EU MITRE ATT&CK® Community Workshops

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

Jan Hoff

June 2, 2021

– TLP:WHITE –

Agenda

1. Whoami, Motivation and Background
2. Approach
3. Solution and Graph Design
4. Summary and Future Work

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.
This talk is not related to or explicitly endorsed by my employer.

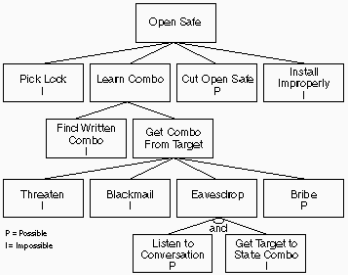
Motivation

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

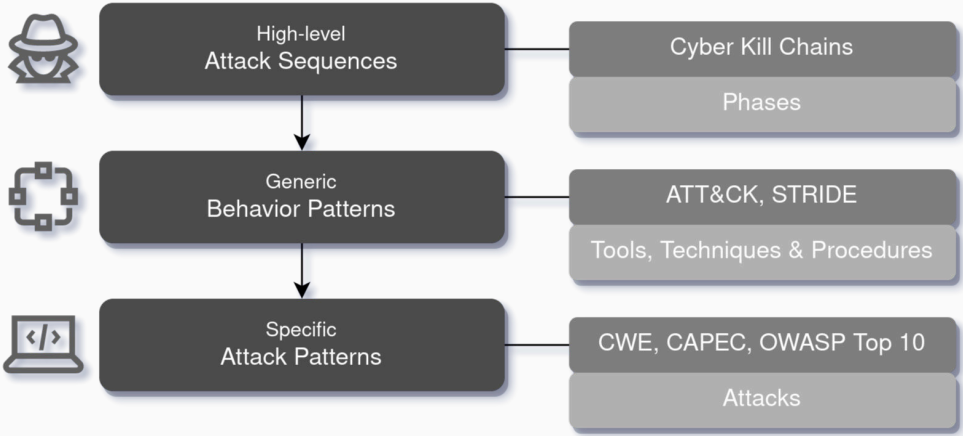
Use Cases

Exercises and Adversary Behavior Execution

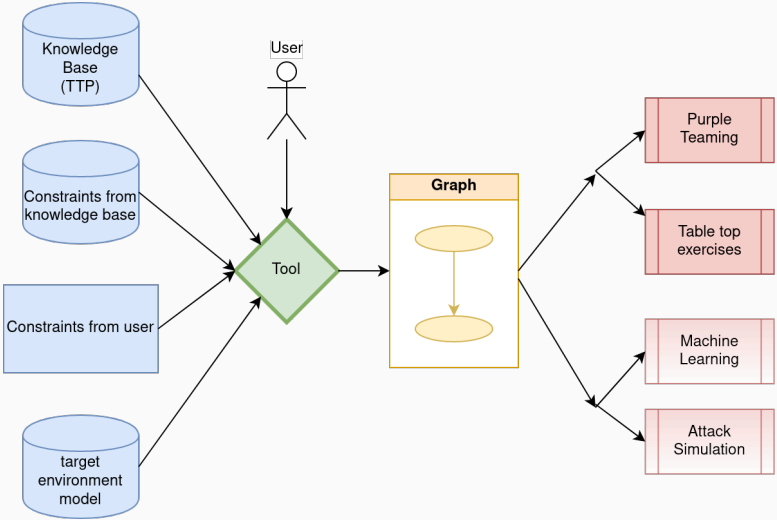
1. Exercises
   - Red and Purple Teaming
   - Table-Top Exercises
2. Automated execution
   - Simulation
   - Machine Learning

Classification of Attack Models

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

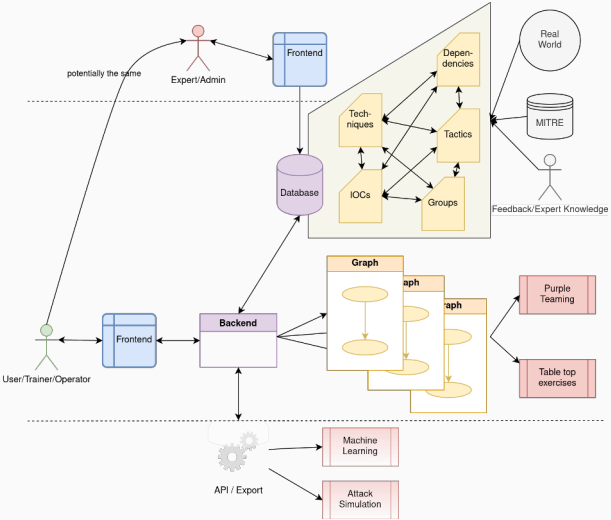


Use Cases and Input/Output

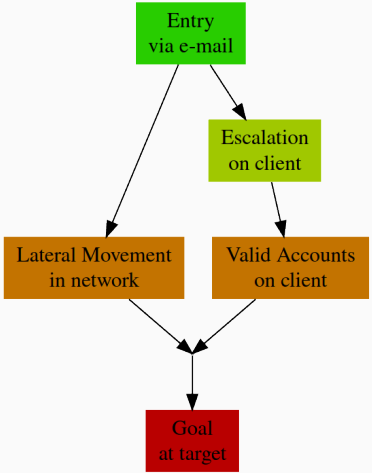


Solution and Graph Design

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

Shallow Cyber 1067.BO

Example Generated Graph

🤖 Live Demo?

🤓 Just deploy it on your own!

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

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

Further Reading

Get the full text and source of the application from

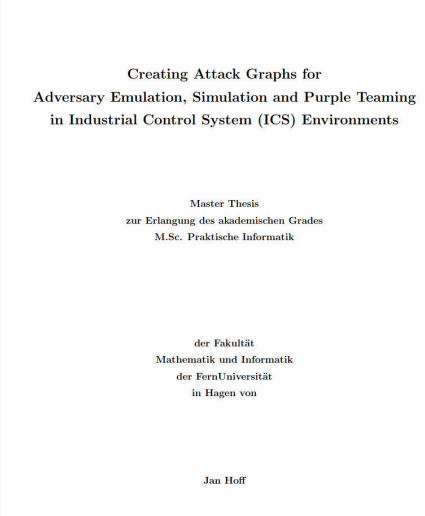
📖 https://www.pull-the-plug.net/thesis/

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

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.