Supercomputing manuscript No.
(will be inserted by the editor)

Energy-Oriented Denial of Service Attacks: an Emerging Menace for Large Cloud Infrastructures

Francesco Palmieri (✉) · Sergio Ricciardi · Ugo Fiore · Massimo Ficco · Aniello Castiglione

Received: date / Accepted: date

Abstract This work analyzes a new and very subtle kind of security threat that can affect large scale cloud-based IT service infrastructures, by exploiting the computational resources of their component data center in order to waste as much energy as possible. The consequence of these threats range from increased costs in the energy bill, to penalization for exceeding the agreed quantity of green house gases (GHG) emissions, up to complete denial of service caused by electrical outages due to power budget exhaustion.

We analyzed the different types of such attacks with their potential impacts on the energy consumption, modeled their behavior and quantified how current energy-proportional technologies may provide attackers with great opportunities for raising the target facility emissions and costs. These efforts resulted in a simple model with some parametric reference values that can be used to estimate the impact of such attacks also in presence of very large infrastructures containing thousands or millions of servers.
The final publication is available at:
http://link.springer.com/article/10.1007%2Fs11227-014-1242-6

Keywords Cloud Infrastructures · Data Center Security · Power Consumption · Denial of Service · Energy-Oriented Attacks

Francesco Palmieri (✉), Massimo Ficco
Department of Industrial and Information Engineering,
Second University of Naples
Via Roma 29, I-81031 Aversa (CE), Italy
E-mail: francesco.palmieri@unina.it,massimo.ficco@unina2.it

Sergio Ricciardi
Departament d'Arquitectura de Computadors,
Universitat Politècnica de Catalunya - BarcelonaTech (UPC)
Carrer Jordi Girona 31, E-08034, Barcelona, Spain
E-mail: sergio.ricciardi@ac.upc.edu

Ugo Fiore
Centro Servizi Informativi, Federico II University of Naples
Via Cinthia 5, I-80131 Napoli, Italy
E-mail: ugo.fiore@unina.it

Aniello Castiglione
Department of Computer Science, University of Salerno
Via Ponte don Melillo, I-84084 Fisciano (SA), Italy
E-mail: castiglione@ieee.org, castiglione@acm.org

1 Introduction

The Cloud Computing paradigm is experiencing an astonishing success within the IT arena due to its extreme effectiveness and flexibility in providing computing and storage resources according to a self-service, on-demand and pay-per-use scheme [50][1]. In order to support such services on an Internet scale, a large number of data centers and computing farms distributed throughout the world, need to share their resources and cooperate to provide the ever growing number of their users with an adequate amount of runtime and storage facilities. However, with the success of Cloud Computing, the consolidation of IT infrastructures in very large data centers is introducing several critical scalability and manageability issues related to the growing electrical power demand of the involved hardware facilities and cooling systems. These are the most critical factors affecting both the operational cost and the carbon footprint of cloud-related data centers, thus worsening, on a large scale, the problem of global warming. Furthermore, together with the alarming rise in the electrical power needed to ensure the correct operation of the above data centers, there is an equally dramatic increase in security problems affecting the large scale distributed infrastructures built starting from them, which usually consolidate hundreds of thousands of servers

with other auxiliary facilities such as cooling, storage and network communication, and support millions of concurrent e-commerce transactions and Web queries per day. In this scenario, the demand for efficient methods for preventing, detecting and mitigating intrusions and other hostile activities, leading to the development of complex analysis techniques and attack countermeasures, resulted in a simultaneous improvement in the cleverness and effectiveness of attack strategies and tools, also characterized by the exploitation of new attack targets and goals that are very different from the traditional ones that essentially involve the availability or performance of the data center elements providing specific services as well as the confidentiality or integrity of data stored or transmitted on/by them. These new attack targets and aims are mainly inspired by the critical energy/power-related issues affecting large data centers operating within cloud infrastructures and strive to exploit weaknesses in power-saving and management facilities in order to increase the energy consumption of entire farms, by causing significant increase in their energy bills/operational costs and hence financial damages to the involved service providers. In the worst cases, these attack strategies may also cause service disruptions due to the exhaustion of data center power budgets leading to power outages, or overheating resulting in automatic protection-driven shutdown of many devices.

Until now, security and energy efficiency have been two completely separated research areas with no (or, at the best, minimal) contact points and common issues. In this work, that extends the preliminary studies presented in [38], we explore an intersection area between these two fields by addressing a new energy-related security perspective that may become an ordinary matter over the next years. Therefore, in considering future security challenges, we cannot disregard the energy-efficiency of the involved targets by carefully understanding and managing in a joint way both the energy-related requirements/constraints and the underlying security strengths and weaknesses. Accordingly, we analyzed and evaluated the impact of common network-based denial of service (DoS) attacks on the energy consumption of modern data center infrastructures by highlighting their troublemaking potential in terms of financial damages (due to the additional energy costs introduced) and service disruption on poorly dimensioned farms.

2 The Critical Role of Power Demand in Cloud Infrastructures

Modern large scale IT service infrastructures, usually based on the cloud paradigm, are built by aggregating through the Internet several huge data center farms, distributed throughout the world and sometimes owned by different organizations, but operating in a fully coordinated way as a unique federated entity. Each of these data centers contains a large number of computing and mass-memory devices (usually servers and disk arrays) providing computing and storage capabilities to users' tasks/demands incoming from the Internet. All these devices are interconnected through high speed and low-latency local area network (LAN) switches (usually 10Giga Ethernet or Infiniband). Every server has a processing capacity, depending essentially on the number of cores and/or processors, whereas the capacity of storage arrays, often organized into storage area networks (SANs) depends on the number and the size of the disk devices they contain. The power demand in these data center farms is mainly originated by the above computing, storage and LAN devices (also known as the *runtime system*), where servers are the most energy-hungry elements. There are different kind of servers, ranging from small ones with computing capabilities comparable to personal computers to large supercomputers or special purpose servers optimized for specific tasks such as Web servers and database management, each characterized by its specific power demand and energy-efficiency degree, often supported by specific energy-proportional architectures [4] making power consumption depending on their real operating load [48]. The CPU contributes to most of the server power consumption, ranging from 25% to 55% of the overall one, depending on the server architecture, followed by memory and networks interfaces [16], [4]. On the other hand, disks, motherboard and fans consume less energy (see Table 1).

Table 1 Energy consumption breakdown of a low-end server

Component	*Avg Power Consumption*
CPU [21]	80 W
Memory [20][23]	36 W
Motherboard [16]	25 W
Disk subsystem [27]	12 W
Fans [16]	10 W
Network Interface [44]	2 W

However, a significant amount of the whole energy required for data center operations (about 48% accord-

ing to [15]) is also drained by the so-called *auxiliary* or *support* subsystems such as the HVAC (heating, ventilation and air conditioning, summing up to 38%), UPS (uninterruptible power supply, with about 8-9%) and lighting/surveillance facilities. While the more sophisticated data centers are usually able to implement more efficient cooling strategies, their stricter resiliency and availability requirements imply the use of redundant high-capacity UPS equipment, resulting, in turn, in a higher power demand. The *power usage effectiveness* (PUE) index, defined by the Green Grid [47], measures the energy-efficiency of an entire data center as the ratio of the total amount of power used by the whole facility to the power delivered to the computing equipment alone. A PUE value of 2 is the current average [48], meaning that the impact of HVAC and UPS doubles the runtime subsystem's energy requirements, by absorbing as much energy as the computing and storage resources themselves.

It has been estimated that the worldwide data centers electrical power demand amounts to about 26 GW, corresponding to about 1.4% of the global electrical energy consumption, with a growth rate of 12% per year [22], [9]. At the state of the art, a medium-sized 5,000-square-foot data center is characterized by an average daily energy demand of 27 MWh [15], as much as 9,000 houses at full load. Consequently, the cost of the electrical energy needed to power the data centers becomes one of the main items to be taken into account when estimating their *operational expenditures* (OPEX). As a simple reference, the annual power cost for US data centers ranges as high as 3.3 billion dollars [15] and the yearly energy bill for a medium-sized 2 MW data center with a 50% base-load energy consumption could be as high as US$ 604,000 in the US, about US$ 1,112,000 in the UK and about US$ 1,375,000 in Germany [2] (due to the differences in price of power). In Spain, the Barcelona Supercomputing Center (considered a medium-sized data center) consumes 1.2 MW, as much power as a town of 1,200 houses [26], and pays every year more than 1 million Euros just for the energy bill [40]. For this reason, the farm owners usually negotiate their contracts with the electrical energy providers according to a flat-rate payment model, where a fixed fee is due for any consumption under a previously established usage threshold, regardless of the actual cost or consumption, and an additional (typically high) proportional price per KW is required only when the power drawn exceeds such threshold. By properly negotiating such usage threshold, both data center owners and electrical companies are shielded from fluctuations in the energy demand/offer, and cloud operators can achieve significant financial savings if they carefully estimate their energy consumption profile by considering that in modern energy-efficient server equipment the energy consumption increases proportionally with the load (apart from the fixed energy consumption which accounts for about 50% of servers full operational power [16]). The typical load in data centers is not constant over time but characterized by high utilization periods (e.g., limited in some peak hours of the day) followed by often long low utilization periods (e.g., during the night). In particular, it has been observed that the load fluctuations are almost predictable within certain fixed time periods (e.g., day-night, months or years) and resemble a pseudo-sinusoidal trend [3], [28]. These considerations drive the data center analysts in dimensioning the above flat usage threshold as low as possible, just sufficiently higher than the average demand observed in the above trends, in order to avoid additional prices due to exceeding the flat-rate threshold and simultaneously reduce their recurrent expenses. This implies that any unforeseen increment in the data center energy consumption exceeding the flat-rate usage threshold may have devastating effects on its operational costs.

3 A New Perspective in DoS Attacks

Denial of Service (DoS) attacks are an ever increasing menace for corporate and government organizations doing their core business activities through the Internet. The main targets of these attacks include all the available resources at both the runtime (computing power, memory buffers, disk drives) and network (communication protocols and interface bandwidth) service layers with the final effect of the total disruption or degradation of such services. The hostile activities are usually performed throughout a network connection and originated by machines scattered throughout the Internet. Countermeasures may be complex and of limited effectiveness, since it is very difficult to distinguish between a genuine and a malicious connection/service request and thus apply the filtering rules/policies needed selectively to block the hostile traffic. By affecting the servers, the storage systems and the Internet connections of the victim sites, the attackers may be able to prevent any access to cloud services such as Web-based applications or virtual machines providing online banking, e-commerce, computing services, etc. [30]. Often, in order to increase the attack power and make the reaction even more difficult, a huge number of remotely controlled machines can be used as the origin of multiple simultaneous attacks against a single target or a whole organization. This type of menace is also known as Distributed Denial of Service (DDoS) attack.

3.1 Network Bandwidth Exhaustion DoSes

DoS attacks against the network connectivity aim at exhausting the available bandwidth on the Internet connection interfaces through the generation of an extremely large number of packets or service requests directed to the target site. Typically, these packets are ICMP or UDP ECHO packets, forcing the target system to generate a corresponding reply traffic in the opposite direction, but in principle they may be anything [10] flooding the network connection with service or connection requests (e-mails, HTTP requests, etc.). Another very dangerous network attack is the SYN flood one, overloading a target victim with a large quantity of initial TCP connection attempts but preventing the completion of the three-way handshake process leading to successful connection establishment. This results in exhausting, with bogus "half-open" connections, the maximum number of simultaneous connections on the victim machine but also in bandwidth exhaustion on the involved network interfaces, in presence of an high sustained SYN transmission rate. Finally, also very aggressive network or port scan activities toward the cloud's exposed address space may have the adverse effect of completely saturating the Internet connection bandwidth of the associated sites, in particular when stealth scanning strategies, not easy to detect and filter in transit, are used.

3.2 Processing Power Exhaustion DoSes

Alternatively, the computing resources available on the target sites can be saturated by overwhelming them with a large amount of CPU-intensive requests, such as continuous transaction attempts on HTTP, HTTPS or any kind of server operating through the network. For example, a randomized HTTP requests flood can be used to exhaust the available communication channels on a target victim Web server [46]. In addition, also the CPU may be overloaded by cryptographic operations when HTTPS or any kind of SSL-empowered services are targeted. For example, by using the attack described in [14], a malicious Web client can coerce a Web server, reached through an SSL connection, in performing expensive RSA decryption operations until its CPU load reaches 100%.

Furthermore, several vulnerabilities in Web Services (WS) technologies [24], [25], [35] that exploit the XML verbosity and the complex parsing process of the SOAP message body are available. For example, the processing of a large number of name-space declarations, oversize prefix names or name-space URIs, and very deeply nested XML structures/tags), can exhaust most of the computational resources of the target systems (mainly CPU and memory) according to a technique known as *coercive parsing*. The same effect can be achieved by pointing to a bogus external schema location providing a large or malicious payload (malformed schemes leading to coercive parsing). In addition, attackers can exploit a WS security vulnerability allowing encryption to be used almost anywhere within a SOAP message without any robust schema validation, so that the CPU capacity may be overloaded by introducing a large number of nested encrypted header blocks within a single SOAP message. That is, an oversize security header of a SOAP message can cause the same effects of an oversize payload, where as a further adverse effect, a chained encrypted key can lend to high memory and CPU capacity consumption. Some possible solutions could be the adoption of anomaly detection techniques such as the ones proposed in [18][36]Palmieri2010737 and [37]. Nevertheless, the energy-related attacks are very difficult to be detected since they are very simple and easy to implement, but extremely difficult to stop because there is no way to distinguish between legitimate and illegitimate requests and hence no way to filter such traffic.

Finally, the more subtle and recent processing power attacks are those ones that exploit algorithmic deficiencies in many common data structures, protocols and tools characterizing networked applications. For example, a long list of technologies, including PHP, ASP.NET, Java, Python, Ruby, Apache Tomcat, Apache Geronimo, Jetty and Glassfish, as well as Google's open source JavaScript engine V8 are known to be vulnerable to DoS attacks exploiting the hash table structures they use. In detail, these attacks strive to find a sufficient number of collisions in the involved hashing algorithms, causing worst-case behavior in the above applications' hash table usage [13]. The effects on the target hosts may vary from an increased workload to complete collapse due to total CPU capacity exhaustion.

3.3 Disk Hardware Solicitation DoSes

Also traditional or more recent disk drives may be the indirect target of DoS attacks, performed through the interfaces provided by the various available network file systems (e.g., NFS, CIFS, AFS or SAMBA) or file servers (FTP, FSP, RPC tools, etc.) by overwhelming the drive hardware with a huge number of different randomized read/write requests on always different files, by frustrating as much as possible the effect of buffer caches or disk scheduling algorithms. This may have the effect of introducing a significant burden on

the mechanical components of magnetic drives, by reducing their effectiveness and lifetime, together with the overall drive performance. Also, the more recent non-mechanical devices such as the solid state drives (SSD) can be affected by attacks that, by soliciting their NAND-based memorization hardware cells with multiple continuous write operations, reduce both the device performance and its lifetime (by reaching the limit of re-write operations supported on the same cell).

3.4 The New Menace: Energy-Related DoSes

The above DoS activities can become more effective against large scale organizations, such as cloud service providers, by simultaneously exploiting new, more subtle, objectives and attack scenarios, soliciting proportional electric power consumption as well as energy efficiency and power management features on the highest possible number of servers operating on the target sites. Simply stated, these attacks leverage hardware components on server equipment experiencing the maximum energy demand gaps between busy and idle operational states. The hostile activities consist in generating the maximum possible workload on the target components, by always keeping them 100% busy so that they can never enter low power usage states (usually implying an average 22% reduction in power usage), and thus forcing them to continuously operate at their near-maximum frequency/speed, voltage and temperature (this also reduces their lifetime). In such a way, since in modern server systems the energy demand is tightly related to all the above operating features, also the electric power absorbed is maximized, with the obvious consequences on the involved data centers' operational expenses and PUE (since also HVAC effectiveness is reduced by unnecessary overheating). In such a scenario, the most critical components from the power absorption perspective are CPU and memory since the relevancy of disks in the overall server's power budget is strictly related to the presence of a significant number of these devices. Anyway, overloading the server's hard disks with millions of read or write operations by forcing them to constantly operate at their maximum sustained transfer rate or to continuously spin up and down the hard disks spindle engines is another effective way of draining more and more system power.

However, in order to correctly quantify the damaging potential of an energy-oriented DoS attack launched throughout the network, we have not only to concentrate our attention on the most power demanding devices, but we have to consider all the available energy-sensible ones, that is, those whose energy consumption strongly varies with the network-generated traffic load. Among these components, network interface cards (NICs) need a specific attention because, depending on their implementation features, an increased load on them also implies a cascaded load on CPU and memory.

Unexpectedly, also the existence of security tools can be sometimes exploited as an opportunity for very subtle types of energy-oriented attacks. In fact, while being essential to ensure the system integrity, such tools, that continuously monitor the server activity, have often a significant impact on their CPU/memory/disk usage and hence on the overall power consumption [6]. In many tightly-managed farms, for example, most of the servers have at least an anti-virus/malware tool installed on them, usually scanning on-the-fly any content trying to be stored locally. Since such scanning activity is strongly CPU and I/O-intensive, causing significantly long periods of both CPU and disk load, a disruptive energy-aware attack can be orchestrated by choosing a specific, eventually legitimate content, triggering the anti-virus reaction in order to waste a great amount of CPU power, and having the malicious content massively delivered to the target by a large number of different origins. Analogously, also e-mail spam can be exploited for energy-oriented attacks to relay servers running anti-spam software in order to identify and filter out unwanted messages, since these tools usually eat great amounts of CPU and memory resources, apart from the network saturation effects introduced by unsolicited e-mail messages [29]. An energy-oriented attack could then increase the footprint on a target mail server by simply increasing the amount of spam addressed to it.

Finally, properly crafted computer worms and trojans can gain, by exploiting system vulnerabilities and backdoors, the ability to run malicious code directly on the target nodes. In these cases, such malicious entities can trick the operating system kernel or some application binary code so that a lot of additional energy is needed for their execution, while continuing to work correctly from the users' perspective.

4 Modeling and Evaluating the Impact of Energy-Oriented Attacks

Any successful energy-oriented attack maximizes the overall server's power consumption and harshly solicits its hardware components, while presenting to both its users and administrators the appearance that the system is operating normally, with the possible exception of an increased CPU, disk or network activity. In contrast to a successful DoS attack, a successful energy-oriented attack can be stealthy, thriving on the cumu-

lative result of low-rate activities sustained over a long time. Side effects that can flag the presence of these subtle menaces include legitimate user requests being served slowly, CPU fan turning on while the server is performing some action that does not normally cause the fan to come on, the operating system becoming less interactive than usual, the network losing part of its speed/responsiveness and the hard drive spinning up immediately after a spin down.

In this section we focus on these specific menaces by modeling and analyzing their impact on the individual server's energy consumption, in order to obtain, if possible, some reference measurements and infer from them the fundamental properties and evolution trends, that can be used as a general framework to estimate the effects of energy-oriented DoSes on large scale cloud infrastructures of various sizes.

In doing this we set up a very simple measurement testbed realized by using a small single processor server, manufactured by HP, and equipped with a quad-core/8 thread (2.00 GHz/thread), Intel i7 64 bits CPU, 8 Gb DDR3 SDRAM, a 7200 rpm 500 GB HD and a Gigabit Ethernet interface connected to the LAN. Such server, that is used as the target for all the attacks, runs the Linux operating system and has its input power constantly monitored through a SCT-013-000 (Beijing Yao-Huadechang Electronic Co., Ltd) non-invasive AC split-core current sensor clip, driven by an Arduino Mega 2560 control board, collecting all the power usage measurements (1 sample/sec). Several Linux-based laptop PCs, connected via Gigabit Ethernet to the same LAN are used to launch the individual attacks against the aforementioned measurement station.

4.1 Bandwidth Exhaustion Energy-Oriented Attacks

The first device/component that can be solicited in network-based DoS attacks is the NIC, and this also holds with energy-oriented attacks. In all the NIC implementations supporting Low Power Idle (LPI) [19] or Adaptive Link Rate (ALR) [11] technologies, the energy consumption depends on the actual transmission rate/load. In detail, with LPI, the interface switches from full speed to low power mode when it is not used. The power consumption during such low power mode is about 10% of the power required when operating at its maximum rate [41]. ALR, on the other hand, provides the ability to dynamically modify the link rate according to the real traffic needs in order to reduce the power consumption. Clearly, the disruption of these attack schemes depends on how much power the device consumes in maximum speed mode with respect to low power mode; such a gap may be as high as 90% between idle and full load states for higher speed interfaces [12]. Such dependency on the current interface load can be easily observable by looking at the measured energy consumption profile on the target monitored station when attacked respectively by a SYN flood (Fig. 1) or an ICMP flood (Fig. 2).

While the additional consumption introduced by a SYN flood is definitely less uniform and valuable in size, due to its lower impact on the interface bandwidth (as compared to the other attack that is significantly more aggressive), the ICMP flood achieves an abrupt increase (and fall at the end) with an almost uniform consumption difference profile (about 11.3 W) with only some slight intermittent fluctuations during the attack, eventually due to the effect of hardware buffering mechanisms at the interface level. However, in presence of a huge number of servers the effectiveness of the attacks wasting a lot of communication bandwidth is implicitly limited by the availability of the capacity on the upstream connection to the Internet, that assumes the role of a bottleneck also for the attack itself.

In order to model the NIC energy demand increment during bandwidth exhaustion attacks, we have to differentiate between the behavior of LPI or ALR interfaces. The energy consumption of a LPI network interface (such as the Energy-Efficient Ethernet compliant, EEE) is given by:

$$E_{LPI} = P_{idle}\,(1 - t_{load}) + P_{active}\,t_{load}, \tag{1}$$

where the power demand in idle mode P_{idle} is about 10% of the power in active mode P_{active} and t_{load} is the time share percentage in which the interface is being used.

Alternatively, in ALR, the network interface is always active, but the line rate is dynamically selected to best fit the traffic rate [42]. As an example, a 1000 Mbps ALR interface can slow down to 10 or 100 Mbps when the corresponding traffic rate is required, thus saving energy. In this case, energy consumption of an ALR network interface is given by:

$$E_{ALR} = \sum_{i \in \{10,100,1000\}} P_{(i)}\,t_{(i)} \tag{2}$$

where $P_{(i)}$ is the power consumption of the interface working at link rate $i \in \{10, 100, 1000\}$ Mbps and $t_{(i)}$ is the time spent at line rate i.

Therefore, both LPI and ALR network interfaces consume according to their instantaneous line rate, and network-based attacks are aimed at increasing the working rate of the interfaces for the longest possible amount of time, that means also reducing the overall interface idle time.

In the LPI case, let's consider a parameter $\alpha \in [0, 1]$ that models the percentage of time spent by the LPI

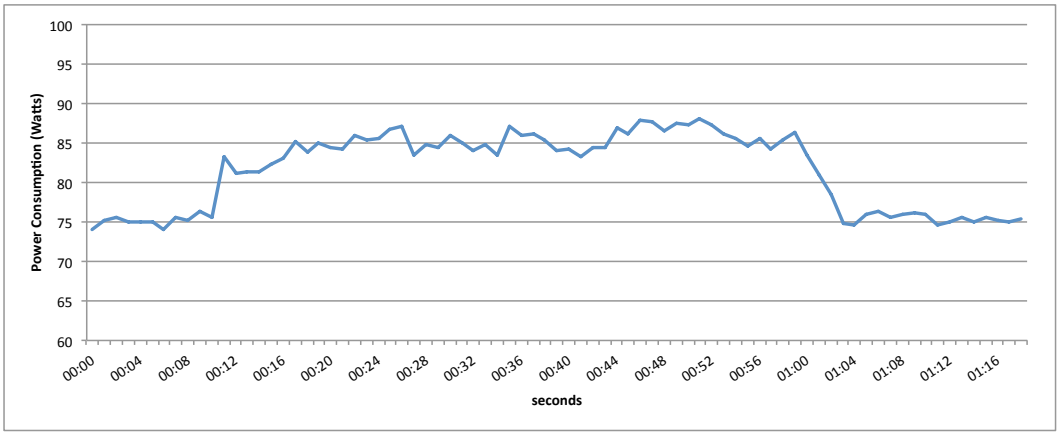

Fig. 1 SYN flood attack energy consumption.

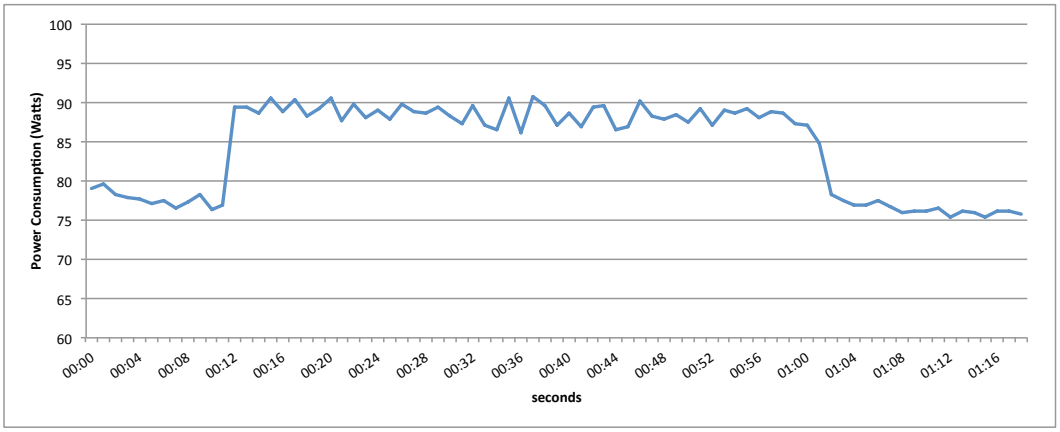

Fig. 2 ICMP flood attack energy consumption.

interface in active mode, and let the corresponding average power consumption be $P_{avg}^{LPI} = \alpha\, P_{active} + (1-\alpha)\, P_{idle}$, then the additional energy consumption induced by an attack of duration t_d on a LPI interface is given by:

$$\begin{aligned} \Delta E_N^{LPI} &= (P_{active} - P_{avg})\, t_d \\ &= ((1-\alpha)\, P_{active} + (\alpha - 1) P_{idle})\; t_d. \end{aligned} \tag{3}$$

Analogously, in the ALR case, let's consider the weights $\alpha_{(i)} \in [0,1] : \sum_{i \in \{10,100,1000\}} \alpha_i = 1$, modeling the percentage of time spent by the ALR interface at each link rate i, then the average power consumption of an ALR interface is described by:

$$P_{avg}^{ALR} = \sum_{i \in \{10,100,1000\}} P_{(i)}\, \alpha_{(i)}. \tag{4}$$

Therefore, by starting from Eq. (4) and assuming that an attack succeeds to raise the interface line rate at its maximum, then the additional energy consumption introduced by an attack of duration t_d is given by:

$$\begin{aligned} \Delta E_N^{ALR} &= (P_{(1000)} - P_{avg}^{ALR})\, t_d \\ &= ((1-\alpha_{(1000)}) P_{(1000)} - \alpha_{(100)}\, P_{(100)} + \\ &\quad -\alpha_{(10)}\, P_{(10)}) t_d. \end{aligned} \tag{5}$$

4.2 CPU Exhaustion Energy-Oriented Attacks

The most critical component, in terms of power demand, is the CPU/memory subsystem whose energy consumption is known to scale linearly with its utilization and frequency [16], [31]. Since the goal of energy-oriented attacks aimed at exhausting computing capacity is to maximize the power consumption by keeping the CPU and memory on the target system as busy as possible, these attacks generate across the network a large number of "tricky" service request subtracting most of the resources to the legitimate ones and letting the CPUs working at their maximum speed and operating frequency. In order to quantify the effects of these menaces, we attacked the measurement station with a

Deeply-Nested XML WS resource exhaustion scheme, which exploits the XML message format by inserting 10000 nested XML tags in the message body until (almost immediately) the CPU is fully committed to process the malicious messages [17]. We can observe from Fig. 3 a sharp increase in energy consumption of about 20W, sustained almost uniformly for the whole duration of the attack and immediately falling to the baseline demand value after its termination. It should be considered that this attack, differently from the flood-based ones, requires a significantly lower bandwidth on the Internet connection, and hence can affect a much larger number of victim servers simultaneously, with a really increased effectiveness in presence of a large number of targets.

In order to stress DRAM usage we also used a buffer overflow vulnerability on the Apache Web-server to force the continuous execution of a huge number of random read and write operations on very large arrays located in memory, with the effect of generating a large quantity of cache misses and hence maximizing the physical accesses to power-hungry DRAM hardware. Since this attack scheme also introduces a significant impact on CPU activity, the measurable effects are almost the same as reported in the previous experiment (see Fig. 3), and hence not shown for space reasons. Furthermore, differently from the previous one, such attack requires specific vulnerabilities to be present on the target machine and the complete compromise of the machine itself.

For completeness sake, we also studied the effects of a slow DoS attack against a traditional Web server, using minimal bandwidth and with no side effects on unrelated services and ports. For this purpose we used the Slowloris scheme [43], trying to keep open the highest possible number of connections to the target Web server and hold them open for the maximum possible time, until the Web server connection resources are totally exhausted. This is accomplished with partial requests to the target server, by sending multiple HTTP headers without completing any request. The maximum concurrent connection pool will be saturated by denying any additional connection attempts. While completely shutting down the involved server, the above attack generates a certain amount of additional computing burden but does not completely exhaust the available CPU capacity. The consequent effects on the server's energy consumption are considerably lower than the ones observable in the previously presented attacks, but however appreciable (with an increase slightly greater than 4W), as shown in Fig. 4. Such phenomenon highlights the strong dependencies of servers' energy consumption from the computing and DRAM memory load.

When modeling the impacts of these types of attacks, we have to consider that modern CPUs, in order to minimize their energy consumption during idle or low usage periods, dynamically adapt their operating frequency f accordingly to the current load: lower frequency requires a lower voltage, which will consume less energy.

Let f_{min} and f_{max} be respectively the minimum and the maximum operating frequency of a CPU; then, the required CPU voltage $V(f)$ at frequency f will be approximately given by:

$$V(f) = V_{max}\frac{f}{f_{max}}, \tag{6}$$

where V_{max} is the maximum operating voltage required at frequency f_{max}. The power consumption of a modern CPU can be represented [31] as a function of the operating frequency f, given by:

$$P(f) = \frac{1}{2}C\,V(f)^2\,A\,f. \tag{7}$$

In the above formula, C and A are constants depending on the specific CPU technology, namely *aggregated load capacity* and *activity factor* respectively. From Eq. (6), we can observe that the voltage $V(f)$ scales linearly with the frequency f, and from Eq. (7) that the power consumption of the CPU scales quadratically with the voltage (and thus cubically with the frequency).

Therefore, the attack will try to increase the operating frequency in order to consume more energy. Considering that the average CPU utilization in data centers' servers is only about 30% [5], [8], [16], we can estimate the average additional energy consumption introduced by a CPU-based DoS attack as:

$$\Delta E_C = [P(f_{max}) - P(f_{30\%})]\,t_d \tag{8}$$

where t_d is the duration of the attack and $f_{30\%}$ is the frequency corresponding to the 30% load. Thus, the energy increase depends only linearly on the attack duration but is proportional to the difference of the squares of the maximum voltage and the normal operating voltage. In other words, the intensity of the attack is more critical than its duration. As an example, a short-lived strong attack can be as effective as a long-lived, lower intensity one.

4.3 Disk Solicitation Energy-Oriented Attacks

Differently from CPUs, hard disks have mechanical moving parts (here we do not consider solid state drives), which considerably affects their energy consumption.

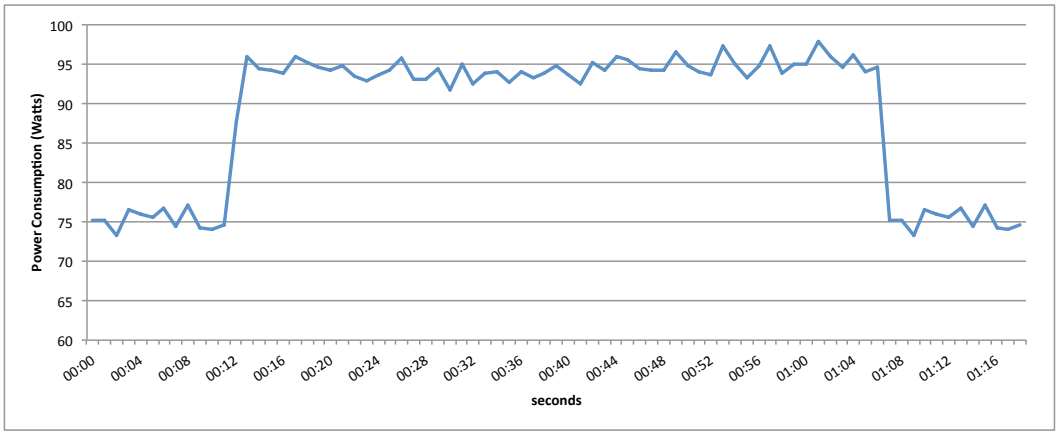

Fig. 3 Deeply-Nested XML attack energy consumption.

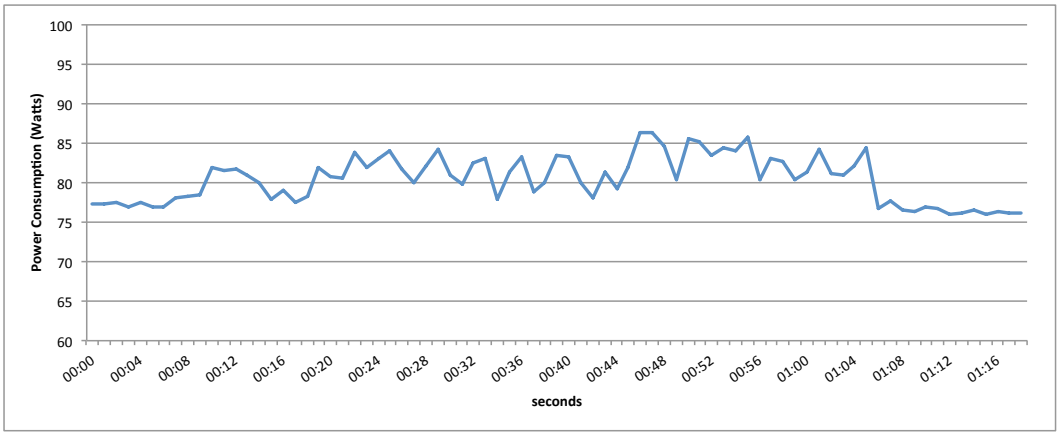

Fig. 4 Slowloris attack energy consumption.

Apart from the mechanical movements, the energy consumption of a disk depends on the number of read/write operations on it and on the involved transfer rates. Attacks that try to add additional stress on the disk hardware by forcing the continuous execution of a huge number of physical read and write operations may have significant but intermittent effects (presumably due to the file system buffer caching mechanisms causing not all the disk access request to correspond to physical disk operations) on the server's overall energy demand, that gradually decays after the attack termination. This can be observed from Fig. 5 referring to the scenario of a SMB networked file system operating on the target machine, solicited by an ad-hoc application running on a portable PC remotely mounting the SMB volume. A typical read operation at the maximum rate r_{max} consumes approximately $P_{read} = 10\mu$J/block or 2.5μJ/kB, and a typical write operation requires about the same power [34]. If the current transfer rate r varies between $[r_{min}, r_{max}]$, then a read/write operation at rate r will consume:

$$P(r) = w_r P_{op}, \tag{9}$$

where P_{op} is either P_{read} or P_{write} and

$$w_r = \frac{r}{r_{\max}} \tag{10}$$

is the scaling factor depending on the transfer rate r.

The energy consumption of a disk is given by the sum of the mechanical power consumption depending on the angular velocity ω and the logic power consumption depending on the involved operation and transfer rate.

$$P(\omega, r) = \underbrace{\frac{K^2\omega^2}{R}}_{mechanic} + \underbrace{D_r w_r P_{op}}_{logic} \tag{11}$$

In Eq. (11), K is a motor voltage constant, R is the motor resistance and D_r is the operation demand (kB) [49]. Thus, the disk power consumption depends on the square of the angular velocity ω and linearly on the transfer rate r. Also, the mechanical part is much more prone to faults with respect to logic circuits. Therefore, an attack aimed at forcing sparse, high data rate operations on the disk will have the maximum disruption and induce the highest energy consumption. Let P_{avg} and P_{max} be

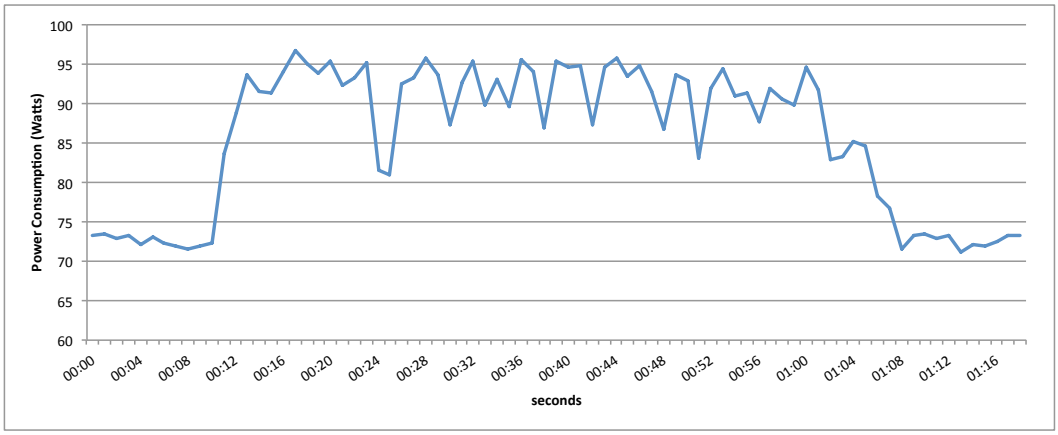

Fig. 5 Disk hardware solicitation attack energy consumption.

respectively the average and the maximum power consumption of a disk, then the additional required energy during a disk-based DoS attack is given by:

$$\Delta E_D = (P_{max} - P_{avg})\, t_d \tag{12}$$

In recent times, the evolution of solid state memory technologies is allowing high performance storage architectures to partially fill the performance gap between traditional hard disk drive technology and RAM, overtaking historical limitation in terms of latency, transfer times and costs/sustainability. Thus the storage systems in many new generation cloud data centers are starting to be equipped with a certain (growing) percentage of high performance solid state disk (SSD) devices.

Besides ensuring much better response times SSDs are inherently more energy-efficient than their mechanical drives counterparts, since they do not require moving parts, by storing data on flash chips that contains, in a single package, multiple NAND memory dies in a 3D die stacking. However, even though SSDs don't have to spin and move a mechanical read head to locate data and thus the concept of latency and seek disappears, they also exhibit a variable power draw depending on their usage, also if, at the state of the art, their power demand *is not energy-proportional* but only depends on the operating state (active, idle) or on the specific operation involved (read, write).

An estimation of the energy required by an SSD is given in the following formula:

$$E_{SSD} = P_{idle}\, T_{idle} + P_{active}\, T_{active} \tag{13}$$

where P_{active} is the power consumption when the SSD is active, and T_{active} is the time spent by the SSD while satisfying SSD requests whereas P_{idle} is the power consumption in the idle mode, and T_{idle} is the sum of all the idle periods. We have to consider that when in idle state, an SSD device is not handling any I/O operation. Ideally, an idle device should not consume any power but in real world in that idle devices require some amount of power to be up and running, that however, should be less than power required by traditional disks. In order to enhance the I/O performance, operations are parallelized on multiple flash devices whose NAND memory chips are organized into multiple channels and ways. However, as the number of channels, and the degree of parallelism in operations, increases, so does the instantaneous power consumption. This may cause the average power usage to actually increase when changing from traditional disks to highly parallel SSDs, especially the earlier and cheaper ones, which are known to manage in an inefficient way their idle state. Thus, keeping the device as active as possible (i.e., minimizing T_{idle}) is the simplest form of an energy-oriented attack.

Furthermore, due to specific characteristics of the NAND memory units, no rewrite operations are allowed on already written locations, so that when an update is needed, the involved locations have to be erased before a new data is written on them. Such "*erase before write*" behavior implies doubling the operations needed and hence introduces an additional power burden to any write access that can be maliciously exploited in energy-aware attacks based on overloading SSD devices with large number of writes.

Accordingly, we have to consider that the power drained in active mode depends on the kind of operation issued, with the power P_{read} required by read operations being significantly lower that the one required for erase (P_{erase}) and rewrite (P_{write}) ones, so that:

$$P_{read} \ll P_{erase} + P_{write} \tag{14}$$

Thus since the maximum (or worst case) power consumption of a solid state disk P_{max}, is the one characterized only by write operations ($P_{max} = P_{erase} + P_{write}$) then the additional required energy during a

SSD-based DoS attack is also given by eq. 12 where P_{avg} is the average power consumption of the specific SSD devices involved. A reference estimation for the above power consumption values (that however are very NAND flash device-dependent) comes from the models and hardware details presented in [33][39] and [7].

5 Effects and Consequence of Energy-Related DoSes

The effects of the previously presented attack types, in terms of average increment of the energy demand on the target machine can be immediately appreciated by observing the chart reported in Fig. 6.

The fundamental consequences that may be associated to these phenomena are reported in the following.

5.1 Impacts on the Energy Bill

An increase in power consumption will bear an immediate and sizable financial impact. For the sample 5,000-square-foot data center with 1000 servers [15], a sustained computing capacity exhaustion energy-oriented attack (about 20 W for each server, as reported in fig. 6) brings an additional daily consumption of about 480 KWh. Furthermore, if we also consider the cascaded effect reported in [15] where an additional amount of 1.84 W is added to each Watt drained at the processor level, due to the combined effects of Power Conversion, Distribution, UPS and Cooling, a more realistic estimation will result in a daily increment of about 1,360 KWh.

This increment may have a devastating In presence of the aforementioned flat supply contracts with an agreed-upon consumption threshold, where the attackers strive to force the farm resources to behave in a way resulting in a sustained power consumption excess over the threshold. Alternatively, also when the cost schemes per kWh are more traditional, rates may vary for daytime and nighttime. In these cases, attackers who can control the energy drawn may cause financial loss, e.g., by forcing high consumption rates over the maximum cost hours.

5.2 Causing Power Outages

Attacks may not only increase energy bills. Sometimes, their consequences can also include power outages. Power provisioning strategies in data centers have generally been designed with the objective of maximizing the computing and storage capacities, with the power budget being viewed as a constraint [16]. Such strategies aim at filling the gap between the theoretical maximum power usage and the current one, in order to deploy more computing and storage resources within the power budget. The power draw indicated by manufacturers in the documentation accompanying their product is a conservative estimate [32]. Thus, when designing the power infrastructure, barely considering the nominal power consumption will leave abundant extra power to be used when adding or updating components. On the other hand, if the actual peak power draw closely approaches the nominal value, the data center is using its power budget efficiently. However, the risk increases that fluctuations caused by attacks may cause SLA violations or, worse, outages due to trying to draw more power than what is allowed by the physical infrastructure. Note that successful attacks will depend on quality and freshness of knowledge about limits, contractual or physical, and about how close the consumption values are to critical values.

5.3 Affecting Energy-Saving Mechanisms

Normally, data centers deploy techniques to save energy. These techniques may be as simple as shutting down temporarily unused machines or using complex predictive models to adapt the power draw to the actual necessity. Energy-saving mechanism, however, may become powerful weapons in the hands of attackers who can control, to an extent, the energy consumption. Again, attackers need to know details about the energy-saving techniques in place. They also need the ability to estimate critical power draw values at which these mechanisms operate and how close actual measured values are to those limits. Then, extra work can be artificially inserted in the system to make the energy-saving mechanism ineffective. Note that attackers only need to increase the power consumption of the minimum amount that will cause the energy-saving system not to be triggered. Thus, additional activity will be less likely to be detected than massive workload that saturates the CPU. As a simple example, consider a data center where servers are put to sleep when they are idle for a given amount of time. By merely constructing fake traffic that reaches each of the servers, or all servers simultaneously, an attacker may prevent servers to enter sleep mode even if legitimate activity is low. With a very low workload added, the energy-saving strategy may be made useless, impacting the total consumption significantly.

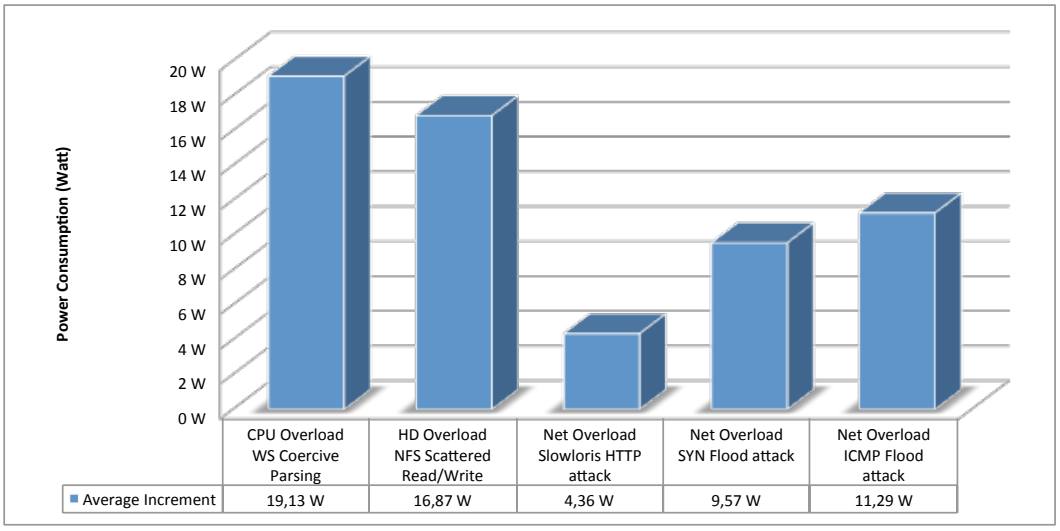

Fig. 6 Average increments on power demand for energy-oriented attacks.

5.4 Effects on Operating Temperature and Hardware Lifetimes

When CPU is overloaded, the clock is constantly kept at values close to the maximum, and consequently the chip temperature increases dramatically. The temperature becomes, therefore, an extremely important factor. By making temperature increase, an attacker is guaranteed to raise the power bill of the victim. The cooling system will in fact be solicited to cope with the temperature raise, consuming more energy. For this reason, any increment in demand-side energy usage immediately cascades on the the HVAC side, so that in the medium-sized 5,000-square-foot sample data center reported in [15] every Watt of power consumption increment on the runtime system (processor, memory, hard disk, etc.) results in approximately 1.07 Watts of additional power demand for the whole facility. Hence, thermal attacks bear a close similarity to attacks aimed at neutralizing energy-saving systems. In fact, the main goal of a thermal attack is not the saturation of resources, but only to keep the CPU constantly active with useless instructions/activities. This also prevents the circuitry to enter low-power or suspend modes, where clock is reduced and the CPU is allowed to cool, as it normally does during idle periods until an interrupt is raised. As a side effect, temperature also influences the rate of failures in electronic components, with higher temperatures reducing the component life span. The expected operating lifetime of a chip will instead double if temperature gets lower by 10℃. Thermal attacks have, therefore, tremendous potential, especially if they can be effected a large number of servers over long periods.

5.5 Exploiting Costs Related to Ecological Footprint

The energy used to power a service infrastructure has a cost, but also a *source*, whose features strongly characterize the ecological footprint of the overall infrastructure itself. Dirty sources such as, for example, fossil-based fuels, are being discouraged in response to industry and governmental efforts to promote renewable sources with low green house gases (GHG) emissions [45]. This is accomplished by introducing an additional carbon tax, according to which users pay an additional tax if they use power derived from sources with high GHG emissions. As seen before, characteristics of the taxing and rating system can be exploited by attackers, and carbon tax is no exception. Many data centers are powered by an hybrid energy source, i.e., a *green* one, such as solar or tidal energy, providing the power needed during a specific time interval (e.g., during the day) or within a specific power budget, and a *dirty* one, that is active when such budget is exceeded or when the green source is not available. An attacker that is able to control and increase the power usage during specific time intervals or over specific thresholds is also able to raise the GHG emissions related to the energy consumption of a facility, so that the victim organization will incur additional costs, for both the increment in overall power draw and for the additional tax paid.

5.6 Gaining Information from Power-Management Infrastructure

Modern infrastructural components for both the power distribution system and the HVAC system offer advanced monitoring and control capabilities. While such

capabilities allow checking the state of power distribution and cooling systems as well as adapting energy supply and cooling to the requests, "smart" components can be exploited by attackers: they can obtain a wealth of information about the support systems or even get control over them. Data that can be of interest to attackers includes, for example, details about topology, operating conditions, available energy source, temperature, peaks in the power draw or in temperature and time needed for the cooling system to respond to temperature spikes. As previously said, such information can be very valuable for attacked effecting a reconnaissance phase before designing and refining their weapons. The ability to modify operating parameters would, of course, mean that attackers may wreak havoc with the infrastructure. Additional care when regulating the access to the power infrastructure is, thus, required in order to achieve an acceptable level of security.

6 Conclusions

DDoS attacks have the potential not only of denying the service of the target facility, but may be specifically targeted at incrementing its energy consumption as well as the associated ecological footprint. Some of these attacks are non-invasive, very effective and relatively easy to implement, e.g., CPU and network-based ones, whilst others are more difficult to be put into action. An energy-oriented attack does not need to gain control of the victim system in order to be successful. As an extreme example, forcing a software firewall or Intrusion Detection/Prevention solution, running on the target host, to work more would cause an increased energy consumption without the need of breaking the system security or having access to legitimate transactions or software interfaces. In any case, the potential of energy-related attacks should not be underestimated. In fact, power consumption may be particularly relevant from a side-channel point of view in presence of an energy-proportional behavior of the target devices. However, that the adverse effect introduced by energy-related attacks may significantly depend on the current workload of the target systems. As an example, in presence of an already overloaded system, only a limited effect on power consumption may be experienced by introducing additional CPU workload. Finally, from the detectability perspective, an energy attack is characterized by a more subtle and stealthy nature, since its damaging effects can be perceived only over a relatively long period of time and, in the meanwhile, no specific anomalies such as tangible service degradation may be perceived on the victim hosts. Consequently, great attention should be given to such menaces, mainly in presence of large cloud infrastructures empowered by a large quantity of computing and storage resources.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. Commun. ACM **53**(4), 50–58 (2010). DOI 10.1145/1721654.1721672
2. Ascierto, R., Lawrence, A.: Will energy prices power US datacenter growth or short-circuit energy efficiency? URL: `https://451research.com/report-short?entityId=76124&referrer=marketing/` (2013)
3. B. Heller, S. Seetharaman, P. Mahadevan, Y. Yiakoumis, P. Sharma, S. Banerjee, N. McKeown, Elastictree: Saving energy in data center networks, in Proceedings of the 7th USENIX Symposium on Networked System Design and Implementation (NSDI), pages 249–264. ACM, 2010.:
4. Barroso, L.A., Holzle, U.: The case for energy-proportional computing. Computer **40**(12), 33–37 (2007)
5. Bash, C., Forman, G.: Cool Job Allocation: Measuring the Power Savings of Placing Jobs at Cooling-Efficient Locations in the Data Center. In: USENIX Annual Technical Conference, vol. 138, p. 140 (2007)
6. Bickford, J., Lagar-Cavilla, H.A., Varshavsky, A., Ganapathy, V., Iftode, L.: Security versus energy tradeoffs in host-based mobile malware detection. In: Proceedings of the 9th international conference on Mobile systems, applications, and services, pp. 225–238. ACM (2011)
7. Bjorling, M., Bonnet, P., Bouganim, L., Jónsson, B.P., et al.: uflip: Understanding the energy consumption of flash devices. IEEE Data Engineering Bulletin **33**(4), 48–54 (2010)
8. Bohrer, P., Elnozahy, E.N., Keller, T., Kistler, M., Lefurgy, C., McDowell, C., Rajamony, R.: The case for power management in web servers. In: Power aware computing, pp. 261–289. Springer (2002)
9. BONE project, WP 21 Topical Project Green Optical Networks: Report on year 1 and updated plan for activities, NoE , FP7-ICT-2007-1 216863 BONE project, Dec. 2009.:
10. CERT Coordination Center: Denial of service attacks. URL: `http://www.cert.org/tech_tips/denial_of_service.html` (2001)
11. Christensen, K., Nordman, B.: Reducing the energy consumption of networked devices. IEEE 802.3 tutorial (2005)
12. Christensen, K., Reviriego, P., Nordman, B., Bennett, M., Mostowfi, M., Maestro, J.A.: IEEE 802.3az: The Road to Energy Efficient Ethernet. Communications Magazine, IEEE **48**(11), 50–56 (2010)
13. Crosby, S.A., Wallach, D.S.: Denial of service via algorithmic complexity attacks. In: Proceedings of the 12th USENIX Security Symposium, pp. 29–44. Washington: USENIX (2003)
14. Dean, D., Stubblefield, A.: Using Client Puzzles to Protect TLS. In: USENIX Security Symposium, vol. 42 (2001)
15. Emerson Network Power: Energy logic: Reducing data center energy consumption by creating savings that cascade across systems. White paper, Emerson Electric Co, URL: `http://www.cisco.com/web/partners/downloads/765/other/Energy_Logic_Reducing_Data_Center_Energy_Consumption.pdf` (2009)

16. Fan, X., Weber, W.D., Barroso, L.A.: Power provisioning for a warehouse-sized computer. ACM SIGARCH Computer Architecture News **35**(2), 13–23 (2007)
17. Ficco, M., Rak, M.: Intrusion tolerant approach for denial of service attacks to web services. In: Data Compression, Communications and Processing (CCP), 2011 First International Conference on, pp. 285–292. IEEE (2011)
18. Fiore, U., Palmieri, F., Castiglione, A., De Santis, A.: Network anomaly detection with the restricted Boltzmann machine. Neurocomputing **In press** (2013). DOI 10.1016/j.neucom.2012.11.050. URL `http://dx.doi.org/10.1016/j.neucom.2012.11.050`
19. Hays, R.: Active/idle toggling with 0BASE-x for energy efficient Ethernet. Presentation to the IEEE **802** (2007)
20. Inc., M.T.: Calculating Memory System Power for DDR. URL: `http://download.micron.com/pdf/technotes/ddr/TN4603.pdf` (2001)
21. Intel Corporation: Intel Xeon Processor with 512KB L2 Cache at 1.80 GHz to 3 GHz Datasheet. URL: `http://download.intel.com/design/Xeon/datashts/29864206.pdf` (2003)
22. J. Koomey, Estimating Total Power Consumption by Servers in the U.S. and the World, February 2007.:
23. Janzen, J.: Calculating Memory System Power for {DDR}{SDRAM}. Designline **10**(2) (2001)
24. Jensen, M., Gruschka, N., Herkenhner, R.: A survey of attacks on web services. Computer Science - Research and Development **24**(4), 185–197 (2009). DOI 10.1007/s00450-009-0092-6. URL `http://dx.doi.org/10.1007/s00450-009-0092-6`
25. Jensen, M., Gruschka, N., Herkenhoner, R., Luttenberger, N.: SOA and Web Services: New Technologies, New Standards - New Attacks. In: Web Services, 2007. ECOWS '07. Fifth European Conference on, pp. 35–44 (2007). DOI 10.1109/ECOWS.2007.9
26. Jordi Torres, Green Computing: the next wave in computing, Ed. UPCommons, Technical University of Catalonia (UPC), February 2010.:
27. LLC, S.T.: Product manual Barracuda 7200.7. URL: `http://www.seagate.com/support/disc/manuals/ata/cuda7200pm.pdf` (2005)
28. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the Clouds: A Berkeley View of Cloud computing, Technical Report No. UCB/EECS-2009-28, University of California at Berkley, USA, Feb. 10, 2009.:
29. McAfee and ICF International: The Carbon Footprint of Email Spam Report. URL: `http://resources.mcafee.com/content/NACarbonFootprintSpam` (2009)
30. McDowell, M.: Understanding denial-of-service attacks. National Cyber Alert System, Cyber Security Tip ST04-015.2004 (2004)
31. Meisner, D., Gold, B.T., Wenisch, T.F.: PowerNap: eliminating server idle power. In: ACM Sigplan Notices, vol. 44/3, pp. 205–216. ACM (2009)
32. Mitchell-Jackson, J., Koomey, J., Nordman, B., Blazek, M.: Data center power requirements: measurements from Silicon Valley. Energy **28**(8), 837 – 850 (2003). DOI 10.1016/S0360-5442(03)00009-4. URL `http://dx.doi.org/10.1016/S0360-5442(03)00009-4`
33. Mohan, V., Bunker, T., Grupp, L., Gurumurthi, S., Stan, M.R., Swanson, S.: Modeling power consumption of nand flash memories using flashpower. IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS **32**(7), 1031 (2013)
34. Molaro, D., Payer, H., Le Moal, D.: Tempo: Disk drive power consumption characterization and modeling. In: ISCE '09. IEEE 13th International Symposium on Consumer Electronics, pp. 246–250 (2009)
35. Padmanabhuni, S., Singh, V., Senthil Kumar, K., Chatterjee, A.: Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach. In: Web Services, 2006. ICWS '06. International Conference on, pp. 577–584 (2006). DOI 10.1109/ICWS.2006.102
36. Palmieri, F., Fiore, U., Castiglione, A.: A distributed approach to network anomaly detection based on independent component analysis. Concurrency and Computation: Practice and Experience **In press** (2013). DOI 10.1002/cpe.3061. URL `http://dx.doi.org/10.1002/cpe.3061`
37. Palmieri, F., Fiore, U., Castiglione, A., De Santis, A.: On the detection of card-sharing traffic through wavelet analysis and Support Vector Machines. Applied Soft Computing **13**(1), 615 – 627 (2013). DOI 10.1016/j.asoc.2012.08.045. URL `http://dx.doi.org/10.1016/j.asoc.2012.08.045`
38. Palmieri, F., Ricciardi, S., Fiore, U.: Evaluating network-based DoS attacks under the energy consumption perspective: new security issues in the coming green ICT area. In: Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, pp. 374–379. IEEE (2011)
39. Park, J., Yoo, S., Lee, S., Park, C.: Power modeling of solid state disk for dynamic power management policy design in embedded systems. In: Software Technologies for Embedded and Ubiquitous Systems, pp. 24–35. Springer (2009)
40. Peter Kogge, The tops in flops, pp. 49-54, IEEE Spectrum, Feb. 2011.:
41. Reviriego, P., Hernández, J., Larrabeiti, D., Maestro, J.A.: Performance evaluation of energy efficient Ethernet. Communications Letters, IEEE **13**(9), 697–699 (2009)
42. Ricciardi, S., Careglio, D., Fiore, U., Palmieri, F., Santos-Boada, G., Solé-Pareta, J.: Analyzing local strategies for energy-efficient networking. In: Lecture Notes in Computer Science, vol. 6827, pp. 291–300. Springer (2011)
43. RSnake, J.K., Lee, R.: Slowloris HTTP DoS. URL: `http://ha.ckers.org/slowloris/` (June 2009)
44. Sohan, R., Rice, A., Moore, A.W., Mansley, K.: Characterizing 10 Gbps network interface energy consumption. In: Local Computer Networks (LCN), 2010 IEEE 35th Conference on, pp. 268–271. IEEE (2010)
45. St Arnaud, B.: ICT and Global Warming: Opportunities for Innovation and Economic Growth (2011)
46. Stewart, J.: HTTP DDoS Attack Mitigation Using Tarpitting. Securework.com, `http://www.secureworks.com/research/threats/ddos` (2007)
47. The Green Grid, The Green Grid Data Center Power Efficiency Metrics: PUE and DCiE, Technical Committee White Paper, 2008.:
48. W. Vereecken, W. Van Heddeghem, D. Colle, M. Pickavet, P. Demeester, Overall ICT footprint and green communication technologies, in Proc. of ISCCSP 2010, Limassol, Cyprus, Mar. 2010.:
49. West, W., Agu, E.: Experimental Evaluation of Energy-Based Denial-of Service Attacks in Wireless Networks. IJCSNS **7**(6), 222 (2007)
50. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications **1**(1), 7–18 (2010)