Birdf meeting- task 7

Jan 24 2022

Ron Insler – Rad Data Communication

Task 7: Malware Threats Mitigation

Your Network's Edge®

Sub-task: **Edge Critical Network Functions**

- Protection of electric substations and remote locations

Problems addressed

- Legacy SCADA protocols are unsafe and require add-on security
- Existing SCADA devices are computationally limited and rarely patched

Research directions

- Edge computation in demarcation devices alongside centralized intelligence
- Collect and aggregate statistics, detect and block attacks remotely
- Secure synchronization distribution for synchrophasors

Cooperate

- with Arava Power and Delek on requirements and use cases
- with GIT and ASU on network statistics needed for malware detection
- with Nexant and SIGA on disaggregating cyber functionality
- with ASU sync security for synchrophasors, teleprotection, distributed generation

Impacts

- Cost effective threat mitigation
- Content agnostic attack detection
- Securing synchronization

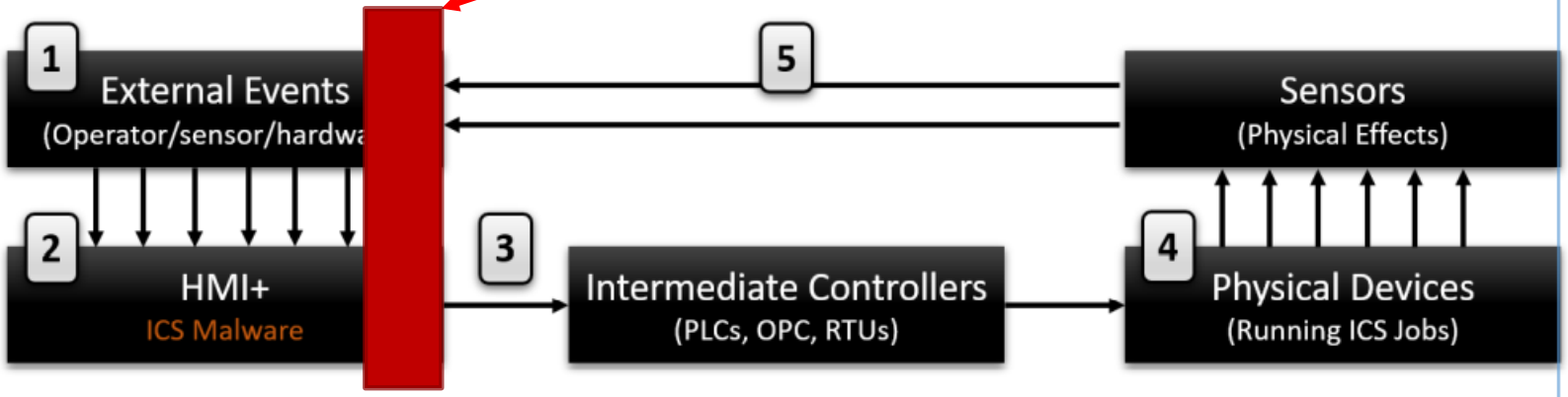
SCADA: Supervisory Control And Data Acquisition, NF: Network Function, MiCLK: Link, GIT: Georgia Institute of Technology, ASU: Arizona State University

RAD IOT GW

Will monitor all data send or received by HMI

Protocols like
Modbus
DNP3
IEC104

physical behaviors which are unique and essential to ICS malware attack operation.



Data point 1 *are external event inputs that induce activity in HMI host.*
Point 2 *are system behaviors in HMI host*
Point 3 *is traffic from the HMI.*
Point 4 *are properties of the physical world.*
Point 5 *are observed effects from the physical world.*

Past methods: Categorized into host and network anomaly detection techniques

Task 7 current activities in progress until end of 2022

- Definition of the information to be collected by RAD's GW
  - Scada related information – protocol information such as Modbus , DNP3 , IEC104 , data packets paring and sequencing (time stamp)
  - Network related Information : Jitter , delay , loss , rate (time serious)
  - Synchronization related information
    - PTP packet related information [rate and timestamp, sequence, content]
    - GPS related information [SNR , Elevation and altitude and more]
- Research of what info needs to be locally process and what needs to be send for further analysis in the central analytic process.
- Definition of API's to send the info to GIT system
- Implementation of SW on RAD's GW.

Task 7 Commercialization and Collaboration

Your Network's Edge®

- Commercialization
  - RAD is deployed with it's IOT GW at utilities like Exelon EVN CPC and much more. We are going to add Task 7 features to enhance the security of the overall solution by SW upgrade.
- Collaboration
  - We are going to collaborate with Delek US , GIT and possible ARAVA power both for testing the overall solution and real deployment as well as selling overall solution RAD GW/ GIT malware detection system.

RAD

Your Network's Edge®

Thank you

For your attention