Identifying SCADA Devices and their Vulnerabilities on the IoT

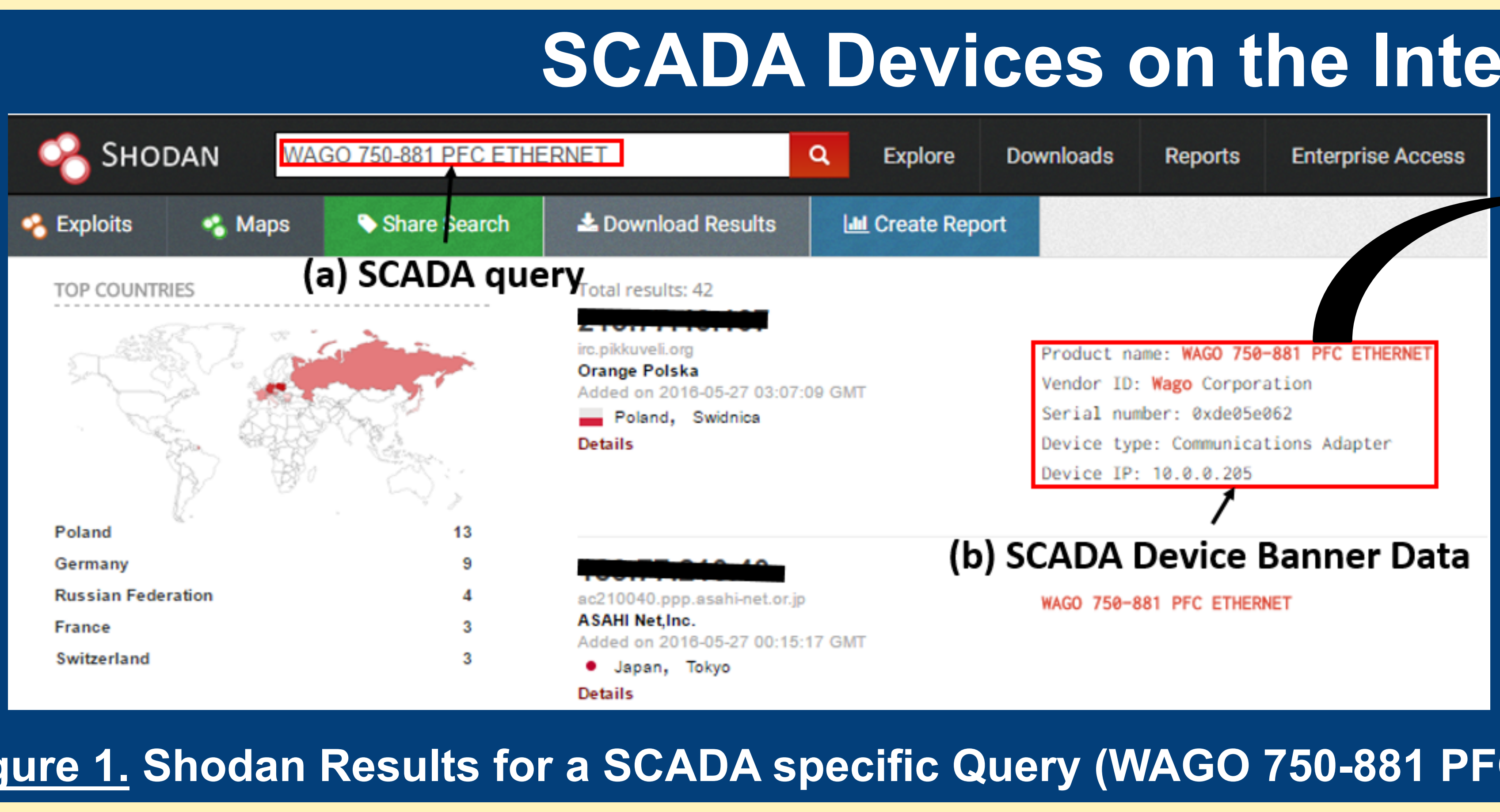
SBE TTP: Medium: Securing Cyber Space: Understanding the Cyber Attackers and Attacks via Social Media Analytics (NSF SES-1314631)
https://ai.arizona.edu/research/cyber

Principal Investigators:
Dr. Hsinchun Chen, University of Arizona
Dr. Salim Hariri, University of Arizona
Dr. Ron Breiger, University of Arizona
Dr. Tom Holt, Michigan State University

Overview

- Supervisory Control and Data Acquisition (SCADA) systems supervise, maintain, control, and collect data from critical infrastructure (e.g., power plants).
- Shodan, a search engine for the Internet of Things (IoT), regularly scans, and indexes provides data about publicly accessible, internet-enabled SCADA systems.
    - However, minimal work has attempted to identify all SCADA devices and their vulnerabilities.
- **This work uses machine learning and vulnerability assessments to identify SCADA systems and their vulnerabilities available on Shodan.**

SCADA Devices on the Internet of Things (IoT)



TOP COUNTRIES

Poland	13
Germany	9
Russian Federation	4
France	3
Switzerland	3

Total results: 42

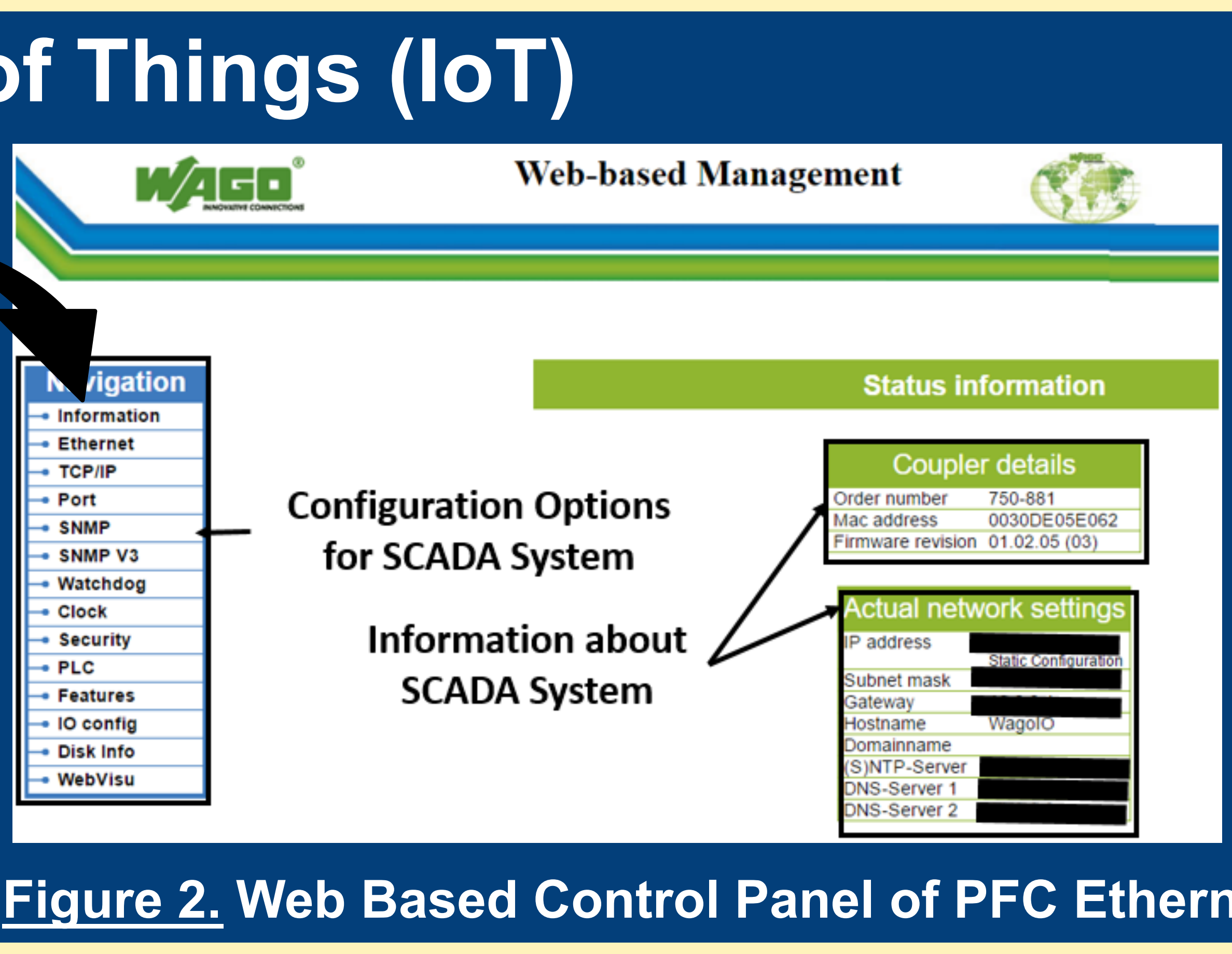
[redacted]
irc.pikkuveli.org
Orange Polska
Added on 2016-05-27 03:07:09 GMT
Poland, Swidnica
Details

[redacted]
ac210040.ppp.asahi-net.or.jp
ASAHI Net,Inc.
Added on 2016-05-27 00:15:17 GMT
Japan, Tokyo
Details

```
Product name: WAGO 750-881 PFC ETHERNET
Vendor ID: Wago Corporation
Serial number: 0xde05e062
Device type: Communications Adapter
Device IP: 10.0.0.205
```

WAGO 750-881 PFC ETHERNET

Figure 1. Shodan Results for a SCADA specific Query (WAGO 750-881 PFC)



Coupler details

Order number	750-881
Mac address	0030DE05E062
Firmware revision	01.02.05 (03)

Actual network settings

IP address	[redacted] Static Configuration
Subnet mask	[redacted]
Gateway	[redacted]
Hostname	WagoIO
Domainname	
(S)NTP-Server	[redacted]
DNS-Server 1	[redacted]
DNS-Server 2	[redacted]

Figure 2. Web Based Control Panel of PFC Ethernet

Methodological Approach

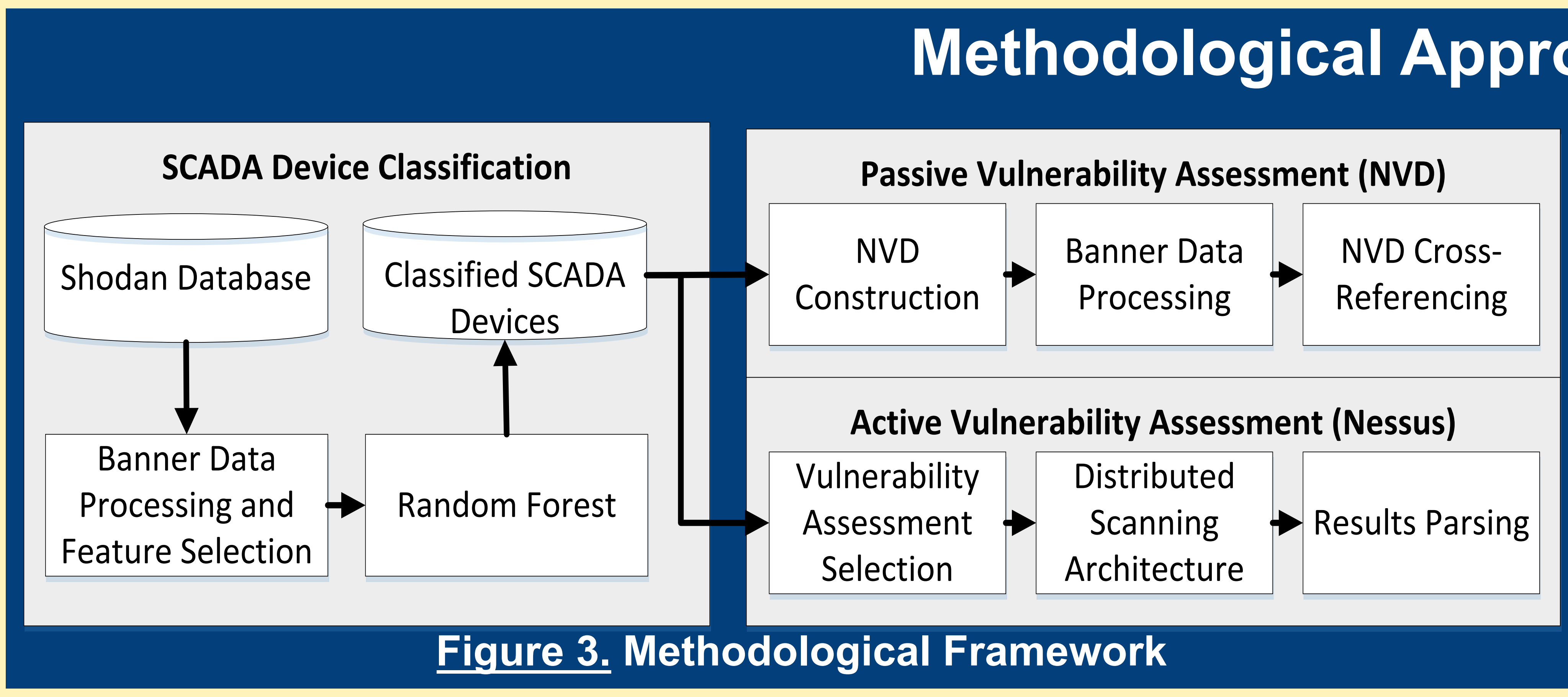

SCADA Device Classification
Shodan Database
Classified SCADA Devices
Banner Data Processing and Feature Selection
Random Forest
Passive Vulnerability Assessment (NVD)
NVD Construction
Banner Data Processing
NVD Cross-Referencing
Active Vulnerability Assessment (Nessus)
Vulnerability Assessment Selection
Distributed Scanning Architecture
Results Parsing

Figure 3. Methodological Framework

SCADA Device Classification:

- Extract features (e.g., port, n-grams) from banner data for all devices in Shodan
- Classify devices as SCADA/non-SCADA with Random Forest (F-Measure – 99.3%)

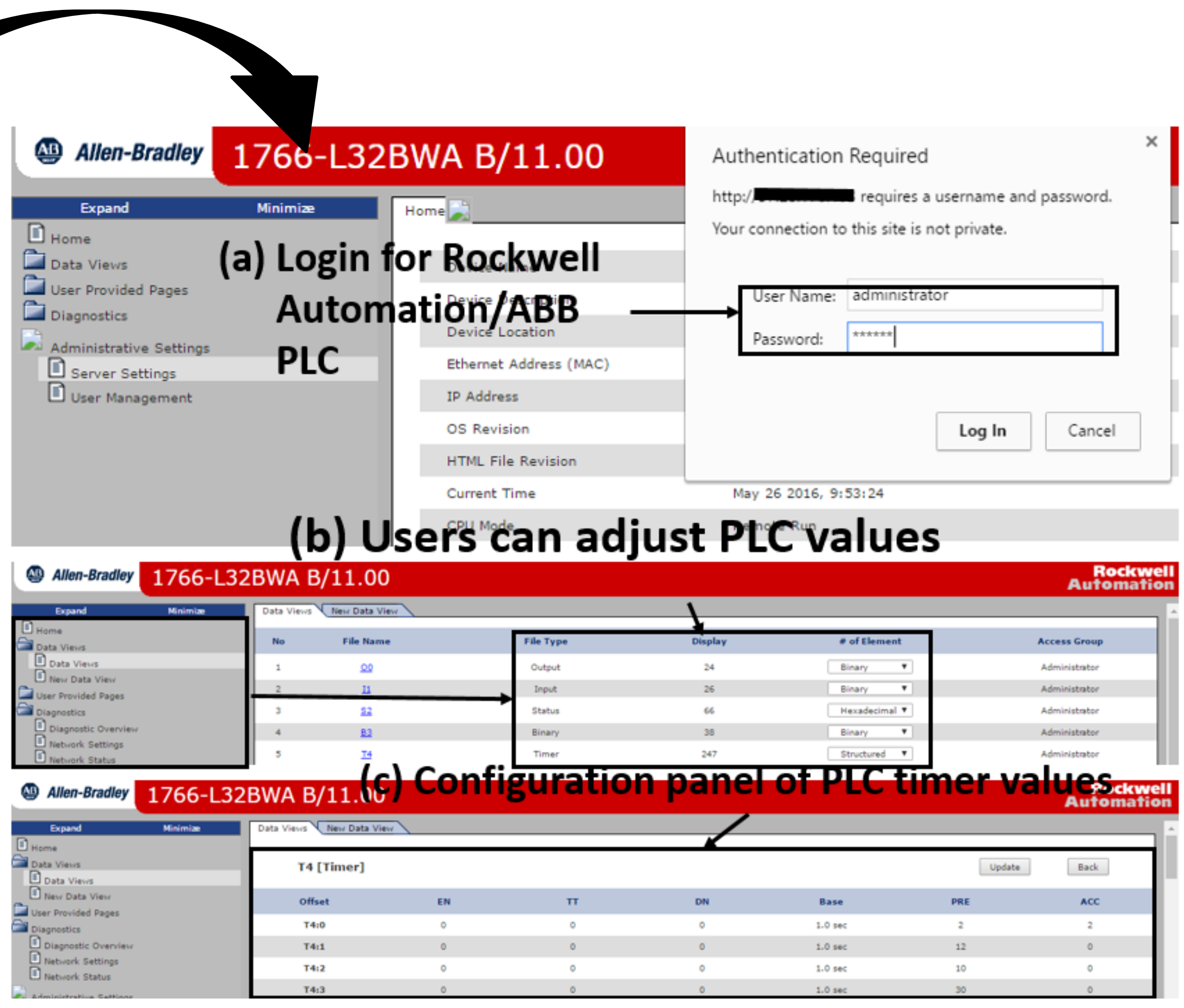
Vulnerability Assessment:

- Passive Assessment
    - Cross reference banner data with National Vulnerability Database (NVD)
- Active Assessment
    - Use Nessus in a distributed architecture actively probe devices for vulnerabilities

Selected Vulnerability Assessment Results

Risk Level	Number of Devices	Vulnerability Names(s)	Selected Affected Vendors
Critical	131	Rockwell Automation MicroLogix 1400 PLC Default Credentials	Rockwell Automation/ABB
	15	InduSoft Arbitrary Script Execution	InduSoft
	14	Default Credentials	HP, RuggedCom
	4	Conficker Worm Detection	Siemens
High	111	OpenSSH and DropBear SSH Vulnerabilites	Rockwell Automation/ABB, Siemens, Schneider Electric, Honeywell
	29	Default Credentials	Schneider Electric
Medium	1,407	Unencrypted Telnet Server	Rockwell Automation/ABB, Siemens, Schneider Electric, Power Measurement, Acromag, Honeywell
	607	Modbus Coil Access	Schneider Electric, Rockwell Automation/ABB, Acromag, Lantronix, Power Measurement
	524	OpenSSH Multiple Vulnerabilities	Rockwell Automation, Siemens, Schneider Electric, Honeywell, AKCP, RuggedCom

Table 1. About 4,009/20,461 (19.59% of devices) are susceptible to critical, high, and medium vulnerabilities such as default credentials, script execution, and Modbus coil access.



Authentication Required
http://[redacted] requires a username and password.
Your connection to this site is not private.
User Name: administrator
Password: ******
Log In Cancel

May 26 2016, 9:53:24

No	File Name	File Type	Display	# of Element	Access Group
1	O0	Output	24	Binary	Administrator
2	I1	Input	26	Binary	Administrator
3	S2	Status	66	Hexadecimal	Administrator
4	B3	Binary	38	Binary	Administrator
5	T4	Timer	247	Structured	Administrator

T4 [Timer]

Offset	EN	TT	DN	Base	PRE	ACC
T4:0	0	0	0	1.0 sec	2	2
T4:1	0	0	0	1.0 sec	12	0
T4:2	0	0	0	1.0 sec	10	0
T4:3	0	0	0	1.0 sec	30	0

Figure 4. Vulnerable Rockwell Automation PLC. Users can:
(a) Logging into PLC,
(b) potential PLC adjustment, and
(c) configure panel of timer values

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

Artificial Intelligence Lab
Management Information Systems