NSF SATC: TTP: Small:
Tracking Run-time Anomalies in Code Execution (TRACE)

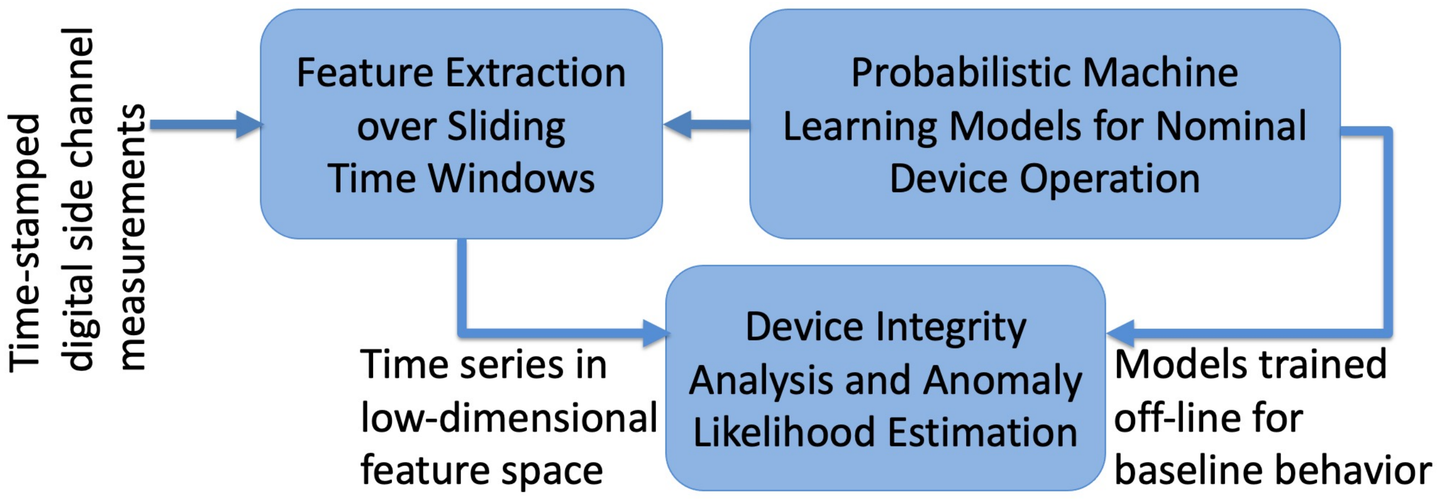
F. Khorrami (Lead PI), R. Karri (Co-PI), P. Krishnamurthy (Senior Person)
Department of Electrical and Computer Engineering
NYU Tandon School of Engineering, Brooklyn, NY 11201
https://www.nsf.gov/awardsearch/showAward?AWD_ID=2039615

Challenge

- Robust cybersecurity is crucial in interconnected embedded devices in cyber-physical systems (CPS); in particular, power grid devices. Rootkits and other malware as well as firmware modifications, configuration changes, and unauthorized code injection can cause significant impacts to the CPS.
- In-field integrity verification and anomaly detection for fielded devices is a crucial capability.

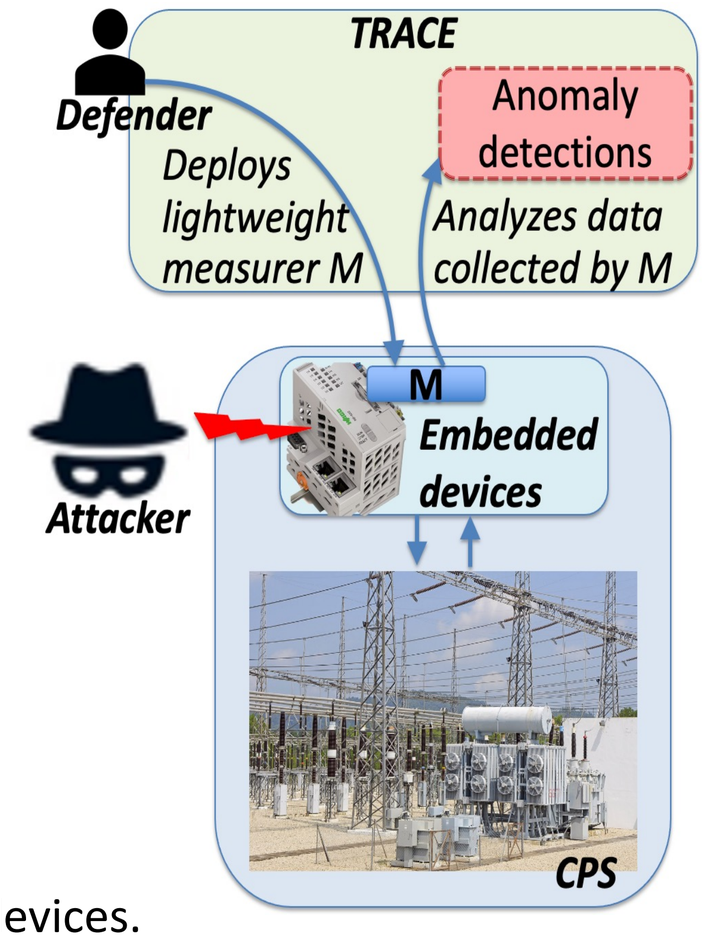
Solution

- TRACE: automated, lightweight, multi-modal measurers deployed to target devices + off-device device integrity analysis + machine learning based threat detection.
- TRACE detects anomalies (e.g., rootkits) using multi-modal on-device measurements – time series readings of device activity (e.g., Hardware Performance Counters, stack traces), memory-based measurements, kernel measurements (e.g., system calls, kernel rootkit effects detectors). Baseline-relative and baseline-independent anomaly detection.
- Time-domain and frequency-domain feature extraction over sliding time windows; feature-based probabilistic classification and anomaly likelihood estimation using machine learning models and dynamic event sequence analysis.



Scientific Impact

- TRACE mitigates security threats in embedded CPS devices by enabling on-demand/continuous integrity verification of embedded CPS devices, focusing on power grid devices (e.g., substation automation controllers). TRACE is scalable to a wide range of device architectures and measurement modalities.
- TRACE enables in-field anomaly detection leveraging temporal behavior and code structure characteristics of CPS devices; complements general computer/network security methods.



Broader Impact and Broader Participation

- Near-zero-cost solution for malware detection/characterization in CPS devices.
- TRACE TTP builds on NYU's work in DARPA RADICS and will expand operating envelope, increase automation, reduce deployment friction, and license/commercialize TRACE.
- Organized panel on power-grid security (https://www.youtube.com/watch?v=QgSR6X4jyrY, https://www.eventbrite.com/e/power-grid-cyber-security-challenges-opportunities-webinar-tickets-164876029643); panelists: Farshad Khorrami (NYU), Chris Murphy (CISO, National Grid), Joe Cummings (Cybersecurity Program Lead, New York Power Authority – NYPA), Ashif Muhammad (Siemens), Mikhail Falkovich (CISO, Con Edison), Michael Locasto (CTO, Narf). Moderators: Yury Dvorkin (NYU), Frank Vallese (NYU).
- Utilization in system being deployed to NYPA's AGILe platform as part of new effort (DOE: https://www.energy.gov/articles/doe-announces-12-million-enhance-cybersecurity-americas-energy-systems) on integrated cross-domain integrity monitoring and anomaly detection/localization in power grid CPS.