Detection/Interdiction of Malware Carried by Application-Layer AMI Protocols

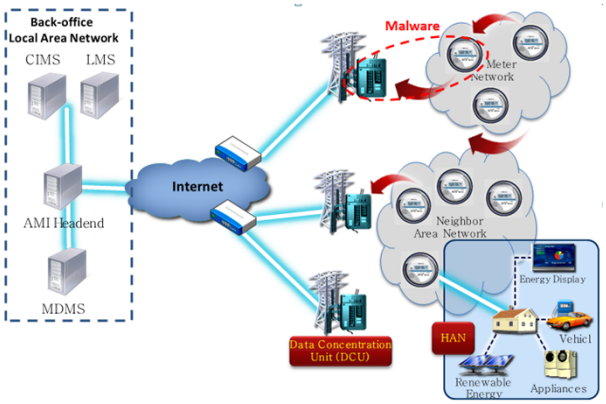
David M. Nicol and Huaiyu Zhu

GOALS

- Develop policy engine to provide a general framework for executing rules that stop suspect traffic.
- Develop policy rules and algorithms to identify malicious traffic.
- Evaluate the effectiveness of the policy engine.
- Evaluate the performance impact on building the policy engine in AMI applications.

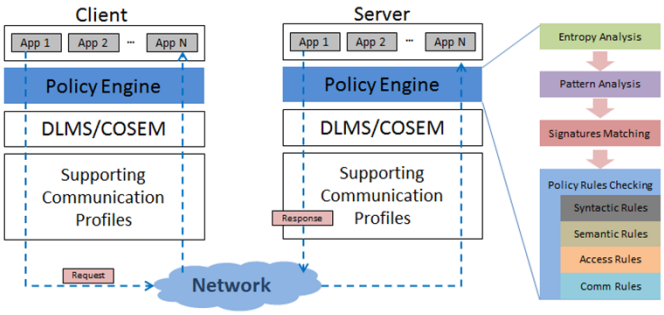
FUNDAMENTAL QUESTIONS/CHALLENGES

- Malware can disrupt the operation of services in advanced metering infrastructure (AMI).
- Malware is hidden within the data payloads of legitimate control traffic.
- The attacker might encrypt, compress, or permute bytes to avoid detection.
- Challenge 1: How do we develop the policy engine with high effectiveness and low error rates?
- Challenge 2: How do we design and implement the policy engine with minimal performance overhead?



RESEARCH PLAN

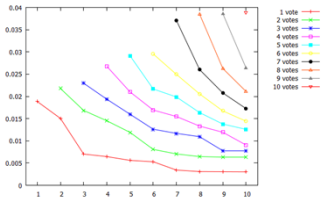
- Develop a general framework for executing policy rules.
- Develop effective policy rules; implement within the framework.
- Evaluate effectiveness in terms of false positive and false negative errors.
- Conduct performance analysis that evaluates the impact the policy engine has on the throughput and latency of protocol messages.
- Bring the framework into a suitable state for open-source release.



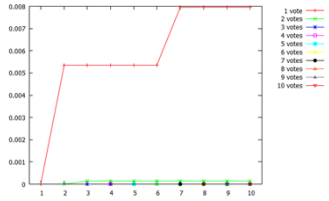
RESEARCH RESULTS

- Integrated a prototype policy engine with an open-source implementation of DLMS/COSEM.
- Designed policy rules tuned to DLMS/COSEM protocol and detection of ARM executables.
- The experimental results show that the prototype policy engine is effective with low error rates.
- Only 0.265% performance overhead is introduced.

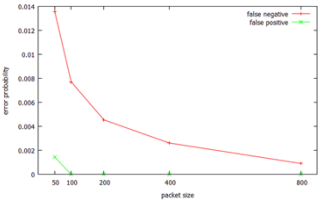
False Negative



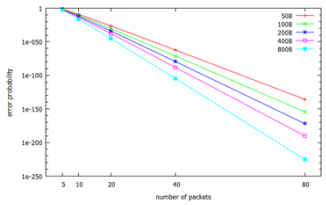
False Positive



Packet Size Sensitivity



Packet Number Sensitivity



BROADER IMPACT

- Provides a open-source framework for malware detection.
- Provides a general method for developing effective rules for policy engine.
- Provides experiment designs to evaluate such a host-based malware detection system.
- Reduces the resource requirement for deploying the policy engine.

INTERACTION WITH OTHER PROJECTS

- This host-based malware detection technology can be combined with other hardware-based or software-based intrusion detection systems (TCIPG) to detect and stop cyber attacks in AMI systems.

FUTURE EFFORTS

- Extend policy engine with C12.22 protocols.
- Extend signature set for x86 executables.
- Implement policy engine with C12.22 application.
- Evaluate performance of policy engine running on embedded systems.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T