SAND2022-9579D

The Center for Cyber Defenders

Expanding computer security knowledge

ICS Telnet Extraction

Extracting ICS Config Data from Network Traffic for Anomaly Detection

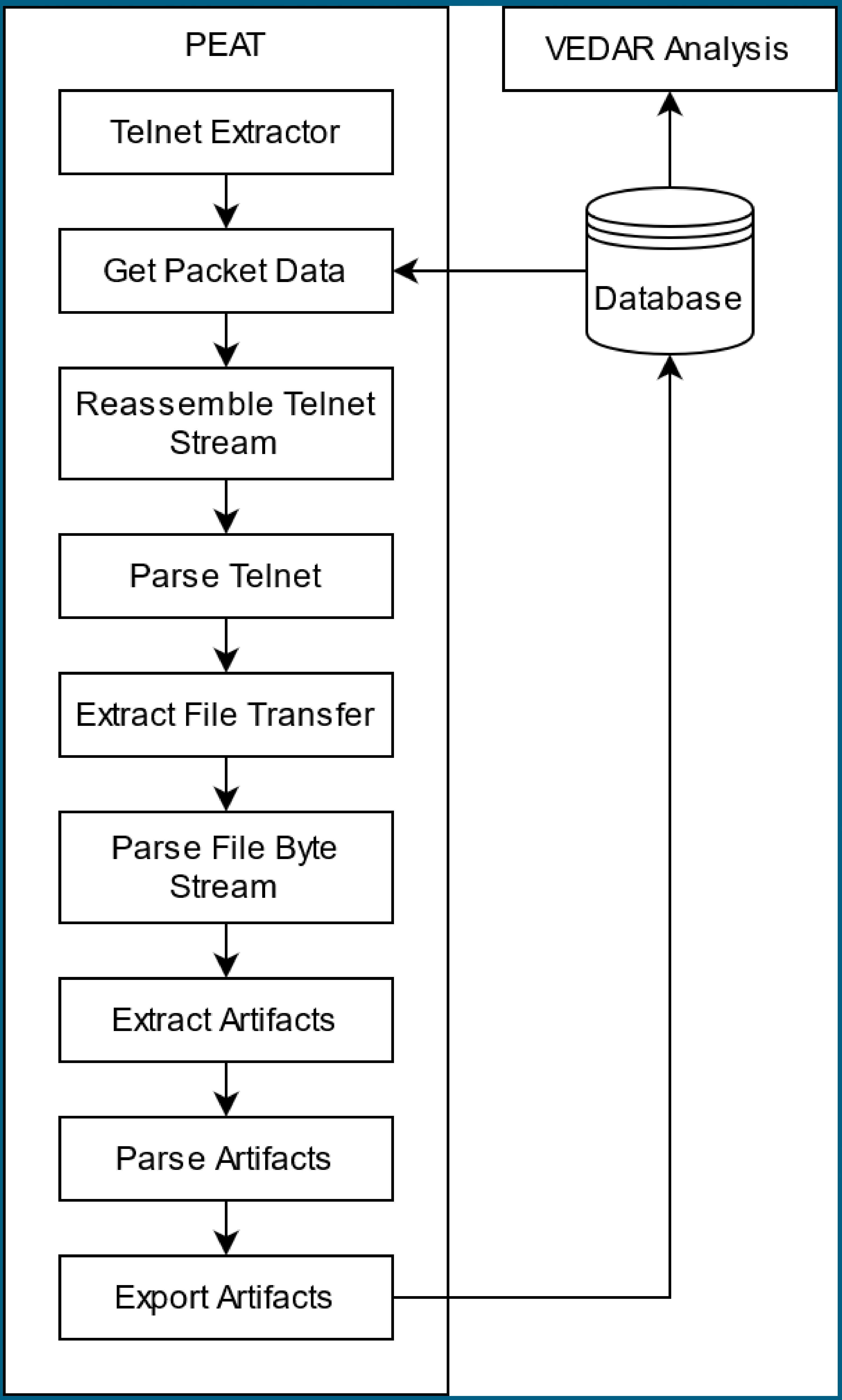
July 2022

Walt Weiffenbach | Purdue University | MS Computer Science | December 2023

Chris Goes, John Jacobellis | Jason Haas | 05621, 05627, 05551

Introduction:

Cyberattacks on critical infrastructure such as those in Ukraine are increasing in severity and frequency against industrial control systems (ICS) to cause real-world damage to civilian, government, or military targets. The VEDAR tool assists by building and analyzing a data model of the ICS environment. PEAT is a component of VEDAR which can interrogate ICS devices. Our goal is to develop a module for PEAT that can extract device configuration data from captured Telnet traffic to enhance VEDAR's data profile of a system.



PEAT

Telnet Extractor

Get Packet Data

Reassemble Telnet Stream

Parse Telnet

Extract File Transfer

Parse File Byte Stream

Extract Artifacts

Parse Artifacts

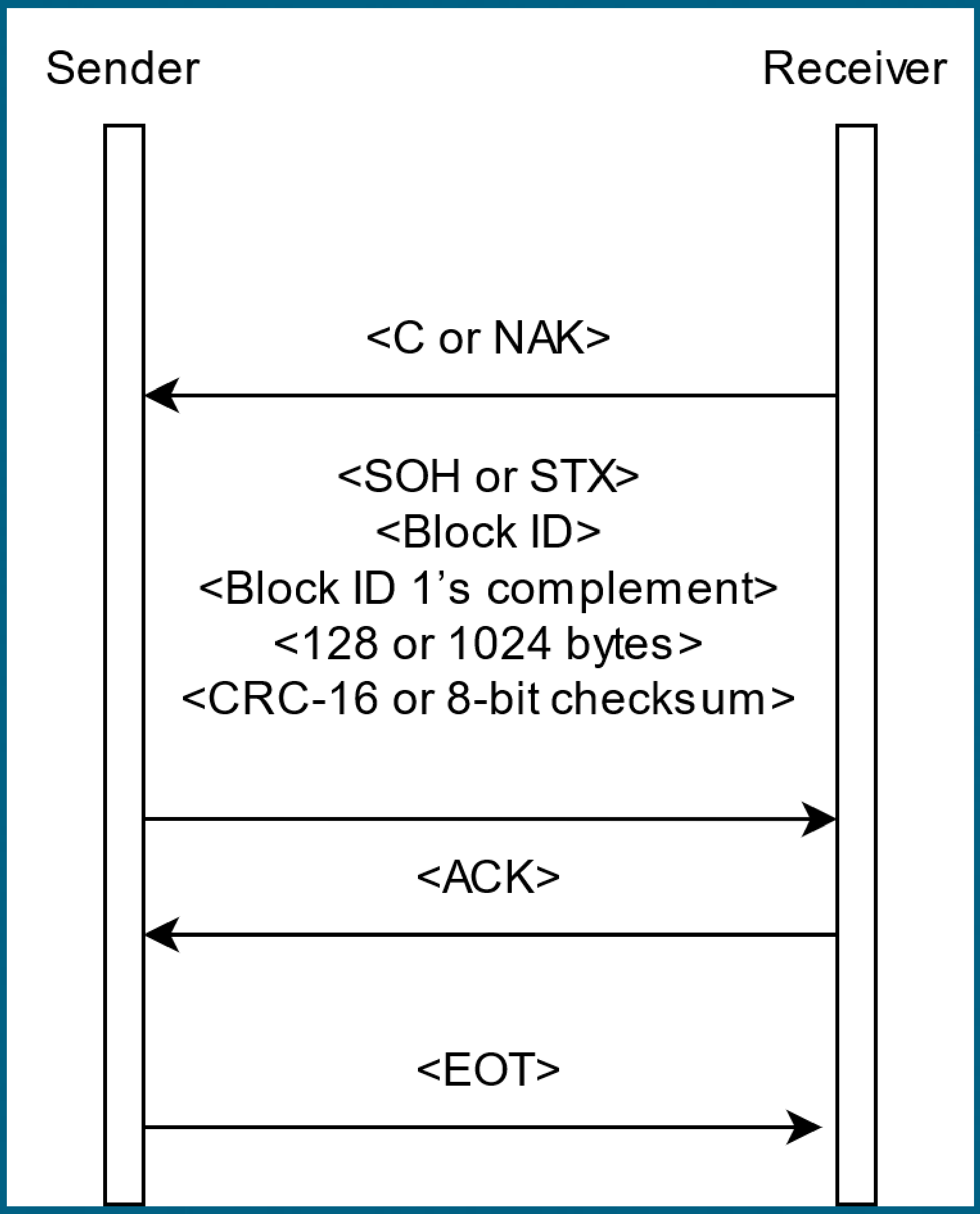
Export Artifacts

VEDAR Analysis

Database

Objectives and Approach:

PEAT's Telnet extractor extracts artifacts and parses them. The tool follows a process as seen in the diagram to the left. A challenge was the manufacturer did not provide the protocol used for some file transfers, and we reverse engineered and identified the YMODEM protocol.



Sender

Receiver

<C or NAK>

<SOH or STX>
<Block ID>
<Block ID 1's complement>
<128 or 1024 bytes>
<CRC-16 or 8-bit checksum>

<ACK>

<EOT>

Results and Discussion

After implementing the Telnet extractor, PEAT can automatically parse artifacts from streams of Telnet data. This system reconstructs the artifacts with minimal errors across uploads and downloads. In the future, extending to additional manufacturers and protocols would be ideal to enhance PEAT's interrogation capabilities.

Impact and Benefits:

The changes here provide benefit to the customer by expanding VEDAR's capability to identify inconsistencies throughout the system with configuration data. This enhances the safety and security of ICS systems that utilize VEDAR by enabling better decision-making from our users.