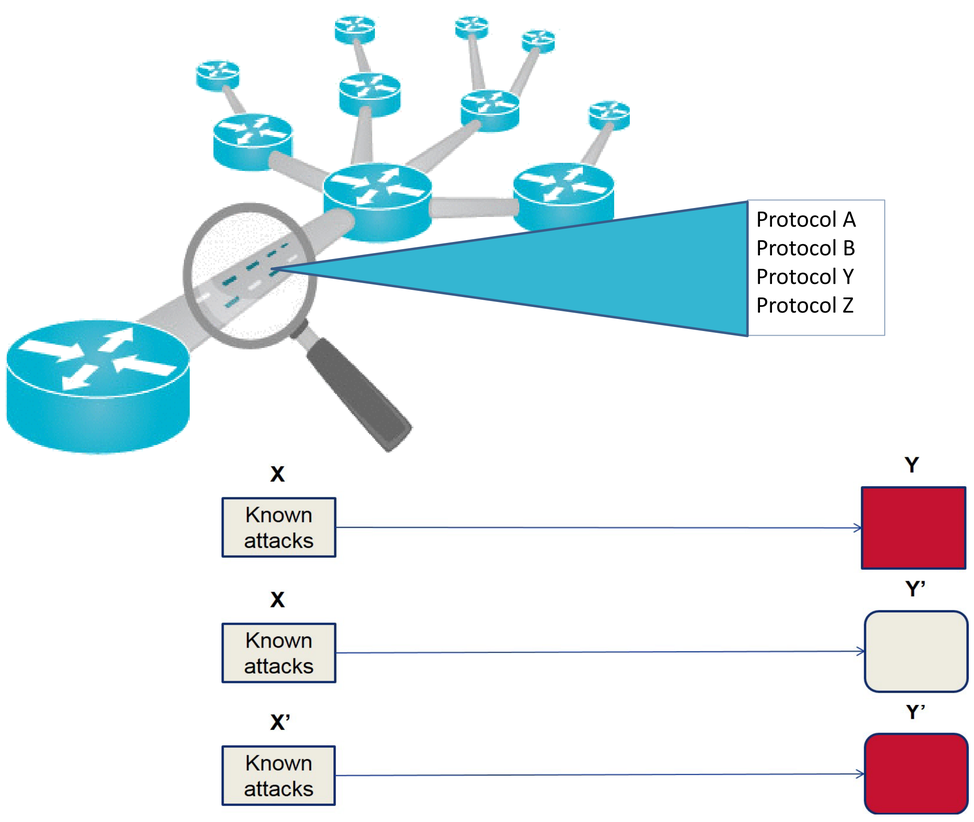
Traffic Based Model Generation

S&T Campaign: Assessment and Analysis
Developing Tools, Techniques, and Methodologies
Cyber SLV

Jaime C. Acosta, Ph.D.
(575) 678-8115, jaime.c.acosta.civ@mail.mil
Caesar Zapata
(575) 678-5764, caesar.zapata.civ@mail.mil

Objectives

- Develop a tool that will automate the generation of network protocol models that can be used to support the analysis of systems that use these protocols.
- Enable further analysis of network protocols within stringent time constraints by automatically generating client software capable of communicating with them.



Analysts target protocols of interest and evaluate their survivability against a set, *x*, of known attacks. Variations in the effectiveness of such attacks have been observed across assessments. Often, these can be attributed to modifications within the target protocols.

Challenges

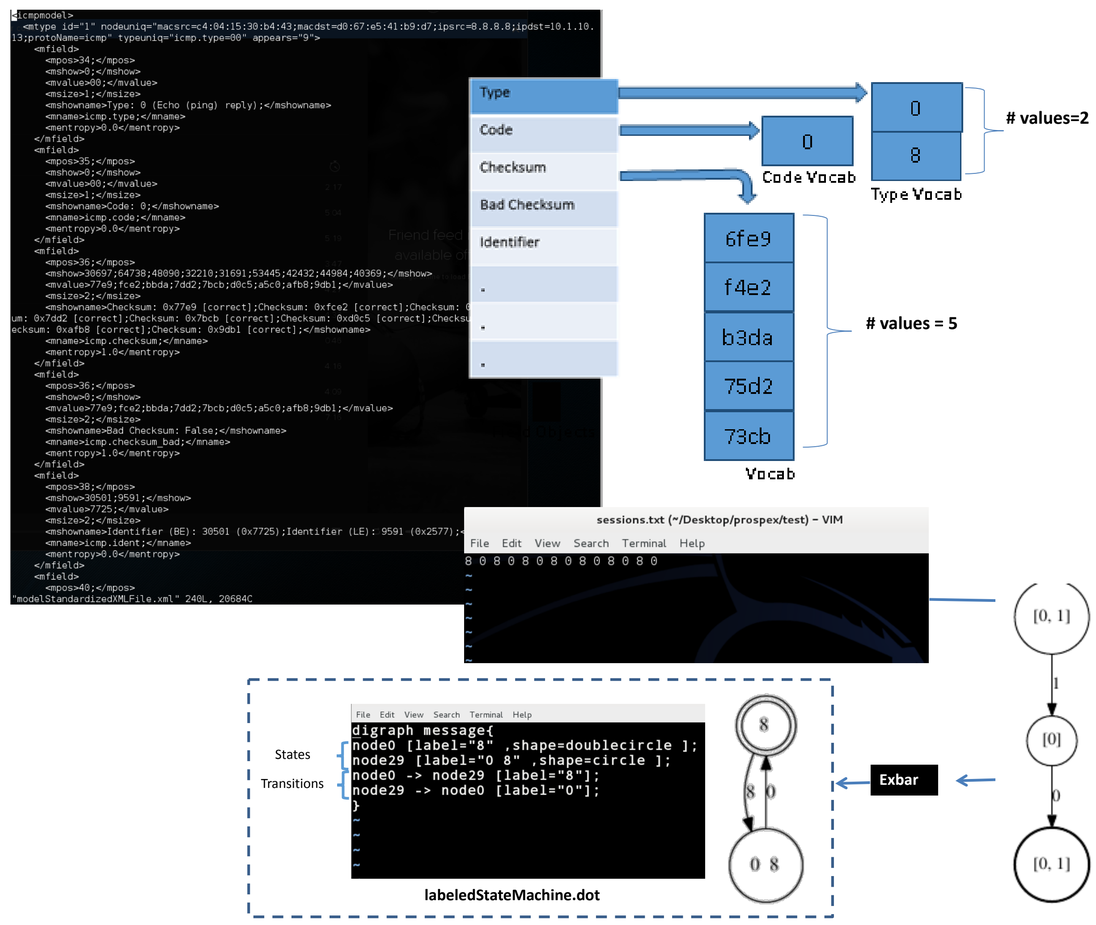
- Determining message types and packet format.
- Extracting protocol behavior.
- Automating the process of translating protocol behavior to model and simulation code.

Approach

- Leverage a dictionary of known message types and Wireshark's dissector library.
- Utilize Prospex's (Protocol Specification Extraction tool) inference module to extract network protocol state machine.
- Generate ns-3 protocol models and simulations based on network captures.
- Develop a pluggable software framework that enables analysts to generate code for multiple platforms.

Progress

- Extracted protocol specific data (e.g., fields, field properties, message type, packet format, etc.) and the state machine for the ICMP protocol successfully from a network traffic capture.
- Leveraged the extracted protocol behavior to automatically generate an ns3 (Network Simulator Engine) model.
- Incorporated the automatic generation of Scapy models utilizing the extracted protocol specification data.



Vocabulary extraction and state machine generation.

Limitations

- Manual intervention is still required when selecting the vocabulary to use for fields exhibiting high entropy.
- Input files must be filtered to contain only one communication stream.
- Fixed length fields are assumed.

Sought Collaboration

- Develop a flexible architecture that allows cross platform inter and intra packet algorithm development e.g., checksum and sequence numbers
- Test the model's ability to establish a connection and communicate with real network protocols.