IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45SP/2025/4535725/
Vol. 2025 (23), Article ID 4535725

Stochastic Methods for Assessing the Security of An Organisation's ICT*

Jerzy Dorobisz

Affiliation e.g. Institute of Information Technology and Cyber-security, Faculty of Cybernetics, WAT, 2 Gen. Sylwestra Kaliskiego St., 00-908 Warsaw

Correspondence should be addressed to: Jerzy Dorobisz, jerzy.dorobisz@wat.edu.pl

* Presented at the 45th IBIMA International Conference, 25-26 June 2025, Cordoba, Spain

Introduction

In this chaotic digital world, securing your tech isn't just optional—it's a must for any business that wants to stay afloat. They change the game, catch you off guard, and pretty much laugh at your old security checklists. It's all about things like Markov chains and Monte Carlo simulations. These methods help you understand potential attacks and figure out just how risky things could get if you're hoping for the best. The real world isn't that simple. You'll know which defenses matter, where to strengthen things, and just how much trouble you could be in if you don't act. Real case studies show that taking this probabilistic approach makes your security smarter and much more adaptable. Cyber threats can change quickly, so your defenses should be able to adjust just as fast. It can truly change the game for anyone who wants to avoid getting caught off guard by the next big cyber threat. If you want to stop leaving your digital security to chance, it might be time to embrace these strategies.

Context of the problem

Modern targeted cyber attacks (APTs) are evolving into complex, multi-stage campaigns aimed at long-term infiltration of infrastructure. For example, the SolarWinds (2020)[24][25] attack used the supply chain to insert a backdoor into software updates, remaining undetected for nine months. In contrast, the Colonial Pipeline incident (2021)[25] showed that even organisations with high levels of security are vulnerable to critical outages caused by ransomware attacks.

Statistics illustrating the scale of the problem (source: Verizon DBIR 2023, IBM X-Force):

a. 68% of companies have experienced an APT attack in the last 2 years.

b. The average cost of a data breach is $4.35m (up 12% from 2020).[25]

c. 83% of attacks use living-off-the-land techniques (using legitimate tools for malicious purposes).[1][26] [27]

Cite this Article as: Jerzy Dorobisz, Vol. 2025 (23) "Stochastic Methods for Assessing the Security of An Organisation's ICT " Communications of International Proceedings, Vol. 2025 (23), Article ID 4535725, https://doi.org/10.5171/2025.4535725

Statistics Illustrating the Scale of the Cybersecurity Problem

These figures underscore the need for advanced risk assessment methods, such as stochastic modeling, to address evolving threats.

d. Main limitations of current analytical models:

1. Assumption of attackers' rationality: Classical game theory models (e.g. Nash equilibrium) assume that the opponent always chooses the optimal strategy. In practice, attackers make mistakes (e.g. leave logs in the system), which is not taken into account.

2. Unrealistic time distributions: Markov process-based models require exponential distributions of attack phase durations, whereas empirical data (e.g. from the MITRE ATT&CK platform) indicate log-normal or Weibull distributions.[2]

3. Lack of dynamic interactions: Current models do not take into account the adaptability of both sides - attackers do not learn from the defender's reactions, and defensive systems do not modify strategies in real time.

Purpose of the work and innovations

This section explains what's new in this thesis and why it matters. We're trying to link theory with real cyber threats by using a hybrid stochastic framework. Regular methods often miss how attackers adapt or the complex nature of multi-stage breaches. To tackle this, we present three main ideas:

1. Semimartingale Petri Nets (SPNs) with Cox Approximation
   a) This models different attack paths, like when multiple weaknesses are targeted.
   b) It also approximates various time distributions, such as log-normal, using Cox phases.
2. Evolutionary Game Theory with Entropy Metrics
   a) This simulates different types of attackers, from novices to experts.
   b) It looks at unpredictability using conditional entropy H(A|S).
3. Adaptive Defenses
   a) Detection based on Reinforcement Learning (RL).
   b) Dynamic honeypots that cut phishing success rates by 40%, based on real data.

To show how this works, we looked at a case study: in financial systems, our model helped cut mean response time from 48 hours to just 12 hours. The main objective of this thesis is to develop a hybrid stochastic model that combines quantitative methods (Petri nets) with qualitative behavioural analysis (evolutionary game theory) to:

1. Reflect the actual behaviour of the attackers, including cognitive errors and limited rationality.
2. Allow the modelling of arbitrary time distributions for the different phases of an attack (e.g. power escalation time, defender response time).
3. Integrate adaptive defences based on machine learning and information theory.[3]

Key innovations:

- Semimarker Petri nets (SPNs) with Cox approximation:
  a. Modelling of non-linear and parallel attack paths (e.g. simultaneous exploitation of multiple vulnerabilities).
  b. Approximation of arbitrary time distributions by combinations of exponential distributions (Cox distribution), which allows mathematical analysis without loss of generality.
- Evolutionary game theory with entropy metrics:
  a. Simulation of attacker populations with different skill levels (e.g. novices vs. experts).
  b. Introducing conditional entropy H(A| S) as a measure of the unpredictability of an attacker's actions in a given state of system S.

- Adaptive defence strategies:

a. Detection systems based on reinforcement learning (RL) that dynamically adjust sensitivity to observed attack patterns.

b. Honeypots with variable attractiveness, affecting the probability of detecting an intruder.[4]

An example of application in the financial sector - the model estimates that the introduction of dynamic honeypots reduces the probability of success of a phishing attack by 40%, while reducing the mean time to respond (MTTR) from 48 to 12 hours.

Structure of the document

The document is divided into six essential sections to ensure a clear flow from theory to validation:

1. Introduction (current chapter) - diagnosis of the problem, purpose of the work and theoretical basis.
2. Literature review - critical analysis of existing models (AMC, Attack Trees) and motivation for proposed innovations.
3. Theoretical model - formal description of semimartingale SNPs, integration with evolutionary game theory and machine learning algorithms (HMM, RL).[5]
4. Implementation - system architecture, complexity reduction methods (lumping, aggregation) and tools used (Mesa, TensorFlow, Julia).
5. Validation - test scenarios based on MITRE ATT&CK data, simulation results (MTTA, MTTR, ROC curves) and comparison with baseline models.
6. Conclusions - summary of achievements, limitations of the model and directions for future work (e.g. integration with quantum optimisation algorithms).[6]

Key Terms

- Stochastic Petri net (SPN): A mathematical formalism for modelling concurrent systems where transitions between states are described by probability distributions.
- Cox distribution: An approximation of any probability distribution by a sequence of exponential distributions. E.g. a log-normal distribution can be approximated by three Cox phases.
- Conditional entropy H(A| S) - a quantitative measure of the uncertainty of an action A with a known state S.[7]
- Evolutionary game theory: A branch of game theory where strategies are selected not by rational analysis, but by mechanisms analogous to natural selection (e.g. replicator equations).
- MTTA (Mean Time To Attack): The average time it takes for an attacker to break through . In the model calculated as the expected value of the trajectory in the SNP.
- Reinforcement learning (RL): A method of machine learning where an agent (e.g. a sensing system) learns optimal actions by interacting with the environment and maximising rewards.[8]
- Honeypot: A dummy system or service that mimics real resources to lure attackers and collect data on their tactics.

The table summarises the key differences between traditional models (e.g. Markov chains, attack trees) and the proposed approach.

Table 1.1. Comparison of traditional models with the proposed solution

Aspect	Traditional models	Proposed solution
Assumption of reasonableness	Full rationality (Nash equilibrium)	Evolutionary strategies+ decision entropy
Timetables	Exponential (Markov)	Any (Cox approximation)
Adaptability of the defence	Static policies	Reinforcement Learning (RL)
Modelling of attack phases	Linear (AMC)	Non-linear (SPN+ HMM)

Validation tools	Theoretical simulations	Integration with MITRE ATT&CK, Cuckoo Sandbox

- Row 1: The proposed model replaces the assumption of full rationality with evolutionary dynamics and entropy metrics.
- Row 2: The Cox approximation allows realistic attack phase durations (e.g. log-normal) to be modelled.
- Row 4: The non-linearity of the SNP better reflects the parallel actions of the attackers (e.g. lateral movement).[9]

Literature Review

In the field of ICT security modelling, there is a rich tradition of research based on stochastic methods and decision theories. This chapter examines the key approaches that provide a starting point for the proposed model, and identifies the gaps that motivate innovation.

Traditional safety assessment models

Markov chains of attacks (AMCs) are one of the most widely used tools for modelling cyber risk. In this approach, system states represent horizontal phases of an attack (e.g. 'initial access', 'privilege escalation') and transitions between them are described using exponential time distributions. An example is the model of Szwed and Kowalczyk (2017), which estimated the average time to breach online banking security to be 72 hours. Although AMCs provide simple probability analyses, their main limitation is the assumption of no memory (the Markov property), which makes it impossible to model the time dependencies found in real APT attacks.[10]

The Meta Attack Language (MAL) (Johnson et al., 2018) provides a formal foundation for the design of domain-specific languages (DSLs) in cyber security, enabling the generation of attack graphs and the simulation of times of compromise (TTC). MAL integrates attack logic with systems modelling to analyse the relationship between attack steps (OR/AND) and defence mechanisms.

Modern approaches, such as MITRE ATT&CK matrix-based modelling (Xiong et al., 2022), enable systematic classification of techniques attacks (e.g. Lateral Movement, Credential Access) and integration with simulation tools (e.g. secureCAD), which significantly increases the realism of models.

The pwnPr3d approach (Johnson et al., 2018) offers automation of attack graph generation with embedded security analysis, eliminating the need for manual rule definition. The model uses a layered architecture (Layer-0: attack graph theory, Layer-1: system logic), probabilistic compromise time distributions (TTCs) and specialised attack steps (e.g. as_min, as_max), allowing for accurate representation of non-linear attack paths. Unlike MAL, pwnPr3d introduces object-oriented component libraries (e.g. operating systems, firewalls), which significantly reduces modelling costs.[11]

In the context of automating attack graph generation and countermeasure selection, an important development of MAL is the work of Widel et al. (2022), which introduces an iterative algorithm for optimising countermeasure selection given budget constraints and dependencies between agents (e.g., mutual exclusions, sequence requirements). The proposed solution integrates attack simulations with evolutionary game theory, enabling the selection of defence strategies that minimise the mean time to compromise (TTC) while maintaining realistic cost parameters. In contrast to pwnPr3d, the approach focuses on analysing the attack paths returned by the simulations rather than the full graph, increasing scalability for large infrastructures.

Attack Trees, proposed by Schneier in 1999, focus on the representation of all possible paths leading to an attack target. This method, although intuitive, becomes impractical for complex systems due to the combinatorial growth of the number of nodes. A study by Mauro et al. (2020) showed that for an infrastructure with 50 vulnerabilities, a full attack tree would require more than 10^15 nodes, which is beyond the computational capacity of modern systems.[12]

In the context of critical infrastructures such as power grids, modelling based on taxonomies and reference architectures that integrate IT (information technology) and OT layers (operational technology) is receiving increasing attention. An example is the ArchiMate framework extended to include cyber-physical components (e.g. remote RTU terminals, transformers, smart meters) and the functional dependencies between them. The

research of Jiang et al. (2023) demonstrate how reference models based on IEC 62351 and NIST SP 800-82 standards enable the analysis of cascading effects of failures, e.g. the impact of router compromise on the stability of the physical transmission network. These models, unlike classical attack trees, take into account data heterogeneity, IT/OT convergence and dynamic dependencies between components."[13

Stochastic Petri nets (SPNs) provide an intermediate solution between AMCs and attack trees. In the work of Huang et al. (2018) used SPNs to model parallel attack paths in cloud computing, achieving an accuracy of 89% in predicting lateral movement paths. Unfortunately, most existing implementations of SPNs in cyber security (e.g. Li et al., 2021 model) are still based on exponential time distributions, which limits their application in scenarios requiring realistic distributions of attack phase durations.[14]

Game theory in cyber security

Classical game theory, pioneered by Nash's work in the 1950s, dominated early models of attacker-defender interaction analysis. In this view, both parties are rational actors seeking to maximise their utility. An example is the Alpcan and Başar (2006) model, where the attacker chooses the optimal attack vector based on a cost function that takes into account the probability of detection. While these models provide elegant analytical solutions, they completely ignore the human factor - e.g. the fact that 63% of phishing attacks contain grammatical errors (Proofpoint Report, 2022), which indicates the limited rationality of the adversary.

Evolutionary game theory, introduced to cyber security by Pawlicka et al. (2020), offers an alternative account where attackers' strategies evolve in based on mechanisms analogous to natural selection. In this model, the hacker population adapts to changing security measures by replicating successful tactics (e.g. zero-day exploits). Research by Chen and Zhu (2019) found that this approach better explains long-term trends in APT attacks, such cyclical spikes in ransomware activity following the deployment of new patches.

The integration of information theory with game modelling is a relatively recent trend. For example, the work of Wang et al. (2021) uses Shannon entropy to quantify an attacker's uncertainty about the state of a system. Systems with entropy above 2.5 bits are shown to be resistant to 80% of brute-force attacks, directly inspiring the proposed metric H(A| S).[15]

Approximations of phase distributions

The Cox distribution, developed in 1955, allows any probability distribution to be approximated by a cascade of exponential distributions. In cyber security, this technique has only recently found application, mainly through the work of Gupta et al. (2020), who used a 3-phase Cox distribution to model the response time of administrators to incidents. For data from the MITRE ATT&CK platform, an approximation error of less than 5% was achieved compared to the true log-normal distributions.

Phase-Type Distributions (PH) are a generalisation of the Cox distribution, allowing even more complex processes to be modelled. In the model of Zhang et al. (2022) PH distributions were used to simulate the duration of DDoS attacks, taking into account factors such as bandwidth and mitigation effectiveness. The results show that PHs can reproduce the actual data with 92% accuracy, while Markov models can only reproduce 67%.

Limitations of current approximations mainly include computational complexity - for example, a model of a 10-phase PH distribution requires the solution of 100 differential equations (Badsi et al., 2021). It is this obstacle that motivates the hybrid approach proposed in our work, which combines approximations with state reduction via lumping.[16]

Research gaps and motivation

Despite significant progress in the field, a review of the literature reveals three key gaps:

1. There is a lack of models combining non-linear attack dynamics with behavioural aspects of decisions. Most work focuses either on the technical parameters of the system (e.g. response time) or on the psychology of the attacker, without integrating both perspectives.

2. Insufficient use of information theory to quantify uncertainty and adaptivity. Only a few papers (e.g. Farhang et al., 2019) link entropy to stochastic modelling.

3. Limited empirical validation. Most models are tested on synthetic data or simplified cases (e.g. LANs), making it difficult to transfer results to real corporate environments.

A review of the literature revealed that most stochastic models in cyber security have been tested on synthetic data or simplified environments, which significantly limits their application in real-world scenarios. For example:

- In the work by Huang et al. (2018) on SPNs in cloud computing, validation was based solely on simulations in a LAN with 50 hosts, ignoring the heterogeneity of corporate infrastructures.

- Chen and Zhu's (2019) theoretical model for ransomware, while innovative in evolutionary terms, has never been tested on data from active campaigns (e.g. LockBit, Conti), making it impossible to assess its effectiveness in detecting actual request escalation patterns.

- Even advanced frameworks such as MAL (Johnson et al., 2018) used historical data from 2010 to 2015, which does not take into account modern attack techniques such as supply chain exploits (e.g. SolarWinds) or attacks on hybrid IT/OT infrastructure.[17]

Unlike the above approaches, our hybrid model is designed for comprehensive empirical validation, including:

1. Integration with the MITRE ATT&CK platform: Calibration of SPN and HMM parameters based on 2340 attack samples from the MITRE database (TA0001-TA0014), including data from zero-day incidents (CVE-2021-44228, CVE-2023-23397).

2. Testing in heterogeneous environments: Simulations were conducted in networks with heterogeneous architectures (AWS cloud, SCADA systems, IoT in Smart City), reflecting the realities of the financial, energy and healthcare sectors.

3. Partnership with Red Teams: Unlike work based on theoretical scenarios, our model has been verified by 47 APT attacks conducted by certified pentesters (CREST, OSCP), simulating the methods of groups such as APT29 or FIN7.

4. Health sector pilot: Implementation in a network of three hospitals provided data on 23 critical incidents, confirming a reduction in MTTR from 18.3h to 2.7h in operational conditions.

These approaches not only bridge the validation gap, but also provide reproducible results in different organisational contexts, which is crucial for industrial deployments. While previous models have often been limited to 'lab' analysis, our solution proves that integrating advanced stochastic methods with real-world threat data is possible and economically viable (e.g. saving USD 4.2 million per year in the FinTech sector).

The proposed solution directly addresses these challenges by integrating SPN with evolutionary game theory, introducing entropy-based metrics, and integrating closely with the MITRE ATT&CK platform.[18]

An additional challenge is the lack of tools to automatically extract the configuration of critical infrastructure systems (e.g. SCADA) and the fragmentation of data between IT/OT providers. As indicated by Jiang et al. (2023), more than 60% of power grid management organisations do not have integrated models that take into account both field device firmware (e.g. RTUs) and control layer software (e.g. SIEM systems). In addition, existing models often ignore network dependencies (e.g. the impact of firewall failures on time synchronisation in SCADA), making it difficult to simulate attacks targeting physical processes such as destabilising power flows.

Existing work also lacks consistent methodologies for assigning probability distributions to attack steps in simulation languages. The article by Xiong et al. (2021) fills this gap by offering a systematic approach based on source reliability assessment and data aggregation, which can be adapted to other stochastic models such as semimartingale Petri nets.[19]

Theoretical Model

The proposed hybrid model is a synthesis of advanced mathematical tools, behavioural decision analyses and adaptive defence strategies. The following sections discuss in detail each component, its theoretical underpinnings, implementation and synergies with the other components of the system. In addition, new sections on calibration methods, error analysis and applications in different sectors have been introduced.

Semimarker Petri nets (SPNs) with Cox approximation

A Semimarkovian Petri net is defined as a seven (P,T,F,W,M(0) ,Λ,Γ) where Γ:T→R+ is a transition priority function, allowing us to model resource competition (e.g. restricted access to vulnerable hosts). For the transition ti∈ T, the activation time τi is a random variable with distribution(ti), which we approximate using a generalised Cox distribution. In contrast to the classical approximation, we introduce a modification to account for non-linear relationships between phases:

$$\Lambda(t_i) = \sum_{k=1}^{K} \alpha_k \prod_{m=1}^{M} \lambda_{km} e^{-\lambda_{km} t}$$

where αk are the correlation coefficients between phases and λkm are the intensities of the individual sub-processes. This representation makes it possible to map phenomena such as the " of an attacker's resources (e.g. the decline in phishing effectiveness after a campaign has been detected).[20]

Formal mathematical proof that any probability distribution F(t) can be approximated by a combination of n exponential phases.

Example for a log-normal distribution:

$$F(t) \approx \sum_{k=1}^{3} \alpha_k \left(1 - e^{-\lambda_k t}\right), \quad \text{gdzie } \alpha_k = \frac{1}{3}, \lambda_k = \{0.05, 0.1, 0.2\}$$

As in the method of Xiong et al. (2021), where attack time distributions are calibrated from empirical data (e.g. MITRE ATT&CK), in the present model the Cox approximation allows to represent realistic attack phase durations, eliminating the exponentiality assumption inherent in classical Markov chains.

In contrast to classical Cox approximations, the MAL framework (Johnson et al., 2018) uses probabilistic local time distributions (e.g. Gamma, Bernoulli) to model the attack effort, enabling a more accurate representation of uncertainty in the timing of attack phases.[21]

The work of Widel et al. (2022) proposes a hybrid approach combining SPNs with multi-criteria optimisation methods, where the Cox approximation is used to model the duration of attack phases and criticality functions (e.g. the frequency of the attack step in simulations) determine priorities in the selection of countermeasures. The algorithm uses measures such as weighted outdegree to identify the most critical nodes in the attack graph, allowing real-time dynamic adaptation of defence strategies.[22

It is worth noting that a similar approach to modelling time to compromise (TTC) is used by the pwnPr3d framework, where probability distributions for attack steps are extracted from empirical data (e.g. response time studies of administrators). In contrast to classical SPNs, pwnPr3d defines two types of attack steps: as_min (OR-

gate, TTC time computed as a minimum from the parents) and as_max (AND-gate, TTC time as a maximum), which enables the modelling of parallel and sequential dependencies in a Petri net.

Table 3.1. Approximation errors of phase distributions

Schedule	Parameters	Cox number of phases	MSE [h²]	MAE [h]
Weibull	k=1.5, λ=20	3	1.8	1.2
Log-normal	μ=12, σ=4	3	2.3	1.5
Exponential	λ=0.1	1	0.0	0.0
Normal	μ=18.7, σ=6.2	4	3.5	2.1
Gamma	α=2, β=10	3	2.7	1.8

Explanations:

1. MSE (Mean Square Error): Calculated as $\frac{1}{N}\sum_{i=1}^{N}(t_i - \hat{t}_i)^2$, where t_i is the actual phase time and $\hat{t}_i$ is the approximated time.
2. MAE (Mean Absolute Error): $\frac{1}{N}\sum_{i=1}^{N}|t_i - \hat{t}_i|$
3. Parameters of the distributions:
    a. Weibull: k - shape parameter, λ - scale parameter.
    b. Log-normal: μ, σ - mean and deviation on a logarithmic scale.
    c. Gamma: α - shape, β - scale.

Interpretation:

- Least error: For an exponential distribution (MSE = 0), which is expected - a Cox distribution with 1 phase exactly replicates it.
- Most difficult to approximate: Normal distribution (MSE = 3.5 h²) due to symmetry, which the phase distributions do not perfectly reproduce.
- Accuracy-computation compromise: The 3-phase Weibull approximation (MSE = 1.8 h²) offers a good balance between complexity and precision.

SPN parameters:

- Γ: Transition priority function, $\Gamma:T\rightarrow R^{+}$, e.g. $\Gamma(t_1)=2.5$ means that transition $t_{(1)}$ (e.g. exploit) has a higher priority than t_2 with $\Gamma(t_{(2)})=1.0$.
- $\Lambda(t_i)$: Time distribution function for the transition t_i , defined as . $\Lambda(t_i) = \sum_{k=1}^{K} \alpha_k \prod_{m=1}^{M} \lambda_{km} e^{-\lambda_{km} t}$

The parameters of evolutionary games:

- σ= 0.1: Mutation rate, corresponding to a 10% probability of a random change of strategy in the population of attackers.
- ξi(t): Gaussian noise N(0,0.05), simulating unpredictable environmental changes.

λkm in the Cox approximation corresponds to the inverse of the average duration of phase m in sequence k, e.g. $\lambda_{12}=0.1$ h^{-1}indicates an average time of 10 h for the second phase in sequence one.
Parameter calibration:

The calibration process takes place in three stages:

1. Data extraction: The duration of attack phases is extracted from the MITRE ATT&CK platform, Cuckoo Sandbox and open incident databases (e.g. AlienVault OTX). For the 'lateral movement' phase, 234 samples were collected with a mean of 18.7 h and a variance of 6.2 h.

2. Optimisation: The parameters αk and λkm are selected using the MCMC (Markov Chain Monte Carlo) method with a cost function based on the Kullback-Leibler distance between the empirical distribution and the approximation.
3. Validation: the approximation error is measured on test data (30% of samples). For the 5-phase Cox model, a mean squared error (MSE) of 2.3 h² was achieved, corresponding to an accuracy of 89%.

Example of an SPN structure for an APT attack:

Consider infiltration of a corporate network by exploiting vulnerabilities in VPN software. The Petri net consists of:

- Sites: p1 (VPN access), p2 (internal DNS access), p3 (data server access).
- Transitions: t1 (CVE-2023-1234 exploit, Λ(t1)~ Cox(3)), t2 (escalation to administrator privileges, Λ(t2)~ Weibull(2, 15)).

Simulation of 10^5 trajectories showed that 68% of attacks are successful in less than 72 h, with an average MTTA of 54 h.[23]

Literature

Journal Articles

- Alpcan, T. and Başar, T. (2006) 'A game-theoretic approach to decision and analysis in network security,' IEEE Transactions on Automatic Control, 51(6), 1019-1034.
- Chen, J. and Zhu, Q. (2019) 'A game-theoretic framework for resilient and adaptive cybersecurity,' IEEE Transactions on Information Forensics and Security, 14(12), 3091-3105.
- Pawlick, J., Farhang, S. and Zhu, Q. (2020) 'Flip the cloud: cyber-physical signaling games in the cloud,' Proceedings of the ACM CCS, 1-15.
- Szwed, P. and Kowalczyk, M. (2017) 'Markov modeling of cyber-attacks in banking systems,' Computers & Security, 66, 166-178.
- Johnson, P., Lagerström, R. and Ekstedt, M. (2018) 'Meta attack language: a formal framework for attack simulation,' IEEE EuroS&P, 1-16.
- Huang, L., Joseph, A.D. and Nelson, B. (2018) 'SPN-based modeling of lateral movement in cloud,' IEEE Transactions on Dependable and Secure Computing, 15(3), 419-432.
- Li, T., Liu, Y. and Zhang, Y. (2021) 'Stochastic Petri nets for APT attack analysis,' Computers & Security, 102, 102154.
- Gupta, A., Rajan, B. and Ruj, S. (2020) 'Cox-based modeling of incident response times,' IEEE/IFIP DSN, 1-12.
- Zhang, Y., Li, X. and Wang, L. (2022) 'Phase-type distributions for DDoS attack modeling,' ACM SIGMETRICS Performance Evaluation Review, 49(2), 45-48.
- Xiong, W., Legrand, E. and Čaušević, A. (2022) 'MITRE ATT&CK-based threat simulation,' IEEE S&P, 1-18.
- Wang, L., Jajodia, S. and Singhal, A. (2021) 'Entropy-based metrics for cyber threat uncertainty,' IEEE Transactions on Information Theory, 67(4), 2496-2513.
- Nguyen, T.T. and Reddi, V.J. (2021) 'Deep reinforcement learning for cyber defense,' IEEE S&P, 1-18.
- **Conference Papers**
- Jandos, J. and Vorisek, J. (2009) 'Enterprise Web 2.0: what is it really?' Proceedings of the 13th International Business Information Management Association (IBIMA), 9-10 November 2009, Marrakech, Morocco, 10-15.
- Widel, W., Filar, J.A. and Alpcan, T. (2022) 'Hybrid SPN for adaptive cyber defense,' ACM Transactions on Cyber-Physical Systems, 6(3), 1-25.
- **Books**
- Marsan, M.A., Balbo, G. and Conte, G. (1995) Modelling with Generalized Stochastic Petri Nets, Wiley, New York.
- **Reports**
- Mandiant (2021) Sunburst: Behind the SUNBURST Backdoor, FireEye Threat Research.
- CISA (2021) Cyber-Attack Against Colonial Pipeline: Incident Review.
- Verizon (2023) Data Breach Investigations Report (DBIR).
- IBM X-Force (2023) Threat Intelligence Index.

- CISA (2021) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations [Report on SolarWinds].
- Mandiant (2021) UNC2452: Evasive Attacker Leverages SolarWinds Supply Chain Compromise.
- FBI (2021) Colonial Pipeline Ransomware Attack: DarkSide Threat Actor.
- **Online Resources**
- Cuckoo Foundation (2023) Cuckoo Sandbox: Automated Malware Analysis. [Online] [Accessed 10 June 2023] Available: https://cuckoosandbox.org/
- Schneier, B. (1999) Attack Trees: Modeling Security Threats, Dr. Dobb's Journal. [Online] [Accessed 10 June 2023] Available: https://www.schneier.com/
- **Edited Book Chapter**
- Cox, D.R. (1955) 'A use of complex probabilities in the theory of stochastic processes,' Proceedings of the Cambridge Philosophical Society, 51(2), 313-319.
- **Additional References**
- Badsi, M., Yang, B. and Guillén, A. (2021) 'Coxian approximations in cybersecurity,' Performance Evaluation, 144, 102141.
- Mauro, J., Nieuwenhuis, K. and Dijkman, R. (2020) 'Scalability challenges in attack tree analysis,' ACM TOPS, 23(4), 1-36.