A Model-Based, Decision-Theoretic Approach to Automating Cyber Response

Lashon B. Booker Scott A. Musman

The MITRE Corporation

1st International Conference on Autonomous Intelligent Cyber-defence Agents (AICA2021)

March 15-16, 2021

MITRE

Background

One of the biggest technical challenges for automating cyber defense is managing the many sources of uncertainty about the state of the system, how the current situation will evolve, and what the consequences of defensive responses will be

From an AI perspective, it is advantageous to frame the cyber response problem as a sequential decision-making problem under uncertainty. This leads naturally to considering decision-theoretic approaches to

- Represent the way a human operator understands the system, the adversary, and the mission
- Generate responses that are aligned with risk-aware cost/benefit tradeoffs defined by user-supplied preferences

The goal of our research on ARCR (Automated Reasoning about Cyber Response) is to show how such a decision-theoretic approach to automating cyber response can provide practical solutions to real problems

MITRE

Previous Work: Sequential Stochastic Games

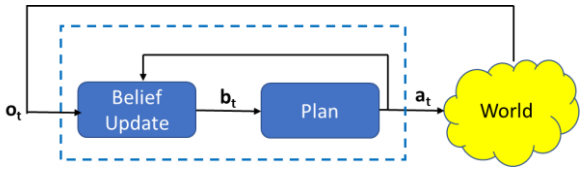
- **One straightforward approach to solving cyber defense problems is in terms of a two-person sequential stochastic game. The Partially Observable Competitive Markov Decision Process (POCMDP) framework is especially helpful.**
  - Problems lend themselves to theoretically sound analysis
  - Value iteration techniques can find good solutions quickly for problems having a manageable number (scores) of states
- **Zonouz et al (2009) have shown how this framework can be used to devise practical cyber defense solutions for small systems (~12 nodes with binary state predicates)**
  - Represent system state with probabilistic IDS alert predicates for each asset
  - Build an attack-response tree (ART) and use it to automatically construct an explicit POCMDP model of defender and attacker behavior
  - A customized version of value iteration can find solutions for ART trees with 900 nodes in about 40 seconds on a standard PC running Linux
- **A major shortcoming of this approach is that the scaling properties are poor, so it is not a realistic alternative for large-scale cyber defense problems**

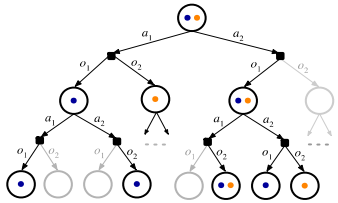
Zonouz, Saman A., Himanshu Khurana, William H. Sanders, and Timothy M. Yardley. "RRE: A game-theoretic intrusion Response and Recovery Engine." In Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on, pp. 439-448. IEEE, 2009.

Previous Work: Online POMDP Planning

Generic Online POMDP planning paradigm

Repeat
1. Generate new plan given current belief
2. Execute the first step in the plan
3. Update the belief given the action taken and the resulting observation





Monte Carlo tree search for an optimal policy

Monte Carlo Sampling

Dynamic Security Model*

1. Determine the set of exploits blocked by the defensive action
2. Sample probability distributions for attack and success
3. Sample probability distributions for the resulting observation

Action outcome estimates from generative model

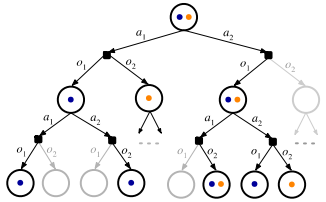
- **Recent efforts have turned to Partially Observable Markov Decision Processes (POMDPs) as a formal framework addressing cyber security problems**
  - Using state-of-the-art online solvers, POMDPs with state spaces as large as 10^{56} can be solved with only a few seconds of computation (Silver & Veness, 2010). The solver only needs to focus on the search space relevant to the current state.
  - There are many ways to design POMDP solutions for a given cyber defense problem
- **Miehling et al (2018) show one way to use simplifying assumptions to solve a class of large-scale cyber defense problems with a POMDP approach**
  - Focus is on selecting defense actions in real-time in order to mitigate the progression of an attacker through the network while minimizing the negative impact to a single security property: availability
  - Defense actions can only block exploits; they do not disable or remove conditions
  - The POMDP manages beliefs by explicitly representing the joint probability distribution of the attacker's current capabilities and true strategy, along with the defender's actions.
  - Simulation results show the approach can successfully find defense policies for a problem on a graph consisting of 134 conditions (nodes), 143 exploits (hyperedges), 64 defense actions, and 30 security alerts
- **The goal of the ARCR project is to craft POMDP solutions capable of handling a broader range of problems at a larger scale**

*Miehling, E., Rasouli, M. and Teneketzis, D., 2018. A POMDP approach to the dynamic defense of large-scale cyber networks. *IEEE Transactions on Information Forensics and Security*, *13*(10), pp.2490-2505.

MITRE

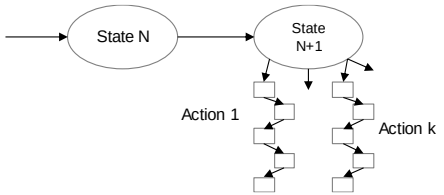
ARCR Technical Approach: Mission-Oriented Online POMDP Planning

Hypothesis: A mission-oriented, event-based simulation, coupled with a hierarchical online POMDP planner, will enable scalable solutions to many real-world cyber defense problems



Hierarchical belief tree search includes abstract states and actions

Monte Carlo Sampling



Action outcome estimates from mission-oriented, event-driven simulation of defender-attacker interactions

- Use the POMDP derived by assuming the attacker behavior in the underlying stochastic game can be modeled as part of the stochastic environment
- Build on POMDP solvers that provide online, anytime, real-time solutions for real-world problems
- Facilitate scaling by using a “separation of concerns” design principle integrating several ideas
  - A mission-oriented, discrete-event simulation (the Cyber Security Game (CSG)) models the stochastic game initiated by a defender action in cyberspace.
    - The focus on factors related to mission risk and mission impact makes the modeling of a broad repertoire of security properties and agent actions much more tractable
    - Discrete events based on the outcome of defender/attacker move pairs allows for compact representations of activities covering time segments having potentially different lengths
  - An online planner manages defender beliefs, projects the consequences of defender action sequences, and makes a decision-theoretic choice of the best action
    - Abstract states and actions help reduce the complexity of the search space
    - Hierarchical search techniques make the search more efficient
  - Interface modules handle sensor algorithms and timing issues related to real-world interactions

MITRE

Key Modeling Assumptions in MITRE's Cyber Security Game (CSG)

- **CSG is a coarse-grained simulation of attacker and defender interactions in cyberspace**
  - Developed by MITRE for assessing defensive architectures and deploying static cyber defenses.
  - Represents interactions as a fully-observable, probabilistic outcome, zero-sum game.
- **CSG's defensive cyber decision-making focuses primarily on defending the mission that the cyber assets are intended to support.**
  - This mission focus reduces the complexity of the defender's problem since often only a subset of the system's cyber assets is relevant at any given time.
  - System assets, physical connectivity, process flow and trust/access relationships are only modeled with the fidelity needed to compute mission impacts.
- **Instead of reasoning about every possible attack instance, CSG reasons about the effects of successful attacks (summarized in the DIMFUI taxonomy).**
- **CSG currently supports two attacker types:**
  - Greedy attacker model always chooses the next action in the game tree toward the highest expected value payoff target(s)
  - Min-Max attacker model chooses the best min-max move available
- **We modified CSG to support queries from an online POMDP planner**
  - For a defender move in a given state, CSG now automatically generates attack trees modeling the detailed interleaving of attacker/defender moves from this starting point
  - Interactions are played forward to identify pathways leading to mission impacts (including compromises of multiple components)

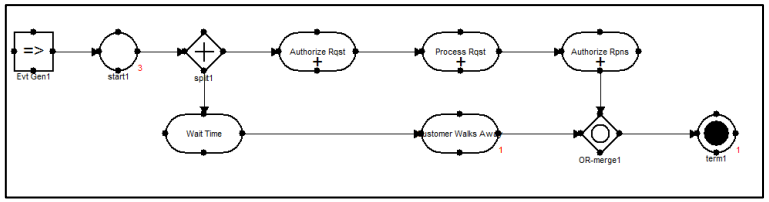
DIMFUI: a coarse-grained but robust taxonomy of cyber incident effects

DIMFUI	Explanation	Typical Attacks
Degradation	1. Reduction in performance or capacity of an IT system 2. Reduction in bandwidth of a communication medium 3. Reduction in data quality	4. Limited-effect DoS 5. Zombie processes using up CPU and slowing server 6. Transfer of non-mission related data over a link that slows the transfer of mission data 7. Dropped packets cause an image to have less resolution
Interruption	IT asset becomes unusable or unavailable	1. Ping of Death 2. Wireless Jamming 3. Wipe disk
Modification	Modify data, protocol, software, firmware, component	1. Change or corrupt data 2. Modify access controls 3. Modify/Replace system files
Fabrication	Attacker inserts information into a system or fakes components	1. Replay attacks 2. DB data additions 3. Counterfeit software/ components
Unauthorized Use	Attacker uses system resources for illegitimate purposes. Related and often a precondition for other DIMFUI.	1. Access account or raise privileges in order to modify/degrade/interrupt the OS 2. Subvert service to spawn a program on remote machine 3. Bandwidth used surfing for porn degrades mission critical exchanges
Interception	Attacker gains access to information or assets used in the system	1. Keylogger 2. SQL injection 3. Crypto key theft 4. Man-in-middle attacks 5. Knowledge of component or process that is meant to be secret

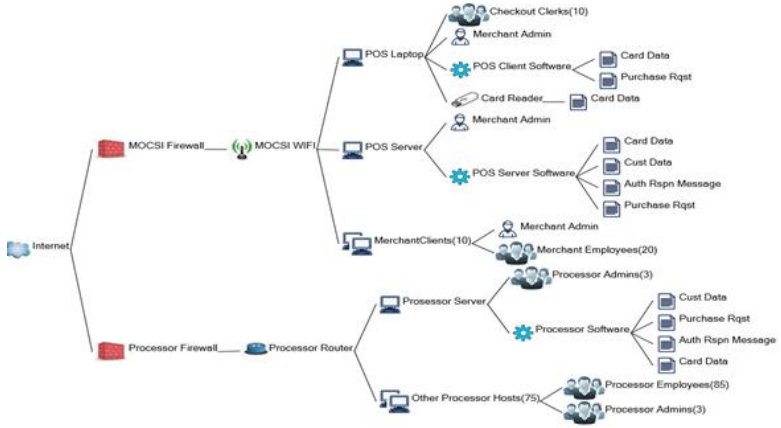
MITRE

Representing a System in CSG

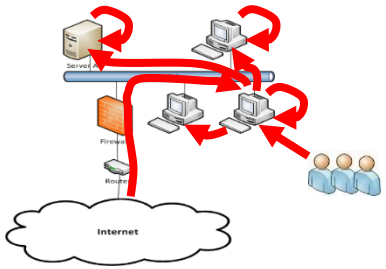
Cyber Mission Impact Assessment (CMIA) Process Model: Simulates mission threads using a process model to compute cyber incident impacts (DIMFUI)



System Terrain Model: Describes how cyber components are interconnected, their type, access and trust relationships (networks, network components , network hosts, user groups, peripherals, applications, services, and information used in performing the mission)



Attacker Move Model: Describes how the attacker capabilities enable it to move across the terrain, based on the type of interaction (e.g. physical access, network access, etc.) the attacker has with targets and how terrain impacts the likelihood of attacker success (based on ATT&CK)

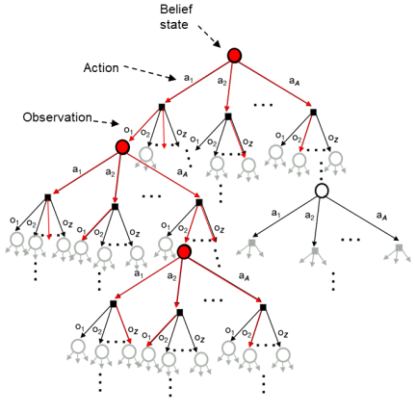


Defender Move Model: Describes the defense methods the defender can deploy, along with their properties and costs

Category	Method	Applies-to	Tool	Purpose	Install Cost	Maintenan	Operationa	Total Cost	Interruptio	Modificati	Fabricatio	Unauthori	Interceptio
Terminal Access Control	Passwords/Token	POS Server	Access Car	To Limit ur	10000	500	2000	12500	0	40	40	50	50
Terminal Access Control	Passwords/Autolock/Logout	POS Server	Built-in + n	To Limit ur	750	50	3000	3800	0	20	20	40	40
Terminal Access Control	Passwords/Token/Autolock/Logout	POS Server	Access Car	To Limit ur	10500	550	5000	16050	0	40	40	60	60
Encryption	Disk & transport Encryption	Cust Accnt	LUKS & TL	Protect da	1000	0	50	1050	0	40	40	40	60
Server Configuration Management	Harden Server	POS Server	Puppet	to harden	2000	2000	100	4100	20	20	20	20	20
POS terminal Configuration Management	Harden POS Term	Laptop PO	MaaS360	to harden	55000	5000	1000	61000	20	60	20	40	20
Network Access Control	NAC	MOCSI Wil	Cisco ISE	Stop unaut	30000	3000	1000	34000	0	20	20	60	20
Network Access Control	NAC + VPN	MOCSI Wil	Cisco ISE +	Stop unaut	35000	3000	-5000	33000	0	20	20	60	20
Network Intrusion Detection	NIDS	POS Server	Security O	reduce the	5000	500	0	5500	20	20	20	20	20
Network Intrusion Detection	NIDS + Applications Monitoring	POS Server	ModSecuri	reduce the	10000	0	0	10000	20	20	20	20	40
Server Intrusion Detection	File Integrity	POS Server	Tripwire	reduce the	15000	1500	1000	17500	0	40	20	20	20
Tokenize	Tokenize Transactions	Cust Accnt	First Data	Ensures th	30000	1000	0	31000	0	0	0	90	90
Host Intrusion Detection	Virus detection/HIPS	Laptop PO	Semantec	Detect anc	5000	500	1000	6500	20	20	20	20	20
EMV	CHIP n Sig	Card Data;	PCI	Authentica	20000	1000	500	21500	0	0	60	0	0
EMV	CHIP n PIN	Card Data;	PCI	Authentica	20000	1000	10000	31000	0	0	85	60	0
Reimage POS Systems	periodic POS terminal re-image	Laptop POS	Software;	Laptop Ha	25000	1000	5000	31000	20	60	20	50	20
Whitelist processes	White Listing	POS Server	Bit9 Parity	run only al	5000	0	500	5500	40	60	20	60	25

MITRE

The ARCR Planner



Generate a heuristically guided, sparse sample of the belief tree. Expand every action edge of a leaf node, but only a sample of the possible observations

The DESPOT algorithm finds online, anytime POMDP solutions to real-world problems

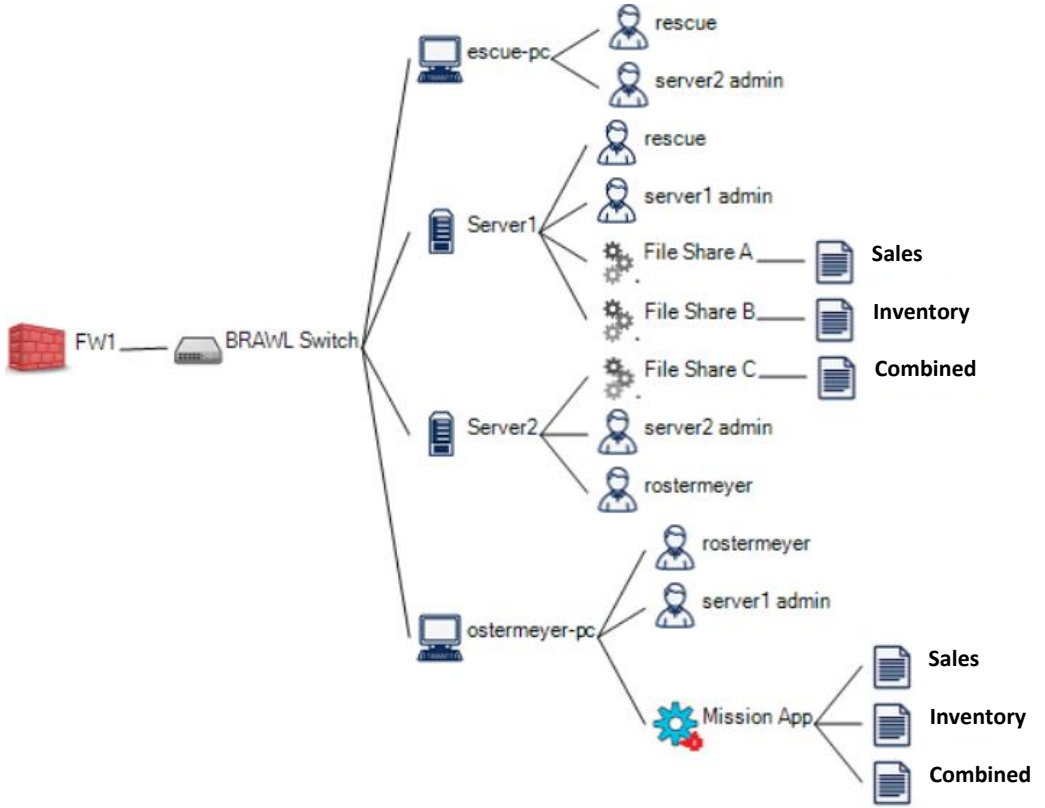
Image source:
Ye, N., Somani, A., Hsu, D. & Lee, W. S., 2017. DESPOT: Online POMDP planning with regularization. *Journal of Artificial Intelligence Research,* Volume 58, pp. 231-266.

- **The DESPOT algorithm (Ye et al., 2017) provides a real-time POMDP solver suitable for automating cyber defense**
  - Real-time algorithm interleaves planning and execution
    - Uses heuristic search with branch and bound pruning and fixed time limits for efficient tree search
    - Uses Monte Carlo sampling to achieve tractable belief estimate (limited number of samples per action considered)
  - Theoretically guaranteed to find a “small” optimal policy if it exists
  - Avoids poor worst-case behavior of methods that use pure Monte Carlo rollouts
- **The ARCR planner includes customizations designed to make it well-suited for the online cyber defense task**
  - States and observations are simple binary strings of DIMFUI predicates
  - Macro-actions replace some action sequences with a single discrete-event lookahead step when the outcome can be calculated analytically. These macro-actions provide a significant speed-up in planner performance.
  - Abstract states and actions reduce the complexity of search. Hierarchical search extensions to the solver (work in progress) will make search more efficient
  - Observations are generated by sensor noise models in the planner interface, which makes the game tree searches in CSG more tractable

MITRE

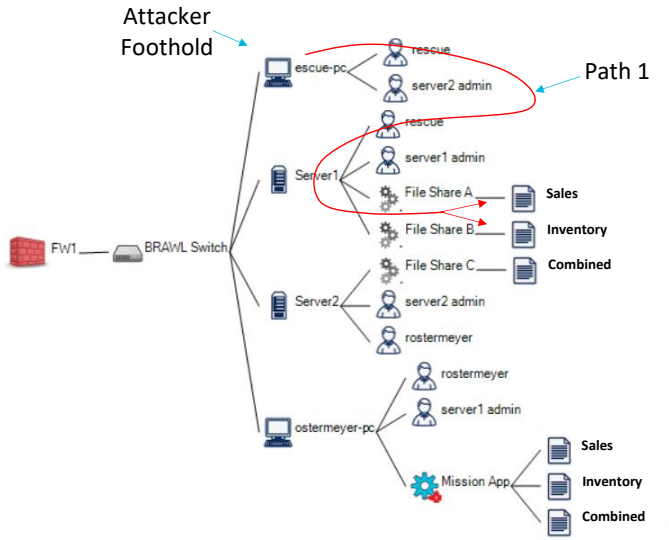
A Simple “Information Fusion” Mission Use Case

- **Business transaction agents (not shown) place Sales and Inventory files in File Shares A and B respectively being served from Server 1.**
- **A client agent accesses paired Sales and Inventory files, performs some (unspecified) fusion operation on them and produces a combined status update file as an output in Shared Folder C being served on Server 2.**
- **Assume a greedy attacker steals a user credential (rescue) on its foothold (escue-pc), then uses that credential to move laterally from the foothold to Server 1. Once on Server 1, the attacker modifies the file share and one (or more) files on the file share**
- **The ARCR planner response actions: RX (restore host), RA (restore all hosts), FX (restore file on share), FA (restore all files on share), DA (disable a user account)**



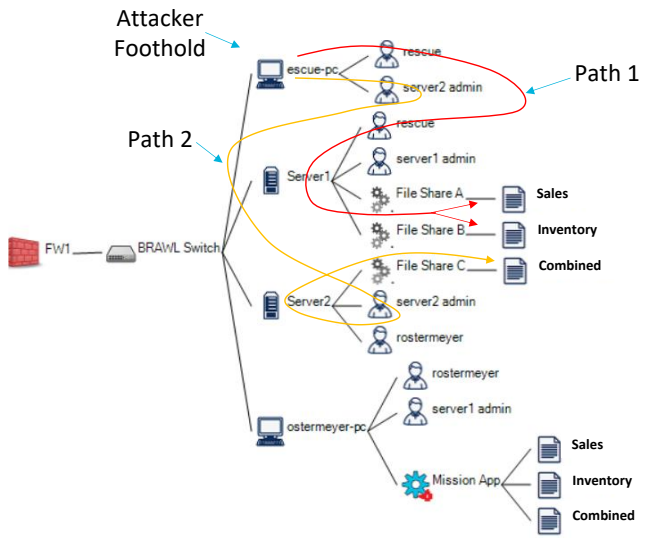
MITRE

Simulated Use Case Scenarios



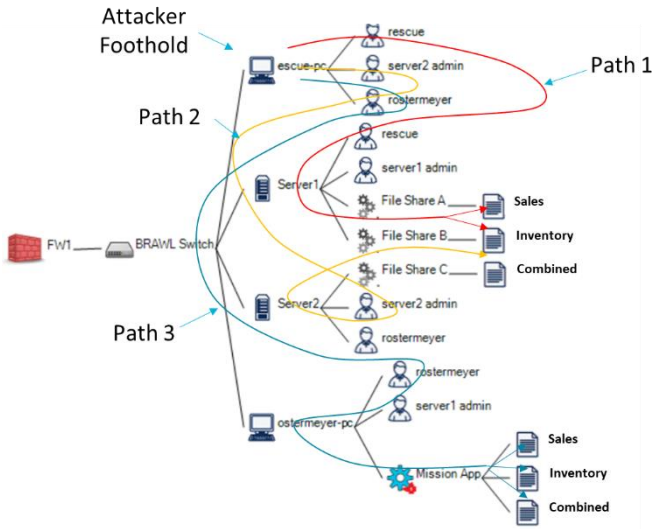
Attack involving 1 credential path

- The attacker steals a user credential on its foothold to move laterally from the foothold to Server 1. Once on Server 1, the attacker modifies the Sales or Inventory data, thereby causing adverse impact to the mission.
- ARCR determines that the DA action completely blocks the attacker from doing any damage and is therefore the preferred solution (unless disabling the account is too costly or adversely impacts the mission, in which case the RX action is used to eject the attacker).



Attack involving 2 credential paths

- In addition to stealing a credential enabling access to Server 1, the attacker also compromises the Server 2 admin account, giving the attacker access to Server 2 and the combined status file.
- ARCR correctly recognizes that if the credentials are not disabled right at the beginning of this scenario, the defender will be forced to take a much more costly action later to avoid adverse mission impact



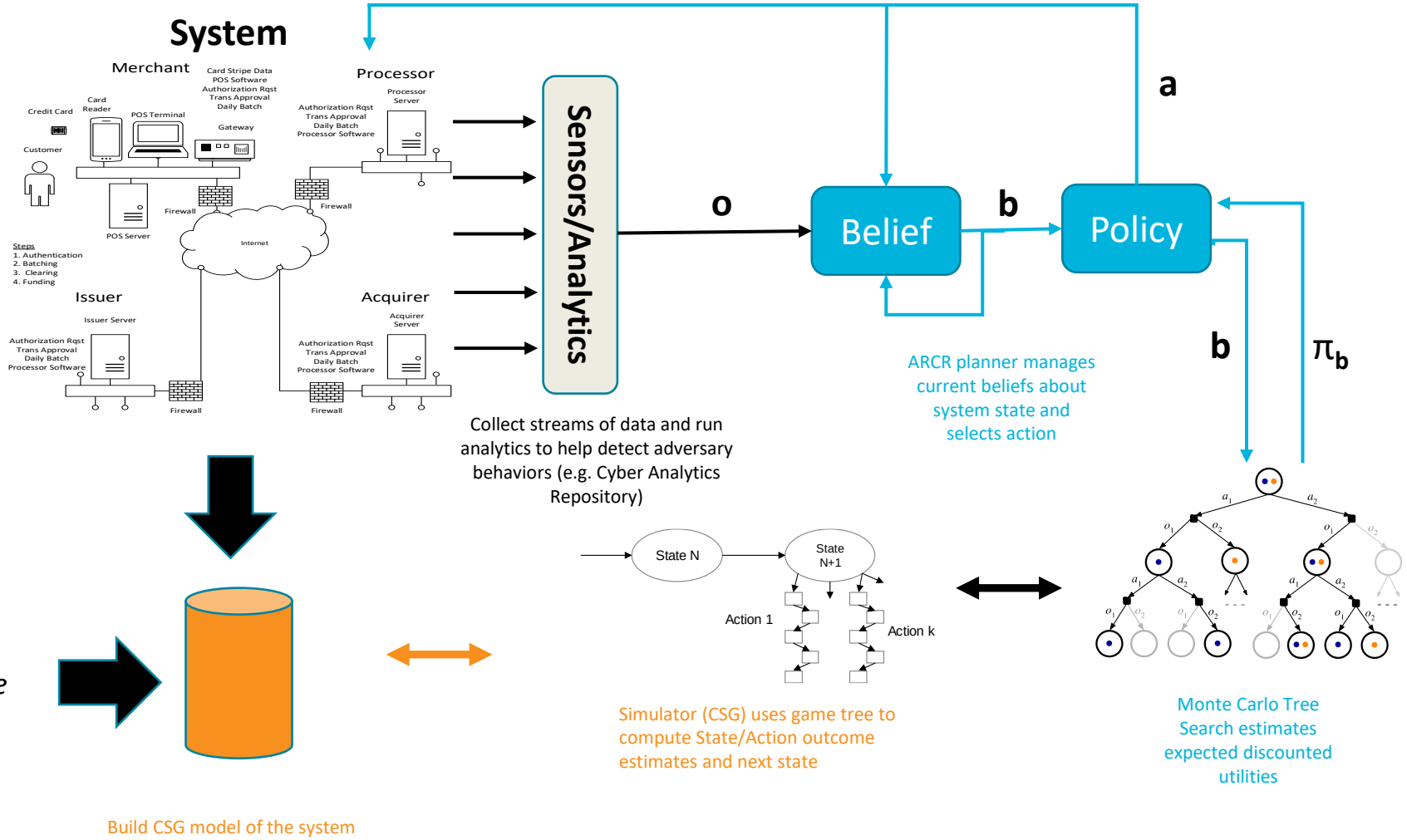
Attack involving 3 credential paths

- The attacker steals three user credentials. There are now 3 paths to targets, but only 2 game steps needed to compromise one of them.
- ARCR uses its action repertoire to disable access to 2 targets in the time available. Given an action that disables all compromised accounts, ARCR would quickly determine how to eliminate all 3 threats.

We are currently implementing a test harness on virtual machines to test ARCR performance on real machines for these scenarios and many others

MITRE

ARCR CONOPS



MITRE

Projected ARCR Impact

- **Technical Contributions**
  - Scalable approach that leverages factors related to mission risk and mission impact to model a broad repertoire of security properties and agent actions
  - Online POMDP planner with an innovative collection of heuristic capabilities to handle large scale problems
  - Techniques for helping to manage the complexities of real-world interactions, including noisy sensors and durative actions
- **Application Potential**
  - ARCR takes steps towards characterizing the essential elements of IPB for cyberspace to support risk planning and real time response
    - Cyber terrain, mission, own capabilities, enemy capabilities
  - ARCR shows how to defend networks in a principled way to counter existing and emerging threats
    - The “brains” behind an effective automated response
  - CSG provides a complimentary capability over existing tabletop or test range experiments
    - ARCR improvements to CSG already make it possible to run many more simulated attack trials, faster than can be run in a real test network
    - This makes it possible to explore the parameter space of a cyber problem more thoroughly

MITRE

Summary

- **Work to date on ARCR shows how to bring together state-of-the-art techniques for anytime online planning in large state spaces with the capabilities for modeling cyber security problems found in the Cyber Security Game (CSG).**
- **This combination appears to be a promising path toward computing tractable solutions to complex cyber security problems.**
- **Our future work will focus on expanding these capabilities and making them more efficient.**
  - Complete implementation of hierarchical POMDP solution strategies to improve the scaling properties of planner.
  - Increase the realism of our cyber models by adding more sensors (including the detection of both action and state), adding more attacker and defender actions, and reasoning about the impacts from multiple incident effects.
  - Estimate heuristic search bounds for the planner automatically from CSG

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org

MITRE