Yongdae Kim

IEEE Fellow
KAIST ICT Chair Professor, KAIST
Professor at School of Electrical Engineering, KAIST
and Graduate School of Information Security, KAIST
Head of Police Science and Technology Research Center, KAIST

yongdaek@kaist.ac.kr,yongdaek@gmail.com
https://yongdaek.github.io
Google Scholar

Research Interests

Current: Cellular Security, Drone Security, Self-driving Car Security, Embedded System Security
Former: Blockchain, Distributed System Security, Internet Security, Applied Cryptography

Work Experience

KAIST ICT Chair Professor Mar. 2025 – Present
Professor

National Academy of Engineering of Korea Mar. 2025 – Present
Member

IEEE Fellow 2024 – Present
Fellow

Police Science and Technology Research Center, KAIST Apr. 2022 – Present
Head

School of Electrical Engineering, KAIST Aug. 2012 – Present
Professor

Graduate School of Information Security Aug. 2012 – Present
Professor (Joint Appointment)

Cyber Security Research Center, KAIST Dec. 2017 – Feb. 2020
Director

KAIST Chair Professor Jan. 2013 – Dec. 2015
Professor

Dept. of Computer Science, University of Minnesota, Twin Cities Aug. 2002 – Jun. 2012
Assistant/Associate Professor

University of Minnesota, Twin Cities Jul. 2006 – Jun. 2008
McKnight Land-Grant Professor

University of California at Irvine Jan. 2001 – Jul. 2002
Visiting Researcher

Dept. of Computer Science, University of Southern California Sep. 1998 – Dec. 2000
Graduate Research Assistant

Electronics and Telecommunication Research Institute Feb. 1993 – Aug. 1998
Member of Research Staff

Education

University of Southern California Sep. 1998 – May 2002
Ph.D. in Computer Science
Advisor: Dr. Gene Tsudik

Yonsei University Mar. 1987 – Feb. 1993
B.S./M.S. in Mathematics

Publications

International Conferences

1. **OTABase: Enhancing Over-the-Air Testing to Detect Memory Crashes in Cellular Basebands**
   C. Park, M. Egli, B. Oh, T. Hoang, S. Jeong, M. Crettol, I. Yun, M. Payer, and **Y. Kim**
   Annual Computer Security Applications Conference (ACSAC'25)

2. **CITesting: Systematic Testing of Context Integrity Violations in LTE Core Networks**
   M. Son*, K. Kim*, B. Oh, C. Park, and **Y. Kim**
   ACM Conference on Computer and Communications Security (ACM CCS '25) **Distinguished Paper Award**

3. **XDAC: XAI-Driven Detection and Attribution of LLM-Generated News Comments in Korean**
   W. Go, H. Kim, A. Oh, and **Y. Kim**
   Annual Meeting of the Association for Computational Linguistics (ACL 2025)

4. **Too Much of a Good Thing: (In-)Security of Mandatory Security Software for Financial Services in South Korea**
   T. Yun, S. Jeong, Y. Lee, S. Kim, H. Kim, I. Yun and **Y. Kim**
   USENIX Security Symposium (Security 2025)

5. **LLFuzz: An Over-the-Air Dynamic Testing Framework for Cellular Baseband Lower Layers**
   T. Hoang, T. Oh, C. Park, I. Yun, **Y. Kim**
   USENIX Security Symposium (Security 2025)

6. **FirmState: Bringing Cellular Protocol States to Shannon Baseband Emulation**
   S. Jeong, B. Oh, K. Kim, I. Yun, **Y. Kim**, C. Park
   ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC 2025)

7. **Enabling Physical Localization of Uncooperative Cellular Devices**
   T. Oh, S. Bae, J. Ahn, Y. Lee, D.-T. Hoang, M. S. Kang, N. O. Tippenhauer, **Y. Kim**
   ACM International Conference on Mobile Computing and Networking (Mobicom 2024)

8. **A Systematic Study of Physical Sensor Attack Hardness**
   H Kim, R Bandyopadhyay, MO Ozmen, ZB Celik, A Bianchi, **Y. Kim**, D Xu
   IEEE Symposium on Security and Privacy (S&P 2024)

9. **Delegation of TLS Authentication to CDNs using Revocable Delegated Credentials**
   D Yoon, T Chung, Y Kim, **Y. Kim**
   Annual Computer Security Applications Conference (ACSAC 2023)

10. **BASECOMP: A Comparative Analysis for Integrity Protection in Cellular Baseband Software**
    E Kim, MW Baek, CJ Park, D Kim, **Y. Kim**, I Yun
    Network and Distributed System Security Symposium (NDSS 2023)

11. **LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper**
    TD Hoang, CJ Park, M Son, T Oh, S Bae, J Ahn, B Oh, **Y. Kim**
    ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC 2023)

12. **Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof**
    Jinseob Jeong, Dongkwan Kim, Joonha Jang, Juhwan Noh, Changhun Song, **Y. Kim**
    Network and Distributed System Security Symposium (NDSS 2023)

13. **Preventing SIM Box Fraud Using Device Fingerprinting**
    BeomSeok Oh*, Junho Ahn*, Sangwook Bae, Mincheol Son, Yonghwa Lee, Min Suk Kang, **Y. Kim** (* co-first)
    Network and Distributed System Security Symposium (NDSS 2023)

14. **Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels**
    Joonha Jang*, ManGi Cho*, Jaehoon Kim, Dongkwan Kim, **Y. Kim** (* co-first)
    Network and Distributed System Security Symposium (NDSS 2023)

15. **Are There Wireless Hidden Cameras Spying on Me?**
    Jeongyoon Heo, Sangwon Gil, Youngman Jung, Jinmok Kim, Donguk Kim, Woojin Park, **Y. Kim**, Kang G. Shin, Choong-Hoon Lee
    Annual Computer Security Applications Conference (ACSAC 2022)

16. **HearMeOut: detecting voice phishing activities in Android**
Joongyum Kim, Jihwan Kim, Seongil Wi, **Y. Kim**, Sooel Son
Annual International Conference on Mobile Systems, Applications and Services (Mobisys 2022)
Media: IT Media

17. **DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices**
CheolJun Park*, Sangwook Bae*, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, **Y. Kim** (* co-first)
USENIX Security Symposium (Security 2022)
CVEs: CVE-2019-2289, CVE-2021-25516, CVE-2021-30826
Github: DoLTEst

18. **Watching the Watchers: Practical Video Identification Attack in LTE Networks**
Sangwook Bae, Mincheol Son, Dongkwan Kim, CheolJun Park, Jiho Lee, Sooel Son, **Y. Kim**
USENIX Security Symposium (Security 2022)

19. **BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols**
Eunsoo Kim*, Dongkwan Kim*, Cheoljun Park, Insu Yun, **Y. Kim** (* co-first)
Network and Distributed System Security Symposium (NDSS 2021)
Github: BaseSpec

20. **FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis**
Mingeun Kim, Dongkwan Kim, Eunsoo Kim, Suryeon Kim, Yeongjin Jang, **Y. Kim**
Annual Computer Security Applications Conference (ACSAC 2020)
CVEs: CVE-2018-19986, CVE-2018-19987, CVE-2018-19988, CVE-2018-19989, CVE-2018-19990, CVE-2018-20114, CVE-2019-11399, CVE-2019-11400, CVE-2019-20082, CVE-2019-20084, CVE-2019-6258

21. **SoK: A Minimalist Approach to Formalizing Analog Sensor Security**
Chen Yan, Hocheol Shin, Connor Bolton, Wenyuan Xu, **Y. Kim**, Kevin Fu
IEEE Symposium on Security and Privacy (S&P 2020)

22. **Impossibility of Full Decentralization in Permissionless Blockchains**
Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, **Y. Kim**
ACM Advances in Financial Technologies (AFT 2019)
Webpage: https://sites.google.com/view/full-decentralization

23. **An Eye for an Eye: Economics of Retaliation in Mining Pools**
Yujin Kwon, Hyoungshick Kim, Yung Yi, **Y. Kim**
ACM Advances in Financial Technologies (AFT 2019)

24. **Is Stellar As Secure As You Think?**
Minjeong Kim, Yujin Kwon, **Y. Kim**
IEEE EuroS&B Workshop 2019
Webpage: https://sites.google.com/view/stellar-analysis
Media: Cointelegraph: Stellar's Blockchain Briefly Goes Offline, Confirming the Project Lacks Decentralization
Safety vs. Liveness in the Stellar Network, David Maziéres

25. **Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web**
Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, **Y. Kim**, Dongsu Han, Sooel Son, Seungwon Shin
Network and Distributed System Security Symposium (NDSS 2019)

26. **Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?**
Yujin Kwon, Hyoungshick Kim, Jinwoo Shin, **Y. Kim**
IEEE Symposium on Security and Privacy (S&P 2019)
Web page: https://sites.google.com/view/btc-vs-bch/

27. **Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane**
Hongil Kim, Jiho Lee, Eunkyu Lee, **Y. Kim**
IEEE Symposium on Security and Privacy (S&P 2019)
Webpage: https://sites.google.com/view/ltefuzz
CVEs: CVE-2019-5307, CVE-2019-20783
Media: ZDNet, SecurityWeek, Huawei, Engadget, Tech Xplore, Security Affairs, E-Crypto, Cybersecurity Insiders, Israel Defense, ITPro, UK, TGDaily, Gizmodo, DailyMail, UK, ···

28. **Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE**
Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, **Y. Kim**
USENIX Security Symposium (Security 2019)
Github: Sigover Injector, Sigover Gen

29. **Hidden Figures: Comparative Latency Analysis of Cellular Networks with Fine-grained State Machine Models**
Sangwook Bae, Mincheol Son, Sooel Son, **Y. Kim**
HotMobile 2019

30. **Who Spent My EOS? On the (In)Security of Resource Management of EOS.IO.**
Sangsup Lee, Daejun Kim, Dongkwan Kim, Sooel Son, **Y. Kim**
WOOT 2019

31. **Doppelgängers on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Services**
Changhoon Yoon, Kwanwoo Kim, **Y. Kim**, Seungwon Shin, Sooel Son
WWW 2019

32. **GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier**
Byeongdo Hong, Sangwook Bae, **Y. Kim**
Network and Distributed System Security Symposium (NDSS 2018)

33. **Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin**
Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Y. Vasserman, **Y. Kim**
ACM Conference on Computer and Communications Security (CCS 2017)
Media: ACM The Morning Paper

34. **Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications**
Hocheol Shin, Dohyun Kim, Yujin Kwon, **Y. Kim**
IACR CHES 2017
Media: The Register

35. **When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks**
Hyunwook Hong, Hyunwoo Choi, Dongkwan Kim, Hongil Kim, Byeongdo Hong, Jiseong Noh, **Y. Kim**
IEEE EuroS&P 2017

36. **Enabling Automatic Protocol Behavior Analysis for Android Applications**
Jeongmin Kim, Hyunwoo Choi, Hun Namkung, Woohyun Choi, Byungkwon Choi, Hyunwook Hong, **Y. Kim**, Jonghyup Lee, Dongsu Han
ACM CoNEXT 2016

37. **PIkit: A New Kernel-Independent Processor-Interconnect Rootkit**
WonJun Song, Hyunwoo Choi, Junhong Kim, Eunsoo Kim, **Y. Kim**, John Kim
USENIX Security (Security 2016)

38. **Doppelganger in Bitcoin Mining Pools: An Analysis of the Duplication Share Attack**
Yujin Kwon, Dohyun Kim, Yunmok Son, Jaeyeong Choi, **Y. Kim**
WISA 2016

39. **Pay as You Want: Bypassing Charging System in Operational Cellular Networks**
Hyunwook Hong, Hongil Kim, Byeongdo Hong, Dongkwan Kim, Hyunwoo Choi, Eunkyu Lee, **Y. Kim**
WISA 2016

40. **Dissecting Customized Protocols: Automatic Analysis for Customized Protocols based on IEEE 802.15.4**
Kibum Choi, Yunmok Son, Juhwan Noh, Hocheol Shin, Jaeyeong Choi, **Y. Kim**
ACM WISEC 2016
Best Paper Award

41. **This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump**
Young-Seok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, **Y. Kim**
WOOT 2016

42. **Sampling Race: Bypassing Timing-Based Analog Active Sensor Spoofing Detection on Analog-Digital Systems**

Hocheol Shin, Yunmok Son, Young-Seok Park, Yujin Kwon, **Y. Kim**
WOOT 2016

43. **Frying PAN: Dissecting Customized Protocol for Personal Area Network**
Kibum Choi, Yunmok Son, Jangjun Lee, Suryeon Kim, **Y. Kim**
WISA 2015

44. **Security Analysis of FHSS-type Drone Controller**
Hocheol Shin, Kibum Choi, Young-Seok Park, Jaeyeong Choi, **Y. Kim**
WISA 2015

45. **BurnFit: Analyzing and Exploiting Wearable Devices**
Dongkwan Kim, Suwan Park, Kibum Choi, **Y. Kim**
WISA 2015

46. **Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations**
H. Kim , D. Kim , M. Kwon , H. Han , Y. Jang, D. Han, T. Kim, **Y. Kim**
ACM Conference on Computer and Communications Security (CCS 2015)
CVEs: VU#943167, CWE-732, CWE-284, CWE-287, CWE-384, CVE-2015-6614
Media: US Cert, IT World, Nexus Security Bulletin, DSLReports, Softpedia, tom's guide, Pocketnow, FierceMobileIT, Techworm, Neowin, Network World

47. **Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors**
Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, **Y. Kim**
USENIX Security (Security 2015)
Media: New York Daily, Discover Magazine, Defense Systems, Techworm, Slashdot, Network World, Gizmodo

48. **Bittersweet ADB: Attacks and Defenses**
S. Hwang, S. Lee, **Y. Kim**, S. Ryu
ASIACCS 2015

49. **Run Away If You Can: Persistent Jamming Attacks against Channel Hopping Wi-Fi Devices in Dense Networks**
I.-G. Lee, H. Choi, **Y. Kim**, S. Shin, M. Kim
RAID 2014

50. **Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission**
Y. Go, J. Won, D. Foo Kune, E. Jeong, **Y. Kim**
Network and Distributed System Security Symposium (NDSS 2014)

51. **Towards accurate accounting of cellular data for TCP retransmission**
Y. Go, D. Foo Kune, S. Woo, K. Park, **Y. Kim**
HotMobile 2013

52. **Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors**
D. Foo Kune, J. Backes, S. Clark, W. Xu, D. Kramer, M. Reynolds, K. Fu, **Y. Kim** and W. Xu
IEEE Symposium on Security and Privacy (S&P 2013)
Media: The Register

53. **Dynamix: Anonymity on Dynamic Social Structures**
A. Mohaisen, H. Tran, T. Zhu, and **Y. Kim**
ASIACCS 2013

54. **Protecting Access Privacy of Cached Contents in Information Centric Networks**
A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, **Y. Kim**
ASIACCS 2013

55. **SocialCloud: Using Social Networks for Building Distributed Computing Services**
A. Mohaisen, H. Tran, A. Chandra, and **Y. Kim**
ASIACCS 2013

56. **Towards a safe Integrated Clinical Environment: A communication security perspective**
D. Foo Kune, E. Vasserman, K. Venkatasubramanian, **Y. Kim**, I. Lee
ACM MedCOMM 2012

57. **Measuring Bias in the Mixing Time of Social Graphs due to Graph Sampling**
A. Mohaisen, P. Luo, Y. Li, **Y. Kim**, Z. Zhang
MILCOM 2012

58. **One-way indexing for plausible deniability in censorship resistant storage**
E. Y. Vasserman, V. Heorhiadi , N. Hopper, **Y. Kim**
Usenix FOCI 2012

59. **On the Mixing Time of Directed Social Graphs and Security Implications**
A. Mohaisen, H. Tran , N. Hopper, and Y. Kim
ASIACCS 2012

60. **Location leaks over the GSM air interface**
D. F. Kune, J. Koelndorfer , N. Hopper, and **Y. Kim**
Network and Distributed System Security Symposium (NDSS 2012)
Media: Ars Technica

61. **Keep your friends close: Incorporating trust into social network-based Sybil defenses**
A. Mohaisen, N. Hopper, and **Y. Kim**
IEEE INFOCOM 2011

62. **Losing Control of the Internet: Using the Data Plane to Attack the Control Plane**
M. Schuchard, E. Vasserman , A. Mohaisen, D. F. Kune , N. Hopper, and **Y. Kim**
Network and Distributed System Security Symposium (NDSS 2011)
Media: New Scientist, ZDNet, The Register

63. **Balancing the Shadows**
M. Schuchard, A. Dean, V. Heorhiadi , **Y. Kim**, and N. Hopper
WPES 2010

64. **Measuring the mixing time of social graphs**
A. Mohaisen, A. Yun, and **Y. Kim**
ACM Internet Measurement Conference (IMC 2010)

65. **Recruiting New Tor Relays with BRAIDS**
R. Jansen, N. Hopper, and **Y. Kim**
ACM Conference on Computer and Communications Security (CCS 2010)

66. **On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage**
A. Yun, C. Shi, **Y. Kim**
ACM Cloud Computing Security Workshop (CCSW 2009)

67. **Membership-concealing overlay networks**
E. Vasserman, R. Jansen, J. Tyra, N. Hopper, **Y. Kim**
ACM Conference on Computer and Communications Security (CCS 2009)

68. **Scalable onion routing with Torsk**
J. McLachlan, A. Tran, N. Hopper, **Y. Kim**
ACM Conference on Computer and Communications Security (CCS 2009)

69. **Hashing it out in public: Common failure modes of DHT-based anonymity schemes**
A. Tran, N. Hopper, **Y. Kim**
WPES 2009

70. **The Frogboiling attack: limitations of anomaly detection for secure network coordinates**
E. Chan-Tin, D. Feldman, N. Hopper, **Y. Kim**
SecureComm 2009

71. **Why Kad Lookup Fails**
H.-J. Kang, E. Chan-Tin, N. Hopper, **Y. Kim**
IEEE International Conference on Peer-to-Peer Computing (P2P 2009)
Thanks: eMule Patch Log Dec, 7. 2009: Added a quick intermediate fix to make certain Kad lookups more reliable, improving the (search/source-) results in some cases [based on research from http://www-users.cs.umn.edu/ hopper/kad.pdf]

72. **Towards Complete Node Enumeration in a Peer-to-Peer Botnet**
B. Kang, E. Chan-Tin, C. Lee, J. Tyra, H. Kang, C. Nunnery, Z. Wadler, G. Sinclair, N. Hopper, D. Dagon, and **Y. Kim**

ASIACCS 2009

73. **Attacking the Kad Network**
P. Wang, J. Tyra, E. Chan-Tin, T. Malchow, D. Foo Kune, N. Hopper, and **Y. Kim**
SecureComm 2008
Thanks: eMule Patch Log Jun, 27. 2008: Several changes were made to Kad in order to defy routing attacks researched by University of Minnesota guys [Peng Wang, James Tyra, Eric Chan-Tin, Tyson Malchow, Denis Foo Kune, Nicholas Hopper, Yongdae Kim]

74. **Building Trust in Storage Outsourcing: Secure Accounting of Utility Storage**
V. Kher and **Y. Kim**
IEEE International Symposium on Reliable Distributed Systems (SRDS 2007)

75. **In-Situ Sensing Area Modeling for Wireless Sensor Networks**
J. Hwang, T. He, **Y. Kim**
ACM Conference on Embedded Networked Sensor Systems (SenSys 2007)

76. **Combating doublespending using cooperative P2P systems**
I. Osipkov, E. Vasserman, N. Hopper and **Y. Kim**
IEEE Conference on Distributed Computing Systems (ICDCS 2007)

77. **Realistic Sensing Area Modeling**
J. Hwang, Y. Gu, T. He, and **Y. Kim**
IEEE Infocom 2007

78. **Robust Accounting in Decentralized P2P Storage Systems**
I. Osipkov, P. Wang, N. Hopper and **Y. Kim**
IEEE Conference on Distributed Computing Systems (ICDCS 2006)

79. **Authenticated Key-Insulated Public Key Encryption and Timed-Release Cryptography**
J.-H. Cheon, N. Hopper, **Y. Kim** and I. Osipkov
Financial Cryptography and Data Security (Financial Crypto 2006)

80. **Experiences in Building an Object-Based Storage System based on the OSD T-10 Standard**
D. Du, D. He, C. Hong, J. Jeong, V. Kher, **Y. Kim**, Y. Lu, A. Raghuveer, S. Sharafkandi
NASA/IEEE Conference on Mass Storage Systems and Technologies (MSST 2006)

81. **SGFS: Secure, Efficient and Policy-based Global File Sharing**
V. Kher, E. Seppanen, C. Leach, **Y. Kim**
NASA/IEEE Conference on Mass Storage Systems and Technologies (MSST 2006)

82. **Strengthening Password-Based Authentication Protocols Against Online Dictionary Attacks**
P. Wang, **Y. Kim**, V. Kher, T. Kwon
ACNS 2005

83. **Batch Verifications with ID-Based Signatures**
H. Yoon, J. Cheon, **Y. Kim**
ICISC 2004

84. **Revisiting Random Key Pre-distribution Schemes for Wireless Sensor Networks**
J. Hwang, **Y. Kim**
ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN 2004)

85. **Admission Control in Collaborative Groups**
Y. Kim, D. Mazzochi, G. Tsudik
International Symposium on Network Computing and Applications (NCA 2003)

86. **An Efficient Tree-Based Group Key Agreement Using Bilinear Map**
S. Lee, **Y. Kim**, K. Kim, D. Ryu
ACNS 2003

87. **On the performance of Group Key Agreement Protocols**
Y. Amir, **Y. Kim**, C. Nita-Rotaru, G. Tsudik
IEEE International Conference on Distributed Computing Systems (ICDCS 2002)

88. **Communication-Efficient Group Key Agreement**
Y. Kim, A. Perrig, G. Tsudik
IFIP/SEC 2001

89. **Exploring Robustness in Group Key Agreement**
Y. Amir, **Y. Kim**, C. Nita-Rotaru, J. Schultz, J. Stanton and G. Tsudik
IEEE International Conference on Distributed Computing Systems (ICDCS 2001)

90. **Simple and Fault-tolerant Group Key Agreement Scheme**
Y. Kim, A. Perrig, G. Tsudik
ACM Conference on Computer and Communications Security (ACM CCS 2000)

91. **Secure Group Communication in Asynchronous Networks with Failures: Integration and Experiments**
Y. Amir, G. Ateniese, D. Hasse, **Y. Kim**, C. Nita-Rotaru, T. Schlossnagle, J. Schultz, J. Stanton and G. Tsudik
IEEE International Conference on Distributed Computing Systems (ICDCS 2000)

92. **On the Design of Stream Ciphers and a Hash Function Suitable to Smart Card Application**
Y. Kim, S. Lee, and S. Park
CARDIS 1996

International Journals and Transactions

1. **Passive Three-Dimensional User Equipment Tracking Using Long-Term Evolution Uplink Signals**
   Y. Jang, J. Park, T. Oh, Y. Kim, **Y. Kim** and S. O. Park
   IEEE Transactions on Instrumentation and Measurement 74, 2025

2. **Revisiting GPS Spoofing in Phasor Measurement: Real-World Exploitation and Practical Detection in Power Grids**
   C. Kim, J. Noh, E. Ghahremani, and **Y. Kim**
   ACM Transactions on Privacy and Security 28 (2), 2025

3. **Enhancing synchrophasor Reliability Through Network-Based Time Synchronization: KEPCO's Practical Approach**
   C. Kim, H. Kim, S. Lee, J. Noh, E. Ghahremani, and **Y. Kim**
   IEEE Power and Energy Magazine, 2025, 23 (1), 2025

4. **Lightbox: Sensor Attack Detection for Photoelectric Sensors via Spectrum Fingerprinting**
   D Kim, M Cho, H Shin, J Kim, J Noh, and **Y. Kim**
   ACM Transactions on Privacy and Security 26 (4), 2023

5. **Revisiting binary code similarity analysis using interpretable feature engineering and lessons learned**
   Dongkwan Kim, Eunsoo Kim, Sang Kil Cha, Sooel Son, and **Y. Kim**
   IEEE Transactions on Software Engineering (TSE) 2022
   Github: FirmKit

6. **Enabling the Large-Scale Emulation of Internet of Things Firmware With Heuristic Workarounds**
   Dongkwan Kim, Eunsoo Kim, Mingeun Kim, Yeongjin Jang, and **Y. Kim**
   IEEE Security & Privacy 19(6), 2021

7. **Amnesiac DRAM: A Proactive Defense Mechanism Against Cold Boot Attacks**
   Hoseok Seol, Minhye Kim, Taesoo Kim, **Y. Kim** and Lee-Sup Kim
   IEEE Trans. Computers (TC) 70(4), 2021

8. **The System That Cried Wolf: Sensor Security Analysis of Wide-area Smoke Detectors for Critical Infrastructure**
   Hocheol Shin, Juhwan Noh, Dohyun Kim and **Y. Kim**
   ACM Transactions on Privacy and Security (TOPS) 23(3), 2020

9. **Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing**
   Juhwan Noh, Yujin Kwon, Yunmok Son, Hocheol Shin, Dohyun Kim, Jaeyeong Choi and **Y. Kim**
   ACM Transactions on Privacy and Security (TOPS) 22(2), 2019
   Media: Electronics Weekly

10. **Large-Scale Analysis of Remote Code Injection Attacks in Android Apps**
    Hyunwoo Choi, **Y. Kim**
    Security and Communication Networks 2018

11. **GyrosFinger: Fingerprinting Drones for Location Tracking Based on the Outputs of MEMS Gyroscopes**
    Yunmok Son, Juhwan Noh, Jaeyeong Choi and **Y. Kim**
    ACM Transactions on Privacy and Security (TOPS) 21(2), 2018

12. **Peeking over the Cellular Walled Gardens - A Method for Closed Network Diagnosis -**
    Byeongdo Hong, Shinjo Park, Hongil Kim, Dongkwan Kim, Hyunwook Hong, Hyunwoo Choi, Jean-Pierre Seifert, Sung-Ju Lee and **Y. Kim**
    IEEE Transactions on Mobile Computing (TMC) 17, 2018

13. **Crime Scene Reconstruction: Online Gold Farming Network Analysis**
    Hyukmin Kwon, Aziz Mohaisen, Jiyoung Woo, **Y. Kim**, Eunjo Lee, Huy Kang Kim
    IEEE Transactions on Information Forensics and Security (TIFS) 12(3), 2017

14. **Private Over-Threshold Aggregation Protocols over Distributed Datasets**
    Myungsun Kim, Aziz Mohaisen, Jung Hee Cheon, **Y. Kim**
    IEEE Transactions on Knowledge and Data Engineering 28(9), 2016

15. **Hijacking the Vuze BitTorrent network: all your hop are belong to us**
Eric Chan-Tin, Victor Heorhiadi, Nicholas Hopper, **Y. Kim**
IET Information Security 9(4), 2015

16. **Timing Attacks on Access Privacy in Information Centric Networks and Countermeasures**
A. Mohaisen, H. Mekky, X. Zhang, H. Xie, **Y. Kim**
IEEE Transactions on Dependable and Secure Computing (TDSC) 12(6), 2015

17. **Revisting Security of Proportional Fair Scheduler in Wireless Cellular Networks**
H. Park, Y. Yi, **Y. Kim**
Elsevier Computer Networks, 75(A), 2014

18. **Secure encounter-based social networks: Requirements, challenges, and designs**
A. Mohaisen, D. Foo Kune, E. Vasserman, M. Kim, and **Y. Kim**
IEEE Transactions on Dependable and Secure Computing (IEEE TDSC) 10(4), 2013

19. **The Frog-Boiling Attack: Limitations of Secure Network Coordinate Systems**
E. Chan-Tin, V. Heorhiadi, **Y. Kim**, and N. Hopper
ACM Transactions on Information and System Security (TISSEC) 14(3), 2011

20. **Exploring In-Situ Sensing Irregularity in Wireless Sensor Networks**
J. Hwang, T. He, and **Y. Kim**
IEEE Transactions on Parallel and Distributed Systems (TPDS) 21(4), 2010

21. **On Homomorphic Signatures for Network Coding (Brief Contribution)**
A. Yun, J. Cheon, **Y. Kim**
Transactions on Computers (TC) 59(9), 2010

22. **Attacking the Kad Network - Real World Evaluation and High Fidelity Simulation using DVN -**
E. Chan-Tin , P. Wang, J. Tyra, T. Malchow, D. Foo Kune, N. Hopper, **Y. Kim**
Wiley Security and Communication Networks, 2009

23. **Secure Localization with Phantom Node Detection**
J. Hwang, T. He, **Y. Kim**
Elsevier Ad Hoc Networks 6(7), 2008

24. **Provably Secure Timed-Release Public Key Encryption**
J. Cheon, N. Hopper, **Y. Kim**, I. Osipkov
ACM Transactions on Information Systems Security (TISSEC) 11(2), 2008

25. **Design and implementation of a secure multi-agent marketplace**
A. Jaiswal, **Y. Kim**, M. Gini
Elsevier Electronic Commerce Research and Application 3(4), 2004

26. **On the Performance of Group Key Agreement Protocols**
Y. Amir, **Y. Kim**, C. Nita-Rotaru, G. Tsudik
ACM Transaction on Information and System Security (TISSEC) 7(3), 2004

27. **Robust Contributory Key Agreement in Secure Spread**
Y. Amir, **Y. Kim**, C. Nita-Rotaru, J. Schultz, J. Stanton, G. Tsudik
IEEE Transaction on Parallel and Distributed System (TPDS) 15(5), 2004

28. **Communication-Efficient Group Key Agreement**
Y. Kim, A. Perrig, G. Tsudik
IEEE Transaction on Computers (TC) 53(7), 2004

29. **Tree-based Group Key Agreement**
Y. Kim, A. Perrig, G. Tsudik
ACM Transaction on Information and System Security (TISSEC) 7(1), 2004

30. **Secure Group Key Management for Storage Area Networks**
Y. Kim, F. Maino, M. Narasimha, K. Rhee, G. Tsudik
IEEE Communications Magazine 41(8), 2003

31. **On the Security of Lin-Chang-Lee Public Key Cryptosystem**
S. Park, **Y. Kim**, and K. Kim
Journal of the Korean Institute of Information Security and Cryptography, 1996

International Patents: Granted

1. **Dynamic security analysis method for control plane and system therefore**
   Y. Kim, Hongil Kim, Jiho Lee, Eunkyu Lee
   US11463880B2
2. **Method for GPS spoofing detection with GPS receivers leveraging inaccuracies of GPS spoofing devices and apparatus therefore**
   Y. Kim, Juhwan Noh, Jaehoon Kim, Dohyun Kim, Song Min Kim
   US12025713B2
3. **Physical signal overshadowing attack method for LTE broadcast message and the system thereof**
   Y. Kim, Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim
   US11405787B2
4. **Apparatus and method for diagnosing abnormality of mobile communication network using operational logic modeling and comparative analysis**
   Y. Kim, Sangwook Bae, Mincheol Son, Sooel Son
   USUS11082866B2
5. **Apparatus and method for diagnosing anomaly in mobile communication network**
   Y. Kim, Byeong Do Hong, Sung-Ju Lee, Shinjo Park, Hongil Kim, HyunWook Hong, Dongkwan Kim, HyunWoo Choi
   US10111120B2

Professional Activities

Organizing and Steering Committee

Steering Committee chair, *ISOC Network and Distributed System Security (NDSS) Symposium*, 2024 – Present

Steering Committee member, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2022 – Present

Program Committee Co-chair, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2022

General Co-chair (with Jong Kim), *ACM Conference on Computer and Communications Security (CCS)*, 2021

Program Committee Co-chair (with Javier Lopez, Taesoo Kim), *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, 2018

Editorial Board Member, *ACM Transactions on Privacy and Security (previously, ACM Transactions on Information and System Security)*, 2013 – 2020

Steering Committee Member, *ISOC Network and Distributed System Security Symposium (NDSS)*, 2013 – 2018

Program Committee Co-Chair (with Adrian Perrig, Heejo Lee), *International Workshop on Information Security Applications (WISA)*, 2013

Guest Editor, *Special Issue on Security and Privacy in Emerging Wireless Networks, IEEE Wireless Communications Magazine*, 2010

Program committee co-chair, *StorageSS, ACM CCS Workshop*, 2008

NSF Student Travel Grant Committee Chair, *IEEE Infocom*, 2007

Local Steering Committee, *Workshop on Economics of Information Security (WEIS)*, 2004

Conference/Workshop Program Committee (Selected)

ACM Conference on Computer and Communications Security (CCS), 2013 – 2015, 2017 – 2022, 2025

IEEE Symposium on Security and Privacy (S&P), 2007 – 2008, 2013 – 2015, 2021 – 2022, 2025

Usenix Security Symposium (Security), 2017 – 2025

ISOC Network and Distributed System Security Symposium (NDSS), 2011 – 2025

ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2014 – 2015, 2023 – 2025

ACM ASIA Conference on Computer and Communications Security (ASIACCS), 2008, 2012 – 2013

IEEE International Conference on Distributed Computing Systems (ICDCS), 2006, 2009-2011, 2013

IEEE European Symposium on Security and Privacy (EuroS&P), 2016

Honors & Awards

Academic awards

The National Academy of Engineering of Korea, Member	2025
KAIST ICT Chair Professor	2025
IEEE Fellow	2024
Best Lecture Award, KAIST Electrical Engineering	2022
Best Paper Award, ACM Wisec	2016
KAIST Chair Professor, KAIST	Jan. 2013 – Dec. 2015
McKnight Land-Grant Professorship Award, University of Minnesota, Twin Cities	2006
NSF CAREER Award	2005