CYBER SECURITY ISSUES IN MODERN ROBOTICS

Dr. Tanvir Arafin

A TALE OF ENABOT

Your Smart Guardian

A TALE OF ENABOT

Our Smart Spy

SECURITY FOR ROBOTICS

- 04/22 – ROS2 Vulnerability Alias Robots
- 04/22 – JekyllBot5: Aethon TUG smart robots
- 07/21 – 17 new CVEs on ROS2: Universal Robots
- 09/20 – Vulnerabilities on UVD Robots

TODAY'S TALK

- How to attack the hardware and software stack of modern robots?
  - Software Stack
    - DoS on ROS
    - ROS2 Recon and Reflection
    - Mitigation: SROS and Beyond
  - Hardware Stack
    - Microarchitectural and Sensor Insecurities

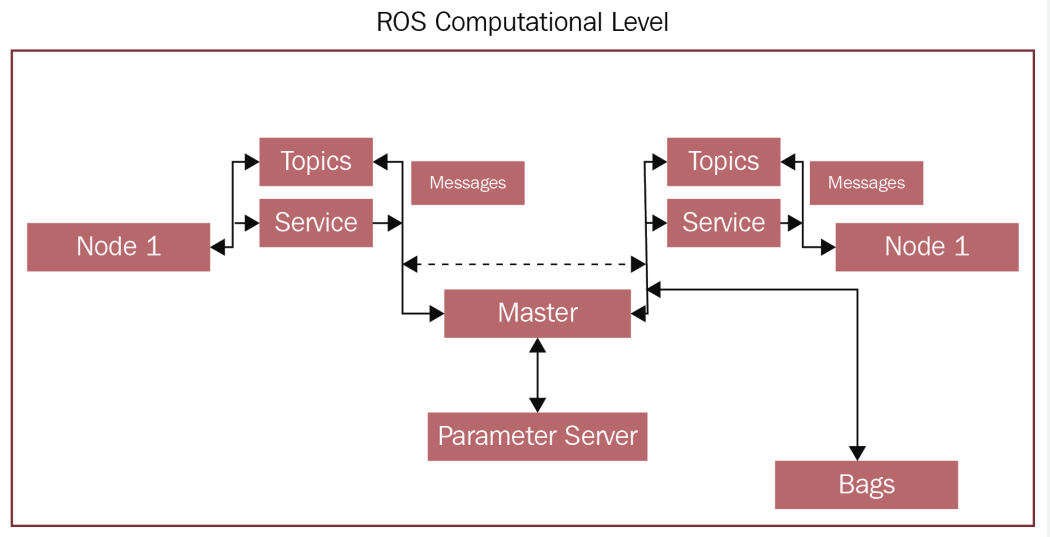
ROS

- Robot Operating System
- Not a real OS
  - Set of software framework
  - Can support heterogeneous compute nodes
- Graph architecture
  - Processing nodes
  - Message passing API
- Not real-time, see ROS2

It's estimated that by 2024, 55% of the total commercial robots will be shipping at least one ROS package

ROS COMPUTATION GRAPH

- Node
- Topics
- Service
- Parameter Server



ROS NETWORK INTERACTIONS

- Data Distribution Service: DDS
  - Middleware
  - Default communication for ROS2
  - Insecure
  - Easy to dissect and craft packages (RTPS)

ROS RECONNAISSANCE

- DDS Discovery
  - Craft discovery requests
  - Send to targets
  - Find DDS participants in the target machine

```
0000  52 54 50 53 02 01 01 10 01 10 5C 8E 2C D4 58 47  RTPS......\.,.XG
0010  FA 5A 30 D3 09 01 08 00 6E 91 76 61 09 C4 5C E5  .Z0.....n.va..\.
0020  15 05 F8 00 00 00 10 00 00 00 00 00 00 01 00 C2  ................
0030  00 00 00 00 01 00 00 00 00 03 00 00 2C 00 1C 00  ............,...
0040  17 00 00 00 44 44 53 50 65 72 66 3A 30 3A 35 38  ....DDSPerf:0:58
0050  3A 74 65 73 74 2E 6C 6F 63 61 6C 00 15 00 04 00  :test.local.....
0060  02 01 00 00 16 00 04 00 01 10 00 00 02 00 08 00  ................
0070  00 00 00 00 38 89 41 00 50 00 10 00 01 10 5C 8E  ....8.A.P.....\.
0080  2C D4 58 47 FA 5A 30 D3 00 00 01 C1 58 00 04 00  ,.XG.Z0.....X...
0090  00 00 00 00 0F 00 04 00 00 00 00 00 00 31 00 18 00  ............1...
00a0  01 00 00 00 6A 7A 00 00 00 00 00 00 00 00 00 00  ....jz..........
00b0  00 00 00 00 C0 A8 01 55 32 00 18 00 01 00 00 00  .......U2.......
00c0  6A 7A 00 00 00 00 00 00 00 00 00 00 00 00 00 00  jz..............
00d0  C0 A8 01 55 07 80 38 00 00 00 00 00 2C 00 00 00  ...U..8.....,...
00e0  00 00 00 00 00 00 00 00 00 00 00 00 1D 00 00 00  ................
00f0  74 65 73 74 2E 6C 6F 63 61 6C 2F 30 2E 39 2E 30  test.local/0.9.0
0100  2F 4C 69 6E 75 78 2F 4C 69 6E 75 78 00 00 00 00  /Linux/Linux....
0110  19 80 04 00 00 80 06 00 01 00 00 00              ............
```

DDS response from CycloneDDS

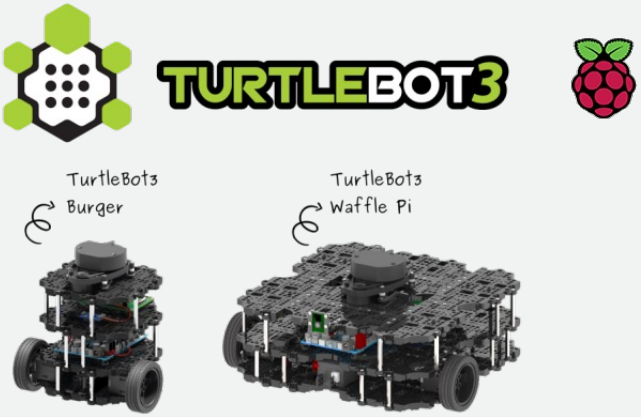
LET'S DO SOME ATTACKS

- Reflection
  - Open multicast interaction: PID_METATRAFFIC_MULTICAST_LOCATOR
  - No IP sanitization
  - Attacker injects random IP in this field and induce a ROS2 Node
  - Generate continuous traffic and overload the stack
  - CVE-2021- 38487, CVE-2021- 38425

NODE CRASHING

- Fuzzing
  - CVE-2021- 38447
    - OCI OpenDDS versions prior to 3.18.1 are vulnerable when an attacker sends a specially crafted packet to flood target devices with unwanted traffic, which may result in a denial-of-service condition.
  - CVE-2021- 38445
    - OCI OpenDDS versions prior to 3.18.1 do not handle a length parameter consistent with the actual length of the associated data, which may allow an attacker to remotely execute arbitrary code.

ROS2 TO TURTLEBOT



- DoS attack on TurtleBOT nodes
  - TB3s use security aware DDS: RTI Connext
  - Applications: Aeorspacve, medical, and military
  - CVE-2021- 38435
    - RTI Connext DDS Professional, Connext 2* DDS Secure Versions 4.2x to 6.1.0, and Connext DDS Micro Versions 3.0.0 and later do not correctly calculate the size when allocating the buffer, which may result in a buffer overflow
    - Segmentation fault BY malformed RTPS packet
    - Trigger remotely over the network

SECURING ROS: SROS

- A set of security enhancements for ROS
- Three levels of concepts
  - Transport Security level → Secure Communication
  - Access Control level → Trusted Access
  - Process Profile level → Application Security

SROS: TRANSPORT LAYER

- TLS to protect all ROS related traffic.
- Use TLS by shimming its way between the network stack and the ROS client library.
- SROS wrap all socket level ROS communication via TLS
- Malicious actors can not redirect or replay network traffic, nor could they modify or spoof messages via man-in-the-middle attacks.

SROS: PROCESS PROFILE LAYER

- AppArmor ("Application Armor")
  - A Linux kernel security module that allows the system administrator to restrict programs' capabilities with per-program profiles.
  - Ssecurity policies completely define what system resources individual applications can access, and with what privileges.
  - Malicious or dysfunctional nodes can be restricted
  - Safeguard robotic subsystems from unexpected behavior or bad actor exploits

OPPORTUNITIES

- Hack it like the ‘90s
  - ROSChaos – Pentesting
  - RoboSpolit
  - ISF (Industrial Control System Exploitation Framework)
- Weak and Security-oblivious Implementation
- Life-cycle management
- Security fundamentals are preached but rarely practiced

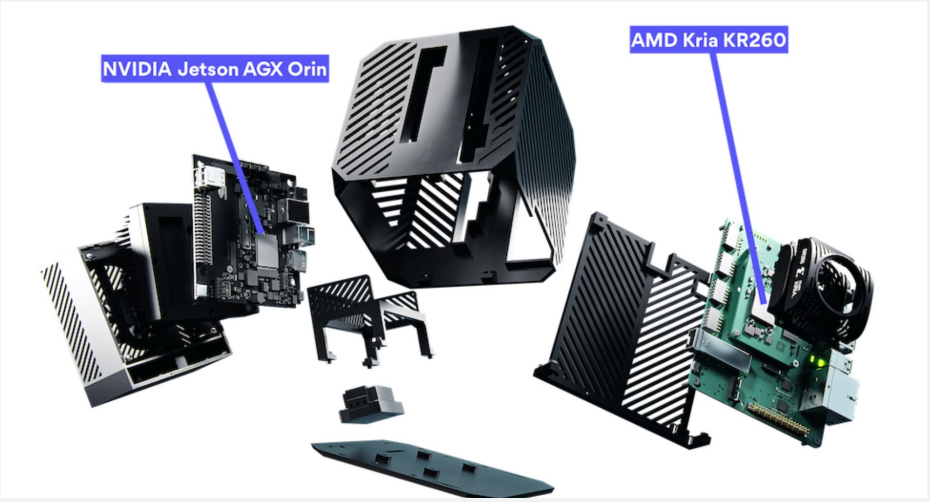
HARDWARE SECURITY IN ROBOTICS

- Embedded Systems Security
  - Processor
  - Sensors/ Actuators
  - I/O

OUR CURRENT WORKS

- Side channel and fault injection in robotic SoC
- Security flaws in NVDLA
- Secure sensor integration using split learning

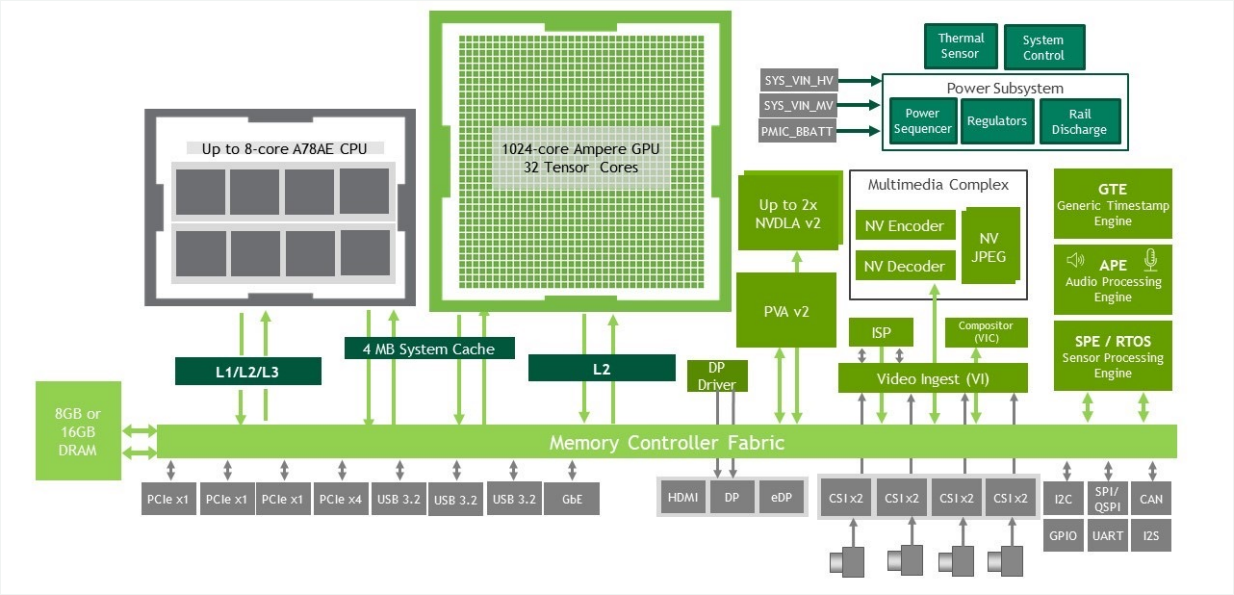
HARDWARE ACCELERATION



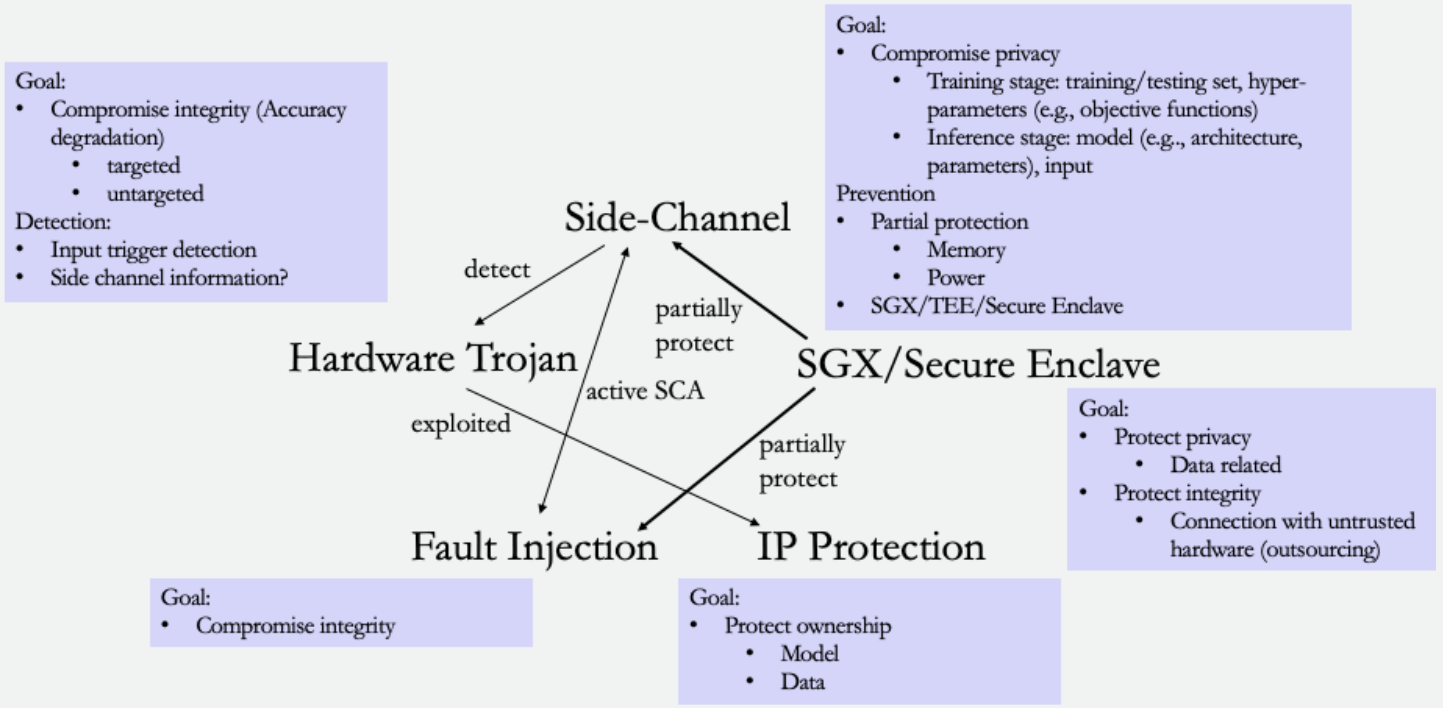
ROBOT CORE

JETSON ORIN

- "The ideal solution for a new age of robotics"



HARDWARE SECURITY OF THE AI MODELS



Xu, Qian, Md Tanvir Arafin, and Gang Qu. "Security of neural networks from hardware perspective: A survey and beyond." *Proceedings of the 26th Asia and South Pacific Design Automation Conference*. 2021.

ATTACK ON SENSOR FUSION[5]

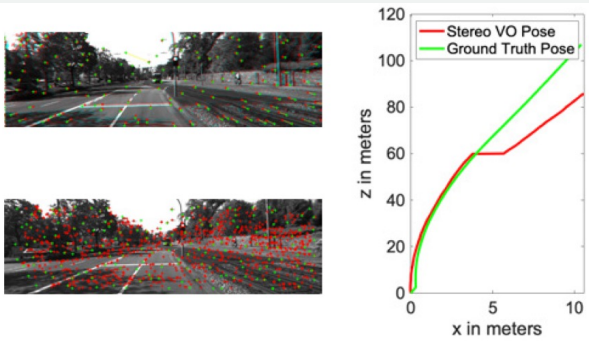


Fig. Example of replay attack on stereo visual odometry. Stereo-visual experiments are performed using SOFT algorithm and code presented in [16], [17] Flow matching (Left top) and feature selection(left bottom) for stereo-visual odometry on KITTI data-set [14]. The right figure demonstrates a replay attack on the camera inputs that affects the stereo visual odometry. The left figure has spoofed data on both of the stereo sensors for 20 frames, which results in the large deviation of the stereo odometry pose (red line) from the ground truth (green line).

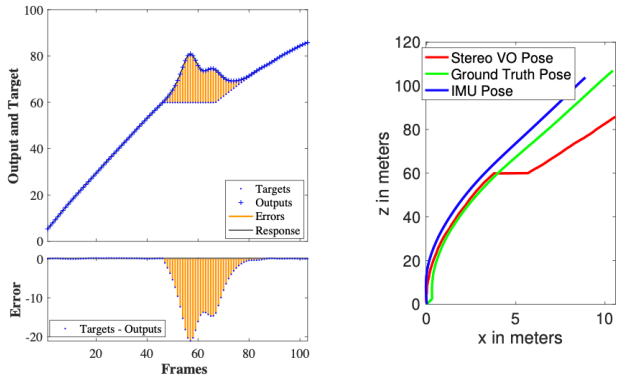
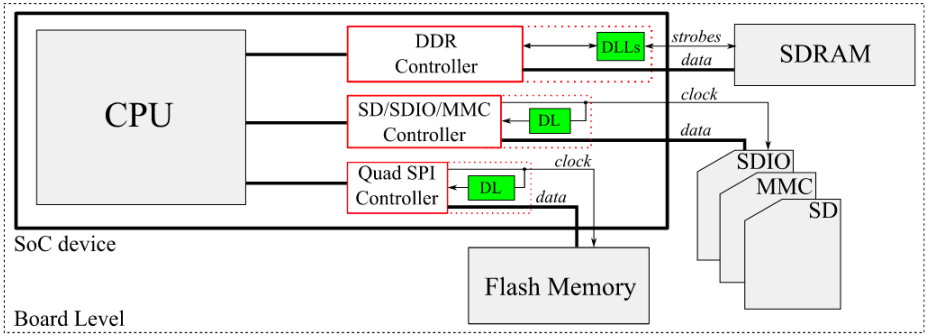


Fig. Example of replay attack detection. Using the IMU data, the closed loop network predicts the VO pose, and updates itself based on the VO pose. The VO measurements has the frequency of 10Hz. Thus, the x-axis in the left figure represents a window of 10 seconds.

Arafin, Md Tanvir, and Kevin Kornegay. "Attack Detection and Countermeasures for Autonomous Navigation." *2021 55th Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2021.

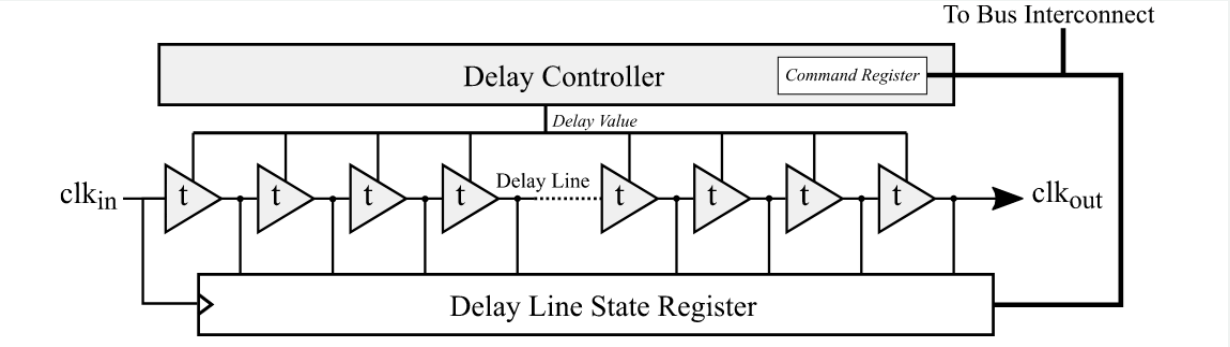
POWER SIDE-CHANNEL VIA MEMORY SYNCHRONIZATION[6]

- Typical SoC connectivity with external memories.
- Delay-lines are implemented to synchronize clock and data signals arrival in the memory controllers

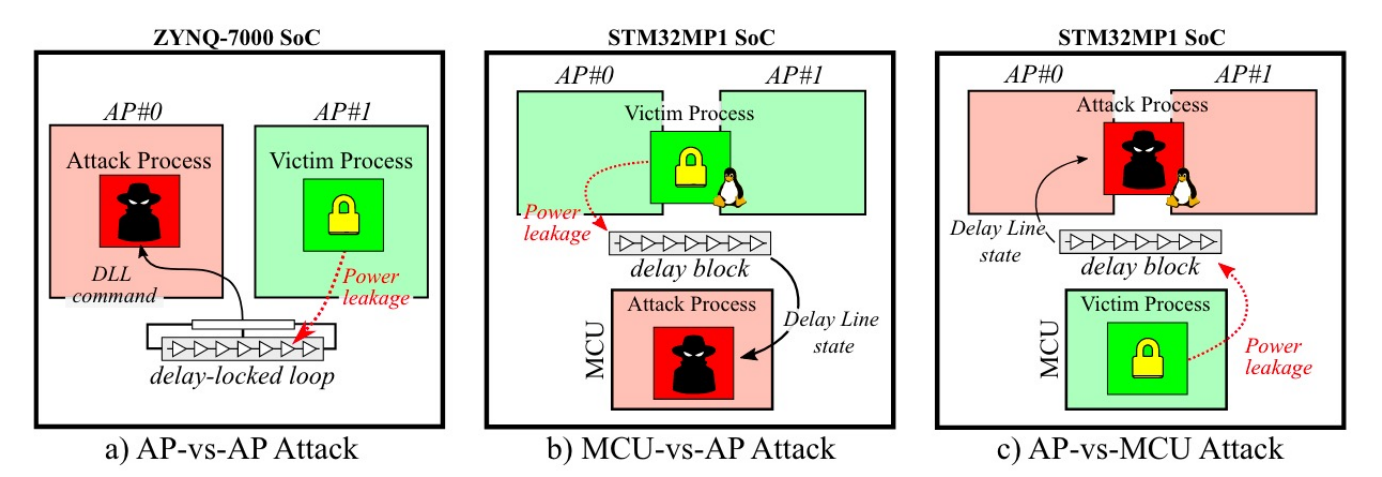


DELAY CONTROLLER[6]

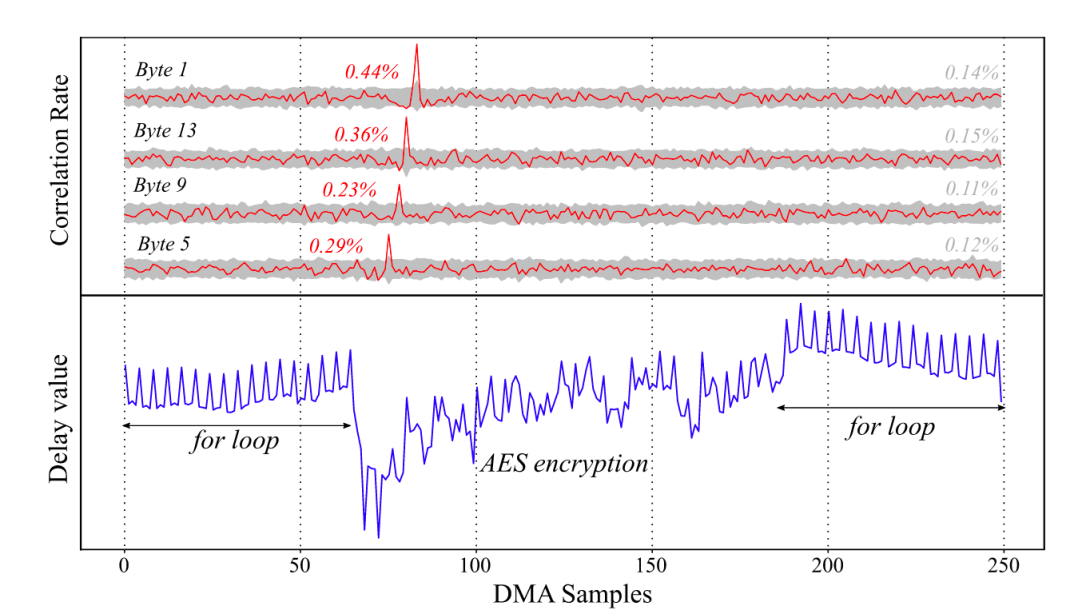
The delay-line is calibrated to provide a phase shift to a clk signal using both coarse and fine delay elements



USING DELAY LINES FOR POWER ANALYSIS[6]



POWER SIDE CHANNEL[6]



CONCLUSIONS

- Hardware and Software Security for Robotics is imperative
- Software security issues plagues current gen robots
- Hardware security issues presents more attack surfaces
- Poor lifecycle management for legacy HW and SW
- The time is NOW for Robot Cybersecurity

REFERENCES

- [1]https://www.usenix.org/system/files/conference/atc12/atc12-final39.pdf
- [2] https://cybersecurityrobotics.net/resources/
- [3] http://wiki.ros.org/SROS/Tutorials/AppArmorAndROS
- [4] http://wiki.ros.org/SROS/Tutorials#Access_Control
- [5] https://accelerationrobotics.com/robotcore.php
- [6] Gravellier, Joseph, et al. "Sideline: How delay-lines (may) leak secrets from your soc." *Constructive Side-Channel Analysis and Secure Design: 12th International Workshop, COSADE 2021, Lugano, Switzerland, October 25–27, 2021, Proceedings 12*. Springer International Publishing, 2021.
- [7] Arafin, Md Tanvir, and Kevin Kornegay. "Attack Detection and Countermeasures for Autonomous Navigation." *2021 55th Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2021.