Cyber Risk and Resilience Analytics

Sachin Shetty, Ph.D.

Executive Director, Secure and Intelligent Critical Systems, Virginia Modeling, Analysis and Simulation Center

Professor, Department of Computational Modeling and Simulation Engineering

Old Dominion University

About Me

- Executive Director, Center for Secure and Intelligent Critical Systems, Virginia Modeling, Analysis and Simulation Center, Old Dominion University
- Joint Appointment- Professor, Department of Computational Modeling and Simulation and Engineering
- Faculty Appointment, Naval Surface Warfare Center, Crane, Indiana (Secret Level Clearance)
- Research supported by AFRL, AFOSR, DHS, DOE, NSF, NEEC, ONR, Sentara, and Boeing

Research Goal

- Modeling and analysis of threats to protect next generation Internet, cloud, mobile systems and networks and critical infrastructures.

Research Interests

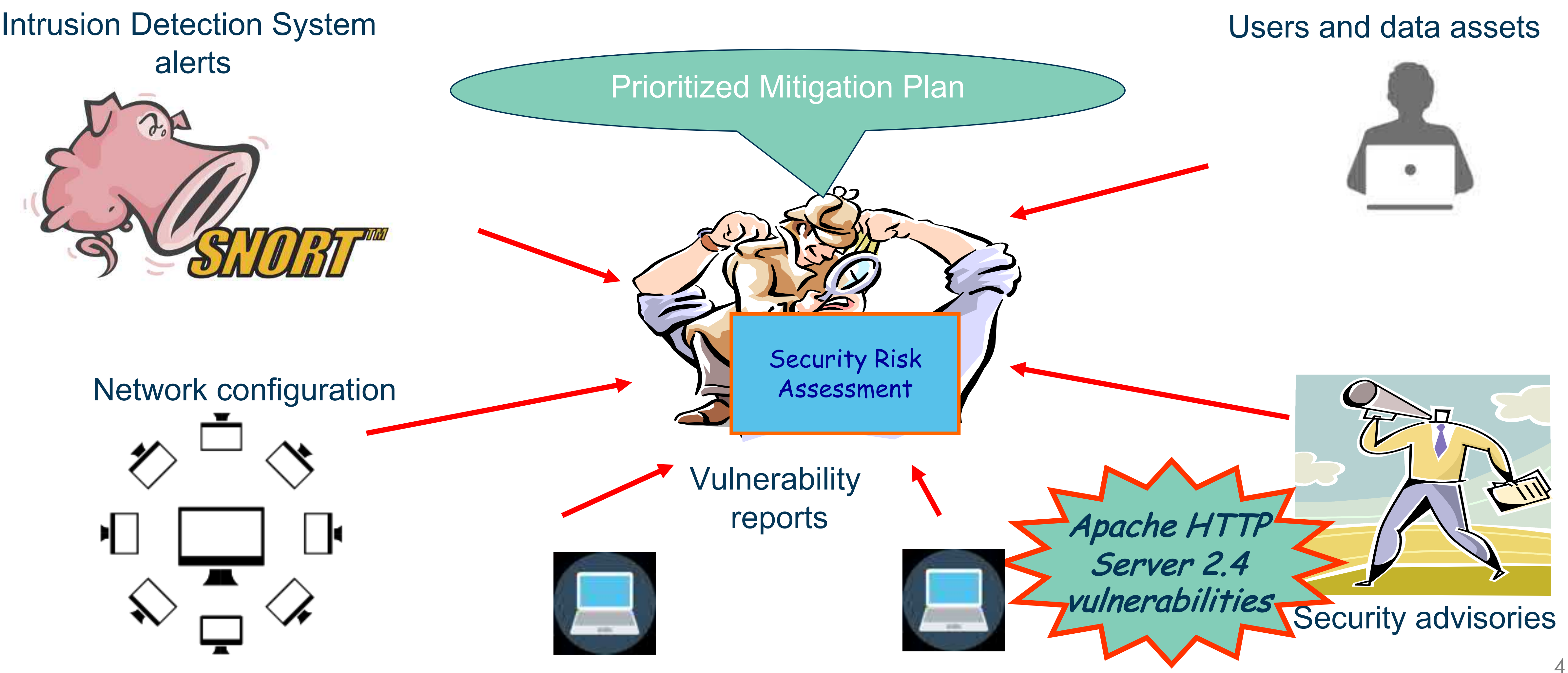
- Cyber security risk and resilience modeling and assessment
- Blockchain for distributed systems security
- Machine learning for anomaly detection

Course Overview

- June 17
  - Cyber Risk and Resilience Analytics Overview
  - Modeling Attacker Opportunity
  - Lateral Propagation Analysis
  - Assess Adversarial Effort
  - Infer Adversarial Action and Intent

- June 18
  - Hands on exercise in virtualized environment
  - Learn to generate and analyze attack graphs
  - Computer cyber risk and resilience metrics

Life in the Security Operation Center



TRENDS IN CYBER THREATS

EVOLVING TARGETS

- Data and Knowledge
- Critical Infrastructure systems, such as ICS
- Information theft
- Hacking for disruption

EVOLVING TECHNIQUES

- Using human layer (weakest link)
  - Phishing, malicious insiders
- Complex multi-stage (low and slow APTs)

EVOLVING IMPACTS

- Data still a target
- Theft is not always the outcome
- Data being destroyed – or changed – which generates mistrust

Mining Industry Cyber Threat landscape, IDEFENSE, Accenture Security

Motivation

- The cyber integration with critical infrastructure (CI)
  - Enables high reliability and fast operability
  - Impose risk of disruption of safe and secure operation
- Resilient cyber infrastructure- Ability to anticipate, withstand from deliberate attacks, threats or incidents
- Critical targets often segregated and often deployed away from the perimeter, hard to get into with direct access
- Defense-in-depth architecture forces attackers to conduct lateral propagation.

Motivation Cont…

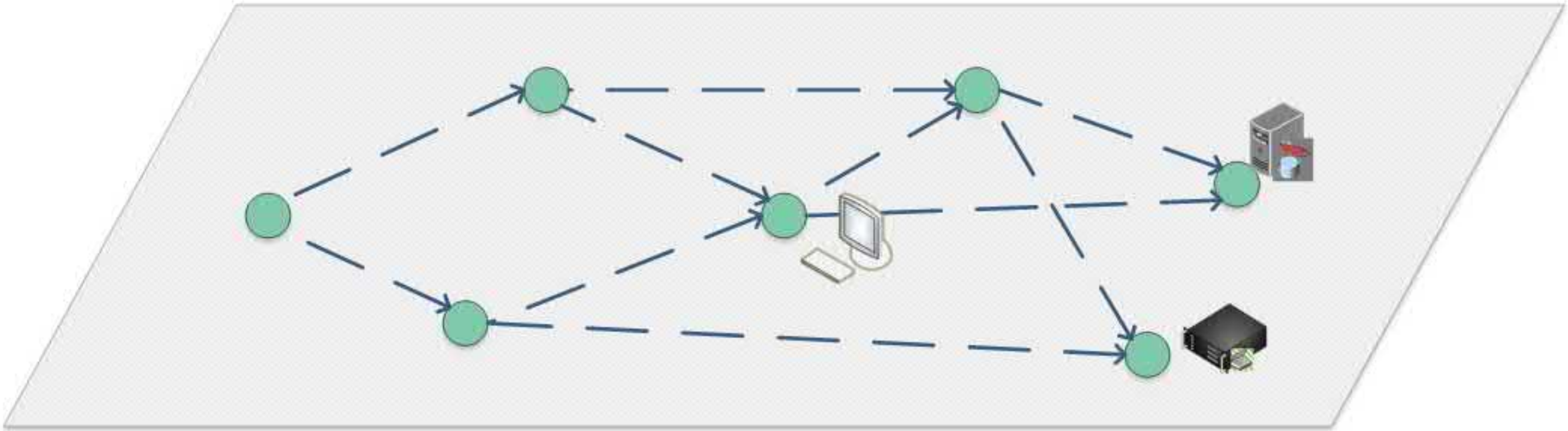
- Adversaries need to propagate a long span of attack surface to reach their goal
- Recently executed more attacks took advantage of this architecture
- Resilience analysis is quite challenging due to—
  - Large scale
  - Heterogeneous network
  - Interdependency

- Adversarial opportunity and behavior is critical to understand the threat cycle
- Detection, prioritization and mitigation is a complex problem in CIs security

Analytics Playground- Attack Surface

- Subset of system resources that can be potentially used by an attacker to launch an attack.
- A larger attack surface-
  - Higher threat landscape
  - Increased risk of compromise
- Different attempts has been taken to dynamically modulate attack surface.
- Some possible challenges:
  - Costly overhead to the legitimate users
  - Maintenance complexity
  - Disruption of service
- Existing work doesn't consider attack life cycle.

Analytics Playground- Attack Surface

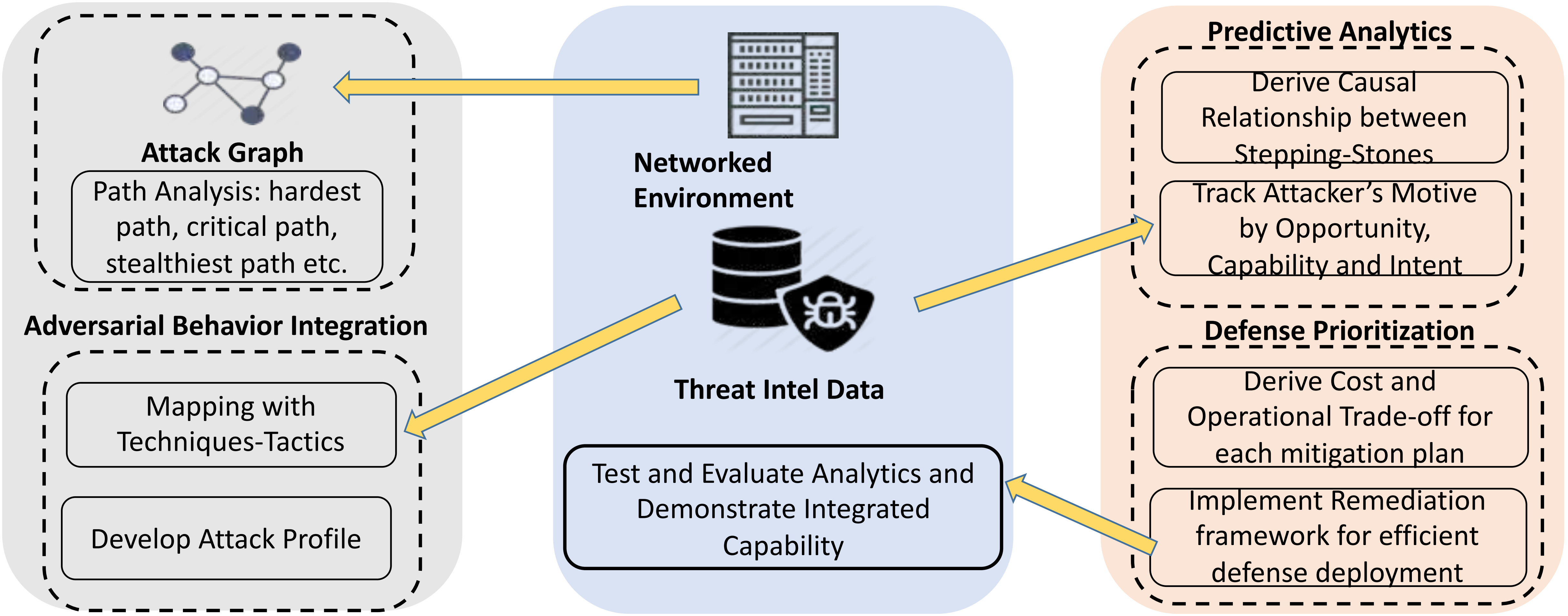


Our attack surface analysis aim to protect critical functionality of the systems amid adversarial events

Cyber Resilience Assessment in Critical Infrastructure (CI)

Attack Progression	**Opportunity**: Identify stepping stones and lateral propagation	**Capability:** Adversary skill set to conduct successful exploitation	**Intent:** Attack plans, attacks goals
Defender	Holistic View of the CI. Potential exploitation and impact	Technical exposure through attack paths	Identify accessible critical assets
	Limited View of the CI. Increased insight with successful exploitation	Intrinsic Knowledge. Evolving skill	Strategic plan driven by motivation and constraint

Cyber Resilience Analytics



Goal 1- Problem Statement

- Existing work model lateral propagation-
  - Graph spectral matrices
  - Bypassing contextual analysis.
- Host in attack surface facilitates attack progression within this.
- Need to conduct susceptibility analysis of hosts along the path to the target
- Heterogeneous network architecture and expands diverse opportunity

How to model attacker's opportunity within each host in the attack surface and how evolves through attack progression

Goal 2- Problem Statement

- Opportunity gives different options to propagate
- Sophisticated attacker's progression dictates by their motivation
- Static cyber defense doesn't provide effective intrusion response
- Existing work doesn't consider different aspects of attack strategy
- Need an efficient situational awareness to restrict persistent threats from deeper penetration

Given attacker's opportunity space, how to model an intrusion response system by considering diverse strategy an attacker could employ in lateral propagation

Goal 3- Problem Statement

- Attacks are diverse in terms of techniques, progression and impacts
- Attacks often follows-
  - Sequence of steps towards target
  - Sequence of actions in each step
- Existing analysis only consider topological connection between stepping stones
- Assuming pre-defined skill set ignoring attack complexity in the propagation path.
- Opportunity gives attackers potential expanse
- Additional Inspection needed to reveal hidden insight of attack step

How to assess attacker's evolving effort by characterizing potential adversarial behavior in the attack surface

Goal 4- Problem Statement

- Followed sequence depends on preference
- Understanding attackers' motive is critical to track the behavior
- Conventional IoC doesn’t provide adequate defense against malicious campaign
- Meaningful campaign information could shrink huge attack surface
- Extract attack pattern not IoC

How to infer attackers prioritized action and the respective motive in the attack surface

Modeling Attacker’s Opportunity

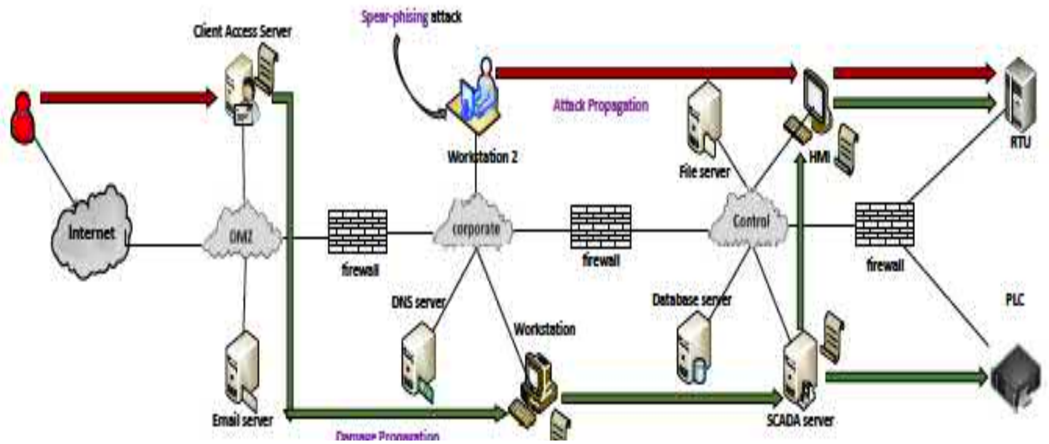
- Sharif Ullah, Sachin Shetty, Amin Hassanzadeh, "Towards Modeling Attacker’s Opportunity for Improving Cyber Resilience in Energy Delivery Systems”, Resilience Week, Denver August 2018.
- Ullah, Ullah, Sharif, Sachin Shetty, Amin Hassanzadeh, Anup Nayak and Kamrul Hasan, “On the Effectiveness of Intrusion Response Systems against Persistent Threats." In 2020 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2020.

Overview of the approach

- Goal- Modeling attacker's opportunity for lateral propagation

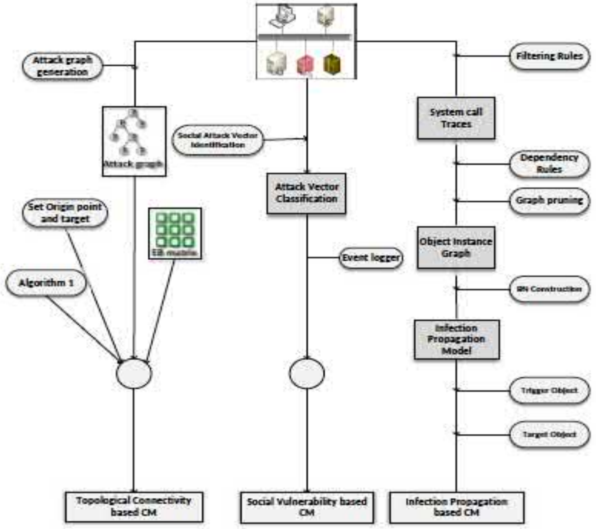
Opportunity can be categorized as :

- ***Use case 1*** – Attack propagation
- ***Use case 2-*** Attack origin
- ***Use case 3-*** Damage propagation



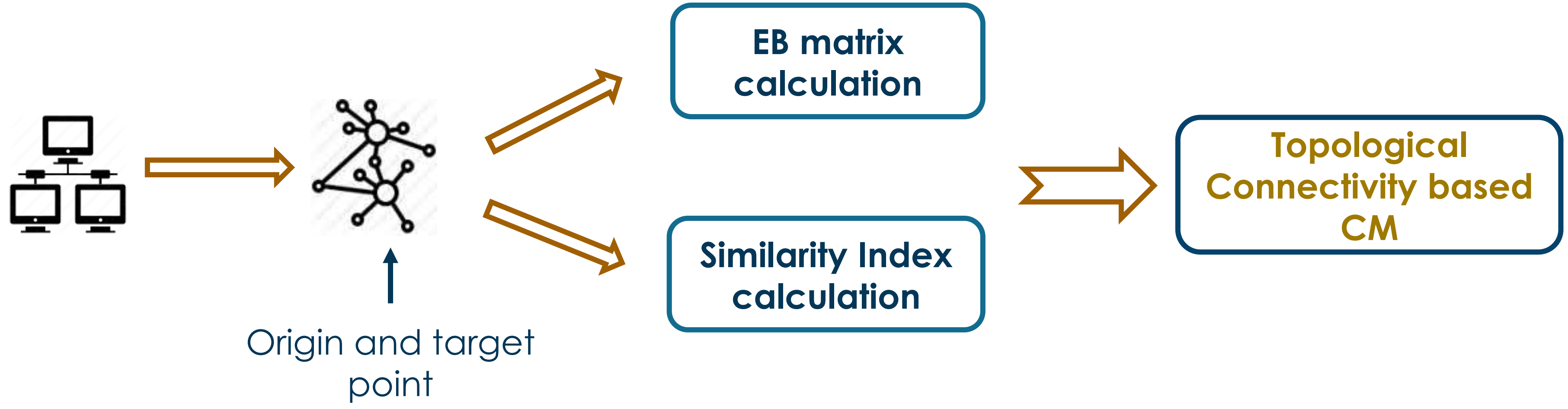
Three criticality metric:

- Topological Connectivity based Criticality Metric (TCCM)
- Social Vulnerability based Criticality Metric (SVCM)
- Infection Propagation base Criticality Metric (IPCS)



TCCM and SVCM

- TCCM captures Attacker’s propagation itself by means of connectivity and other resources.
- Along with Global info. the contextual info incorporated to identify correlated risk



- SVCM captures Opportunity to attacker’s prior to penetration.
- Assign score to hosts based on the susceptibility of social engineering attack.

TCCM- Parameters

- Model the opportunity each exploitable host provides.
- Attack graph is generated
  - Network connectivity map
  - Attacker's privilege and security condition of host

- Attack path is characterized-
  - **Global info-** degree of exploitability
  - **Contextual Info-**
    - Vulnerable Service *(VS)*
    - Operating System *(OS)*
    - Isolation Pattern *(IP)*

Along with global info. the contextual info is incorporated to identify the correlated risk

TCCM- Parameters

- ***Similarity Index***: relative abundance of difference instances of contextual parameter in an attack path
- Similarity index of parameter $\boldsymbol{z}$ in attack path $\boldsymbol{p_y}$ is given as

$$S_{index(p_y,z)} = w_z \times r_{p_y,z}$$

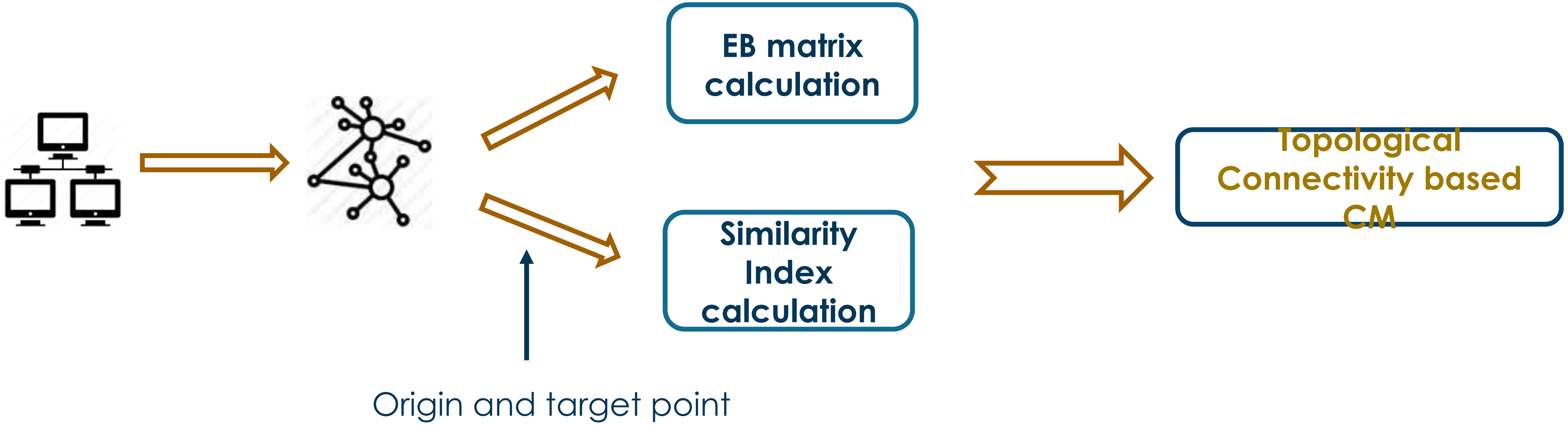
Where Effective richness of parameter z

$$r_{p_y,z} = \prod_{j=1}^{q} \frac{m_j}{|H_y|}$$

- Each path has $\boldsymbol{q}$ types of instances of a parameter
- $\boldsymbol{m_j}$: number of instances of type $\boldsymbol{j}$
- $|\boldsymbol{H_y}|$: Total number of host/instances in whole attack path
- $\boldsymbol{w_z}$: weight factor

TCCM- Parameters

- $Effort - betweenness\ matrix\ (EB)$: describe the cost of each host through a path.
- Element of EB: $e^t_{p_y n} = \dfrac{candidate\ host\ cost\ (c^t_{p_y} n)}{path\ cost\ (C^t_{p_y})}$
- TCCM- $$C^n_{top} = \sum_{t \epsilon \mathcal{T}} \Big(\sum_{p_y \epsilon \mathcal{G}} \frac{1}{\mathcal{E}^t_{p_y n}} \times [e_{p_y n}]_t \times \prod_j \frac{1}{1 - S_{index(p_y, j)}} \Big) \times \mathcal{D}^t$$



SVCM- Parameters

- Attack path analysis is not sufficient to capture the opportunity of insider attack.
- This metric assign score to hosts based on the susceptibility of social engineering attack.

- Classify each attack vector (AV) in terms of stages an attack spans.
- Major stages is divided by multiple sub-stages, marked by classification parameter.
- Each sub-stage classification parameters is mutually exclusive.

Table I: Classification parameters for AVs

Orchestration	Target chosen	Explicit target (l_1) Promiscuous target (l_2)
	Method of Distribution	Local (l_3) Remote (l_4)
	Mode of Automation	Manual (l_5) Automatic (l_6)
Exploitation	Deception vector	Cosmetic (l_7) Behaviour (l_8) Hybrid (l_9)
Execution	Attack Persistence	One-off (l_{10}) Continual (l_{11})
	Execution step	Single step (l_{12}) Multi-step (l_{13})

SVCM- Metric

- Importance of classification parameter vary from network to network.
- Define score on each attack vector ➡ **social vulnerability score *(SVS)***
- Weight Z_k for classification parameter k based on defenders policy and strategy.
- Compute SVS for attack vector i given the set of classification parameter L_i

$$SVS_i = \frac{\sum_k (Z_k \times l_k)}{|L_i|}$$

Our second criticality is derived by summing ***SVS*** and frequency of interaction ***f*** over all AVs for host ***n*** and multiply with network diversity

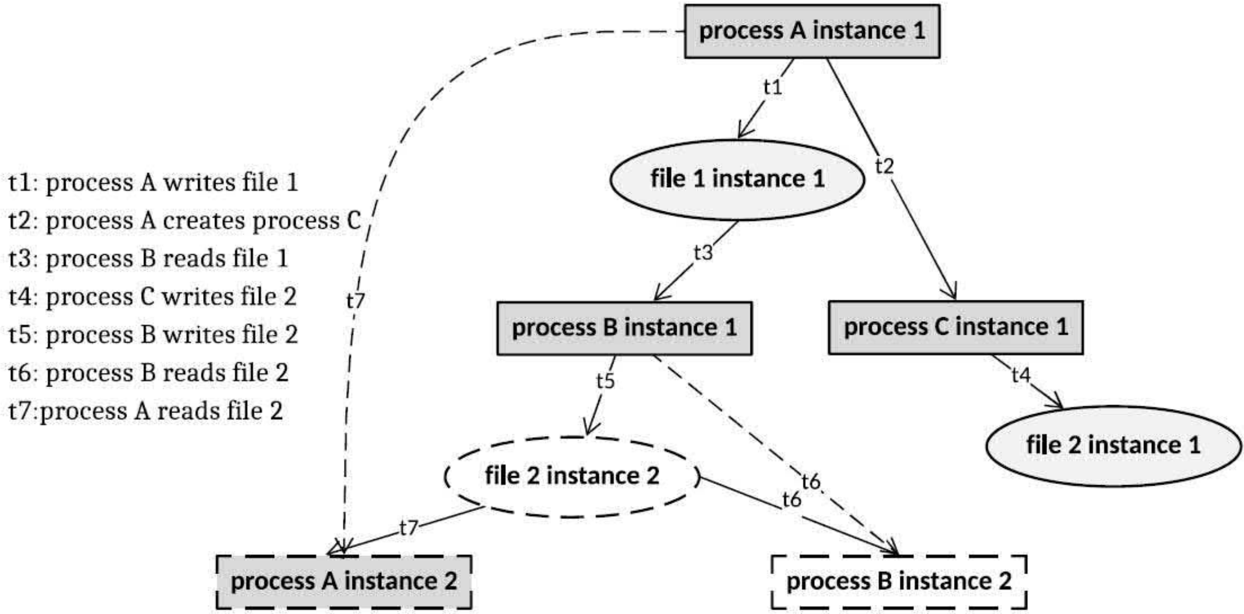
$$C_{sv}^n = (\sum_{i=1}^{m} SVS_i \times f_i) d_{sv}$$

IPCM- Infection Propagation

- Interaction between system objects could be new opportunity for the attacker
- We classify three types of objects : process, files and sockets for our analysis

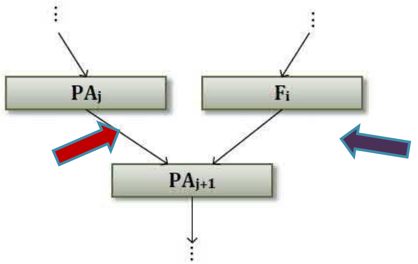
- Capture the dependency between objects by **control** and **information flow** between them
- Thus intrusion among any object could initiate **infection propagation**
- We model this propagation by **object instance graph**
  - Host object instance graph $(HOIG) \equiv (V, E, O_v, d_E)$

➢ $O_v : V \rightarrow \sum_T$ *vertex to syscall trace*
➢ $\boldsymbol{E}: set\ of\ edges \equiv functional\ dependency$
➢ $V: set\ of\ vertices \equiv obejct\ instances$
➢ $d_E : E \rightarrow dep_e\ edge\ with\ specific\ source \rightarrow sink\ dependency$



IPCM- BN formulation & Metric

- Infection propagation can be classified:
  - Intra-object infection propagation
  - Inter-object infection propagation



CPT at node PA_{j+1}

PA_{j+1}=T	PA_j	F_i
0	F	F
ρ	F	T
1	T	F
	T	T

- Bayesian Network (BN) is effective tool to incorporate intrusion evidence in order to characterize infection propagation

- Probability of infection can be calculated with the CPT and the given equation

$$Pr(X_i) = 1 - \prod_{j=1, i \neq j}^{m} [1 - Pr(X_i|X_j) \times Pr(X_j)]$$

SVCM (maximum damage):

Set of objects related to process control and operation

Intrusion evidence

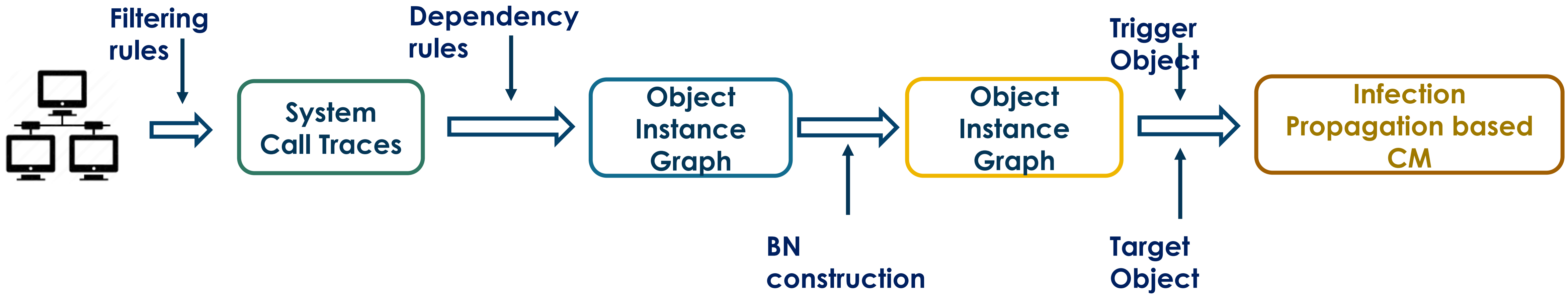
Impact on substation operation

$$C^n_{inf(max)}(\eta) = \{Pr[o_1, o_2, ...o_i|e_1, e_2, ...e_j]\} \prod_{o_c \epsilon \{O_c\}} I_{o_c}$$

SVCM (minimum damage):

$$C^n_{inf(min)}(\eta) = \{1 - Pr[o^c_1, o^c_2, ...o^c_i|e_1, e_2, ...e_j]\} \sum_{o_c \epsilon \{O_c\}} I_{o_c}$$

IPCM- System Model



Simulation Results: TCCM

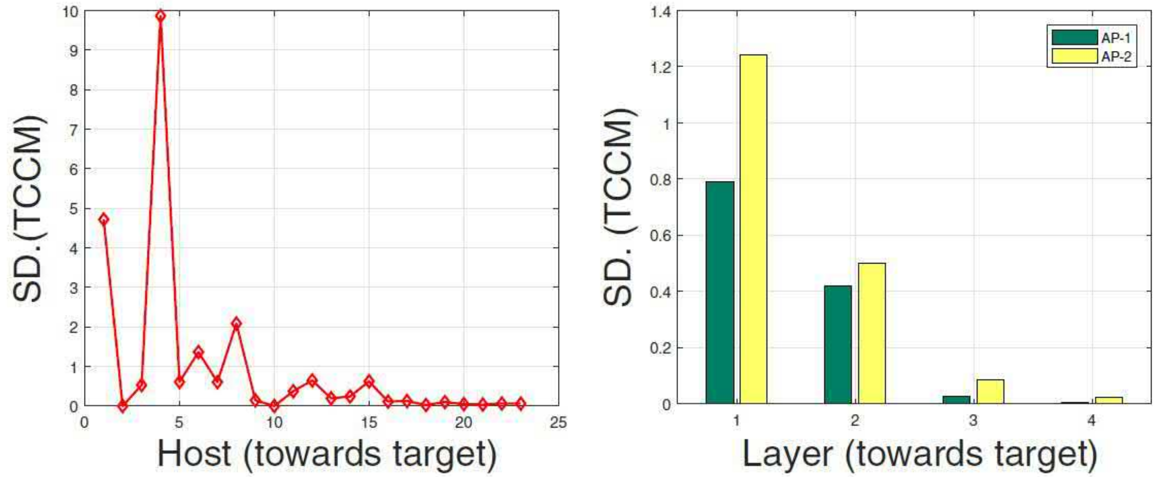


Fig. 2: Standard deviation of TCCM due to multiple initial attack points, for each host (left) & for hosts within layer (right)

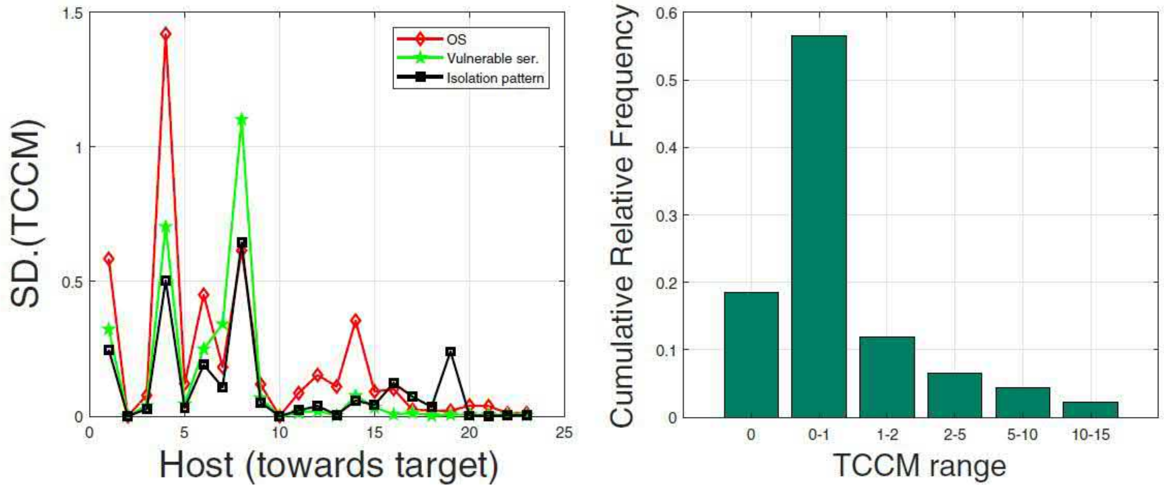


Fig. 3: Evaluation result for SD of TCCM due to OS, VS and IP (left), risk of the network for particular attack points

Simulation Results: SVCM and IPCM

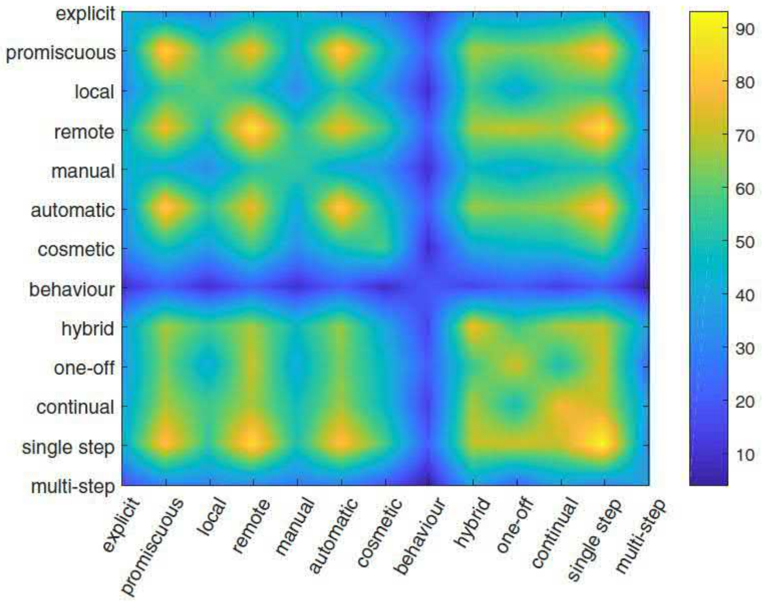


Fig. 4: Network diversity in terms of social attack vectors

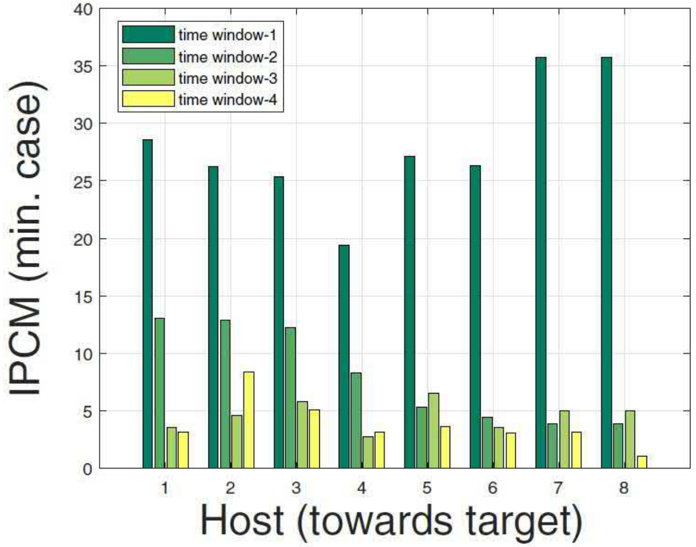


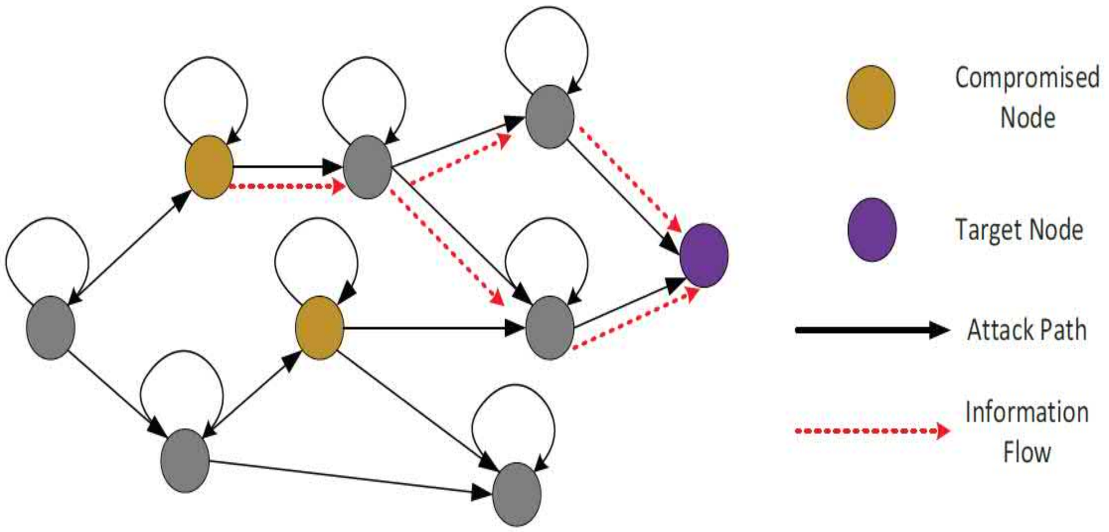
Fig. 5: Infection Propagation based CM for hosts

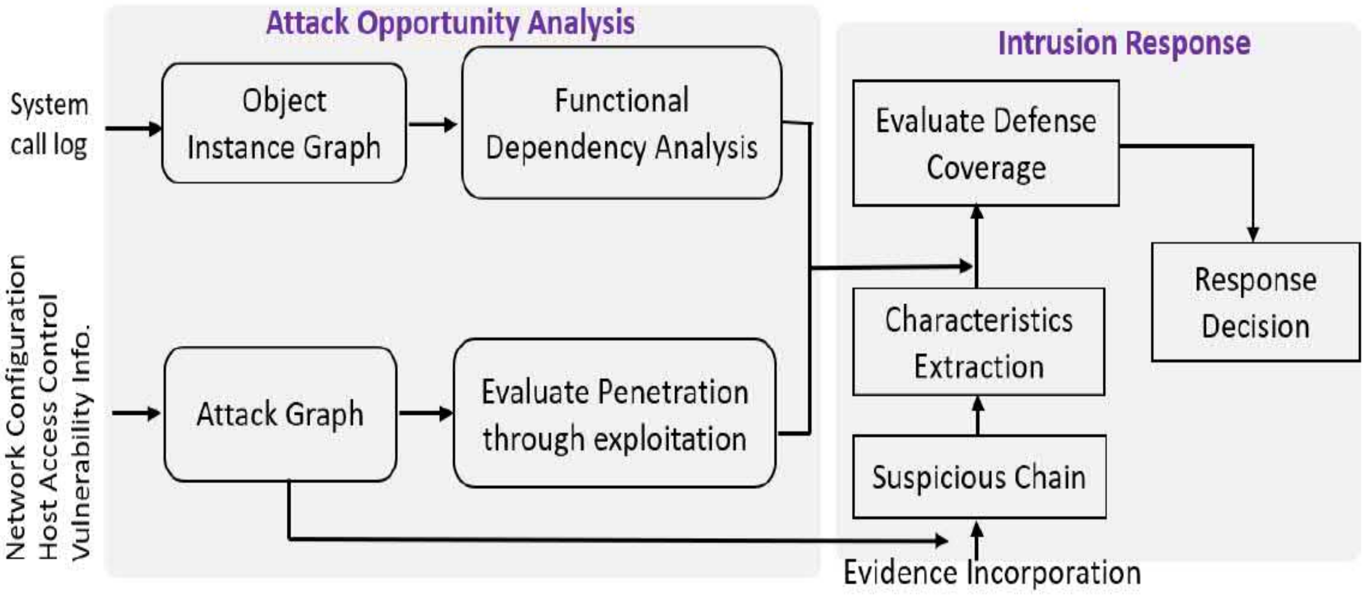
Intrusion Response- Proposed Approach

- Capture and analyze dynamic behavior of attacker within attack path
- Model attacker's opportunity corresponding to each strategy
- Extract post compromise sequence characteristics to inflict next adversarial options.
- An online dynamic intrusion response system
- Deter attack occurrence by increasing the cost and uncertainty in attack planning and execution

- Ullah, Ullah, Sharif, Sachin Shetty, Amin Hassanzadeh, Anup Nayak and Kamrul Hasan, "On the Effectiveness of Intrusion Response Systems against

System Model





- Investigate different options of potential opportunity of adversary.
- Opportunity attack surface explore—
  - Attack graph
  - Object instance graph
- Intrusion response phase examine suspicious chain and enforce appropriate decision

Progression through Exploitation

- Model the opportunity each exploitable host provides
- For node j in path p_k the cost value is calculated as

$$c^t_{p_k j} = \prod_i^j \frac{y_v}{10}$$

- Known vulnerability exploitation by CVSS exploitability score

- The cost of target host t also determined in a similar way—

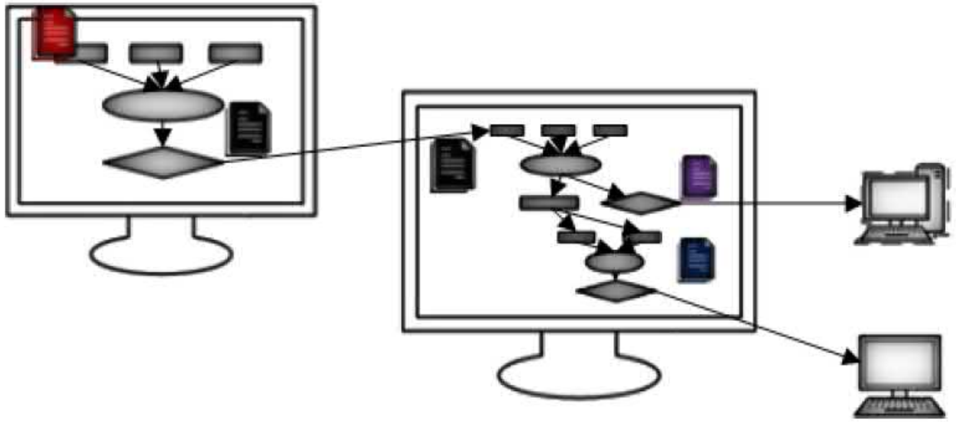
$$C^t_{p_k} = c^t_{p_k t} = \prod_i^t \frac{y_v}{10}$$

- The exploitation score

$$ES_j = \mathcal{D}^t \sum_{t \epsilon T} \sum_{p_k \epsilon P} \left(\frac{1}{\xi^t_{p_k j}} \times \frac{c^t_{p_k j}}{C^t_{p_k}} \times \prod_x \frac{1}{1 - S_{index(p_k, x)}} \right)$$

Functional dependency Estimation

- Functional dependency between hosts could be a stealthy malicious link.
- Capture the dependency between objects by information flow between then and model it through infection propagation.



Functional dependency score:

Set of objects from target node

Object from host node

Impact on control and operation

$$FS_j(\tau) = \{Pr[o_{t_1}, o_{t_1}, ...o_{t_i} | o_{j1}, o_{j1}, ...o_{j_z}]\} I_{O_t}$$

Intrusion Response Module

- The IRS module has three stages:
  - Uncertainty of security state
  - Uncertainty of attackers’ behavior
  - Response decision making process

- SIEM acquire and analyze real-time information
- Response function triggered after identifying a steeping stone
- Suspicious chain comprised with the set of connected compromised nodes from SIEM events.
- Extract apparent capability for parameter x from chain s_i
- Plugin the weight into exploitation score to model future threat propagation modeling--

$$w_x^{s_i} = \frac{\sum_{l=1}^{q_x^{s_i}} \left(\frac{1}{\phi_l} \sum_l e^{\frac{t_l}{\lambda}}\right)}{\sum_{z=1}^{n} e^{\frac{t_z}{\lambda}}}$$

$$ES_j^{s_i} = \mathcal{D}^t \sum_{t \epsilon \mathcal{T}} \sum_{p_k \epsilon P} \left(\frac{1}{\xi_{p_k j}^t} \times \frac{c_{p_k j}^t}{C_{p_k}^t} \times \prod_x 1 + \left(\frac{1 - w_x^{s_i}}{1 - S_{index(p_k, x)}}\right)\right.$$

Intrusion Response Module

- Capture two behavior from suspicious chain:
  - Diverse capability
  - Aggressiveness

- Aggressiveness is tracked by using temporal information associated with each evidence
- How much penetration deviates from most aggressive attacks
- Candidate node has two scores:
  - Exploitation - Aggressiveness
  - Functional dependency - Stealthy
- Attacker constrained to take one strategy in single time-slot
- Finding optimum node *j* for response--

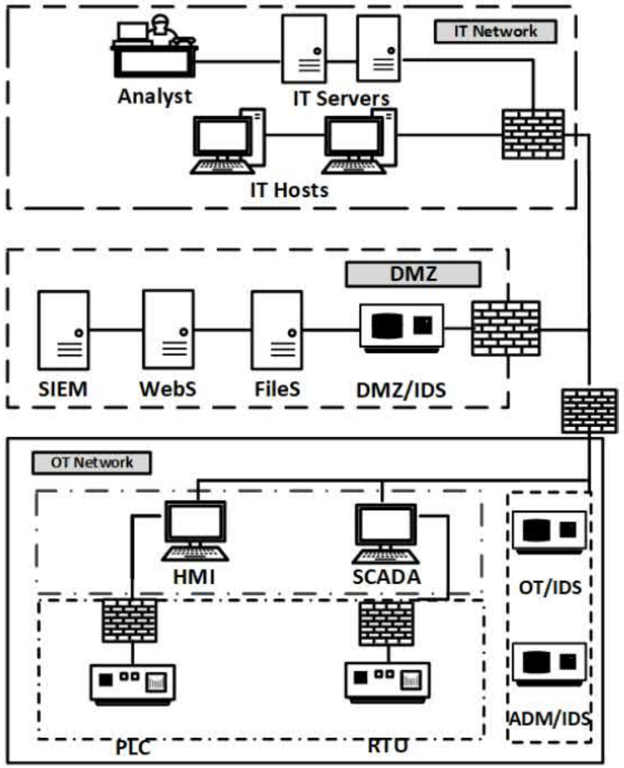
$$\alpha_i = \frac{\sum_{z=2}^{n} e^{\frac{z}{\lambda}}}{\sum_{z=2}^{n} (t_z - t_{z-1}) e^{\frac{z}{\lambda}}}$$

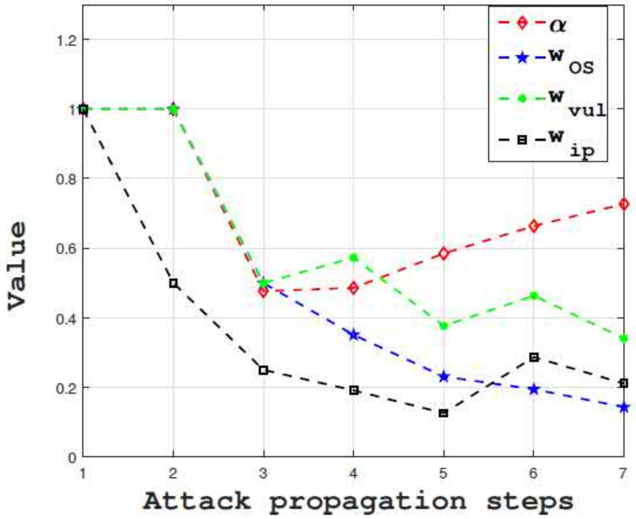
$$\begin{aligned} \underset{j \in G}{\text{argmax}} \quad & \frac{df_{ES_j^{s_i}} + df_{FS_j}}{\mathcal{C}_j} \\ \text{subject to} \quad & df_{ES_j^{s_i}} \geqslant \alpha_i \\ & df_{FS_j} \geqslant (1 - \alpha_i) \\ & \mathcal{C}_j \leq 1 \end{aligned}$$

$$df_{ES_j} = \frac{ES_j}{maxES_i}$$

$$\mathcal{C}_j = \frac{cost_j}{maxA_j}$$

Implementation and Results





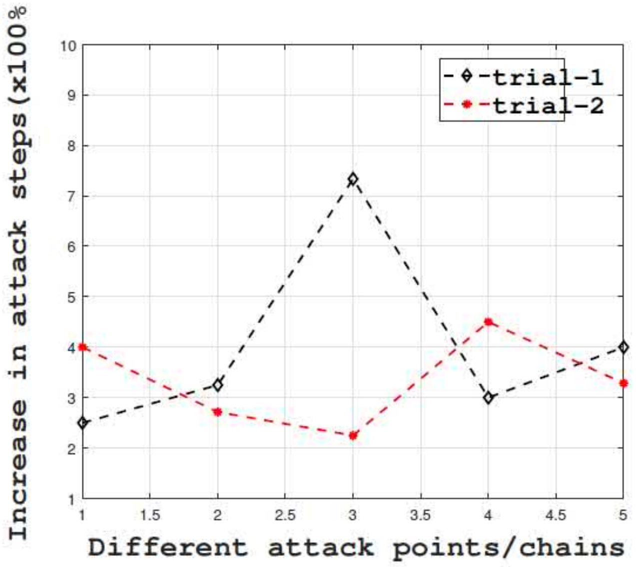


Fig 1: Attacker's evolving characteristics in penetration steps(left) & Performance evaluation of IRS with respect to attack propagation delay(right)

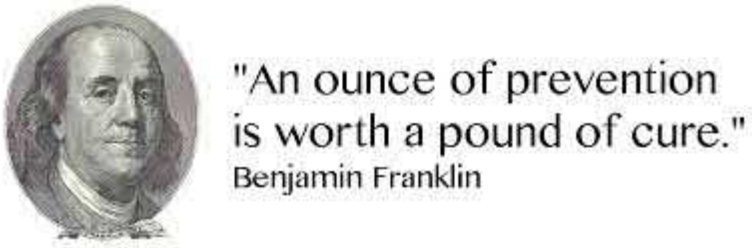
- IEC-62443 architecture including IT, OT and DMZ zones.
- Set PLC and RTU as critical target
- Randomly take initial attackers' position from IT zone

Modeling Attacker’s Capability (SecureComm’19)

Sharif Ullah, Sachin Shetty, Anup Nayak, Amin Hassanzadeh and Kamrul Hasan "Cyber Threat Analysis based on Characterizing Adversarial Behavior for Energy Deliver System", Securecomm, 2019

Kamrul Hasan, Sachin Shetty, Sharif Ullah, Amin Hassanzadeh, Ethan Hadar, " Towards Optimal Cyber Defense Remediation in Energy Delivery Systems", IEEE Globecom, Hawaii, 2019

In Depth APT



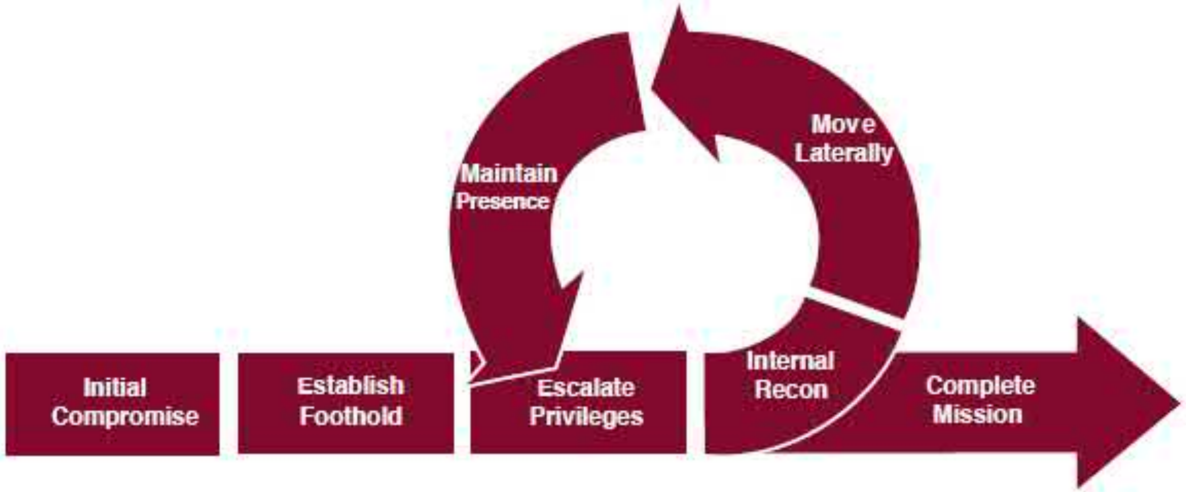
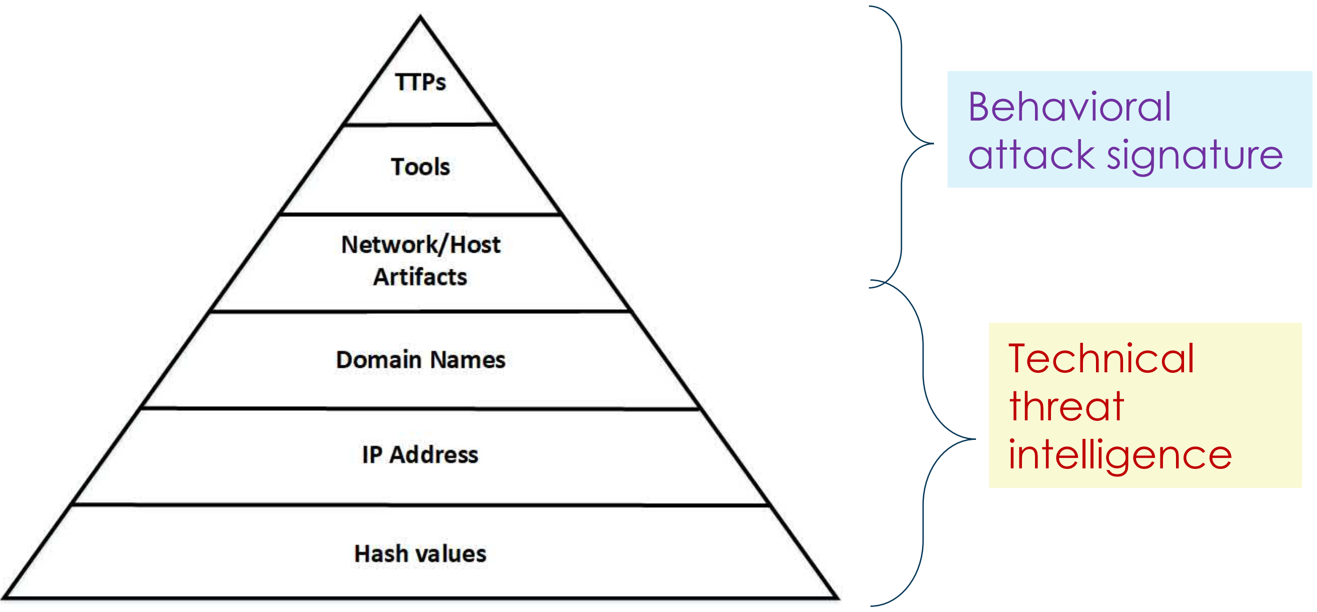


Fig. 1: APT Life-cycle[2]

- Understanding the motivation and operation of APT actors play a vital role.
- Kill chain provides a reference to understand and map APT actors-
  - Targets
  - Motivations
  - Actions

Pyramid of Plain Model



Pyramid of plain model[1]

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting			Multilayer Encryption
Bootkit	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association		Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
				Query Registry	Taint Shared Content				Standard Application Layer Protocol
Component Firmware		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares				
Hypervisor				Security Software Discovery					Standard Cryptographic
Logon Scripts		InstallUtil							
Modify Existing Service		Masquerading		System Information Discovery					
Redundant Access		Modify Registry							
Registry Run [illegible]		NTFS Extended Attributes		System [illegible]					

Tactics: *why* an adversary performs an action

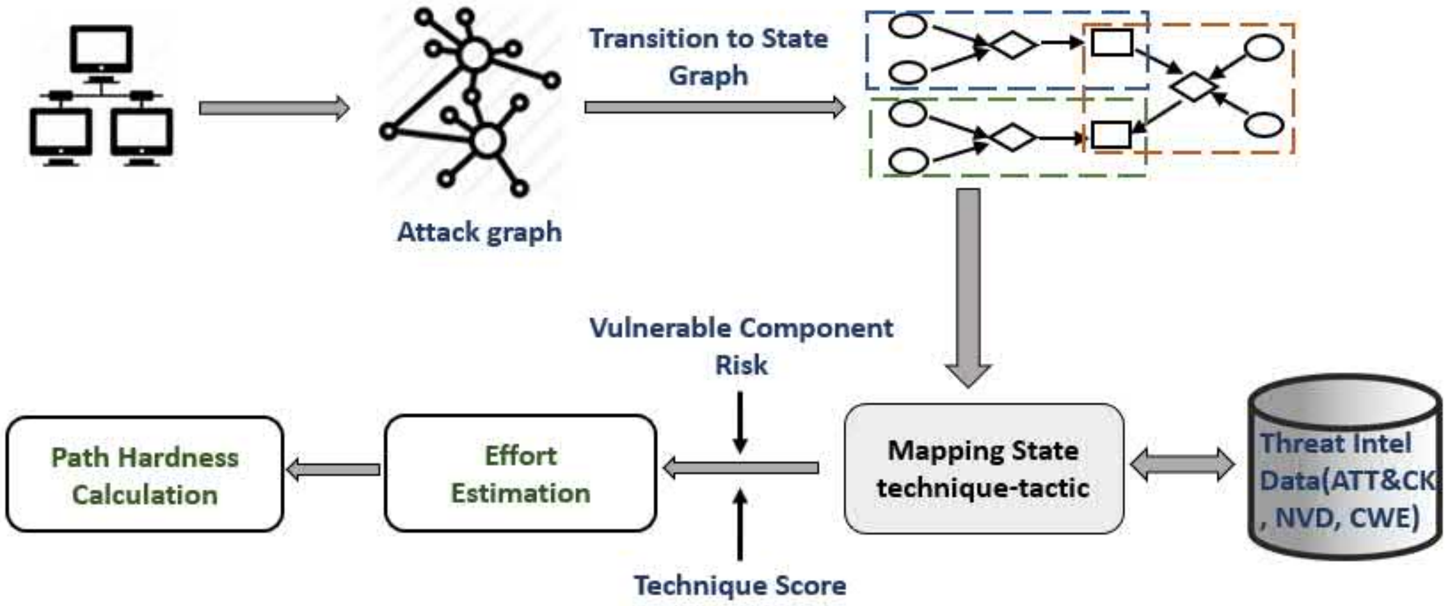
Techniques: *how* they take the action

- Described from both the offensive and defensive points of view

1. D. Bianco. (2014) The pyramid of plain. [Online]. Available: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html dossier.pdf

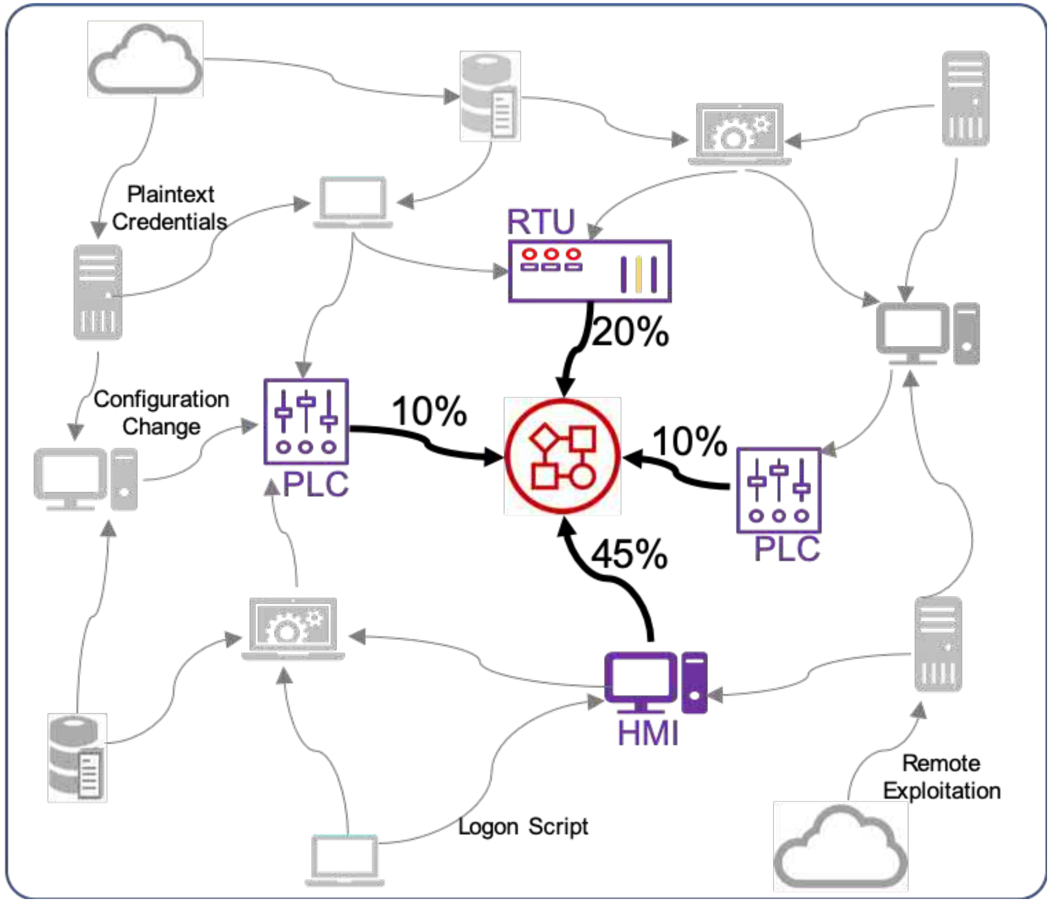
Framework

- ✓ Adding more **context** into each attack phase
  - Network/host artifacts form scanning info, Attack graph
  - TTP from **MITRE, CAPEC** etc.
  - Tools, threat intelligence from attacks in the wild from **iDefense**.



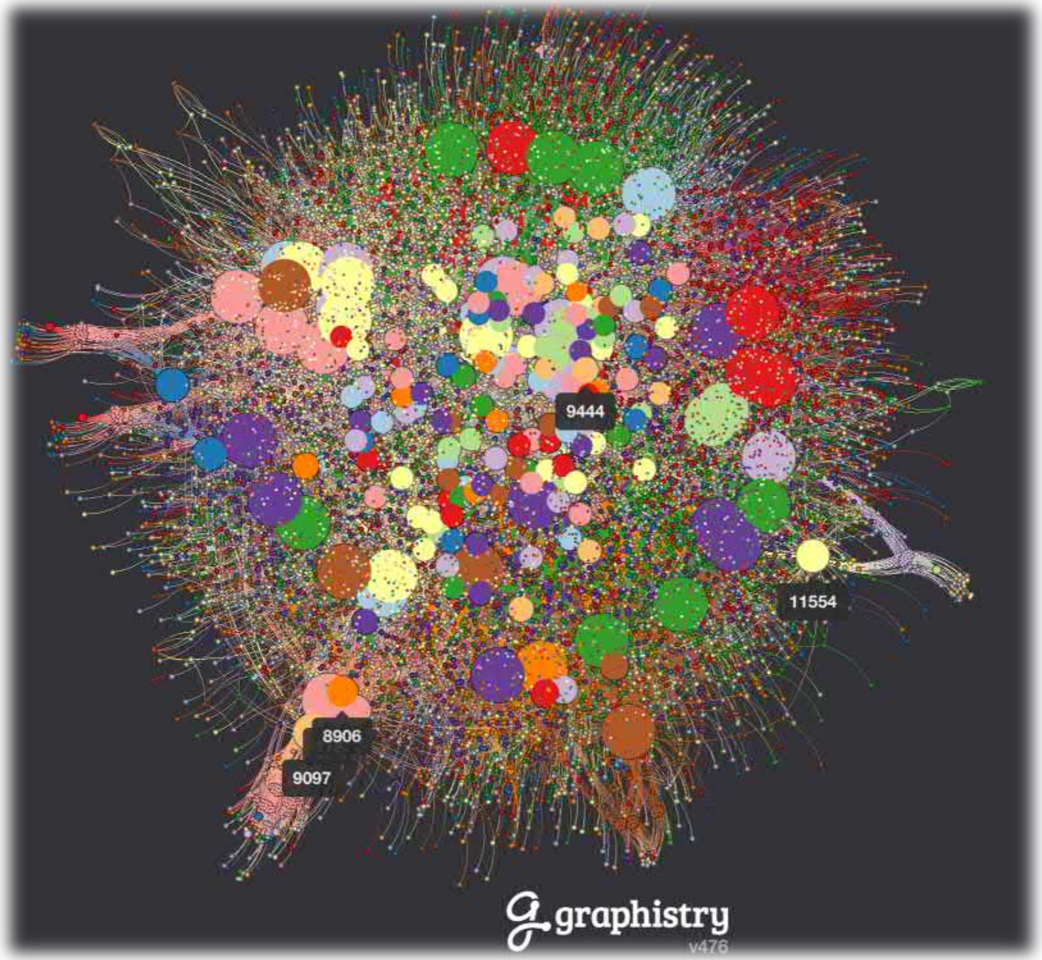
Attack Graph

1. Choose business process with the highest monetized risk
2. Start with highest value critical asset
3. Examine easiest **attack paths** to the asset
4. Fix according to ease of attack and cost of remediation



ATTACK GRAPH
ANALYTICS ENGINE

- What are the possible impacts on asset X?
- What are the possible paths to a target?
- What is the most probable attack path from outside the network to asset X?
- Given a path, what are all the configuration issues across it?
- What asset if compromised, provides more lateral movement options (TTPS) for attacker to proceed?
- How to avoid all possible impacts on a given asset?



Background: Attack Graph

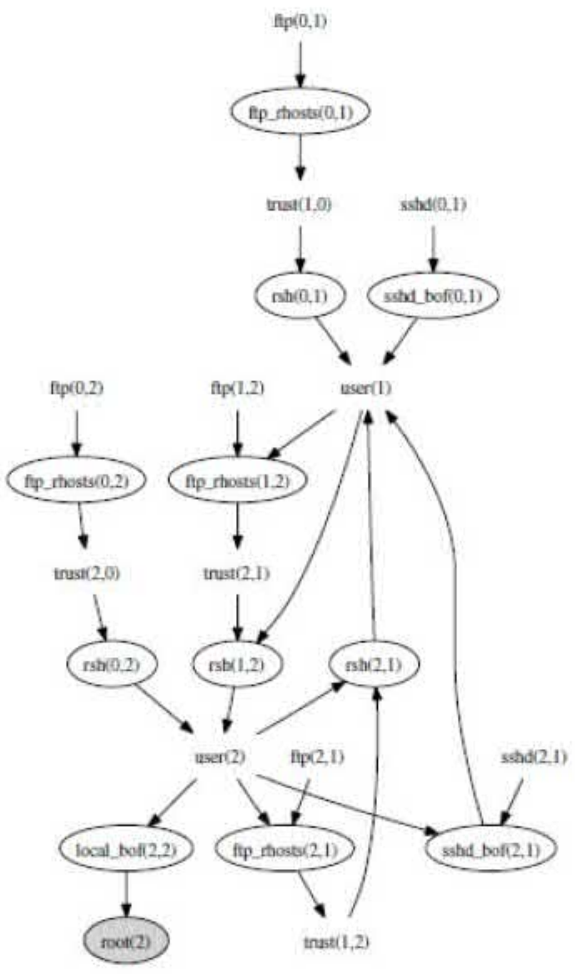
- An attack graph is the mathematical abstraction of details of potential attacks leading to a specific target
- Major two parameters:
    - Node: Probable states
    - Edge: Corresponding changes of states
- Different attack graph model comprised of:
    - Different system parameters
    - Application behaviors
- Multiple use cases in security and risk analysis.

Background: Attack Graph

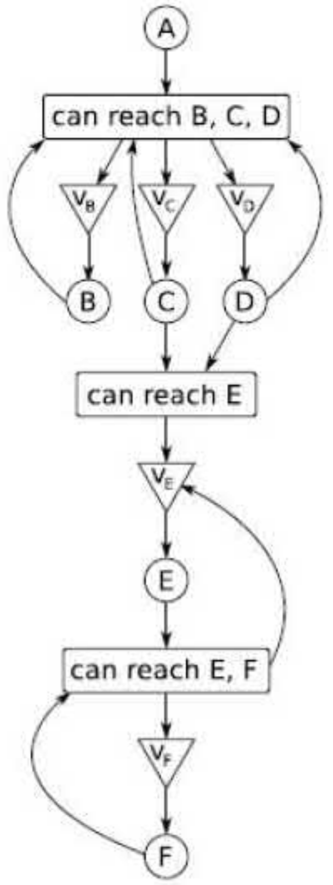
- Different representation of attack graph is proposed
- State enumeration attack graph:
  - Emerged from model checking technique
  - Node represents entire network state
  - Shows all possible attack paths to particular goal attacker state
  - Suffers from state explosion problem
- Dependency attack graph:
  - First comes with exploit dependency attack graph
  - Node → State condition
  - Edge → Causal relationship between conditions
  - # of nodes scales linearly

Background: Attack Graph Models

- Topological Vulnerability Analysis(TVA):
  - Model attacker’s exploit as transition between security conditions
  - Exploit and security condition nodes
- MulVal reasoning engine:
  - Derivation and fact nodes
  - Directed graph
- NetSPA attack graph:
  - Multi-prerequisite attack graph
  - State node, prerequisite node and vulnerability instance node



TVA Attack Graph[1]

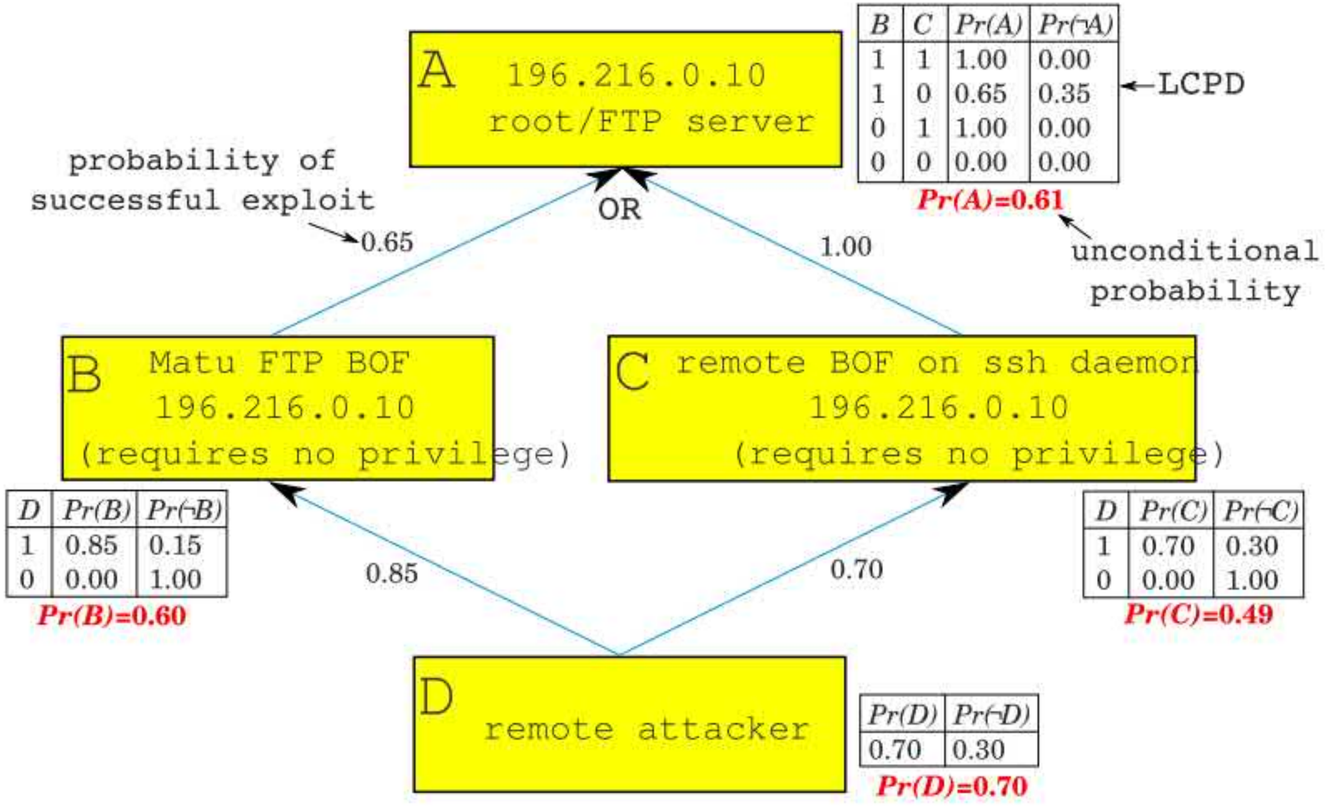


NetSPA Attack Graph[2]

1. Wang, Lingyu, Anoop Singhal, and Sushil Jajodia. "Measuring the overall security of network configurations using attack graphs." In *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 98-112. Springer, Berlin, Heidelberg, 2007.
2. Ingols, Kyle, Richard Lippmann, and Keith Piwowarski. "Practical attack graph generation for network defense." In *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, pp. 121-130. IEEE, 2006.

Background: Bayesian Network (BN)

- Probabilistic graphical model representing variables and relationship between them
- Demonstrate causal dependency between exploits
- Quantify the likelihood of attack goals and predict potential attacks.
- Bayesian attack graph is a directed acyclic graph
- A great analyzer for security under uncertainty



Simple Bayesian Attack Graph[1]

1. Poolsappasit, Nayot, Rinku Dewri, and Indrajit Ray. "Dynamic security risk management using bayesian attack graphs." *IEEE Transactions on Dependable and Secure Computing* 9, no. 1 (2011): 61-74.

Attack Graph and Action State

Advisories
Host Configuration
Network Configuration
Principles
Policy

→ Attack Graph Generator → Attack Graph

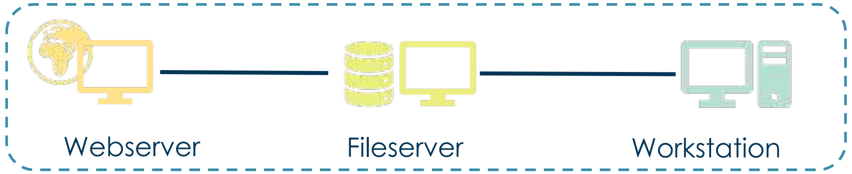
C — **Configuration:** Condition, provide possibilities of action by adversary

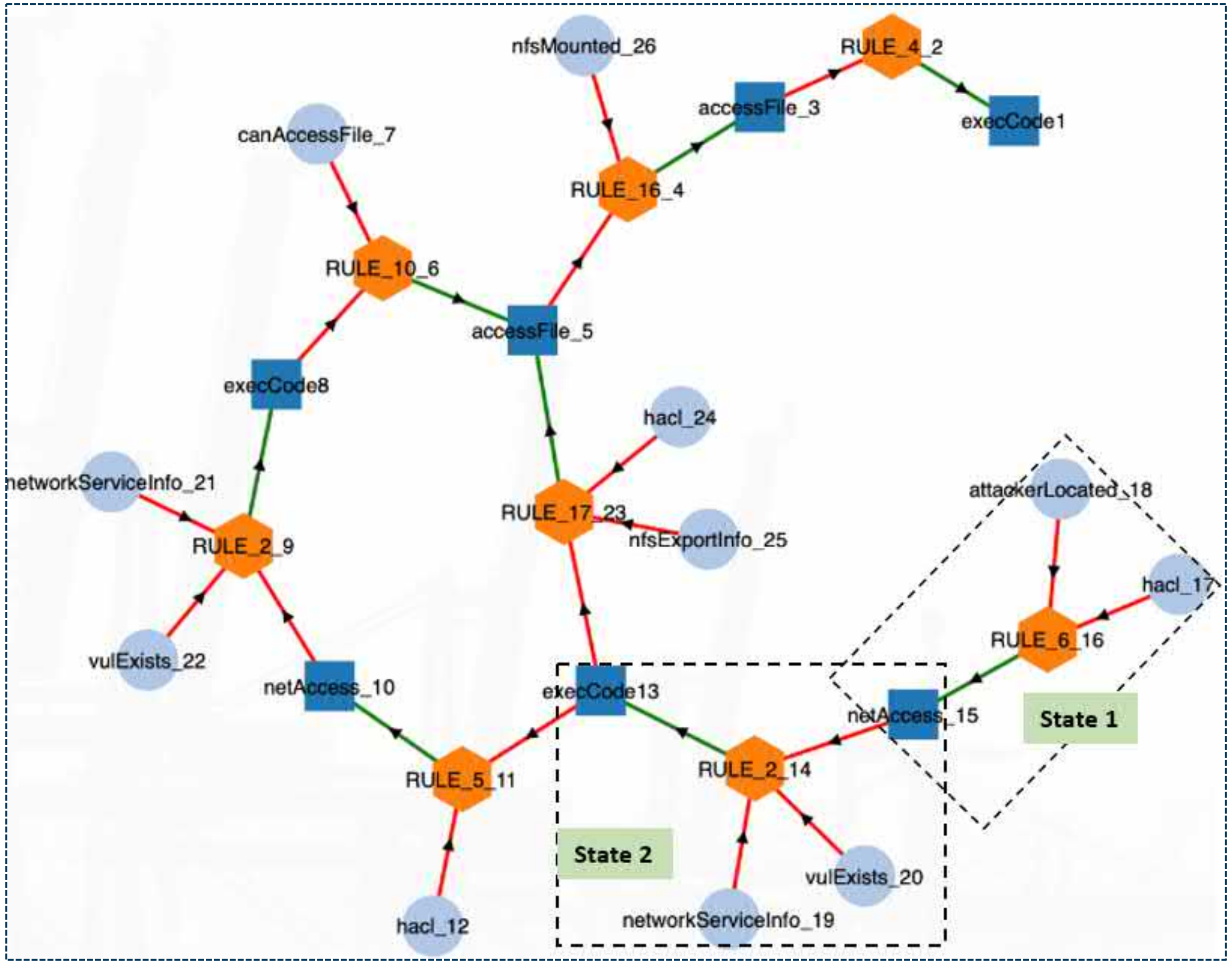
r — **Rule:** Attack methodology attacker can leverage

i — **Impact:** Sub-goal achieved by the former action

- Incorporate conditional dependency to transfer attack graph to state graph
- Action State

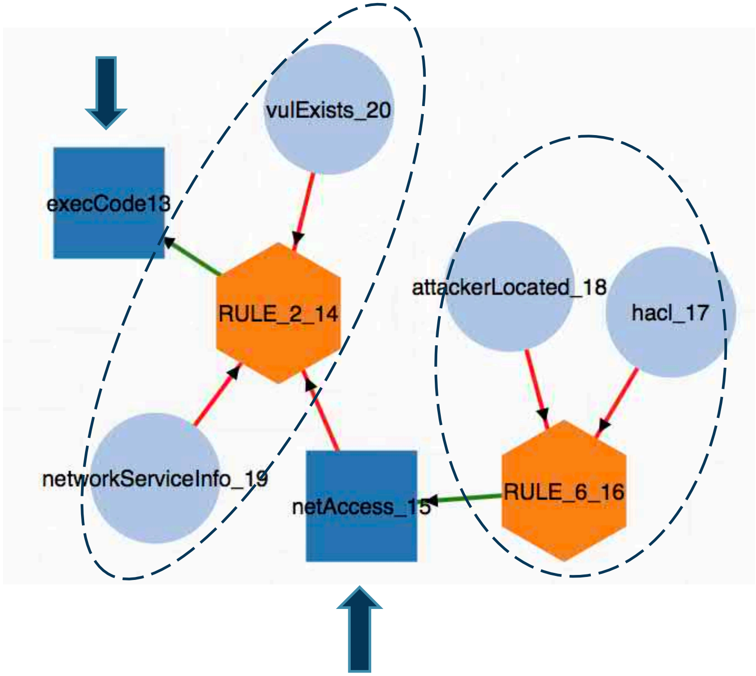
Network Topology





Mapping to Techniques-Tactics

- ✓ We map each action state to distinct Technique-Tactic(TT) pair
- ✓ Unfolds the current phase of attack strategy
- ✓ Each attack path eventually exposes a sequence of TT



- ✓ Mapping Attack State to Technique-tactic:
  - Use ***rule*** and ***configuration*** information to map state to ***technique***
  - ***Impact*** information to map state to ***tactic***
  - Correlated technique pre-requisite in a sequence to improve mapping accuracy

Mapping to Techniques-Tactics

```
netAccess('192.168.15.123',tcp,'1433'):-
    execCode('192.168.15.124',someUser)
    hacl('192.168.15.124','192.168.15.123',tcp,'1433')
rule_desc('multi-hop access')
```

Tactic: *lateral movement*

```
execCode('192.168.15.124',someUser):-
    vulExists('192.168.15.124','CVE-2015-2808',
    safari,remoteExploit,privEscalation)
    networkServiceInfo('192.168.15.124',safari,tcp,
    '1433',someUser)
    netAccess('192.168.15.124',tcp,'1433')
rule_desc('remote exploit of a server program')
```

Tactic: *execution*, Technique- *Exploitation for Client Execution (T1203)*

~~Tactic: *lateral movement*, Technique- *Exploitation of Remote Service (T1210)*~~

```
netAccess('192.168.15.124',tcp,'1433'):-
    attackerLocated(internet)
    hacl(internet,'192.168.15.124',tcp,'1433')
rule_desc('direct network access')
```

Tactic: *initial access*

Initial access → *execution* → *lateral movement*

Path Complexity and Effort Estimation

- High CVSS base score doesn't exhibit the risk
- 14% of the vulnerable hosts are patched when exploits are released publicly
- 15% of known vulnerability exploited in the wild

Intrinsic Skill

Correlation Coefficient Calculation:
- Attack Method Correlation
- Environmental Correlation

Vulnerable Component Risk

Hardness of Path

Technique Priority:
- Adaptability
- Exploitation

Exploitability level	Likelihood level		
	Unproven	Proof-of-concept	Exploit in the wild
Easy	3	4	7
Medium	2	3	5
Hard	1	2	4

Path Complexity and Effort Estimation

- **Vulnerable Component Risk**:
  - *Unproven*
  - *Proof of concept*
  - *Exploited in the wild*

Table 1: Vulnerable component risk matrix

Exploitability level	Likelihood level		
	Unproven	Proof-of-concept	Exploit in the wild
Easy	H	MH	VH
Medium	M	H	MH
Hard	VL	L	M

✓ Technique Priority Score:

- **Two factors considered.**
  - ***Adaptability***: depends on the environment and conditions allowing a technique to be exercised.
  - ***Exploitation:*** Depends on how it has been manifested in real world.

$$ASc(ta_t) = pl_t \times \sum_{i=1}^{p} pr_i^t \times \tau_t$$

$$ExSc(ta_t) = sf_t \times gr_t$$

$$TSc(ta_t) = \beta ASc(ta_t) + (1 - \beta) ExSc(ta_t)$$

Path Complexity and Effort Estimation

- ❖ **Correlation Coefficient Calculation**:
  - State integrated with ATT&CK, NVD, CWE
  - Track attacker's evolving skill

$$CC_{x,y} = \underbrace{AMCC_{x,y}}_{\text{Attack method correlation}} + \underbrace{ENCC_{x,y}}_{\text{Environmental correlation}}$$

- ✓ **Hardness of Path:**
  - State hardness is defined as a function of two parameters
  - Decay factor (λ) represent the effort reduction in similar ac

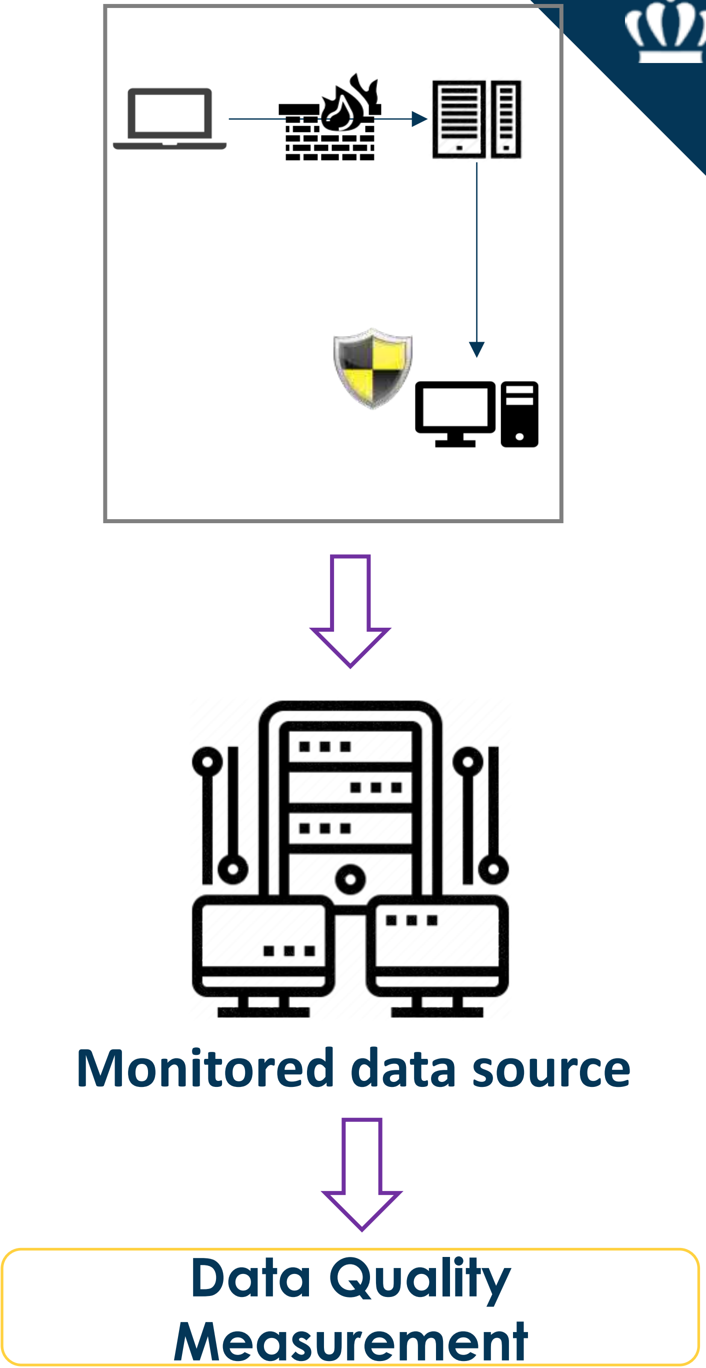
$$H_{P^k_{j,j'}} = \sum_{i \in \mathcal{AS}_{P^k_{j,j'}}} \underbrace{H_{as_i}(intr)}_{\text{Intrinsic hardness}} * \underbrace{H_{as_i}(corr)}_{\text{Correlated hardness}}$$

$$H_{P^k_{j,j'}} = \sum_{i \in \mathcal{AS}_{P^k_{j,j'}}} \underbrace{(\alpha_i^{-1} + TSc(ta_t)^{-1})}_{\text{Criticality of the state}} \underbrace{e^{-\sum^{i}_{q=\mathcal{AS}_{P^k_{j,j'}}(0)} \frac{CC_{iq}}{\lambda}}}_{\text{Effort reduction}}$$

Path Stealthiness

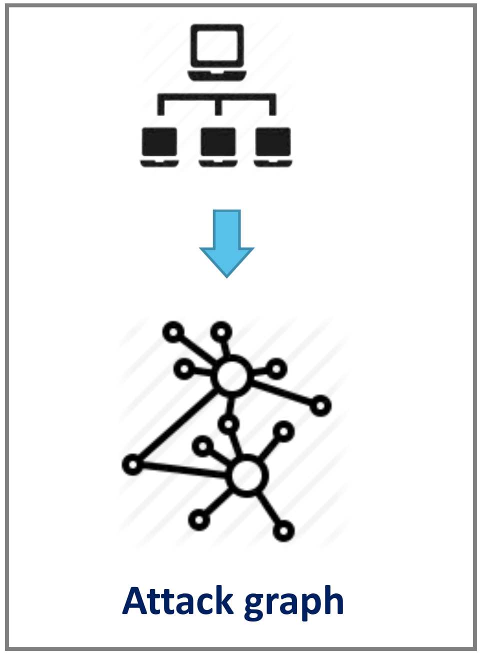
- Hypothesis behind the stealthiness: The more isolation a path introduces –
  - More detectable by the defender
  - Less exploitable by the attacker
- Adversary Categorization:
  - Persistent or goal specific adversary (tailored attack)
  - Different constraint (time, resource etc.) bounded adversary (commodified attack)
- **Strategic** plan through attack graph help to find the motive of attacker.

- Data Quality parameters (DeTTECT):
  - Data Field Completeness: Indicates to what degree the data has the required information/fields as well data in the field
  - Timeliness: Indicate how accurate the timestamp of the data corresponding to the actual time an event occurred.
  - Consistency: Indicate the correlation with other data sources in terms of data field names and types.



Path Stealthiness Calculation

- Operation Pipeline:
  - Generate Attack graph (AG) from network
  - Identify security control
  - Identify data sources monitored by security control
  - Map data sources to AG analytics
  - Path stealthiness calculation



Isolation Pattern	Security Control
Access Control	Firewall, Proxy server, Egress filter
Secure Communication	VPN, SSL, IPSec
Authentication	Identity and Access Management System, ISE
Payload Inspection	HIDS, NIDS, Log auditing, Anomaly Detection
Deception	Honeypot, Honeynet, NAT

Stealthiness of Path: $S^{th}_{P^k_{j,j'}} = S^{th}_{as_1} + S^{th}_{as_2} + \ldots\ldots + S^{th}_{as_m} = \sum_{i=1}^{m} S_{as_i}$

$$S^{th}_{as_i} = \frac{\sum_k\{(z^k_{as_i} \times \omega^k_{as_i}) + dQ^k\}}{|SC_{as_i}|} \qquad S^{th}_{P^k_{j,j'}} = \sum_{i \in AS_{P_{j,j'}}} S^{th}_{as_i}$$

$\omega^k_{as_i}$ =Security Control *k* deployed in action state as_i

SC_{as_i} =Required Security Control in as_i

$dQ^k_{as_i}$ =Data quality of Security Control *k* deployed in action state as_i

Additional Analytics:

Additional analytics using the Framework

Investigate critical data sources:

- Detect additional exploited techniques
- Determine new attack paths
- Monitored frequently in the attack graph and determine mitigation plan for attack paths

Map critical data sources into security control to effective security control

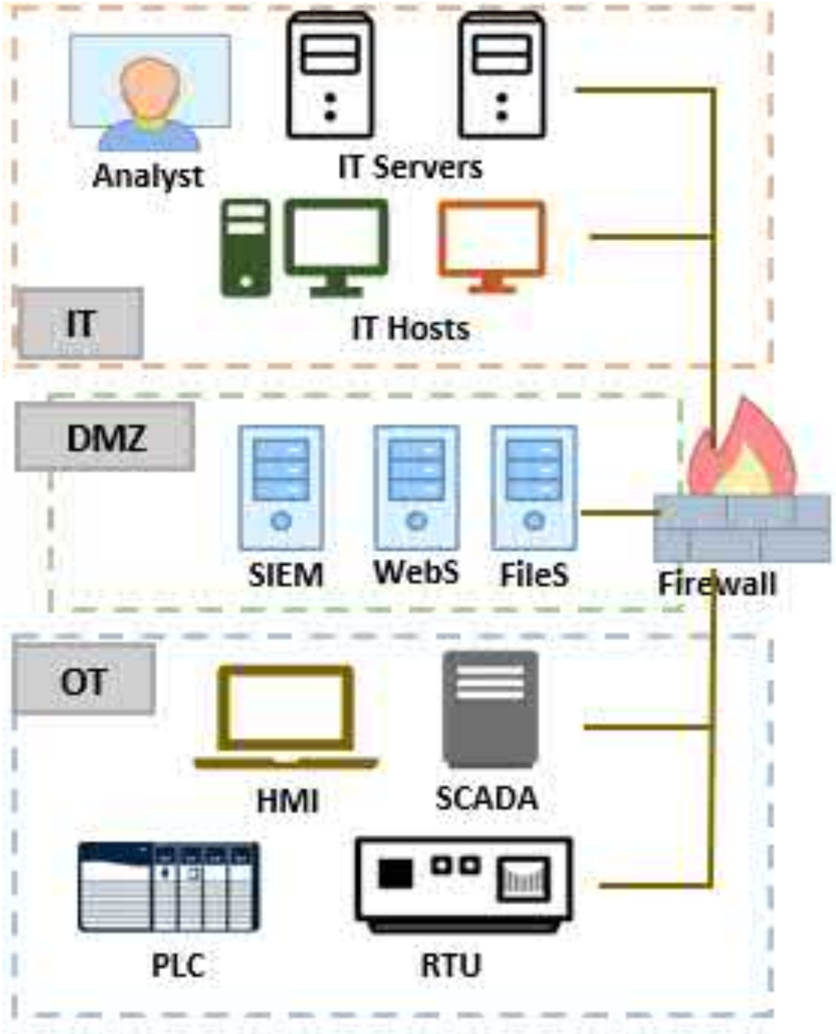
Cyber Analytics Repository (CAR)

MITRE

- Impose more granular information from data sources
- Each data model is comprised of {object/action/ field} e.g., {driver, file/ load, create / md5_hash, pid }
- Extract unique data model which should be monitored to prevent all ATT&CK techniques from exploitation

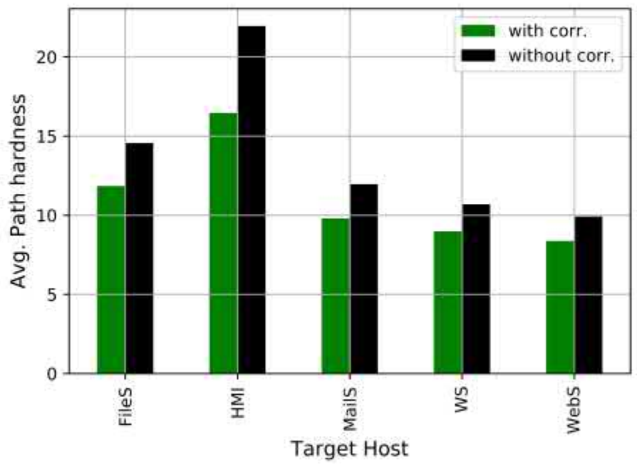
Prioritize the defense.

Validation on ICS

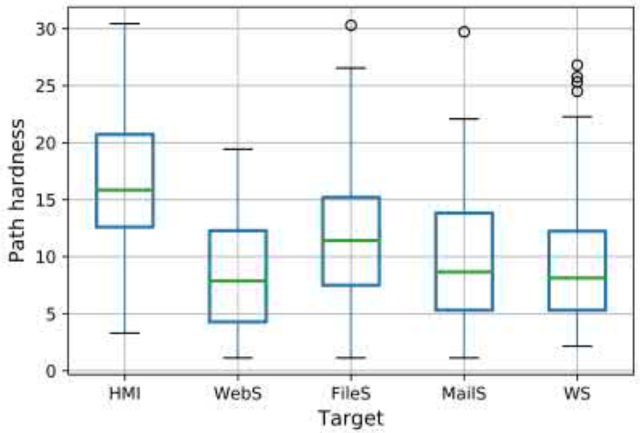


Accenture ICS Testbed

- Active scanning with Nessus for IT network
- Passive scanning with Grassmarlin and ClarOty for OT network.
- Extract attack paths terminating into multiple targets

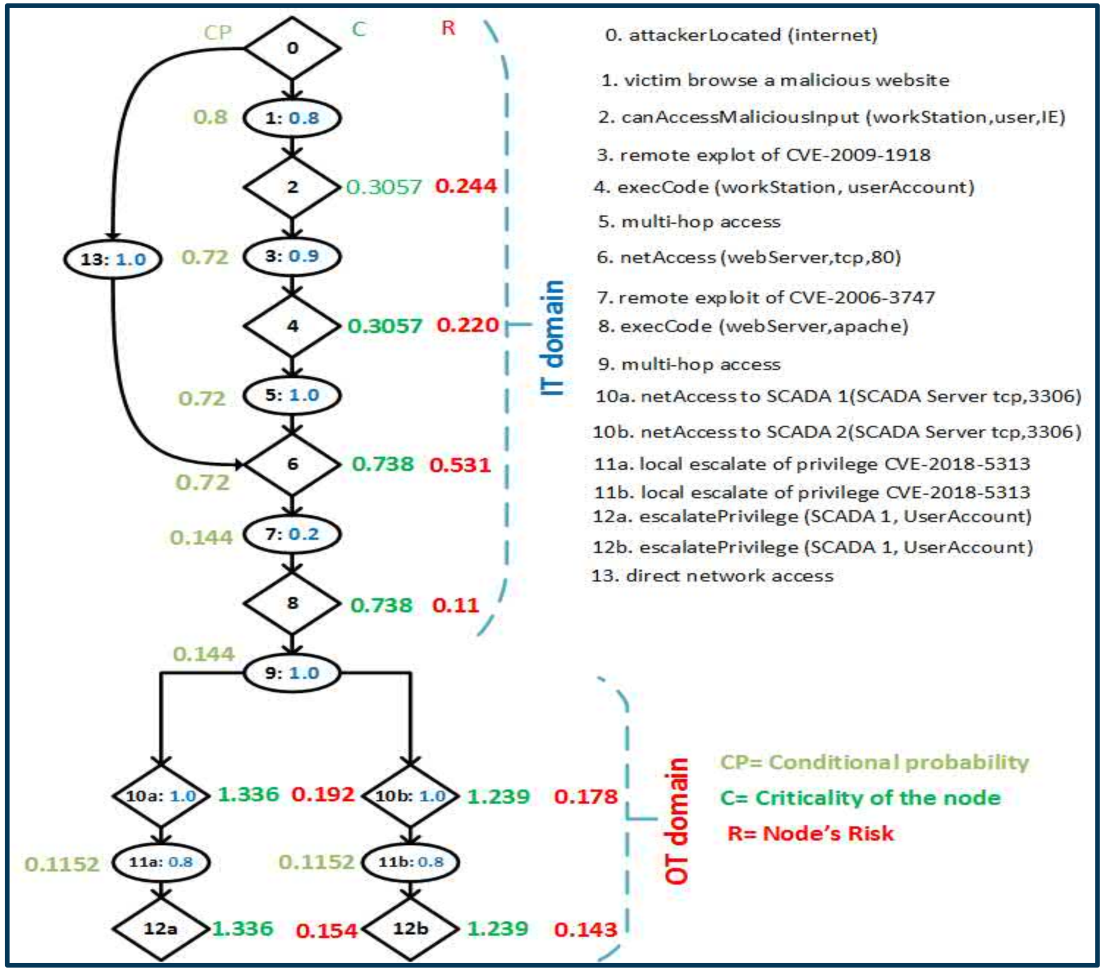


Deviation of Path Hardness



Distribution of Attack path

Attack Graph and Criticality Analysis



- *Attack Paths*: $0 \to 1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 7 \to 8 \to 9 \to 10a \to 11a \to 12a; 0 \to 13 \to 6 \to 7 \to 8 \to 9 \to 10a \to 11a \to 12a$ - **SCADA1 (target).**
- *Attack Paths*: $0 \to 1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 7 \to 8 \to 9 \to 10b \to 11b \to 12b; 0 \to 13 \to 6 \to 7 \to 8 \to 9 \to 10b \to 11b \to 12b$ **SCADA2 (target).**
- Though paths have identical exploitation probability from attacker starting node to SCADA1/SCADA2, the damages along the paths are different.
- Attacker has opportunity to analyze options and select the path that can make the most damage to the target

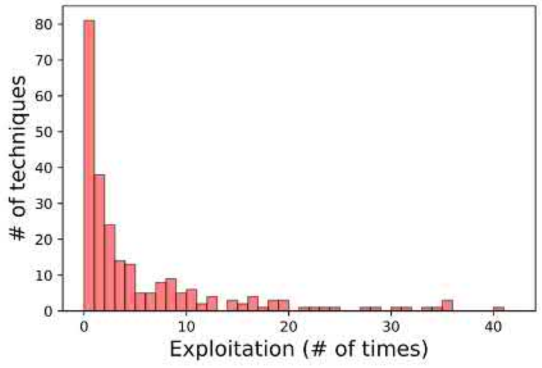
Modeling Attacker’s Intent

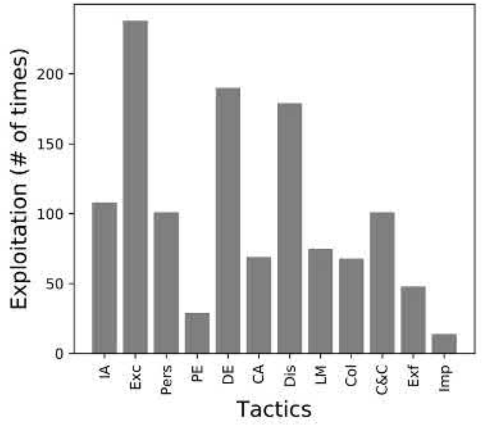
Charles Kamhoua, Alexander Kott, Laurent Njilla, Sachin Shetty**,** “Modeling and Design of Secure Internet of Things”, John Wiley &Sons, 1 edition, 2020, ISBN 978-1-119-59336-2

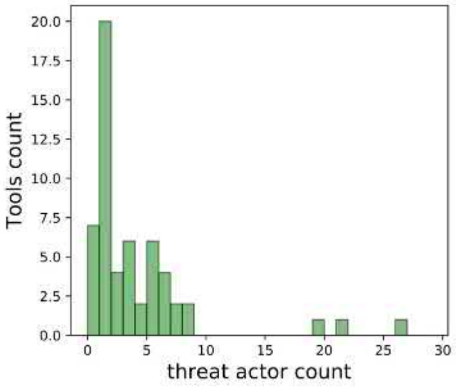
Goal

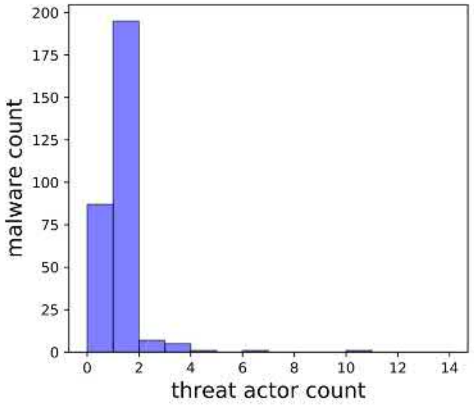
- Understand adversary Strategy
- Predict attackers' movement into the system using TTP Chain
- Observe suspicious activity and predict future action

Threat Actor Insight from MITRE

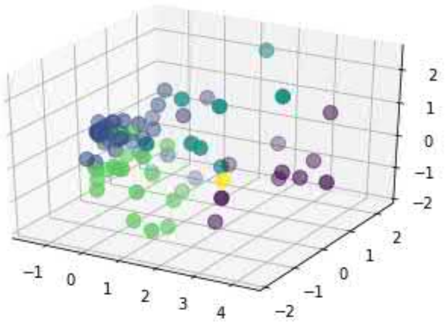




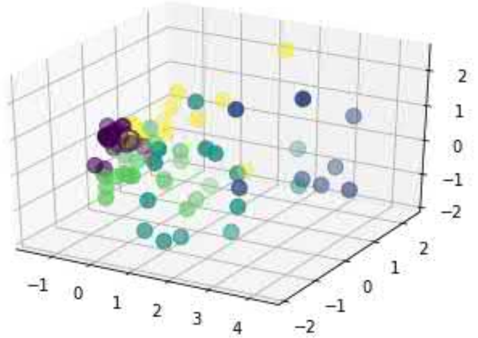




PCA + K-means clustering

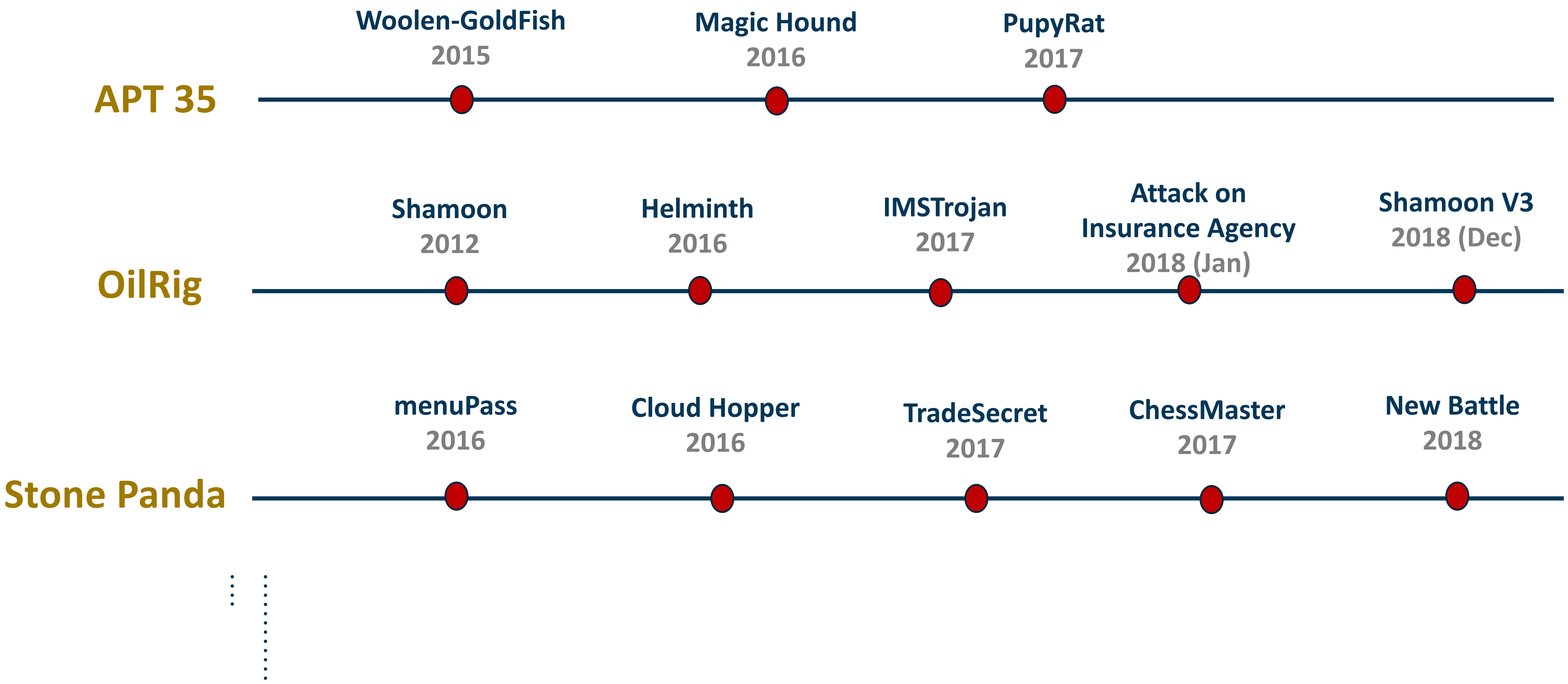


Threat Actor Cluster based on Technique



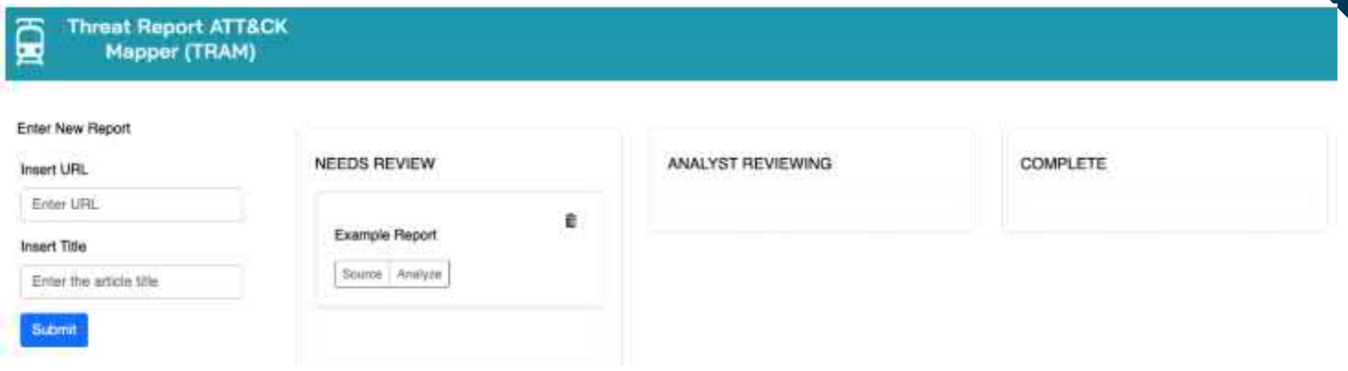
Threat Actor Cluster based on Tactic

Threat Campaign Information



Ongoing efforts

- The **Threat Report ATT&CK Mapper (TRAM)** is a web-based tool from MITRE to analyze report and extracting ATT&CK technique.
- It takes the procedure example from ATT&CK to train the model.
- Use logistic regression with tokenized data to match the technique to the report

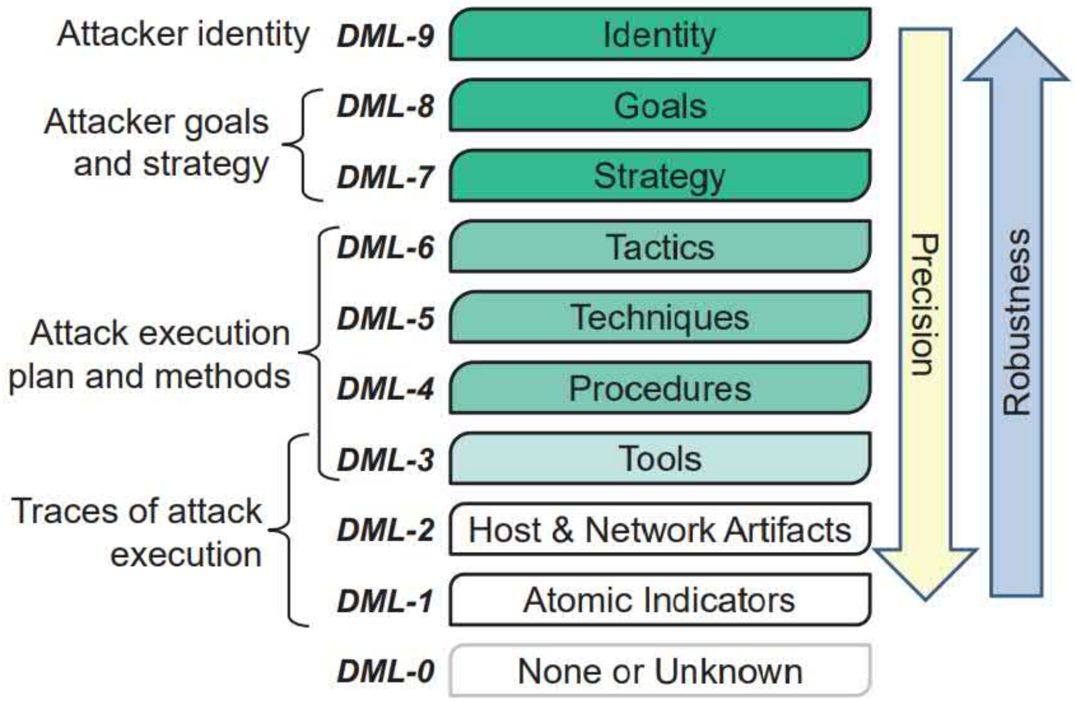


Limitation--

- A beta release. Needs analyst review for better accuracy.
- It only used count vectorizer for feature extraction which could embed lot’s of noisy data during training.
- It failed to extract the context of each technique could turn out error prone result.

Attack life cycle and defense strategy

Attack Life Cycle in APT Progression



Detection Maturity Level model

Threat Intelligence Sources

Symantec

Symantec Security Response

View Profile

Symantec Official Blog

+6
6 Votes

Sowbug: Cyber espionage group targets South American and Southeast Asian governments

Group uses custom Felismus malware and has a particular interest in South American foreign policy.

By: Symantec Security Response SYMANTEC EMPLOYEE

APT REPORTS

MuddyWater expands operations

By GReAT on October 10, 2018. 10:00 am

CONTENTS

Summary

n conducting highly targeted cyber attacks
avily focused on foreign policy institutions and
stealing documents from the organizations it

and Saudi
untries in

FIREEYE Solutions Services Customers

Home > FireEye Blogs > Threat Research > Pick-Six: Intercepting a FIN6 Intrusion, an Actor ...

Threat Research

Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware

April 05, 2019 | by Brendan McKeague, Van Ta, Ben Fedore, Geoff Ackerman, Alex Pennino, Andrew Thompson, Douglas Bienstock

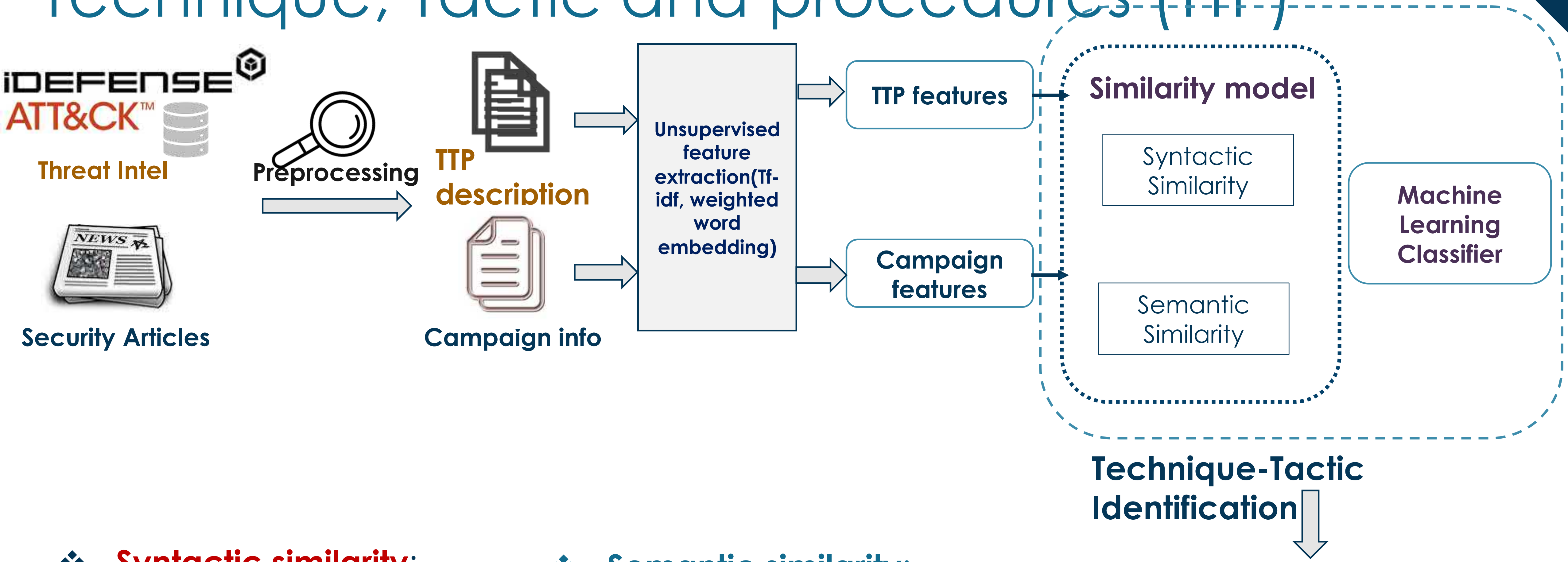
RANSOMWARE MANAGED DEFENSE FIN GROUP

CROWDSTRIKE | BLOG Featured

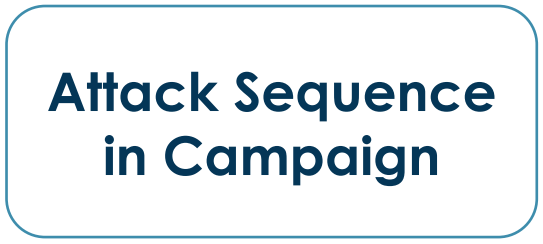
Deep in Thought: Chinese Targeting of National Security Think Tanks

July 7, 2014 Dmitri Alperovitch Executive Viewpoint

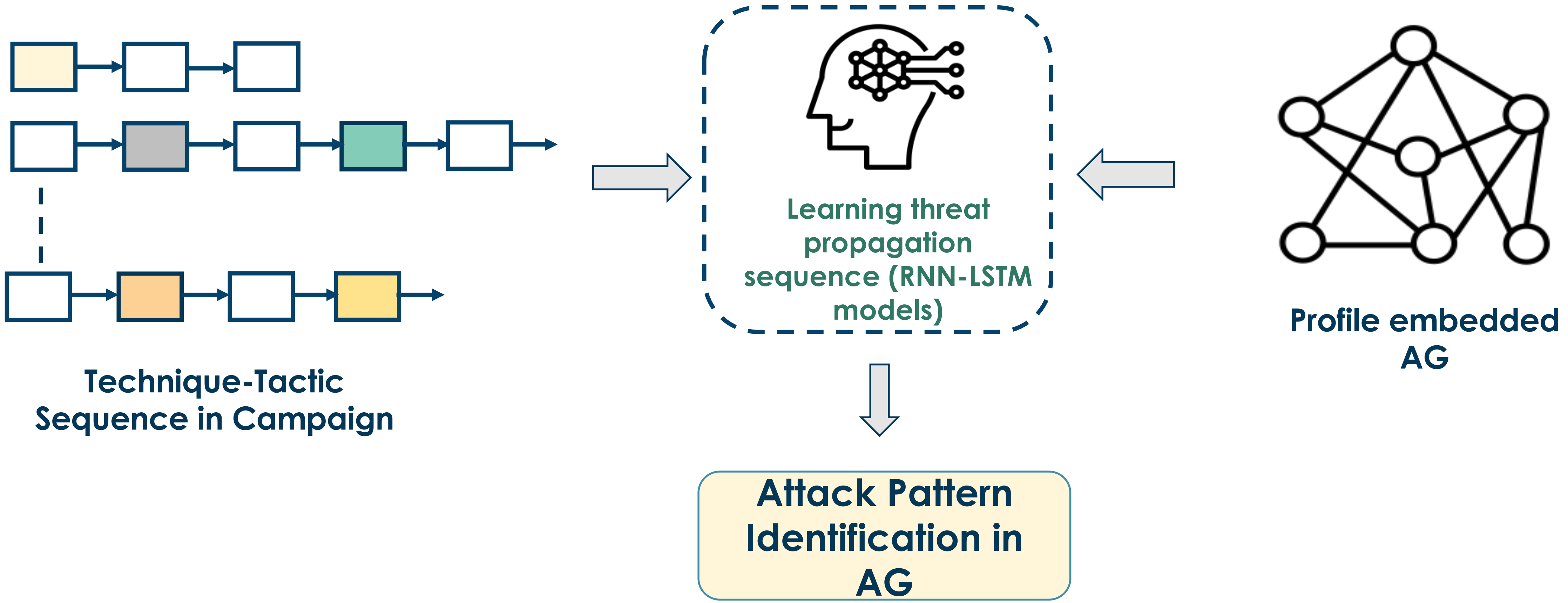
NLP Approach to Identifying Adversarial Technique, Tactic and procedures (TTP)



- **Syntactic similarity:**
  - TF-IDF/Tf-IGM + Cosine Similarity
- **Semantic similarity:**
  - Embedding method+ Similarity



Threat Propagation Sequence Analysis



Data Preprocessing

The encoded payload was a Cobalt Strike httpsstager that was injected into the PowerShell process that ran the command. The Cobalt Strike httpsstager was configured to download a second payload from hxxps://176.126.85[.]207:443/7sJh. FireEye retrieved this resource and determined it was a shellcode payload configured to download a third payload from hxxps://176.126.85[.]207/ca. FireEye was unable to determine the final payload due to it no longer being hosted at the time of analysis.

Second technique: FIN6 also leveraged the creation of Windows services (named with a random 16-character string such as IXiCDtPbtGWnrAGQ) to execute encoded PowerShell commands. The randomly named service is a by-product of using Metasploit, which creates the 16-character service by default. The encoded command contained a Metasploit reverse HTTP shellcode payload stored in a byte-array like the first technique. The Metasploit reverse HTTP payload was configured to communicate with the command and control (C2) IP address

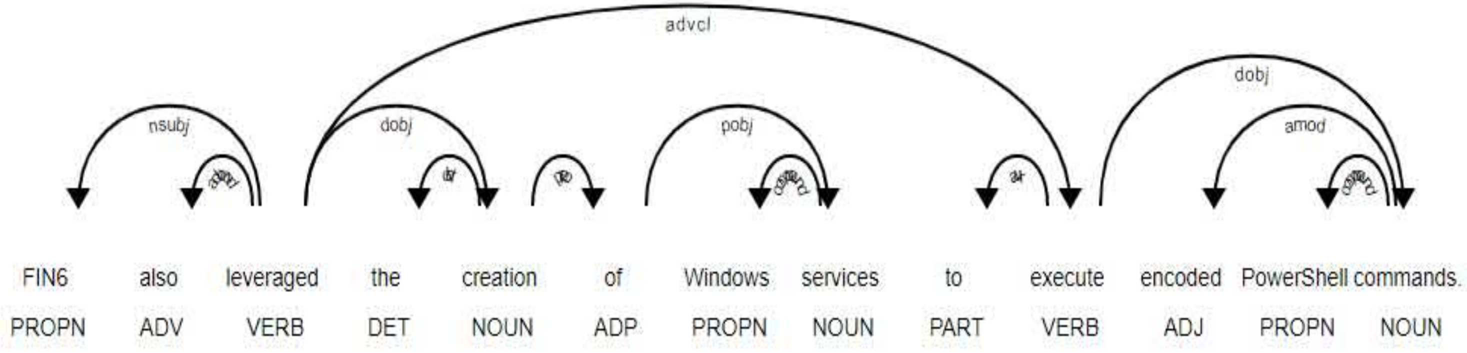
Feature

Indicator of compromise (IoC)

Noise + Stop words

- **Data Scraping and Preprocessing:**
  - Extract unstructured text data from web (threat reports) and MITRE (threat intel)
  - Initially remove noise from the text like advertisement and other unnecessary information by regular expression
  - Perform Stemming and Lemmatization: the process of reducing inflection of words in their roots form belong to the dictionary form as well
  - Remove Stop words
  - Initially extract features by dependency

Dependency Parsing



Techniques Extraction

$$tf - idf = tf(t,d) * \log(N/(df + 1))$$

$$df = Occurance\ of\ t\ in\ docuemnts$$

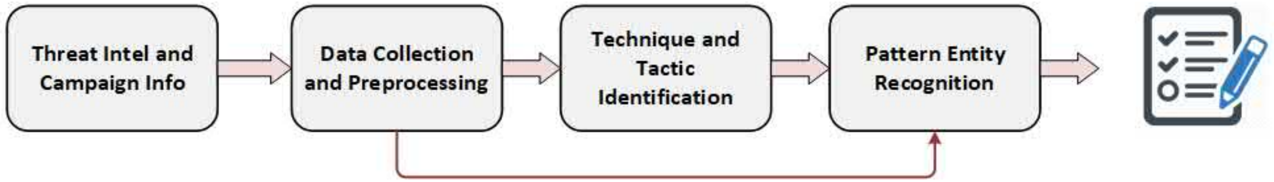
$$t - term(word), d - document(set\ of\ words), N - count\ of\ corpus, corpus$$

- We extract potential adversary techniques from the threat reports
- TF-IDF is used to put weight on each feature we previously extracted by dependency parsing.
- $TF - IDF = Term\ frequency * Inverse\ Document\ Frequency$
- This process signifies the importance of words in the document and corpus.
- In our model, we investigate which TTP features are more important for a particular technique than others.
- Then cosine similarity is used to measure cosine angle of two vectors
  - TTP feature vectors from threat intel
  - Campaign feature vectors from threat report
- Result shows some of the techniques probability based on our analytics on a specific threat report.

$$\text{similarity} = \cos(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\| \|\mathbf{B}\|} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \sqrt{\sum_{i=1}^{n} B_i^2}}$$

Application Window Discovery	0.079472
Binary Padding	0.249444
Fallback Channels	0.253859
System Service Discovery	0.121529
File System Logical Offsets	0.039606
Data from Local System	0.118763
Winlogon Helper DLL	0.133888
Credential Dumping	0.199588
Data Compressed	0.106594
Data Obfuscation	0.280427

Tool Architecture



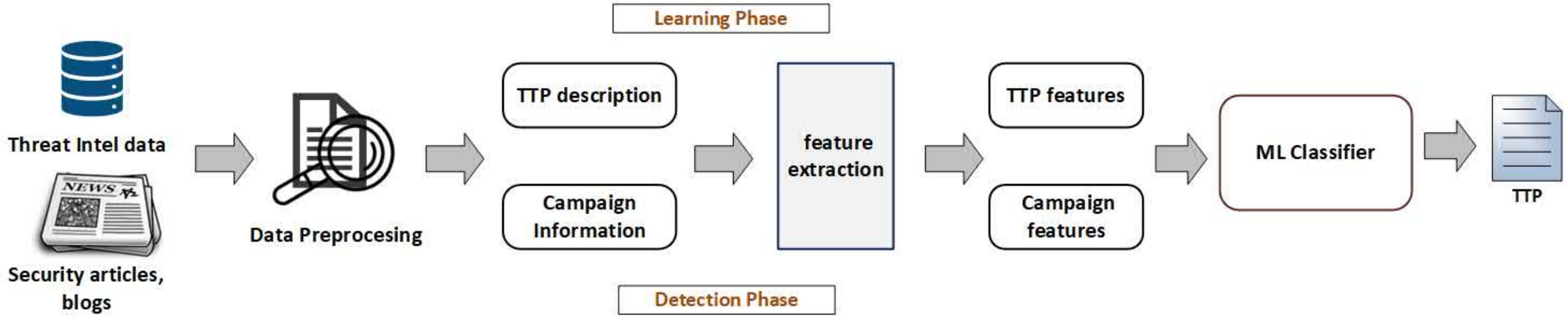
Adversarial Attack Pattern Learning Pipeline

- Multistage learning pipeline to mine threat intel resources to unfold attack pattern
- Convert every letter to lowercase an stopwords like ‘for’, ‘the’, ‘to’ tc.
- Reduce noise- , ; : .
- Trun the word in root form
- Multi-word frequently co-occur together- tokenize together

Data Collection and Preprocessing

Multi-word Expressions
white lambert, peppy trojan, moonwind rat, royal dns, metasploit stager, black lambert, sakula rat, googledrive rat, apt3 keylogger, havex rat, poison ivy, byebye shell, blue lambert, cobra carbon system

Technique-tactic Identification



Feature Extraction- Bag of words

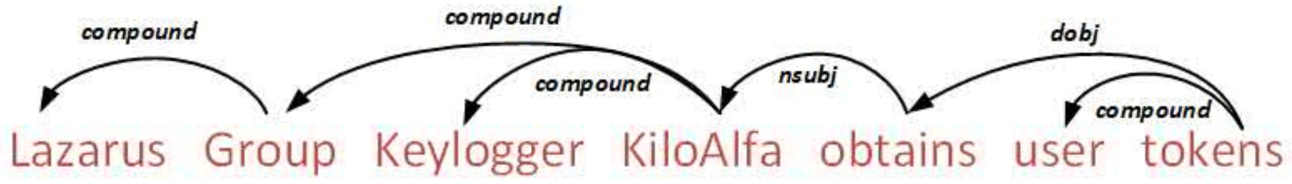
- Form One-hot vector corresponding to every term
  - Term frequency Inverse document frequency (Tf-IDF): $f_{t,d}$ *is* number of times the term appear t in document d

$$TF - IDF_{t,d} = tf_{t,d}.log\frac{N}{df_t}$$

  - Term frequency Inverse gravity Moment (TF-IGM): $f_{k,r}$ frequency of term occurring t_k in different class, which sorted in descending order, r is the rank

$$igm(t_k) = \frac{f_{k1}}{\sum_{r=1}^{n} f_{kr}.r}$$

Feature Extraction- Sentence Embedding



- Normalize the word vectors in the sentence
- Two types of word embedding is used-
- Glove Embedding- Global word-word co-occurrence matrix
- Dependency based embedding – Use Skip Gram model. Linear context to arbitrary context

Words	Contexts
Lazarus	Group/$compound^{-1}$
Group	KiloAlfa/$compound^{-1}$
Keylogger	KiloAlfa/$compound^{-1}$
KiloAlfa	Group/$compound$, Keylogger/$compound$, obtains/$nsubj^{-1}$
obtains	KiloAlfa/$nsubj$, tokens/$dobj^{-1}$
user	tokens/$compound^{-1}$
tokens	obtains/$dobj$, user/$compound$

Technique and Tactic Classification

Model	Features	Accuracy LR/SVM	Precision LR/SVM	Recalls LR/SVM	F1-Score LR/SVM
Bag of Words	Tf-IDF	51.72(cos sim)	-	-	-
	Tf-IGM	53.83(cos sim)	-	-	-
Word Embedding (Glove)	Universal	58.63/54.28	58.24/56.41	58.63/54.28	56.39/53.9
	Universal(Tf-IDF Weighted)	72.65/65.57	74.62/69.95	72.65/65.57	71.68/65.23
	Pre-trained	54.69/53.60	53.50/54.55	54.69/53.60	52.31/52.17
	Pre-trained(Tf-IDF Weighted)	74.01/66.12	74.60/70.56	74.01/66.12	72.38/65.72
Dependency based Embedding	Pre-trained	49.79/45.17	48.95/47.24	49.79/45.17	46/44.46
	Pre-trained(Tf-IDF Weighted)	47.75/46.53	45.82/46.69	47.75/46.53	43.66/44.59

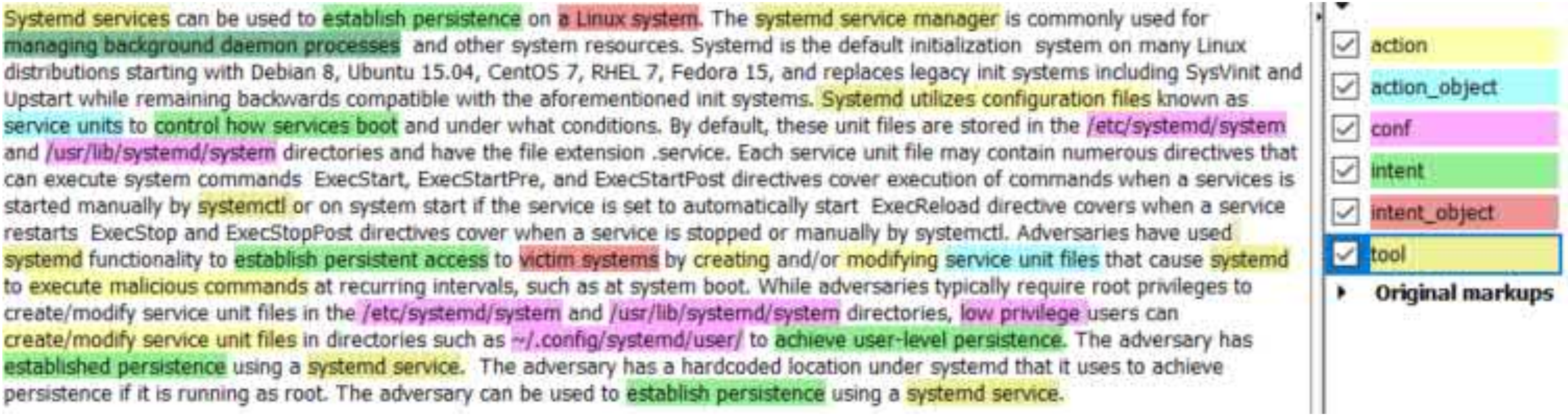
- BoW formed a very sparse vector- cosine similarity used
- Universal – trained on general corpus
- Pre-trained- trained on our corpus
- 6600 sentence for training and 1050 for testing
- Topical dependency is more relevant than functional dependency
- High dimension turns out more distinct feature

Dimensions	Accuracy	Precision	Recalls	F1-Score
50	65.03	69.77	65.03	64.77
100	69.25	72.72	69.25	68.40
300	72.65	74.62	72.65	71.68

Performance with different word embedding dimension (Glove)

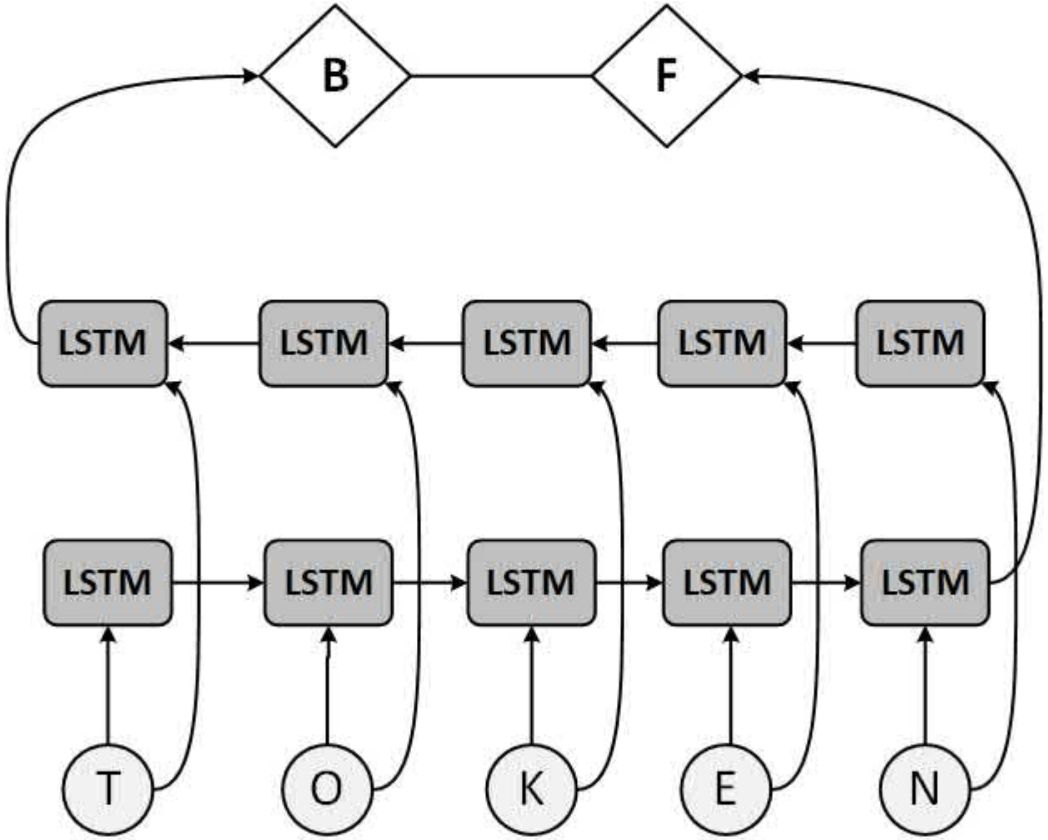
Pattern Entity Recognition- Annotation

Label	# Description
O	Does not contain useful information
Action	Action performed in cyber campaign
Intent	Motive of an action
Tool	Utilities and tools used in cyber campaign
Conf	Configuration facilitate malicious action
Action Object	Surface of action
Intent Object	Surface of potential action or objective


Systemd services can be used to establish persistence on a Linux system. The systemd service manager is commonly used for managing background daemon processes and other system resources. Systemd is the default initialization system on many Linux distributions starting with Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15, and replaces legacy init systems including SysVinit and Upstart while remaining backwards compatible with the aforementioned init systems. Systemd utilizes configuration files known as service units to control how services boot and under what conditions. By default, these unit files are stored in the /etc/systemd/system and /usr/lib/systemd/system directories and have the file extension .service. Each service unit file may contain numerous directives that can execute system commands ExecStart, ExecStartPre, and ExecStartPost directives cover execution of commands when a services is started manually by systemctl or on system start if the service is set to automatically start ExecReload directive covers when a service restarts ExecStop and ExecStopPost directives cover when a service is stopped or manually by systemctl. Adversaries have used systemd functionality to establish persistent access to victim systems by creating and/or modifying service unit files that cause systemd to execute malicious commands at recurring intervals, such as at system boot. While adversaries typically require root privileges to create/modify service unit files in the /etc/systemd/system and /usr/lib/systemd/system directories, low privilege users can create/modify service unit files in directories such as ~/.config/systemd/user/ to achieve user-level persistence. The adversary has established persistence using a systemd service. The adversary has a hardcoded location under systemd that it uses to achieve persistence if it is running as root. The adversary can be used to establish persistence using a systemd service.

Pattern Entity Recognition – Char-embedding

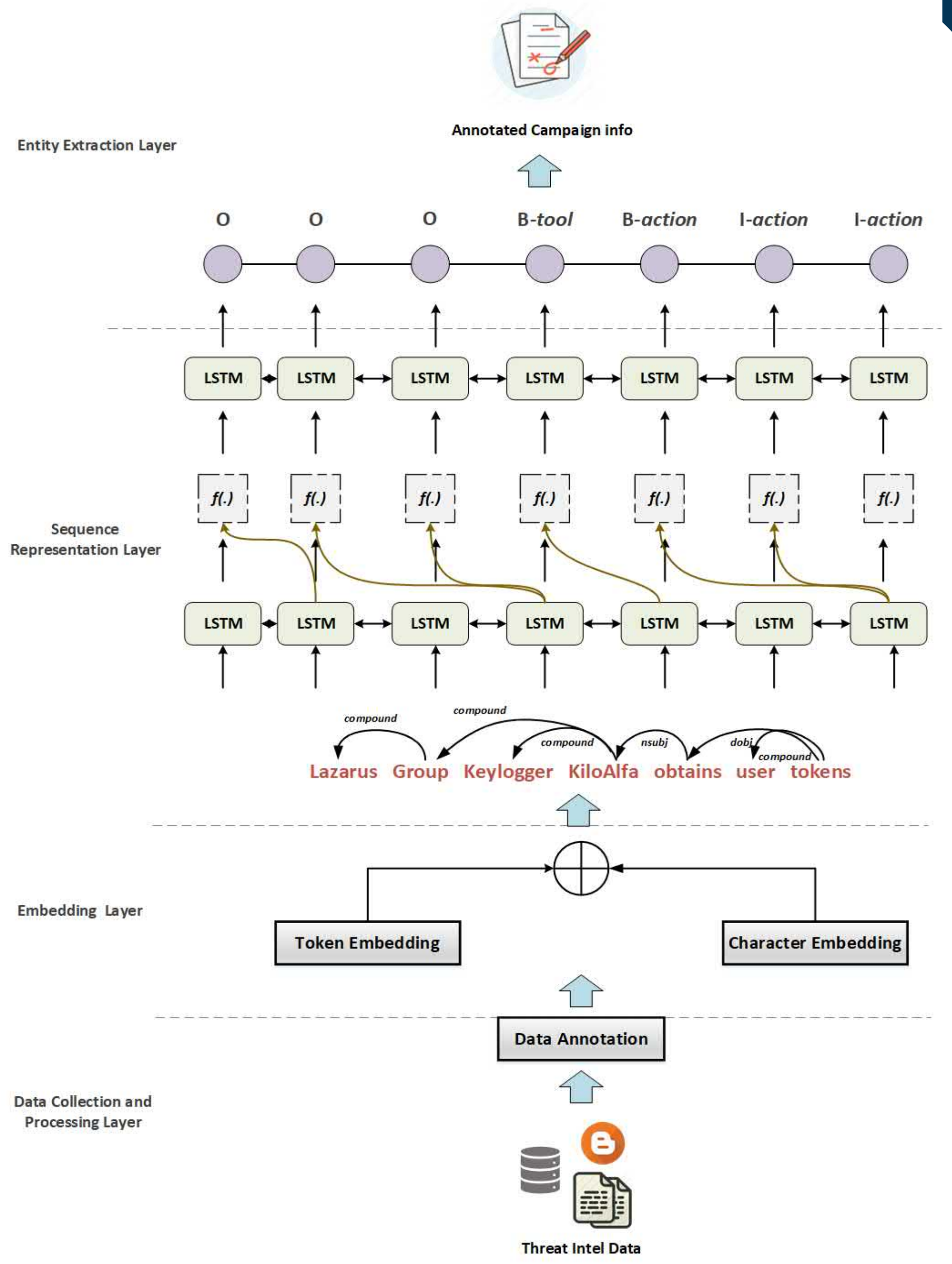
- Threat Intel often has out-of- vocabulary token
- Mostly software, malware, threat actors
- Concatenation of forward and backward representation



Neural Network Architecture for PER

- Word vector is concatenated with character vector
- Input embedding $e = [w_i, w_h, d_r]$
- BiLSTM captures contextual information
- Interaction function captures the interaction between word and parents
- For higher layer BiLSTM - $H^{l+1} = BiLSTM(H^l)$
- Score from BiLSTM $score(y,x) = \sum_{i=1}^{n} p_i[y_i] + \sum_{i=0}^{n} T[y_i, y_{i+1}]$
- CRF – $P(y|x) = \frac{\exp(score(y,x))}{\sum_{y`} \exp(score(y,x))}$

Interaction Function	$f(\mathbf{h_i}, \mathbf{h_{pi}})$
Self connection	$\mathbf{h_i}$
Concatenation	$\mathbf{h_i} \oplus \mathbf{h_{pi}}$
Addition	$\mathbf{h_i} + \mathbf{h_{pi}}$



Data Preparation

- Transform the annotated data into BIO – 'Begin', 'Inside', 'Outside' schema.
- Then transform into CONLL-X format

```
Adversaries	_	_	_	_	4	nsubj	_	_	O
may	_	_	_	_	4	aux	_	_	O
also	_	_	_	_	4	advmod	_	_	O
compromise	_	_	_	_	0	ROOT	_	_	B-intent
shared	_	_	_	_	7	amod	_	_	I-intent
network	_	_	_	_	7	compound	_	_	I-intent
directories	_	_	_	_	4	dobj	_	_	I-intent
through	_	_	_	_	4	prep	_	_	O
binary	_	_	_	_	10	amod	_	_	B-tool
infections	_	_	_	_	8	pobj	_	_	I-tool
by	_	_	_	_	4	prep	_	_	O
appending	_	_	_	_	11	pcomp	_	_	B-action
or	_	_	_	_	12	cc	_	_	I-action
prepending	_	_	_	_	12	conj	_	_	I-action
its	_	_	_	_	16	poss	_	_	I-action
code	_	_	_	_	14	dobj	_	_	I-action
to	_	_	_	_	14	prep	_	_	I-action
the	_	_	_	_	20	det	_	_	I-action
healthy	_	_	_	_	20	amod	_	_	I-action
binary	_	_	_	_	17	pobj	_	_	I-action
on	_	_	_	_	20	prep	_	_	O
the	_	_	_	_	25	det	_	_	O
shared	_	_	_	_	25	amod	_	_	B-action_object
network	_	_	_	_	25	compound	_	_	I-action_object
directory	_	_	_	_	21	pobj	_	_	I-action_object
.	_	_	_	_	4	punct	_	_	O
```

PER- results

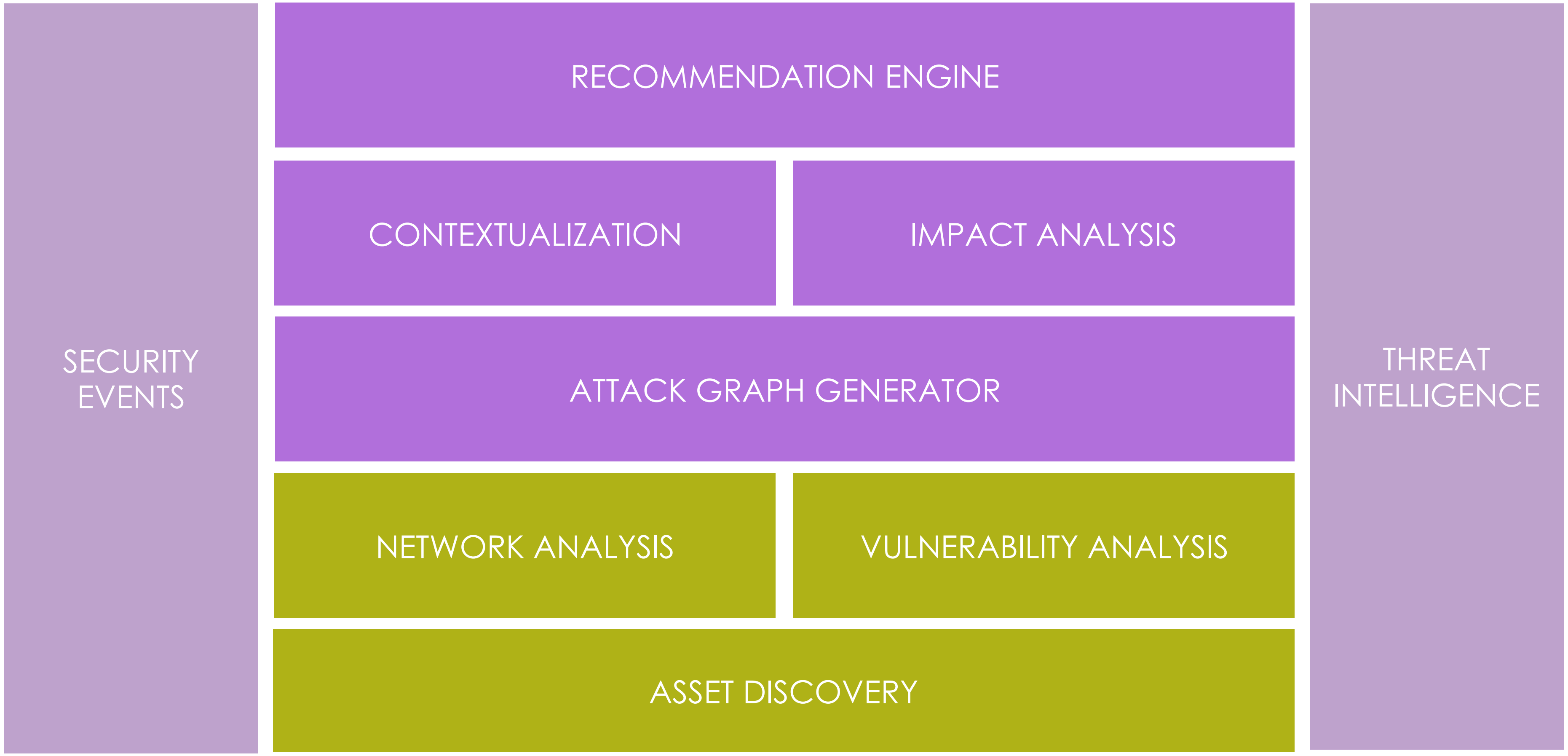
Hyper-parameter	value	Test Set			
		Accuracy	Precision	Recalls	F1-Score
Word Embedding	Glove (100d)	88.61	60.5	61.84	61.17
	Cyber-embedding (100d)	88.14	63.79	59.88	61.77
LSTM Layer	Layer-1	88.61	60.5	61.84	61.17
	Layer-2	89.23	60.55	62.70	61.60
Optimizer	SGD	88.61	60.5	61.84	61.17
	Adam	88.66	58.34	60.49	59.40

	Dimensions	Test Set			
		Accuracy	Precision	Recalls	F1-Score
Word Embedding	100	88.61	60.55	61.84	61.17
	200	89.41	62.24	59.88	61.04
	300	88.71	60.62	55.34	57.86
LSTM unit	100	89.04	61.68	59.63	60.64
	150	88.05	62.67	53.87	57.76
	200	88.61	60.55	61.84	61.17

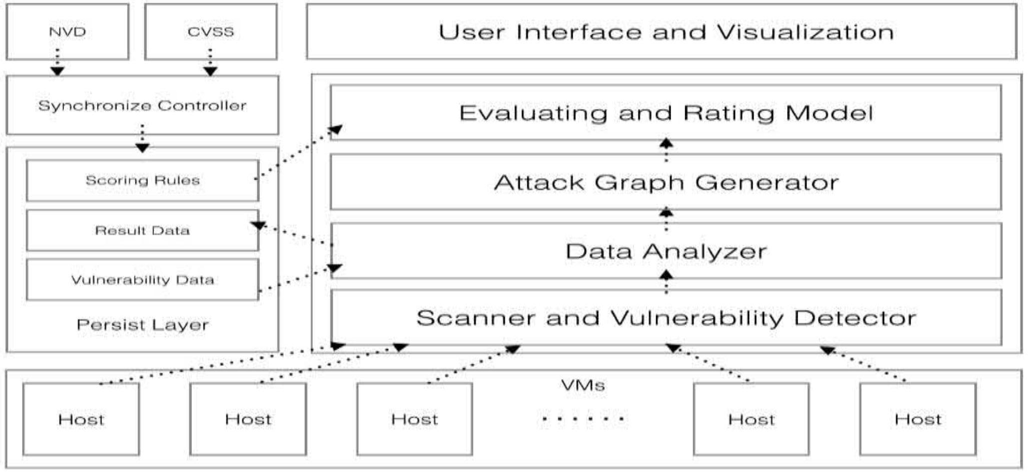
- Use universal word embedding
- Use concatenation as interaction function
- Unlike TTp adding more learning state doesn't help for pattern entity recognition

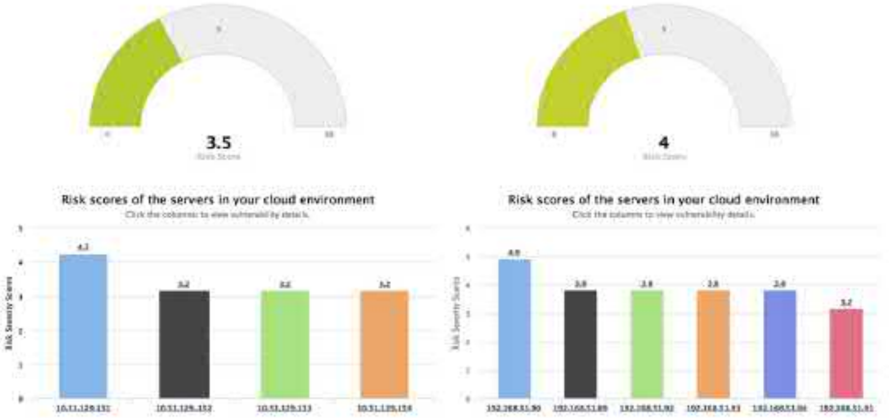
CYBER RISK MANAGEMENT

PROACTIVE AND REACTIVE APPROACHES



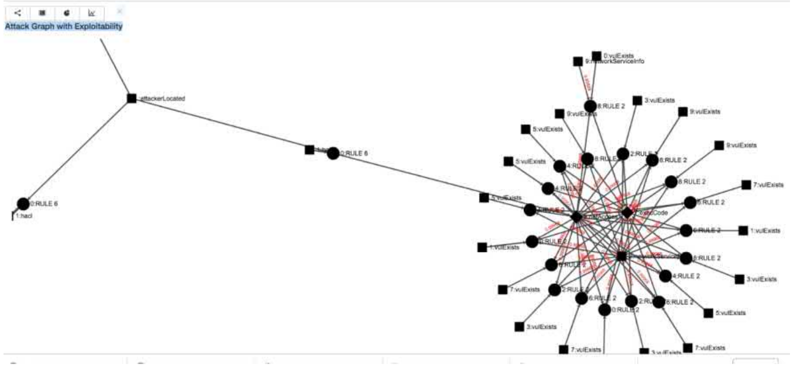
Cyber RIsk Scoring and Mitigation (CRISM©)





Vulnerability List

IP Address	Vulnerability	Risk	Fix Information
10.0.0.16	Discard port open CVE-1999-0636	10	GO
10.0.0.16	IIS .IDA ISAPI filter applied CVE-2001-0500	10	GO
10.0.0.16	Windows NT NNTP Component Buffer Overflow CVE-2004-0574	10	GO
10.0.0.16	Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote CVE-2008-411	10	GO
10.0.0.16	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) CVE-2010-002	10	GO
10.0.0.16	Message Queuing Remote Code Execution Vulnerability (951071) - Remote CVE-2008-3479	10	GO
10.0.0.16	Microsoft IIS FTPd NLST stack overflow CVE-2009-3023	9.3	GO



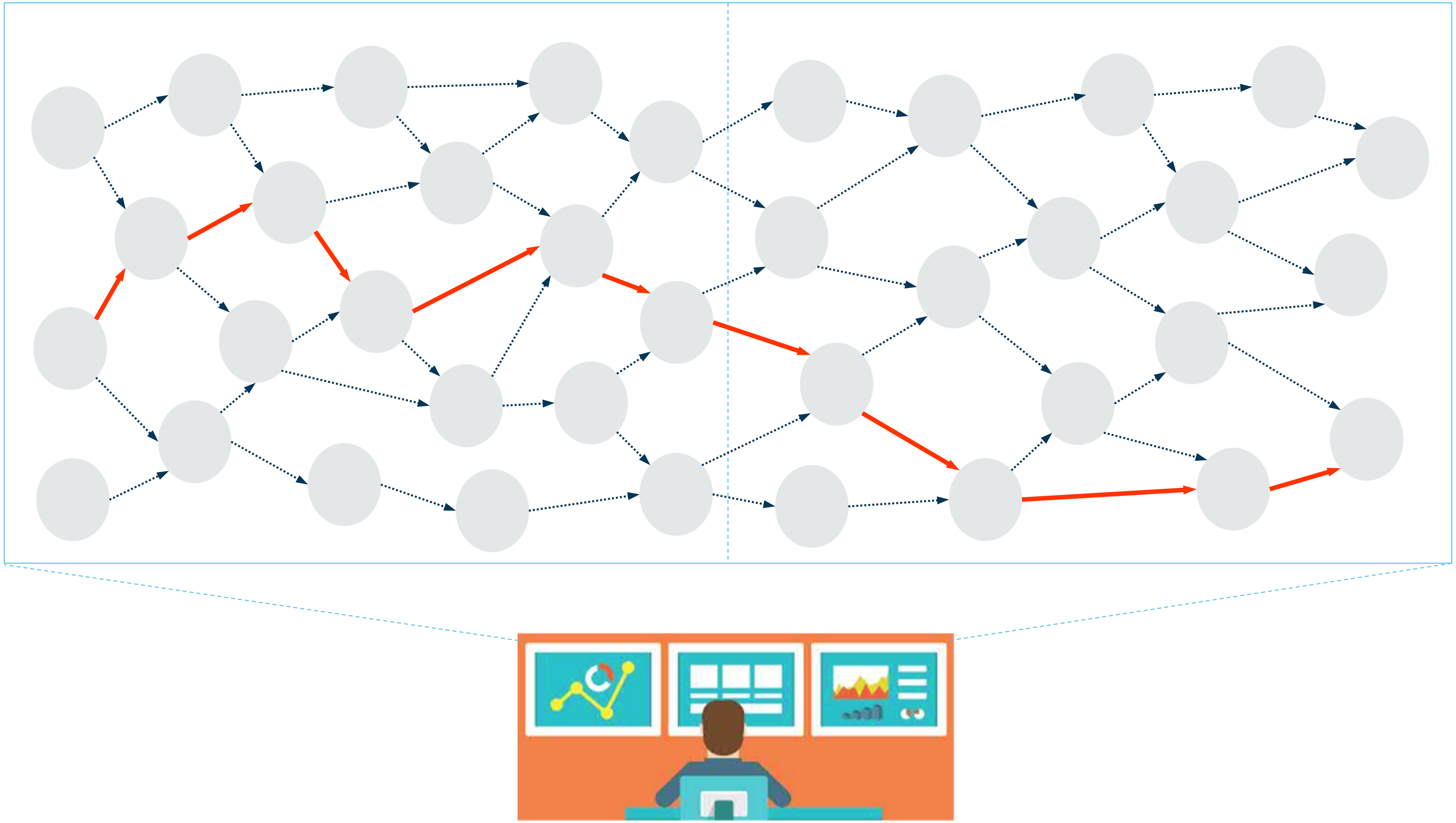
Sachin Shetty, Michael McShane, Linfeng Zhang, Jay Kesan, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, " Reducing Informational Disadvantages to Improve Cyber Risk Management", Geneva Papers on Risk and Insurance, April 2018, Volume 43, Issue 2, pp 224–238

Marco Gamarra, Sachin Shetty, Oscar Gonzalez, David Nicol, Charles A. Kamhoua, Laurent Njilla, "Analysis of Stepping Stone Attacks in Dynamic Vulnerability Graphs," IEEE International Conference on Communications (ICC) 20-24 May 2018, Kansas City, MO

Opportunity

Attacker technique-tactic Integration

In-depth Behavior Analysis



Thank You

Sachin Shetty, Ph.D.
Email – sshetty@odu.edu
Web – www.odu.edu/~sshetty