Developing intrinsic security in Cyber-physical Systems by leveraging precise clock synchronization

Dhananjay Anand, Cyber Infrastructure Group

National Institute of Standards and Technology

Paper Summary:

Improving security for data networks is listed as a priority in research directives spanning health information networks to industrial control networks. Networks of the future are purportedly more vulnerable given their eventual evolution to large, amorphous, cyber-physical systems (CPSs).

The focus of our research is to leverage a precisely synchronized network of clocks embedded within a CPS to design implicit security features. We intend to demonstrate that the mature area of networked clock synchronization, in which there has been significant development in recent years, offers several insights that can be used to identify network intrusion, adversarial attacks and unauthorized reconfiguration. Our premise is that while network topology, data content and size may change unpredictably in a CPS, the use of precise clocks to profile the physics of individual nodes and to accurately model the relative timing differences between nodes offers a unique structure-semantic oracle for node authentication and link validation.

The outcome of the research will be a set of algorithms specifically designed to secure a CPS used to control a regional natural gas supply, processing and distribution network.

Background and Motivation:

Current networks used for cyber-physical systems face a new class of threats, intent on the breaching its availability, confidentiality and integrity. This class of threat has been given the moniker "Advanced Persistent Threat" (APT). To date, most organizations have relied on the technologies implemented to mitigate risks associated with automated viruses and worms, which do not sufficiently address focused, manually operated APT intrusions. Conventional incident response methods fail to mitigate the risk posed by APTs because they make two flawed assumptions: response should happen after the point of compromise, and the compromise was the result of a fixable flaw [*"Computer Security Incident Handling Guide" NIST report, March 2008*].

More recently, cybersecurity researchers propose using an intelligence-driven approach to study intrusions. Security is mapped to a "kill-chain" of discrete stages through which an adversary must progress successfully before it can achieve its desired objective. Each discrete phase of the intrusion is mapped to courses of action for detection, mitigation and response ["Joint Publication 3-13 Information Operations" U.S. DoD report, Feb. 2006.]. Just one successful counteraction along the chain disrupts the chain and the adversary. While most of the research in the area applies to corporate and government information networks, APTs are also prevalent in networks used to control widely distributed critical infrastructure such as the power network or, in our case, a network of natural gas pipelines and processing plants. To this effect, a report from the President's Council of Advisors on Science and Technology [Dec. 2010] on R&D requirements for Networking and IT specifically observes the need for improved robustness, security and interoperability in real-time industrial control networks for critical infrastructure.

Proposed research:

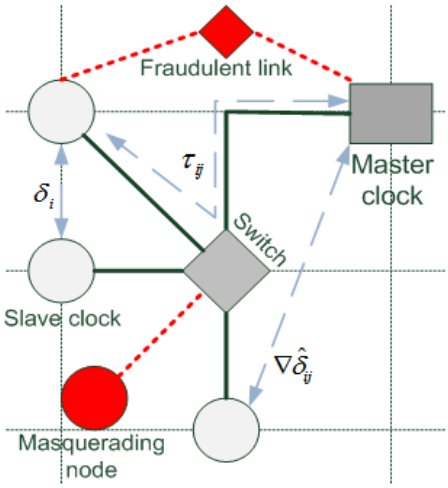

Figure 1: Chronometric representation of four network synchronized nodes.

We propose methods to detect and avert APTs to CPSs early in their kill-chain by 1) identifying masquerading nodes 2) detecting network path changes and 3) cross-verifying dynamics of individual physical processes. We aim to achieve these functions by leveraging the inherent precise synchronization of clocks in a control network. We have worked extensively in developing and evaluating clock synchronization algorithms such as the IEEE-1588 Precision Time Protocol, which is now the standard clock synchronization protocol used in high performance industrial control networks such as EtherCAT and CIPMotion.

The clock resolution awarded by IEEE-1588 allows very precise estimation (in the order of microseconds) of network path delay (τ), relative clock offsets between nodes (δ) and the trajectory of clock convergence ($\nabla\hat{\delta}$). As illustrated in Figure 1, a fraudulent link, where network communications are intercepted and rerouted, is detected by observing changes in the transit time for link τ_{ij}. The relative clock offsets δ_i provide a rich source of data about the drift and convergence characteristics of time keeping clocks on each node in the network. Clock characteristics form a unique fingerprint for each node based on its hardware configuration and processing workload. Currently, a feature classifier has been developed to authenticate legitimate nodes and to automatically classify masquerading nodes based on differences in the clock convergence trajectory $\nabla\hat{\delta}_{ij}$ and clock offsets δ_i. Lastly, in a CPS it is also necessary to automatically verify that physical components in the network have not been compromised. We intend to develop a decentralized system identification algorithm to uniquely identify the physical dynamics of each node in the network based on node-to-node measurements of dynamic response. These identified models are encoded into a hash function, which is unknown to the adversary. Since an adversary cannot reconstruct the hash with knowledge about the dynamics of individual nodes, the hash function serves to verify the integrity of the CPS as a whole. In the case of the natural gas supply system, parameters associated with the fluid dynamics of the distribution network may be hashed using precise time stamped measurements to verify that distribution conduits (pipelines) are intact.

Potential impact on CPS:

Our proposal addresses one of the key roadblocks (verification of integrity) listed in the NIST report on "Strategic R&D opportunities for 21st century CPS" [Jan. 2013]. CPSs are intended to be modular and scalable, but current methods of propagating 'trust' between nodes and verifying system level integrity do not meet those CPS principles. Research is needed to develop trust metrics and security tools that are perpetually modular. It is our thesis that the notion of time is well suited as a trust metric as it plays a critical role in the union of cyber and physical components and is an inviolate constant that may be used in multiple CPS application domains as a metaphor for integrity.