Hood S. Mukiibi

hudmukiibi@gmail.com || rudegentleman.github.io || +256 703 316361

Summary of Qualifications

- Over six years of experience as a security engineer, specializing in securing IT infrastructure (on-prem, hybrid and cloud), Industrial IoT systems and optimizing security operations.
- In-depth knowledge of security frameworks, protocols, and IT Service Management best practices, including ISO 27001, NIST, ITIL, Secure Development Lifecycle (DevSecOps) and CIS benchmarks.
- Strong understanding of network security, intrusion detection and prevention systems, deep packet inspection, network analysis, firewalls, VPNs, and access control systems.
- Proficient in conducting vulnerability assessments, penetration testing, and risk analysis and mapping to identify and mitigate potential security risks.
- Extensive experience in incident response and handling security incidents, including conducting forensic investigations and implementing remediation measures.
- Skilled in implementing and managing security tools and technologies, such as SIEM, DLP, antivirus, and encryption solutions.
- Excellent analytical and problem-solving abilities with a keen attention to detail.
- Strong communication skills, able to convey complex security concepts to non-technical stakeholders.

Education

2016 - 2018   Carnegie Mellon University - Pittsburgh, PA
Master of Science in Information Technology
Advisors: Prof. Bruce Krogh, Prof. Edwin Mugume

2008 - 2012   Makerere University - Kampala, Uganda
Bachelor of Science in Computer Science
Advisors: Dr. Mary Nsabagwa, Dr. John Ngubiri and Dr. Ronald Azairwe

Industry Experience

2023 - 2024   **Senior Developer II (OT/IT Security Engineer): Rohde and Schwarz - Kigali, Rwanda / Leipzig, Germany**
As a senior developer within the R&D engineering team, my responsibilities centered on investigating security vulnerabilities within IIoT systems and 5G core networks. This involved conducting thorough analysis and simulations of potential attacks on the 5G core network to assess changes in network functions. Additionally, I led the development of monitoring solutions utilizing Prometheus for log and metric scraping, coupled with Grafana for visualization. Furthermore, I spearheaded the integration of DPI tools for comprehensive network analysis, covering both user and control plane traffic.

2019 - 2023   **Lead Security Engineer: Tabiri Analytics Inc - Kigali, Rwanda**
As a lead security engineer, I was part of an exceptional team dedicated to constructing and developing an intelligent automated intrusion detection system. Our innovative approach involved harnessing the power of open source tools and integrating machine

learning concepts to effectively identify and mitigate threats and anomalies in various systems. Together, we built a cutting-edge solution that enhanced the security posture of our organization and the companies we supported.

Fall 2017   **System Architecture Intern: Inmarsat - Kigali, Rwanda**
For my graduate practicum, we designed and tested LoRaWan enabled sensors within a tea factory to supplement the tea manufacturing process to come up with desired optimal tea grades. The project focused on the fermentation process of tea where smell, image, temperature and humidity sensors were used to supplement the existing human expert knowledge.

Summer 2017   **Information Security Analyst Intern: Rwanda Revenue Authority - Kigali, Rwanda**
For my graduate internship, I worked on a project that assessed the cyber security measures implemented at this government revenue facility. Among other things, my work involved reviewing prior security audits, auditing IT business processes as well as laying a foundation for the ISO27001 certification.

2016 - 2018   **IT and Lab Support Technician: Carnegie Mellon University - Kigali, Rwanda**
I provided first level support to students, faculty and staff for all their IT requests. This among other things involved setting up and configuring all classroom technology, managing the school local web servers as well as asset management.

2015 - 2016   **Engineer EUS: MTN - Multiple Locations**
As an end user support engineer, my role encompassed providing crucial assistance for software and hardware inquiries within five operational countries (OPCOs) at MTN. This entailed promptly addressing internal client queries, resolving technical issues, and ensuring the smooth operation of the organization's network, software, and hardware peripherals. I actively participated in noteworthy projects, such as devising and implementing the internal technical process for Office365 migration across all OPCOs, virtualizing the customer contact center for all OPCOs, and automating customer queuing at customer service points throughout all OPCOs.

2013 - 2015   **Lead Service Desk Engineer: MTN - Multiple Locations**
In this role, I had the responsibility of overseeing a team of engineers who served as the primary point of contact for all IT inquiries across five operational countries (OPCOs) at MTN. Alongside various other tasks, this included proficiently handling global SLAs for reported incidents and service requests, as well as effectively monitoring and managing critical infrastructure and applications on a comprehensive scale. It is worth noting that a strong understanding of ITIL processes was essential for successfully fulfilling these responsibilities.

2009 - 2011   **Customer Service Advisor: MTN Uganda - Kampala, Uganda**
In this position, I managed the customer service helpline by responding to all customer queries. This involved collecting and analyzing customer data, queries while also communicating with them on what strategies we are taking to improve productivity and customer satisfaction.

Research Interests

Computer Security; Usable Security and Privacy; Cyber Psychology; Human Factors in Security; Social Computing; Data in Security

Teaching Experience

Spring 2021, 2022	**Teaching Assistant: Intrusion Detection Systems (04-800)**, **Carnegie Mellon University.** I provided in-class support to students, administered and graded assignments, conducted guided student labs as well as developed class quizzes. The IDS class introduced students to fascinating mathematical fields such as Probability theory, Statistics and Detection Theory which are all underlying components of intrusion detection systems (IDS).
Spring 2018, 2019	**Teaching Assistant: Wireless Networks (18-759-RW)** **Carnegie Mellon University.** I provided support to students for this course and this included administering and grading of assignments, conducting guided student labs and development of class quizzes. The class introduced students to fundamental concepts of wireless networks as well as an overview of wireless data communications standards among other advanced topics.
Fall 2018	**Teaching Assistant: Vulnerability Assessment and Penetration Testing (04-800K), Carnegie Mellon University.** I provided support to students for this course and this included administering and grading of assignments, conducting guided student labs and development of class quizzes. The course introduces students to professional penetration testing by teaching offensive security tactics, along with the appropriate methodologies and responsibilities it takes to ethically attack systems.
Fall 2017	**Teaching Assistant: Internet of Things (04-801-N), Carnegie Mellon University.** I provided support to students for this course and this included administering and grading of assignments, conducting guided student labs and development of class quizzes. In this course, students learned how to interconnect different Things to the Internet, using well-known web technologies. Students also learned how to send back information to the Things to actuate a given requirement.

Publications

2019	**Cyber Security in Africa: The boring technology story that matters** H Mukiibi (XRDS: Crossroads, The ACM Magazine for Students 26 (2), 56-59)

Technical Skills

Programming Languages

Java, Bash (Unix/Linux), Python, Matlab, SQL

Security

Cloud Security, Corporate Governance, Risk and Operational Assessment, Threat Hunting, Incident Response, User and Entity Behavioral Analysis, Network and Vulnerability Assessment, Penetration Testing, Security Information and Event Management (SIEM), Network Security (IDS/IPS), Security Assessment and Auditing, Identity and Access Management.

Data Science

Data Inference, Exploratory and Explanatory Data Analysis, Data Wrangling, Data Visualization, Feature Engineering.

Service and Mentorship

2017 - Present **Rotaractor: Rotaract Club of Kigali City (RCKC) - Kigali, Rwanda**
I am an active member of RCKC where I've recently served as social media content creator. In this club, we collaborate with other youth in the execution of humanitarian service projects as well as building efforts towards peace, friendship and reconciliation within our community.

2017 - 2020 **Mentor and Trainer - GDG Kigali Chapter - Kigali, Rwanda**
Mentoring and introducing computing and programming concepts to youth in Kigali, Rwanda. Special focus was on high school students as well as fresh graduates.

Spring 2017 **Mentor and Trainer - Women in Tech Kigali Chapter - Kigali, Rwanda**
Mentoring and introducing computing and programming concepts to youth in Kigali, Rwanda specifically young girls. The essence is to encourage young women to take on STEM subjects.