Network Security Systems?

ICS Security Task Force Division

Pete Maynard
@pgmaynard

March 12, 2015

Threats

- Havex Malware.
- OPC to scan for SCADA devices.
- Reports back to command and control server.
- Recently detected July 2014.
  - European ICS.
  - Team Since 2011.
- State sponsored?

Scanning for SCADA Devices

- Readily available scanners.
  - SCADA StrangeLove.
- Simple Python Script.
- NMap Plugins.
- Return Device name, IP, software version.

SCADA Fuzzers

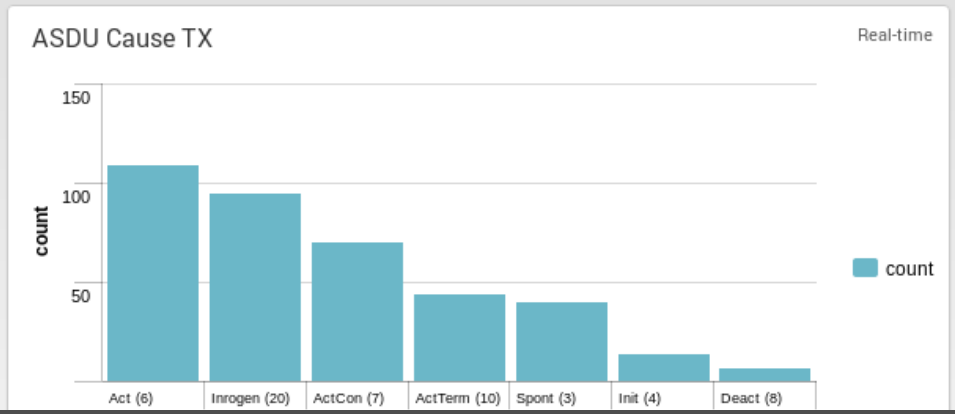
- Protocol Fuzzers.
- Project Robus.
  - DNP3.
  - Identified many vulnerabilities.
- Fuzzing can kill.

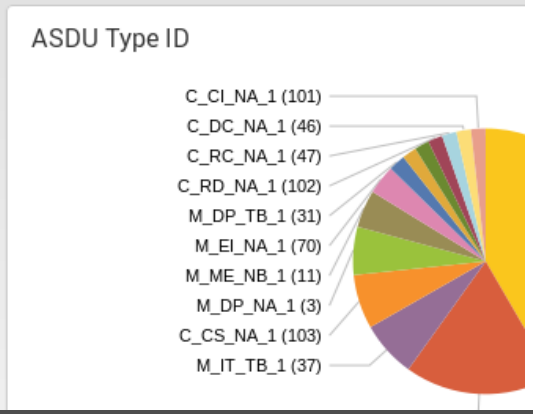
Protocol Analyzers

11 580.482611	10.50.50.105	10.50.50.2	104asdu	89 [TCP Previous segment lost] 0,0->0 M_SP_TB_1 Spont IOA=0
12 580.818871	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
13 581.219513	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
14 581.497612	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
15 596.590691	10.50.50.105	10.50.50.2	104asdu	89 [TCP Previous segment lost] 0,0->0 M_SP_TB_1 Spont IOA=0
16 596.871768	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
17 597.086642	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
18 597.232636	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
19 682.755574	10.50.50.105	10.50.50.2	104asdu	89 [TCP Previous segment lost] 0,0->0 M_SP_TB_1 Spont IOA=0
20 683.210556	10.50.50.105	10.50.50.2	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
21 2228.761677	10.50.50.105	10.50.50.75	104asdu	89 0,0->0 M_SP_TB_1 Spont IOA=0
22 2228.761864	10.50.50.105	10.50.50.75	104asdu	77 [TCP Retransmission] 0,0->0 M_SP_TB_1 <CauseTx=42> IOA=0

```
ame 21: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
thernet II, Src: RealtekU_6d:a8:fc (52:54:00:6d:a8:fc), Dst: Netgear_e3:94:bd (00:09:5b:e3:94:bd)
nternet Protocol Version 4, Src: 10.50.50.105 (10.50.50.105), Dst: 10.50.50.75 (10.50.50.75)
ansmission Control Protocol, Src Port: iec-104 (2404), Dst Port: 55561 (55561), Seq: 1, Ack: 1, Len: 23
EC 60870-5-104-Apci: ->I(3,1)
 ApduLen: 21
 .... ..00 = ApciType: I (0x00)
EC 60870-5-104-Asdu: 0,0->0 M_SP_TB_1 Spont IOA=0 'single-point information with time tag CP56Time2a'
 TypeId: M_SP_TB_1 (30)
 .000 0001 = NumIx: 1
 ..00 0011 = Caus
 .0.. .... = Nega
 0... .... = Test
 OA: 0
 Addr: 0
 IOA: 0
 IEC 60870-5-104-
```

```
 ff d7 76 ba 0C
 d8 2f 68 15 0E
 00 01 26 5a 1c
```



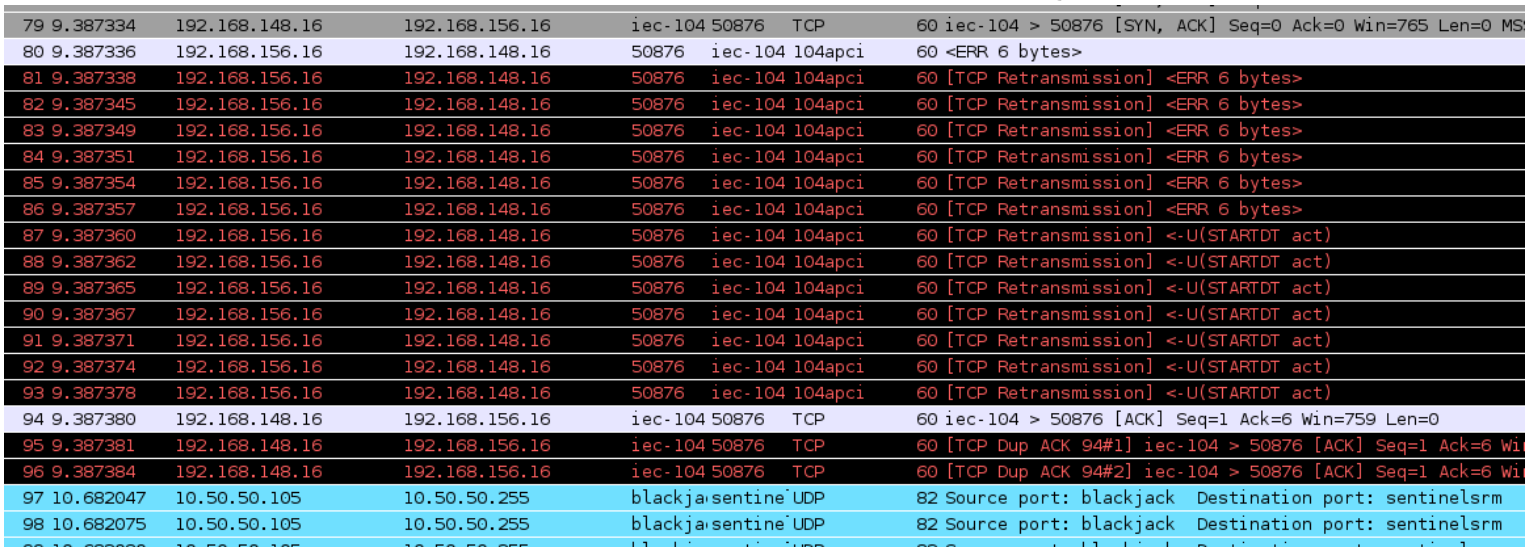


Overview of IEC 60870

- IEC 60870 developed periodically between the years 1988 and 2000.
- Consists of 6 main parts and four companion sections.
- Open Standard.
- IEC 60870-5-101 Defines transmission over serial links.
- IEC 60870-5-104 Defines transmission over TCP/IP.
- No encryption, authentication.

Replay Attack

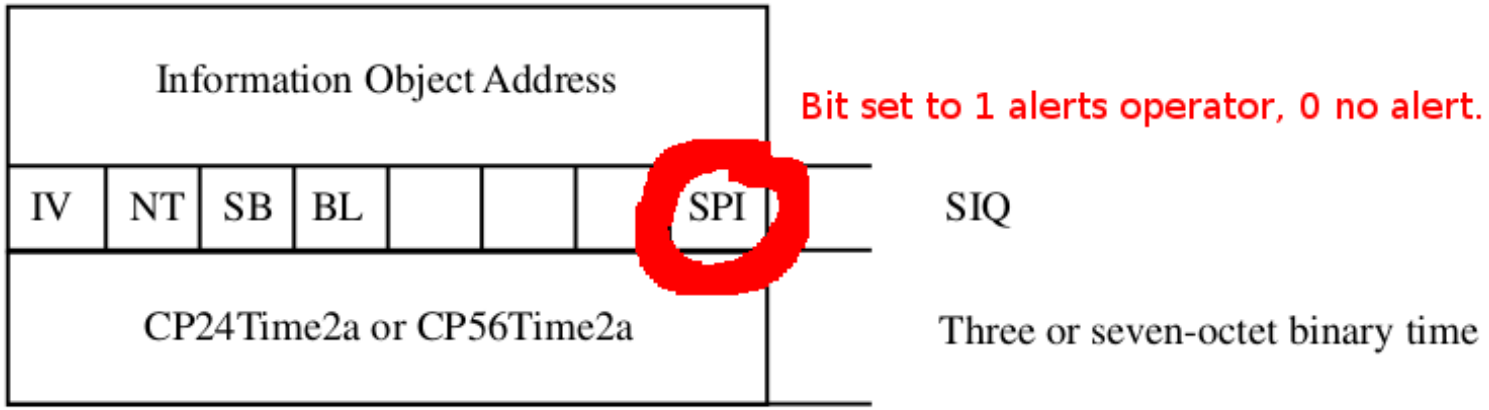
- Captured packets using the switch SPAN port.
- Command, Readings, Alerts, Firmware updates...
- Replayed packets dropped by kernel.
- TCPREPLAY alternatives needed to modify SEQ values.



79 9.387334	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 iec-104 > 50876 [SYN, ACK] Seq=0 Ack=0 Win=765 Len=0 MS
80 9.387336	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 <ERR 6 bytes>
81 9.387338	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
82 9.387345	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
83 9.387349	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
84 9.387351	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
85 9.387354	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
86 9.387357	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <ERR 6 bytes>
87 9.387360	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
88 9.387362	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
89 9.387365	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
90 9.387367	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
91 9.387371	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
92 9.387374	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
93 9.387378	192.168.156.16	192.168.148.16	50876	iec-104	104apci	60 [TCP Retransmission] <-U(STARTDT act)
94 9.387380	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 iec-104 > 50876 [ACK] Seq=1 Ack=6 Win=759 Len=0
95 9.387381	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 [TCP Dup ACK 94#1] iec-104 > 50876 [ACK] Seq=1 Ack=6 Wi
96 9.387384	192.168.148.16	192.168.156.16	iec-104	50876	TCP	60 [TCP Dup ACK 94#2] iec-104 > 50876 [ACK] Seq=1 Ack=6 Wi
97 10.682047	10.50.50.105	10.50.50.255	blackja	sentine	UDP	82 Source port: blackjack Destination port: sentinelsrm
98 10.682075	10.50.50.105	10.50.50.255	blackja	sentine	UDP	82 Source port: blackjack Destination port: sentinelsrm

Man-In-The-Middle

- Ettercap plug-in written for IEC 104.
- Intercepts 104 packets and modifies them.
- Able to hide an earth fault from the operators.
- Simply flip a bit on a plaintext connection.



Detection

- CISCO's ARP Detection.
- Duplicate packets seen by a switch.
- Use TCP/IP headers to identify a MITM packet.
- Signature based rules, meh.

Anomaly Detection

- One-Class Support Vector Machine.
- WEKA or MOA (Massive Online Analysis).
- Plan to use the following attributes:

Network level	**IEC 104 Application Level**	**APCI**	**ASDU**
Packet Size	no. packets in control direction	Start Bit	Type ID
Packet Rate	no. packets in monitor direction	APDU Length	Structure Qualifier
no. packets to destination		Type ID	Cause of Transmission
no. packets src to destination			Common Address of ASDU
no. ARP packets			no. packets to Common Address

Questions/Ideas/Feedback?