



U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

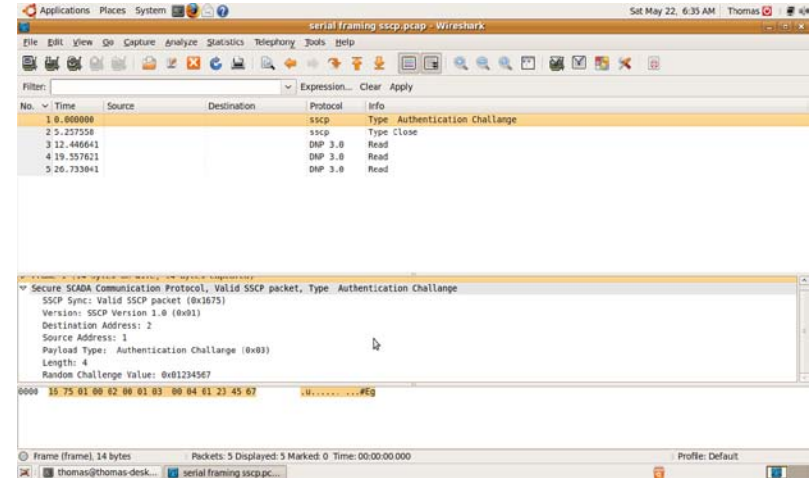
Mark Hadley

Pacific Northwest National Laboratory

Protocol Analyzer

Summary Slide: Protocol Analyzer

- **Outcomes:** Provide operators of SSCP-deployed technologies the tools to view and troubleshoot SSCP-protected communication.
- **Roadmap Challenge:** Standardized test plans and upgrades for new technology are not widely available.
- **Major Successes:** Demonstration of Open Source solution shown at DistribuTECH.



- **Schedule:** Open source candidate (Q3), Demonstration (Q2)
- **Level of Effort:** \$159K
- **Funds Remaining:** None
- **Performers:** Pacific Northwest National Laboratory
- **Partners:** Wireshark Project, ASE, FTE (future partner)

Technical Approach and Feasibility

- **Approach**

- Utilize PNNL-developed technology to import SSCP protected data into Wireshark's normal interface
- Add SSCP digester to Wireshark
- Modify Wireshark (via libpcap) to natively process serial data
- Hand off encapsulated control system protocol to its digester

Technical Approach and Feasibility

- **Metrics for Success**
 - Public demonstration of technology
 - Open source candidate released to community for review
 - Future commercial product support for SSCP

Technical Approach and Feasibility

Frame Display - NetDecoder EFS

File Edit View Live Summary Decode Radix Character Event Filter Options Window Help

Summary Layer: Secure SCADA Communication Protocol with Auto-traverse

All Protocols Data Secure SCADA Communication Protocol

Bookmark	Frame#	Dest Address	Src Address	Payload Type	Length	Fram...	Delta	Timestamp
•	1	1	0	DH Key Exchange	144	154		7/19/2010 4:51:36.6114 ...
•	2	0	1	DH Key Exchange	150	160	00:00:00.3...	7/19/2010 4:51:36.9767 ...
•	3	1	0	DH Key Exchange	22	32	00:00:00.2...	7/19/2010 4:51:37.2644 ...
•	4	0	1	Session Establish Request	0	44	00:00:22.0...	7/19/2010 4:51:59.2905 ...
•	5	1	0	Authentication Challenge	4	14	00:00:00.0...	7/19/2010 4:51:59.3078 ...
•	6	1	0	DH Key Exchange	144	154	00:00:00.1...	7/19/2010 4:51:59.4886 ...
•	7	0	1	DH Key Exchange	150	160	00:00:00.3...	7/19/2010 4:51:59.8524 ...
•	8	1	0	DH Key Exchange	22	32	00:00:00.2...	7/19/2010 4:52:00.1342 ...
•	9	1	0	Data	25	35	00:01:58.0...	7/19/2010 4:53:58.2160 ...
•	10	1	0	Data	25	35	00:00:10.0...	7/19/2010 4:54:08.2579 ...
•	11	1	0	Data	25	35	00:00:09.9...	7/19/2010 4:54:18.2476 ...
•	12	1	0	Data	25	35	00:00:10.0...	7/19/2010 4:54:28.2536 ...
•	13	0	1	Data	64	74	00:00:02.1...	7/19/2010 4:54:30.4081 ...
•	14	1	0	Data	25	35	00:00:02.3...	7/19/2010 4:54:32.7384 ...
•	15	0	1	Data	64	74	00:00:02.1...	7/19/2010 4:54:34.8922 ...
•	16	1	0	Data	25	35	00:00:02.3...	7/19/2010 4:54:37.2231 ...

Frame 9: [DCE] Len=35

- Secure SCADA Communication Protocol:
 - SYNCH: 0x1675
 - Protocol Version: 1
 - Dest Address: 1
 - Src Address: 0
 - Payload Type: Data
 - Length: 25
 - Data:
 - Raw Data: 0x01000107ca91b5648cd1a618f53b4f0a9b4c0f6089
 - HMAC: 0xd6560b54

```

BINARY
00000000 00000001 00000000 00011001 00000001 00000000
00000000 00000011 11001010 10010001 10110101 01100100
10001100 11010001 10100110 00011000 11110101 00111011
PAYLOAD
01001111 00001010 10011011 01001100 00001111 01100000
RADIO
16 75 01 00 01 00 00 01 00 19 01 00 01 07 ca 91 b5 64 8c
D1 a6 18 f5 3b 4f 0a 9b 4c 0f 60 89 d6 56 0b 54
HEX
C
S Y U H U H U H U H U H U H U H L A I S D C I B N S ; O L F B L T 9 B V T T
    
```

Event 767 to 801 of 2,345 (35 events) 7/19/2010 4:53:58.2160 PM to 7/19/2010 4:53:58.2514 PM

Rate	Delta	RTS	CTS	DSR	DTR	CD	RI	Errors
960 ev/sec	00:00:00.0354	On	On	On	On	On	Off	

For Help Press F1

Technical Approach and Feasibility

- **Challenges to Success**

- Laboratory acceptance of open source technology transfer
 - Identified an advocate in PNNL Commercialization office
- Catch-22 with commercialization vendor
 - Defined SSCP filter using FTE's NetDecoder script interface
 - Transfer to industry planned for FY11

Technical Approach and Feasibility

- **Technical Achievements to Date**
 - Wireshark library (Libpcap) updated to support serial traffic
 - SSCP digester defined within Wireshark
 - Defined SSCP using script language for NetDecoder protocol analyzer

Collaboration/Technology Transfer

- **Plans to gain industry input**
 - Leverage success of Hallmark project and other technology transfer efforts
 - Make the SSCP an industry standard, targeting IEEE and IEC
 - Encourage adopters of SSCP to request support from their protocol analyzer vendors

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
 - Target protocol analyzer vendors currently supporting electric industry
 - Initial approach targets protocol analyzer products
 - Future integration into test set products desired
 - Operational support of cryptographically protected communication meets industry security objective of availability

Next Steps

- **Approach for FY11**
 - Incorporate SSCP into FTE's NetDecoder Product
 - Risks include acceptance by FTE and/or other protocol analyzer and test set vendors
- **This approach supports deployment of SSCP-enabled products. PNNL will collaborate with other CEDS projects to integrate serial and security technology into Wireshark.**