EU MITRE ATT&CK® Community Workshops

Creating Attack Graphs for Adversary Emulation, Simulation and Purple Teaming in Industrial Control Systems (ICS) Environments

Jan Hoff

May 27, 2021

Agenda

1. Whoami, Motivation and Background
2. Approach
3. Solution and Graph Design
4. Evaluation
5. Summary and Future Work
6. Q & A

Whoami, Motivation and Background

whoami

- Currently: Red Teaming and Penetration Testing
- Previously: Forensics and Incident Response, ...
- 10+ years of experience with infosec for critical infrastructures

- I ❤️ energy – mainly 🔌 on all ⚡ levels
- "🐿️ Rodents [still] cause more power outages than 😈 hackers"

Disclaimer

This presentation is a result from personal research and interest.
It is not related to or explicitly endorsed by my employer.

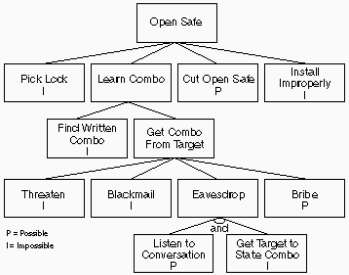
Motivation

Ukraine Power Outages 2015 & 2016

Petrochemical Plant TRISIS Incident 2017

Research Question

“Is it possible – and if yes to what extent – to algorithmically **generate attack graphs** that can be used for **practical adversary behavior execution** in ICS environments and can the process be supported by a **corresponding application**?”



Attack Tree
(Schneier, Dr. Dobb’s Journal, 1999)

Foundation and Existing Work

ADTree
(Kordy et. al)

ATT&CK Framework
(Strom et. al / MITRE)

1. Attack Graphs

   (Schneier, Kordy, LeMay, Ekstedt and many more)

   - Attacks can be modeled intuitively with graphs/trees
   - Focus mainly on assets less on the actions
   - Used for modeling defenses and critical paths
   - Automated generation has been shown to be possible

2. Ontologies, Kill Chains and MITRE ATT&CK

   (Strom, Applebaum, Hutchins, Pols and many more)

   - Common language to describe attacks/actions
   - Attacks follow common sequences/patterns
   - Large repository about information on attacks and behavior (TTP)
   - Specific ICS related repositories available

Approach

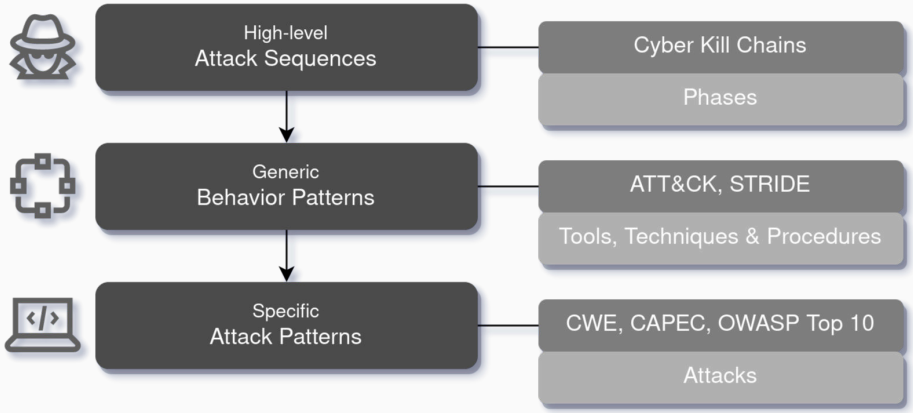
Use Cases

Exercises and Adversary Behavior Execution

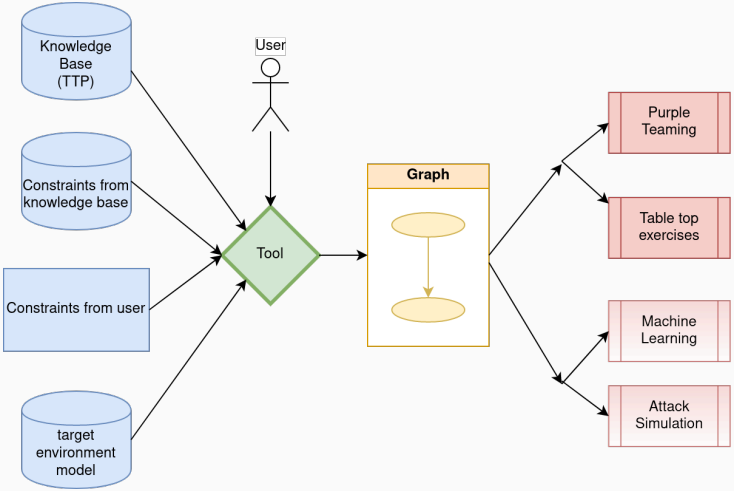
1. Exercises
   - 1.1 Red and Purple Teaming
   - 1.2 Table-Top Exercises
2. Automated execution
   - 2.1 Simulation
   - 2.2 Machine Learning

Classification of Attack Models

Which **level of detail required** for designing attack graphs for adversary behavior execution?

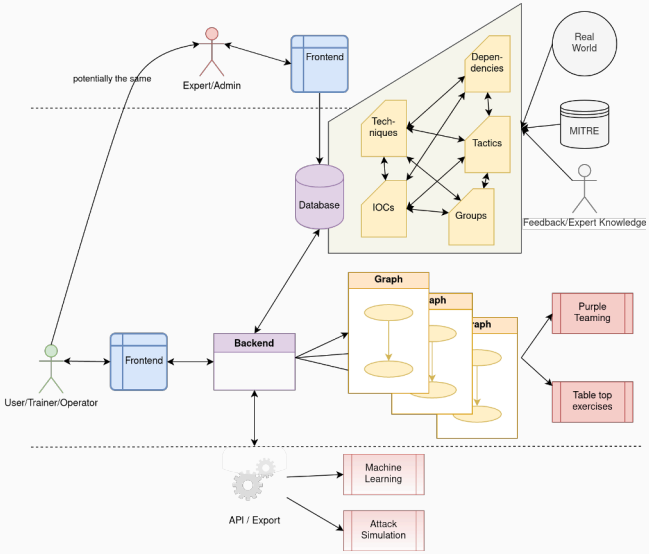


Use Cases and Input/Output

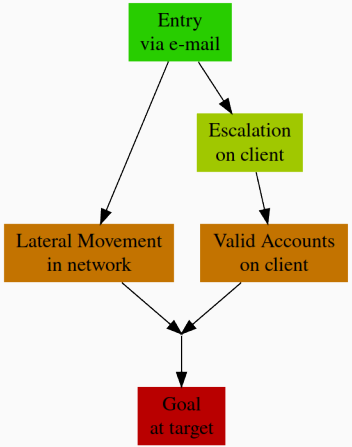


Solution and Graph Design

System design

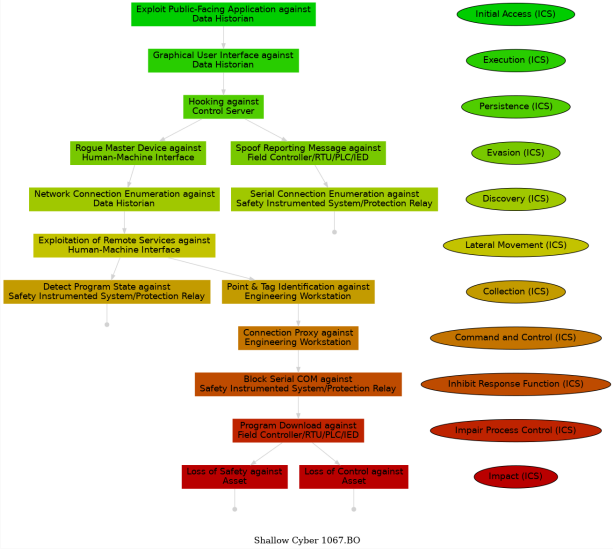


Graph Design



1. Graphs
   - Set of nodes and edges describing the adversary profile
   - Focus on emulation/simulation of attack Techniques
   - Sequential along MITRE Tactics (the “what”)
2. Nodes
   - Instantiated Techniques as individual hacking steps (the “how”)
   - Associated with targets and indicators
3. Edges
   - Technique’s results and status

Example Generated Graph



Example Generated Graph

Live Demo

Evaluation

Evaluation

Evaluation Approach

- **13 interviews** with experts
- Guided **1-1,5h interview** and live demonstration
- **12 Questions** regarding expert's background, experience with attack graphs and adversary behavior execution, feedback on the prototype as well as potential future use cases
- Author's **critical reflection** of thesis' results

Questionnaire

Research question:
Is it possible – and if yes to what extent – to algorithmically generate attack graphs that can be used for practical adversary behavior execution in ICS environments and can the process be supported by a corresponding application?

General context questions

1. Which organization are you related to (corporate/academia/government/other)?
2. In how far are you in contact with ICS systems?
3. How far did you have contact with adversary **emulation** or adversary **simulation**?
4. How have you used the ATT&CK framework previously?

Adversary behavior execution (ICS specific, else general enterprise context)

5. Are you or your organization already doing Purple Teaming or adversary emulation? If not are, you considering? What would be goals of adversary emulation in your opinion or experience?
6. If you have contact with ICS environment, have you considered active exercises like Purple Teaming in your ICS environments? If not, why?
7. How have you used attack graphs in the past? If so, did you model adversary behavior (TTP) in that context?
8. What requirements (functional and non-functional) would you see for a tool regarding graph generation for adversary behaviour modeling with attack graphs?

Graph walk-through (Interviewee is guided through the application)

9. Given the following graphs, would you consider those a valid attack chains in ICS (considering a generic ICS landscape)?

Application walk-through (Interviewee is guided through the application)

10. How far is the protype use case, application flow and the context clear?
11. Is there any room for improvement, when it comes the application and workflow?

Application in the context

12. Where else do you see potential use cases for such a tool in your area of work?

Selected Evaluation Results

- Purple Teaming and Attack Graphs
  - Adversary behavior execution can be used to train defenders
  - Maturity in industrial organizations often does not allow for Purple Teaming or active adversary behavior execution yet
  - Existing attack graph approaches are considered too complex for real-world use
- Prototype and Walkthrough
  - Real world and vetted dataset results in valid attacks and generation algorithm creates syntactically correct graphs
  - Wide range of expectations (from management level to low-level technical level)
  - Workflow and exercise lifecycle supports activities
- Selected Additional Use Cases
  - Defense modeling to design countermeasures to attack chains
  - Guided graph generation to create graphs starting from a node or subgraph
  - Risk and threat modeling to validate and assess security posture

Summary and Future Work

Summary and Future Work

- Conclusion
  - Automated attack graph generation for adversary behavior execution is possible
  - Experts confirm viability of approach and prototype
- Future work
  - Detailed node generation (IOC level) and integration with formal models/languages
  - Machine learning use cases and Bayesian networks
  - Defender profile mapping with threat and defense modeling

Q & A

Further Reading

Get the full text and source of the application from

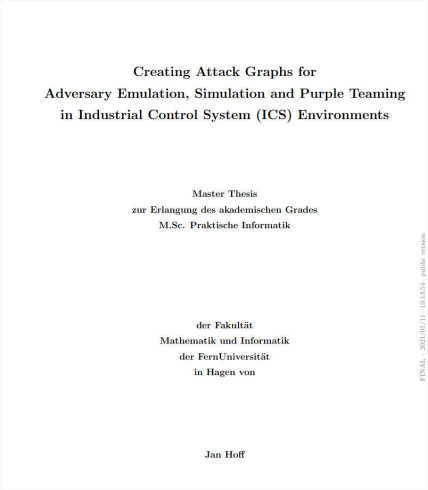
📖 https://www.pull-the-plug.net/thesis/

Get in touch at

🌐 https://www.linkedin.com/in/jahoff/

🐦 @mehgrmlhmpf

✉️ thesis@pull-the-plug.net



Creating Attack Graphs for
Adversary Emulation, Simulation and Purple Teaming
in Industrial Control System (ICS) Environments

Master Thesis
zur Erlangung des akademischen Grades
M.Sc. Praktische Informatik

der Fakultät
Mathematik und Informatik
der FernUniversität
in Hagen von

Jan Hoff

FINAL - 2021/01/11 - 10:13:54 - public version

Thank you

References and Credits

1. Latex beamer template: `https://github.com/matze/mtheme`
2. ”Ukraine” power lines: `https://unsplash.com/`
3. Petro Rabigh plant: `https://www.meed.com/petro-rabigh-[...]-owners`
4. All other photos: `https://unsplash.com/`
5. Further references and a complete bibliography can be found at: `https://www.pull-the-plug.net/thesis/`

Thanks to my supervisors and all interview participants for providing guidance and input.