Eihal Alowaisheq, Ph.D.
Bloomington, IN, US
• eihal.ksu@gmail.com • https://www.linkedin.com/in/cybersecurity-researcher/
+1 (812) 369-3045

Experienced Cybersecurity Researcher with a track record of impactful contributions to tier 1 security conferences. Specialized in cybercrime defense, traffic analysis, web security, and internet measurement. I'm seeking an opportunity to utilize my skills in cybersecurity.

SKILLS

- Cybersecurity Research
- Cybercrime Defense
- Traffic Analysis
- Cyber Threat Intelligence (CTI)
- Open Source Intelligence (OSINT)
- Vulnerability Assessments
- Artificial Intelligence
- Natural Language Processing (NLP)
- Scientific Writing
- *Programming Languages:* Python, Shell Scripting, JavaScript, C, C++, PHP, Java, Assembly

EDUCATION

Ph.D., Doctor of Philosophy, Computer Science, Indiana University **08/2012 - 12/2020**
Dissertation: "Security Traffic Analysis Through the Lenses of: Defenders, Attackers, and Bystanders"
M.Sc., Master of Computer Science, Computer & Information Sciences, King Saud University
B.Sc., Bachelor of Computer Applications, Computer & Information Sciences, King Saud University

AWARDS:

Distinguished Paper Award at the NDSS19 for the paper: "Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Takedowns.

SELCETED PROJECTS

Assessment of cybercrime defense actions:

- Built a comprehensive methodology to analyze a large collection of OSINT, including various blacklist feeds, passive DNS data spanning six years, and historical WHOIS information
- Conducted a longitudinal analysis on the take-down process of more than 620K seized domains, identifying weaknesses in the operations.
- Demonstrated cases of seized domains that have been maliciously re-used after being released.
- Ethically hijacked a domain the FBI inadequately seized.

Presenting a stealthy domain-hijacking technique:

- Presented a DNS misconfiguration risk in domains using DNS hosting providers that leads to domain hijacking.
- performed a large-scale analysis on over 1M high-profile domains, 17 DNS hosting providers, and 12 popular public resolver operators to confirm the prevalence of this security risk.
- Discovered 628 domains that are hijackable by the proposed attack, including high-profile domains (e.g., 6 government entities and 2 payment services), 14 affected DNS hosting providers (e.g., Amazon Route 53), and 10 vulnerable public resolver operators (e.g., Cloudflare)

Utilizing NLP for semantic-analysis:

- Used NLP techniques (e.g., NLTK) and machine learning algorithms to infer fake Amazon's reviews.
- Used Twitter's API and OpenAI API to infer tweets' sentiments and identify trending impressions towards specific hashtags.

PROFESSIONAL EXPERIENCE

King Saud University KSU, Riyadh, Saudi Arabia 01/2007 - Present

Assistant Professor, Computer & Information Sciences (Remote) **03/2021 - Present**

- Research
- Direct graduate students' research

Lecturer, Computer & Information Sciences **01/2009 - 08/2012**

- Taught web application programming, operating systems, software engineering, Assembly language, and ASP.net to undergraduate students.
- Contributed as a member of the Accreditation and Intellectual Property units in the Information Technology Department
- Co-advised students' graduation projects.

Teaching Assistant, Computer & Information Sciences **08/2007- 12/2008**

- Taught web application programming, operating systems, software engineering, Assembly language, and ASP.net to undergraduate students.

Expert People, Riyadh, Saudi Arabia **09/2006 - 07/2007**
Programmer, ASP.net

- Developed web solutions for several public and educational organizations.

King Saud University KSU, Riyadh, Saudi Arabia

Teacher, Training Center **01/2005 - 05/2005**

Instructed Microsoft Access, Photoshop, Flash, and Dream Weaver to students and staff.