Research Statement

Dinh Duc Nha Nguyen (Tony)
Deakin University, Melbourne, Australia

One of my most significant contributions to cybersecurity research includes the development of an innovative authentication framework, to authenticate (Internet of Things) IoT nodes in 5G networks or beyond. We demonstrate that the physical features are unclonable and therefore attackers cannot mimic them. The approach is unique as it employs the unique physical (unclonable) characteristics of IoT devices and statistical theory making it suitable for resource-constrained IoT environments; whereas the previous works use internet traffic features (which can be spoofed) to develop authentication models. Our approach has also laid the groundwork for further research into using the physical features of nodes to design authentication models that protect critical network infrastructure. My work, as lead-author, is published in a top-notch network security outlet, IEEE Transactions on Dependable and Secure Computing (TDSC).

Other works of mine focus more on machine learning, where we proposed approaches to enhance model accuracy by mitigating data sparsity and reducing data dimensionality. These contributions have significantly impacted how machine learning technology is applied in the cybersecurity domain.

Furthermore, during my role as an Associate research fellow on Industry funded project, I have extended my contributions to the cybersecurity field by integrates Post-Quantum Cryptography (PQC) and VPN (Virtual Private Networks), which has garnered attention within the research community, especially as quantum technology is predicted to disrupt all current cryptography.

Past and Current Research

Intrusion Detection in IoT and Next-Generation Networks

The increasing connectivity of devices in IoT ecosystems has exposed networks to new forms of attacks, particularly impersonation and intrusion attempts. My work has contributed significantly to the development and enhancement of intrusion detection mechanisms for these environments. I have explored the use of RF (Radio Frequency) fingerprinting techniques (Physical Unclonable Function) and statistical techniques (Mahalanobis Distance and Chi-squared distribution) to authenticate IoT nodes in a secure and efficient manner. This work outperforms current authentication methods, which rely on supervised and unsupervised learning models to detect anomalies in network traffic, thereby preventing unauthorized access to IoT networks. The research has been applied in various case studies, particularly in 5G networks, which require fast and scalable solutions for intrusion detection. This work also provides a practical solution for ensuring security in environments where devices may have varying computational capabilities and communication protocols.

AI and Machine Learning in Cybersecurity

The integration of AI into cybersecurity has been a key theme in my research. AI-driven models enable more adaptive and efficient security systems that can respond to threats in real time. My work on federated learning-based intrusion detection schemes, published in IEEE TNSM, demonstrates the potential of distributed AI models to secure large-scale networks without compromising user privacy. These models learn from distributed datasets while keeping the data localized, reducing risks associated with centralized data storage.

Moreover, my research proposed effective framework for intrusion detection in 5G networks by leveraging data dimension reduction and anomaly detection architecture at the network edge. This design significantly decreases the training time of traditional machine learning models and enables faster anomaly detections. This framework represents a significant step towards providing an efficient and effective way to empower networks to detect attacks in 5G. The work has been published in IEEE Transactions on Information Forensics and Security, a widely recognized top-tier venue known for its high citation rates and influence within the academic and professional cybersecurity communities.

Furthermore, one of my research focuses is on the challenges of data sparsity in AI models. Data is the backbone of AI models. However, in many real applications, data collection may introduce missing or compromised data caused by device faults, environmental impacts, and attacks. Data sparsity affects the accuracy of AI models, which leads to inaccuracies in any applications based on these models. By exploring correlation values and Fuzzy Information Decomposition theory, we can predict compromised or missing data samples and recover the original values. This method addresses an important problem: recovering compromised or missing sensor values in IoT environments by proposing a sound theoretical approach. This work was funded by the Australian Department of Defence, and it has been submitted to IEEE Transactions on Mobile Computing, where it received a major revision.

Post-Quantum Cryptography and Hybrid Security Models

My recent research centres around hybrid security models that integrate both traditional cryptography and PQC methods, ensuring robust protection against quantum and classical computational threats. As part of the SOCRATES project at Deakin University, I have developed and implemented an automatic hybrid PQC system. This system leverages post-quantum algorithms such as Dilithium and Falcon, alongside traditional algorithms like RSA and ECDSA, to build a secure VPN solution. By testing this system under varying network conditions, we evaluated its resilience and performance in mitigating potential threats posed by quantum computing advancements. This work is critical, as current cryptographic systems are vulnerable to future quantum attacks, and transitioning to quantum-resilient systems is paramount for the security of sensitive data.

Future Research Directions

Intrusion Detection in IoT and Next-Generation Networks

While Physical Unclonable Functions (PUFs) provide robust security at the device level by focusing on the unique physical characteristics of hardware, they primarily authenticate the device itself. This presents a limitation in scenarios where an unauthorized user gains access to the device, as they can still pass authentication based solely on the hardware's identity. To address this gap, we propose extending security to both the user level and the behaviour level. At the user level, authentication will focus on verifying the identity of the specific user operating the device, adding a layer of protection beyond the device itself. At the behaviour level, we aim to monitor and analyse user activities for any abnormal patterns, which can signal unauthorized access or malicious behaviour. By integrating these dimensions, our goal is to develop a comprehensive authentication method and intrusion detection system that not only secures devices but also ensures that both legitimate users and their behaviours are consistently verified. This approach will provide enhanced protection against both device theft and misuse, making security systems more robust and adaptive.

AI-Enhanced Intrusion Detection Systems

Building on my previous work, I intend to explore more on data sparsity, data drift. advanced AI techniques for enhancing intrusion detection systems in next-generation networks. By integrating these systems with cloud-based platforms, I aim to develop scalable solutions that can protect distributed networks from increasingly sophisticated cyberattacks. Additionally, I am interested in investigating the use of AI in automating security decision-making processes. This research will focus on developing AI models that can autonomously adjust security policies in response to real-time threats, thereby reducing the need for human intervention in critical cybersecurity systems.

Quantum-Safe Secure Communication Protocols

As quantum computing becomes more prevalent, my future research will focus on transitioning critical infrastructure systems to quantum-safe cryptographic solutions. This research will involve evaluating the performance of various PQC algorithms across different network infrastructures and exploring how hybrid models can be optimized for real-time applications, such as secure communications in healthcare, finance, and defence sectors. I plan to continue my work on the hybrid PQC system, expanding it to incorporate more dynamic algorithm selection mechanisms based on network conditions like bandwidth and latency. This approach will ensure that systems can adapt to changing network environments while maintaining the highest possible security standards.

Another important aspect of my future research is the development of quantum-safe communication protocols for VPNs and other secure communication systems. As part of this effort, I plan to evaluate the performance of PQC algorithms in different real-world scenarios, ensuring that these protocols can be seamlessly integrated into existing network infrastructures without compromising performance or security. This research will involve close collaboration with industry partners and government agencies to ensure that the proposed solutions meet the needs of critical sectors, such as defence and finance, where secure communication is essential.

Conclusion

My research is at the intersection of cybersecurity, AI, and quantum technology. With the rapid evolution of cyber threats and the impending rise of quantum computing, I am committed to developing innovative solutions that can safeguard our digital infrastructure for years to come. Through my work University and ongoing collaborations with academic and industry partners, I aim to contribute to the global effort to secure networks against both current and future threats.