THE TIMES OF INDIA

Date: 07-06-18

In the coming era of 'Internet of Things' (IoT), cryptography will be the key to ensuring security

Atanu Biswas and Bimal Roy, [The writers are Professors at the Indian Statistical Institute, Kolkata]

In the 2017 Hollywood movie 'The Fate of the Furious' Cipher, the cyberterrorist, and her henchman hacked more than a thousand cars. They sent some of the hacked cars careening through Manhattan streets and crashed others through the windows of a five-storey parking garage to land on a politician's motorcade. We infer that the security of connected 'things' in this era of 'Internet of Things' (IoT) is quite vulnerable.

Today, in the shadow of unfolding scandals let alone Hollywood movies, we need to protect the information the 'things' might know about us. We fail to understand how every bit of information related to our security and privacy are lying in the public domain, with the information being transmitted through devices of day-to-day usage. There are billions of such 'things', ranging from micro-sensor to car, and the ever-expanding global market of IoT is in trillions of dollars. A simple modus operandi of any 'smart city' is usage of cameras and sensors to detect irregularities. People's health status may be monitored by sensors on a 24×7 basis.

While convenient, by the same token it is easy to track almost every bit of lifestyle, health status or even when our house remains unoccupied by hacking the usage data of internet-connected appliances like the refrigerator, television, air conditioner, insecure routers, IP cameras, digital video recorders, or even the health sensors, causing serious threat to privacy and security. The infamous denial of service attack of October 2016, on both sides of the Atlantic, illustrated how cheap IoT devices without security could be hacked.

Consider a smart city where surveillance is conducted by sensors and cameras. Before any misconduct a hacker might try to corrupt the communication channel by introducing some noise, which would dominate the captured message. Thus, proper encryption is a must to safeguard the messages. Cryptography can be effectively used to ensure that encryption can resist any attack, information in transit remains confidential, and integrity and authenticity of information is guaranteed. For IoT devices, the sender needs to use a strong hashing algorithm and generate shared secret keys known as a message authentication code (MAC). The receiver will have to use the same hashing algorithm to decode the MAC. Take the example of Googlemail. Naturally Google encrypts the mails in such a way that only their trusted people get the key.

Double-checking through OTP (one time password) while making any online payment is a check and balance to avoid fraudulent use of credit or debit card. Patients' medical data are recorded in the computer server of the hospital. The attending doctors can login remotely to access them. Attribute-

based encryption is needed for such purposes, required number of keys would depend on the number of attributes. If only the doctors are the attributes, only they will have access to the data. If the insurance company is an attribute as well, the company also will have access to it. The memory and energy consumption level of most IoT devices are small, and security has to be ensured within these limitations. A relatively new technology called "lightweight cryptography" is believed to be particularly useful for IoT, due to its efficiency of end-to-end communication and possibilities of more network connections with lower resource devices.

Ensuring security in IoT is basically a mathematician's job. 'Breaking' the security means solving a very difficult mathematical problem. Encryption should be such that the mutual information between the actual message and the one being sent is almost zero, using Shannon's notion. Cryptography is certainly not free at the point of use, but security for IoT is as important as low power consumption, affordability, and wireless connectivity of the devices, if not more important. Also, cryptography is not a kind of magic security dust for IoT; designing and implementing of 'things' according to the state of the art is very crucial. Remember that it is a continual war, as the hackers will also become smarter. It is impossible to ensure that no car will be hacked in future. But our endeavour is to make that more and more difficult.

THE HINDU

Date: 06-06-18

Life in plastic

It's far from fantastic India's framework on discouraging its use is in disarray

EDITORIAL

As a major producer pof plastic waste that ends up in the oceans, India is arguably the best place to host World Environment Day. Union Environment Minister Harsh Vardhan has said the government means business, and the UN theme, "Beat Plastic Pollution", will not remain an empty slogan. His claim would have inspired greater confidence had India taken its own rules on waste management seriously. Both the Solid Waste Management Rules and the Plastic Waste Management Rules of 2016, which built on previous regulations, mostly remain on paper. State governments have simply not given them the necessary momentum, and the producers of plastic articles that are invariably used just for a few minutes have shown little concern about their negative environmental impact. The Centre's somewhat liberal estimate shows over 60% of about 25,000 tonnes of plastic waste generated daily is collected. That essentially means a staggering 10,000 tonnes of trash is being released into the environment, a lot of it going into the sea. Also, not every piece of plastic collected by the system is scientifically processed. It is no surprise, therefore, that the Ganga-Brahmaputra-Meghna river system is on the UN map of 10 rivers worldwide that collectively carry the bulk of the plastic waste into the oceans. The effects are evident: they threaten marine life and the well-being of people, as microplastics are now found even in drinking water.

In their response to the crisis, communities and environmentally minded individuals are ahead of governments and municipal authorities. They segregate waste, compost at home, conduct "plastic free" social events and help recover materials that would otherwise just be dumped in the suburbs and wetlands. But, valuable as they are, voluntary efforts cannot achieve what systemic reform can. It is the Centre's responsibility to ensure that the Environment (Protection) Act, the overarching law that enables anti-pollution rules to be issued, is implemented in letter and spirit. Ideally, regulation should help stop the manufacture of single-use plastic articles such as carry bags and cutlery, and encourage the use of biodegradable materials. There is a challenge here, though. The provisions of the Plastic Waste Management Rules require manufacturers of compostable bags to get a certificate from the Central Pollution Control Board, but this has not stopped counterfeit products from entering the market. Local bodies mandated under rules to ensure segregation, collection and transfer of waste to registered recyclers have spectacularly failed to fulfil their responsibilities. The State Level Monitoring Committees provided for under the rules have not been made accountable. The waste management framework is dysfunctional, and Mr. Vardhan's assertions on beating plastic pollution alone will not inspire confidence. India and the world face a plastics crisis. Solving it will take more than slogans.