Safeguarding Cyber Security: Encryption in the age of IoT (Carmel)

(Photo by: Eli Gross)

Main Researcher: Prof. Orr Dunkelman

Background

The IoT (Internet of things) era brings with it a lot of promises: from energy saving to smart devices and smart homes, from better medical treatment to personal helpers that save time. This era relies heavily on many technologies, ranging from networking technologies that keep everything online and connected (such as internet, Wi-Fi and mobile communications), to machine learning (and especially deep learning) technologies for making smart predictions.

At the heart of all these technologies lies a huge volume of data, and most importantly private and sensitive data which includes not only medical information but also general private information that can be easily inferred. (e.g., daily schedules, shopping habits, political views, sexual preferences).

In addition to privacy concerns, the IoT vision is of a world controlled by many devices (e.g., for saving energy). This control should be highly protected and cherished, as a misuse of it can have a devastating impact. (Consider the DDoS attack on Dyn, for example, which relied on building a zombie network of IoT devices.)

To resolve these security and privacy issues, computer security must adapt. It must expand its reach from protecting fully fledged operating systems and strong devices to protection of low-end devices, using low-end computing power (computing power that is unlikely to be upgraded). The task of protecting the IoT ecosystem is key to progress in IoT development worldwide.

From lightweight to resource-heavy cryptography

Prof. Orr Dunkelman is an associate professor in the Department of Computer Science at the University of Haifa. His research focuses on cryptanalysis, cryptography, security, and privacy, especially in the context of biometric data. During his research he has worked on designing low-cost cryptographic primitives, such as the KATAN/KTANTAN families of block ciphers. The security building blocks that will be used to offer security and privacy to the IoT world will rely on the design and analysis of such lightweight cryptographic solutions.
Prof. Dunkelman has also worked on the new and exciting topic of white-box cryptography. Comprising yet another layer of security for the IoT world, white-box primitives try to maintain security in the presence of a continuous adversary which observes not only communications but also internal computations. As part of a joint research with a large international company, his research team has developed a family of new white-box primitives for their IoT solutions.

Potential Application
Security and privacy for IoT devices

Contact us for further information.

Related pages :

[Prof. Orr Dunkelman researcher page]

Carmel-Haifa University Economic Corporation Ltd.
Eshkol Tower, 25th floor, Room 2509 , Haifa University, Mount Carmel
Haifa 31905, ISRAEL
Tel: 972-4-8288500
Fax: 972-4-8288499