CPTB Beta Specification Sheet

Overview

Threat Surface Solutions Group (TSSG) is a partnership of premier cybersecurity companies whose principals have directly encountered cyber adversaries, dissected their motivations, and thwarted their attempts to breach critical infrastructure and national security assets. Our focus on test and measurement (T&M), test and evaluation (T&E), cybersecurity, software and hardware platforms, and risk mitigation, allows us to offer comprehensive solutions to protect connected devices such as Internet-of-things (IOT) products, and Industrial IoT (IIOT) systems from penetration; mitigating the liability of manufacturers, and protecting the consumer from possible catastrophic loss. Our focus is on Smart Devices, Smart Household Appliances, Power Grids, Medical Devices, Transportation, and HVAC systems in critical IT Infrastructure such as Federal, State & Local Data Centers

We combine functional and cybersecurity testing into a platform that we are calling a Cybersecurity Physical Test Bench (CPTB). We believe supporting both functional and cyber testing in all phases of the product/system life cycle is becoming increasingly more important. The evidence for this is shown by the demonstrations of IoT devices being able to cause people physical harm, and IoT devices increasingly being used in our nation's critical infrastructure.

We are using our team's experience conducting T&M and T&E for the National Institute and

Standards and Technology (NIST), and working with the NIST Cyber Security Framework (CSF) to have a clear, structured approach for communicating our tools test results. This approach allows us to map results into industry specific standards to show compliance where appropriate. With this methodology, we can provide cyber & functional evidence of compliance, and a quantitative metric.

Short functional description CPTB:

CPTB is a software/hardware platform designed to test connected devices such as IOT devices for safety and function against cybersecurity threats. The CPTB consists of a software suite designed to facilitate large-scale TCP/IP network communications testing, as well as data acquisition hardware to monitor and control physical parameters from the Device Under Test (DUT). The goal of the CPTB is to ensure the safety and function of the DUT as it operates under normal conditions during cyber vulnerability and penetration testing. The CPTB uses the CSF to communicate security categories that are being tested. The CSF can help to identify DUT best practices. While this function is outside the scope of the CPTB, the DUT best practices can be added to the CPTB reports. Our platform takes maximum advantage of a virtualized operating system architectures for ease of testing complex network flow and data acquisition scenarios.

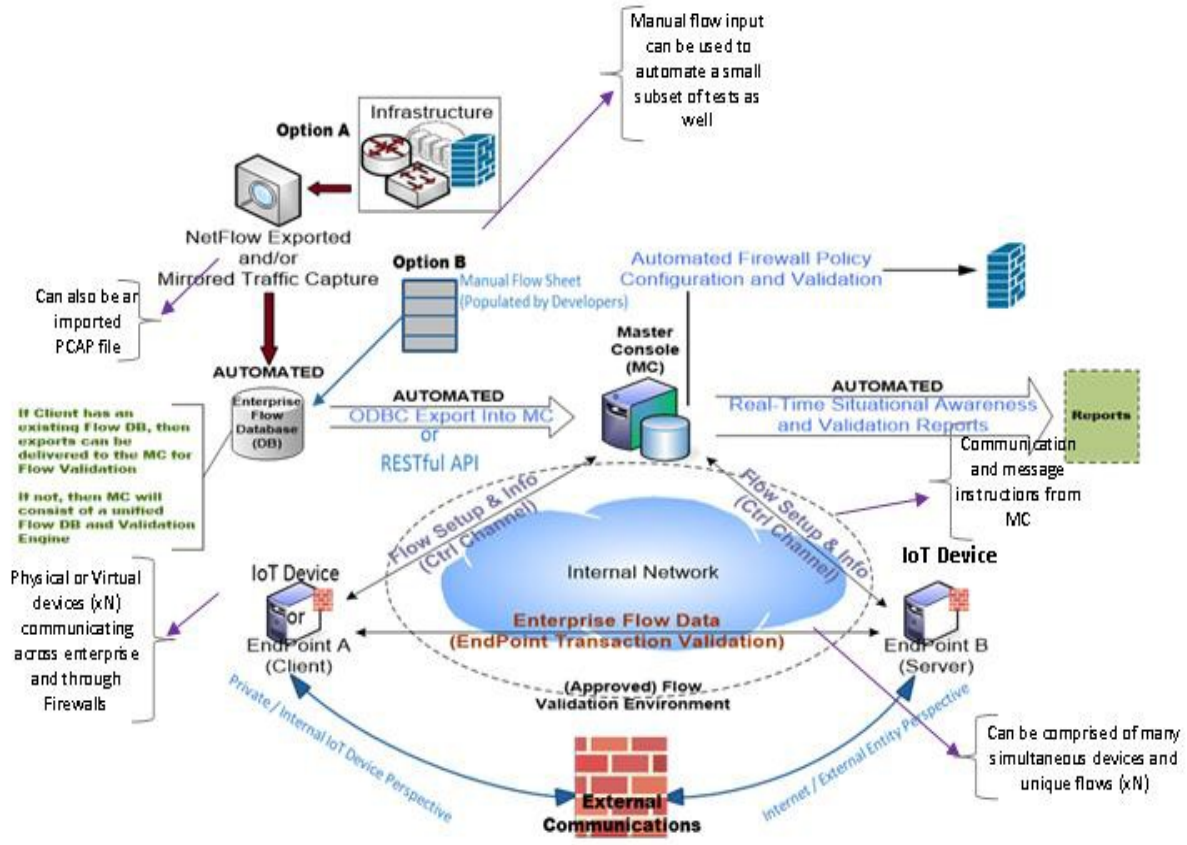
Network parameters such as route hops, delay, jitter, MTU, and latency characteristics, as well as physical parameters such as data acquisition rates and tolerances are considered to be variable test conditions to provide arbitrary complexity. The test results reflect: existence of firewall connectivity, end-to-end throughput, bandwidth and jitter characteristics, and real application layer proxy firewall functionality. CPTB operates with either in-band or out-of-band stateful signaling over TCP based SQL port 3306 to be initiated from each Endpoint to the Master Console server. In addition, CPTB will have Statistical Process Control and Test Data Management for analysis such as First (1^{st}) Pass Yield and Process Capability (C_p, C_{pk}).

Figure 1 indicates the high-level overview of system inputs and outputs (IO) for the CPTB software suite. The software operational states are broken into three main functions: Endpoint Mode, Master Console Mode, and finally Reporting Mode. The Graphical User Interface (GUI) is the preferred method of all non-Endpoint operations.

The CPTB can be tailored to a large number of connected devices. Its multifunction data acquisition hardware can monitor signals such Radio Frequency (RF), Acoustic/Vibration, and

video/Images.

Figure#1


Manual flow input can be used to automate a small subset of tests as well
Infrastructure
Option A
NetFlow Exported and/or Mirrored Traffic Capture
Can also be an imported PCAP file
Option B
Manual Flow Sheet (Populated by Developers)
Automated Firewall Policy Configuration and Validation
AUTOMATED
Enterprise Flow Database (DB)
If Client has an existing Flow DB, then exports can be delivered to the MC for Flow Validation
If not, then MC will consist of a unified Flow DB and Validation Engine
AUTOMATED
ODBC Export Into MC
or
RESTful API
Master Console (MC)
AUTOMATED
Real-Time Situational Awareness and Validation Reports
Reports
Communication and message instructions from MC
Flow Setup & Info (Ctrl Channel)
Flow Setup & Info (Ctrl Channel)
Internal Network
Enterprise Flow Data (EndPoint Transaction Validation)
(Approved) Flow Validation Environment
IoT Device
or
EndPoint A (Client)
IoT Device
EndPoint B (Server)
Physical or Virtual devices (xN) communicating across enterprise and through Firewalls
Private / Internal IoT Device Perspective
Internet / External Entity Perspective
External Communications
Can be comprised of many simultaneous devices and unique flows (xN)

System Architecture

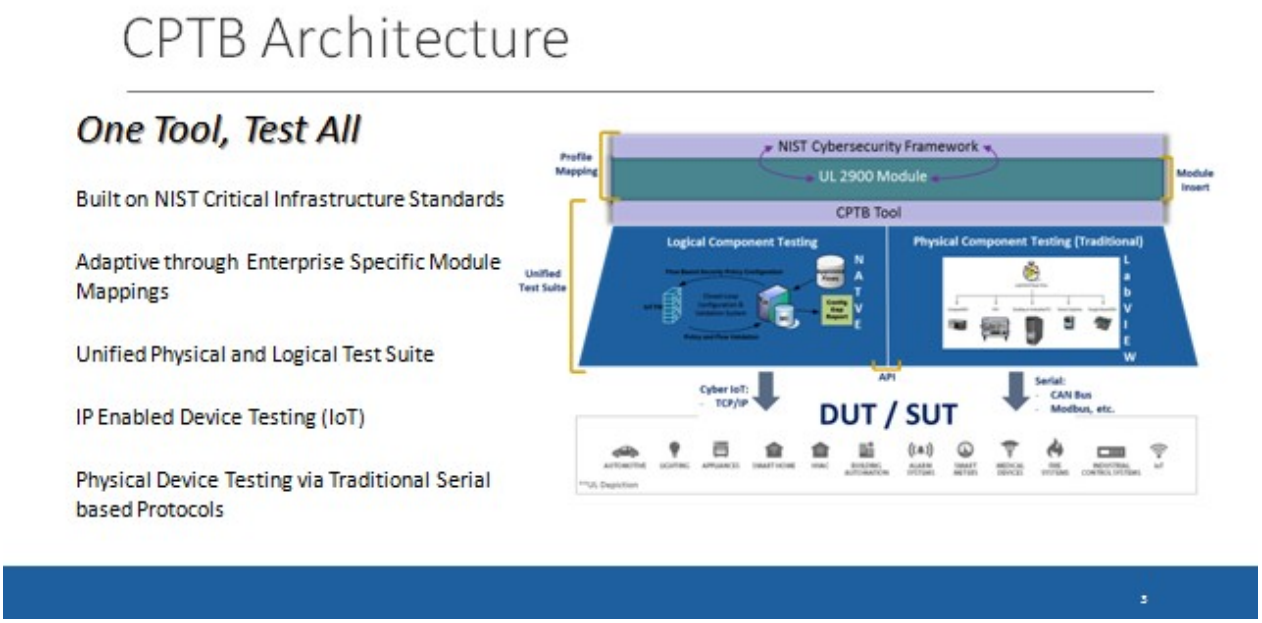


Figure #2

CPTB Test Data Flow

Cyber and Physical Protocols

Unified Interface

Multi-function Test Unit

Correlation and Context Mapping

Comprehensive Physical and Logical Protocol Coverage

Single Chassis Build

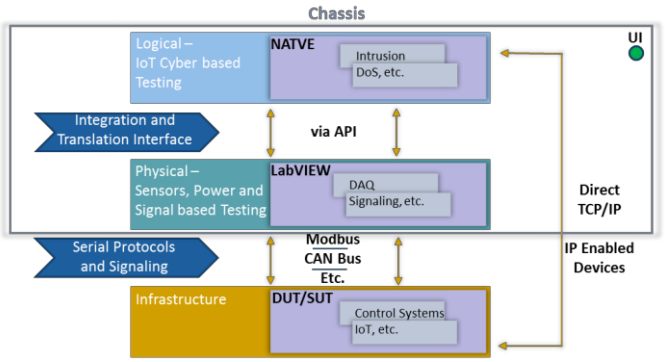


Figure #3

Protocols that will be delivered:

a. TCP/IP, UDP
b. NAT
c. SQL, DNS, sshV2, ftp passive mode, http, https
d. Any Enterprise Protocols Recorded
e. MODBUS
f. CAN BUS
g. Profibus
h. Custom Buses and Protocols

Input Data Sets that will be delivered:

a. XML
b. Flat File
c. CSV

Report formats that will be delivered:

a. High level measurements communicated with the NIST Cyber Security Framework, based on lower level detailed measurements.
b. GUI Tables (Lower level detailed measurements.)
c. Flat File (Lower level detailed measurements.)
d. CSV (Lower level detailed measurements.)
e. 1st Pass Yield
f. Process Capabilities

Software that will be delivered:

a. CPTB 1.0 Beta Installer
b. CPTB Beta Monitor and Control Software

Recommended Types of Devices Under Test (DUT):

a. Virtual Machines
b. Windows and Linux OS based Devices
c. IoT Devices
d. Connected Devices (We are defining these as IoT devices within bigger systems. (Ex. Smart Homes and Automotive Vehicles)

Types of Simulated/Emulated devices:

a. Virtual Machines
b. Windows and Linux OS based Devices
c. IoT Devices
d. Connected Devices

Scale of DUT:

a. 400,000 flows per run, on a Windows 2003 (or later) server w/4GHZ processor
b. 1 DUT
c. Analog I/O
d. Digital I/O
e. Relays

Scale of Simulated/Emulated devices:

a. 400,000 flows per run, on a Windows 2003 (or later) server w/4GHZ processor
b. Analog I/O (Simulated/Emulated devices required are use case dependent). Our Beta delivery will have the capacity for 32 Analog Input channels (Voltage +-10 V), 16 Analog Input channels (Voltage +-10 V), and 16 Analog Output channels (Current +-21.5 mA). The mix of channels will be agreed upon before delivery.)
c. Digital I/O (Simulated/Emulated devices required are use case dependent. Our Beta delivery will have the capacity for at least 32 Digital Input/output channels.)
d. Relays

Hardware that will be delivered, see diagram and table below:

a. Packaging
b. Interfaces
c. Power

NOTE: This is Beta packaging for the CPTB.


NATIONAL INSTRUMENTS
NI cRIO-9033

TECHNICAL H/W SPECS

Hardware Line	Industrial Line
System Cooling	Fanless
Processor Socket	Onboard (BGA)
Processor Generation	Broadwell
Processor Cores	2
Graphics/GPU	Intel HD Graphics 5500
Memory Type	DDR3L SO-DIMM (non-ECC)
Memory Capacity	16 GB
Memory Speed	1600 MHz
Memory Slot Count	2
Rear I/O	2 USB 3.0 ports 1 Gb LAN port (with vPro on i5) 2 Mini-DisplayPorts 1 DC jack (Terminal Block Power Optional)
Front I/O	2 USB 3.0 ports 1 mic/headphone connector 1 RS-232 COM port (optional) Power button
Expansion Options	M.2 NGFF
Storage Options	M.2 NGFF SSD 22x80
LAN Controller	Intel I218LM GbE
Input Voltage	12-19 V (DC jack) , 24 V (Terminal block)
Power Input	DC jack
Operating Temperature Range	0°C ~ 50°C
Dimensions (WxHxD)	142 x 62 x 107 mm 5.6" x 2.4" x 4.2"
Case Type	Compact Fanless
Case Material	Aluminum Extrusion Steel
Port Punchouts	2 Antenna holes
Mounting Options	DIN-mount VESA-mount Wall-mount
VESA Mounting	MIS-D 100
Included Accessories	Rubber feet DC Jack Retaining Clip
Manufacturer Launch Date	Q1'15
Expected Life Cycle	3 Years
Regulatory Information	CE standards applied (EN 55022 / EN 55024 / EN 60950) FCC - Assembled using FCC certified components RoHS
Warranty	2 year limited warranty on parts and services

Hardware Specifications

CPU: Intel Atom E3825
Number of Cores: 2
CPU Frequency: 1.33 GHz
On-die L2 cache: 1 MB (shared)
FPGA Type: Xilinx Kintex-7 7K70T
Input Voltage V1: 9 V to 30 V
Input Voltage V2: 9 V to 30 V
Maximum power consumption: 40 W
Typical battery life: 10 Years
Number of Reconfigurable I/O Slots: 4

Operating System

Supported Operating System: NI Linux Real-Time (64-bit)
Supported Application Software: LabVIEW Real-time 2014 or later
Driver Dependency: NI-RIO Device Drivers August 2014 or later

Front I/O

Network/Ethernet Port: 2 Network Interface Ports
USB, A Connector: 2 Standard ports
USB, B Connector: 1 Standard Port
Mini Display Port: 1 Port, 2506 x 1600 resolution @ 60
Hz Serial Ports: RS-232, RS-485/422
SD Cart Slot Support: SD and SDHC standards

Reconfigurable I/O

Analog Input Modules (Current/Voltage)
Analog Output Modules (Current/Voltage)
Digital I/O Modules
MODBUS Interface Modules
CAN Interface Modules
Temperature Input Modules
Motor Drive Interface Modules
Local Interconnect Network (LIN) Interface Modules
Serial Communication Interface Modules