Dealing with Advanced Persistent Threats: Case Studies*

Professor Wanlei Zhou

Vice Rector (Academic Affairs)

Dean of Faculty of Data Science

City University of Macau

wlzhou@cityu.mo

https://cityu.edu.mo/; https://sites.google.com/site/wanleizhou/Home

* Based on the following work from my research group:

1. Lu-Xing Yang, Pengdeng Li, Xiaofan Yang, Yong Xiang, Frank Jiang and Wanlei Zhou, "Effective quarantine and recovery scheme against advanced persistent threat," **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, 51(10): 5977-5991 (2021).
2. Dayong Ye, Tianqing Zhu, Sheng Shen, Wanlei Zhou: "A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries". **IEEE Transactions on Information Forensics and Security.** 16: 569-584 (2021).
3. Lu-Xing Yang, Pengdeng Li, Yushu Zhang, Xiaofan Yang, Yong Xiang, Wanlei Zhou: "Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach". **IEEE Transactions on Information Forensics and Security.** 14(7): 1713-1728 (2019).

澳門城市大學
Universidade da Cidade de Macau
City University of Macau

Outlines

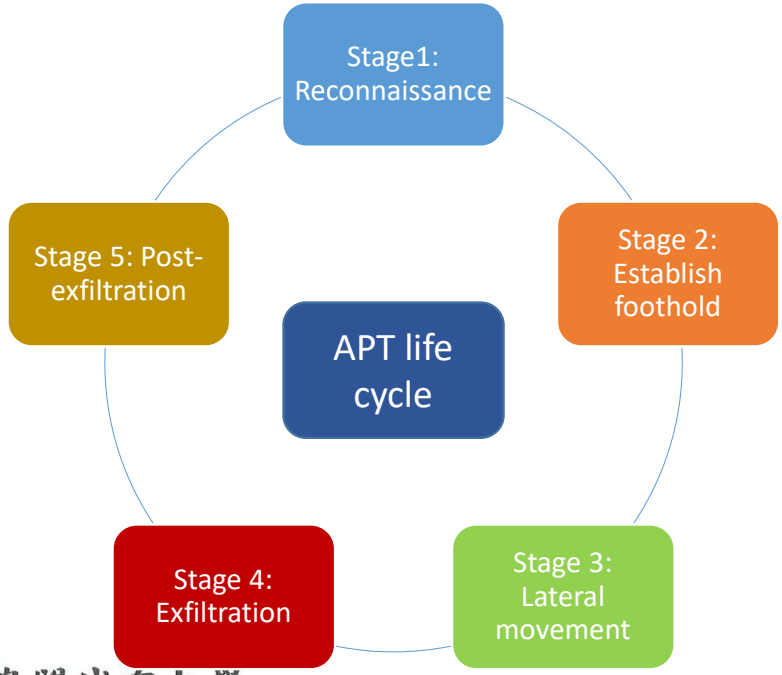
- Advanced Persistent Threats
- Three case studies to deal with APT attacks in various stages
  - A counter-measure to defend against reconnaissance
  - A counter-measure to defend against lateral movement
  - A counter-measure to customize a dynamic quarantine and recovery (QAR) scheme to minimize the APT impact.
- Discussions

Advanced Persistent Threats

澳門城市大學
Universidade da Cidade de Macau
City University of Macau

A severe cyber attack: advanced persistent threats

- An advanced persistent threat (APT) is a stealthy threat actor which gains unauthorized access to a computer network and remains undetected for an extended period.



An APT attack has five stages: reconnaissance, establish foothold, lateral movement, exfiltration, and post-exfiltration.

- **Reconnaissance** means monitoring and scanning systems in the target network.
- **Establish foothold** represents the attacker's successful entry into the target network.
- **Lateral movement** means that the attacker needs to stay undetected within the target network in search of critical components or data.
- **Exfiltration** The attacker's actions, comprising, retrieving and sending sensitive data to the attacker's command and control center, fall under this stage.
- **Post-exfiltration** activities include continuing to exfiltrate critical data or deleting evidence for a clean exit from the target network.

Advanced persistent threats

- The intention of an APT is to exfiltrate or steal data rather than cause a network outage, denial of service or infect systems with malware.
- APT attacks differ from traditional web application threats, in that:
  - They're significantly more complex.
  - They're not hit and run attacks—once a network is infiltrated, the perpetrator remains in order to attain as much information as possible.
  - They're manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets.
  - They often aim to infiltrate an entire network, as opposed to one specific part.
- A successful advanced persistent threat can be extremely effective and beneficial to the attacker. For nation states, there are significant political motivations, such as military intelligence. For smaller groups, APTs can lead to significant competitive advantages or lucrative payouts.

Case study 1: A counter-measure against reconnaissance*

A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries

Dayong Ye, Tianqing Zhu, *Member, IEEE*, Sheng Shen, and Wanlei Zhou, *Senior Member, IEEE*

***Abstract*— Cyber deception is one of the key approaches used to mislead attackers by hiding or providing inaccurate system information. There are two main factors limiting the real-world application of existing cyber deception approaches. The first limitation is that the number of systems in a network is assumed to be fixed. However, in the real world, the number of systems may be dynamically changed. The second limitation is that attackers' strategies are simplified in the literature. However, in the real world, attackers may be more powerful than theory suggests. To overcome these two limitations, we propose a novel differentially private game theoretic approach to cyber deception. In this proposed approach, a defender adopts differential privacy mechanisms to strategically change the number of systems and obfuscate the configurations of systems, while an attacker adopts a Bayesian inference approach to infer the real configurations of systems. By using the differential privacy technique, the proposed approach can 1) reduce the impacts on network security resulting from changes in the number of systems and 2) resist attacks regardless of attackers' reasoning power. The experimental results demonstrate the effectiveness of the proposed approach.**

***Index Terms*— Cyber deception, differential privacy, game theory.**

I. Introduction

NETWORK security is one of the most important problems faced by enterprises and countries today [1]. Before launching a network attack, malicious attackers often scan systems in a network to identify vulnerabilities that can be exploited to intrude into the network [2]. The aim of this scanning is to understand the configurations of these systems, including the operating systems they are running, and their IP/MAC addresses on the network. Once these questions are answered, attackers can efficiently formulate plans to attack the network. In order to prevent attackers from receiving true answers to these questions and thus reduce the likelihood of successful attacks, cyber deception techniques are

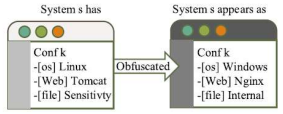


Fig. 1. System s with configuration k is obfuscated to and appears as configuration k'.

induce him to attack non-critical systems by hiding or lying about the configurations of the systems in a network [4]. For example, an important system s with configuration k is obfuscated by the defender to appear as a less important system with configuration k'. Thus, when an attacker scans the network, he observes system s with configuration k' rather than k, as shown in Fig. 1. Since configuration k' is less important than k, the attacker may skip over system s.

To model such an interaction between an attacker and a defender, game theory has been adopted as a means of studying cyber deception [5], [6]. Game theory is a theoretical framework to study the decision-making strategies of competing players, where each player aims to maximize her or his own utility. In cyber deception, defenders and attackers can be modelled as players. Game theory, thus, can be used to investigate how a defender reacts to an attacker and vice versa. Game theoretic formulation overcomes traditional solutions to cyber deception in many aspects, such as proven mathematics, reliable defense mechanisms and timely actions [7].

Existing game theoretic approaches, however, have two common limitations. The first limitation is that the number of

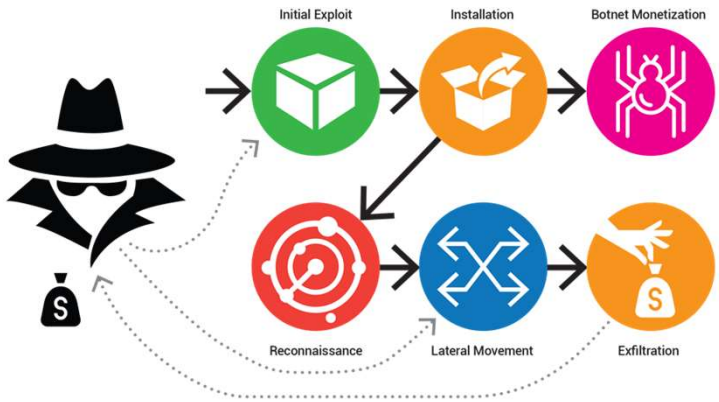
* Based on the following work from my research group:

Dayong Ye, Tianqing Zhu, Sheng Shen, Wanlei Zhou: "A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries". **IEEE Transactions on Information Forensics and Security.** 16: 569-584 (2021).

澳門城市大學
Universidade da Cidade de Macau
City University of Macau

A counter-measure against reconnaissance

- During reconnaissance, the attacker monitors and scans the systems in the target network in order to obtain the configuration information of these systems. Once the information is obtained, the attacker analyses the vulnerabilities of the configurations and then launches his attacks.
- The first important defense research problem against APT attacks is the counter-measure against reconnaissance.
- We adopt the **cyber deception** technique as a counter-measure to deceive the attacker.



Cyber Deception

- Cyber deception is one of the key approaches used to mislead attackers by hiding the real systems' ground truth or providing inaccurate system information to manipulate adversary's course of actions. It utilizes lures and decoys to entice, engage, misdirect and ultimately detect attackers. Legacy: honeypots.
  - Crafted information by the defender (used to mislead), and
  - Wrong actions taken by attackers (as a result of deception).
- The main aim of deception technology is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage.
- Key requirements for deception technology implementation:
  - It is indistinguishable and fresh to the attacker.
  - Automation (e.g., built-in machine learning and AI technologies)

Cyber Deception Games

- Game theoretic concepts provide a framework for defining and quantifying the moves of attackers and defenders and the payoffs associated with each move. By understanding the possible moves for either player in a given state, and the outcome for a certain sequence of actions, the defender can choose to leverage cyber deception and steer the outcome of a cyber attack in the defender's favour.
- A cyber deception game is played with imperfect and incomplete information, where the attacker and defender do not have perfect visibility into the history of all actions of the other player.
  - Attackers normally assume systems operate in the context of honesty, so defender can have the greatest impact if implemented before the attacker can use knowledge of the defender's environment to develop their attack.
  - An attacker operating with incomplete information may assume that the defender only has a legitimate set of moves and real, valuable resources. This assumption can form the basis for cyber deception.

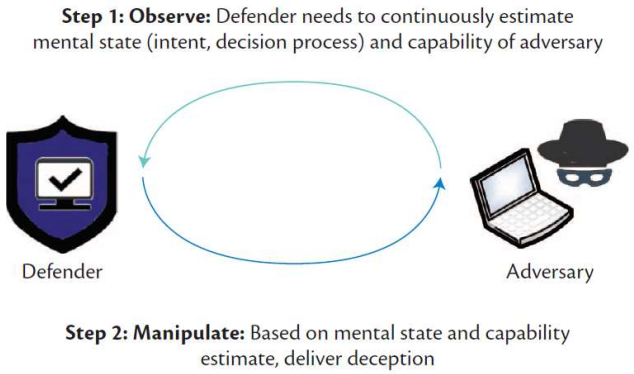


Figure from: Cliff Wang and Zhuo Lu, "Cyber Deception: Overview and the Road Ahead", IEEE Security & Privacy, March/April 2018, pp. 80-85.

Cyber deception game in reconnaissance

- The cyber deception game models an interaction between a defender and an attacker. The attacker aims to scan the configuration of systems, while the defender offers fake configurations to confuse the attacker.

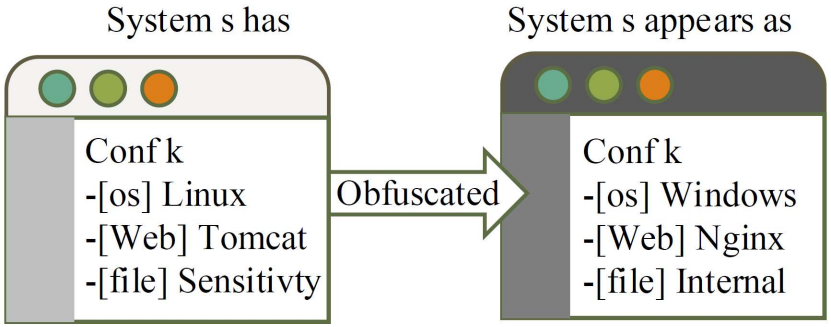
Cyber deception game in reconnaissance

- The challenge of cyber deception is how to obfuscate configuration of systems to deceive the attacker while avoiding the attacker to deduce the real configuration of each system.

Generally, if the defender uses a deterministic strategy to obfuscate configurations, her strategy can be predicted by the attacker who can then deduce the real configuration of each system.

The research problem of defense against APT attacks

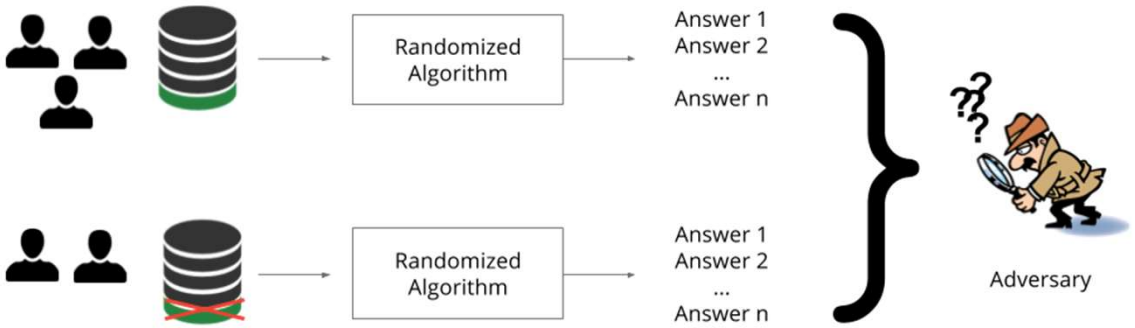
- A counter-measure against the reconnaissance is to use the cyber deception technique to obfuscate the configuration of systems to deceive the attacker.



For example, the real configuration of system *s* is: os-Linux, Web-Tomcat, file-Sensitivity. After obfuscation, the configuration appears as os-Windows, Web-Nginx, file-Internal. The obfuscated configuration is then shown to the attacker to deceive him.

Our solution: differential privacy

- Differential privacy is a promising technique. It can guarantee that any individual record being stored in or removed from a dataset makes little difference on an analytical output of the dataset.



In this work, we adopt a differential privacy mechanism to obfuscate the configuration of systems. As differential privacy can guarantee that an adversary cannot deduce whether a data record is in a dataset, it can also guarantee that the attacker in cyber deception game cannot deduce whether the configuration of a system is real or fake.

Differential privacy in cyber deception game

In each round of the game, there are four steps.

- Step 1: The defender obfuscates the configuration of systems by adding Laplacian noise to the number of systems with each configuration.
- Step 2: The defender allocates systems to configurations based on the probability of a system being attacked.
- Step 3: For each system, the attacker estimates the probability with which an observed configuration k' could be a real configuration k using Bayesian inference
- Step 4: Based on the estimation, the attacker calculates the expected utility gain of selecting each configuration. The attacker selects a configuration with the highest expected utility as the target.

Two evaluation metrics are used to compare our strategy with Greedy and Greedy-mixed approaches:

- The attacker's utility gain (i.e., the defender's utility loss): the utility gain is received by attacking systems;
- The defender's cost: it is the defender's deployment cost used to obfuscate configurations of systems.

Case study 2: A counter-measure against lateral movement*

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 14, NO. 7, JULY 2019 1713

Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach

Lu-Xing Yang, *Member, IEEE*, Pengdeng Li, Yushu Zhang, *Member, IEEE*, Xiaofan Yang, *Member, IEEE*, Yong Xiang, *Senior Member, IEEE*, and Wanlei Zhou, *Senior Member, IEEE*

***Abstract*— Advanced persistent threat (APT) is a new kind of cyberattack that poses a serious threat to modern society. When an APT campaign on an organization has been identified, the available repair resources must be reasonably allocated to the potentially insecure hosts to mitigate the potential loss of the organization. We refer to the feasible repair resource allocation strategies as repair strategies. This paper focuses on the APT repair problem, i.e., the problem of developing effective repair strategies for organizations. First, for an organization with time-varying communication relationship, we establish an evolution model of the organization's expected state, in which the impact of lateral movement of APT is accommodated. On this basis, we model the APT repair problem as a differential Nash game problem (the APT repair game) in which the attacker attempts to maximize his potential benefit, and the organization manages to minimize its potential loss. Second, we derive a system (the potential system) for calculating a potential Nash equilibrium of an APT repair game, and we examine the structure of the potential attack and repair strategies in a potential Nash equilibrium. Next, we solve some potential systems to get the corresponding potential Nash equilibria. Finally, by comparison with a large number of randomly generated attack and repair strategies, we conclude that the potential Nash equilibrium of each APT repair game is a Nash equilibrium of the game. Therefore, we recommend to organizations their respective potential repair strategies. Our findings help to better understand and effectively defend against APT.**

***Index Terms*— Cybersecurity, advanced persistent threat, APT repair problem, epidemic modeling, differential Nash game, potential Nash equilibrium.**

Manuscript received June 1, 2018; revised September 24, 2018 and November 6, 2018; accepted November 28, 2018. Date of publication December 6, 2018; date of current version March 20, 2019. This work

I. Introduction

In RECENT years, many high-profile organizations, ranging from large-scale enterprises and financial institutions to government sectors, have experienced a new type of cyber attack—*advanced persistent threat* (APT) [1], [2]. The notorious Stuxnet, Duqu, Flame, and Gauss are just a few examples of APT [3]. Different from traditional cyberattacks, an APT attacker is typically a well-resourced and well-organized entity, with the intent of stealing sensitive data covertly and on a long-term basis from the target organization. Through extended reconnaissance and employing sophisticated social engineering techniques, an APT can always avoid traditional cyber defense measures to infiltrate the organization, causing serious data leakage. In conclusion, APT has posed a severe threat to modern society. Consequently, how to effectively defend against APT has been a major concern in the domain of cybersecurity [4], [5].

A. Background

Imagine an organization in which there is a storage server used to store all sensitive data as well as a set of hosts used to handle daily affairs. Due to business requirement, every host is authorized to access a certain portion of the storage server and communicate with a subset of other hosts. See Fig. 1 for the diagram of such an organization. In real world, the majority of modern organizations fall into this type.

In this setting, the sensitive data located within the storage server might be the target of APT. If this is the case, the APT

* Based on the following work from my research group:

Lu-Xing Yang, Pengdeng Li, Yushu Zhang, Xiaofan Yang, Yong Xiang, Wanlei Zhou: "Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach". **IEEE Transactions on Information Forensics and Security.** 14(7): 1713-1728 (2019).

澳門城市大學
Universidade da Cidade de Macau
City University of Macau

A counter-measure against lateral movement

- An organization in which there is a storage server used to store all sensitive data as well as a set of hosts used to handle daily affairs. Due to business requirement, every host is authorized to access a certain portion of the storage server and communicate with a subset of other hosts (Fig 1).
- In the lateral movement stage, a covert connection between each hijacked host and the attacker's host (the command-and control server) will be established. As a result, the attacker can exploit the hijacked hosts to (a) gain partial access to the storage server, and (b) infiltrate the secure hosts through lateral movement to obtain more sensitive data (Fig 2).

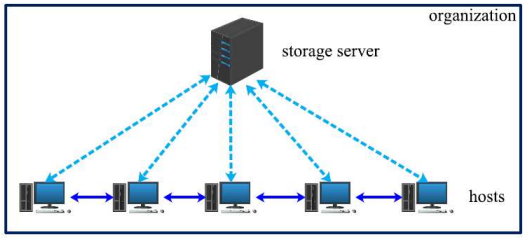


Fig. 1. Diagram of an organization, where the dark blue double-arrowed solid lines represent normal business interactions between hosts, and the light blue double-arrowed dashed lines represent normal data flows between hosts and the storage server.

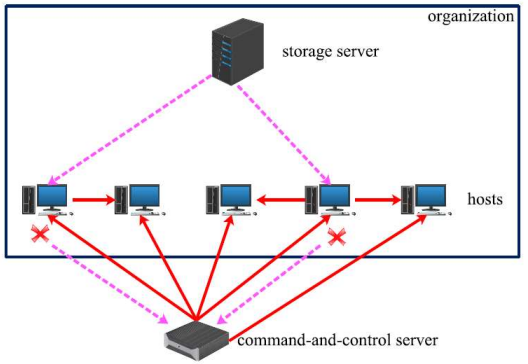
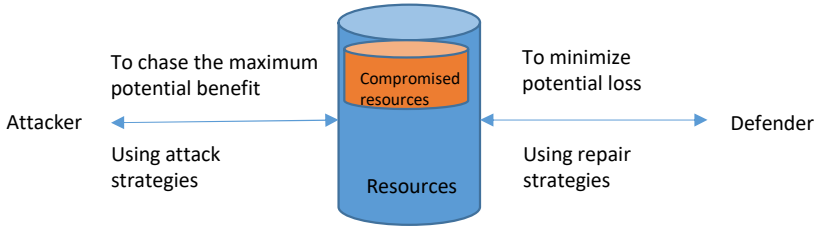


Fig. 2. Diagram of an APT, where the hosts with red cross represent the hijacked hosts, the red single-arrowed solid lines represent direct attacks or lateral movements, and the pink single-arrowed dashed lines represent abnormal data flows from the storage server to the attacker's command-and-control server.

A counter-measure against lateral movement

- The APT Repair Problem: When an APT has been identified and the probability of each host being insecure has been estimated, the next work to do is to ascertain and repair all of the hijacked hosts in a timely manner to mitigate the potential loss of the organization.
- we have to reasonably allocate the available repair resources to the potentially insecure hosts to mitigate the organization's potential loss. We refer all of the feasible repair resource allocation strategies as repair strategies. The APT repair problem can be viewed as seeking a repair strategy to minimize the organization's expected loss.
- We model the APT repair problem as a differential Nash game problem (the APT repair game) in which the attacker chases the maximum potential benefit and the organization manages to minimize its potential loss.

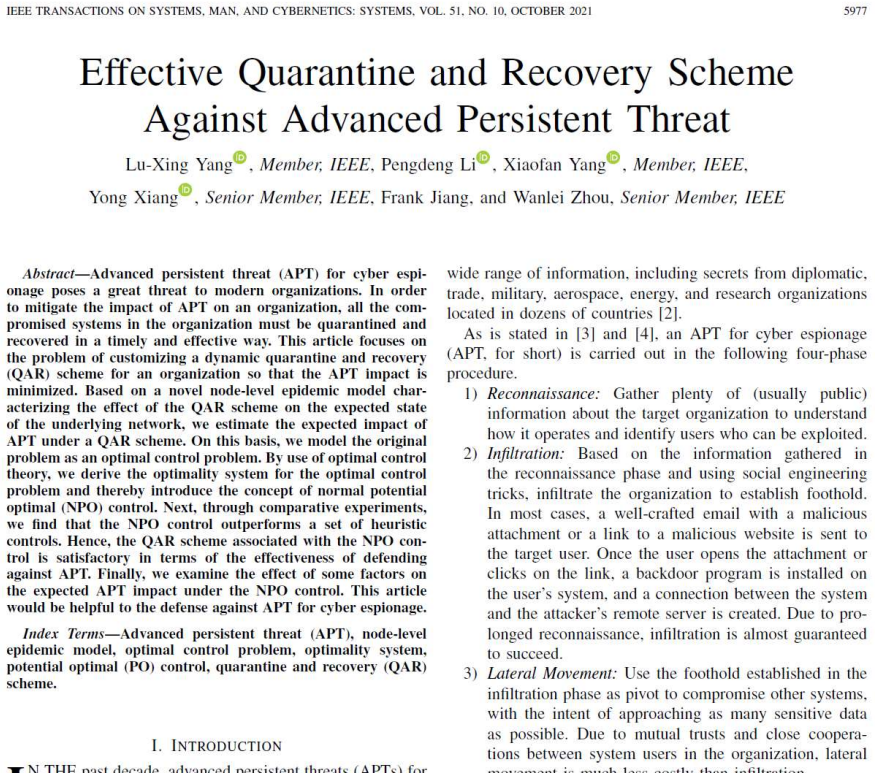


The APT repair game to deal with lateral movement

A counter-measure against lateral movement

- Steps in using the differential game theory:
  1. derive a system (the potential system) for calculating a potential Nash equilibrium of an APT repair game;
  2. examine the structure of the potential attack and repair strategies in a potential Nash equilibrium;
  3. develop an algorithm for numerically solving potential systems; and
  4. solve the potential systems of some APT repair games to obtain the corresponding potential Nash equilibria.
- We propose an algorithm for generating a random strategy pair. By comparison with a large number of randomly generated attack and repair strategies, we conclude that the potential Nash equilibrium of each APT repair game is exactly a Nash equilibrium of the game. Therefore, we recommend to organizations their respective potential repair strategies.

Case study 3: A counter-measure to customize a dynamic quarantine and recovery (QAR) scheme to minimize the APT impact*



Effective Quarantine and Recovery Scheme Against Advanced Persistent Threat

Lu-Xing Yang, *Member, IEEE*, Pengdeng Li, Xiaofan Yang, *Member, IEEE*, Yong Xiang, *Senior Member, IEEE*, Frank Jiang, and Wanlei Zhou, *Senior Member, IEEE*

***Abstract*—Advanced persistent threat (APT) for cyber espionage poses a great threat to modern organizations. In order to mitigate the impact of APT on an organization, all the compromised systems in the organization must be quarantined and recovered in a timely and effective way. This article focuses on the problem of customizing a dynamic quarantine and recovery (QAR) scheme for an organization so that the APT impact is minimized. Based on a novel node-level epidemic model characterizing the effect of the QAR scheme on the expected state of the underlying network, we estimate the expected impact of APT under a QAR scheme. On this basis, we model the original problem as an optimal control problem. By use of optimal control theory, we derive the optimality system for the optimal control problem and thereby introduce the concept of normal potential optimal (NPO) control. Next, through comparative experiments, we find that the NPO control outperforms a set of heuristic controls. Hence, the QAR scheme associated with the NPO control is satisfactory in terms of the effectiveness of defending against APT. Finally, we examine the effect of some factors on the expected APT impact under the NPO control. This article would be helpful to the defense against APT for cyber espionage.**

***Index Terms*—Advanced persistent threat (APT), node-level epidemic model, optimal control problem, optimality system, potential optimal (PO) control, quarantine and recovery (QAR) scheme.**

I. Introduction

IN THE past decade, advanced persistent threats (APTs) for

wide range of information, including secrets from diplomatic, trade, military, aerospace, energy, and research organizations located in dozens of countries [2].

As is stated in [3] and [4], an APT for cyber espionage (APT, for short) is carried out in the following four-phase procedure.

1) *Reconnaissance:* Gather plenty of (usually public) information about the target organization to understand how it operates and identify users who can be exploited.
2) *Infiltration:* Based on the information gathered in the reconnaissance phase and using social engineering tricks, infiltrate the organization to establish foothold. In most cases, a well-crafted email with a malicious attachment or a link to a malicious website is sent to the target user. Once the user opens the attachment or clicks on the link, a backdoor program is installed on the user's system, and a connection between the system and the attacker's remote server is created. Due to prolonged reconnaissance, infiltration is almost guaranteed to succeed.
3) *Lateral Movement:* Use the foothold established in the infiltration phase as pivot to compromise other systems, with the intent of approaching as many sensitive data as possible. Due to mutual trusts and close cooperations between system users in the organization, lateral

* Based on the following work from my research group:

Lu-Xing Yang, Pengdeng Li, Xiaofan Yang, Yong Xiang, Frank Jiang and Wanlei Zhou, "Effective quarantine and recovery scheme against advanced persistent threat," **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, 51(10): 5977-5991 (2021).

Address the quarantine and recovery (QAR) problem

- The industry standard for APT response is as follows.
  - Detection: Use proven APT detection programs to find indicators of APT. This is an automated process.
  - Quarantine: Check all the suspect systems found in the detection phase to see if they are really compromised, followed by isolating all the confirmed compromised systems from the network, with the goal of preventing lateral movements from these systems to other systems.
  - Recovery: Repair all the quarantined systems, followed by putting all the recovered systems back to the network. As a result, these systems become uncompromised and work properly.
- Quarantine and recovery (QAR) manipulations are resource-intensive; but the resources available for QAR manipulations are limited. Hence, we face the following problem.
  - **QAR Problem: For an organization under APT, customize a dynamic QAR scheme so that the APT impact is minimized.**

Address the quarantine and recovery (QAR) problem

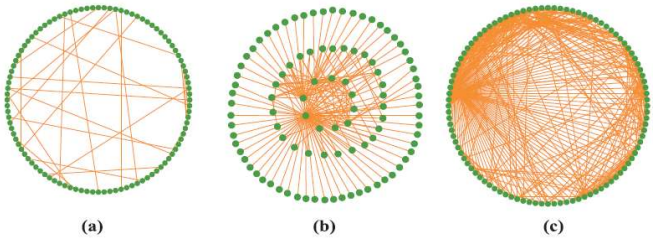
- Estimating the APT Impact
  - Lateral movement of APT can be regarded as a propagation phenomenon, where the compromised state propagates from system to system. In order to estimate the APT impact, we have to establish an epidemic model that accounts for the effect of lateral movement.
  - In recent years, the node-level epidemic modeling technique has been applied to active cyber defense. Here, we establish a node-level epidemic model that characterizes the effect of the QAR scheme on the network's expected statement.
  - We use a closed-loop susceptible-infected-quarantined-susceptible (SIQS) model to describe the lateral movement of APT, where all the QAR rates in the model are time-varying and under control of the defender.

Address the quarantine and recovery (QAR) problem

- Step 1. We introduce a node-level epidemic model characterizing the effect of the QAR scheme on the network's expected state, to estimate the expected APT impact under a QAR scheme.
- Step 2. Use the node-level epidemic model, we reduce the QAR problem to an optimal control problem (the QAR$*$ problem) in which the objective functional stands for the expected APT impact under a QAR scheme, each optimal control stands for a QAR scheme that minimizes the expected APT impact.
- Step 3. We derive the optimality system for the QAR$*$ problem.
  - 3.1. We introduce the concept of normal potential optimal (NPO) control and use it for addressing the QAR problem.
  - 3.2. Although the NPO control may not be optimal, by comparison with a set of heuristic QAR schemes, we find the effectiveness of the NPO control is satisfactory. Therefore, we recommend NPO control schemes to organizations.

Address the quarantine and recovery (QAR) problem

- Through experiments, we examine the effect of some factors on the expected APT impact under the NPO control, finding some interesting results.
  - Experiment setting: Two representative network models: a small-world network and a scale-free network; plus a real-world email network.
  - In all the experiments, we need to obtain the NPO controls of a set of QAR$*$ instances by solving the corresponding optimality systems.
  - Examine the effectiveness of the NPO control: We first describe a set of heuristic quarantine schemes as well as a set of heuristic recovery schemes. Then we compare the NPO control with a set of heuristic QAR schemes in terms of the expected APT impact.
  - Conclusion: The NPO control achieves a satisfactory effectiveness.



(a) A small-world network. (b) A scale-free network. (c). A real email network

Discussions

- We are the first to introduce differential privacy into cyber deception game. By using differential privacy, the attacker cannot deduce the real configuration of each system.
- We are the first to develop an effective repair strategy for an organization using differential game theory. Our findings help to better understand and effectively defend against APT.
- We are the first to address the quarantine and recovery (QAR) problem in APT and developed a counter-measure to customize a dynamic quarantine and recovery scheme to minimize the APT impact.

2021 Major Publications in My Group Related to Security and Privacy

1. Tianrui Zong, Yong Xiang, Iynkaran Natgunanathan, Longxiang Gao, Guang Hua, Wanlei Zhou, "Non-linear-echo Based Anti-collusion Mechanism for Audio Signals", **IEEE/ACM Transactions on Audio, Speech and Language Processing**, Vol. 29, 2021, pp. 969-984.
2. Juan Zhao, Tianrui Zong, Yong Xiang, Longxiang Gao, Wanlei Zhou, Gleb Beliakov, "Desynchronization Attacks Resilient Watermarking Method Based on Frequency Singular Value Coefficient Modification". **IEEE/ACM Transactions on Audio, Speech and Language Processing** 29: 2282-2295 (2021).
3. Jianghua Liu, Jingyu Hou, Wenjie Yang, Yang Xiang, Wanlei Zhou, Wei Wu, and Xinyi Huang, "Leakage-Free Dissemination of Authenticated Tree-Structured Data with Multi-Party Control", **IEEE Transactions on Computers**, Vol. 70, No. 7, July 2021.
4. Jianghua Liu, Jinhua Ma, Yang Xiang, Wanlei Zhou, and Xinyi Huang, "Authenticated Medical Documents Releasing with Privacy Protection and Release Control". **IEEE Transactions on Dependable and Secure Computing**, Jan/Feb 2021, Volume: 18, Issue: 1, pp. 448-459.
5. Dayong Ye, Tianqing Zhu, Sheng Shen, Wanlei Zhou: "A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries". **IEEE Transactions on Information Forensics and Security**. 16: 569-584 (2021).
6. Youyang Qu, Shui Yu, Wanlei Zhou, Shiping Chen, and Jun Wu, "Customizable Reliable Privacy-Preserving Data Sharing in Cyber-Physical Social Network", **IEEE Transactions on Network Science and Engineering**, Vol. 8, No. 1, January-March 2021, pp. 269-281.
7. Jianchao Lu, Xi Zheng, Lihong Tang, Tianyi Zhang, Quan Z. Sheng, Chen Wang, Jiong Jin, Shui Yu, Wanlei Zhou, "Can Steering Wheel Detect Your Driving Fatigue", **IEEE Transactions on Vehicular Technology**, 70(6): 5537-5550 (2021).
8. Lu-Xing Yang, Pengdeng Li, Xiaofan Yang, Yong Xiang, Frank Jiang and Wanlei Zhou, "Effective quarantine and recovery scheme against advanced persistent threat," **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, 51(10): 5977-5991 (2021).
9. Lefeng Zhang, Tianqing Zhu, Ping Xiong, Wanlei Zhou and Philip S. Yu, "More than Privacy: Adopting Differential Privacy in Game-theoretic Mechanism Design", **ACM Computing Surveys**. 54:7, Article 136 (June 2021). Online https://dl.acm.org/doi/fullHtml/10.1145/3460771
10. Aneesh Chivukula, Xinghao Yang, Wei Liu, Tianqing Zhu, Wanlei Zhou, "Game Theoretical Adversarial Deep Learning with Variational Adversaries". Accepted by **IEEE Transactions on Knowledge and Data Engineering**, early access: https://ieeexplore.ieee.org/document/8986751

2021 Major Publications in My Group Related to Security and Privacy

11. Tao Zhang, Tianqing Zhu, Jing Li, Mengde Han, Wanlei Zhou, Philip Yu, "Fairness in Semi-supervised Learning: Unlabeled Data Help to Reduce Discrimination", Accepted by **IEEE Transactions on Knowledge and Data Engineering**, published online as early access: https://ieeexplore.ieee.org/document/9117188
12. Tianqing Zhu, Dayong Ye, Wei Wang, Wanlei Zhou, Philip Yu, "More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence", Accepted by **IEEE Transactions on Knowledge and Data Engineering**, early access: https://ieeexplore.ieee.org/document/9158374
13. Tianqing Zhu, Jin Li, Xiangyu Hu, Ping Xiong, Wanlei Zhou, "The Dynamic Privacy-preserving Mechanisms for Online Dynamic Social Networks". Accepted by **IEEE Transactions on Knowledge and Data Engineering**, early access: https://ieeexplore.ieee.org/document/9165190
14. Dayong Ye, Tianqing Zhu, Zishuo Cheng, Wanlei Zhou and Philip S. Yu, "Differential Advising in Multiagent Reinforcement Learning", accepted by **IEEE Transactions on Cybernetics**, early access: https://ieeexplore.ieee.org/document/9269516
15. Weifa Liang, Yu Ma, Wenzheng Xu, Zichuan Xu, Xiaohua Jia, and Wanlei Zhou, "Request Reliability Augmentation with Service Function Chain Requirements in Mobile Edge Computing", Accepted by **IEEE Transactions on Mobile Computing**, published online as early access: https://ieeexplore.ieee.org/document/9435077
16. Juan Zhao, Tianrui Zong, Yong Xiang, Iynkaran Natgunanathan, Longxiang Gao, Wanlei Zhou, "Desynchronization-attack-resilient audio watermarking mechanism for stereo signals using the linear correlation between channels", Accepted on 1/2/2021 by **The World Wide Web Journal**. early access: https://link.springer.com/article/10.1007/s11280-021-00897-0
17. Jing Li, Weifa Liang, Wenzheng Xu, Zichuan Xu, Xiaohua Jia, Wanlei Zhou, and Jin Zhao, "Maximizing User Service Satisfaction for Delay-Sensitive IoT Applications in Edge Computing", Accepted by **IEEE Transactions on Parallel and Distributed Systems**, early access: https://ieeexplore.ieee.org/document/9521690

Thank you!