

Doowon Kim

PHD STUDENT IN CS @ UMD

Department of Computer Science, University of Maryland, College Park, MD 20742

☎ (+1) 801-960-3235 | ✉ doowon@cs.umd.edu | 🏠 www.cs.umd.edu/~doowon/ | 📱 doowon

Research Interests

Computer security and privacy, code signing PKI, and computer networks

Education

University of Maryland

PH.D. IN COMPUTER SCIENCE

College Park, MD, USA

Jun. 2014 - present

Washington University in St. Louis

PH.D. IN COMPUTER SCIENCE

St. Louis, MO, USA

Aug. 2013 - May 2014

- Advisor: Jonathan S. Turner
- Transferred to UMD due to Dr. Turner's retirement.

University of Utah

M.S. IN COMPUTER SCIENCE

Salt Lake City, UT, USA

Aug. 2011 - May 2013

Hankuk University of Foreign Studies

B.S. IN COMPUTER SCIENCE AND ENGINEERING

South Korea

Mar. 2003 - Feb. 2011

- GPA: 4.21/4.5 (overall), 4.4/4.5 (CS major), 4.34/4.5 (upper)
- Graduated with honors, ranked 1/33

Publications

Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI.

Doowon Kim, Bum Jun Kwon, and Tudor Dumitraş. In CCS 2017: ACM Conference on Computer and Communications Security. October 2017.

Media: Schneier on Security, The Register, The SSL Store, Ars Technica, Threatpost, Tech Wire Asia, End Game, CPS-VO, Systweak, Fortuna's Corner, Security Affairs, The Hacker News, Security Intelligence, Tech Target

fFTP: a fast file transfer protocol for home N-screen platform.

Doowon Kim, Jinsuk Baek, Paul S Fisher, Sangchul Kim. Personal and Ubiquitous Computing. October 2017. DOI: 10.1007/s00779-017-1082-5

Lessons learned from using an online platform to conduct large-scale, online controlled security experiments with software developers.

Christian Stransky, Yasemin Acar, Duc Cuong Nguyen, Dominik Wermke, Elissa M. Redmiles, **Doowon Kim**, Michael Backes, Simson Garfinkel, Michelle L. Mazurek, and Sascha Fahl. In CSET 2017: USENIX Workshop on Cyber Security Experimentation and Test. August 2017

Balancing security and usability in encrypted email.

Wei Bai, **Doowon Kim**, Moses Namara, Yichen Qian, Patrick Gage Kelley, and Michelle L. Mazurek. In IEEE Internet Computing: 21 (3), 30-38. 2017.

How Internet Resources Might Be Helping You Develop Faster but Less Securely.

Yasemin Acar, Michael Backes, Sascha Fahl, **Doowon Kim**, Michelle L Mazurek, Christian Stransky. In IEEE Security & Privacy, vol. 15, no. 2, pp. 50-60, 2017. doi: 10.1109/MSP.2017.24. (The authors are alphabetically ordered.)

Comparing the usability of cryptographic APIs.

Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, **Doowon Kim**, Michelle L. Mazurek, and Christian Stransky. In the 2017 IEEE Symposium on Security and Privacy. May 2017. (The authors are alphabetically ordered.)

An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems.

Wei Bai, **Doowon Kim**, Moses Namara, Yichen Qian, Patrick Gage Kelley, and Michelle L. Mazurek. In SOUPS 2016: USENIX Symposium on Usable Privacy and Security (SOUPS 2016). June 2016.

You get where you're looking for: The impact of information sources on code security.

*Awarded the 5th annual NSA Best Scientific Cybersecurity Paper.

Yasemin Acar, Michael Backes, Sascha Fahl, **Doowon Kim**, Michelle L. Mazurek, and Christian Stransky. In the 2016 IEEE Symposium on Security and Privacy (Oakland 2016). May 2016. (The authors are alphabetically ordered.)

Adaptive Video Streaming over HTTP.

Doowon Kim, Jinsuk Baek, and Paul S. Fisher. In the 49th ACM Southeast Conference (ACM SE 2014). March 2014. (poster session)

Implementation of Framework to Identify Potential Phishing Websites.

Doowon Kim, Chaitanya Achan, Jinsuk Baek, and Paul S. Fisher. In the 2013 IEEE Intelligence and Security Informatics (IEEE ISI 2013). June 2013. (poster session)

An Adaptive Primary Path Switching Scheme for Seamless mSCTP Handover.

Jinsuk Baek, **Doowon Kim**, Paul S. Fisher, and Minho Jo. In the Smart Computing Review (Smart CR). December 2011 (Invited Paper)

Research Experience

University of Maryland, College Park

College Park, MD, USA

GRADUATE RESEARCH ASSISTANT

Jun. 2015 - present

- Supporting Secure Mobile App Development. Advised by Prof. Michelle L. Mazurek
- Code signing PKI abuse. Advised by Prof. Tudor Dumitras

Washington University in St. Louis

St. Louis, MO, USA

GRADUATE RESEARCH ASSISTANT

Jun. 2013 - May 2014

- Forest Overlay Network: Targeted for large distributed real-time applications such as an online virtual world. Advised by Prof. Jonathan S. Turner

University of Utah

Salt Lake City, UT, USA

GRADUATE RESEARCH ASSISTANT

Aug. 2011 - May 2013

- Utah Testing Software: Learning Management System (LMS) for the Chemistry department at Utah in GWT

Korea Electronics Technology Institute (KETI)

South Korea

RESEARCH INTERN

Feb. 2008 - Jul. 2011

- Programmable Communicating Thermostat
- RF Communication Module for Health Data
- Test module compatible with CHA (Continua Health Alliance)
- Platform board compatible with CHA

Honors & Awards

Oct. 2017 **The 5th annual NSA Best Scientific Cybersecurity Paper**, Paper title: "You get where you're looking for: The impact of information sources on code security" *USA*

Feb. 2011 **Valedictorian Award**, Graduated with honors, ranked 1st in Dept. of CSE at HUFS *South Korea*

2003-2010 **Hankuk University of Foreign Studies Scholarships**, Seven merit-based scholarships *South Korea*

Talks

You get where you're looking for: The impact of information sources on code security.

In HCIL Annual Symposium, Maryland, May 2016.

At Bowie State University, Maryland, April 2016.

Academic Activity

NSDI '13 shadow committee

Salt Lake City, UT, USA

SHADOW COMMITTEE MEMBER

Oct. 2012 - Dec. 2012

FAST '12

San Jose, CA, USA

STUDENT GRANT

Feb. 2012

- Received Student Grant and submitted summaries of two sessions (5 presentations)

GNUVILL open source group

South Korea

MEMBER

Mar. 2003 - Feb. 2011

- Open source group
- Linux tutor for the members of the club

Skills

Languages	Java, Python, C, C++, Javascript, Golang, LaTeX
Eclipse Frameworks	GEF, EMF, GMF, CDT
Embedded Systems	Nut/OS, AVR Firmware, ARM Linux, DirectFB, Disko
Web	GWT
Revision control software	GIT, SVN, CVS
Networks	NS-2, openNMS, Mininet, SNMP