components [3]. This test was performed in 2007 by the Idaho National Laboratory, and used a software program to exploit a vulnerability in diesel generators causing them to explode. Moving from tests in controlled environments to cyberattacks against real world systems, two sophisticated attacks targeting the Ukrainian power grid in 2015 and 2016 led to partial blackouts in the Ivano-Frankivsk region and Kiev, respectively [4], [5].

Despite these tangible incidents, there remains a lot of uncertainty among power industry stakeholders regarding the real threat cyberattacks pose to power systems. Such attacks are usually considered to only be within the reach of resource-wealthy nation state actors. However, given the plethora of publicly available information regarding power systems and the dependency of these systems on public infrastructure, we argue that it is feasible for actors with lower budgets to instantiate disrupting attacks. To that end, we introduce a low-budget methodology capable of causing wide area blackouts, solely relying on public information and public infrastructure.

Similar to Open Source Reconnaissance,[1] where meaningful information is extracted from public sources [6], we introduce *Open Source Exploitation* (OSEXP). OSEXP leverages public resources and infrastructure to construct low budget attack vectors against judiciously selected power grid locations. We present an in-depth study of a specific OSEXP vector, namely Global Positioning System (GPS) time spoofing, that exploits the reliance of power systems on GPS for time synchronization. Although the potential of GPS spoofing attacks to affect power system measurements has been demonstrated in literature, it required specialized, expensive equipment and extended technical knowledge [7], [8].

Our main contribution in this work is the characterization and experimental verification of GPS time spoofing attacks against carefully selected power grid devices *using low-cost Commercial-Off-The-Shelf (COTS) equipment and open source software*. Our approach significantly reduces the cost and complexity of GPS time spoofing, "open sourcing" the exploitation phase of campaigns targeting power systems. Furthermore, it enables a one-time design of an exploitation vector and reuse of the same vector worldwide, as GPS is employed for time synchronization purposes in systems across the globe.

The rest of the paper is structured as follows: Section II provides preliminaries on power systems and GPS. We present an end-to-end open source approach for constructing attack vectors against power systems and introduce OSEXP in Section III. We elaborate on a specific OSEXP attack, GPS time spoofing, in Section IV, and experimentally verify the feasibility of this attack using low-cost equipment and open source software in Section V. Related work is discussed in Section VI, and we conclude the paper in Section VII.

[1] The term open source is not related to open source software throughout this work, unless explicitly stated.

II. Preliminaries

A. Power systems

Power systems are collections of networked components that generate, transfer, and utilize electric power. Large scale power systems are also known as power grids, because of the interconnected network topology of their components. In general, power systems are comprised of four stages, namely generation, transmission, distribution, and consumption.

The first stage is *generation*, where electricity is produced in power plants through the conversion of other forms of primary energy to electrical energy. Electricity is then transferred in the *transmission* stage, utilizing an elaborate network of interconnected high voltage lines and substations spanning large geographical distances. In general, overhead transmission lines are preferred to underground lines due to reduced costs, with 97% of U.S. transmission lines being overhead [9]. *Distribution* is the stage at which electricity is distributed to end consumers, using lines that span smaller distances and operate at lower voltages compared to transmission lines and step down transformers to reduce the voltage levels to ranges that match the operational voltages of end consumers. Finally, electricity is utilized in the *consumption* stage.

B. Protection and control equipment

Protection and control devices, such as Circuit Breakers (CBs) and relays, are employed for ensuring the stable and secure power system operation. Their operation guarantees normal grid equipment operation by separating the system into protective zones, and isolating faulty zones as necessary. This separation can limit or prevent damages to equipment and personnel in the case of overloads or faults.

According to the North American Electric Reliability Council (NERC), 70% of the major disturbances in the U.S. are associated with faulty operation of relay controllers [10]. Optimal attack strategies may require changing the breaker status signal at only one transmission line [11], highlighting the necessity of constant and reliable operation of CBs and relay controllers for avoiding severe consequences.

C. Grid modernization

Cyberattacks against power systems are mainly enabled by an ongoing modernization, materialized through the convergence of Operational Technology (OT) and Information Technology (IT). Components in power grid are being upgraded with "smart" counterparts that enable fine-grain control and faster incident response times. To achieve these goals while keeping development costs low, vendors of power equipment typically leverage COTS hardware and software, use common general-purpose microprocessor architectures (e.g., ARM, Intel x86) and real-time versions of commercial operating systems (e.g., Windows and Linux) [12].

In general, Intelligent Electronic Devices (IEDs) deployed in power systems observe the variables and state of the system, store necessary data, make decisions, and take protection and control actions towards preserving performance and stability. For example, Wide Area Monitoring Systems (WAMS) highly rely on IEDs to gather system information from multiple sources. WAMS are mainly enabled by Phasor Measurement Units (PMUs) that take synchronized snapshots of electrical quantities across the system, and use the comparative measurements to estimate the health and power quality of the grid. PMUs are deployed primarily in the transmission stage and provide synchronized phasor (synchrophasor) measurements of voltage and current at several locations to provide time-stamped information of the system's state. Given the dispersed topology of the power grid, accurate time synchronization between such devices is essential for their operation. To that end the majority of PMUs rely on timing provided by GPS modules for capturing synchronized snapshots of the system across geographically dispersed locations.

D. Global Positioning System

Global Navigation Satellite Systems (GNSS), an example of which is GPS, use a collection of earth-orbiting satellites equipped with transmitters. The transmitters include an atomic clock synchronized to the Coordinated Universal Time (UTC) and their location is assumed known at all times, as the satellites follow predetermined trajectories. Each satellite broadcasts a navigation signal including time stamp data and any deviation from its predetermined trajectory [13]. Receivers obtain such signals from satellites within their field of view, and use the signal propagation delays to calculate their three-dimensional location data and time [14]. GPS signals are categorized in those available for civilian use (L1 C/A transmitted at 1575.42 MHz), and encrypted restricted signals (L2 transmitted at 1227.60 MHz), typically used by military applications. In this work we focus on L1 signals, as PMUs utilize these signals for time synchronization.

III. Open sourcing malicious campaigns against power systems

In this section we present an end-to-end open source approach for campaigns aiming to disrupt national power grids. Retracing the steps of a malicious actor whose objective is causing a wide area blackout, we identify three main requirements for achieving this goal. These are:

1) Construct a model of the target system. This model is necessary for understanding the system, its dependencies and interconnections, and identifying its weak spots.
2) Analyze the model to identify and select critical targets. By carrying out analytical, data-driven studies of the system model, adversaries can identify critical locations that when attacked could lead to cascading failures.
3) Construct attack vectors targeting the identified critical locations, disrupting power system operations.

A. Threat model

The threat actors we consider in this work are adversaries that aim to cause power system disruption and large scale power outages. We assume that the adversaries have technical expertise of power system operations and that they can, if required, be in physical proximity to power grid assets.

However, we do not consider them to possess confidential information, or have network access to the equipment and control center of the target power system. In our threat model, we assume the adversaries can leverage publicly available information and infrastructure to achieve their objective, and are thus not limited to resource-wealthy nation states.

B. Modeling a system using public information

Most impactful blackouts to date have been the result of faults occurring at the transmission stage. Thus, adversaries are most likely to focus on this stage to cause power outages. To that end, a model including the network topology of transmission lines, transmission substations and their interconnections, as well as general load and capacity estimations can enable further studies of the target system.

Given the plethora of publicly available sources of information concerning power systems, adversaries may reconstruct a system model from such sources. Evidently, this form of "open source reconnaissance" is employed in an ongoing campaign against U.S. systems [15]. Examples of sources include: a) public reports, such as blackout reports and expansion planning reports, b) power system databases, such as Enipedia [16] and Open Energy Information [17], and c) press releases and success stories from power utilities and power grid equipment vendors. By combining and fusing information from such sources, a model of a target power system can be constructed for carrying out subsequent analyses. Construction of a power system model using public information is out of the scope of this work, and a detailed example can be found in [18].

C. Identifying critical locations with contingency analysis

Power studies of the constructed model can enable judicious selection of target locations for materializing an attack. Considering the objective of power system disruption, contingency analysis studies in particular are useful to malicious actors. Contingency studies aim to analyze unscheduled events (e.g., generator, transformer and/or transmission line failures) in a power system, assessing and ranking their impact [19]. Note that in general power systems must be able to sustain $N-1$ contingencies (e.g., to enable maintenance). However, for all systems there exists a number of contingencies that leads to non-sustainable scenarios and can also lead to cascading failures and blackouts. By applying such contingency analysis techniques on the model constructed in the previous step, adversaries can identify these critical transmission lines and interconnections and direct their attacks against them. Contingency analysis is described in detail in [19].

D. Open Source Exploitation

With knowledge of the critical points of a power system, adversaries need to construct attack vectors against the system. More specifically, they need to devise means towards disconnecting critical transmission lines capable of a nonsustained contingency scenario. In this work, we focus on the exploitation of *public infrastructure*, in a process we name Open Source Exploitation (OSEXP). OSEXP techniques can be used in conjunction with conventional cyberattack techniques (e.g., phishing, credential harvesting, lateral movement, etc.), depending on the campaign objectives. For a campaign whose target is to cause large scale power outages rather than just get information and leverage on a target system, we argue that OSEXP techniques can be advantageous.

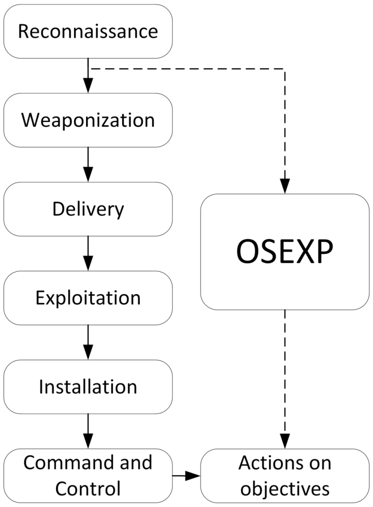

Fig. 1. Conventional Cyber Kill Chain with our proposed OSEXP step.

In general, the Cyber Kill Chain (CKC) is used to describe the structure of a cyberattack [20]. The steps of CKC are: 1) reconnaissance, where information is gathered, 2) weaponization, where a payload is designed, 3) delivery of the payload, 4) exploitation, where a vulnerability of the target system is exploited, 5) installation, where the payload is installed and executed on the target system, 6) command and control, where adversaries remotely tweak and instruct the payload and finally 7) actions on objectives, where adversaries fulfill the objectives of their campaign. By exploiting public infrastructure using OSEXP, steps 2 to 6 are replaced with an OSEXP step leading to an alternative path in the CKC, depicted in Fig. 1. The resulting CKC using OSEXP attacks has fewer steps, is reusable and leaves less evidence behind, making forensic studies and attribution harder.

IV. OSEXP: GPS time spoofing against PMUs

As outlined in Section II-C, PMUs can take protective control actions in addition to their monitoring role. Taking advantage of this, judicious manipulation of PMU measurements can destabilize a system, making PMUs attractive targets for malicious actors. The OSEXP attack against PMUs we describe in this section exploits the reliance of PMUs on GPS (which is a public resource) for time synchronization. Our OSEXP attack introduces erroneous PMU measurements by manipulating the timing source of PMUs, effectively disconnecting selected PMU-controlled transmission links.

Corroborating the feasibility of OSEXP GPS attacks, information, implementation details, and software regarding GPS are part of the public domain. Open source implementations of GPS receivers and transmitters for Software Defined Radios (SDRs), software GPS simulators and available literature lower the technical requirements for successful GPS spoofing attacks [21]. Furthermore, the global nature of GPS ensures that a GPS spoofing attack can be reused in diverse systems employing different hardware across the globe. In contrast, techniques that require identifying and exploiting deployed devices, software, and network channels are system-specific and require undertaking laborious research for each system.

GPS receivers inherently trust the signals they receive, assuming the signals have not been tampered with. In most countries in the world, any transmission in the frequency band of GPS is illegal, addressing the risk with policy safeguards. However, from a technical standpoint L1 GPS signals do not have any built-in integrity protection mechanisms. With OSEXP GPS spoofing attacks, we challenge the inherent trust in the integrity of these signals, arguing that adversaries with far-reaching agendas, such as causing blackouts, will not be bound by ethical and legal concerns.

Given the reliance of PMUs on GPS for capturing the state of a power system in a synchronized manner, we describe the process of introducing errors in PMU measurements by manipulating GPS signals in their vicinity. This can cause desynchronized snapshots of the system state from PMUs in different geographical locations, leading to system destabilization and even cascading failures. In particular, GPS time spoofing attacks can introduce errors in the absolute time perceived by the affected PMUs. For an f-Hz signal the relationship between the clock offset error $\widetilde{t_\delta} - t_\delta$ and the phase angle measurement error ϵ are described by the following equation [22]:

$$\epsilon = [f \times (\widetilde{t_\delta} - t_\delta) \times 360^\circ] \pmod{360^\circ} \tag{1}$$

PMUs with control capabilities have a preconfigured threshold for allowed phase angle difference, that is dependent on the specifics of the system they are deployed in. Phase differences larger than this threshold cause connected CBs to open for avoiding fault propagation and protecting the equipment. However, introducing timing errors with GPS spoofing to instantly change the perceived state of the system for a PMU to exceed this threshold is not possible, because of the standards that govern PMUs. In particular, the IEEE standard for Synchrophasor Measurements for Power Systems (C37.118) dictates that clock synchronization errors between any two measurements from different PMUs should not exceed 31(26) μs for 50(60) Hz systems [23]. For a successful attack, it is thus necessary to slowly drift angle measurements, without exceeding these limits.

Another requirement for a successful GPS spoofing attack is knowledge of the legitimate GPS signal as it is perceived by the target receiver, including location information. This requirement can be fulfilled by co-locating the spoofing equipment in the physical vicinity of the target. The location information of a receiver is static, as the antenna is mounted on a building. Towards measuring the receiver location, attackers can measure their relative distance from the receiving antennas and calculate the offset, for example by employing drones equipped with cameras and GPS receivers. By flying directly over the target antenna, adversaries can capture the x,y location using the drone mounted GPS receiver. Subsequently, the z coordinate can be measured independently. Fig. 2 illustrates this scenario.

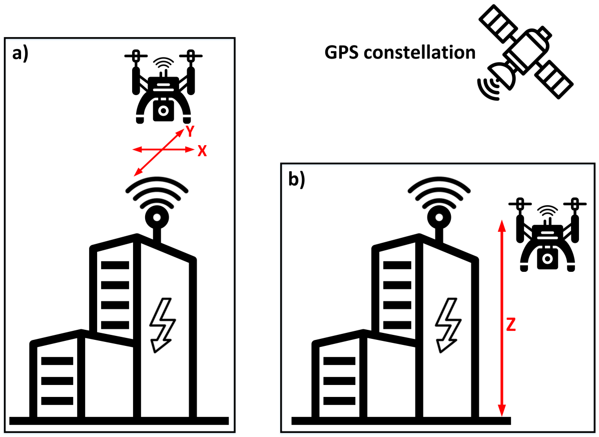

Fig. 2. Estimation of 3D location of a static GPS receiver using a drone. a) x,y coordinates. b) z coordinate.

In addition to identifying receiver location, generation of appropriate synthetic GPS signals requires that the spoofed and legitimate GPS signals are time-synchronized [24]. This enables attackers to concurrently transmit a spoofed signal that is synchronized with the legitimate signal, gradually increase the transmitting power overtaking the GPS receivers in the affected vicinity, and then introduce time delays that will cause erroneous PMU measurements. The naive approach of recording legitimate GPS signals and replaying them after introducing the necessary time delays is not possible due to non-deterministic delays introduced by the retransmitting equipment's hardware components and the strict timing requirements of the IEEE C37.118 synchrophasor standard. To overcome this challenge, attackers can generate a *leading* GPS signal, and then gradually introduce appropriate delays to achieve synchronization between their spoofed and the legitimate GPS signals. The equipment required for this are two GPS receivers (one for the legitimate and one for the spoofed signal) and means to measure the time difference between the two signals.

An observation regarding the GPS OSEXP attack is that it requires simultaneous physical proximity to all target locations is required, meaning that adversaries need to coordinate an attack at k locations in the case of attacking a system to trigger an $N-k$ contingency. For most power systems, opening CBs at two judiciously selected locations is sufficient to destabilize the system. We argue here that requiring two to three field agents for launching an attack of this scale and impact is realistic and by no means prohibitive.

V. Experimental evaluation of GPS OSEXP

In this section we evaluate the feasibility of a low cost GPS time spoofing OSEXP attack. In particular, we verify that open source software and Software Defined Radio (SDR) platforms are capable of launching GPS time spoofing attacks with the necessary granularity as this is defined by IEEE C37.118.

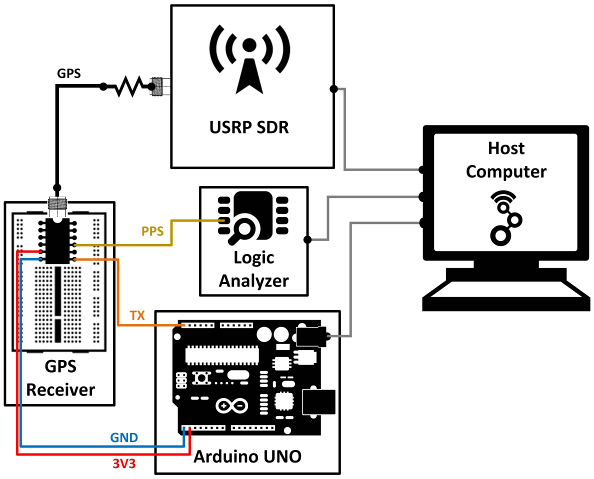

Fig. 3. Experimental setup for GPS spoofing attack.

This can desynchronize PMUs measurements, causing CBs at critical locations to open, and leading to wide area blackouts.

In our experiments we assume that attackers have synchronized their synthetic signals to legitimate GPS signals and have taken over control of the GPS receiver. These are realistic assumptions if an attacker can introduce *arbitrary delays* to a GPS signal, as arbitrary delays can be leveraged to achieve synchronization of leading signals with the legitimate ones. After the two signals are synchronized, attackers can gradually increase the spoofed signal power, overtaking control of receivers within their vicinity [7].

A. Experimental setup

The hardware in our experimental setup consist of a GPS receiver, an Arduino board, a SDR, a logic analyzer and a host computer. The GPS receiver employs the Venus638FLPx chip, which is a commercial, high performance receiver with 29 seconds cold start time-to-first-fix, up to 20 Hz update rate, and built-in jamming detection and mitigation. The GPS receiver is powered by an Arduino UNO board, which is also connected to the host computer for receiving and outputting the decoded NMEA messages. We utilize a Saleae Logic Pro 8 logic analyzer for sampling the Pulse-Per-Second (PPS) output pin of the receiver at a sampling rate of 10 MHz, which is satisfactory given the GPS receiver's PPS measured accuracy of 2 μs. For transmitting GPS signals we use an Ettus USRP N210 SDR, equipped with a GPSDO kit and a 40 MHz SBX 400-4400 MHz Rx/Tx. Respecting the legal framework concerning GPS signal transmission over-the-air, we conduct all of our experiments using cable connections and never transmit signals over-the-air, without loss of generality. To further ensure no side-effects we attenuate the USRP output to -140dBm, which is close to the minimum required signal by our GPS receiver for a fix (-148 dBm) and enclose the experimental setup in RF shielding fabric. Our experimental setup is depicted in Fig. 3.

In terms of software, we rely solely on open source software. For generating synthetic GPS data we use the Software-Defined GPS Signal Simulator (`gps-sdr-sim`) [25]. We download the required ephemerides data that indicate the current state of the satellite constellation from the Crustal Dynamics Data Information System [26]. Using `gps-sdr-sim` and the current ephemerides we create a raw synthetic static L1 GPS signal with a 2.5 MHz sampling rate, that is leading the current wall time by a few seconds. We input this signal to GNU Radio to perform the necessary type conversions, and add a delay block of user-specified duration between the file source and the USRP sink. This entire process is automated.

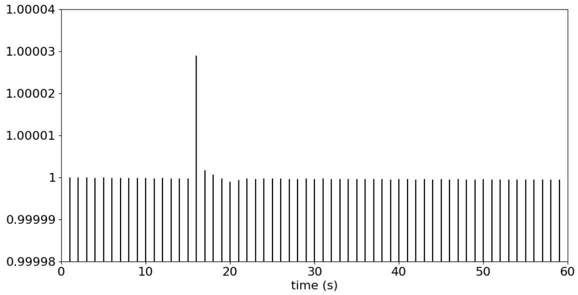

Fig. 4. Experimental results showing GPS receiver output PPS duration. The GPS spoofing attack is launched at $t = 16$ seconds.

B. Experimental results

Assuming a 50 Hz frequency for the target power system, our goal is to introduce a 30 μs delay, which lies within the allowed range according to IEEE C37.118. To that end, we select 30 μs as the user-specified delay duration in our GNU Radio flowchart and launch our automated script. We present the experimental results regarding time as it is perceived by the receiver in Fig. 4. In particular, the figure presents the absolute duration of PPS signals as it is perceived by the GPS receiver and measured by the logic analyzer. We observe that up to $t = 16s$ (which is when the attack is launched), each PPS signal is received exactly every one second, as expected. After the attack is launched, the particular pulse duration at $t = 16s$ becomes 1.0000289 s, indicating a shift in the perceived time by the GPS receiver as a result of our GPS signal manipulation. The introduced delay of 28.9 μs is below the 31 μs threshold, verifying the feasibility of using COTS equipment and open source software to launch fine-grain GPS time spoofing attacks.

Regarding the impact of our GPS time spoofing on a power system, the delay we introduce on PMU measurements results in a shift of $0.54°$ in the measured angle, calculated using (1). By repeatedly applying the same time-shifting technique we can introduce *delays of arbitrary duration*. Accumulation of such delays can gradually increase the phase difference between actual and measured angles, reaching the preprogrammed threshold at which the respective CBs are tripped, leading to sectionalization and cascading failures. Note that in addition to introducing erroneous measurements to PMUs, the same time-shifting technique can be employed to synchronize leading synthetic signals and legitimate GPS signals.

C. Budget

The cost of the equipment we utilize for GPS time spoofing mainly consists of the Ettus USRP SDR (and its respective add-on modules) and the Saleae Pro 8 logic analyzer. Their costs are $3529 USD and $699 USD respectively, for a total of $4228 USD. Launching a concurrent attack against k locations to materialize an $N-k$ contingency would require $k\times$ $4228 USD (typically $k=2$ or $k=3$ locations are sufficient), which is low given the attack's far-reaching impact.

Our equipment costs are dominated by the Ettus USRP SDR and they can be further reduced by replacing it with cheaper hardware, such as the bladeRF ($420 USD), or HackRF ($295 USD). An inherent limitation of these lower-cost devices is the reduced accuracy of their built-in oscillator, which is not adequate for transmitting GPS signals. However, this problem can be alleviated with OSEXP by leveraging another public infrastructure; *GSM base stations* [27]. As cell towers must be accurate within 0.5 parts-per-million (which is sufficient for GPS transmission), we can initially configure SDRs as GSM receivers. Using GSM signals, we can calculate the internal clock drift of our SDR with reference to the GSM base station clock, and then reconfigure the SDR as a GPS spoofer to carry out the spoofing technique as described above.

VI. Related work

The general requirements for successful GPS spoofing attacks are discussed in [24], and an investigation of whether a GPS spoofing attack against PMUs is theoretically feasible is presented in [22]. To the best of our knowledge, the only unclassified device capable of practical GPS spoofing is custom [28]. Among other applications, it was used to spoof GPS signals and desynchronize PMUs in a controlled demonstration [7]. In comparison to previous works, in this paper we demonstrate that COTS SDR hardware and open source software are sufficient for launching practical attacks against power systems. To thwart GPS spoofing attacks several countermeasures have been proposed in literature, including techniques based on signal processing, encryption, drift monitoring, signal direction of arrival, etc. [29]. However, to the best of our knowledge, such countermeasures are not implemented in commercial GPS receivers, including the COTS components used in power grid IEDs.

VII. Conclusion

In this work we introduce OSEXP, a technique that leverages public infrastructure to materialize attacks against power systems. We experimentally verify a specific OSEXP vector, GPS time spoofing, that can desynchronize phase angle measurements of judiciously selected PMUs to cause wide area blackouts. Our GPS spoofing technique relies on COTS hardware and open source software, enabling reusable low-budget high-impact attacks against power systems. With this study we aim to challenge the perception these attacks are feasible only by resource-wealthy nation state actors, and assist stakeholders and regulators take informed decisions to secure power grids around the world.

References

[1] R. Lobenstein and C. Sulzberger, "Eyewitness to DC history," *IEEE Power and Energy Magazine*, vol. 6, no. 3, pp. 84–90, 2008.

[2] Eaton, "Blackout tracker: United States annual report 2017," 2017.

[3] J. Weiss, "Aurora generator test," in *Handbook of SCADA/Control Systems Security, Second Edition*. CRC Press, 2016, pp. 107–114.

[4] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS ICS, Tech. Rep., 2016.

[5] P. Polityuk, O. Vukmanovic, and S. Jewkes, "Ukraine's power outage was a cyber attack: Ukrenergo," http://www.reuters.com, [Accessed 9-May-2018].

[6] R. D. Steele, "Open source intelligence," *Handbook of intelligence studies*, pp. 129–147, 2007.

[7] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 146–153, 2012.

[8] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos, "GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET CPS: Theory & Applications*, 2017.

[9] F. Alonso and C. Greenwell, "Underground vs. Overhead: Power line installation-cost comparison and mitigation," *Electric Light and Power*, vol. 22, 2016.

[10] North American Electric Reliability Council, New Jersey, "NERC Disturbance Reports 1992-2009."

[11] D. Deka, R. Baldick, and S. Vishwanath, "One breaker is enough: Hidden topology attacks on power grids," in *Power & Energy Society General Meeting, 2015 IEEE*. IEEE, 2015, pp. 1–5.

[12] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems security," *NIST special publication SP 800-82*, 2011.

[13] U.S. Government, "Official U.S. government information about the Global Positioning System (GPS) and related topics," http://www.gps.gov, [Accessed 9-May-2018].

[14] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and applications*. Artech house, 2005.

[15] U.S. DHS and FBI, "Russian government cyber activity targeting energy and other critical infrastructure sectors," https://www.us-cert.gov/ncas/alerts/TA18-074A, [Accessed 9-May-2018].

[16] C. Davis, A. Chmieliauskas, and I. Nikolic, "Enipedia," *Energy & Industry group, TU Delft*, 2015.

[17] "Open energy information," http://openei.org, [Accessed 9-May-2018].

[18] C. Konstantinou, M. Sazos, and M. Maniatakos, "Attacking the smart grid using public information," in *IEEE Latin-American Test Symposium*, 2016, pp. 105–110.

[19] S. Pajic, "Power system state estimation and contingency constrained optimal power flow: A numerically robust implementation," 2007.

[20] Lockheed Martin, "Cyber Kill Chain," https://www.lockheedmartin.com, 2014, [Accessed 9-May-2018].

[21] E. Blossom, "GNU radio: tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, p. 4, 2004.

[22] X. Jiang, "Spoofing GPS receiver clock offset of phasor measurement units," Master's thesis, UIUC, 2012.

[23] P. S. R. Committee, "IEEE Standards for synchrophasor measurements for power systems C37.118," *New York, USA*, 2011.

[24] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[25] T. Ebinuma, "Software-Defined GPS signal simulator," https://github.com/osqzss/gps-sdr-sim, [Accessed 9-May-2018].

[26] C. E. Noll, "The Crustal Dynamics data information system: A resource to support scientific analysis using space geodesy," *Advances in Space Research*, vol. 45, no. 12, pp. 1421–1440, 2010.

[27] N. G. Varma, U. Sahu, and G. P. G. Charan, "Robust frequency burst detection algorithm for GSM/GPRS," in *60th IEEE Conference on Vehicular Technology*, vol. 6. IEEE, 2004, pp. 3843–3846.

[28] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS International technical meeting of the satellite division*, vol. 55, 2008.

[29] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.