SCHOOL OF INFORMATICS AND COMPUTING

COMPUTER SCIENCE COLLOQUIUM SERIES

Oğuzhan Külekci

Istanbul Technical University

Tuesday, August 8, 2017

3:00 PM

Lindley Hall, Rm. 102

An Ambiguous Coding Scheme to Achieve Data Security with Less Encryption

Abstract: Achieving security with less encryption makes sense particularly on massive data volumes due to the heavy computational load of the encryption operations. Such a reduction may also help to increase the throughput of a crypto-system without a need to upgrade the computing infrastructures. In power-limited environments such as the mobile devices or sensor networks, performing less encryption is important to increase both the battery life and the throughput of the secure data production. Previously, selective encryption schemes, which encrypt only the selected sections of the data while keeping the rest in plain, have been proposed especially focusing on secure video/image delivery. Instead of encrypting only the selected sections of the input, we provide a solution that provides the security of the whole data with reduced amount of encryption via the introduced ambiguous coding scheme that encodes the input sequence of bits by splitting it into two streams as the payload and the disambiguation information. On ideal conditions that assumes the input data is independently and identically distributed, the payload occupies ≈ $(d-2)/d$, and the disambiguation information takes ≈ $2/d$ of the encoded stream, where $d > 2$ denotes a chosen block size in bits. We show that decoding the payload in absence of the disambiguation info is computationally hard with a complexity of $O(2^{2d}-1)$. Thus, encrypting only disambiguation info while keeping the payload plain can provide practical security of the whole data, which reduces the amount encryption by more than 75 percent for $d \geq 8$. Notice that, the reverse manner, where the payload is enciphered and the disambiguation information is kept intact, still provides 25% gain in encryption. The second case may be preferred to the first case when the ambiguity introduced by the proposed coding is not seen enough while transmitting a top-secret data. We include experimental results on high-entropy data to verify the theoretical claims on real-life cases, which reveals that the proposed coding is quite close to the ideal case on such data.

Biography: Dr. Külekci received his Ph.D. from Sabanci University, İstanbul, Turkey following the B.Sc. and M.Sc. degrees both obtained from Bogazici University, Department of Computer Engineering and Institute of Biomedical Engineering respectively. He has spent Fall-2009 and Spring-2010 semesters working at Texas A & M University, Department of Computer Science & Engineering as a research assistant professor in the research group of Prof. Jeffrey S. Vitter. He was with National Research Institute of Electronics & Cryptology, Turkey for nearly 15 years from 1999 to 2014, where he served at various research positions. He was the acting deputy director of the Genetics Engineering and Biotechnology Institute, Turkey between 2011 and 2013. Currently he is an associate professor at Informatics Institute, Istanbul Technical University, Turkey. His research focuses on algorithmic aspects of processing massive amounts of information both from theoretical and practical perspectives with special emphasize on bioinformatics applications. Combinatorial pattern matching, lossless data compression, compressed data structures, storage and indexing of massive data, and search engines are his most recent topics of interests. More information available at his homepage web.itu.edu.tr/kulekci.

SCHOOL OF INFORMATICS
AND COMPUTING
INDIANA UNIVERSITY
Bloomington