Ala Altaweel

College Station, TX - Email me on Indeed: indeed.com/r/Ala-Altaweel/5dbfb293fb841a38

Seeking a software engineer internship for Summer 2017.
I am eligible to intern in United States with CPT.
Willing to relocate: Anywhere
Sponsorship required to work in the US

WORK EXPERIENCE

Software Engineer

High Performance Computing Center Stuttgart (HLRS) - Stuttgart, AR - August 2008 to August 2009

Implement a GUI using Google web toolkit (GWT) and integrate it with Java web services to facilitate users' SQL queries.

Software Engineer

Javna Mobile Media and Technology Solutions - Amman - February 2006 to August 2007

Design and develop software systems, services, and dynamic link libraries (DLL) for 3-tier web applications using C++ and C#.net.
- Develop short message peer-to-peer (SMPP) services for exchanging SMS messages with SMS center servers
using C#.net.
Software Engineering

EDUCATION

Ph.D. in Student

Texas A&M University - College Station, TX
January 2013 to Present

University of Stuttgart - Stuttgart
September 2014 to September 2016

local directory

Texas A&M University
September 2016

Glomosim network simulator using C

Texas A&M University
September 2013

Master of Science in Information Technology

Jordan University of Science and Technology
September 2007 to July 2009

SKILLS

C++ (4 years), Software Development (5 years), Security (4 years), Wireless (4 years), Networking (4 years), Network Security (4 years), Linux (6 years), Ubuntu (6 years), Windows (10+ years)

LINKS

https://scholar.google.com/citations?user=pQPTHbAAAAAJ&hl=en

https://www.linkedin.com/in/ala-altaweel-51390671/

GROUPS

Laboratory for Embedded & Networked Sensor Systems (LENSS) - Department of Computer Science and Engineering Texas A&M University

January 2013 to Present
http://faculty.cs.tamu.edu/stoleru/

PUBLICATIONS

Providing basic security mechanisms in broker-less publish/subscribe systems

http://dl.acm.org/citation.cfm?id=1827425
July 2010
The provisioning of basic security mechanisms such as authentication and confidentiality is highly challenging in a content-based publish/subscribe system. Authentication of publishers and subscribers is difficult to achieve due to the loose coupling of publishers and subscribers. Similarly, confidentiality of events and subscriptions conflicts with content-based routing. In particular, content-based approaches in broker-less environments do not address confidentiality at all. This paper presents a novel approach to provide confidentiality and authentication in a broker-less content-based publish-subscribe system. The authentication of publishers and subscribers as well as confidentiality of events is ensured, by adapting the pairing-based cryptography mechanisms, to the needs of a publish/subscribe system. Furthermore, an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality. Our approach provides fine grained key management and the cost for encryption, decryption and routing is in the order of subscribed attributes. Moreover, the simulation results verify that supporting security is affordable with respect to the cost for overlay construction and event dissemination latencies, thus preserving scalability of the system.

Traffic-and-resource-aware intrusion detection in wireless mesh networks

http://www.sciencedirect.com/science/article/pii/S1570870514000730
October 2014
As the interest in Wireless Mesh Networks (WMN), as an infrastructureless wireless network, grows, security issues, especially intrusion detection, become of paramount importance. The diversity in hardware along with a variety of WMN applications, have resulted in WMN with different network characteristics (e.g., resource levels, system and security models, etc.). Consequently, different intrusion detection mechanisms have been proposed by the research community. Recently, the community has proposed several monitoring techniques for intrusion detection where each considers different assumptions and presents a different problem formulation for optimal monitoring. This article proposes a taxonomy that categorizes existing solutions in this research area and identifies the similarities and differences in their optimal monitoring problem formulations. We then concentrate on two classes of monitoring techniques for intrusion detection in WMN: Traffic Agnostic and Resourceful and Traffic Aware and Resourceful and present centralized and distributed algorithms for solving optimal monitoring problem in these networks. Through extensive simulations and a real

implementation, we demonstrate the effects of different network characteristics on the problem formulation and consequently the performance (e.g., intrusion detection rate and resource consumption) of proposed solutions for optimal monitoring in WMN.

On secure shared key establishment for mobile devices using contextual information

http://ieeexplore.ieee.org/abstract/document/7410302/

December 2015

In this paper we first show that the Wi-Fi Protected Setup (WPS) protocol (used by Wi-Fi Direct, the de facto adhoc communication mechanism for smartphones and mobile devices) is vulnerable to a brute-force or dictionary attack. To defend against these attacks, we propose the idea of using contextual information (i.e., data obtained from mobile device's sensors) to establish a long (128 bits) secure session key between two Wi-Fi Direct enabled devices, instead of using the keypad. Our solution, Session Key Generated from Sensors (SekGens) employs three phases. In the Quantization Phase, the key is iteratively generated based on different sensors' data. In the Reconciliation Phase, the two devices eliminate minor differences in the bits of their keys by using the Cascade reconciliation mechanism. In the Privacy-Amplification-and-Hashing Phase, the two devices omit all bits exposed during the reconciliation phase and apply hashing to the remaining secret bits. SekGens is implemented and evaluated by modifying the Android kernel code responsible for WPS in Google Nexus 5 and Samsung Galaxy S2 smartphones. The results show that SekGens generates keys with low mismatch ratio (less than 3%), at a fast rate (~20 bits/sec), and with high entropy (~92%).

An efficient pairwise key establishment scheme for ad-hoc mobile clouds

http://ieeexplore.ieee.org/abstract/document/7348021/

October 2015

An Ad-hoc Mobile Cloud (AMC) is a new computing model that allows sharing computing power of multiple mobile devices. For a diverse group of individuals that employ such computing model, in an ad-hoc manner, secure peer-to-peer communication becomes very important. Using private or pairwise keys to secure such communication is preferable to public-keys because of computation and energy requirements [1]. With the advent of sensor enabled mobile devices, a protocol (SekGens) that uses sensor data to generate pairwise keys on demand has been proposed [2]. To work successfully SekGens requires devices to be closely located and becomes infeasible for devices situated multiple hops away. SekGens is also expensive in computation and slow in key generation. In this paper, we investigate how to enable devices in an AMC to establish pairwise keys. We propose an efficient solution which tries to reduce the number of executions of SekGens in the AMC, and establishes pairwise keys between nodes multiple hops away by distributing parts of the key on multiple routing paths. Our results show a reduction of up to 75% in the number of SekGens required to establish keys in an AMC, when compared to a naive approach.

Providing basic security mechanisms in a Publish/Subscribe system

https://131.159.74.67/sites/default/files/DIP_2872.pdf

July 2009

Publish-subscribe supports asynchronous interactions among processes in a distributed system. A process can describe its interest in messages by performing an operation called subscribe and will be notified about messages which match the specific interest.

Provision of basic security mechanisms such as authentication of publishers and subscribers and confidentiality of events and subscriptions is difficult in a publish-subscribe system.

Authentication is difficult to achieve due to the decoupled nature of interactions between the publishers and subscribers. Similarly confidentiality conflicts with the content based routing. Moreover, confidentiality is harder to address in broker-less environment, where the subscribers are clustered according to their interest.

In this thesis, new techniques to provide confidentiality and authentication in a brokerless content-based publish-subscribe built on P2P architecture are presented. Identitybased-encryption is used to provide authentication of publisher and subscriber and confidentiality of events. Furthermore, an algorithm is designed to cluster subscribers according to their subscriptions while preserving a weaker notion of confidentiality. Evaluation results show the feasibility of the technique in terms of dissemination latencies and messageoverhead.

ADDITIONAL INFORMATION

SKILLS:

1-Research: My research aims to build a security framework for Wi-Fi Direct technology (the de facto adhoc communication mechanism for smartphones and mobile devices). We studied the security attacks and issues of the in-band mode of Wi-Fi Protected Setup (WPS) protocol (i.e., used by Wi-Fi Direct devices to establish a secure key and connection between two devices). Our security framework contains a set of secure-key-establishment and challenge-response protocols, and algorithms. Please check my LinkedIn/GoogleScholar accounts for publications.

2-Programming Languages: (Proficient) C/C++, Java; (Familiar) C#.net, ASP.net, MATLAB

3-Kernel Programming: (Proficient) Android Mobile Operating System (CyanogenMod)

4-Web Technologies: (Proficient) HTML, XML, Web Services, Java Script, and Google Web Toolkit (GWT)

5-Database Systems: (Familiar) MySQL