New Emergency Management in a Resilience Era Facing Health, Climate and Energy Challenges

6th to 10th December 2021

9th December 2021, 16:00-16:25

Kéren A. Saint-Hilaire, Joaquin Garcia-Alfaro – Institut Polytechnique de Paris, Télécom SudParis

Frédéric Cuppens,Nora Cuppens – Polytechnique de Montréal

Ontology-based Attack Graph Enrichment

- Motivation
- Background
- Our Approach
- Implementation
- Related Work
- Conclusion

Motivation

- Attack Graph
  - Graphical representation of adversarial paths towards a goal
  - Used by cybersecurity experts to make decisions (e.g., decide
  - remediations & recovery plans)
- Attack Graph Enrichment
  - Network & vulnerability information for graph generation
  - Constant changes in networks & vulnerabilities
  - Graphs must be updated according to those changes
  - Real-time monitoring is needed to confirm successful attacks
    - Mapping alerts to move from proactive to reactive graphs

Background

- **Definition 1 (Graph)** A Graph is a set V of vertices, and a set E of unordered and ordered pairs of vertices, denoted by G(V; E). An unordered pair of vertices is an edge, while an ordered pair is an arc.

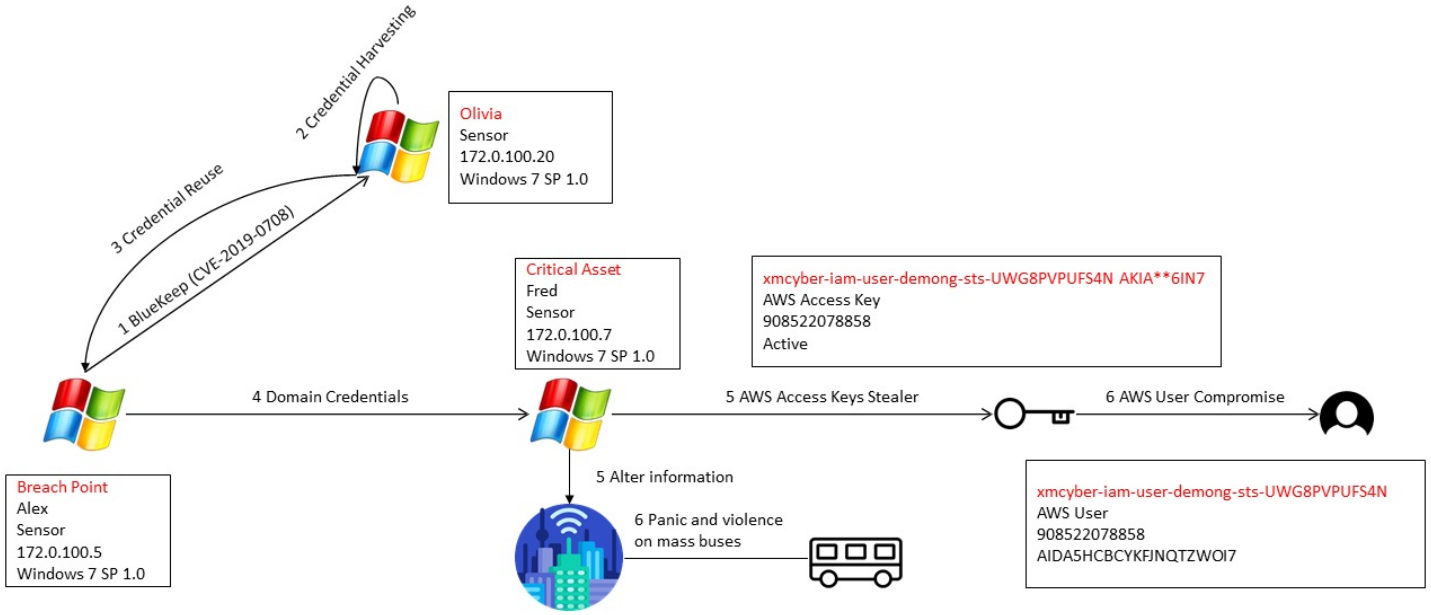
- **Definition 2 (Directed Graph)** A directed graph G(V; A) consists of a non-empty set V of vertices and a set E of arcs formed by pairs of elements of V.

- **Definition 3 (AND-OR Graph)** An AND-OR graph is a directed graph where each vertex v is either an OR or an AND. A vertex represents a sub-objective and according to its type (AND or OR), it requires either the conjunction or disjunction of its children, to be fulfilled. A root node n of an AND-OR graph can be called a precondition as it does not require any other node n to be fulfilled.

- According to Definitions 1, 2, and 3, logical attack graphs are based on AND-OR logical directed graphs. The nodes are logical facts describing adversaries' actions or the pre-requisites to carry them out. The edges correspond to the dependency relations between the nodes.

Our approach

- Use case scenario



Our approach

- Generation of the Attack Graph

$execCode(h, a) \rightarrow canAccesHost(h)$

$execCode(h, a) \wedge hasCredentialsOnMemory(h, u) \rightarrow harvestCredentials(h, u)$

- Monitoring the Information System

$\forall n \in N : (vulExists(h, x, y, z) \wedge networkServiceInfo(h, s, p, a, u) \rightarrow F_1$

- Vulnerabilities and Ontologies
  - An ontology is a formal description of a field of knowledge and is represented by descriptive logic.

CVE-ID	Product	Type	Action	Impact
CVE-2002-0392	Apache	remote	Code Execution	Privilege Escalation

Our approach

- Enrichment of Attack Graphs

Algorithm 1: Enrichment of a proactive attack graph based on a vulnerability ontology and monitored system information

h_1: A threat exists on a vulnerable component of the monitored system.
h_2: Post-conditions of the exploited vulnerability are found in the ontology.
P_1: Add new path on the attack graph.

$$(h_1 \wedge h_2) \rightarrow P_1$$

Algorithm 2: Inference rule for mass on buses scenario

v_1: Node corresponds to reboot of a machine.
v_2: Node corresponds to mass on buses.
The child or destination of an arc $(v_1; v_2) \in A; v_1 \in V; v_2 \in V$, is v_2.

$$(v_1 \wedge v_2) \rightarrow (v_1; v_2)$$

The inference rule is:

$$\frac{v_1 \quad v_2}{(v_1; v_2)} \; \mathrm{r}$$

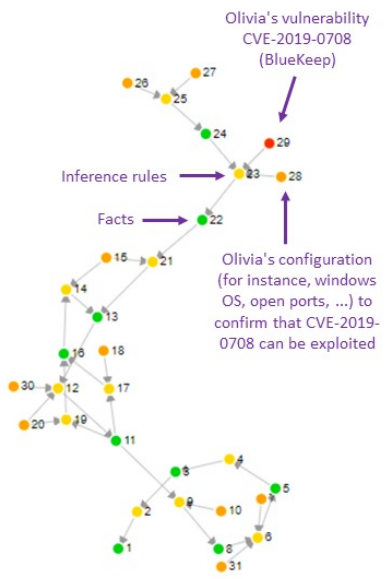
Implementation

- Setup
  - MulVAL
    - A reasoning engine based on logical programming, to generate a logic-based attack graph.
  - Ontology
    - A practical implementation of NIST's Vulnerability Description Ontology
  - Prelude+ELK
    - A SIEM (Security Information and Event Management) tool that collects & centralizes the security information of an organization.
    - Use of an extended version of Prelude-OSS with ELK (Elasticsearch, Logstash, and Kibana).
  - Web Interface
    - Development of a web interface for the attack graph visualization

Implementation

- Results

Now, from proactive to reactive graphs ...

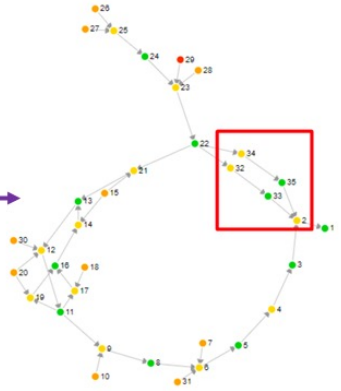


Logical Proactive Attack Graph

+ LOGS
(from city devices, using rsyslog daemon installed at their premises)

+ ALERTS
(installation of PRELUDE-ELK + sensors such as Suricata)

+ NIST's VDO
(Vulnerability Description Ontology)



Logical Reactive Attack Graph

Related Work

Attack Graph Generation Approaches

Year	Authors	Description	Downside
2009	Roschke et al.	An approach of vulnerability information extraction for attack graph generation using MulVAL and SIEM alerts in terms of data fusion and correlation.	The initial state of the network system is not taken into account for the attack graph generation.
2012	Ghosh and Ghosh	A planning-based approach for attack graph generation and analysis.	They don't propose an attack graph enrichment process based on state change of the network.
2019	Shirazi et al.	An approach for modeling attack-graph generation and analysis problems as a planning problem.	They don't propose an attack graph enrichment process based on state change of the network.

Related Work

Ontology and Attack Graph Generation

Year	Authors	Description	Downside
2017	Falodiya et al.	The work proposes an algorithmic solution to traverse an exploit dependency attack graph and add the extracted data into the ontology.	They are not enriching the attack graph based on ontology.
2018	Lee et al.	An approach for converting an attack graph into an ontology.	They are not enriching the attack graph based on ontology.
2019	Wu et al.	An attack graph generation approach based on the inference ability of cybersecurity ontologies.	The attack graph is updated only when the security expert update ontologies.

Conclusion

- Simplification of the inference process
- Consideration of network system state update in real-time
- Successful update of the initial graph predictions into the enriched graph based on attack evidence and semantic augmentation

References

- Xinming Ou, Sudhakar Govindavajhala, and Andrew W. Appel. Mulval: A logic-based network security analyzer. In USENIX Security Symposium, 2005.
- Songyang Wu, Yong Zhang, and Xiao Chen. Security Assessment of Dynamic Networks with an Approach of Integrating Semantic Reasoning and Attack Graphs. 2018 IEEE 4th International Conference on Computer and Communications (ICCC), pages 1166-1174, 2018.
- Hossein Shirazi, Bruhadeshwar Bezawada, Indrakshi Ray, and Charles Anderson. Adversarial sampling attacks against phishing detection. In IFIP Annual Conference on Data and Applications Security and Privacy, pages 83-101. Springer, 2019.
- Sebastian Roschke, Feng Cheng, Robert Schuppenies, and Christoph Meinel. Towards unifying vulnerability information for attack graph construction. Lecture Notes in Computer Science (including subseries Lecture Notes in Articial Intelligence and Lecture Notes in Bioinformatics), 5735 LNCS:218-233, 2009.
- Jooyoung Lee, Daesung Moon, Ikkyun Kim, and Youngseok Lee. A semantic approach to improving machine readability of a large-scale attack graph. Journal of Supercomputing, 75(6):3028-3045, 2019.
- Nirnay Ghosh and Soumya Ghosh. A planner-based approach to generate and analyze minimal attack graph. Applied Intelligence, 36(2):369-390, 2012.
- Komal Falodiya and Manik Lal Das. Security Vulnerability Analysis using Ontology-based Attack Graphs. 2017 14th IEEE India Council International Conference, INDICON 2017, pages 1-5, 2018.
- Harold Booth and Christopher Turner. Vulnerability description ontology (VDO): a framework for characterizing vulnerabilities. Technical report, National Institute of Standards and Technology, 2016.