Solana Networks

Looking to the horizon of network security

As a Canadian SME, Solana Networks is currently working to deliver encrypted traffic analysis solutions for cyber security and serves as a technology vendor providing intelligent software products and solutions for internet protocol (IP) networks, focusing on the area of network and security monitoring. Solana has its roots in two high-tech companies in Ottawa: Nortel Networks, a telecommunications equipment vendor and JDS Uniphase, a vendor for optical communication products. Biswajit Nandy, Chief Technology Officer at Solana Networks, gives us an insightful glimpse into the story of Solana Networks.

Organically grown

"In the early 2000s, the available solutions for network monitoring and management for data communication were in its infancy, and sophisticated tools were missing. Monitoring and measuring took a long time and vendors provided proprietary solutions. So, my current business partners and I saw an opportunity that we could leverage by developing advanced network monitoring solutions that are generic and easy to use. What's unique about Solana Networks is that we don't have external funding. When we started, maybe we were a little bit naïve." Biswajit smiles. "We put some of our own money down but that ran out in no time once we hired a few employees. Then we started bidding for federal government IT projects and won. If we hadn't, perhaps Solana wouldn't exist. 20 years later, we are still an organically grown company and are self-sustaining."

Constant evolution

Solana's flagship product is SmartHawk, a network mapping and topology discovery tool for routed and switched IT networks that has been deployed in enterprise and service providers networks. "Over time, we saw SmartHawk being used more and more in the security domain to observe changes in inventory and connectivity in near real time," explains Biswajit. "Network security is a fast-moving area. Solana has been developing various security analytics solutions for government departments and private sector vendors. In recent years, different AI-based software analytics have changed the paradigm. A lot of analytics are currently being developed that were not possible 20 years ago."

Today, up to 90% of traffic is encrypted, presenting obstacles to ensure IT security and law enforcement. "How will you enforce your policy if you don't know what's going on in your network?" asks Biswajit. Currently, this is managed by a form of data processing called deep packet inspection (DPI), but encryption is drastically reducing its efficiency and accuracy. Within a few years, a complete alternative will be required. This is where the ITEA project ENTA steps in.

Preserving privacy

ENTA stands for Encrypted Network Traffic Analysis for Cyber Security and a key component of this involves the use of artificial intelligence. The temporal and spatial characteristics of traffic are analysed using machine learning and/or deep learning to obtain visibility into encrypted traffic. This enables predictions, such as whether certain encrypted traffic is YouTube, Netflix or Skype. Biswajit: “The interesting part is that you don’t need to look inside the payload data, so you’re not violating any privacy. We’re addressing two use cases in the ENTA project. One is about the detection of encrypted application types. Also, by looking at the traffic characteristics, you should be able to tell what kind of IoT devices you have in your network and whether it’s rogue or not. This is the second use case.”

This kind of publicly funded project is extremely helpful for addressing problems with a longer horizon.

The ability to obtain visibility into encrypted traffic data for network and security monitoring already makes ENTA unique, but the consortium also expects its approach to be applied to many other use cases following the project’s completion. Now at the halfway mark, the final outcome will include a platform to enable researchers to easily do their own encrypted network traffic analysis using AI, presenting the opportunity for this innovation to spread to a huge variety of domains while preserving privacy.

Longer horizons

This achievement is all the more impressive considering that this is Solana Networks’ first ever experience in a RD&I project with European partners. Biswajit contrasts the ITEA experience with privately funded consortia. “You know, when a project is privately funded, your objective is shorter. You want some outcome in one or two years and then you want to productise and leverage that. But this kind of publicly funded project is extremely helpful for addressing problems with a longer time horizon. The problem we are addressing, encrypted traffic analysis, is one such problem.”

Positive differences

As for the difference between Canadian projects and ENTA – which also brings in partners from Austria, Spain, Switzerland, Türkiye and the United Kingdom – Biswajit thinks for a second. “I mean, it’s a little bit different in a sense. People are from different backgrounds, different languages and different cultures; so, maybe it involves a little bit more coordination for project management. Collaboration is the main thing: we have many use cases, so working with various partners essentially means that different requirements come out, which improves the quality of what we’re doing. Everybody has different ideas and we pull it all together.”

“Honestly, Europe has excellent programmes, particularly ITEA and Eureka. It’s well-structured and has been operating for a long time. As I said earlier, these publicly funded projects can nurture long-term innovation. Canada has a good set of innovation programmes but I wish they were as broad and well-funded as in Europe. The last thing I can say is that I appreciate programs such as ITEA and IRAP in Canada and I really see the value.”

More information

https://www.solananetworks.com/