साइड चैनल अटैक को रोकने के लिये 'लो-एनर्जी चिप'

प्रिलिम्स के लिये:

साइड चैनल अटैक, इंटरनेट ऑफ थिंग्स।

मेन्स के लिये:

आईटी और कंप्यूटर साइड चैनल अटैक का मुकाबला करने में कम ऊर्जा चिप का महत्त्व।

चर्चा में क्यों?

हाल ही में दो भारतीय शोधकर्त्ताओं ने एक 'लो-एनर्जी' सुरक्षा चिप का निर्माण किया है, जिसे IoT (इंटरनेट ऑफ थिंग्स) उपकरणों पर 'साइड-चैनल अटैक' (SCAs) को रोकने के लिये डिज़ाइन किया गया है।

- IoT एक कंप्यूटिंग अवधारणा है जो रोज़मर्रा की भौतिक वस्तुओं के इंटरनेट से जुड़ाव और अन्य उपकरणों के लिये खुद को पहचानने में सक्षम होने के विचार का वर्णन करती है।
- इसका उपयोग बिजली, मोटर वाहन, सुरक्षा और निगरानी, दूरस्थ स्वास्थ्य प्रबंधन, कृषि, स्मार्ट होम और स्मार्ट सिटी आदि जैसे विभिन्न कार्यक्षेत्रों से जुड़े उपकरणों का उपयोग करके स्मार्ट बुनियादी ढाँचे को बनाने के लिये किया जा रहा है।

विगत वर्षों के प्रश्न

जब सुबह आपके स्मार्ट फोन का अलार्म बजता है, तो आप उठ जाते हैं और अलार्म को बंद करने के लिये उसे थपकी देते हैं जिससे आपका गीज़र स्वतः ही चल पड़ता है। आपके स्नानागार में लगा स्मार्ट दर्पण दिन के मौसम | को दर्शाता है और आपकी ऊपरी टंकी में पानी के स्तर का भी संकेत देता है। जब आप नाश्ता बनाने के लिये अपने रेफ्रिजिरेटर से कुछ किराना सामान निकाल लेते हैं, यह इसमें भंडारित सामान में आई कमी को जान लेता है और ताज़े किराना सामानों की पूर्ति के लिये क्रयादेश दे देता है। जब आप घर से बाहर कदम रखते हैं और दरवाज़े पर ताला लगाते हैं, तब सभी बत्तियाँ, पंखे, गीजर और ए.सी. मशीनें स्वतः बंद हो जाती हैं। आपके कार्यालय के रास्ते पर आपकी कार आगे आने वाले यातायात की भीड़ के बारे में आपको चेतावनी देती है और वैकल्पिक रास्ते का सुझाव देती है, यदि आपको किसी बैठक के लिये देर हो रही है, तो यह उसके अनुसार आपके कार्यालय में संदेश भेज देती है।

इन आविर्भुत होती हुई संचार प्रौद्योगिकियों के संदर्भ में उपर्युक्त परिदृश्य के लिये निम्नलिखित में से कौन-सा पद सबसे उपयुक्त रूप से लागू होता है?

(a) बॉर्डर गेटवे प्रोटोकॉल
(b) इंटरनेट ऑफ थिंग्स
(c) इंटरनेट प्रोटोकॉल
(d) वर्चुवल प्राइवेट नेटवर्क

उत्तर: (b)

सिक्योरिटी चिप:

- सिक्योरिटी चिप (Security Chip) का अर्थ है एप्लीकेशन विशिष्ट इंटीग्रेटेड सर्किट जो डिवाइस में एम्बेडेड (Embedded) होने के बाद सिक्योरिटी फीचर को इन्स्टैन्शिएट (Instantiates) करता है।

साइड-चैनल अटैक (SCA):

- 'साइड-चैनल अटैक'(SCA) एक विशिष्ट साइबर-सुरक्षा हमला है, जिसका उद्देश्य प्रोग्राम या उसके कोड को सीधे लक्षित करने के बजाय

सिस्टम या उसके हार्डवेयर के अप्रत्यक्ष प्रभावों का उपयोग करके सिस्टम के प्रोग्राम निष्पादन से जानकारी एकत्र करना या उसे प्रभावित करना है।

- आमतौर पर 'साइड-चैनल अटैक' का उद्देश्य सिस्टम की जानकारी, बिजली की खपत और इलेक्ट्रोमैग्नेटिक लीक जैसी सूचनाओं को मापकर क्रिप्टोग्राफिक कुंजी, मशीन लर्निंग मॉडल और पैरामीटर जैसी संवेदनशील जानकारी निकालना होता है।
    - SCA को साइडबार अटैक या इंप्लीमेंटेशन अटैक भी कहा जा सकता है।
    - इसे किसी भी डेटा पर लागू किया जा सकता है, जिसे गुप्त रखने का प्रयास किया जाता है।
        - उदाहरण के लिये इसका उपयोग आपकी स्मार्टवॉच पर आपके ECG और हृदय गति सिग्नल संबंधी जानकारी प्राप्त करने हेतु किया जा सकता है।
    - **SCAs के प्रकार:** टाइमिंग अटैक, इलेक्ट्रोमैग्नेटिक (EM) अटैक, एकॉस्टिक, पावर, ऑप्टिकल, मेमोरी कैश, हार्डवेयर संवेदनशीलता।
- यद्यपि अधिकांश आधुनिक प्रणालियों पर SCAs को निष्पादित करना मुश्किल है, किंतु मशीन लर्निंग एल्गोरिदम के बढ़ते परिष्कार, उपकरणों की अधिक कंप्यूटिंग शक्ति और बढ़ती संवेदनशीलता के साथ मापने वाले उपकरण SCAs को एक वास्तविकता बना रहे हैं।

//

'नए आर्किटेक्चर' का महत्त्व:

- **बहुत कम बिजली का उपयोग करता है:**
    - चूँकि SCAs का पता लगाना और उनके विरुद्ध बचाव करना मुश्किल है, इसलिये उनके खिलाफ कार्यवाही करना काफी अधिक कंप्यूटिंग शक्ति एवं ऊर्जा-गहन होती है। यही कारण है कि 'नया चिप आर्किटेक्चर' काफी महत्त्वपूर्ण हो जाता है।
    - यह चिप एक थंबनेल के आकार से भी छोटा है और SCAs के खिलाफ पारंपरिक सुरक्षा उपायों की तुलना में बहुत कम बिजली का उपयोग करता है।
- **आसानी से शामिल किया जा सकता है:**
    - इसे स्मार्टवॉच, टैबलेट और कई अन्य उपकरणों में आसानी से शामिल करने हेतु डिज़ाइन किया गया है।
    - इसका उपयोग किसी भी सेंसर नोड में किया जा सकता है, जो उपयोगकर्त्ता के डेटा को जोड़ता है। उदाहरण के लिये इसका उपयोग तेल और गैस उद्योग में सेंसर की निगरानी हेतु किया जा सकता है, इसका उपयोग सेल्फ-ड्राइविंग कारों में फिंगरप्रिंट उपकरणों जैसे कई अन्य अनुप्रयोगों में किया जा सकता है।
- **नियर-थ्रेसहोल्ड कंप्यूटिंग का उपयोग:**
    - **नियर-थ्रेसहोल्ड कंप्यूटिंग (Near-Threshold Computing)** का उपयोग एक कंप्यूटिंग विधि है जहाँ डेटा पर कार्य करने के लिये पहले इसे अलग, अद्वितीय और यादृच्छिक घटकों में विभाजित किया जाता है फिर चिप को अंतिम परिणाम हेतु एकत्र किये जाने से पहले प्रत्येक घटक पर यादृच्छिक क्रम में अलग-अलग संचालन किया जाता है।
    - इस पद्धति के कारण, बिजली की खपत माप (**Power-Consumption Measurements**) के माध्यम से डिवाइस से लीक होने वाली जानकारी यादृच्छिक होती है तथा SCA में अस्पष्टता के अलावा कुछ भी प्रकट नहीं करता है।
        - हालाँकि यह विधि ऊर्जा और गणना शक्ति-गहन पर आधारित है, जबकि सूचना को संग्रहीत करने के लिये अधिक आवश्यक सिस्टम मेमोरी की भी आवश्यकता होती है।

मुद्दे:

- सिस्टम में इस **चिप आर्किटेक्चर** के कार्यान्वयन हेतु असुरक्षित सिलिकॉन क्षेत्र के 1.6 गुना ऊर्जा खपत में कम-से-कम पाँच गुना वृद्धि की आवश्यकता होती है।
- इसके अलावा आर्किटेक्चर केवल ऊर्जा खपत-आधारित एससीए (**SCAs**) के खिलाफ सुरक्षा तो करता है लेकिन विद्युत-चुम्बकीय एससीए के खिलाफ बचाव नहीं करता है।

स्रोत: इंडियन एक्सप्रेस

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/low-energy-chip-to-prevent-side-channel-attacks