Information Security Games

Drexel University
Candidacy Exam - March 2 2021

Erick Galinkin

What is Information Security?

Confidentiality: Information can only be read by trusted parties.

Damaged by unauthorized access, exploitation, poor access controls

Integrity: Information can only be written or modified by trusted parties.

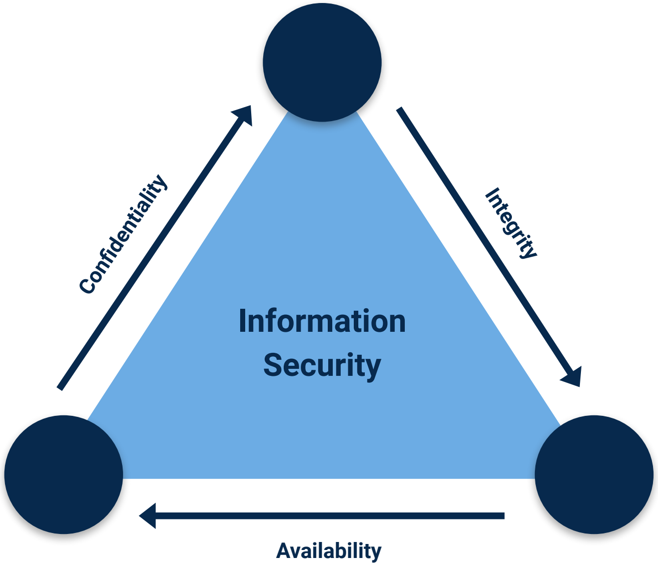
Damaged by person-in-the-middle attacks, data poisoning attacks

Availability: Information can be written or read when trusted parties need it.

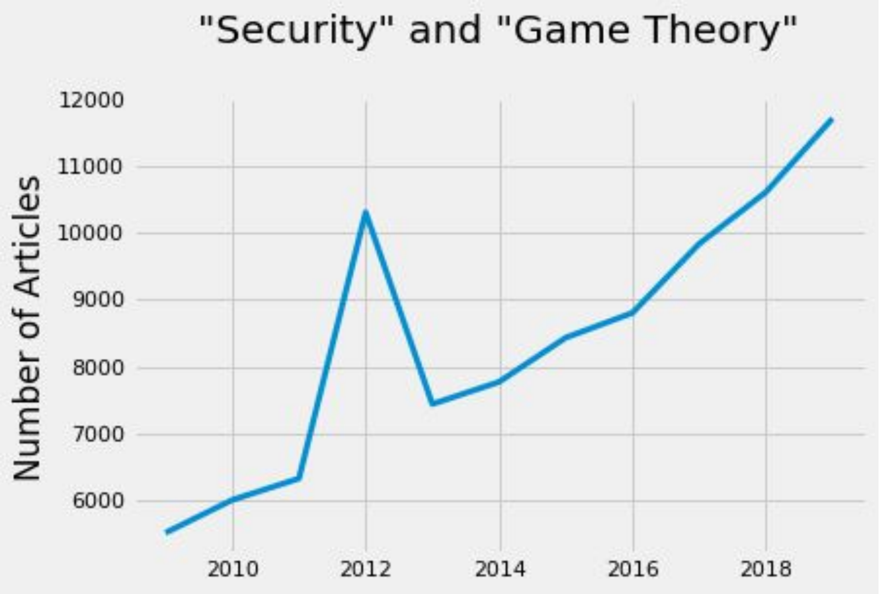
Damaged by ransomware, denial of service attacks

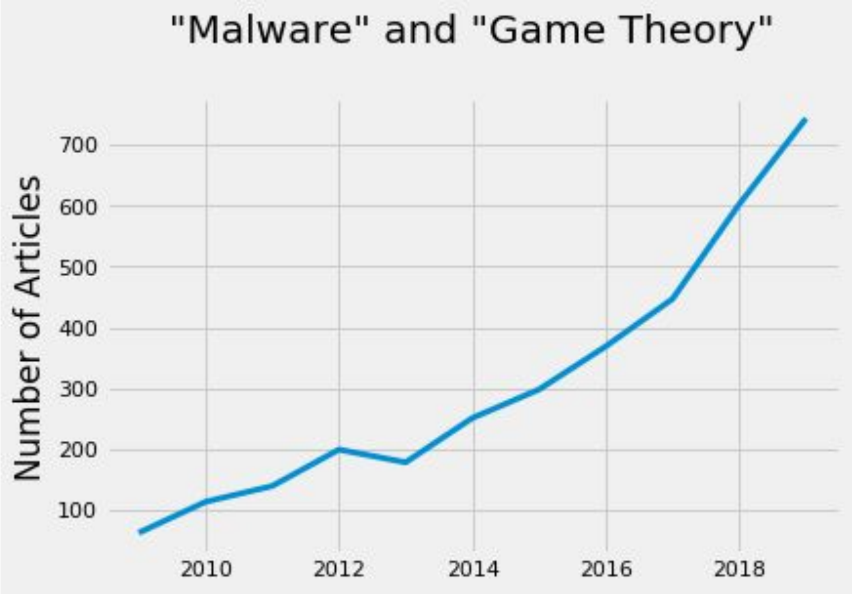
Game Theory & Security

“One of the chief difficulties lies in properly describing the assumptions that have to be made about the motives of the individual” - John vonNeumann [17]



Literature Trends: 2009 - 2019





Attackers and Defenders

We assume that a defender controls a computer network or computer system and an attacker seeks to compromise the confidentiality, integrity, and/or availability of that system.

Brown *et al.*[1], conclude that attackers have the advantage due to the highly asymmetrical nature of cyber attack.

The State of Play

- **Setting:**
  - Network vs. Endpoint
- **Preparation for an attack:**
  - Simultaneous vs. Sequential
- **Utility:**
  - Zero-sum games vs. General-sum games
- **Visibility:**
  - Perfect information vs. Imperfect information
  - Complete information vs. Incomplete information

Network

Most of the literature addresses the network framing. Many consider worms: self-propogating malware.

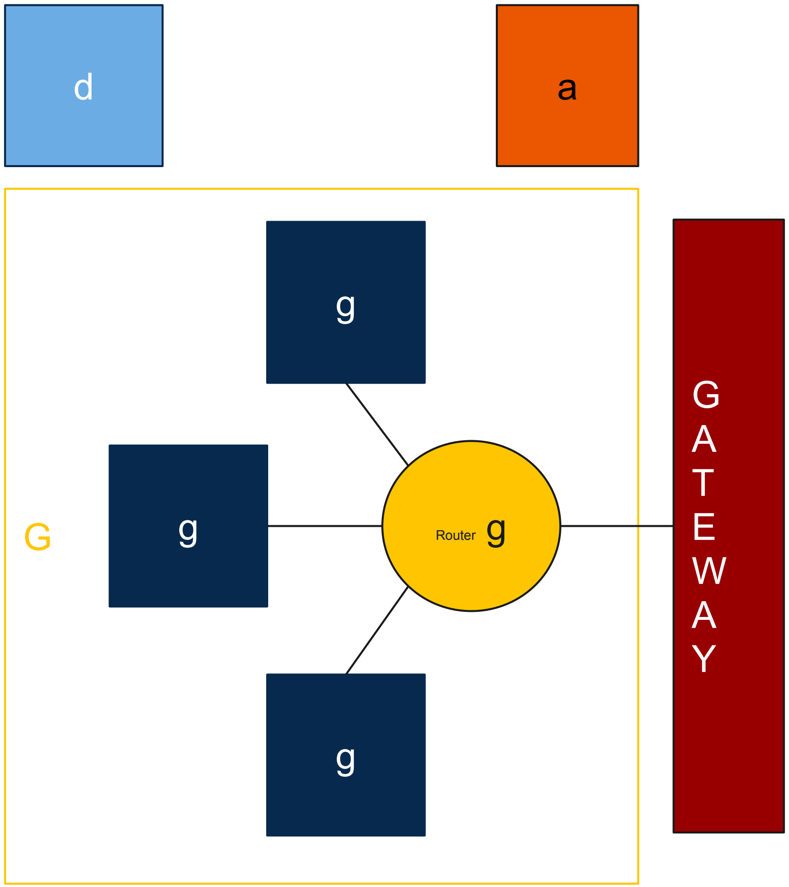
1. Worms are rare (only 8 since 2010)
2. The articles surveyed fail to consider attacker network tactics in a framework like MITRE ATT&CK

Endpoint

Endpoint security is crucial to defending infrastructure since infecting an endpoint is the ultimate goal of most attackers. We also see very little literature consider how game theory and endpoint security.

Agents run on the endpoint using heuristics or signatures [7]

There are also remediations which can be automatically generated [13] following malware attack.



G - Graph of network
g - nodes in network
a - attacker(s)
d - defender(s)

$$\Gamma = (I, \Sigma, \Omega, U)$$

$$I = \{a, d\}$$

$$\Omega = \{\omega_g\}, \forall g \in G$$

Simultaneous Games

Each player in the game must make their decision in the context of the information they have and cannot change their play based on the other player's move.

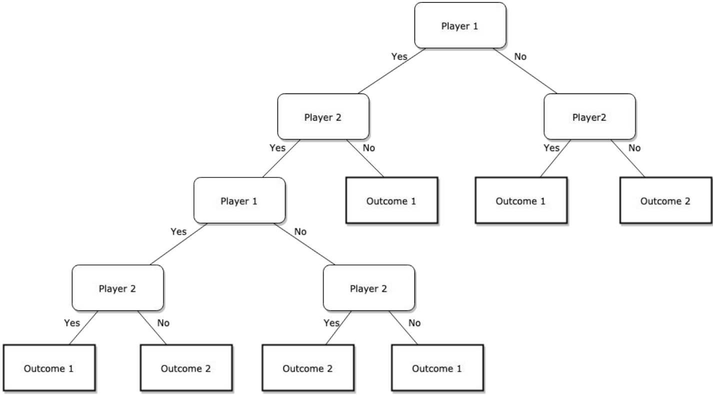
Simultaneous games are rare in the literature [1, 5].

Sequential Games

In sequential games, one player chooses their action before another chooses theirs.

Most authors [1, 5, 7, 9] use them to represent the interplay between attackers and defenders.

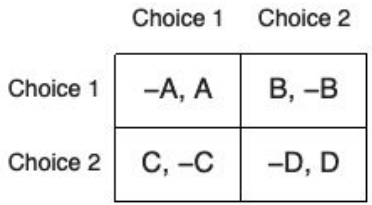
Defender payoff is optimized when they move first [1, 5, 9]



Zero-Sum Games

Zero sum games are games where the attacker’s payoff is exactly the cost to the defender and vice versa.

Zero-sum games allow for the use of the saddle-point strategies developed by Khouzani *et al.* [7] whose threat model is heavily based on human epidemic models.



	Choice 1	Choice 2
Choice 1	–A, A	B, –B
Choice 2	C, –C	–D, D

Image courtesy of Creative Commons

General Sum Games

General sum games are games which have outcomes where both players may have positive or negative utility - there are win/win and lose/lose outcomes.

In general sum games, the attacker can fail to achieve their objective but remediating or preventing the attack still has a cost to the defender, so both players “lose” [17].

Complete Information Games

Complete information games assume that all knowledge about all players is available to all other players. This includes utility functions and payoffs for all players.

This does NOT mean that the state of the game is known to all players.

$$\Gamma = (I, \Sigma, \Omega, U)$$

Incomplete Information Games

In incomplete information games there is some uncertainty about how other players will behave.

Chatterjee [4] considers how this uncertainty manifests itself and propagates in attacker payoffs.

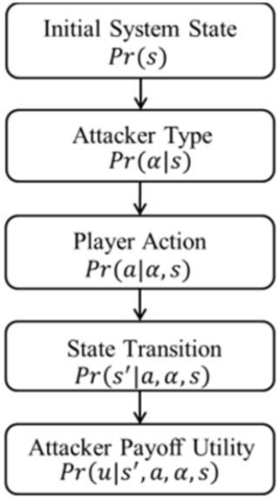
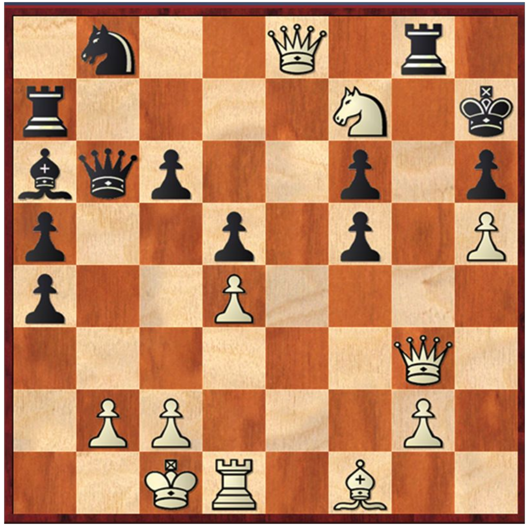


Figure 1 from Chatterjee *et al.* [10]

Perfect Information Games

A perfect information assumes that all players have knowledge of the entire game state - there is no hidden information.

Leader-follower* games [1, 6] are complete, perfect information, sequential games.



Leader-follower games are typically referred to as Stackelberg games in the literature, named after Heinrich Freiherr von Stackelberg.

Imperfect Information Games

Imperfect information games or hidden information games assume that some information about the game state is private - for example, in poker, one’s cards are hidden from their opponents.

Stochastic games [2, 5, 12, 15, 18] are imperfect information games.

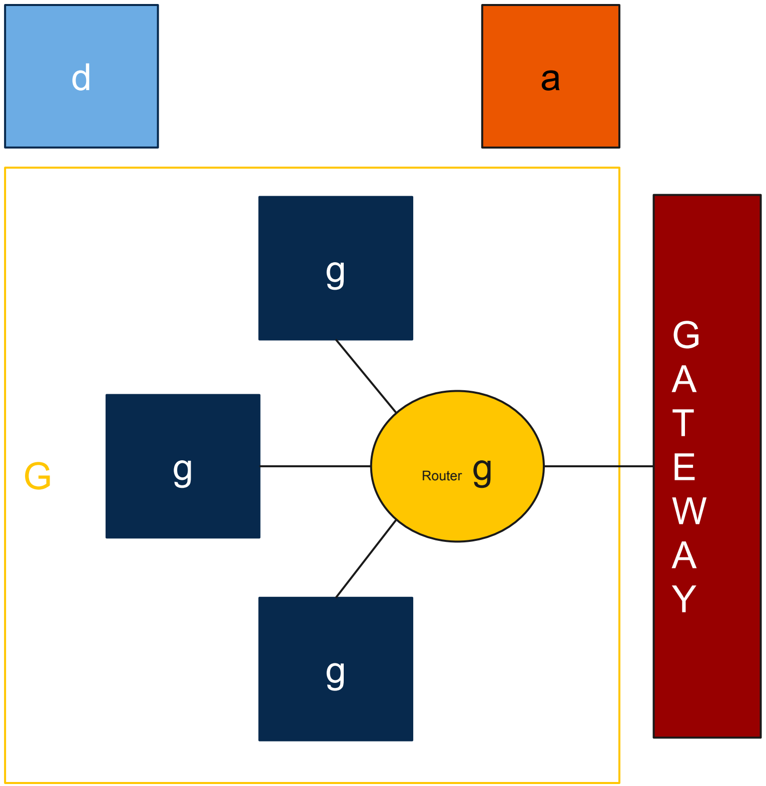
Bayesian games [4, 10, 16] are a particular type of stochastic game.

Coalitional Approaches

Coalitional games are games in which cooperation between several players working toward their common good is considered.

Saad *et al.* [13] seeks to model real-world organizations where interdependencies, vulnerabilities, resources, and organizational friction must defend a single network against attack from a coalition of attackers.

Imperfect Information



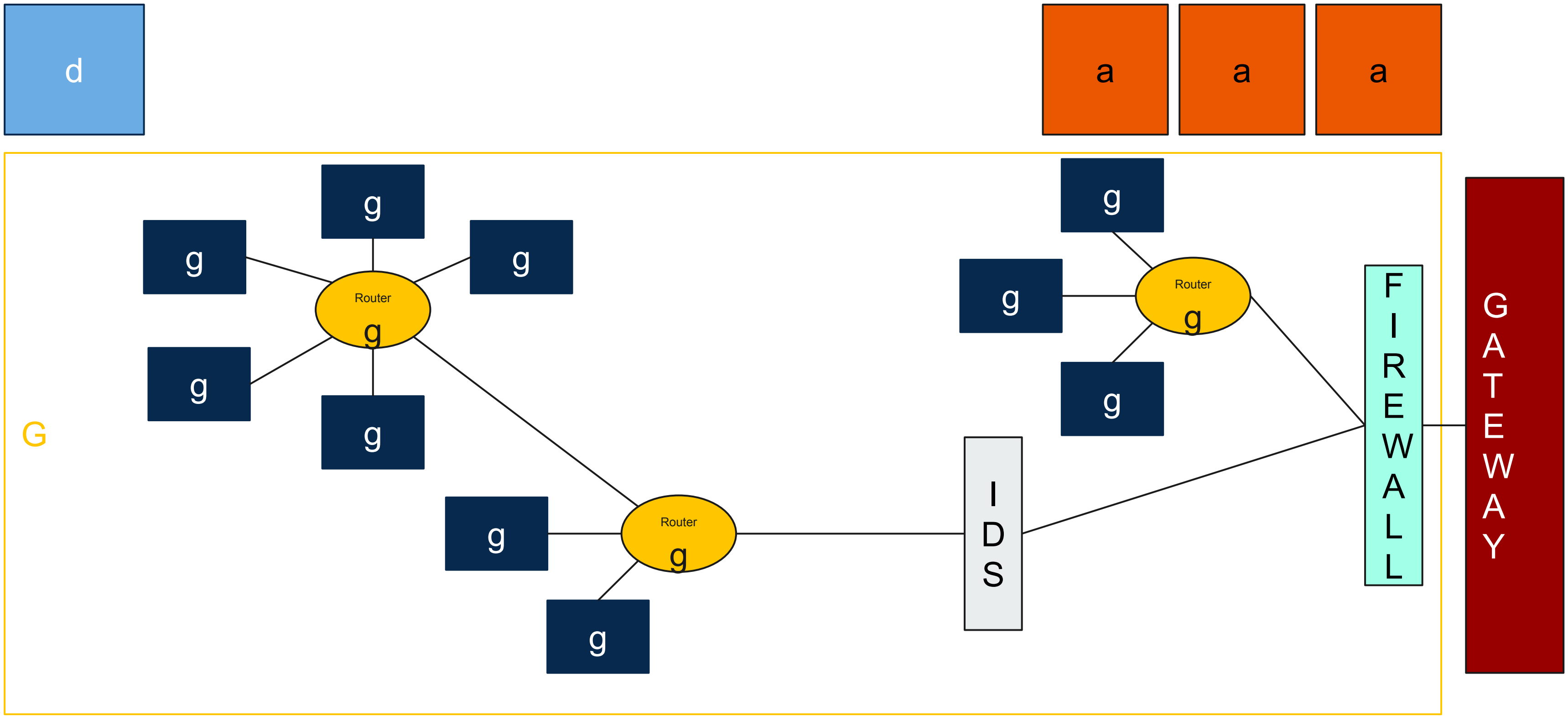
G - Graph of network
g - nodes in network
a - attacker(s)
d - defender(s)

$$\Gamma = (I, \Sigma, \Omega, U)$$

$$I = \{a, d\}$$

$$\Omega = \{\omega_g\}, \forall g \in G$$

Adding Complexity to Games



	Perfect Information	Imperfect Information
Complete Information	He [6] Khouzani [7] Saad [13]	Bommannavar[2] Cui [5] Nguyen [12] Sallhammer [15] Williamson [18]
Incomplete Information	Luo [11]	Chatterjee [4] Liu [10] Sartea [16]

State of the Art

There is no consensus on the state of the art.

Recent work by Khouzani [8] considers a probabilistic attack graph and operates under the least-restrictive set of assumptions.

Evaluation of Models

Information security relies on the applicability of research in real-world scenarios.

Those that do use real data [15, 17] evaluate their model do so on relatively simple problems.

Open Problems and Gaps

- Compositionality and open games
- Attacker’s perspective
- Cloud and mixed environment security
- Empirical verification

1. Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces.*
2. Bommannavar, P., Alpcan, T., & Bambos, N. (2011). Security risk management via dynamic games with learning. IEEE International Conference on Communications.
3. Chatterjee, S., Tipireddy, R., Oster, M., & Halappanavar, M. (2016). Propagating Mixed Uncertainties in Cyber Attacker Payoffs : Exploration of Two-Phase Monte Carlo Sampling and Probability Bounds Analysis.
4. Cui, X., Tan, X., Zhang, Y., & Xi, H. (2008). A markov game theory-based risk assessment model for network information system. Proceedings - International Conference on Computer Science and Software Engineering, CSSE 2008.
5. He, F., Zhuang, J., & Rao, N. (2012). *Game Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures.*
6. Kolbitsch, C., Comparetti, P. M., Kruegel, C., Kirda, E., Zhou, X., & Wang, X. F. (2009). Effective and efficient malware detection at the end host. Proceedings of the 18th USENIX Security Symposium.
7. Khouzani, M. H. R., Sarkar, S., & Altman, E. (2012). Saddle-point strategies in malware attack. *IEEE Journal on Selected Areas in Communications.*
8. Khouzani, M. H. R., Liu, Z., & Malacaria, P. (2019). Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. European Journal of Operational Research.
9. Liu, Y., Comaniciu, C., & Man, H. (2006). A Bayesian game approach for intrusion detection in wireless ad hoc networks. *ACM International Conference Proceeding Series, 199.*
10. Luo, Y., Szidarovszky, F., Al-Nashif, Y., & Hariri, S. (2010). Game Theory Based Network Security. Journal of Information Security.
11. Nguyen, K. C., Alpcan, T., & Başar, T. (2009). Stochastic games for security in networks with interdependent nodes. Proceedings of the 2009 International Conference on Game Theory for Networks, GameNets '09.
12. Paleari, R., Martignoni, L., Passerini, E., Davidson, D., Fredrikson, M., Giffin, J., & Jha, S. (2010). Automatic generation of remediation procedures for malware infections. Proceedings of the 19th USENIX Security Symposium.

13. Saad, W., Alpcan, T., Başar, T., & Hjørungnes, A. (2010). Coalitional game theory for security risk management. 5th International Conference on Internet Monitoring and Protection, ICIMP 2010.
14. Sallhammar, K., Helvik, B. E., & Knapskog, S. J. (2006). On stochastic modeling for integrated security and dependability evaluation. Journal of Networks.
15. Sartea, R., Chalkiadakis, G., Farinelli, A., & Murari, M. (2020). Bayesian active malware analysis. Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS.
16. von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. Princeton University Press.
17. Williamson, S., Ong, C. H., Williamson, S. A., & Hui, O. C. (2012). Active Malware Analysis using Stochastic Games.