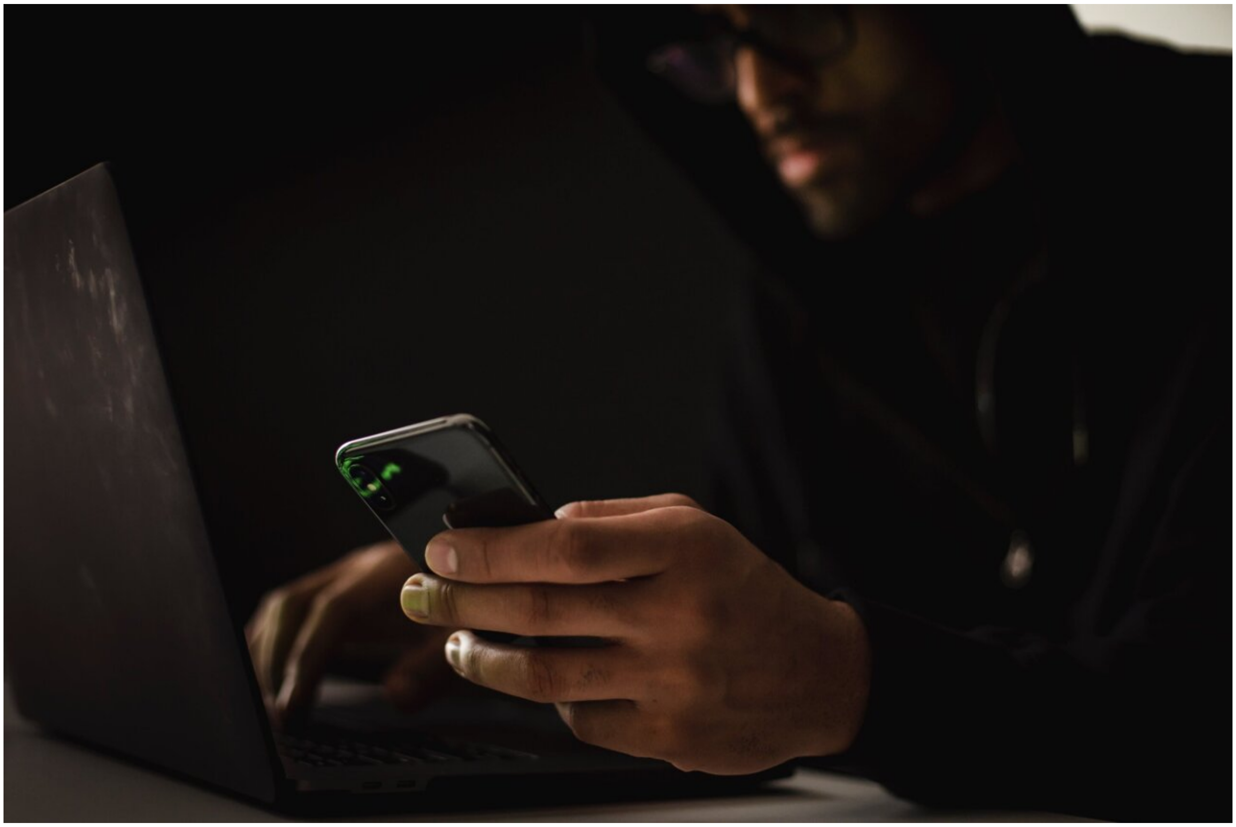
'Ineffable cryptography' to protect critical infrastructure from cyber attacks

November 21 2023, by Michael Quin



Credit: Sora Shimazaki from Pexels

Australia's critical infrastructure—including ports, energy grids and water supplies—reported 143 cyber attacks over the past year, up from 95 incidents the year before.

In response to this growing threat, Federal Minister for Cyber Security Clare O'Neil recently announced 168 of the country's critical infrastructure assets would require enhanced cyber security, almost double the 87 assets previously deemed "systems of national significance."

Now a mathematical breakthrough allows system access authority to be spread invisibly and securely across a network, so there's no weak link.

This enables a fundamentally new approach to cybersecurity for critical infrastructure, which can be especially vulnerable to hacking thanks to legacy systems and their interconnected nature.

The new technology, dubbed "ineffable cryptography," is explained in a new joint study by Tide and RMIT mathematicians, published online on the *arXiv* preprint server.

Study lead author from RMIT's School of Science, Dr. Joanne Hall, said the advance was built on multi-disciplinary collaboration, bringing her team's expertise on mathematics and cryptography together with computing, technology and business insights to produce a thorough, cutting-edge solution.

"With this collaboration, we're really looking ahead at what the next standard will be," Hall said.

The technology has now been incorporated into a prototype access control system specifically for critical infrastructure management, known as KeyleSSH, and successfully tested with multiple companies.

Decentralized authority means no one holds the key

Tide Foundation Co-Founder, Michael Loewy, said traditional passwordprotected approaches to infrastructure access control had proven insecure.

Alternatives such as multifactor authentication and key-based access are expensive, carry their own vulnerabilities and can be overly complicated for users.

"Ultimately, these approaches blindly trust the secrets that protect a system to individuals that hold the keys to the kingdom, an Achilles' heel that today's state of the art doesn't address," he said.

Tide's ineffable cryptography, on the other hand, allows data and devices to be locked with keys that no one will ever hold.

It works by generating and operating keys, in secrecy, across a decentralized network of servers, each operated by independent organizations.

Each server in the network can only hold part of a key: no one can see the full keys, nor the entirety of the processes they are partially actioning, nor the assets they are unlocking.

By spreading the process invisibly across the network, the keys that would-be hackers are seeking are never exposed.

"It means no single point of failure or compromise and ultimately, keys that you can't steal, lose or misuse," Loewy said.

"The applications enabled by this technology go well beyond cybersecurity for critical infrastructure to include securing identities, health information, financial systems, and privacy in AI applications."

Industry collaboration to build a cutting-edge solution

RMIT has been collaborating for three years with Tide—which among other accolades won Australian Information Security Association's Cyber Startup of the Year in 2021.

The technology's bold claims have been scientifically validated during this collaboration, which has involved RMIT's own Chief Information Security Officer, top mathematicians and cybersecurity experts in the School of Science and Centre for Cyber Security Research and Innovation.

Most recently, a select group of cybersecurity students, supported by the RMIT Cloud Innovation Centre and RMIT's AWS Cloud Supercomputing Hub (RACE), worked with industry partners to help them test the technology and prove its ability to solve critical infrastructure security challenges in ways that weren't previously possible.

RACE is Australia's first university cloud supercomputing facility, allowing researchers, students and industry partners to test ideas and solutions together more than 100 times faster than existing on-site servers.

RACE Director Dr. Robert Shen said the student project, "KeyleSSH," focused on integrating the Tide technology with SSH—a method for remote infrastructure management—then testing it with multiple industry partners.

"The resulting project moves from the theoretical to the commercial and elevates the security benefits beyond key-base access control, without the complexity and cost," Shen said.

"This project showcases a key element of what RACE brings to RMIT: empowering our researchers and industry partners with the tools and infrastructure necessary to enhance operational efficiency and accelerate innovation."

The solution has been met with enthusiasm by managed service providers involved in the trial, including Australian company Smart Building Services (SBS) Digital, which offers smart metering systems to industrial complexes.

The company's Chief Technology Officer, Jonathan Spinks, said that in the face of growing geopolitical complexities, it was imperative that entities responsible for servicing vital infrastructure such as airports and utilities could demonstrate they are beyond reproach.

"Integrating Tide's decentralized solution would ensure that access controls in SBS Digital's Netstream utility platform are virtually immune to tampering," Spinks said.

More information: J. L. Hall et al, Manifesting Unobtainable Secrets: Threshold Elliptic Curve Key Generation using Nested Shamir Secret Sharing, *arXiv* (2023). DOI: 10.48550/arxiv.2309.00915

Provided by RMIT University

Citation: 'Ineffable cryptography' to protect critical infrastructure from cyber attacks (2023, November 21) retrieved 12 May 2024 from https://techxplore.com/news/2023-11-ineffable-cryptography-critical-infrastructure-cyber.html