APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

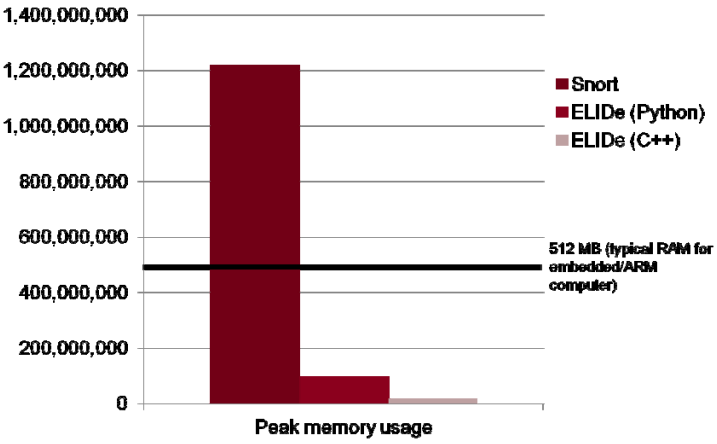
Extremely Lightweight Intrusion Detection (ELIDe)

S&T Campaign: Information Sciences
Cybersecurity

Rich Harang, (301) 394-2444
richard.e.harang.civ@mail.mil

Research Objective

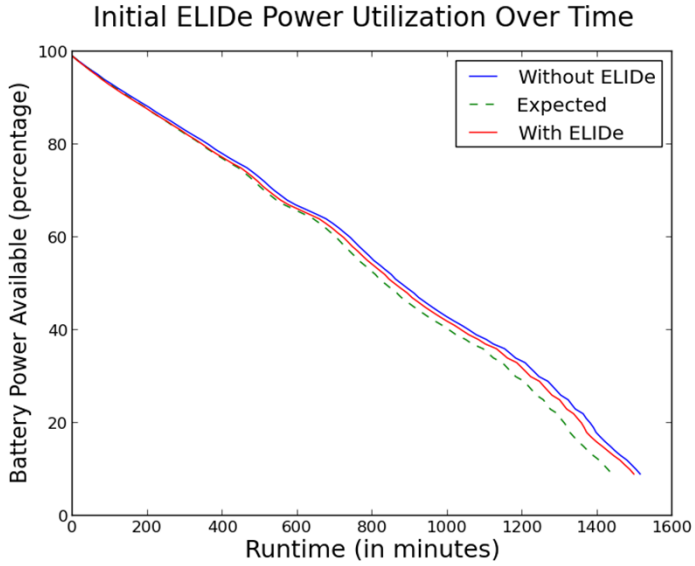
- **Perform real-time signature-based intrusion detection on extremely resource-constrained devices such as mobile phones**



Use of hash kernels to produce a linear n-gram based classifier results in ~1000x decrease in RAM requirements

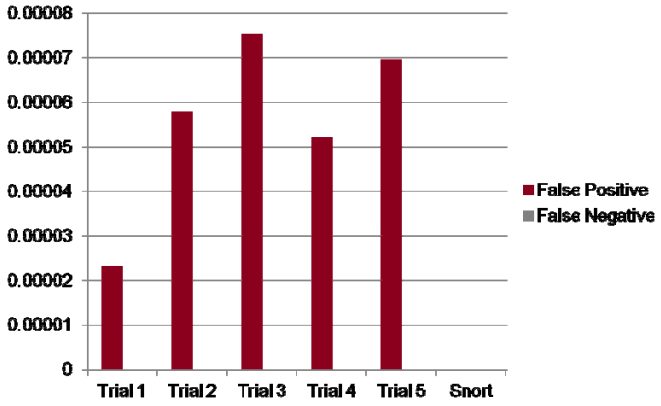
Challenges

- **Wide range of signatures make exact matching infeasible; no clear link between signature set size and classification accuracy**
- **Long training times**
- **Classification is very sensitive to hyperparameter settings, theoretical methods for setting them needed**



ARL Facilities and Capabilities Available to Support Collaborative Research

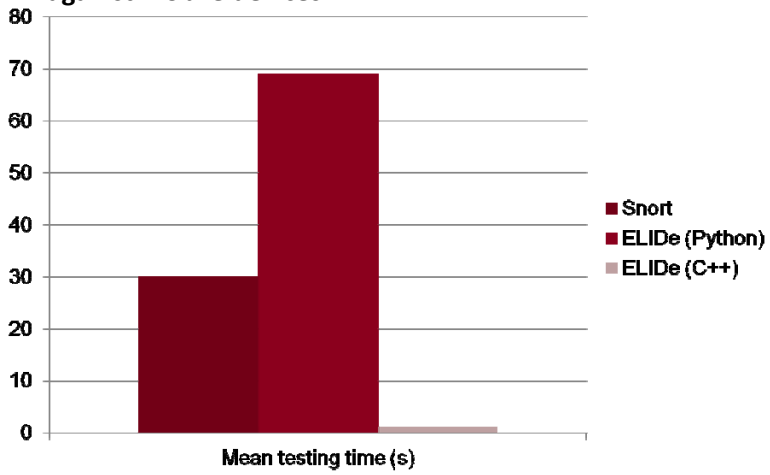
- **ARL Cyber Lab**
- **Network Science Research Lab (Q3 FY15)**
- **DOD HPC supercomputing resource center**
- Chang, Raymond J., Richard E. Harang, and Garrett S. Payer. Extremely Lightweight Intrusion Detection (ELIDe). 2013.
- **Patent application 14052153;** "Method and apparatus for performing intrusion detection with reduced computing resources"



Error rates across five-fold cross-validation (using Snort classification as a baseline)

Complimentary Expertise/ Facilities/ Capabilities Sought in Collaboration

- **Mobile network simulation capabilities for further testing**
- **Cryptographic expertise for assessment of obfuscation properties**
- **Sources of packet-level data featuring active attacks against mobile devices**



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED