



# OWASP Stammtisch Hannover

Angriffsgraphen für Threat Modeling und Adversary Emulation

---

Jan Hoff

April 22, 2021

# Agenda

1. Whoami and Motivation
2. Background
3. System and Graph Design
4. Summary
5. Q&A and Discussion



## **Whoami and Motivation**

---

# whoami

- Currently: Senior Expert Penetration Testing
- Previously: Senior Expert Forensics
- 10 years of experience in infosec in critical infrastructures



# whoami

- Currently: Senior Expert Penetration Testing
- Previously: Senior Expert Forensics
- 10 years of experience in infosec in critical infrastructures
- I like energy – mainly electricity on all voltage levels
- "Squirrels are more likely to cause power outages than hackers"



# whoami

- Currently: Senior Expert Penetration Testing
- Previously: Senior Expert Forensics
- 10 years of experience in infosec in critical infrastructures
- I like energy – mainly electricity on all voltage levels
- "Squirrels are more likely to cause power outages than hackers"
- I am not an engineer or developer



- Currently: Senior Expert Penetration Testing
- Previously: Senior Expert Forensics
- 10 years of experience in infosec in critical infrastructures
- I like energy – mainly electricity on all voltage levels
- "Squirrels are more likely to cause power outages than hackers"
- I am not an engineer or developer



## Disclaimer:

This presentation is a result from personal research and interest.  
It is in no way related to or endorsed by my employer.  
Each topic of this talk deserves a multi-hour deep dive.

# Motivation



Ukraine Power Outages  
2015 & 2016

# Motivation



Ukraine Power Outages  
2015 & 2016



Petrochemical Plant  
TRISIS Incident 2017

# Motivation



Ukraine Power Outages  
2015 & 2016



Petrochemical Plant  
TRISIS Incident 2017

1. **Advanced adversaries (APT)** pose a risk to ICS environments
2. Defenders need to **prevent, detect and react** to incidents, based on indicators (IOC) and behavior (TTP)
3. Defenders need **exercises** (ideally under realistic circumstances)
4. New “**artificial**” **adversaries** are required for effective training
5. Adversaries must be **emulated/simulated**

## Background

---

# Three Core Concepts

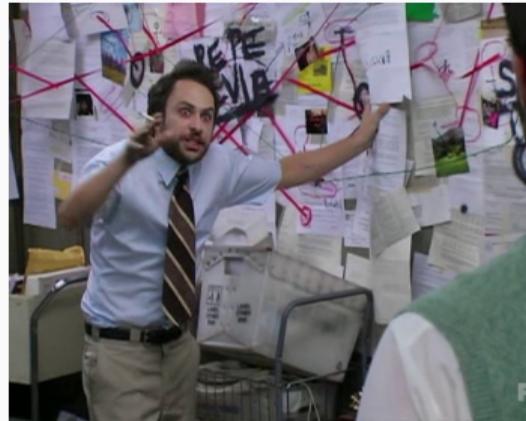


Threat Modeling

# Three Core Concepts



Threat Modeling

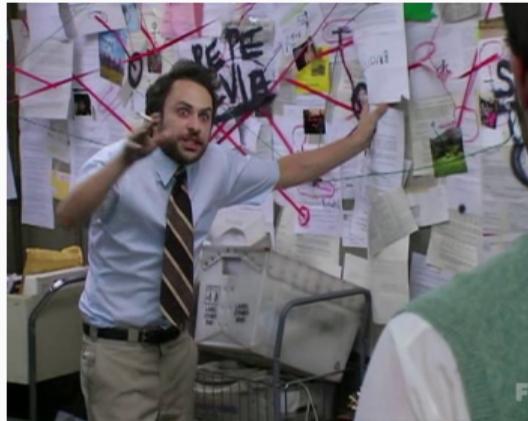


Attack Graphs

# Three Core Concepts



Threat Modeling

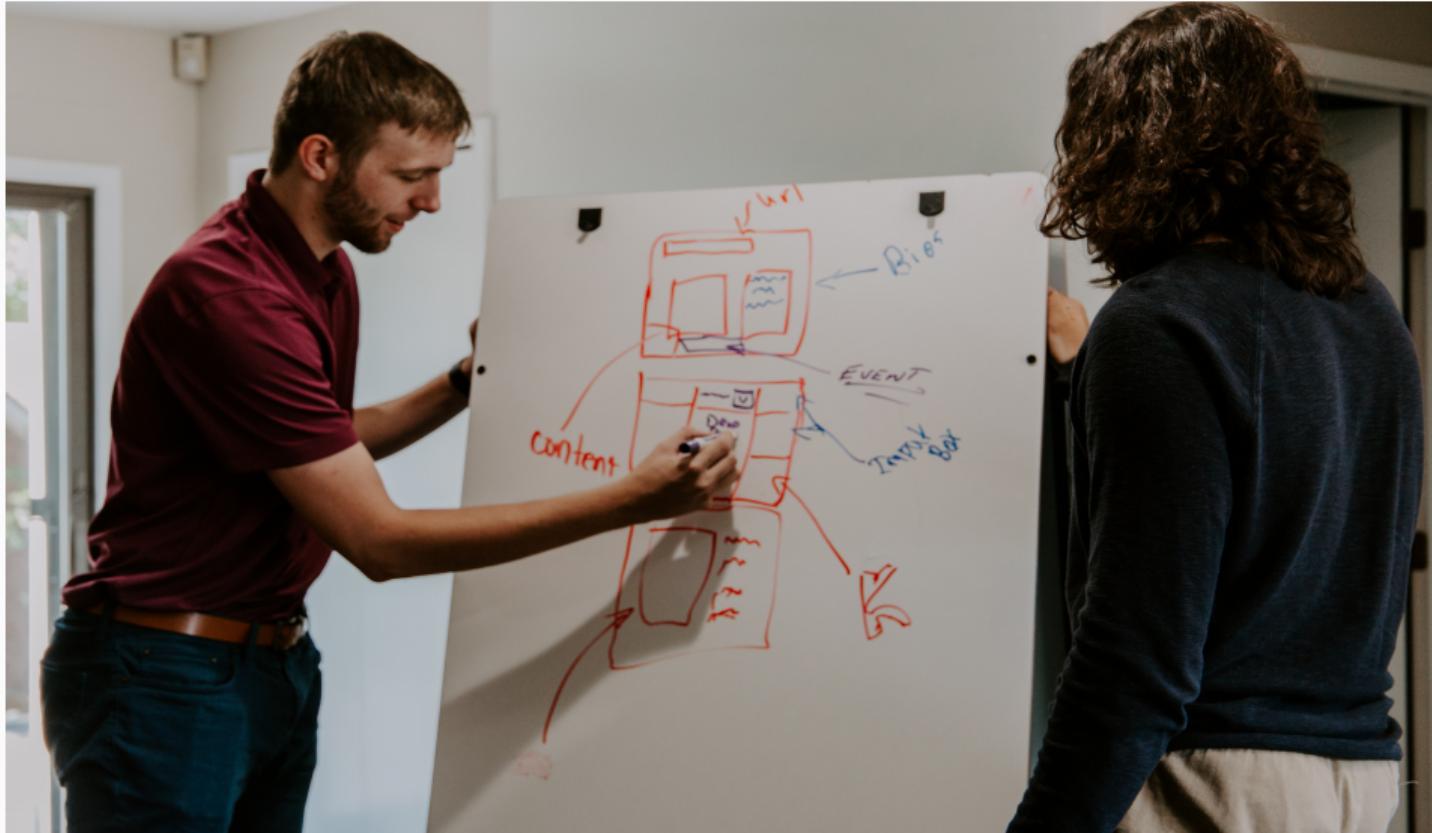


Attack Graphs



Adversary Emulation

# Threat Modeling



# Threat Modeling

- "All models are wrong, but some are useful." – George Box  
(but we need models for understanding, common language and see similarities)

# Threat Modeling

- "All models are wrong, but some are useful." – George Box  
(but we need models for understanding, common language and see similarities)
- Interdisciplinary approach

# Threat Modeling

- "All models are wrong, but some are useful." – George Box  
(but we need models for understanding, common language and see similarities)
- Interdisciplinary approach
- No one-size-fits-all – know your audience/targets
- Centricity: Attacker vs. Asset vs. Software

# Threat Modeling

- "All models are wrong, but some are useful." – George Box  
(but we need models for understanding, common language and see similarities)
- Interdisciplinary approach
- No one-size-fits-all – know your audience/targets
- Centricity: Attacker vs. Asset vs. Software
- Should start as early as possible – explicit and implicit
- No fire-and-forget – it is a continuous effort along the whole product lifecycle  
(yes, also in "agile")

# Threat Modeling - Key Questions

- Must read:

Adam Shostack – "Threat Modeling: Designing for Security"



# Threat Modeling - Key Questions

- Must read:  
Adam Shostack – "Threat Modeling: Designing for Security"
- What are we working on?

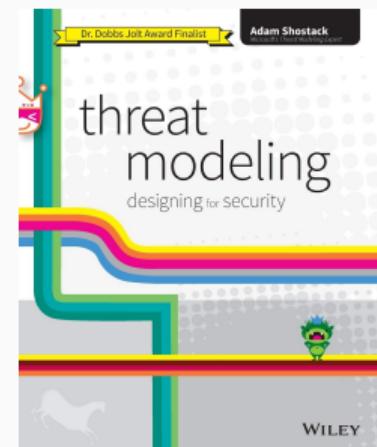


# Threat Modeling - Key Questions

- Must read:

Adam Shostack – "Threat Modeling: Designing for Security"

- What are we working on?
- What can go wrong?

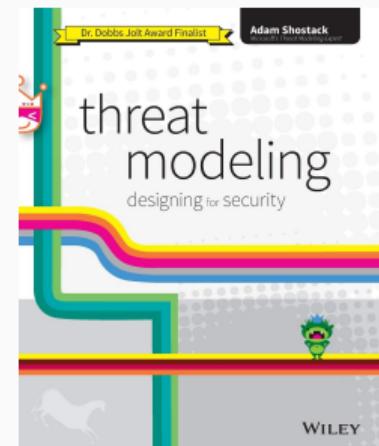


# Threat Modeling - Key Questions

- Must read:

Adam Shostack – "Threat Modeling: Designing for Security"

- What are we working on?
- What can go wrong?
- What are we going to do about it?

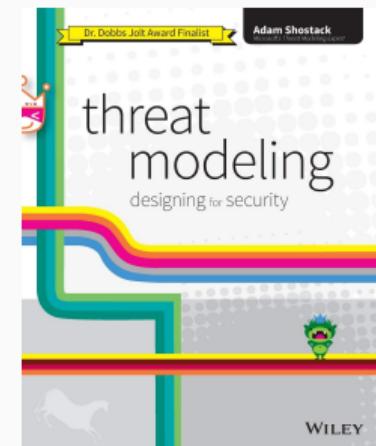


# Threat Modeling - Key Questions

- Must read:

Adam Shostack – "Threat Modeling: Designing for Security"

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

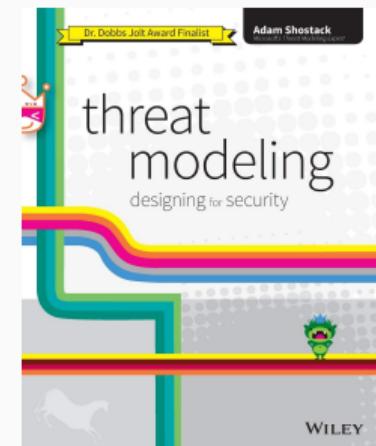


# Threat Modeling - Key Questions

- Must read:

Adam Shostack – "Threat Modeling: Designing for Security"

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?



[https://wiki.owasp.org/index.php/OWASP\\_Threat\\_Model\\_Project](https://wiki.owasp.org/index.php/OWASP_Threat_Model_Project)

# STRIDE - a mnemonic for threat modeling

S-T-R-I-D-E by Garg/Kohnfelder

<https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/>

# STRIDE - a mnemonic for threat modeling

S-T-R-I-D-E by Garg/Kohnfelder

<https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/>

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial-of-Service
- Elevation-of-Privilege

# STRIDE - a mnemonic for threat modeling

S-T-R-I-D-E by Garg/Kohnfelder

<https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/>

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial-of-Service
- Elevation-of-Privilege

other methodologies are LINNDUN, hTMM, PASTA, CIA, and many many more

(<https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/>)

# Cyber-Kill-Chain

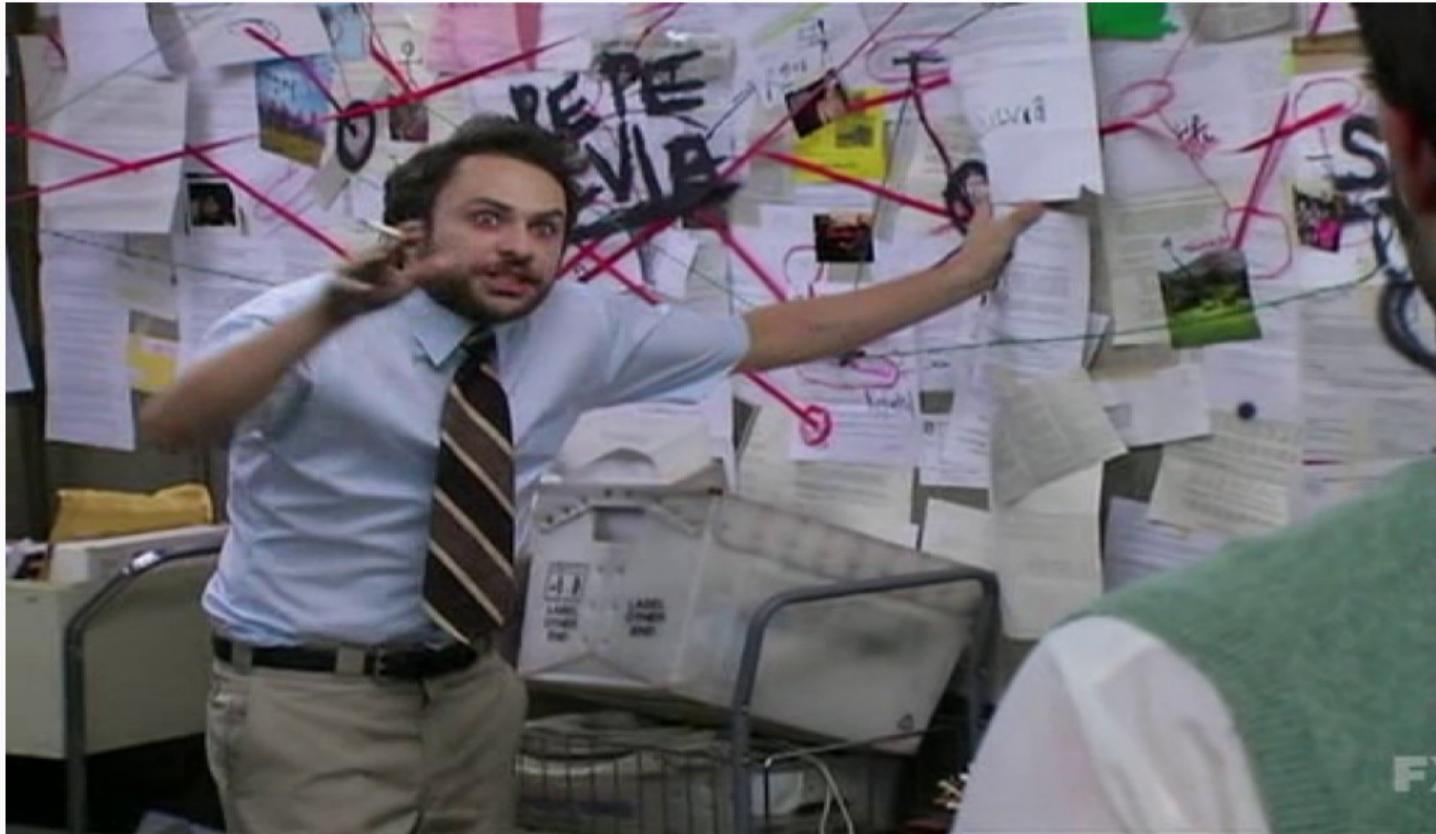


# MITRE ATT&CK

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques
Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)
BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)
Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)
Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)
Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)
Create Account (3)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels
Create or Modify System Process (4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer
Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (6)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels
External Remote Services	Hide Artifacts (6)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Non-Application Layer Protocol	Non-Standard Port
Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Data Staged (2)	Protocol Tunneling
	Process Injection (11)	Impair Defenses (6)	Steal or Forge Kerberos Tickets (3)	Peripheral Device Discovery		Email Collection (3)	Proxy (4)
		Indicator Removal on Host (6)	Steal Web Session Cookie	Permission Groups Discovery (3)		Input Capture (4)	Remote Access Software
		Indirect Command Execution		Process Discovery			Man in the Browser
	Scheduled			Query Registry			

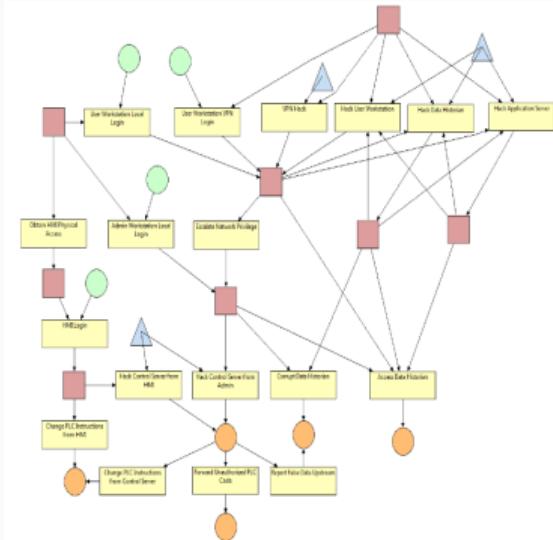
Excerpt from <https://attack.mitre.org/>

## Attack Graphs



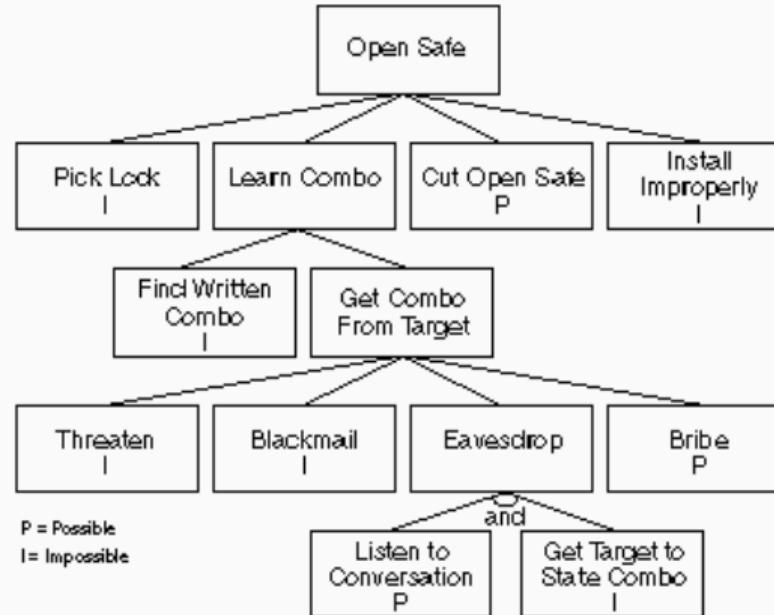
# Attack Graphs

- Schneier, Kordy, LeMay, Ekstedt and many more
- Started with fault tree analysis
- Attacks can be modeled intuitively with graphs/trees
- Focus mainly on assets less on the actions
- Used for modeling defenses, attack chains and critical paths
- Automated generation has been shown to be possible



(LeMay et al., Attack Execution Graphs, 2011)

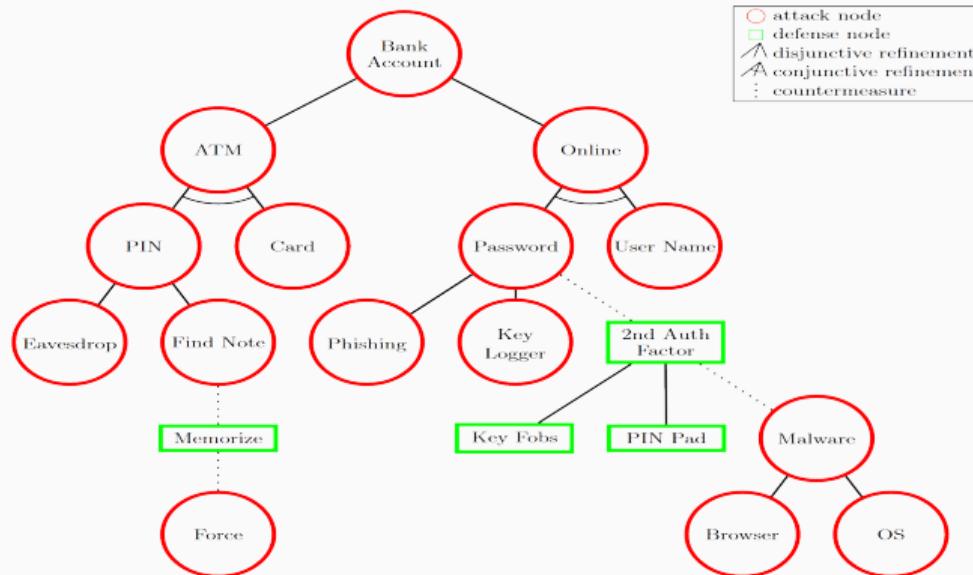
# Early Forms of Attack Graphs



## Attack Tree

(Schneier, Dr. Dobb's Journal, 1999)

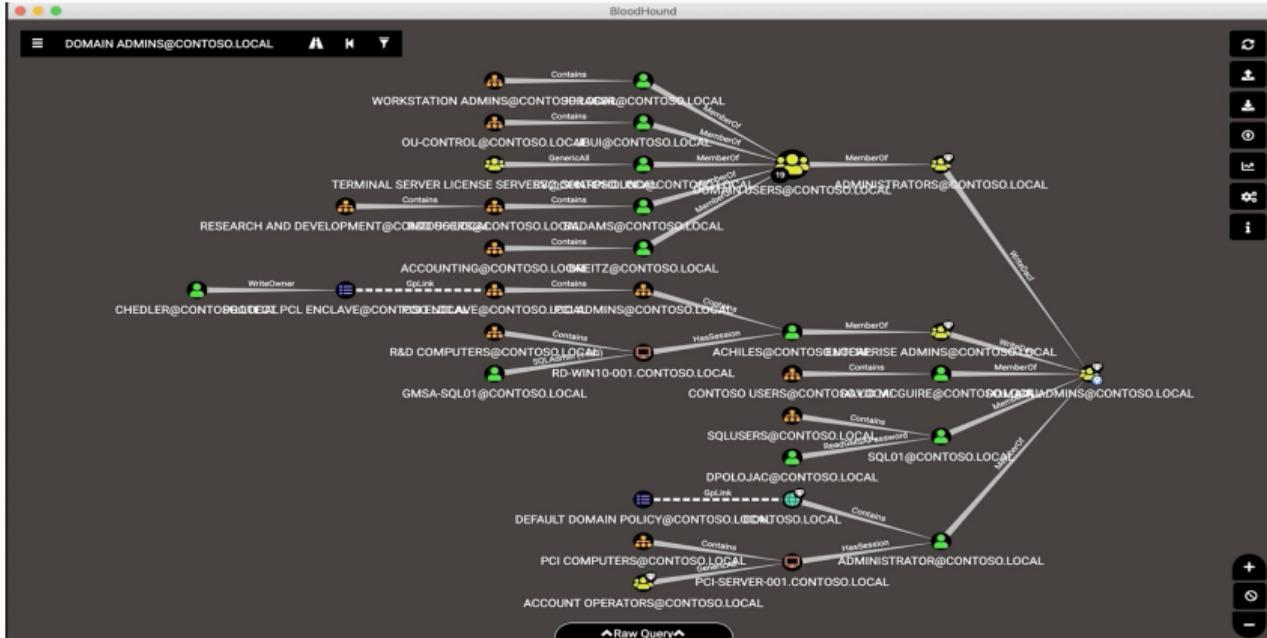
# Attack-Defense-Trees



## Attack-Defense-Tree

(Kordy et al., Foundations of attack-defense trees, 2010)

# Bloodhound Attack Tree



## Bloodhound Active Directory

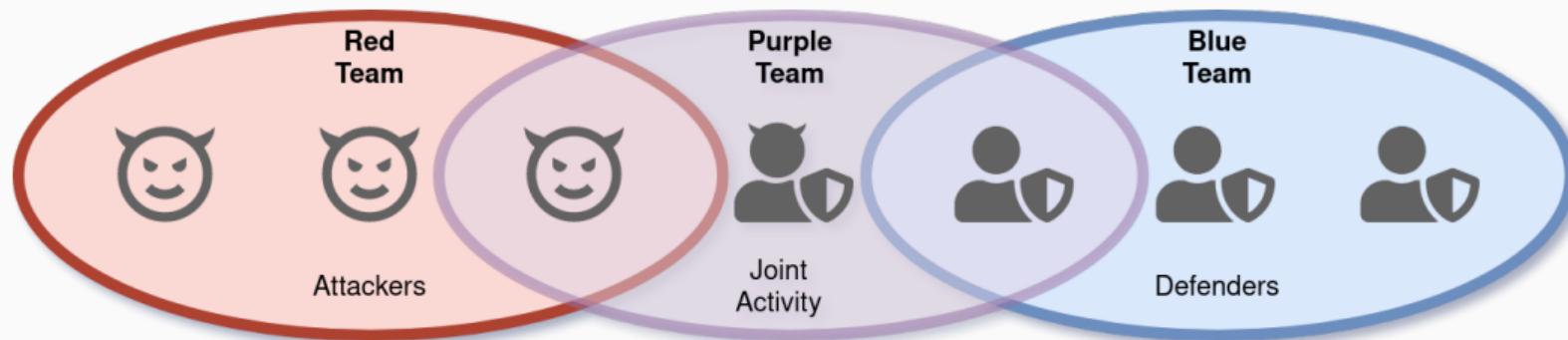
<https://bloodhound.readthedocs.io/en/latest/index.html>

# Adversary Emulation

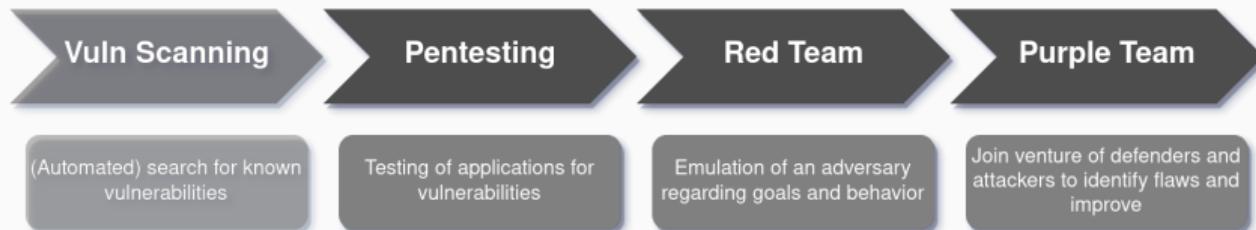


# Different Teams

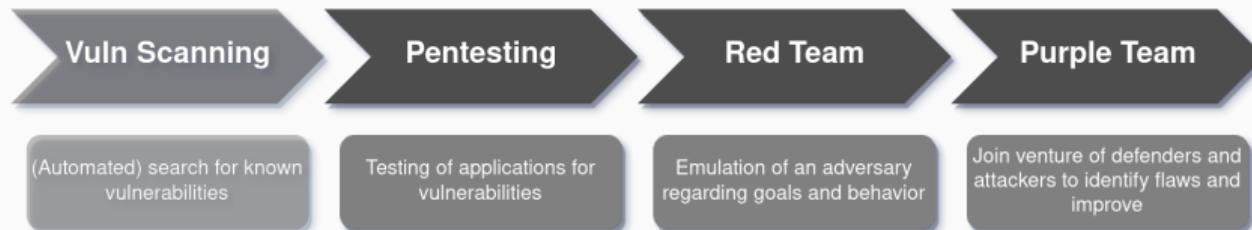
Who is involved in adversary emulation and simulation?



# Adversary Emulation and Simulation



# Adversary Emulation and Simulation



- Offensive Security for Defensive Activities
- Reproduction of adversarial behavior (TTP) to train/assess/improve defender's capabilities
- Purple teaming is highest maturity for offensive security activities
- Adversary Emulation vs. Adversary Simulation

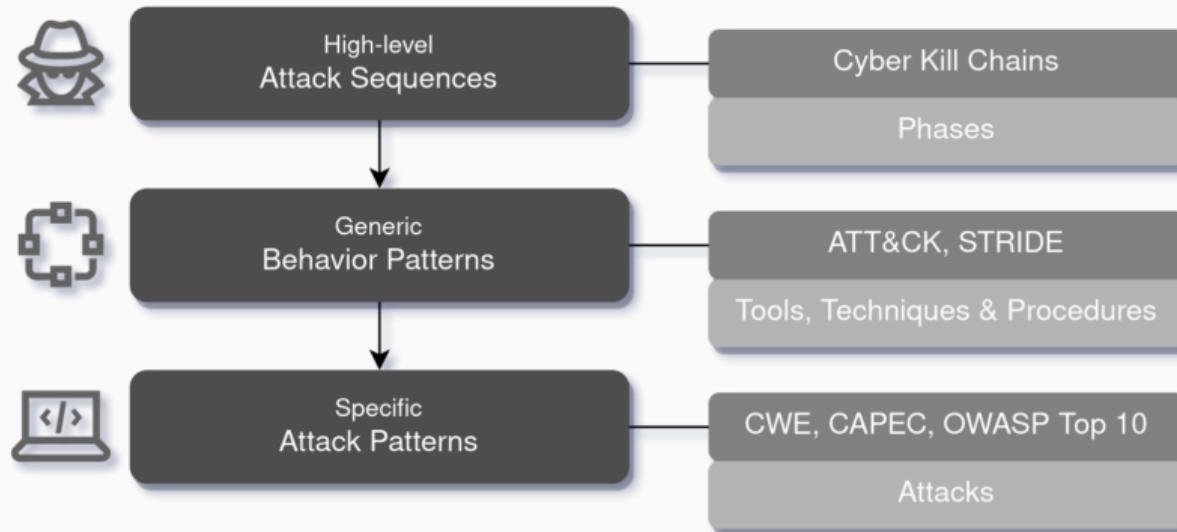
# Adversary Behavior Execution

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



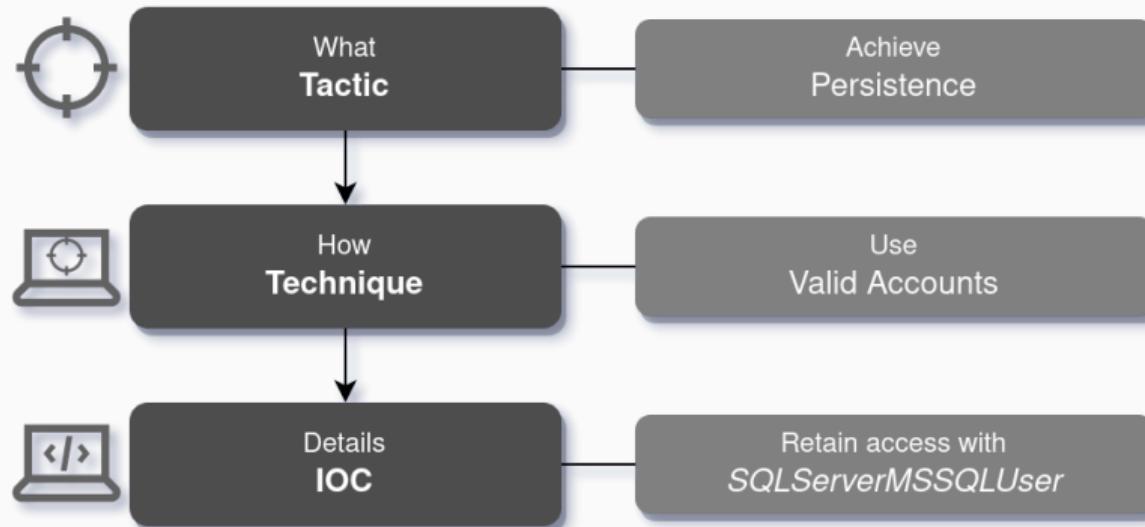
# Classification of Attack Models

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



# From high level goals to actions

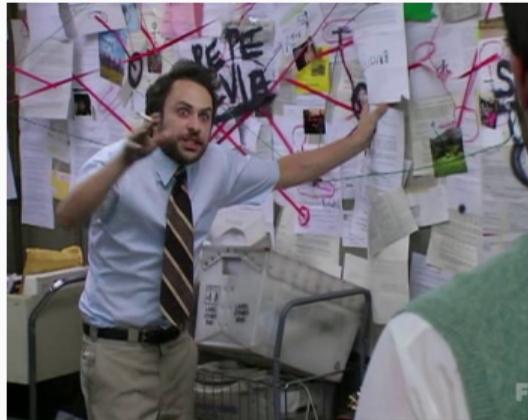
For an effective adversary behavior execution low level activities have to be developed.



# Three Core Concepts



Threat Modeling



Attack Graphs

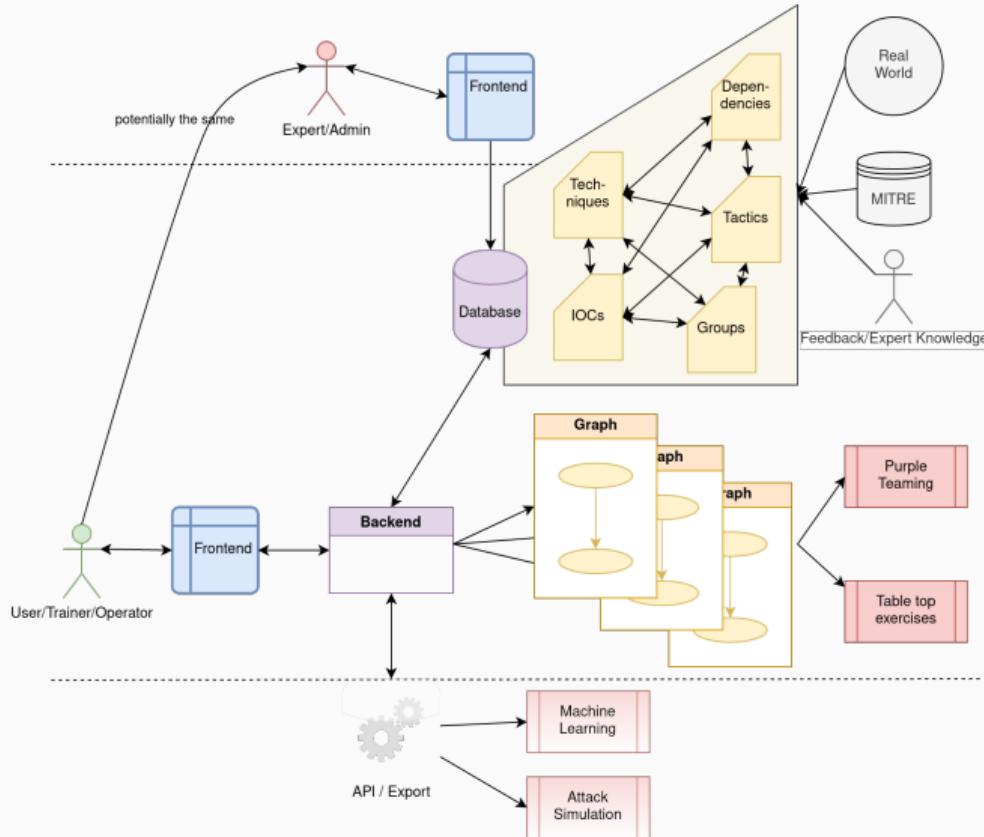


Adversary Emulation

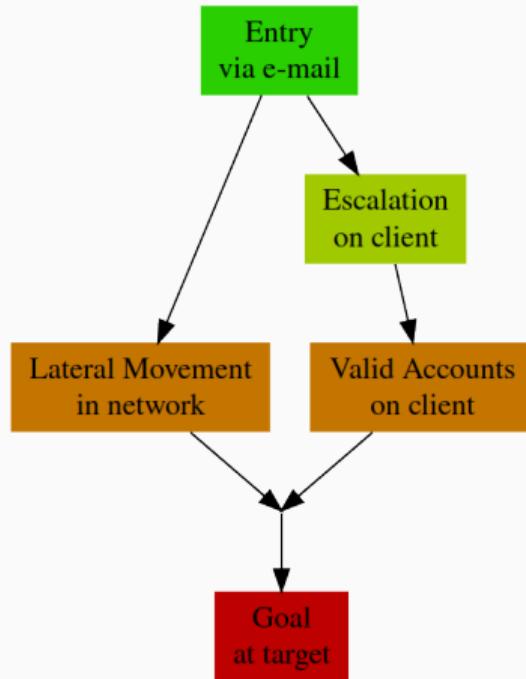
## **System and Graph Design**

---

# System Design



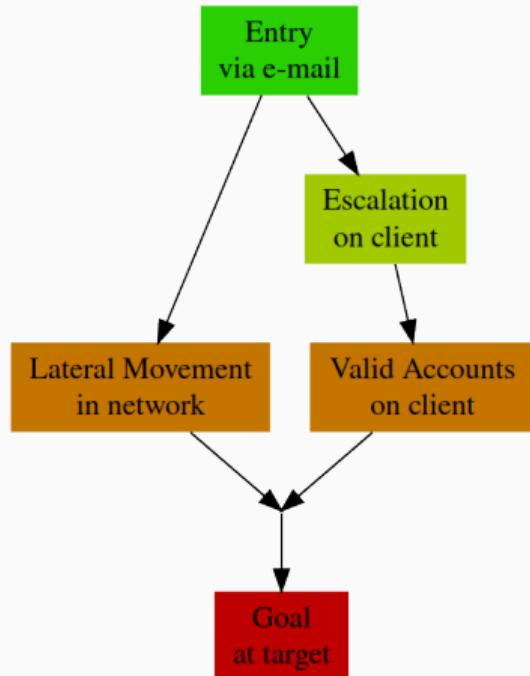
# Graph Design



## 1. Graphs

- Set of nodes and edges describing the adversary profile
- Focus on emulation/simulation of attack Techniques
- Sequential along MITRE Tactics (the “what”)

# Graph Design



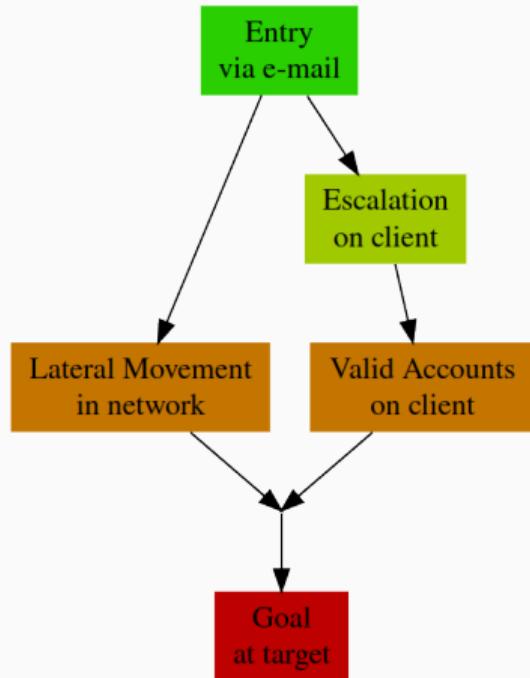
## 1. Graphs

- 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

# 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

## Summary

---

## Summary and Future Work

- Conclusion
  - Threat modeling is a powerful methodology to include security early on
  - Automated attack graph generation for adversary behavior execution is possible
  - Experts confirm viability of approach and prototype



# Summary and Future Work

- Conclusion
  - Threat modeling is a powerful methodology to include security early on
  - 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 and Discussion**

---

# 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/>

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-\[...\]-from-co-owners](https://www.meed.com/petro-rabigh-[...]-from-co-owners)
4. All other photos: <https://unsplash.com/> or common memes
5. Further references and a complete bibliography can be found at:  
<https://www.pull-the-plug.net/thesis/>