Dr Sanjay Bahl

Cyber Security and Digital Trust

The future of cybersecurity and digital trust will belong to those who compute the safest with security and privacy addressed, and not the fastest, those who adopt continuous resilience models that evolve with technology, ensuring cyber resilience as the backbone of cybersecurity and trust in the digital age and our digital future.

Most of you in urban India or rural *Bharat* must be owners of a vehicle and would have witnessed the amazing amount of transformation across the automotive sector in the country. Today your vehicles are no longer considered just mechanical machines. Why? They now have millions of lines of sophisticated software, which is more than that of your Android smartphone or social media platform such as Facebook or a Boeing 787 aircraft! Once you are in your vehicle, it is a fusion of physical, biological, and digital worlds. This sophisticated mobility platform, your vehicle, has complex communication running across engine management, braking, and steering, rich personal information including your biometric data, regular travel destinations along with routes followed, or your detailed profile with respect to behaviour or movement patterns, as well as entertainment equipped with sensors/Internet of Things (IoT) devices for your favourite radio FM bands or browsing history, connectivity including satellite communication, automation, and cloud-driven intelligence.

We are living in an AAJA (*Asthirta, Anishchita, Jatilta, Aspashtata*) or VUCA (Volatile, Uncertain, Complex, Ambiguous) world, driven by BRAIN (Biotechnology, Robotics, Artificial Intelligence and Nanotechnology). These vectors are reshaping science and society, not just as engines of progress but also as essential for national security, scientific research, and global economic leadership. These have also created a dramatically expanded cyberattack surface, threatening the fragile backbone of trust in the digital age. The urgent need

The author is the Director General of the Indian Computer Emergency Response Team (CERT-In) and Controller of Certifying Authorities (CCA). Email: sanjay.bahl@nic.in

is for the backbone to be resilient, adaptive and protected across the six layers, namely: materials, devices and communication links layer; hardware and systems layer; operating system and network layer; application layer; assignment/task layer; and human layer. While you possess a driving license to drive your car safely by following the rules and regulations laid down in the country, did you also invest in understanding or being aware of basic cybersecurity and related hygiene? Did you say why? Let us consider, in brief, the six layers with respect to vehicles.

Materials, Devices and Communication Links Layer

Consider a supply chain attack on your vehicle's batteries, which could introduce a few faulty semiconductor materials to allow remote exploitation later, such as tampering with battery temperature sensors, leading to overheating or fire. Vehicles now provide satellite communication as a backup to traditional 4G and 5G for ensuring uninterrupted voice calls, as well as for providing navigation, thereby enhancing driver assistance. However, almost 99% of voice, data including daily transactions worth trillions of rupees/dollars, and streaming images are carried across the world through undersea cables. The attacks on satellites and undersea cables can be in the form of physical attacks/destruction, cyber intrusions, eavesdropping, causing widespread digital disruption due to loss of communication, disrupting the digital economy including global trade and e-commerce. Imagine you were traveling in the night on a hill road by your vehicle using satellite Global Positioning System (GPS) navigation, and someone decides to jam/spoof the GPS signals, disabling your ability to determine your location or traverse further. Or, what if you wanted to send photographs of your road travel, from your vehicle using your social media on your smartphone to your friends and family across continents, but could not because the undersea cables were destroyed. The cables would require repairs in a complex international waters governance structure.

Hardware and Systems Layer

It is now well known that backdoor implants are embedded into the hardware by adversaries, which can trigger malfunction, performance loss, and surveillance. Your vehicle has numerous electronic control units interconnected into an in-vehicle network. Modifying the memory of these control units and fake commands from an attacker at this layer can disrupt engine control or shut down and render your vehicle inoperable.

Operating System (OS) and Network Layer

Hackers exploit poorly secured over-the-air mechanisms for updates by inserting fraudulent messages, which could cause steering manipulation or disabling brakes. A ransomware attack could lead to a wider automotive ecosystem being impacted, causing delays in your vehicle delivery or its manufacturing or loss of your vehicle service history.

Application Layer

Using poor authentication and insecure application programming interfaces or cloud interfaces, or plugging in malware-ridden USB drives having your favourite songs or downloading malicious apps, which could result in your personal data being stolen, triggering unlocking doors or starting the engine or remote takeover of your vehicle by an adversary.

Assignment/Task Layer

If your vehicle's infotainment system is compromised, the threat actor can move laterally to manipulate the safety-critical functions of the vehicle or can exfiltrate your personal data or can send fake data to your vehicle's sensors, thereby poisoning control algorithms and tricking the vehicle to take wrong actions such as delayed brake response.

Human Layer

Humans are the weakest link, and an attacker can use social engineering to trick you. Your remote locking/unlocking key and ignition key signals can be captured for signal cloning or carried out replay attacks to exploit vulnerabilities in your vehicle, thereby allowing the fraudster complete access to your vehicle.

It should be clearly understood that cybersecurity is a risk that you need to manage by safeguarding your Device (vehicle), Identity and Data. Why do you trust your vehicle and its manufacturer? You trust the manufacturer to address all cybersecurity concerns! In today's AAJA world, trust is necessary to decrease the complexity or *jatilta*. Trust like quality, is a process which can be created, developed, maintained or destroyed, thus making it complex and subtle. It is based on perception of competence, goodwill and behaviour thus implying it can be managed by the manufacturer. How should a manufacturer ensure perception of competence from a cybersecurity perspective? By ensuring all necessary cybersecurity good practices are followed starting from developing components with security built in during the design stage, hardening all components and paths against various abuse cases, continuous monitoring and auditing of the ecosystem for any anomaly or vulnerability, gathering and acting upon threat intelligence, responding with agility during any cyber incident or crisis situation, and deploying public key infrastructure (PKI) as the backbone of digital trust through digital certificates for authentication, encryption, as well as integrity checks thereby allowing trusted interactions including data exchanges between the various IoT devices; provide scalable and cost-effective services in the cloud; and creating systems that are resistant to attacks from future quantum computers. This would help from a resilience perspective. Resilience is required for competitive advantage, leadership, as well as survivability of the manufacturer.

It is not a static skill, but employees and citizens can be trained through specific cognitive and behavioural practices, such that it can become habits thereby enhancing the individual's skills to face adverse situations or sudden disruptions. Hence, resilience requires a unified trust model where one PKI fabric binds digital compute, physical control, and biological processes into a single verifiable ecosystem to define the future of secure and trustworthy manufacturing, where trust is not just a differentiator but ensures safety, security and sovereignty for citizens.

Apart from the industry (automotive and technology) and citizens, the government too has a significant role to play:

- It needs to create enabling mechanisms for investing in talent. The convergence of the physical, biological, and digital worlds, along with sector or industry-specific needs, creates a profound skills gap. The clarity regarding the need for interdisciplinary experts who understand this space in depth and take up leadership positions is required.
- Cybersecurity for this converged world is a global issue. The government, industry, and academia must now collaborate with the vision for developing forward-looking policies and regulations, sovereign technologies, standards, threat sharing, & ethical guidelines to emerge as a global leader while being open for global collaboration by further improving ease of doing business for cutting-edge technology players, facilitating their tax holidays, and promoting startups.
- Commit to responsible innovation from a safety and security perspective for citizens thereby enhancing their trust in cutting-edge technologies. The understanding about immense power of this converged technology carrying dual-use risks, requiring strong ethical and governance frameworks before full-scale deployment.
- Ensuring futuristic flexible government structures, nimble and agile government entities staffed with sufficient talented officers and national level resilient defense mechanisms in place to implement adaptive and continuous protection of citizen and their data while providing the ability to proactively manage threats, hone decision making in crisis situations and working together with industry and citizens as a community to proactively thwart any malicious actor's plans and ecosystem.

With this in place, the future of cybersecurity and digital trust will belong to those who compute the safest with security and privacy addressed and not the fastest, those who adopt continuous resilience models that evolve with technology, ensuring cyber resilience as the backbone of cybersecurity and trust in the digital age and our digital future. We need to transition from the dusk of the AAJA or VUCA world to a new dawn of AAJA (*Akshi, Avdharana, Jaagrukta, Asthil*) or VUCA (Vision, Understanding, Clarity, Agility) world. This can shape India's developmental trajectory and future readiness to lead the world to a better tomorrow. ❑