CEATEC

2019
10.15 火
10.18 金
幕張メッセ
10:00 ▶ 17:00

Overview

岡山大学ブースでは、IoTセキュリティ研究に関する展示を行います。経済発展と社会的課題の解決を両立し、人間中心の社会を実現する「Society 5.0」時代に向けて、各種センサーや入力などを通じて収集・保存されているデータを安全に取り扱う、IoTセキュリティに対する取り組みがますます重要になってきています。本学には、情報セキュリティ分野、特にIoTセキュリティ分野の研究者が数多くそろっており、今回はその研究内容の中から、暗号技術の実装、ハードウェアセキュリティ技術に関する研究について展示いたします。

皆様におかれましては、本学のブースに是非お立ち寄りいただき、研究者との交流を深め、御社のビジネスの発展のためにご活用いただければと思います。

IoT時代を支える暗号技術の安全な実装について
Secure Implementation of Cryptographies in IoT Era

大学院自然科学研究科 産業創成工学専攻
教授
野上 保之
Yasuyuki Nogami

IoT（モノのインターネット）時代においては、様々なものがインターネットに接続され、様々な種類の情報がコンピュータだけでなく小型のデバイス間でも送信されます。ID、誕生日、クレジットカード番号などの機密性の高い個人情報も含まれています。安全な送信のために、PCは効率的かつ安全に暗号化および復号を実行できるかも知れませんが、ICカードやマイクロコントローラなどの小型デバイス、つまりIoTデバイスにとっては非常に重い処理になります。IoTパラダイムにおいては、私たちを取り巻く多くのデバイスがネットワーク上で互いに接続されるため、セキュリティ確保が重要になります。一般的なサイバー攻撃（ウイルス攻撃、マルウェアなど）だけでなく物理的な攻撃も考慮する必要があります。その安全な実装について、暗号技術からの対策アプローチを展示するとともに，IoTセキュリティ・AIを軸とした岡山県からの寄附講座も紹介します。

IoT (Internet of things) era has come. Everything will be connected to the Internet and various types of information are transmitted between not only computers but also small devices. Of course, it includes very sensitive and private information such as ID, birthday, credit card number, and so on. PC can efficiently and securely carry out encryption and decryption for the secure transmission; however, it is very heavy for small devices such as IC card and microcontrollers, namely IoT devices. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be connected to each other on the network that is why the importance of security becoming the most crucial concern. Generally, most of the people think that only the cyber attack (such as virus attacks, malware) can happen through the internet. On the other hand, in the IoT era, we have to consider the physical attack along with the cyber attack. We will exhibit an approach from cryptographic technology for its secure implementation and also introduce the donation course from Okayama Prefecture focused on IoT security and AI.

暗号ハードウェアのセキュリティ評価・設計技術
Evaluation and Design Techniques for Cryptographic Hardware Security

大学院自然科学研究科 産業創成工学専攻
助教
五百旗頭 健吾
Kengo Iokibe

IoT機器にハードウェア実装される暗号アルゴリズムに対するセキュリティ上の脅威の一つであるサイドチャネル攻撃について、暗号回路の安全性評価および設計に関する技術を展示します。IoT機器に要求される情報セキュリティを実現するためには暗号技術が使われます。最新の暗号アルゴリズムは高度な数学に基づいており、理論的には現実的な時間（年数）では解読不可能と言われています。しかし製品で使用するため半導体ICに実装すると、新たな脅威にさらされます。サイドチャネル攻撃です。暗号化や復号処理を実行時に半導体ICから発生する電圧変動や電磁ノイズを観測され、分析されると、暗号鍵を特定される可能性があります。そこで製品に搭載される暗号回路のサイドチャネル攻撃耐性を評価するための測定技術、効率的な設計のための方法論を開発しています。さらに低コスト評価を可能にする組込み基板を紹介します。

We exhibit technology related to security evaluation and design of cryptographic circuits for side-channel attacks, one of the security threats to cryptographic algorithms implemented on hardware in IoT devices. Cryptographic technology is used to realize the information security required for IoT devices. Modern cryptographic algorithms are based on advanced mathematics and are theoretically unbreakable in realistic time (years). However, mounting it on a semiconductor IC for use in a product poses a new threat: side-channel attack. Some adversary can observe the voltage fluctuation or the electromagnetic noise generated from the semiconductor IC and analyzes at the time of executing the encryption and decryption processing. Then, they may identify the cryptographic key. Therefore, we are developing measurement techniques for evaluating side-channel attack resistance of cryptographic circuits incorporated in products and methodology for efficient design. We will also introduce embedded boards that enable low-cost evaluation.

Contact

OKAYAMA UNIVERSITY
研究推進機構
Organization for Research Strategy and Development
〒700-8530 岡山県岡山市北区津島中一丁目1番1号
TEL 086-251-8463／E-mail kikou@adm.okayama-u.ac.jp

国際展示場 岡山大学ブース（E072-67）