The Greenhouse Effect Attack

Pietro Marchetta, Valerio Persico, Antonio Pescapé
University of Naples "Federico II" (Italy)
{pietro.marchetta,valerio.persico,pescape}@unina.it

***Abstract*—A simple Denial-of-Service (DoS) attack is ICMP flooding, i.e. overwhelming the victim with ICMP Echo Request packets: by soliciting ICMP Echo Reply responses, the attacker aims at consuming CPU cycles as well as incoming and outgoing bandwidth of the victim. In this work, we present an evolution of this basic attack, we named *Greenhouse Effect Attack (GEA)*: the attacker issues exactly the same amount of ICMP Echo Request packets of the basic ICMP flooding attack but inducing the victim to handle double of the requests. This result is achieved transparently by making the routers of the victim's network effective yet unaware agents of the attacker.**

I. Introduction

In physics, the Greenhouse Effect is a process by which thermal radiation from a planetary surface is absorbed by atmospheric greenhouse gases, and is re-radiated in all directions[1]: due to this process, the sunlights hit the earth multiple times. In this paper, for the first time in literature, we introduce an attack – we called ***Greenhouse Effect Attack (GEA)*** – that has a very similar effect in a computer network: the attacker (the *sun*) issues a single packet (a *sunlight*) toward the victim device (the *earth*) while the solicited response is blocked along the reverse path by a network router (a *greenhouse gas*) causing the generation of another packet (*re-radiation*) sent back to the victim. GEA can be seen as an evolution of the ICMP flooding attack, one of the well known and simplest Denial-of-Service (DoS) attacks [1], [2], where the attacker overwhelms the victim with ICMP Echo Request packets triggering ICMP Echo Reply responses in order to steal CPU cycles as well as incoming and outgoing bandwidth of the victim. More specifically, GEA issues special ICMP Echo Request packets equipped with purposely crafted IP Timestamp option in order to both trigger ICMP Echo Reply packets from the victim and ICMP Parameter Problem messages from the routers encountered along the reverse path. In this work, we introduce GEA, the basic idea behind the attack, and we report some preliminary results on the applicability of GEA and its impact in a small and controlled testbed.

II. Background

GEA makes use of ICMP Echo Request packets equipped with the IP Timestamp option. We have recently observed the rise of a multitude of advanced Internet measurement techniques built on top of IP options and then they are gaining a momentum [3], [4], [5], [6], [7], [8]. The ICMP Echo Request packets equipped with the IP Timestamp option are crafted such that the ICMP Echo Reply message generated by the destination will trigger an ICMP Parameter Problem error message along the reverse path. In this way, by issuing a single packet, the attacker forced the victim to receive two packets, i.e. the ICMP Echo Request packet sent from the attacker as well as an ICMP Parameter Problem message sent by a network router of the reverse path. We briefly provide in this section the basic background required to understand the main idea behind the attack.

ICMP Parameter Problem. According to the standards (RFC792, RFC1812, RFC1122) when an incoming packet has to be discarded and no other ICMP message covers the detected problem, a router (host) must (should) send a notification to the source by using an ICMP Parameter Problem message. The ICMP type field is set to 12 while the code field can vary among 0 (invalid IP header), 1 (a required option is missing), and 2 (bad length). When code is 0, the pointer field identifies the octet where the error occurred: indeed, as usual in case of ICMP error messages, part of the original datagram which caused the error is carried back as payload.

IP Timestamp (TS) option. This IP option is defined along with three variants according to the flag field (RFC791). In this work, we adopt the TS option with the flag set to 0: with this variant, if enough space is available, each traversed device is requested to insert in the option data a 32-bit timestamp. If not enough space is available, the device is requested to increment by one the *overflow* field of the option header: this field counts the number of IP modules that could have not inserted timestamps due to lack of space. Since the overflow field consists of 4 bits and the maximum size of an IP option is 40 bytes, the overall number of IP modules that can be registered within a packet equipped with the TS option is 24 (9 timestamps in the option data plus 15 overflow increments). According to the standard, when the overflow field counts itself in overflow (i) the packet is discarded and (ii) an ICMP Parameter Problem message is sent back to source as a notification. GEA exploits this behavior to hit the destination with both ICMP Echo Request and ICMP Parameter Problem packets.

III. Greenhouse Effect Attack

GEA consists of two phases described in the following.

Preliminary phase. The goal of this phase is to estimate the number (R) of devices managing the TS option along the reverse path from the victim back to the attacker. To this end, the attacker first estimates the routers managing the option on both the forward and reverse path (O) and then those involved only along the forward path (F) in order to compute R as $O - F$. To estimate O, the attacker issues an ICMP Echo Request packet to the victim equipped with a TS option where (i) the option data is large enough to collect all the 9 timestamps along the path; (ii) the overflow field is set to 0; (iii) the pointer field is set to 5 pointing to the first available timestamp slot. Since the TS option of an incoming ICMP Echo Request packet is typically replicated inside the ICMP

[1] http://en.wikipedia.org/wiki/Greenhouse_effect July 2014.

Echo Reply packet, the attacker can estimate O by counting how many routers inserted timestamps and incremented the overflow field inside the TS option returned in the ICMP Echo Reply. Successively, to estimate F, the attacker issues a UDP packet to the victim (i) toward a high and presumably unused destination port and (ii) equipped with a TS option crafted as before. This new probe packet solicits an ICMP Port Unreachable response carrying in the payload the UDP packet that arrives at the victim, TS option included. The attacker estimates F by counting the routers that have managed the TS option contained in the payload of the collected ICMP Port Unreachable. In case of lack of reply for the UDP probe packet, the attacker may assume an equal number of routers managing the option on the forward and reverse path, thus coarsely estimating R as $\frac{O}{2}$.

Attacking phase. During this phase, the attacker exploits the knowledge gathered during the previous step to attack the victim. The goal of this phase is to trigger an ICMP Parameter Problem packet from a router of the reverse path to hit the victim with an additional packet. We discuss here a first basic possibility: the attacker sends to the victim a sequence of ICMP Echo Request packets equipped with a TS option crafted such that only $K \in]F, O[$ devices are allowed to manage the option before the overflow counts itself in overflow. In this way, (1.) all the F routers along the forward path can manage the option contained in the ICMP Echo Request message; (2.) the victim receives the ICMP Echo Request packet and generates the ICMP Echo Reply in which the received TS option is replicated; (3.) after $K - F$ routers managing the option along the reverse path, the overflow counts itself in overflow, the ICMP Echo Reply packet is discarded and an ICMP Parameter Problem is sent by the involved router back to the victim; (4.) the victim receives an ICMP Parameter Problem packet from a network router. Note that an interesting feature of this attack is the ability to convert unaware network routers into agents under control of the attacker.

IV. Preliminary results

Since GEA works as long as the targets (i) reply to ICMP Echo Request packet equipped with the TS option and (ii) replicate the TS option within the Echo Reply message, we performed a preliminary experimental campaign to evaluate the fraction of devices potentially vulnerable to this type of attack at the edge and within the core of the network by respectively targeting the *Alexa Top-5000*[2] sites and the IPs of the routers discovered by the *iPlane*[3] project. Results are summarized in Tab. I: preliminary results suggest that a significant fraction of hosts ($1,295$ over $5,000$, thus 25.9%) and routers ($7,507$ over $21,864$, thus 34.3%) is vulnerable to this type of attack. We also preliminary evaluated GEA in a controlled testbed. Two hosts, A and B, are connected through an intermediate router R: A is the attacker, B is the victim and R is the unaware ally of A in this attack. Fig. 1 reports the trains of ICMP Echo Request packets sent from A to B over time (top), the ICMP Echo Reply messages originated by B and sent back to A (middle) as well as the ICMP Parameter Problem messages triggered by the ICMP Echo Reply packets sent from R back to B (bottom). The figure clearly shows the ability of a remote attacker to induce a router to hit a victim with ICMP Parameter Problem packets.

[2]http://www.alexa.com/topsites

[3]http://iplane.cs.washington.edu/data/data.html

TABLE I. Targets vulnerable to GEA.

Dataset	Category	IPs	ASes	Vulnerable IPs
Alexa Top5000	End Hosts	5,000	1,519	1,295 (25.9%)
iPlane project	Routers	21,864	1,907	7,507 (34.3%)
Total		**26,864**	**3,089**	**8,802 (32.8%)**

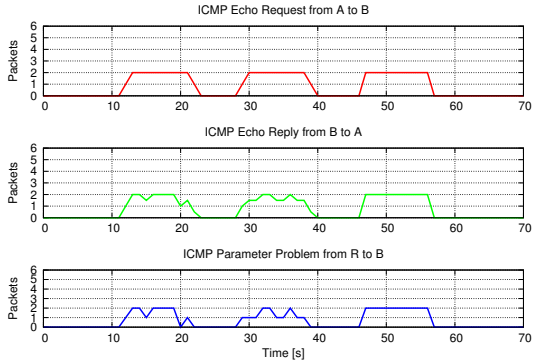

Fig. 1. Controlled testbed – A is the attacker, B is the victim, R is the router connecting A and B.

V. Conclusion

To stimulate a discussion and to shed light on the security aspects of the IP options, in this paper – for the first time in literature – we have proposed the Greenhouse Effect Attack. We have described the basic idea behind the attack and we have just shown and discussed very preliminary results on the applicability of the Greenhouse Effect Attack and its impact in a small and controlled testbed.

Acknowledgements. This work is partially funded by the MIUR projects: PLATINO ($PON01\_01007$), SMART HEALTH ($PON04a2\_C$), S^{2}MOVE ($PON04a3\_00058$) and SIRIO ($PON01\_02425$).

References

[1] C. Douligeris and A. Mitrokotsa, "Ddos attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004.

[2] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 3. IEEE, 2000, pp. 2275–2280.

[3] J. Sherry, E. Katz-Bassett, M. Pimenova, H. Madhyastha, T. Anderson, and A. Krishnamurthy, "Resolving IP aliases with prespecified timestamps," in *ACM SIGCOMM IMC*, 2010, pp. 172–178.

[4] P. Marchetta, V. Persico, and A. Pescapè, "Pythia: Yet another active probing technique for alias resolution," in *ACM CoNEXT*, 2013.

[5] P. Marchetta, A. Botta, E. Katz-Bassett, and A. Pescapé, "Dissecting Round Trip Time on the Slow Path Using a One-Packet Approach," in *PAM*, 2014.

[6] P. Marchetta, W. de Donato, and A. Pescapé, "Detecting Third-Party Addresses in Traceroute Traces with IP Timestamp Option," in *PAM*, 2013.

[7] P. Marchetta and A. Pescapè, "DRAGO: Detecting, Quantifying and Locating Hidden Routers in Traceroute IP Paths," in *IEEE Global Internet Symposium*, 2013.

[8] E. Katz-Bassett, H. Madhyastha, V. Adhikari, C. Scott, J. Sherry, P. Van Wesep, T. Anderson, and A. Krishnamurthy, "Reverse traceroute," in *USENIX NSDI*, vol. 10, 2010, pp. 219–234.