

# Haehyun Cho

✉ haehyun@asu.edu

🔗 <https://haehyun.github.io>

🌐 <https://github.com/haehyun>

## ○ EDUCATION

---

### Ph.D., Computer Science

Arizona State University, Tempe, AZ

Aug 2016–Present

### M.S., Computer Science and Engineering

Soongsil University, Seoul, Korea

Feb 2015

- Thesis: *Mobile App Tamper Detection Scheme Based on Core Code Attestation*

### B.S., Computer Science and Engineering

Soongsil University, Seoul, Korea

Feb 2013

## ○ PUBLICATIONS

---

### • Conference Presentation with Proceedings (refereed)

1. Penghui Zhang, Adam Oest, **Haehyun Cho**, Zhibo Sun, RC Johnson, Brad Wardman, Shaown Sarker, Alexandros Kapravelos, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn, “CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing,” in *Proceedings of the 42nd IEEE Symposium on Security and Privacy (IEEE S&P)*, San Francisco, CA, May 2021.
2. **Haehyun Cho**, Jinbum Park, Joonwon Kang, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn, “Exploiting Uninitialized Stack Memory Uses in the Linux Kernel for Leaking Kernel Pointers,” in *Proceedings of the 14th USENIX Workshop on Offensive Technologies (Usenix WOOT)*, Online, Aug 2020. (33% acceptance rate.)
3. **Haehyun Cho**, Jinbum Park, Donguk Kim, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn, “SmokeBomb: Effective Mitigation Against Cache Side-channel Attacks on the ARM Architecture,” in *Proceedings of the 18th ACM International Conference on Mobile Systems, Applications, and Services (ACM MobiSys)*, Online, Jun 2020. (19% acceptance rate.)
4. Penghui Zhang, **Haehyun Cho**, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn, “iCORE: Continuous and Proactive Extrospection on Multi-core IoT Devices,” in *Proceedings of the 34th ACM/SIGAPP Symposium On Applied Computing (ACM SAC)*, Limassol, Cyprus, Apr 2019. (24% acceptance rate.)
5. **Haehyun Cho**, Penghui Zhang, Donguk Kim, Jinbum Park, Choong-Hoon Lee, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn, “Prime+Count: Novel Cross-world Covert Channels on ARM Trust-Zone,” in *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC)*, San Juan, Puerto Rico, USA, Dec 2018. (20% acceptance rate.)
6. Jaejong Baek, Sukwha Kyung, **Haehyun Cho**, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn, “Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling,” in *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC)*, San Juan, Puerto Rico, USA, Dec 2018. (20% acceptance rate.)

### • Published and Accepted Journal Articles (refereed)

1. **Haehyun Cho**, Jeong Hyun Yi, and Gail-Joon Ahn. “DexMonitor: Dynamically Analyzing and Monitoring Obfuscated Android Applications,” *IEEE Access*, Volume 6, pp.71229–71240 Nov 2018.
2. **Haehyun Cho**, Jiwoong Bang, Myeongju Ji, and Jeong Hyun Yi, “Mobile application tamper detection scheme using dynamic code injection against repackaging attacks,” *The Journal of Supercomputing*, Vol.72, No.9, pp.3629–3645, Sep 2016.
3. Yiming Jing, Gail-Joon Ahn, Hongxin Hu, **Haehyun Cho**, and Ziming Zhao, “TRIPLEMON: A Multi-layer Security Framework for Mediating Inter-Process Communication on Android,” *Journal of Computer Security*, Vol.24, No.4, pp.405–426, Sep 2016.
4. **Haehyun Cho**, Jiwoong Bang, Myeongju Ji, and Jeong Hyun Yi, “Anti-debugging scheme for protecting mobile apps on android platform,” *The Journal of Supercomputing*, Vol.72, No.1, pp.232–246, Jan 2016.
5. Jongwon Choi, **Haehyun Cho**, and Jeong Hyun Yi, “Personal Information Leaks with Automatic Login in Mobile Social Network Services,” *Entropy Journal*, Vol.17, No.6, pp.3947–3962, Jun 2015.

#### • Invited Paper

1. Bernard Ngabonziza, Daniel Martin, Anna Bailey, **Haehyun Cho**, and Sarah Martin. “Trustzone explained: Architectural features and use cases.” in *Proceedings of the IEEE 2nd International Conference on Collaboration and Internet Computing*, Pittsburgh, PA, Nov 2016.

#### ○ PATENTS

---

1. Jeong Hyun Yi, **Haehyun Cho**, Jiwoong Bang, and Myeongju Ji, “Application Code Analysis Apparatus and Method for Code Analysis Using the Same,” KR Patent, Patent No.: 10–1557455, Sep 2015.
2. Jeong Hyun Yi and **Haehyun Cho**, “User Terminal to Detect the Tampering of the Applications Using Core Code and Method for Tamper Detection Using The Same,” KR Patent, Patent No.: 10–1518689, Apr 2015.

#### ○ EXPERIENCE SUMMARY

---

<b>SEFCOM - Security Engineering for Future Computing</b> — Graduate Research Associate	Arizona State University, Tempe, AZ Mar 2016–Present
<b>Secure Systems Group</b> — PhD Intern	Qualcomm, San Diego, CA May 2020–Aug 2020
<b>Qualcomm Product Security Initiative (QPSI)</b> — PhD Intern	Qualcomm, San Diego, CA May 2019–Aug 2019
<b>Cyber Security Research Center</b> — Research Associate	Soongsil University, Seoul, Korea Mar 2015–Feb 2016
<b>Cyber Security Research Center</b> — Graduate Research Associate	Soongsil University, Seoul, Korea Mar 2013–Feb 2015
<b>Republic of Korea Army</b>	Feb 2007–Feb 2009

## ○ RESEARCH/PROJECT EXPERIENCE

---

### **Computers and humans Exploring Software Security (CHESS)**

Source: Defense Advanced Research Projects Agency (DARPA)

Jan 2019–Present

### **ASU–Samsung Research Membership Projects**

Source: Samsung Research

Jan 2017–Present

### **Development of Security Technology for Mobile System Software**

Source: National Research Foundation of Korea

Aug 2014–Feb 2017

### **Vulnerability Analyses and Countermeasures of Mobile Obfuscation**

Source: Samsung Electronics

Nov 2013–Sep 2014

### **Credential Management for Smart Device Apps**

Source: Supreme Prosecutors' Office of Korea

Aug 2013–Jan 2014

## ○ HONORS AND AWARDS

---

### **• The Engineering Graduate Fellowship**

by Ira A. Fulton Schools of Engineering, Arizona State University, May 2020.

### **• The CIDSE Doctoral Fellowship**

by the School of Computing, Informatics, and Decisions Systems Engineering (CIDSE), Arizona State University, Mar 2020.

### **• The Cybersecurity Fellowship**

by the School of Computing, Informatics, and Decisions Systems Engineering (CIDSE), Arizona State University, Aug 2019.

### **• Scholarship for Human Resources Development**

by Soongsil University, Seoul, Korea, Oct 2018.

### **• Academic Excellence Scholarship**

by Soongsil University, Seoul, Korea.

### **• Travel Grant**

by the 25th ACM Conference on Computer and Communications Security (CCS '18).

## ○ INVITED TALKS

---

### **• “PhD Lecture Series: Information Leaks from Systems Software and Mitigations”**

· Qualcomm Technologies, Inc., Online, Aug 2020.

### **• “Introduction and Security Concerns of Cache on ARM architecture”**

· Samsung Research, Seoul, Korea, Jun 2018.

· Soongsil University, Seoul, Korea, May 2018.

## ○ TEACHING EXPERIENCE

---

### **• Teaching Assistant**

· System Security Principles, Samsung Electronics, Jan 2015.

· Android Security, LG Electronics, Jul 2014.

- System Security Principles, Samsung Electronics, Jan 2014.
- Network Security and Practice, Samsung Electronics, Aug 2013.

## ○ SERVICE

---

- **Journal Reviewer**

- IEEE Transactions on Information Forensics & Security (TIFS)

- **External Reviewer**

- 2019 ACM Conference on Computer and Communications Security (CCS)
- 2019 ACM Conference on Data and Application Security and Privacy (CODASPY)
- 2018 ACM Conference on Computer and Communications Security (CCS)
- 2018 European Symposium on Research in Computer Security (ESORICS)
- 2017 ACM Conference on Computer and Communications Security (CCS)
- 2017 ACM Asia Conference on Computer and Communications Security (AsiaCCS)
- 2017 ACM Conference on Data and Application Security and Privacy (CODASPY)

## ○ TECHNICAL STRENGTHS

---

- |                                 |  |
|---------------------------------|--|
| • <b>Skills &amp; Tools</b>     | System Programming, Program Analysis, LLVM |
| • <b>Computer Languages</b>     | C, C++, Python, Java, Assemblies           |
| • <b>Operating Systems</b>      | Linux, OP-TEE OS, Android, Tizen, Windows  |
| • <b>Computer Architectures</b> | ARM, Intel                                 |

## ○ REFERENCES

---

### **Gail-Joon D. Ahn**

E-mail: gahn@asu.edu

Professor of Computer Science  
Fulton Entrepreneurial Professor  
Director, Center for Cybersecurity and Digital Forensics  
Director, Laboratory of Security Engineering for Future Computing (SEFCOM)  
School of Computing, Informatics and Decision Systems Engineering  
Ira A. Fulton Schools of Engineering  
Arizona State University

### **Adam Doupe**

E-mail: doupe@asu.edu

Assistant Professor of Computer Science  
Associate Director, Center for Cybersecurity and Digital Forensics  
co-Director, Laboratory of Security Engineering for Future Computing (SEFCOM)  
School of Computing, Informatics and Decision Systems Engineering  
Ira A. Fulton Schools of Engineering  
Arizona State University

### **Yan Shoshitaishvili**

E-mail: yans@asu.edu

Assistant Professor of Computer Science  
co-Director, Laboratory of Security Engineering for Future Computing (SEFCOM)  
School of Computing, Informatics and Decision Systems Engineering  
Ira A. Fulton Schools of Engineering  
Arizona State University

### **Ruoyu (Fish) Wang**

E-mail: fishw@asu.edu

Assistant Professor of Computer Science  
co-Director, Laboratory of Security Engineering for Future Computing (SEFCOM)  
School of Computing, Informatics and Decision Systems Engineering  
Ira A. Fulton Schools of Engineering  
Arizona State University

### **Tiffany Bao**

E-mail: tbao@asu.edu

Assistant Professor of Computer Science  
co-Director, Laboratory of Security Engineering for Future Computing (SEFCOM)  
School of Computing, Informatics and Decision Systems Engineering  
Ira A. Fulton Schools of Engineering  
Arizona State University