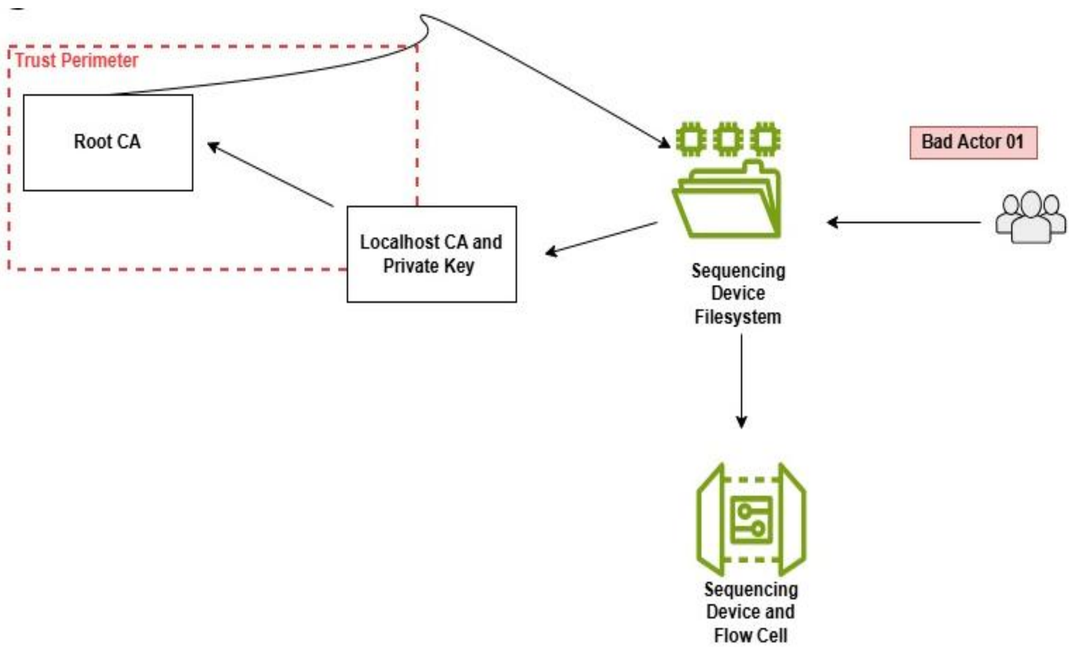
Hardware Security in the Illegal Wildlife Trade: A Secure Architecture Study Leads to Compromised Sequencing Devices and Genomic Data

Problem Statement and Goals

Metagenomics pipelines are at risk for being exploited by bad actors that undermine data integrity. Can vulnerabilities be discovered that lead to possible attacks? How are attacks prevented and how can biodiversity research data be safeguarded?



Approach

- Placed reagent in flow cell buffer mix with priming port instead of sample loading port. Flow cell loaded into sequencer where buffer reacted to reagent with electric current, oxidizing ASIC.
- Flow cell check with healthy flow cell, began sequence protocol with flow cell expired. Carried out sequencing process in 1 hour and generated report.
- Accessed report locally and discovered file system vulnerabilities leading to privilege escalation. Discovered highly sensitive data related to sequencing device.
- Power analysis conducted on flow cell and sequencing device. Combined libraries in Python used in genomic data survey.

Results

- Discovered invalid certificate authority in sequencing report file system and associated private key. Bad actors can extract the private key and alter parameters or identifiers, with the potential for Man-in-The-Middle interception.
- Malicious insiders, poachers, and organized crime mules can access intellectual property and change basecalling read accuracy, leading to results in ecosystem biodiversity interpreted as abundant when in reality are depleted. This inhibits ecosystem/population recovery and increases risk of zoonotic diseases impacting both animal and human health.
- Future work includes obtaining primary field sources and exploring parallels between physical and digital attacks. Research is currently ongoing.

- Acknowledgments – Dr. Frederic Lemieux and Professor Kathleen Moriarty
- References:
- Fayans, Iliya, Yair Motro, Lior Rokach, Yossi Oren, and Jacob Moran-Gilad. “Cyber Security Threats in the Microbial Genomics Era: Implications for Public Health.” *Euro Surveillance: Bulletin Europeen Sur Les Maladies Transmissibles = European Communicable Disease Bulletin* 25, no. 6 (2020): 1900574. https://doi.org/10.2807/1560-7917.ES.2020.25.6.1900574.

Clara Kellermann-Bryant
Georgetown University
GEORGETOWN UNIVERSITY School of Continuing Studies

Hardware Security in the Illegal Wildlife Trade: A Secure Architecture Study Leads to Compromised Sequencing Devices and Genomic Data

Abstract

Conservation Metagenomics is an emerging field that utilizes microbial deoxyribose nucleic acid (DNA) to analyze microbiome communities in wildlife populations and ecosystems. This effort includes microbial DNA analysis for biodiversity and effective decision-making relating to organism health, disease, and endangered species management. On a broad spectrum, DNA is sequenced using next-generation sequencing (NGS) and associated devices that connect to critical and network infrastructure. This study investigates the plausibility of attacks on the omics and technological aspects of the Conservation Metagenomics field using foundations in Cyberbiosecurity. The study also develops a comprehensive approach for addressing physical health information, species assessment, and pathogen identification that can produce inaccurate results leading to advantages in kinetic biological warfare.

A next-generation sequencing device and its corresponding flow cell were used as part of this study. Side channel power analysis was performed on the field-programmable gate array (FPGA) and application-specific integrated circuit (ASIC) components of the devices using the Hantek DSO2D15 oscilloscope. Next, Wireshark USB captures, FASTA files, Microbial Nucleotide BLAST, BedTools, and endangered species data from the IUCN Red List were part of the metagenomic data collection process for simulating impacts to wildlife biodiversity.

Results indicated the potential for compromise of publicly available genomic data, field data, and related devices. One attack method discovered is to use a pre-existing flow cell check while sequencing an expired flow cell and to export the sequence report connected to directories in the sequencing intranet. The combined attack enables malicious users to upload FASTA files manually that could contain altered DNA, and to perform privilege escalation to gain initial access and manipulate basecalling reads. This primary attack method undermines the integrity of data used in conservation metagenomics by altering files. Additional attacks and considerations are proposed to enhance research in this area for the future.

Clara Kellermann-Bryant
Georgetown University

GEORGETOWN UNIVERSITY
School of Continuing Studies