सत्यनिष्ठा

डॉ संजय बहल

साइबर सुरक्षा और डिजिटल विश्वसनीयता

साइबर सुरक्षा और डिजिटल विश्वसनीयता का भविष्य उनके हाथ में होगा जो सुरक्षा और निजता का ध्यान रखते हुए सर्वाधिक सुरक्षा के साथ कंप्यूट (आकलन) करेंगे और केवल सबसे तेज़ आकलन पर ही ध्यान केंद्रित नहीं रखेंगे, उनके हाथ में भी रहेगा जो लगातार ऐसे लचीले मॉडल अपनाएंगे जिन्हें प्रौद्योगिकी की मदद से इस प्रकार विकसित किया जाएगा कि साइबर लचीलेपन को ही साइबर सुरक्षा का मुख्य आधार माना जाए और डिजिटल दौर तथा डिजिटल भविष्य के प्रति पक्का विश्वास भी बना रहे।

देश के शहरी या ग्रामीण किसी भी क्षेत्र में रहने वाले अधिकांश लोगों के पास अपना वाहन है और उन्होंने भारत के वाहन उद्योग (मोटर चालित वाहन उद्योग) में हुए आश्चर्यजनक बदलावों को जरूर देखा - समझा होगा। आज के दौर में आपके वाहन केवल यंत्रचालित मशीन नहीं रह गए हैं। क्यों? अब इन वाहनों में लाखों आधुनिकतम सॉफ्टवेयर लगे हैं जो आपके एंड्रॉयड स्मार्टफोन या फेसबुक जैसे सोशल मीडिया अथवा बोइंग 787 विमान जितने ही जटिल हैं। जब आप अपने वाहन में बैठते हैं तो वह स्थिति भौतिक, जैविक और डिजिटल दुनिया का सम्मिश्रण होती है। इस चलते-फिरते अति उन्नत प्लेटफ़ॉर्म यानी आपके वाहन में अत्यंत ही जटिल संचार व्यवस्थाएं होती हैं। जिनमें इंजन के नियंत्रण तथा ब्रेक और स्टीयरिंग को संभालने के साथ ही आपके बायोमेट्रिक डेटा (शारीरिक विवरण), आपके आने-जाने के नियमित स्थानों तथा वहां जाने के मार्गों का ब्यौरा भी रहता है; फिर, आपके व्यवहार या चलने-फिरने के तरीकों का डेटा भी वाहन के सॉफ्टवेयार में आता रहता है। साथ ही आपके मनपसंद रेडियो के एफएम बैंडों की या उन्हें बदलने से जुड़ी जानकारी भी सेंसरों / इंटरनेट ऑफ थिंग्स (आईओटी) उपकरणों के माध्यम से आपकी कार में उपलब्ध रहती है तथा उपग्रह संचार, ऑटोमेशन और क्लाउड चालित मेधा (बुद्धिमत्ता) सहित आपकी ब्राउजिंग की समूची जानकारी और कनेक्टिविटी का विवरण भी वाहन में पूरी तरह उपलब्ध रहता है।

हम वर्तमान दौर में ब्रेन (जैव प्रौद्योगिकी, रोबोटिक्स, कृत्रिम मेधा और नैनोप्रौद्योगिकी) द्वारा संचालित 'आजा' (अस्थिरता, अनिश्चितता, जटिलता तथा अस्पष्टता) अथवा 'वुका' (वोलेटाइल यानी परिवर्तनशीलता, अनिश्चित, जटिल, अस्पष्ट) दुनिया में जी रहे हैं। ये वेक्टर (वाहक) तत्व विज्ञान और समाज को नया आकार प्रदान कर रहे हैं और वह भी केवल प्रगति के वाहक बनकर ही नहीं बल्कि राष्ट्रीय सुरक्षा, वैज्ञानिक अनुसंधान, और वैश्विक आर्थिक

लेखक भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम के महानिदेशक और प्रमाणन प्राधिकरणों के नियंत्रक हैं। ईमेलः sanjay.bahl@nic.in

नेतृत्व के अनिवार्य तत्वों के रूप में भी ये तत्व क्रियाशील हैं। इन तत्वों ने साइबर हमले के आधार का नाटकीय ढंग से विस्तार करके डिजिटल युग के प्रति विश्वास की कच्ची नींव को भी हिलाकर रख दिया है। ऐसे में सबसे बड़ी जरूरत इस नींव को लचकदार और परिस्थितियों के अनुकूल तथा छह स्तरों तक सुरक्षित बनाने की है; ये छह स्तर हैं सामग्रियों, उपकरणों और संचार संपर्कों से जुड़ा स्तर; हार्डवेयर और सिस्टम स्तर; संचालन प्रणाली और नेटवर्क स्तर; एप्लीकेशन स्तर, असाइनमेंट/टास्क स्तर, और ह्यूमन (मानवीय) स्तर देश के निर्धारित नियम-क़ानूनों का पालन करते हुए अपनी कार को सुरक्षित ढंग से चलाने का ड्राइविंग लाइसेंस प्राप्त करते समय आपने क्या बुनियादी साइबर सुरक्षा और उससे जुड़ी हाइजीन (स्वच्छता) को जानने-समझने की भी कोशिश की थी? आप पूछते हैं क्यों ? आइये वाहनों के संदर्भ में इन छह स्तरों के बारे में संक्षेप में विचार करें।

सामग्री, उपकरणों और संचार संपर्कों से जुड़ा स्तर

ज़रा अपने वाहन की बैटरियों पर सप्लाई चेन हमले की कल्पना कीजिए, जिसकी वजह से एक दोषपूर्ण सेमीकंडक्टर लगा दिया जाए जो आगे चलकर इंजन या बैटरी को बेहद गर्म करने या उसमें आग लगने जैसी स्थिति का कारण बन सकता है। अब वाहनों में निर्बाध वॉयस कॉल की पक्की व्यवस्था करने के उद्देश्य से परम्परागत 4जी और 5जी के बैकअप विकल्प के तौर पर उपग्रह संचार प्रणाली लगाई जाती है जिससे नेविगेशन (दिशा संचालन) के साथ-साथ चालक को और ज्यादा सहायता उपलब्ध कराई जाती है। वैसे भी, समुद्र के नीचे बिछाए गए केबल नेटवर्क के जरिये लगभग 99 प्रतिशत वॉयस डेटा रोज हैंडल किया जाता है और लाखों चित्र भी इधर-उधर भेजे जाते हैं, कुल मिलाकर इनके माध्यम से खरबों रुपये / डॉलर का दैनिक कारोबार होता है। उपग्रह संचार और समुद्र के नीच बिछे केबल नेटवर्कों पर सीधे या साइबर हस्तक्षेप करके, ईव्सड्रॉपिंग अर्थात् चोरी-छिपे सुनने के जरिये संचार व्यवस्था काटकर / संचार को बहुत ज्यादा बाधित करके अथवा डिजिटल अर्थव्यवस्था को भारी नुकसान पहुंचाकर इन हमलों को अंजाम दिया जा सकता है क्योंकि इस प्रकार वैश्विक कारोबार और ई-कॉमर्स में रुकावट डाली जा सकती है। सोचिए कि आप रात के समय किसी पहाड़ी सड़क मार्ग पर जीपीएस (ग्लोबल पोजिशनिंग सिस्टम) की मदद से अपनी कार चला रहे हैं और अचानक कोई जीपीएस सिग्नलों को जाम (बंद) करने के इरादे से आपकी कार तक इन सिग्नलों को पहुंचने से रोक देता है; ऐसे में आप यह भी नहीं जान पाते कि आप कहां फंसे हैं तथा आगे चल पाना असंभव सा हो जाता है। यह भी कल्पना करें कि आप सड़क पर कार चलाते समय अपनी यात्रा के चित्र स्मार्टफोन के जरिये सोशल मीडिया पर या दूर किसी अन्य महाद्वीप में अपने मित्रों या परियजनों को भेजना चाहें लेकिन समुद्र के नीचे का केबल नेटवर्क नष्ट हो जाने की वजह से ऐसा नहीं कर पा रहे। अंतरराष्ट्रीय जलसीमा की कठिनाइयों के बीच केबलों की मरम्मत को जरा भी आसान नहीं समझा जा सकता। इसीलिए यह समस्या अत्यधिक जटिल और कठिन बन जाती है।

हार्डवेयर और सिस्टम का स्तर

यह तथ्य पूरी तरह सामने आ चुका है कि आपके दुश्मन बिना बताए कोई गैजेट लगाकर आपके हार्डवेयर में गड़बड़ी पैदा कर सकते हैं या उसकी क्षमता को घटा सकते हैं तथा उसकी चोरी-छिपे निगरानी भी कर सकते हैं। आपके वाहन में अनगिनत इलेक्ट्रॉनिक कंट्रोल यूनिटें लगी होती हैं जो कार के भीतर ही एक नेटवर्क के माध्यम से आपस में जुड़ी रहती हैं। इन कंट्रोल यूनिटों की मेमोरी में बदलाव लाकर या फेक कमांड (जाली आदेश) के जरिये इंजन को बेकाबू या बंद करके ऐसी स्थिति बनाई जा सकती है कि आपकी कार चलने के लायक न रह जाए।

संचालन प्रणाली और नेटवर्क स्तर

गलत इरादों से आपके सिस्टम में जबरन छेड़छाड़ करने वाले ये हैकर्स हल्की सुरक्षा-व्यवस्था प्रणालियों को अपडेट करने के बहाने से धोखाधड़ी वाले संदेश डाल देते हैं जिनके असर से वाहन की स्टेयरिंग बेकाबू हो सकती है या ब्रेक काम करना बंद कर सकते हैं। फिरौती मांगने की नीयत वाले साइबर हमले से तो कार के इकोसिस्टम को ज्यादा व्यापक नुकसान पहुंच सकता है जिससे आपके वाहन की डिलीवरी में देरी हो सकती है या उसके मेन्युफैक्चरिंग में देरी हो सकती है या फिर आपके वाहन का सर्विस रिकॉर्ड ही खत्म हो सकता है यानी मिटाया जा सकता है।

एप्लीकेशन स्तर

प्रमाणीकरण या पुष्टिकरण का असुरक्षित / हल्का कोड रखने या प्रोग्रामिंग इंटरफेस अथवा क्लाउड इंटरफेस सुरक्षित न होने या अपने पसंदीदा गाने के सुनने के लालच में नुकसान कर सकने वाले घटिया यूएसबी ड्राइव में प्लग-इन करने अथवा ऐसे घटिया ऐप डाउनलोड करने के कारण आपका निजी डेटा चुराया जा सकता है, कार के दरवाजे आसानी से खोले जा सकते हैं या कार का इंजन स्टार्ट किया जा सकता है या फिर आपके वाहन को रिमोट कंट्रोल से संचालित किया जा सकता है।

असाइनमेंट टास्क स्तर

यदि आपके वाहन के इंफोटेनमेंट सिस्टम से छेड़छाड़ संभव हो गई तो आपको नुकसान पहुंचाने का इरादा रखने वाला वाहन की सुरक्षा से जुड़े अहम फंक्शन्स में गड़बड़ी पैदा कर सकता है या आपका निजी डेटा कहीं भी या किसी को भी भेज सकता है या फिर आपके वाहन के सेंसरों तक जाली / फर्जी डेटा भेजकर उसके कंट्रोल से मनमानी छेड़छाड़ कर सकता है तथा इस प्रकार वह आपके वाहन में ब्रेक का प्रभाव देरी से होने जैसी गड़बड़ी पैदा कर सकता है।

मानवीय स्तर

मानव सबसे कमज़ोर कड़ी होते हैं और हैकर या साइबर हमलावर सोशल इंजीनियरिंग इस्तेमाल करके आपको धोखा दे सकता है। आपकी रिमोट लॉकिंग / अनलॉकिंग 'की' (चाबी) तथा इग्निशन 'की' के सिग्नल पकड़कर उनसे सिग्नलों के क्लोन तैयार

किए जा सकते हैं या आपकी कार के सिस्टम की खामियों का फायदा उठाकर बार-बार साइबर हमले करके धोखेबाज (हैकर) आपकी कार के संचालन को पूरी तरह अपने काबू में कर सकता है।

यह अच्छी तरह समझ लेना होगा कि साइबर सुरक्षा ऐसा खतरा है जिससे बचाव के लिए आपको अपने उपकरण (कार), उसकी पहचान तथा डेटा को सुरक्षित रखना होगा। आप अपनी कार या उसके मैन्युफेक्चरर (निर्माता) पर भरोसा क्यों करते हैं? साइबर सुरक्षा संबंधी सभी मामलों में आप निर्माता पर भरोसा करते हैं। आज के 'आजा' दौर में जटिलता से बचने के लिए भरोसा रखना जरूरी है। गुणवत्ता की तरह ही भरोसा भी एक समग्र प्रक्रिया है जो पैदा किया जा सकता है, विकसित किया (बढ़ाया) जा सकता है, बरकरार रखा जा सकता है या समाप्त किया जा सकता है; तभी तो इसे जटिल और नाजुक माना जाता है। भरोसा क्षमता, साख और व्यवहार की अवधारणा पर आधारित होता है जिसका सीधा अर्थ है कि यह पूरी तरह निर्माता (मैन्युफेक्चरर) पर निर्भर होता है। साइबर सुरक्षा के परिप्रेक्ष्य में निर्माता को क्षमता की धारणा कैसे सुनिश्चित करनी चाहिए? इसके लिए उसे सुनिश्चित करना होगा कि साइबर सुरक्षा से जुड़ी सभी क्रियाओं का सही तरीके से पालन हो अर्थात् डिज़ाइन तैयार करने के समय से ही सुरक्षा पेटी के अंगों का विकास शुरू किया जाए, सभी हिस्से पुर्ज़ों और सभी भागों को ऐसा बनाया जाए कि उनका दुरुपयोग न होने पाए, पूरे इकोसिस्टम की लगातार मॉनिटरिंग और ऑडिटिंग की जाए ताकि उसमें कोई खामी या कमी न रहे, खतरे की जानकारी मिलने पर पूरा ध्यान दिया जाए, साइबर घटना होने या साइबर खतरे की स्थिति लगने पर पूरी सतर्कता के साथ बचाव के उपाय किए जाएं तथा प्रमाणीकरण के लिए डिजिटल प्रमाणपत्रों के जरिये 'पब्लिक की इंफ्रास्ट्रक्चर' (पीकेआई) को डिजिटल भरोसे का मुख्य आधार माना जाए। साथ ही, क्लाउड में प्राप्त करने योग्य किफायती सेवाएं उपलब्ध की जाए; और ऐसे सिस्टम विकसित किए जाएं जो भविष्य के बड़े कंप्यूटरों से होने वाले हमलों को झेल सकें। इस तरह हम भावी व्यवस्था में लचीलापन ला सकेंगे। निर्माता को स्पर्धा में बेहतर स्थिति लाने, नेतृत्व संभालने और मज़बूती से टिके रहने में मदद देने के लिए लचीलापन होना जरूरी है। यह कौशल एक ही स्तर पर टिके रहने वाला नहीं है बल्कि कर्मचारियों और नागरिकों को विशिष्ट तौर-तरीकों की ट्रेनिंग देकर उनका कौशल विकसित किया जा सकता है और इससे खराब स्थिति या अचानक रुकावट आने पर अपने इसी कौशल के सहारे आगे बढ़ते रह सकते हैं। अतः लचीलेपन के लिए भरोसे के ऐसे एकीकृत मॉडल की जरूरत है जिसमें पीकेआई का एक सूत्र ही डिजिटल आकलन, भौतिक नियंत्रण और जैविक प्रक्रियाओं को एक ही इकोसिस्टम में समाहित करके सुरक्षित और विश्वासयोग्य निर्माण का भविष्य परिभाषित कर सकता है जहां भरोसा ही नागरिकों के बचाव, सुरक्षा और सार्वभौमिकता को सुनिश्चित करेगा।

इसमें उद्योग (मोटरवाहन और प्रौद्योगिकी) के साथ ही नागरिकों और सरकार को भी अहम भूमिका निभानी होगीः

- प्रतिभा में निवेश के लिए उपयुक्त तंत्र विकसित करने होंगे। भौतिक, जैविक और डिजिटल व्यवस्थाओं में समन्वयन के साथ ही क्षेत्र और उद्योग के हिसाब से खास जरूरतों पर ध्यान देने के साथ गहरा कौशल अंतराल भी पैदा हो जाएगा। इस अंतराल को समझकर उपयुक्त उपाय करने वाले विभिन्न विशेषज्ञों की भी आवश्यकता होगी जो उचित नेतृत्व भी कर सकें।
- परस्पर जुड़े इस विश्व में साइबर सुरक्षा वैश्विक मुद्दा बन चुका है। सरकार, उद्योग और शिक्षा क्षेत्र को एकजुट होकर भविष्य की नीतियां और नियम बनाने, मानक निर्धारित करने, खतरों पर ध्यान देने तथा नैतिक दिशा-निर्देश तय करने का सपना साकार करने की दिशा में प्रयास करने चाहिए ताकि भारत विश्व नेता के रूप में उभरकर अंतरराष्ट्रीय सहयोग बढ़ाने के लिए आधुनिकतम प्रौद्योगिकी अपनाने वाले देशों के लिए व्यापार की सुगमता अपनाकर करछूट की व्यवस्था तथा स्टार्ट-अप्स को बढ़ावा देने की व्यवस्था कायम कर सके।
- नागरिकों की रक्षा और सुरक्षा की दृष्टि से दायित्वपूर्ण नवाचार का संकल्प लेकर उनके मन में आधुनिक प्रौद्योगिकियों के प्रति विश्वास बढ़ाया जाए। इस समेकित प्रौद्योगिकी की जबरदस्त शक्ति को समझना होगा क्योंकि इसका दोहरा इस्तेमाल जोखिम भरा हो सकता है तथा इसे पूरी ताकत से लागू करने से पहले कड़ी नैतिक और संचालन नियमावली बनाना जरूरी है।
- भावी लचीले सरकारी ढांचों की सुनिश्चित व्यवस्था के लिए सतर्क और सक्षम सरकारी निकायों को अपने प्रतिभाशाली अधिकारियों तथा राष्ट्रीय स्तर के लचीले रक्षा तंत्रों के सहारे नागरिकों और उनके डेटा के निरन्तर संरक्षण की उपयुक्त नीति लाने के लिए जुट जाना होगा ताकि वे खतरों को पहले से ही भांपकर संकट की स्थिति के अनुरूप निर्णय ले सकें और उद्योग तथा नागरिकों के साथ मिलकर एक समुदाय के रूप में दुर्भावपूर्ण तत्वों की साजिशों को नाकाम करके इकोसिस्टम को सुरक्षित बना सकें।

ऐसा होने पर साइबर सुरक्षा और डिजिटल विश्वसनीयता का भविष्य न केवल उन लोगों के हाथ में होगा जो सुरक्षा और निजता को ध्यान में रखते हुए सर्वाधिक सुरक्षा के साथ आकलन करेंगे तथा सबसे तेज़ आकलन को ही अहमियत देंगे बल्कि उनके हाथ में भी रहेगा जो निरंतर ऐसे लचीले मॉडल अपनाएंगे जिन्हें प्रौद्योगिकी के सहारे इस तरह विकसित किया जाएगा कि साइबर लचीलेपन को ही साइबर सुरक्षा का प्रमुख आधार माना जाए और डिजिटल युग तथा डिजिटल भविष्य के प्रति पक्का विश्वास बना रहे। हमें 'आजा' और 'वुका' विश्व की गोधूलि बेला से 'आजा' (अक्षी, अवधारणा, जागरूकता, अस्थिल) के नवप्रभात या 'वुका' (विजन, सूझबूझ, स्पष्टता और सतर्कता) के विश्व के नवप्रभात की दिशा में बढ़ना होगा। यही भारत की विकास गति और विकास की ऊंचाई तथा विश्व के बेहतर कल में जाने की भावी तैयारियों को साकार बनाने का मूल मंत्र है। ❑