Announcing the Final Examination of Amerah Alabrah for the degree of Doctor of Philosophy

Time & Location: November 7, 2014 at 3:00 AM in Harris Corporation Engineering Center 438
Title: IMPROVED INTERNET SECURITY PROTOCOLS USING CRYPTOGRAPHIC ONE-WAY HASH CHAINS

In this dissertation, new approaches that utilize the one-way cryptographic hash functions in designing improved network security protocols are investigated. The proposed approaches are designed to be scalable and easy to implement in modern technology.

The first contribution explores session cookies with emphasis on the threat of session hijacking attacks resulting from session cookie theft or sniffing. In the proposed scheme, these cookies are replaced by easily computed authentication credentials using Lamport’s well-known one-time passwords. The basic idea in this scheme revolves around utilizing sparse caching units, where authentication credentials pertaining to cookies are stored and fetched once needed, thereby, mitigating computational overhead generally associated with one-way hash constructions.

The second and third proposed schemes rely on dividing the one-way hash construction into a hierarchical two-tier construction. Each tier component is responsible for some aspect of authentication generated by using two different hash functions. By utilizing different cryptographic hash functions arranged in two tiers, the hierarchical two-tier protocol (our second contribution) gives significant performance improvement over previously proposed solutions for securing Internet cookies. Through indexing authentication credentials by their position within the hash chain in a multi-dimensional chain, the third contribution achieves improved performance.

In the fourth proposed scheme, an attempt is made to apply the one-way hash construction to achieve user and broadcast authentication in wireless sensor networks. Due to known energy and memory constraints, the one-way hash scheme is modified to mitigate computational overhead so it can be easily applied in this particular setting.

The fifth scheme tries to reap the benefits of the sparse cache-supported scheme and the hierarchical scheme. The resulting hybrid approach achieves efficient performance at the lowest cost of caching possible.

In the sixth proposal, an authentication scheme tailored for the multi-server single sign-on (SSO) environment is presented. The scheme utilizes the one-way hash construction in a Merkle Hash Tree and a hash calendar to avoid impersonation and session hijacking attacks. The scheme also explores the optimal configuration of the one-way hash chain in this particular environment.

All the proposed protocols are validated by extensive experimental analyses. These analyses are obtained by running simulations depicting the many scenarios envisioned. Additionally, these simulations are supported by relevant analytical models derived by mathematical formulas taking into consideration the environment under investigation.

Major: Computer Science

Educational Career:
Bachelor’s of Computer Applications, BS, 2006, King Saud University
Master’s of Computer Science, MS, 2008, Colorado State University

Committee in Charge:
Mostafa Bassiouni, Chair, Electrical Engineering and Computer Science
Sheau-Dong Lang, Department of Electrical Engineering and Computer Science
Cliff C. Zou, Department of Electrical Engineering and Computer Science
Yuanli Bai, Department of Mechanical and Aerospace Engineering

Approved for distribution by Mostafa Bassiouni, Committee Chair, on October 23, 2014.

The public is welcome to attend.