SHARKS: Smart Hacks, Attacks, RisKs and Security in IoT based on Machine Learning

Tanujay Saha, Najwa Aaraj, Niraj K. Jha

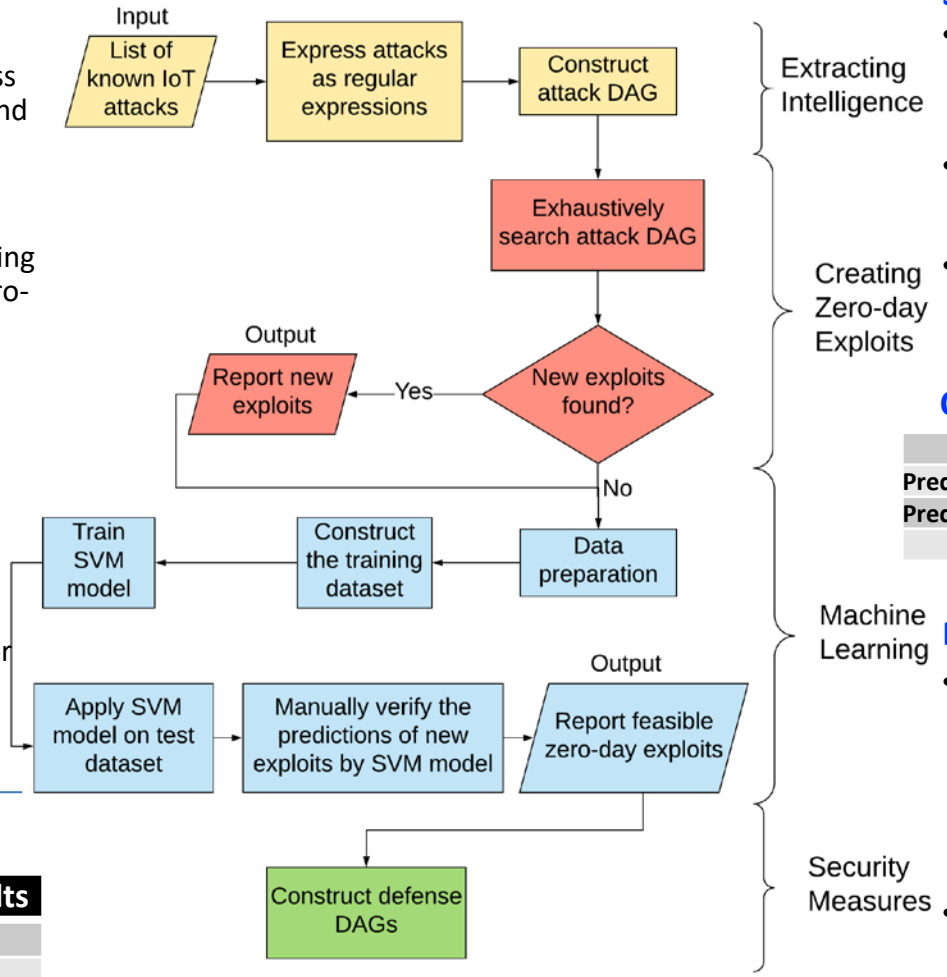
Challenges:

- Automatic generation of novel attack vectors across the hardware, software and network stack of an IoT system.
- Optimized defense mechanisms against existing attacks and generated zero-day exploits.

Solution:

Flowchart depicts the overall approach of our method.

Defense mechanism involves categorizing a resource into *Top Secret*, *Secret*, *Restricted* or *Unclassified*.



Results:

Dimension	Results
Zero-day exploits	128
Total Attacks	169
Training Accuracy	97.14%
Test Accuracy	97.4%
Reduction in manual checks	87.5%

Grant number: CNS-1617628
Institution: Princeton University
Contact: tsaha@princeton.edu

Scientific Impact / Novelty:

- Using machine learning at the system level: ***Makes this approach applicable to all apps and platforms.***
- Exploration of attacks at the intersection of hardware, software, and network stacks.
- Defense mechanisms of optimum cost.

Confusion Matrix:

N = 1192	Actual=No	Actual=Yes	
Predicted=No	1043	0	1043
Predicted=Yes	31	118	149
	1074	118	

Broader Impact:

- SHARKS provides a unified and generalized vulnerability detection framework, unlike the current state-of-the-art frameworks that are application- and platform-specific.
- Any organization with source code of an IoT application can use it.
- Opens up new directions of automated attack generation in cybersecurity.