A single cybersecurity breach might be enough to put a startup out of business, says Dr Somitra Kumar SanadhyaVoice&Data

Thursday 05 October 2017

By Anusha Ashwin

India needs a strong cybersecurity law! In an interaction with *Voice&Data*, Dr Somitra Kumar Sanadhya, who is an Associate Professor at the Department of Computer Science and Engineering at IIT Ropar, shares his insights – on right from the definition of cryptography and the much talked about bitcoins, to cyber security laws and policies in India, and its impact on startups.

Dr Sanadhya is an expert on Cryptology and has worked closely with many government agencies and defense forces for development and analysis of cryptographic primitives. His research is supported by grants from DRDO, Ministry of Defense and Indian Navy. He has published many papers in reputed peer reviewed journals and conferences in the area of Cryptology and has organized many workshops, events and international conferences on Cryptology in the last decade. Excerpts from the interaction:

Voice&Data: What is Cryptology and how far has the knowledge about this spread to the budding startup entrepreneur eco-system in India?

Dr Sanadhya: Cryptology is the science and art of secret computations. Initially, it was concerned only with secure communications, traditionally needed by diplomatic missions and armed forces, but is now also required when one attempts to log-in to a bank account online. However, in the past 30 years, it has also expanded to performing secure computations on shared data while not revealing our own data, convincing someone of having some information, without giving away that information etc. Today, we have cryptocurrencies, like bitcoin and ethereum, which are based on the theory of Cryptology. On the negative side, ransomwares also use cryptographic tools to extract ransom from people by encrypting their data.

Many startups focused on ransomware detection/prevention and cryptocurrencies are coming up in India. However, in my opinion, there is a lot of work yet to be done by Indian companies in this field.

Voice&Data: Post demonetization, there has been a marked increase in online shopping and digital transactions and the launch of many startup companies in this space. What is your advice to such startups on having a strong security system?

Dr Sanadhya: Security is of paramount importance in today's digital world. Not only do companies need to secure their transactional data, even individual customers need to be careful to prevent unauthorized use of their credentials or online wallets. Start-ups usually find it hard to run

even their basic business and hence focus less on security. However, they need to realize that a single crucial security breach might be enough to put them out of business.

My advice to such companies is to have a strong internal team focusing on security, which is tasked with security auditing of not only the product but also the processes of the organization. They should not go with the pressure of a 'new release' without a security audit of the code. They must invest in preventive technologies, educate their workforce on security best practices, and have a process in place to contain, and learn from any security breach if it takes place.

Voice&Data: What is your opinion about cybersecurity in telecom networks?

Dr Sanadhya: Cybersecurity in telecom networks has many attack vectors, which need to be guarded for long term security of the infrastructure as well as service.

With the merging of voice and IP networks, many attack vectors which were not of significance for telecom networks earlier have now started becoming crucial. Network protocols and DNS servers can be attacked for denial-of-service attacks, impacting one of the most important "always on" functionalities of telecom operators. Telecom equipment could be packaged and sold with a pre-installed malware by state level actors. IoT devices are expected to dominate the market in future and will lead to the demand of 5G services and cloud infrastructure opening further areas of potential security breaches.

I believe that telecom providers are already aware of the risk landscape to their business and are actively monitoring their networks. However, I am not sure if they are having comprehensive and actionable cybersecurity policies.

Voice&Data: What is blockchain and how do you perceive this technology's growth in India?

Dr Sanadhya: Blockchain is a "chain" of "blocks" connected together by using some cryptographic primitives. The blocks may contain any kind of data, and once subsequent blocks are added to the chain, the previous blocks can't be modified. These security guarantees are achieved by a careful application of some Cryptographic primitives in the design of this system. This allows the blockchain to be used as a secure distributed ledger storing, for example, transaction history of a digital currency. The main advantage of this technology is that there is no central authority, which controls the growth of the chain. The chain is controlled by a peer-to-peer network, which follows a standard protocol for adding a new block. The state of the current chain i.e., the records which are universally accepted by all, can be seen by any peer in the system.

The potential for this technology is beyond just digital currencies. There are a few companies in India, which are working on adaption of this technology into various domains, primarily in finance. Some of these are Trestor, Auxesis, Coinsecure, Ezyremit etc. However, as of today, it hasn't caught on much in India. Further, there is not much happening in adapting this technology in non-financial domains. I believe one of the reasons for this is the absence of legal framework in the country.

Voice&Data: What are Bitcoins? Are they legal in India and are they secure? For a layman investor in Bitcoins, what is your word of caution?

Dr Sanadhya: Bitcoin is a digital currency based on blockchain technology. It was the first real application of blockchain technology and has been extraordinarily successful since its first implementation in 2008. They have enabled anonymous payments. On the flip side, this has also led to their use in illegal and unethical businesses such as selling of drugs, weapons and extracting ransom from ransomware victims.

RBI's press release in February 2017 mentioned that it has not given any license/authority to any entity/company to deal with bitcoins or any virtual currency. On the other hand, the same notification says that "anyone dealing with virtual currencies will be doing so at their own risk". Thus, it appears that RBI is not making it illegal to do business in virtual currencies

but is only taking a cautionary approach.

For a layman investor, the first thing to note is the absence of any legal support from RBI/our judicial system in case of any dispute. Secondly, the virtual currency is traded just like any other commodity on share market and hence the value of the currency is volatile. In Aug 2016, the value of 1 bitcoin was about US$ 600 whereas after a year today, it is valued at about US$4250.

From the technical point of view, a user must protect his private keys if he/she is dealing in this currency. There have been numerous incidents of people unable to use their bitcoin funds since they lost the private key to their bitcoin wallets.

Voice&Data: According to you, what should the Indian Government do to create cybersecurity awareness?

Dr Sanadhya: I believe that the government is already doing a lot to create cybersecurity awareness, especially via academic institutions. The multiple ways in which this is being done is by training manpower, supporting the development of course content for many areas of security training, organizing workshops, etc. However, it is not enough for an area like cybersecurity where new ways to defraud people with their data or finances keep on emerging.

I believe that there are not enough startups/industries working in various domains of security in the country. Probably, it has got something to do with the lack of government support. In my opinion, the government must come up with policies to encourage research and deployment of new security technologies and practices; and support incubation of start-ups at leading educational institutes like IITs and IISc. Secondly, a legal framework supporting research and adaption of security technologies is very much the need of the hour in the country.

Voice&Data: Are there any workshops for startup entrepreneurs on cryptography? Also, please name some institutes that conduct such

workshops?

Dr Sanadhya: The RC Bose Centre for Cryptography and Cybersecurity at ISI Kolkata organizes specialized workshops on Cryptography regularly. We are currently planning to organize such events at IIT Ropar in near future. The cybersecurity center at IIT Kanpur is very active on many areas of cybersecurity. Apart from these, IIT Kharagpur, IIT Bombay, IISc Bangalore, IIIT Bangalore and IIIT Hyderabad have many good faculty members working in various areas of Cryptology and/or Security. Among industry research labs, Microsoft Research Bangalore, IBM Research Bangalore, Infosys Innovation centers at Hyderabad and Kolkata are the prominent ones.

Voice&Data: There have been some very significant cyberattacks this year such as WannaCry etc. How is India preparing to face such attacks and what is the threat scenario for our country?

Dr Sanadhya: WannaCry is a ransomware, which uses vulnerabilities in the Windows operating system to take control of a victim's machine and encrypt the files on this machine. There are many other ransomwares most of which utilize some loophole in the operating system to gain access to the system. There have also been instances of attackers using weak login credentials used by real users to gain access to their systems.

The most important activity to reduce the chances of being hit by a ransomware like WannaCry is to ensure that the operating systems updates, specially the critical ones, are applied regularly. Secondly, strong login credentials should be chosen by users, especially if the machine contains important data. Finally, one should be careful not to fall for phishing emails and phone calls.

I believe that attacks like this are easy to launch against individuals but it is significantly harder to succeed against organizations which really care for their data security. For example, most security conscious organizations do not keep their crucial data in one location, apply crucial patches regularly and keep track of unusual activity on their network traffic. However, zero-

day attacks are not necessarily prevented by these precautions. In this regard, Indian infrastructure is as vulnerable as that of any developed country. The primary difference between the developed countries and India is not in the ability to completely prevent such attacks, but in the response after such an attack takes place. Their computer security response teams are likely to get to know of such attack as soon as it begins and will begin appropriate measures to contain the spread and prevent further loss of data. We are unfortunately not well prepared in this.

Voice&Data: On a comparative scale with other developed countries, how do you view India's position in uptake of cybersecurity technologies?

Dr Sanadhya: Two of the leading countries in the area of development of new cybersecurity technologies in the world are USA and Israel. India is nowhere close to them. The same holds for application of these technologies in Indian industry.

Voice&Data: How strong are India's laws in Cybersecurity?

Dr Sanadhya: I am not a legal expert but from what I understand, our laws are not ready for the modern cyberworld. To give an example, if an online seller commits a fraud then the current Information Technology Act does not provide the affected party with sufficient recourse. One has to approach cyber cell of police and register cases under standard clauses of the penal code. From what I gather from learned cyber-lawyers, our cyber laws are outdated and need an immediate upgrade.

Related Posts