Virtualization towards stealth analysis

2021-03415 - PhD Position F/M TANSIV-Tx: Time-Accurate Network Simulation Interconnecting VMs with Hardware Virtualization towards stealth analysis

Type de contrat : CDD
Niveau de diplôme exigé : Bac + 5 ou équivalent
Autre diplôme apprécié : Master degree in (distributed) systems and/or Cloud computing
Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria Rennes - Bretagne Atlantique Centre is one of Inria’s eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institutes, etc.

Contexte et atouts du poste

This project will be conducted within the IRISA Myriads team which is working on the design of innovative infrastructures and middleware for future fog computing platforms.

Mission confiée

Malware analysts often rely on sandboxes to study malware and their interaction with the environment. In this context, the malware payload is executed in a virtual machine (VM) on top of a custom hypervisor. Various analysis tools can then safely analyze the malware execution from outside of the VM.

Attackers have however developed different evasion techniques; to detect sandboxes and hide their malicious behavior [1]. A class of evasion techniques relies on timing analysis. For instance, a malware can compare several time references to detect discrepancies that can be caused by the analysis environment. To the best of our knowledge, the currently known evasion techniques solely rely on comparing time references that are local to the VM (e.g., execution loops’ timings). Some sandboxes ensure that all local time references remain consistent to achieve stealthiness with that regard [2, 3, 4].

The TANSIV project focuses on making sandboxes stealth with respect to timing-analysis-based evasion techniques using network interactions as part of their time references. Such evasions are easy enough to implement to be considered as real threats from the analyst perspective. In the general case, a malicious targeting a specific victim could compare its network environment with a fingerprint embedding the knowledge of the victim environment, including the local network size, performance, and geo-location. Similarly, with no prior knowledge of the victim environment, the evasion decision could be taken based on the performance of the communication to its Command and Control (C&C) servers as the network latency must follow approximately a distribution known in advance.

To add timing-based network-fingerprinting resistance to sandboxes, the TANSIV approach consists in interconnecting sandboxes and the network end-points of its environment with a scalable, performance-accurate, discrete-event network simulator. TANSIV decouples the wall-clock execution time from the time perceived inside the sandbox and its network environment, as the simulator coordinates the progression of time on all network end-points and when communications are delivered to their target end-points.

In a first step, we have implemented a prototype of TANSIV with the Qemu PC emulator and the SimGrid simulator [5]. The emulation mode of Qemu especially allows TANSIV to precisely control the progression of time in the VM. However, although some sandboxes are based on Qemu [6, 7], the emulation mode has 3 major drawbacks:
- wall-clock execution speed (as perceived by the human analyst) is much slower than in a real environment;
- emulation mode is easily detected from inside the VM (e.g. it is not cycle-accurate) and is a clear sign of a sandboxed execution;
- many sandboxes rather use hardware-assisted virtualization [8, 9], both for better speed and stealthiness.

The goal of the TANSIV project is twofold. First, we should extend TANSIV to hardware-assisted virtualization, for which we must design solutions to precisely control the progression of time. Second, the added precise yet decoupled control of time may interfere with the time-related testing of sandboxes. Therefore, the approach must be tailored to minimize the required changes on the sandboxes tools.

The different approaches will be implemented in open-source sandboxes and experimentally evaluated, taking into account the achievable execution speed, the portability to new sandboxes, as well as the analysis power gained for analysts.

Bibliography


Informations générales

- Thème/Domaine : Systèmes distribués et interconnexions
- Système & réseaux (BAP E)
- Ville : Rennes
- Centre Inria : CRI Rennes - Bretagne Atlantique
- Date de prise de fonction souhaitée : 2021-10-01
- Durée de contrat : 3 ans
- Date limite pour postuler : 2021-05-14

Contacts

- Equipe Inria : MYRIADS (DGG-S)
- Directeur de thèse : Rilling Louis / louis.rilling@irisa.fr

A propos d’Inria

Inria est l’institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2 600 personnes. Ses 200 équipes-projets, en général communes avec des partenaires académiques, impliquent plus de 3500 scientifiques pour relever les défis du numérique, souvent à l’interface d’autres disciplines. L’institut a fait appel à de nombreux talents dans plus d’une quinzaine de métiers différents. 900 personnels d’appui à la recherche et à l’innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 180 start-up. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

Consignes pour postuler

Please submit online: your resume, cover letter and letters of recommendation eventually

For more information, please contact matthieu.simoner@inria.fr or martin.quinson@irisa.fr

Sécurité défense :

Ce poste est susceptible d’être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n° 2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L’autorisation d’accès à une zone est délivrée par le chef d’établissement, après avis ministériel favorable, tel que défini dans l’arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l’annulation du recrutement.

Politique de recrutement :

Dans le cadre et à l’initiative de son projet Aggreg, Inria a travaillé avec de nombreuses entreprises et à accompagné la création de plus de 180 start-up. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

Atention : Les candidatures doivent être déposées en ligne sur le site Inria.
Principales activités

The goal of the TANSIVTx project is twofold. First, we should extend TANSIV to hardware-assisted virtualization, for which we must design solutions to precisely control the progression of time. Second, the added precise yet decoupled control of time may interfere with the time-related tooling of sandboxes. Therefore, the approach must be tailored to minimize the required changes on the sandbox tools.

The different approaches will be implemented in open-source sandboxes and experimentally evaluated, taking into account the achievable execution speed, the portability to new sandboxes, as well as the analysis power gained for analysts.

Compétences

Required skills:
Networks and VMs; System programming on Linux.

Appreciated but not mandated skills:
Deep understanding of OSes; x86 assembly; Programming in C; Programming in Rust.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

Inria :

monthly gross salary amounting to 1982 euros for the first and second years and 2085 euros for the third year.