SHORT TERM SCIENTIFIC MISSION (STSM) SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127
STSM title: Denial-of-Service Vulnerability of Cloud-based Measurement and Remediation Systems
STSM start and end date: 18/07/2017 to 25/07/2017
Grantee name: Dr. Gábor Rétvári

PURPOSE OF THE STSM:

The main goal of the STSM was to study the feasibility of migrating the measurement and detection mechanisms used for locating regional failures into the cloud, with special emphasis on the resilience of the cloud-based remediation system to Denial-of-Service and Degradation-of-Service attacks against the multi-tenant data-center network infrastructure. The first goal of the STSM was to identify vulnerabilities in common hypervisor switch implementations, most importantly, Open vSwtich (OVS), concentrating on the attack surface offered by the shared flow caches in the fast path of OVS. The second goal was to design attack vectors to launch overload and poisoning attacks on the OVS flow caches, exploiting the theoretical complexity of order-independent transformations that are used by OVS to build these caches. Third, algorithms were to be considered to identify attackable patterns in OpenFlow flow tables. Finally, preliminary measurements were planned to assess the effect of DoS attacks on the switching performance provided by OVS.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

-
The following action points have been worked on during the STSM:

1. *Identified the Open vSwitch (OVS) flow cache infrastructure as an attack surface for tenant-initiated DoS attacks, whereas the attacker generates a specially crafted packet stream to overflow the flow caches.*
2. *Gave a clear description of the attack model (partially or wholly known OpenFlow pipeline) and discussed consequences of relaxing some of the assumptions in the model.*
3. *Defined two OVS flow-cache generation models: a minimalistic adversarial model in which OVS is allowed to solve NP-hard problems online or to know the future and the attacker can still overflow the flow caches, and a targeted model that identifies further weaknesses in the OVS cache-generation heuristics.*
4. *Fixed a precise model for the flow-cache lookup code in the fast-path of OVS.*
5. *Showed that the problem OVS needs to solve to generate an optimal flow cache for a given packet sequence is NP-hard.*
6. *Showed that it is also NP-hard to generate a "maximally malicious" packet sequence under the adversarial model.*
7. *Showed two heuristics for the attacker to craft malicious packet sequences and gave lower bounds for the number of the resultant cache entries.*
8. *Discussed worst-case flow tables that allow tens of thousands of flow-cache entries to be spawned by just a couple of hundred specially crafted packets.*

Funded by the Horizon 2020 Framework Programme
of the European Union

9. *Carried out a number of measurements that show real promise for the attack sequence: for the “hole-punched” pipeline pattern it is easy to generate a packet sequence that causes orders of magnitude performance loss in OVS due to flow-cache exhaustion.*

DESCRIPTION OF THE MAIN RESULTS OBTAINED

The main results for the STSM are as follows:

1. *A formal attack model for cache overflow attacks in multi-tenant clouds against the hypervisor switch.*
2. *Two OVS models, one with formal description, that serve as adversaries for the attacker.*
3. *Identification of the computational complexity of the underlying mathematical problems (on the side of OVS and the attacker).*
4. *Definition and partial implementation of the heuristics for malicious packet sequence generation.*
5. *Parsing, converting, and setting up the “Standford OpenFlow rule set” as published by the Mini-Stanford project, which will serve as real-world flow-tables to test our heuristics.*
6. *Initial measurements with our malicious packet sequences.*
7. *An initial paper draft that summarizes the results of the work carried out so far.*

FUTURE COLLABORATIONS (if applicable)

The current plan is to develop the initial results obtained during the STSM into a research paper that comprehensibly identifies the attack surfaces in OVS flow caches and gives methodology to exploit these. For the collaboration, we have Dr. Dimitrios Pezaros (senior) and Dr. Levente Csikor (post-doc) from the side of the University of Glasgow, and Attila Kőrösi (research fellow) and Dr. Gábor Rétvári (senior) from the Budapest University of Technology and Economy working towards that goal and we would like to involve at least one further cloud-expert. We have also discussed contributing a book chapter to the RECODIS book.