Mahdi Daghmehchi Firoozjaei

Curriculum Vitæ (August 29, 2017)

Address	Sungkyunkwan University, Suwon 440-746, Republic of Korea
Phone	(+82) 31-299-4104
E-Mail	mdaghmechi@skku.edu
WWW	http://seclab.skku.edu/people/mahdi/

STATUS

PhD Candidate 2014-present
Electrical and Computer Engineering
Advisor: Professor Hyoungshick Kim

in Department of Electrical and Computer Engineering, College of Information and Communication Engineering, Sungkyunkwan University, Suwon, Republic of Korea

EDUCATION

M.Sc. Telecommunication-Cryptology 2002-2005
Imam Hossein Comprehensive University, Tehran, Iran
Thesis: "Review Security Weaknesses of IPSec and Suggestions for Improving Them"
Advisor: M. Saleh Esfahani (Imam Hossein Comprehensive University) / A. Yazdian Varjani (Tarbiat Modares University)

B.Sc. Telecommunication Engineering 1996-2000
Scientific-Applied Faculty of Post and Telecommunication, Tehran, Iran
Thesis: "Designing and Implementing an Announcement System for Public Phone Systems"

RESEARCH INTERESTS

- Cryptography; Network Security
- Users' Privacy Preserving in the Cellular Networks
- Secure Emergency Messaging Systems & False Requests Detecting
- Network Functions Virtualization- NFV; Security Issues
- Geo-encryption; Secure Location Based Services

REFEREED PUBLICATIONS

12. **Mahdi Daghmehchi Firoozjaei**, Sangmin Lee, and Hyoungshick Kim, "O^{2}TR: Offline Off-the-Record (OTR) Messaging", *WISA: The 18th World Conference on Information Security Applications 2017* , Jeju Island, Korea (2017).

11. **Mahdi Daghmehchi Firoozjaei**, Jaehoon (Paul) Jeong, Hoon Ko, and Hyoungshick Kim, "Security Challenges with Network Functions Virtualization", *ELSEVIER- Future Generation Computer Systems 67 (Feb 2017)* , 315-324 (2017).

10. **Mahdi Daghmehchi Firoozjaei**, Jaegwan Yu, Hyoungkee Choi, and Hyoungshick Kim, "Privacy-Preserving Nearest Neighbor Queries Using Geographical Features of Cellular Networks", *ELSEVIER- Computer Communications 98 (Jan 2017)* , 11-19 (2017).

9. **Mahdi Daghmehchi Firoozjaei**, Minchang Kim, and Hyoungshick Kim, "How Practical is OTR?", *CISC-S'16: Conference on Information Security and Cryptography 2016* , Busan, Korea (2016).

8. **Mahdi Daghmehchi Firoozjaei**, Jaewoo Park, and Hyoungshick Kim, "Detecting False Emergency Requests Using Callers' Reporting Behaviors and Locations", *DC2-2016: The 3rd International Workshop on Device Centric in conjunction with IEEE AINA* , Crans-Montana, Switzerland (2016).

7. Jinyong Kim, **Mahdi Daghmehchi**, Jaehoon (Paul) Jeong, Hyoungshick Kim, and Jung-Soo Park, "SDN-based Security Services using Interface to Network Security Functions", *ICTC: The 6th International Conference on ICT Convergence* , Jeju Island, Korea (2015).

6. **Mahdi Daghmehchi Firoozjaei**, Jaegwan Yu, and Hyoungshick Kim, "Privacy Preserving Nearest Neighbor Search based on Topologies in Cellular Networks", *DC2: The 2nd Workshop on Device Centric Cloud held in conjunction with IEEE AINA* , Gwangju, Korea (2015). **(Selected as "best paper")**

5. **Mahdi Daghmehchi Firoozjaei** and Javad Vahidi, "Implementing Geo-encryption in GSM cellular Network", *COMM 2012: 9th International Conference on Communication* , Bucharest, Romania (2012).

4. **Mahdi Daghmehchi Firoozjaei** and Ali Yazdian, "Evaluating Geo-encryption application in a cellular network, case study using GSM", *ISCEE 2011: 14th Iranian Student Conference on Electrical Engineering* **(in Persian)**, Kermanshah, Iran (2011).

3. **Mahdi Daghmehchi Firoozjaei** and Ali Yazdian, "Improving IPSec Security Weaknesses in the decryption key forgery situation", *16th Annual Computer Society of Iran Computer Conference* **(in Persian)**, Tehran, Iran (2011).

2. **Mahdi Daghmehchi Firoozjaei**, "Using MS location information in GSM encryption key generation, Study case: Geo-Encryption algorithm", *National Conference on Information and Communication Security* **(in Persian)**, Ahvaz, Iran (2010).

1. **Mahdi Daghmehchi Firoozjaei**, "Comparison between VPN solutions: MPLS, SSL, and IPSec", *7th Computer Engineering Student Conference* **(in Persian)**, Tehran, Iran (2005).

AWARDS

- **The 2nd Prize for the Superior Research Award**, College of Information and Communication Engineering, Sungkyunkwan University, August 3th 2017
- **The Best Paper Award**, DC2: The 2nd Workshop on Device Centric Cloud, 2015
- **The SKKU Scholarship for Outstanding International Students**, Sungkyunkwan University, 2014-2018

PROFESSIONAL SOCIETIES AND SERVICE

- Reviewer of:
  - Telecommunication Systems Journal- Springer
  - Computer & Electrical Engineering Journal- ELSEVIER
  - COMM2014, 10th International Conference on Communications
- Membership:
  - Iranian Society of Cryptology- ISC

TECHNICAL/SPECIAL SKILLS

- **Programming:** C/C++, Python, and Pascal
- **Simulation and Math package:** Matlab
- **Languages:** English, Arabic, and Persian (native language)