Research Statement

Ping Fan KE
School of Computing and Information Systems, Singapore Management University
Tel: (65) 6828-1346; Email: pfke@smu.edu.sg
20 (Day) 12 (Month) 2024 (Year)

Background

There is currently a paradigm shift underway in the design of information systems, moving from a focus on tasks and data to a design approach that emphasizes security and trust. This new secure-by-design approach includes concepts like DevSecOps and Blockchain, which aim to maintain security throughout the system's lifecycle. Several factors may contribute to this change, including the saturation of functional design in software development due to the widespread use of libraries and artificial intelligence, as well as the growing media coverage of cybersecurity incidents and fraud. As a result, improving cybersecurity management has become the primary concern for end-users, businesses, and policy makers.

My research interests span several topics related to security and trust. I primarily focus on cybersecurity, which stems from my experience as a security hacker since the age of nine. Although my early experience centred on the technical aspects of cybersecurity, my subsequent training in business and economics led me to recognize the vital role that management and policy play in this field. As such, my current research focuses on both technical and human factors of cybersecurity, including human behaviour such as incentive issues, strategic reactions, and the misuse of security systems. By taking a comprehensive approach to cybersecurity, my research aims to develop effective strategies to address cybersecurity challenges. In addition, my research interests have expanded beyond traditional business contexts to include emerging technologies due to the prevalence of user-generated content and the resulting trust issues that have shifted from organizational settings to individual settings. The development of artificial intelligence, such as DeepFake, has further exacerbated these issues. Therefore, my research is now exploring the impact of emerging technologies on cybersecurity and trust.

In particular, the growing concern on cybersecurity and trust played a crucial role in the development of Bitcoin, the first application of the Blockchain concept. Its founder, Satoshi Nakamoto, left a message that hinted at the lack of trust in the current financial system worldwide following the bankruptcy of Lehman Brothers, and recent events such as the collapse of Silicon Valley Bank have underscored the persistence of this trust issue. Despite the challenges and open questions facing the Blockchain technology ecosystem, including scalability and privacy issues, its potential as a trust-by-design system offers numerous possibilities for both research and practical applications.

In my capacity as a researcher, I have a broad interest in several themes that pertain to security and trust, encompassing areas such as cybersecurity policy and risk management. My investigations centre on a variety of contexts that are germane to the business world, ranging from supply chain management to Blockchain. In my studies, I utilize both analytical and empirical models. Figure 1 provides a summary of my research framework of cybersecurity and trust. Notably, the emergence of generative artificial intelligence not only introduces opportunities for businesses such as applications for hyper-automation, but also imposes cybersecurity threats when the tools are misused by malicious parties.

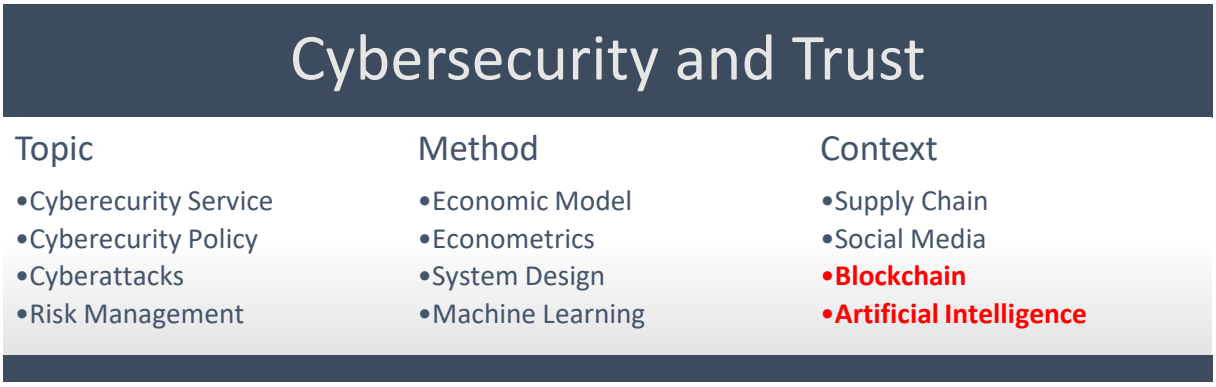

Figure 1. Summary of Research on Cybersecurity and Trust

Research Areas

1. Cybersecurity service

The first part of my thesis focuses on the policy aspect of cybersecurity service. Specifically, I investigate the optimal regulatory options for information security outsourcing services offered by managed security service (MSS) providers. In this context, there are several undesirable characteristics that need to be addressed. Firstly, the service provider may have an incentive to under-provide efforts since the service quality cannot be directly observed by the clients. Consequently, clients may be reluctant to use the services offered by the provider. Although service providers often offer compensation for security breaches, this practice may encourage clients to shirk since compensation is guaranteed. This free-riding issue can lead to both parties caring less about protecting the system, resulting in social inefficiency. Additionally, when a system managed by the service provider is compromised, it can affect other systems in the provider's network, resulting in system interdependency risk, which further undermines the protection offered. To address these issues, I propose a self-regulatory approach that conditions the compensation on the client's *ex post* information on security effort. This information can be obtained through audit trails, which help achieve the socially optimal outcome [1]. Compared to other types of contracts in the literature, my proposed contract solution is also more efficient, even if the market is constrained, such as when service providers are only willing to bear a limited amount of liability. This research has been published in a prestigious journal, Information Systems Research.

Other than the free riding problem, the trust issue is salient in the information security outsourcing services context because of the complexity of cybersecurity solutions and the knowledge discrepancy between clients and service providers. This is called credence good problem in the literature where the service provider can take advantage of information gap such as risk level of the client [2]. With this setting, I find that although it is not feasible to have a market-based contract that induces socially optimal outcome, policy makers could introduce tax and subsidy based on the contract type offered by the service provider to achieve socially optimal outcome [3]. This study is significant not only in contributing to the economic literature on outsourcing, but also in aiding policy makers and practitioners to design incentive-aligning mechanisms to provide better quality in cybersecurity outsourcing services.

2. Cybersecurity policy

Besides market-level analysis, I also study cybersecurity policy at the national level in my thesis. In particular, I examine the effect of national protection policies, particularly PC-based content filtering across the country, on the degree of security of the country. Filtering is a common solution to secure information assets from the harm of malicious software. Industry also proposed the use of national filtering based on the rationale of public health model. For example, Microsoft suggested the computers that are infected by botnet should be quarantined by the Internet service providers. Although policy makers are interested in introducing such a policy, Internet users raise concerns about the effectiveness and possibility of censorship. As the effectiveness of national filtering has never been formally established, I conduct a natural experiment using the policies implemented in Australia and China during 2007 and 2008. To draw statistical inference, I collected cyber-attack data from DShield distributed intrusion detection system, which offers statistics on the daily attack initiated by a country. Since attackers are often using compromised computers to launch cyberattacks, the measurement from DShield reflects the degree of insecurity of a country [4].

Using econometric analysis with a difference-in-difference approach, I found that the policy had worsened the overall security level, despite the effectiveness of the filtering software in blocking malicious content [5]. One possible explanation for this counterintuitive result is the prevalence of filter circumvention tools that emerged due to the implementation of the filtering scheme. By analyzing search interest data from Google Trends, I discovered that cyberattacks increased when there was more interest in circumvention tools like proxies. Another explanation is that the use of filtering software created a false sense of security, as evidenced by the fact that people were less interested in looking for other security protection tools during the policy's effective period. This finding has significant implications for the deployment of national filtering or protection policies, as policymakers should consider the strategic reactions of users [6]. This work has been nominated for the best paper award in a prestigious conference, WITS.

3. Cyberattacks

The prevalence of ransomware attacks has a huge impact on organizations, especially small and medium-sized enterprises (SMEs). One of the most common reasons that SMEs suffer from ransomware attacks is a lack of security controls due to limited resources. Threat monitoring and backup and recovery solutions can be a financial burden for SMEs, which forces them to take unnecessary risks. To address this issue, a more effective security operations center designed to tackle ransomware attacks, named RansomSOC, is proposed [7]. By leveraging open-source intelligence (OSINT) and exploiting the design flaws of ransomware, our solution can detect and respond to ransomware attacks at a lower cost.

One increasingly common type of cyberattack involves the spread of false information, especially on online platforms such as e-commerce sites and social media. This can significantly influence the decision-making process of users who receive such information and may even result in legal consequences for the platform operators. To help these platforms detect false information more efficiently, a framework for domain adaptive transfer learning using adversarial training has been proposed. This framework involves collecting a set of general news articles from trustworthy and untrustworthy sources to serve as the source domain for the deep learning model. A small set of platform-specific data, such as financial news and online reviews, is then used as the target domain for the model. Domain adaptation is used instead of directly training on the platform-specific data, as it can be difficult to collect high-quality labeled data. The framework has been shown to be efficient and provides high balanced accuracy in classifying false content, especially when the transferability score – a metric that measures the similarity between the

source and target domains – is sufficiently high [8]. This research has been published in a prestigious journal, Production and Operations Management.

On the other hand, cyberattacks on Blockchain systems have become increasingly popular due to their potential for financial gain. While many researchers focus on the technical details of smart contract security, I took a different approach by examining the systematic weaknesses of Blockchain using an economic model. Specifically, I discovered that the transaction fees in Blockchain-based payment systems can be even higher than those of traditional centralized monopolistic payment systems, such as SWIFT, when the transaction arrival rate is high. This is because Blockchain has a limited block size for each transaction, which is necessary for convergence and consensus in a distributed system. When there is a limited block size and a high transaction arrival rate, every miner will only select the transactions with the highest transaction fee that can fit into the limited block space. This finding shed light on a new type of cyberattack on Blockchain that involves manipulating transaction fees.

The issue of transaction fees in Blockchain can have a significant impact on the reliability of data in smart contracts, which are designed to be self-executing and trustworthy. If the expected benefit of verifying a contract is less than the cost of paying the fee, some participants may choose not to execute the contract. This creates a vulnerability that can be exploited by malicious actors who gradually degrade the contract's quality over time, which I named it as a “boiling frog attack”. To demonstrate this concept, I used a Token-curated Registry (TCR), which is a smart contract application used to create a trusted list. The result of my economic model showed that participants without a significant holding of tokens were less likely to correct mistakes in the system, which allows adversaries to contaminate the smart contract [9].

The transaction cost in smart contracts not only serves as a deterrence factor but also a tool for adversaries to manipulate the transactions processed by the miners. For instance, Blockchain-based auctions, which are popular in Decentralized Finance (DeFi), can be modeled as a two-stage sequential auction. I have found that adversaries may bid multiple times with a very high transaction fee to crowd out other bidders in the auction, known as a block stuffing attack. This attack can cause market inefficiency and threaten the availability of Blockchain-based auctions. Unlike the boiling frog attack mentioned previously, the block stuffing attack can also be profitable for the adversary [10]. This work has been nominated for the best paper award in a prestigious conference, WISE.

In addition to researching the detection and technical analysis of cyberattacks, I also examine their impact. The DeFi ecosystem has seen a rise in cybersecurity incidents, which have resulted in significant market crashes and instability. While some DeFi protocols have not been able to survive such incidents, others have managed to continue operating well. To better understand the factors that contribute to the resiliency of a DeFi protocol, I compared the total value locked (TVL) of two decentralized lending protocols, Alchemix and Compound, before and after a security incident caused by human error [11]. The results indicate that Alchemix's TVL did not drop significantly after the incident, whereas Compound's TVL fell by 6.19%. One notable difference between the two protocols is that Alchemix is a relatively new project with a flexible governance mechanism, while Compound is a mature project with a strict governance process. For example, after the incident was confirmed, Alchemix's developer could stop the related smart contracts for loss control, whereas Compound's token holders had to vote to suspend the smart contract and wait for a week to enforce the result. This raises an interesting debate about the trade-off between availability (emergency stop) and integrity (developer abuse of the emergency mechanism). This work has been nominated for the best short paper award in a prestigious conference, ICIS.

Digital identity management has become more important to individuals and organizations as online

entities are getting more and more digital identities used in multiple different platforms like Facebook and GitHub. The intersection with the Web3 ecosystems has introduced the concept called decentralized identity (DID), which is often managed as a non-fungible token (NFT) using smart contracts. However, the nature of NFT facilitates easy trading and speculative behavior, and attacks like cybersquatting, where adversaries register for and occupy other famous entities' digital identity and then ask for a high resale price. To assess the economic impact of potential cybersquatting, I examined the trading pattern of the Web3 domain marketplace [12], and the results show that the present of counterfeit Web3 domains from "Ether Name Service" will increase the subsequent resale price of the authentic Web3 domains from "Ethereum Name Services". This work has received the second runner-up of the best short paper award in a prestigious conference, PACIS.

4. Risk management

In June 2014, the online voting platform in Hong Kong called PopVote received an unprecedented distributed denial-of-service (DDoS) attack, which was probably due to its politically sensitive nature. Since there is a shortage of case studies on cybersecurity risk management in real-life settings, I collaborated with cybersecurity professionals in the industry to initiate a project to write a new business case on cybersecurity risk management. We interviewed the PopVote project owner, Dr. Robert Chung, and the IT manager, Jazz Ma, at the University of Hong Kong to discuss the system architecture of PopVote, the incident's process, as well as managerial considerations. We elaborate on the technical aspect of the incident and discuss the alternative choices in the case [13].

When it comes to sensitive information, one major risk that authors or disclosers face is personal threats from accused parties. The accused may even compromise the publisher to obtain the discloser's identity for retaliation purpose. At the same time, the author or discloser may want to receive attribution and compensation for their research and investigation work. These conflicting objectives create a trilemma: the author wants privacy to prevent retaliation but also attribution to receive compensation, and the publication should not rely on a centralized system like a typical publisher to prevent compromise. To address this trilemma, I proposed a decentralized trust system that allows the author to have better control over privacy while receiving attribution and being independent of centralized systems [14].

5. Future Research

The rise of generative artificial intelligence, such as ChatGPT, has brought both opportunities and threats to society and businesses. For example, I have developed a tool to assist the survey developer process and even simulate and data collection part using Large Language Model [15]. However, there are concerns around the privacy and security of these tools, highlighted by incidents like Samsung employees leaked corporate data due to the use of ChatGPT. Therefore, it is essential to investigate the best security practices for using generative artificial intelligence software and tools.

Furthermore, governments worldwide are introducing new laws to manage cybersecurity and tackle cyber threats. For example, Singapore implemented the Cybersecurity Service Provider Licence requirement in October 2022 to ensure quality cybersecurity services, while the Hong Kong government is currently holding a public consultation on reforming cybercrime laws. As an academic, it is vital to provide objective evidence of the potential impact of these policy changes, which can assist policy makers and the public in understanding them better.

Selected Publications and Outputs

1. Hui, K. L., **Ke, P. F.**, Yao, Y., & Yue, W. T. (2019). Bilateral Liability-Based Contracts in Information Security Outsourcing. *Information Systems Research, 30*(2), 411-429.
2. **Ke, P. F.**, Hui, K. L., & Yue, W. T. (2013). Information security as a credence good. In: Adams, A.A., Brenner, M., Smith, M. (eds) *Financial Cryptography and Data Security, Lecture Notes in Computer Science* (Vol. 7862, pp. 83-93). Springer Berlin Heidelberg.
3. Hui, K. L., **Ke, P. F.**, & Yue, W. T. (2014, December). Regulating Information Asymmetry in Information Security Outsourcing Market. In *25th Workshop on Information Systems and Economics (WISE)*, Auckland, New Zealand.
4. **Ke, P. F.**, Hui, K. L., & Yue, W. T. (2015, December). Cybersecurity Regulations and Cyberattacks: A Case Study in China. In *26th Workshop on Information Systems and Economics (WISE)*, Dallas, TX.
5. Hui, K. L., **Ke, P. F.**, & Yue, W. T. (2017, December). An Empirical Study of the Effect of Government-initiated Filter Schemes on Cybersecurity. In *16th Workshop on e-Business (WeB)*, Seoul, South Korea.
6. **Ke, P.F.**, Hui, K. L., & Yue, W. T. (2020, December). The Effect of Content Filtering on the Internet: An Empirical Investigation. In *Workshop on Information Technologies and Systems (WITS)*, Virtual. **[Best Paper Nomination]**
7. Lai, A. C. T., **Ke, P. F.**, Chan, K., Yiu, S. M., Kim, D., Wong, W. K., Wang, S., Muppala, J., & Ho, A. (2022). RansomSOC: A More Effective Security Operations Center to Detect and Respond to Ransomware Attacks. *Journal of Internet Services and Information Security (JISIS)*, 13.
8. Ng, K. C., **Ke, P. F.**, So, M. K., & Tam, K. Y. (2023). Augmenting Fake Content Detection in Online Platforms: A Domain Adaptive Transfer Learning via Adversarial Training Approach. *Production and Operations Management*.
9. **Ke, P.F.** (2018, December). Influence of Transaction Cost on Smart Contract: An Economic Analysis on Token-Curated Registry. In *Pre-ICIS SIGBPS Workshop on Blockchain and Smart Contract (BPS'18)*, San Francisco, CA.
10. **Ke, P. F.**, Chen, J., & Guo, Z. (2021, December). Strategic Behavior and Market Inefficiency in Blockchain-Based Auctions. In *32nd Workshop on Information Systems and Economics (WISE),* Austin, Texas. **[Best Paper Nomination]**
11. **Ke, P.F.,** & Ng, K.C. (2022, December). Bank Error in Whose Favor? A Case Study of Decentralized Finance Misgovernance. In *International Conference on Information System (ICIS) 2022*, Copenhagen, Denmark. **[Best Short Paper Nomination]**
12. **Ke, P. F.** & Lau, Y. M. (2024, July) Exploring the Market Impact of Web3 Identity Imitation in Ethereum Name Service. In *Pacific-Asia Conference on Information Systems (PACIS)* 2024. **[Best Short Paper Award, Second Runner-up]**
13. Hui, K. L., Huang, M., **Ke, P. F.,** & Lai, A. (2016). PopVote: Assessing the Risk of DDoS. Thompson Center for Business Case Studies, HKUST Business School.
14. **Ke, P.F.** (2019, December). The information disclosure trilemma: Privacy, attribution and dependency. In *Workshop on Information Security and Privacy (WISP)*, Munich, Germany.
15. **Ke, P. F.,** & Ng, K. C. (Forthcoming). Human-AI Synergy in Survey Development: Implications from Large Language Models in Business and Research. *ACM Transactions on Management Information Systems*.