Strategy and Synergy for Security

SOCIETY FOR ELECTRONIC TRANSACTIONS AND SECURITY (SETS)

MGR Knowledge City, CIT Campus, Taramani, Chennai - 600113

17th November 2023 10.30 AM to 5.00 PM

WORTICS 2023

Workshop on Technology Trends in Cyber Security 2023

Summary of the Proceedings of the Fourth Workshop on Technology Trends in Cyber Security - WORTICS 2023 held on

November 17, 2023

at

SETS, Chennai

I. Inaugural Session

Welcome Address

Dr. N. Subramanian, ED, SETS

In the welcome address, Dr. N. Subramanian, the Executive Director, welcomed distinguished guests, including Prof R.K. Shayamasundar, Smt. Sunita Verma, Dr. Soundarapandian, Dr. Prem Laxman Das, invited speakers and participants. Dr. N. Subramanian provided a glimpse into SETS' 22-year journey, primarily focused on Cryptology and Computing, emphasizing SETS' leading role in National Blockchain Framework and implementing Postquantum Crypto algorithms for Digital signature schemes, aligning with evolving standards. He shed light on SETS' commitment to two critical aspects of hardware security: side channel analysis and implementation security. He detailed the established hardware labs, equipped for various analyses such as power play analysis, timing, and EM analysis. Moving forward, he delved into Quantum Random Number Generators and collaborative initiatives like Metro Quantum Area Access Network, contributing significantly to the National Quantum Mission. Highlighted the significance of this initiative amid the national Quantum Mission, emphasizing SETS' role in contributing to and partnering in this transformative journey. The Executive Director concluded by expressing excitement about the convergence of the Telecom Revolution and 6G, foreseeing excellent opportunities in the cybersecurity space. Dr. N. Subramanian emphasized SETS' eagerness to engage in academic and industry partnerships, collaborate with the government, and meet the evolving expectations in the realm of cybersecurity.

Evolving Scenario in PKI Infrastructure

Dr. Soundrapandian, Scientist, CCA

Dr. Soundrapandian from the Controller of Certifying Authorities (CCA) provided a comprehensive overview of the crucial role of Public Key Infrastructure (PKI) in ensuring trust and security in online transactions. Highlighting CCA's mission to foster trust in electronic transactions, he explained how the enhancement of the Ecosystem played a pivotal role in achieving this objective. Under the Central government, the CCA worked to promote digital transactions and ensured that interoperability standards were adopted globally to advance e-commerce and e-governance through the widespread use of digital technology. Dr. Soundrapandian also discussed the complexities of e-signatures, explaining how they worked with hardware tokens and how important it was for Certification Authorities to have control over the ecosystem. He also delved into the CCA's initiatives in Quantum computing, the adoption of new technologies, and the development of platforms for PKI certificates and IoT device certificates. Moreover, he outlined the CCA's roadmap for postquantum cryptography, covering areas like zero architecture, IoT, Blockchain, PKI, and HSM. Dr. Soundrapandian concluded by expressing gratitude for the opportunity to elucidate how the PKI system worked to establish trust in the Indian ecosystem.

Security in the perspective of Indigenous Hardware

Smt Sunita Verma, Group Coordinator, R&D in E & IT, MeitY, Govt. of India

Smt. Sunita Verma from the Ministry of Electronics and Information Technology (MeitY) expressed the significance of the workshop on Technology Trends and Cyber Security, considering it as a crucial roadmap for future initiatives. She emphasized the transformative shift from traditional cash transactions to digital wallets and mobile phones in the current generation, with India leading the technological evolution.

Highlighting the increasing technology adoption, Smt. Sunita Verma stressed the crucial need for robust cybersecurity and system security. She commended the government's various initiatives, especially in sectors like E-Governance, Finance, and Health, focusing on user-friendly and trustworthy experiences.

Smt. Sunita Verma also highlighted India's endeavours in developing indigenous hardware technology, emphasizing the government's focus on digitization across sectors such as Automotive, Transportation, and Smart Power. The comprehensive program for semiconductor and display manufacturing ecosystem development, along with the Independent India Semiconductor Mission (Semicon), was emphasized as a critical step to establish a trusted supply chain and create microprocessors for the country's future. She also stressed the importance of security integration in every aspect of the system, including hardware, through cryptographic primitives and quantum-resistant methods. Initiatives for web browser development by MeitY and a focus on self-sufficiency in the face of geopolitical challenges were also discussed. Overall, she expressed optimism about the workshop fostering a forward-looking roadmap based on emerging trends in technology.

Keynote Address: Trust Model - > Secure-by-Design

Prof. R. K. Shyamasundar, Dept. of CSE, IIT Bombay

Keynote address by Prof. R. K. Shyamasundar from the Department of Computer Science and Engineering at IIT Bombay provided a comprehensive exploration of the zero-trust strategy. He introduced the fundamental concept that underlies this approach: the idea that no user or asset is implicitly trusted. This strategic paradigm assumes that a security breach has either already occurred or is imminent, challenging the traditional notion of granting access based on a single verification at the enterprise perimeter. Prof. Shyamasundar highlighted the crucial shift from the conventional location-centric security model, emphasizing that the adoption of the zero-trust strategy provides enhanced visibility. This visibility, in turn, supports the development and evaluation of security policies, enabling a more proactive and adaptive approach to cybersecurity. The speaker delved into the core tenets of the zero-trust strategy, emphasizing its departure from the location-centric model. All data sources and computing services are considered as resources, and communication is secured irrespective of the network location. Access to resources is determined dynamically by policies, reflecting a departure from the static access controls of traditional security models. Additionally, Prof. Shyamasundar introduced the audience to the zero-trust maturity journey, outlining various implementations such as traditional, initial, advanced, and optimal stages. This nuanced exploration provided attendees with a holistic understanding of the evolution and implementation of the zero-trust framework.

Moving forward, Prof. Shyamasundar addressed the significant threat of phishing in the cybersecurity landscape. Phishing, a cybercrime tactic, involves the targeted deception of individuals through emails, telephone calls, or text messages, with the aim of extracting sensitive data like banking and credit card details. He introduced the concept of a phishing kit, describing it as a web component designed to mimic the appearance of legitimate websites. The anatomy of a phishing kit was briefly explained, shedding light on the deceptive techniques employed in these cyber-attacks.

In the latter part of his address, Prof. Shyamasundar delved into the complexities of mutual authentication, shedding light on the challenges posed by the disparity between human perception (look and feel) and browser authentication (SSL certificate). He concluded with a discussion on the secure-by-design principles, advocating for a flexible architectural approach, the implementation of layered controls for defense in depth, continuous assurance integration, and the importance of secure change management. This multifaceted exploration provided workshop participants with valuable insights into the intricacies of zero trust, phishing threats, and foundational principles of secure design in the dynamic field of cybersecurity.

II. Panel Discussion: Post Quantum Cryptography and Usecases

The panel discussion on Post-Quantum Cryptography (PQC) and its use cases was hosted as a highly engaging and insightful event. The event organized by SETS Chennai, which brought together a diverse group of participants, including experts from Controller of Certifying Authority (CCA) MeitY, C-DOT, UTIMACO, Odyssey Tech, and SETS India. The primary focus of the discussion was to explore the implications and applications of PQC while emphasizing collaboration between the Government, Industry, and academia.

Context Setting

Dr. Prem Laxman Das, Sr. Scientist, SETS

The speaker Dr M. Prem Laxman Das skillfully set the context for the panel discussion on Post-Quantum Cryptography and its use cases, addressing several key points. He began by acknowledging the widespread awareness of the NIST competition, highlighting its significance in the realm of cryptographic advancements, particularly in the domains of digital signatures and Key Encapsulation Mechanisms (KEMs). Emphasizing the critical role of digital signatures in ensuring authentication, the speaker posed a crucial question about the transition strategy to Post-Quantum Cryptography. Furthermore, he underscored the diversity of use cases and applications in this evolving cryptographic landscape. As the audience anticipated a rich and insightful panel discussion, the stage was set for an exploration of the challenges and opportunities presented by Post-Quantum Cryptography in various contexts.

Summary of Panel Discussion

Mr. Asad Ansari, HARMAN , Mr. Manish, UTIMACO, Dr. Soundrapandian, CCA, MeitY,Mr. Robert Raja, Odyssey Technologies Ltd.,, Mr. Prashant Chugh, C-DoT, Dr. Natarajan, Scientist, SETS and Dr. Reshmi, Scientist, SETS

The discussion commenced with the moderator Dr Reshmi T. R. (Scientist, SETS) setting the tone for an engaging and insightful conversation with the participants. Panelist Dr. Robert Raja shared insights into his experience with customer-facing applications during the discussion. Meanwhile, Mr. Prashant Chugh advocated for a hybrid approach, emphasizing the need to combine Post-Quantum Cryptography with classical systems. He mentioned the importance of crypto agility, emphasizing the necessity to swiftly transition to new products incorporating updated algorithms if the security of existing ones is compromised. During the panel discussion, Mr. Asad Ansari emphasized the importance of collaboration with other organizations, expressing a keen interest in partnering with both academia and industries. In response, Dr K.K. Soundra Pandian delved into the critical aspects of system performance, addressing concerns about the weight of classical algorithms and the need for improvement in IoT device performance. Moreover, he stressed the significance of enhancing the security of the Indian trust system and commended CCA's initiative to reduce complexity while increasing efficiency. The potential compromise of RSA encryption prompted discussions on the need for heightened security measures and the adoption of quantum-safe browsers. Mr. Manish contributed to the conversation by expressing optimism about the realization of a digital society and emphasized the value of close collaboration with academic institutions. Dr. Natarajan brought insightful perspectives to the discussion by addressing the integration of Post-Quantum Cryptography (PQC) with Quantum Key Distribution (QKD) systems. He emphasized the importance of both, acknowledging that QKD has faced criticisms related to its perceived incompleteness and hardware dependencies and proposed a forward-looking approach by suggesting the development of a hybrid solution that combines QKD and PQC, ensuring end-to-end security in the era of quantum computing. The discussion extended to the security challenges associated with cloud-based quantum computing, including a noteworthy mention of Amazon's initiatives in quantum computing. Furthermore, Dr. Natarajan delved into the complexities of securing remote quantum computing, offering valuable insights into the evolving landscape of quantum-safe solutions and the need for comprehensive strategies.

As the first round concluded, the moderator steered the discussion towards the intricacies of Public Key Infrastructure (PKI), embedded systems, and Hardware Security Modules (HSM). Highlighting the existence of multiple levels of cryptosystems within these domains, the moderator posed a thought-provoking question to the panelists. Dr Reshmi inquired about the strategies employed to nurture Post-Quantum Cryptography (PQC) within specific domains in the current era and prompted insights into how standardization efforts could progress to achieve broader acceptance. The panel discussion unfolded with diverse perspectives on the standardization and adoption of Post-Quantum Cryptography. Panelist Mr. Robert Raja emphasized a sequential approach of first standardizing and then regulating, acknowledging the potential constraints posed by regulations and standards on technology. In contrast, Mr. Prashant Chugh advocated for proactive measures, suggesting the monitoring of NIST processes and immediate integration of emerging standards into products. He urged the initiation of product rollouts in critical sectors like banking, emphasizing the need to act swiftly. Panelist Mr. Asad Ansari shared insights on the challenges of key selection within a product lifecycle, particularly in automotive sectors where robust key choices are crucial. Another notable point from him highlighted the importance of research in quantum computing, emphasizing potential applications in healthcare, such as cancer research. Meanwhile, Mr. Manish offered a realistic perspective, acknowledging the evolving nature of the transition process and expressing concern about India lagging behind in PQC transition. He underscored the need for continuous efforts to navigate the complex landscape of PQC adoption and transition. In summary, the panelists collectively addressed the challenges and opportunities associated with PQC, covering topics such as standardization, regulation, proactive adaptation, key selection, and the significance of trust at every level of implementation. The insights provided a comprehensive view of the multifaceted considerations surrounding the transition to Post-Quantum Cryptography.

During the audience Q&A session, the moderator posed a question about potential domains in Post-Quantum Cryptography for researchers and students to explore. In response, Panelist Mr. Prashant Chugh offered valuable insights. He highlighted the role of mathematics students in contributing to the development of mathematical algorithms within the realm of PQC. Additionally, Mr. Manish raised awareness about India's relatively modest contribution to the NIST competition, sparking a critical discussion on how to address and enhance India's participation in the evolving landscape of PQC research and development. In response to an audience question comparing the key sizes of Post-Quantum Cryptography (PQC) algorithms to classical algorithms, Panelist Dr K.K Soundra Pandian provided insights into the Dilithium digital signature scheme. He explained that Dilithium operates with three security levels, and the key sizes are standardized based on the specific attack scenarios and desired security levels. Furthermore, Mr. Manish contributed by mentioning the significance of lightweight cryptography, addressing concerns related to the computational efficiency of cryptographic algorithms.

In the concluding remarks, the moderator encouraged a spirit of knowledge sharing among the participants, fostering a collaborative atmosphere for continued exploration and understanding in the dynamic field of Post-Quantum Cryptography.

III. Summary of Technical Talks

R&D at SETS and Opportunities for collaboration

Ms. Suganya, Sr. Scientist, SETS

Ms. Suganya, a Senior Scientist at the Society for Electronic Transactions and Security (SETS), eloquently introduced SETS as a trailblazing organization in information security R&D. With a rich history of 22-23 years, SETS was committed to directed basic research, prototype translation, and collaborative consultancy and training within the cyber community, aspiring to lead in the field. Her talk navigated through SETS' diverse ongoing projects and innovative pursuits, unveiling the organization's research groups: cryptology and computing, quantum security, network security, hardware security, and services and training. The cryptology research group, a bastion of innovation, concentrated on post-quantum cryptography, ransomware analysis, blockchain networks, and cutting-edge AI-based cybersecurity. The hardware security team, with its pivotal role, operated a Side Channel evaluation lab, rigorously testing crypto modules against sectional attacks and contributing significantly to security analysis and implementation. Expanding its reach, the network security group was actively engaged in developing an Integrated Threat Management System (ITMA), a viral private network, and a robust network security solution tailored for the protection of smart cities and IoT systems. Their forward-looking approach included a strategic focus on AI-driven decision-making upon the release of the next generation of ITMA. Delving into quantum security, SETS explored quantum-safe cryptography, key distillation engines, quantum key distillation, and the innovative Metro Area Quantum Access Network (MAQAN). Ms. Suganya's presentation masterfully encapsulated SETS' multifaceted endeavors, positioning it as a pioneering force in the ever-evolving landscape of information security research and development.

Embracing Privacy Engineering

Dr. Sachin Lodha, Chief Scientist, TCS

Dr. Sachin Lodha, a principal scientist at CCS Research and the principal investigator for TCS Stanford University Research Collaboration on Data Privacy, shared insights on the intersection of security and privacy, focusing on their collaborative work. The session delved into the balance between technology and privacy, the challenges of privacy policies in India, and the impact of government regulations. Addressing the challenges of privacy implementation in India, he emphasized the delicate balance between user privacy and data utility. He addressed the complex challenge of balancing technology and privacy, proposing methods like query restriction and data modification. The discussion delved into methods like query restriction, answer dishonestly, and answer range to address privacy concerns, with a spotlight on the complexities introduced by user behavior as potential threats. The speaker discussed the importance of data privacy and confidentiality in different countries, such as Australia, India, China, and Russia. The speaker also mentioned the General Data Protection Regulation (GDPR) framework, which can be used to comply with data privacy regulations. He discussed the guidelines for organizations and companies to properly implement the Data Protection Directive and Privacy in Processing Act (DPDP and PIPA) in South Africa.

The presentation underscored the importance of Privacy Engineering as a discipline, with a focus on building systems that meet privacy expectations. Dr. Lodha discussed approaches like privacy by policy and privacy by architecture, emphasizing the need for organizations to limit data collection and ensure processing aligns with the intended purpose. The speaker encouraged privacy by architecture, stating that it is necessary and sufficient for ensuring a properly engineered privacy system, which includes limiting data collection and use for specific purposes, and only processing the data necessary for the intended use. Differential privacy, data masking, and consent management were explored as tools in privacy engineering, along with the introduction of India's unique concept of data empowerment and protection architecture (DEA), which focused on community-based consent and protected users by having others take responsibility for their consent. Dr. Lodha discussed privacy in the context of cloud computing and artificial intelligence. The talk also included the significance of incorporating privacy considerations early in the development process, leveraging technologies such as encryption and federated learning. Dr. Lodha highlighted encryption in cloud computing, federated learning, and the ongoing struggle to find a balance between utility and privacy.

Dr. Lodha discussed post-quantum cryptography, secure blockchain networks, and AI-based cybersecurity solutions. In a detailed exploration, he discussed smart contract security on blockchain networks, emphasizing the need for resilience against attacks and the role of tools considering user experience. Lastly, the final section discussed the intricacies of privacy consent, tracking data sources, and differential privacy implementations by major technology companies. In addition, he pointed out disparities between legal frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and technology understandings. Dr. Lodha concluded by emphasizing the multidisciplinary approach needed for effective security solutions, as discussed by SETS at WORTICS 2023.

Trusted Computing Environments with RISC-V Microprocessors

Prof. Chester Reberio, IIT Madras

In a captivating technical talk at the workshop on technology trends in cybersecurity, Dr. Chester Reberio, an esteemed associate professor at IIT Madras, delivered a technical talk on the intricacies of Trusted Computing Environments with RISC-V microprocessors. Dr. Reberio initiated the discussion by underscoring the critical imperative of protecting sensitive data, acknowledging its diverse storage locations within computers. The introduction of the compute stack, accompanied by a detailed diagram and summary, laid the foundation for understanding the comprehensive architecture that contributes to data security. Central to the discourse was the overarching principle that unauthorized users should be barred from accessing sensitive data, particularly as vulnerabilities, often rooted in memory-related issues, pose a constant threat.

Dr. Reberio meticulously dissected the various threats to data security, categorizing them into applications, monolithic software, system software, and hardware vulnerabilities. Noteworthy were the insights into side-channel leakage, exemplified by SCA attacks on RSA through the analysis of power consumption during decryption, and the nuanced exploration of bus probing vulnerabilities, particularly in embedded devices. Transitioning to the engineering of secure systems, Dr. Reberio extolled the virtues of RISC-V processors, emphasizing their open standard industry set architecture, transparency, customizability, and status as an open platform for research. This included an overview of notable RISC-V processors like VEGA by CDAC and SHAKTI by IIT Madras, showcasing the advancements in microprocessor design.

The latter part of the talk delved into pragmatic strategies for addressing vulnerabilities in applications, particularly through the innovative concept of compartments. Dr. Reberio proposed the use of unikernels instead of large legacy operating systems, reducing code size and potential vulnerabilities. Acknowledging the complexity of transitioning from established programming languages like C or C++, he emphasized the need to protect legacy code while adopting new methodologies. Furthermore, the talk explored measures for mitigating bus probing vulnerabilities, specifically through the implementation of memory encryption in operating systems.

Dr. Reberio concluded with an insightful discussion on the challenges inherent in this paradigm shift, including considerations of performance overhead and cost implications. His comprehensive address provided a profound understanding of the evolving landscape of Trusted Computing Environments with RISC-V microprocessors and the strategic measures required to safeguard sensitive data in the realm of cybersecurity.

Emerging Trends and Challenges in Cybersecurity

Mr. Manish Kaushal Kushwaha, McAfee

In a thought-provoking technical talk on "Emerging Trends and Challenges in Cybersecurity: Navigating the Evolving Landscape," Mr. Manish Kaushal Kushwaha from McAfee delivered a comprehensive overview of the dynamic field of cybersecurity. Beginning with a fundamental introduction, he elucidated the essence of cybersecurity, emphasizing its role in defending computer systems, networks, and data from unauthorized access and digital threats. Mr. Kushwaha highlighted the escalating global cybersecurity threats, touching upon the current landscape characterized by attacks against cloud services, the proliferation of IoT devices, a surge in insider threats, and the emergence of high-level threats such as deep fakes, crypto mining, AI-powered spyware, and password cracking. A key focal point of the talk was the discussion on quantum computing's impact on encryption, shedding light on the potential paradigm shift in cryptographic methods. The speaker then delved into the realm of generative AI and its implications, particularly in the context of identity theft. Illustrating the use of fake voices generated by generative AI as a widespread threat, Mr. Kushwaha provided examples of banking frauds and synthetic identity fraud. Addressing the impact of remote work on cybersecurity, he explored the challenges arising from the greater use of public cloud services, the scarcity of security talent, reduced oversight by security staff, and increased susceptibility to phishing attacks. In conclusion, Mr. Kushwaha underscored the evolving threat landscape, attributing it to the influence of generative AI, the rise in work-from-home trends, increased IoT and mobile usage, and the emergence of quantum computers. He advocated for a multifaceted approach to securing the environment, encompassing self-ethics, government regulations, and the paramount importance of digital hygiene and ethics for ensuring safety in an increasingly complex cybersecurity landscape. The talk provided valuable insights into the multifaceted challenges and strategies required to navigate the evolving landscape of cybersecurity effectively.

Strategy and Synergy for Security

SOCIETY FOR ELECTRONIC TRANSACTIONS AND SECURITY (SETS)

MGR Knowledge City, CIT Campus, Taramani, Chennai - 600113

17th November 2023 10.30 AM to 5.00 PM

WORTICS 2023

Workshop on Technology Trends in Cyber Security 2023

Inauguration and Keynotes (10.30 AM to 11.30 AM)

Dr. N Subramanian
Executive Director, SETS
"Welcome Address"

Shri. Aashish Banati
Deputy Controller(Technology), CCA MeitY
"Talk on Evolving Scenario in PKI Infrastructure"

Smt. Sunita Verma
Scientist G and Group Coordinator, MeitY
"Talk on Security in the perspective of Indigenous Hardware"

Prof. R. K. Shyamasundar
JC Bose National Fellow & Distinguished V. Professor, IITB
"Keynote Address"

Dr. Prem Laxman Das
Senior Scientist, SETS
"Vote of Thanks"

Strategy and Synergy for Security

WORTICS 2023

17th November 2023 10.30 AM to 5.00 PM

Panel Discussion
(11:45 AM to 1:00 PM)

Theme: Post Quantum Cryptography and Usecases

Context Setting Talk - Dr. Prem Laxman Das
(Senior Scientist, SETS)

IoT/Embedded Devices - Mr. Asad Ansari (HARMAN)

Hardware Security Module (HSM) - Mr. Manish (UTIMACO)

PKI - Dr. K K Soundra Pandian (CCA, MeitY)

Blockchain - Mr. Prasanna Lohar (Blockchain Forum)

Digital Signature - Mr. B. Robert Raja (Odyssey Technologies Limited)

Usecases/Applications - Mr. Prashant Chugh (C-DOT)

Quantum Computing - Dr. Natarajan (SETS)

Lunch Break

Technical Talks - Theme: Emerging Trends & Challenges in Cybersecurity
(2.30 PM to 5.00 PM)

Introduction: Smt. A. Suganya (Senior Scientist, SETS)

Keynote: Shri. Manoj Jain
(Director (R&D), BEL)

Technical Talk 1- Dr. Sachin Lodha
(Chief Scientist, TCS Research)

Technical Talk 2 - Shri. R S Mani
(Deputy Director General, NIC) Technical

Technical Talk 3 - Dr. Chester Reberio
(Associate Professor, IIT-M)

Technical Talk 4 - Shri. Manish Kushwaha
(Director of Data Engineering, McAfee)

Vote of Thanks - Dr. Reshmi TR (Scientist, SETS)

WORTICS 2023

17th November 2023 10.30 AM to 5.00 PM

10.30 Hrs.	Invocation & Lighting of Lamp	
10.35 Hrs.	Welcome Address	Dr. N Subramanian
10.45 Hrs.	Talk on Evolving Scenario in PKI Infrastructure	Shri. Aashish Banati
11.00 Hrs.	Talk on Security in the perspective of Indigenous Hardware	Smt. Sunita Verma
11.15 Hrs.	Keynote Address	Prof. R. K. Shyamasundar
11.30 Hrs.	Vote of Thanks	Dr. Prem Laxman Das
11.35 Hrs.	High Tea	

Panel Discussion (11:45 AM to 1:00 PM)
Theme: Post Quantum Cryptography and Usecases

Lunch Break

14.30 Hrs.	Introduction	Smt. A Suganya
14.35 Hrs.	Keynote Address	Shri. Manoj Jain
15.05 Hrs.	Technical Talk 1	Dr. Sachin Lodha
15.30 Hrs.	Technical Talk 2	Shri. R S Mani
15.55 Hrs.	Technical Talk 3	Dr. Chester Reberio
16.20 Hrs.	Techical Talk 4	Shri. Manish Kushwaha
16.45 Hrs.	Vote of Thanks	Dr. Reshmi TR
16.50 Hrs.	High Tea	