Elektrotechnik & Informationstechnik (2018) 135/3: 250–255. https://doi.org/10.1007/s00502-018-0618-3

Botnets causing blackouts: how coordinated load attacks can destabilize the power grid

A. Dabrowski, J. Ullrich, E. R. Weippl

Power grids are a prime example of critical infrastructure, and their reliable operation is of utter importance for life and economy in most parts of the world. To stabilize the nominal frequency, power production and consumption have to be continuously kept in balance. As consumers are predominantly uncontrolled, operators have to adapt power plants' output to the demanded power using elaborated models including parameters like weather, season, and time of the day. These models are based on the premise of a large number of small consumers averaging out their energy consumption spikes. The remaining gap is closed by power plants in stand-by.

In this technical report, based on Dabrowski et al. (Grid shock: coordinated load-changing attacks on power grids. Proceedings of the annual computer security applications conference (ACSAC 2017), 2017), we show how an adversary can violate this assumption by coordinated load attacks. Gaining control over a large number of Internet-connected computers and Internet-of-Things (IoT) devices with a botnet, he can modify their power consumption in a synchronized fashion. Such sudden load changes can then outperform the power grid's countervailing mechanisms, i.e., primary and secondary reserve, and push the power grid into an unstable state eventually triggering automatic load shedding or tie-line tripping. We further emphasize that this adversary does not have to rely on any current or future smart grid features for a successful attack as the communication infrastructure for synchronized large-scale power modulation is already available – the Internet.

Keywords: botnets; load spikes; primary reserve

Wie koordinierte Lastspitzen Stromnetze destabilisieren können.

Stromnetze sind ein Paradebeispiel für kritische Infrastrukturen, deren zuverlässiger Betrieb von grundlegender Bedeutung für viele Wirtschaftszweige in den meisten Teilen der Welt ist. Um die Nennfrequenz zu stabilisieren, müssen die Stromerzeugung und der Verbrauch kontinuierlich im Gleichgewicht gehalten werden. Da die Verbraucher überwiegend „unkontrolliert" sind (d. h. ihren Stromverbrauch nicht vorab anmelden müssen), müssen Netzbetreiber den Bedarf mittels Vorhersagemodelle antizipieren und die Differenz über schnell steuerbare Generatoren ergänzen. Diese Modelle basieren auf der Prämisse einer großen Anzahl unabhängiger Kleinverbraucher, so dass sich einzelne Schaltvorgänge im Mittel ausgleichen.

In diesem technischen Bericht zeigen die Autoren, wie ein Gegner diese Annahme durch koordinierte Lastangriffe ausnützen kann. Gewinnt dieser die Kontrolle über eine große Anzahl von Internet-verbundenen Computern und Geräten (z. B. IoT), so kann dieser den Energieverbrauch koordiniert modifizieren. Diese Lastspitzen können die Regelleistung des Stromnetzes übertreffen und dieses in einen instabilen Zustand bringen. Diese synchrone Leistungsmodulation im großen Maßstab funktioniert ganz ohne aktuelle oder zukünftige Smart Grid-Systeme, sondern mit konventionellen Stromnetzen.

Schlüsselwörter: Botnetze; Lastspitzen; Regelleistung

Received April 10, 2018, accepted April 24, 2018, published online June 4, 2018

1. Introduction

In system theory, *emergence* describes a larger, complex, or surprising phenomenon caused by many smaller or simple entities. The latter are creating new system properties by interacting with each other without central orchestration or guidance. These effects are studied and explored in biology, chemistry, or agent theory among many others. For example, fractal snowflakes form from the much simpler flat hexagonal structure of the water ice grid: the six corners are slightly more likely to encounter surrounding water molecules than the flat edges. Thus, new material is preferably deposited at those, forming new – even stronger – peaks and eventually fractal snowflakes.

Emergent insecurity can arise from many smaller entities interacting in an *unexpected* manner – *unexpected* insofar as the system designers did not anticipate this behavior when initially modeling it, i.e., their model of the comprising entities is wrong. In a stable system, the individual benefits of system-preserving behavior must outweigh destructive behavior. Thus, selfish behavior substantially overlaps with the goals of the whole system. Additional resilience is achieved by being able to tolerate a certain number of misbehaving entities. The simplest form of structured (destructive) collaboration is collusion. However, this typically involves beneficial properties for all colluding parties, i.e., a selfish benefit. In contrast, today many cyber-physical systems or Internet-of-Thing (IoT) devices

Dabrowski, Adrian, SBA Research, Favoritenstraße 16, 1040 Vienna, Austria (E-mail: adabrowski@sba-research.org); **Ullrich, Johanna,** SBA Research, Favoritenstraße 16, 1040 Vienna, Austria (E-mail: jullrich@sba-research.org); **Weippl, Edgar R.,** SBA Research, Favoritenstraße 16, 1040 Vienna, Austria (E-mail: eweippl@sba-research.org)

can be weaponized without their knowledge in large quantities, and thus also without a benefit for the individual entities.

In this technical report, we show how emergent insecurity can substantially harm power grids by breaking the fundamental assumption of all power grids: the independance of small-scale consumers. This report is based on the results that have been published by the same authors in [5], though focusing on the aspect of emergent insecurity.

2. Background

A power grid has to maintain a constant balance between consumption and supply of electrical power. However, many large-scale and cheap – such as nuclear or hydroelectric – power plants cannot adjust their output quickly enough for fast load fluctuations. Thus, a mix of cheap but sluggish large-scale turbines and expensive however low-latency generators, e.g., gas turbines, together with a prediction model of average day-to-day power consumption enables a stable power grid operation. The equilibrium between consumption and supply itself is measured as the deviation from the nominal frequency. Higher power consumption will put more apparent counter-force on the turbines slowing them down, thus reducing the frequency. Likewise, the frequency increases by overproduction. Primary control reserve (or spinning reserve) [14, 15] is used within a negative feedback loop to push the grid into balance again. European regulations demand 3000 MW regulatory reserve to be fully activatable within 30 seconds. Additionally, automatic emergency provisions [8], [17, p.65], [14, p.26] take action to automatically disconnect consumers or producers if the grid frequency degrades too much. For example, in the continental European grid (ENTSO-E or UCTE) with its nominal $f = 50$ Hz the first 10–15% customers are automatically disconnected at 49.0 Hz, further 10–15% at 48.7 Hz with multiple further thresholds down to 47.5% where all power plants are disconnected to protect their turbines from mechanical stress.

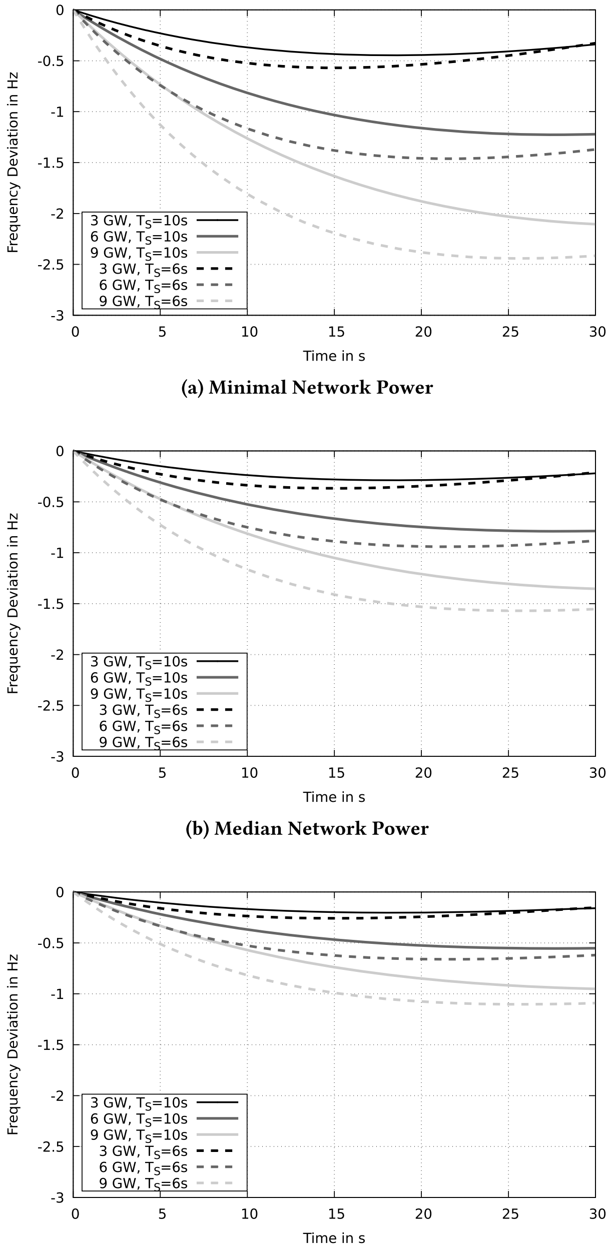
In computer networks, a botnet consists of an automated program (a bot) under single (remote) control, covertly running on a (potentially large) set of distinct computers [11]. Botnets typically can choose from a large set of covert communication channels with different topologies, making them hard to track. Botnets can grow several tens of millions devices and operate for years before they are detected. A professional botnet industry sells and rents out hijacked computers. In the past, botnets have been used to steal private data, infect other computers, and for distributed denial-of-service attacks – where a large number of requests (or traffic) to a single target renders the latter unusable.

However, this software also has substantial influence on the power consumption of a device. For example, high CPU load typically leads to more power consumption. Together with the connected peripherals of a computer, a piece of software has the ability to modulate the individual power consumption of a device and its surrounding devices.

3. Load changing attacks in power grids

For the context of this report, we assume short-term load changes to be caused by compromised devices that are part of a botnet and remotely controlled by an adversary. We consider two distinct types of attacks, static attacks and dynamic attacks.

Static attacks all of a sudden increase the power consumption of all devices of a botnet to their maximum. This behavior contradicts the inherent assumption of independent loads, and shifts the generation and consumption out of its equilibrium. Increasing consumption faster than the power grid's stabilization mechanism, in particular primary reserve, the grid frequency decreases and causes load shedding or shutdown of power plants when reaching certain frequency thresholds. It appears advantageous to piggyback such attacks on power spikes and oscillations that usually happen in the grid, e.g., every 15 minutes at a trading time-slot boundary.



(a) Minimal Network Power

(b) Median Network Power

(c) Maximum Network Power

Fig. 1. Impact of static load attack on frequency in a grid with high rotational inertia ($T_S = 10$ s), i.e., predominantly fed by conventional power plants, and low rotational inertia ($T_S = 6$ s), i.e., fed by a high share of renewables, at different levels of total network power

Dynamic attacks aim to increase the attack's frequency deviation in comparison to static attacks by exploiting negative feedback of closed-loop control systems and their tendency to over- and undershooting. This way, frequency thresholds triggering load shedding might be reached more easily, i.e., by less load that has to be controlled by the adversary's botnet. To form a closed-looped control

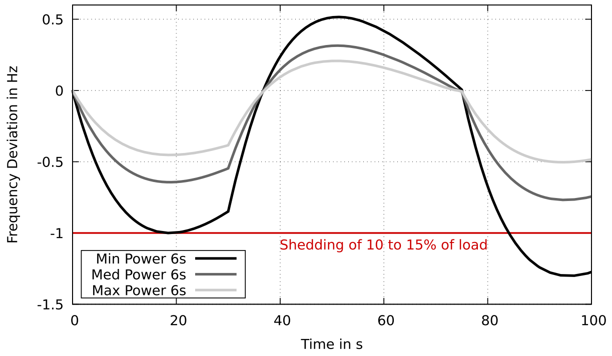


Fig. 2. Dynamic load attack of 4.5 GW at different levels of total network power

the adversary has to establish a return channel in order to measure the grid's current state, i.e., its frequency, and adapt the attack accordingly. This is however easily achieved by measuring the frequency at any power outlet within the ENTSO-E synchronous grid. Our dynamic attack increases power consumption and waits for full activation of primary control before returning power consumption back to its original value and vice versa.

Assessing the impact of these attacks, we developed a Matlab/Simulink model that is based on Ulbig et al. [12]. The model includes the power grid's frequency response to frequency deviation, the self-regulation effect as well as primary as well as secondary control and is parameterized according to the ENTSO-E operation handbooks that are publicly available. Then, we simulated the power grid's response to such static and dynamic attacks with varying amounts of attack load, total load in the power grid as well as the start time constant. The results for the static attack are depicted in Fig. 1 and can be summarized as follows:

- The more power an adversary is able to modify, the more impact she has on power grid frequency.
- The more total load in the European power grid, the less impact has an attack. This implies that it remains easier for an adversary to strike in times of low power, e.g., on national holidays or in summer.
- The shorter the start time constant T_S, the more an attack impacts power grid frequency. The start time constant is proportional to the system's mass inertia of all turbines. Mass inertia however becomes lower with the increased use of renewables as wind turbines and PV cells are connected to the power grid by inverters. Therefore do not contribute to the overall system mass inertia, and allow to destabilize the system more easily.

The results of the dynamic attacks are shown in Fig. 2. Modulating 1.5 times the reference incident (RI = 3000 MW), the grid's frequency shift at the second swing is higher than at the first one albeit the attacker is modulating the same load. The attack eventually triggers the automatic load-shedding threshold at 49.0 Hz causing the first group of households to loose power.

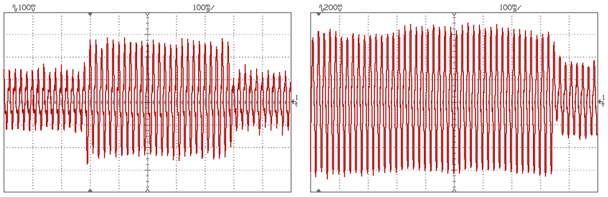
4. Forming a botnet for load changing attacks

Acquisition [6], synchronization [19], and geo-location [4, 9] of infected bots are solved problems. For our herein described attack to work, an attacker has to additionally understand the dynamics (amplitude and response times) the bots offer for modulating their load towards the power grid.

Based on measurements and data sheets we compiled Table 1. We denote the software-modulated part ΔLoad = peakload − baseload and the response times. Since multiple power converters (and stabilizers) can sit in between the component and the grid smearing the load peaks, we made our measurements at the 230 V level.

Table 1. Modulated load by device (Sources: own measurements, data sheets, and [3])

Device	Type	Latency	Δ Load
CPU	Core2 Duo	20–60 ms	35 W
	i3	20–60 ms	55–73 W
	i5	20–60 ms	73–95 W
	i7	20–60 ms	77–95 W
	i7-E	20–60 ms	130–150 W
GPU	Low-end	20–60 ms	20–76 W
	Mid-end	20–60 ms	102–151 W
	High-end	20–60 ms	150–238 W
	Top-end	20–60 ms	201–297 W
HDD		20–60 ms	3–7 W
Screen TFT	Size dep.	1–5 s	60–100 W
Laser printer	SOHO	1–3 s	800–1300 W
Smart thermostat	elec. Heating	1–10 s	1–15 kW
Smart oven		1–10 s	2–3 kW
Smart refrigerator		1–10 s	300–500 W
Smart kettle		1–10 s	1000–1500 W



(a) Intel i7 ZCPU stress test

(b) 3D mark benchmark ending

Fig. 3. In a typical gaming PC the PSU ramps up the current within a single AC cycle to a multiple compared to idle usage

As an example, Fig. 3 displays current measurements over a shunt resistor. CPUs and GPUs can multiply the computer's power usage within 1–3 AC power cycles. Laser printers turned out to be a heavy software-controllable load, whereas hard disks have a very low load for modulation as most of the energy is used for spinning.

In order to estimate the attacker's ΔLoad per infection, we created prototypical hardware setups: some botnets specialize in server software for infections whereas other specialize on security vulnerabilities in games for infections. This implies that the first targeting servers offers more hard discs and not laser printers, but the latter more gaming PCs with more powerful graphics controllers (GPU). The four profiles of office, home, gaming, and server computer result in control-able ΔLoad of 338 W, 600 W, 715 W, and 233 W respectively.

Orthogonal to these hardware profiles, we defined two conservative IoT mixes were we mix in a single digit percentage of IoT devices. The final estimation is presented in Table 2 and discussed in the section below.

5. Discussion

Until now, power grid operation was based on the assumption that power consumers act independently; generally speaking, if a light bulb was switched on in one household, it was probable that a bulb in another household had been switched off. Sophisticated load profiles allowed energy suppliers to predict power consumption accord-

Table 2. Infections needed (est)

Configuration		No IoT	Low IoT	Medium IoT
	avg. Δ*Load*	*Distribution 1*	*Distribution 2*	*Distribution 3*
Office PC	338.45 W	40%	40%	30%
Home PC	600.75 W	30%	30%	40%
Gaming PC	715.8 W	15%	15%	20%
Server	233.8 W	15%	15%	10%
IoT AC	800 W	–	0%	4%
IoT thermostat	8,000 W	–	4%	8%
IoT oven	2,500 W	–	0%	1%
IoT refrigerator	400 W	–	0%	1%
IoT kettle	1,250 W	–	0%	1%
Avg. Δ load p. infection		458.045 W	778.045 W	1,201.125 W
Infections 3000 MW (1 RI)		6,549,575	3,855,819	**2,497,659**
Infections 4500 MW (1.5 RI)		**9,824,363**	5,783,728	3,746,488

ing to the season, weather, the day of the week, etc. in a quite accurate manner. Minor imbalances between consumption and supply were handled by control reserve.

Independent consumers were a valid assumption in the past but nowadays the latter does not hold anymore. This assumption is threatened by millions of devices that are connected to the Internet with many more to follow in the next years. In a well-known pattern, adversaries tend to bundle a high number of compromised computers in a botnet and control them in a coordinated way; this way, an adversary is able to send a single command to the bots – the compromised computers – and they act simultaneously. For example, in 2016, the Mirai botnet mainly consisting of embedded and IoT devices attacked various high profile targets like telecommunication operators or DNS providers [1].

So far, attacks in the cyber domain had their impact mostly in the same domain. However, in a concerted action of such devices, a cyber-launched attack is now able to influence the physical world by destabilizing the power grid. Our work emphasizes the existence of this threat and concludes that between 2.5 and 10 millions bots – depending on their distinct power consumption behavior, see Table 2 – are sufficient to negatively affect the European Synchronous Grid causing large-scale blackouts. Past botnets in the wild were known to have tens of millions of devices [9]; thus, our results show that such attacks against the power grid are indeed feasible for larger actors and nation states. These attacks lack the attributional properties that physical attacks typically have.

In a world of increasing density of interconnected large and small computers with an increased share of the total power consumption, botnet-based attacks against the power grid are expected to become more viable over time. This specifically includes Internet-of-Things (IoT) devices such as smart fridges, smart thermostats, or smart air-conditioning. Such devices typically lack the stringent updating infrastructure that help protect personal computers.

The Northeast Blackout of 2003 [16] and the Norwegian Pearl incident in Europe in 2006 [13] demonstrate that power grids tend to experience fatal cascading effects in failure situations. Bringing the power grid back into full operation is a tedious task and might take multiple days or even weeks even without any physical defects. Among other problems, only so-called black-start-capable power plants can start operation without an external power source. Resynchronization of multiple grid areas is time-consuming. Extended periods of power loss does not only negatively impact comfort of life, hygiene, and economy, but also lead to life-threating situations for people that need medical attention or are dependent on supply of refrigerated medicine, e.g., Insulin.

While these attacks do not explicitly rely on smart-grid features of current of future grids, some of the envisioned smart-grid functionality could help in defeating the problem. *Demand-side management* allows the control of electric loads based on predetermined factors; for example, putting the washing machine into operation when the energy costs are low or shifting heating/cooling of houses to a time of an energy surplus in the power grid. In this respect, the smart grid is a curse and a savior at the same time: On the one hand, demand-side management could be used as a countermeasure towards the described attacks and certain types of loads could become switched off in presence of an attack to stabilize the power grid. In comparison to today's countermeasures of the power grid, i.e., primary and secondary reserve, demand-side management is able to react nearly as fast as the attack and does not have to obey underlying physical mass inertia of power plant turbines. On the other hand, an adversary might exploit this very functionality to perform her load-changing attacks if it has not been implemented in a secure manner.

6. Related work

Irregular behavior in power grids happens from time to time, mostly due to unexpected incidents and not as a consequence of malicious behavior. ENTSO-E investigates and publishes such incidents to advance the knowledge for proper incident response. Thereby, ENTSO-E reported on the impact of solar eclipses on power production [10], a blackout in larger parts of central Europe caused by a cascade of tripping lines [13] after a ship transfer demanded disconnection of a pair of tie lines in Germany in 2006, and a similar one in Turkey [7]. The first targeted cyber-action against a power grid happened in the Ukraine in 2015. The adversaries used malware delivered via e-mails, stole credentials and finally got access to the power providers' SCADA systems [2]. The adversaries used attack vectors well-known in traditional IT, whereas our attacks strike the power grid – a cyber-physical system – in its physical part. Xu et al. [18] aimed to increase loads in data centers to trip their circuit breakers. The load increase is caused by the adversary renting cloud services or by using external web services to trigger computationally expensive operations. The authors sought to unplug a cloud provider's data center, but this did not negatively impact the power grid itself.

7. Conclusion

Insecurity and attacks can occur by emergent behavior, i.e., where small sub-systems produce new (surprising) properties for the whole system. Our described attack undermine one of the fundamental assumptions of power grids: the independent small-scale power grid customer. An attacker can easily buy or build a large enough botnet to threaten the stability of a power grid by using software to synchronously manipulate the latters' power consumption.

Power grids are the largest man-made closed-loop control system in the world that predate the Internet by decades. With current telecommunication technologies an attacker can bind millions of those formerly independent power consumers to attack the grid. By lowering the grid's frequency to fixed thresholds, e.g., 49.0 Hz in Europe, the attacker is able to trigger automatic emergency load-shedding thereby disconnecting a significant number of consumers from the power grid. Depending on the distribution of infected computers and IoT devices as well as environmental conditions, we calculated a critical mass of 2.5 to 9.8 million infected devices for the whole Continental European grid. Botnets of that size have been easily surpassed in the past. The attacks demonstrates that power grids are not only vulnerable by classic IT vectors or the upcoming transformation into smart grids but already in their current form: by attacking the physical part of the cyber-physical system through the Internet.

Acknowledgements

This work was partially sponsored with the *CyPhySec* project by the *Bridge Frühphase* program and the *COMET K1* program, both by the Austrian Research Promoting Agency (FFG).

References

1. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., Zhou, Y. (2017): Understanding the Mirai Botnet. In 26th USENIX security symposium (USENIX security 17) (pp. 1093–1110). Vancouver, BC: USENIX Association. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.
2. Harrell, B. (2017): Why the Ukraine power grid attacks should raise alarm. http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html.
3. Power consumption of PC components in watts (2017): http://www.buildcomputers.net/power-consumption-of-pc-components.html. Accessed 2017-05-06.
4. Bureau, P.-M. (2009): Malware trying to avoid some countries. https://www.welivesecurity.com/2009/01/15/malware-trying-to-avoid-some-countries/. Accessed 2017-05-30.
5. Dabrowski, A., Ullrich, J., Weippl, E. (2017): Grid shock: coordinated load-changing attacks on power grids. In Proceedings of the annual computer security applications conference (ACSAC 2017), New York: ACM.
6. Danchev, D. (2013): How much does it cost to buy 10,000 U.S.-based malware-infected hosts? https://www.webroot.com/blog/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/. Accessed 2017-05-30.
7. European Network of Transmission System Operators for Electricity (2015): Report on blackout in Turkey on 31st March 2015.
8. Forum Netztechnik (2012): Technische Anforderungen an die automatische Frequenzentlastung. In German.
9. Porras, P., Saidi, H., Yegneswaran, V. (2009): An analysis of conficker's logic and rendezvous points. Technical report. SRI International. http://www.csl.sri.com/users/vinod/papers/Conficker/. Accessed 2017-05-30.
10. Regional Group Continental Europe and Synchronous Area Great Britain (2015): Solar eclipse 2015 – impact analysis.
11. Rodríguez-Gómez, R. A., Maciá-Fernández, G., García-Teodoro, P. (2013): Survey and taxonomy of botnet research through life-cycle. ACM Comput. Surv., 45(4), 33 pages.
12. Ulbig, A., Borsche, T. S., Andersson, G. (2014): Impact of low rotational inertia on power system stability and operation. arXiv:1312.6435.
13. Union for the Co-Ordination of Transmission of Electricity 2007 (2007): Final report: system disturbance on 4 November 2006. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf.
14. Union for the Coordination of the Transmission of Electricity (UCTE) (2004): Continental Europe operation handbook. European network of transmission system operators for electricity. Appendix 1 – Load-frequency control and performance. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy_1_Appendix%20_final.pdf.
15. Union for the Coordination of the Transmission of Electricity (UCTE) (2004): Continental Europe operation handbook. European network of transmission system operators for electricity. Chapter policy 1 – Load-frequency control and performance. https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy1_final.pdf.
16. U.S.-Canada Power System Outage Task Force (2004): Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.
17. Verband der Netzbetreiber (VDN) (2007): TransmissionCode 2007 – Netz- und Systemregeln der deutschen Übertragungsnetzbetreiber. https://www.bdew.de/internet.nsf/id/A2A0475F2FAE8F44C12578300047C92F/$file/TransmissionCode2007.pdf (in German).
18. Xu, Z., Wang, H., Xu, Z., Wang, X. (2014): Power attack: an increasing threat to data centers. In Proceedings of the network and distributed system security symposium 2014. Internet Society.
19. Zorn, G. (2010): RADIUS attributes for IEEE 802.16 Privacy key management version 1 (PKMv1) protocol support. RFC 5904 (Informational), 15 pages https://doi.org/10.17487/RFC5904.

Authors

Adrian Dabrowski

is a Ph.D. candidate at Vienna University of Technology (TU Wien), lecturer there, and employed at SBA Research. Before going into computer security he was engaged in several robotics projects where he also published a paper on reverse engineering of a RADAR system. When he eventually switched to security, he never forgot his cyber-physical roots. For his master's degree he broke a widely-used RFID-based door locking mechanism. For this work he was awarded the IEEE Section Austria Diploma Thesis Award. His paper on detection of fraudulent base stations in mobile phone networks won the Best Student Paper Award at ACSAC 2014. Adrian teaches graduate courses on Internet security and is engaged in Capture the Flag (CTF) contests.

Johanna Ullrich

is a senior researcher at SBA Research. Her research interests include network security, and raising awareness for security and privacy in traditional engineering. She received a bachelor's degree in electrical engineering and information technology and a master's degree in automation engineering, both with distinction from the TU Wien. In 2016, she obtained a Ph.D. degree sub auspiciis praesidentis with a thesis focusing on side channels and their practical exploitation in attacks. Beyond, Johanna teaches graduate courses at universities and universities of applied sciences.

Edgar R. Weippl
is research director of SBA Research and Privatdozent at the TU Wien. After graduating with a Ph.D. from the TU Wien, Edgar worked in a research startup for two years. He then spent one year teaching as an Assistant Professor at Beloit College, WI, USA. From 2002 to 2004, while with the software vendor ISIS Papyrus, he worked as a consultant in New York, NY and Albany, NY, USA, and in Frankfurt, Germany. In 2004 he joined the TU Wien and founded the research center SBA Research together with A Min Tjoa and Markus Klemen.