Digital twin for security evaluation using an attack agent

Manuel Poisson, Sébastien Kilian, Valérie Viet Triem Tong, Jean-François Lalande, Gilles Guette, Frédéric Ghihéry, Damien Crémilleux

▶ **To cite this version:**

Manuel Poisson, Sébastien Kilian, Valérie Viet Triem Tong, Jean-François Lalande, Gilles Guette, et al.. Digital twin for security evaluation using an attack agent. USENIX 2024 - 33rd USENIX Security Symposium, Aug 2024, Philadelphia, United States. , pp.1-1, 2024. hal-04708718

HAL Id: hal-04708718
https://inria.hal.science/hal-04708718v1

Submitted on 25 Sep 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Digital twin for security evaluation using an attack agent

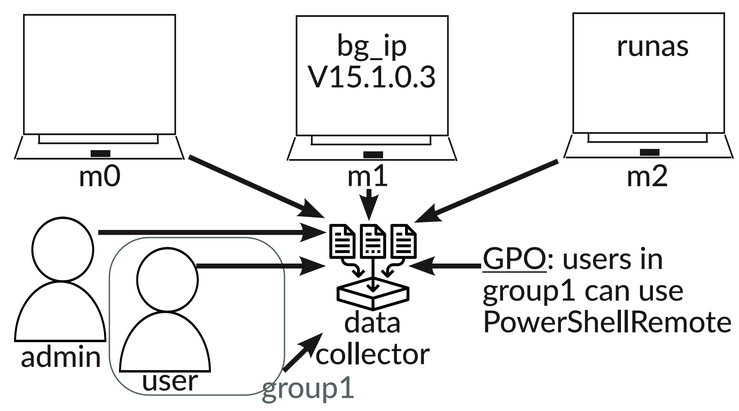
Manuel POISSON, Sébastien KILIAN
manuel.poisson@irisa.fr sebastien.kilian@centralesupelec.fr
V. VIET TRIEM TONG, J-F LALANDE, G. GUETTE, F. GUIHÉRY, D. CRÉMILLEUX

Discover attack paths in an information system without affecting the services in production.

Collect data in an information system (IS) in production

✓ Dynamic data collection

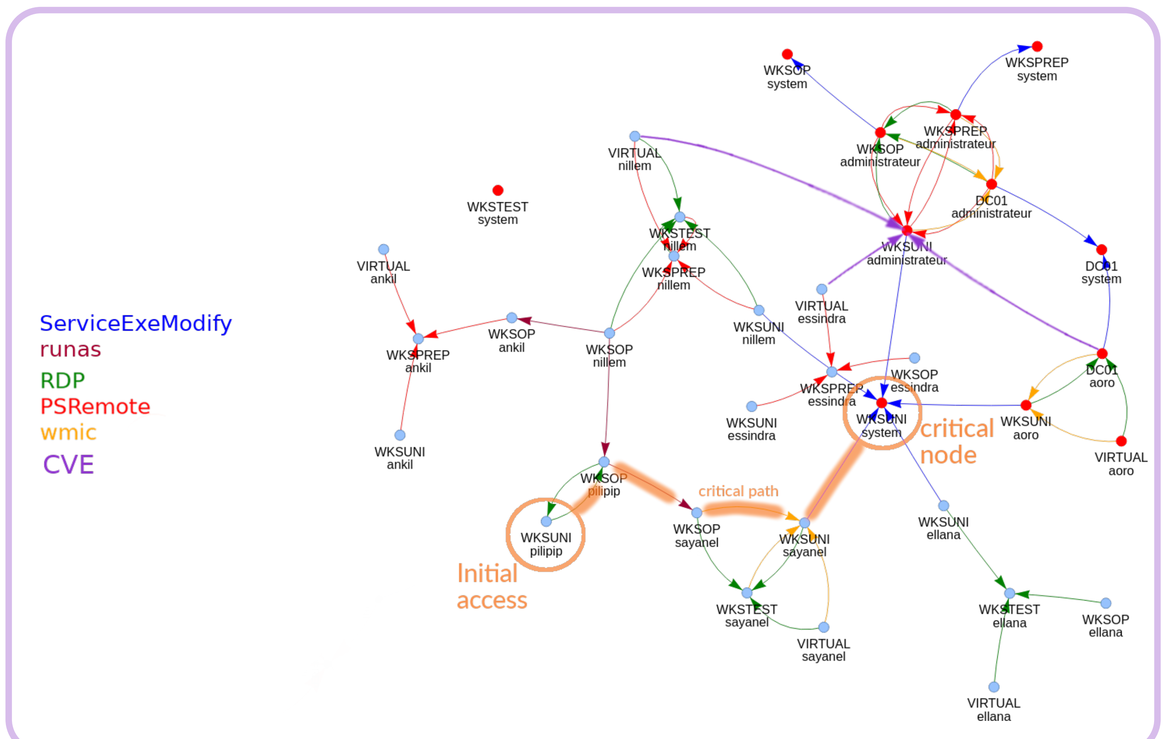
- Machines, users and groups
- GPO (in Active Directory): define settings and permissions for groups in the IS
- Living of the Land (LotL): legitimate tools abused by attackers
- Software and their version



Model all potential attackers' actions

✓ Organize data and model potential attack paths [1]

- Discover attack positions and lateral/vertical movements
- Highlight attack path in a graph



Generate a digital Twin

Virtual topology deployment

Generate and provision virtual machines in a virtual network

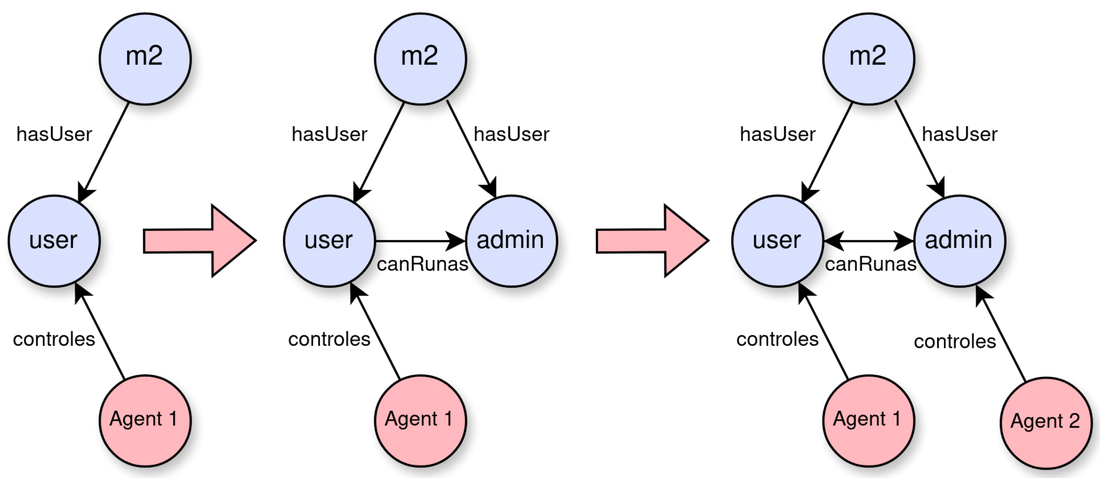
✓ URSID [2] https://gitlab.inria.fr/pirat-public/ursid

✓ M&NTIS https://mantis-platform.io

Discover attacker's perception of IS

Attack agent

- Automated exploits are parameters of the system
- ✓ Attack agent's knowledge is represented as a knowledge graph [3]
- Real exploits reveal the true exploitability of the information system



Assess overall security

Assess and improve the security level

- Evaluate attack detection: stealthiness of attack paths
- Prevent known attack paths: propose remediations
- Remediations can be tested on the digital twin

Replicate systems with high fidelity

- Security features are replicated
- Evaluation is done on a digital twin
- Usable attack paths are highlighted by the attack agent

[1] M. Poisson et al. Unveiling stealth attack paths in Windows Environments using AWARE. CSNet 2023 - 7th Cyber Security in Networking Conference, IEEE ComSoc, 2023
[2] P-V Besson et al. URSID: Automatically Refining a Single Attack Scenario into Multiple Cyber Range Architectures. FPS 2023
[3] A. Berady et al. PWNJUTSU: A Dataset and a Semantics-Driven Approach to Retrace Attack Campaigns - IEEE TNSM 2022
This work has benefited from a government grant managed by the National Research Agency under France 2030 with reference "ANR-22-PECY-0007"

CentraleSupélec/Amossys/CNRS/Univ. Rennes
IRISA Rennes, France