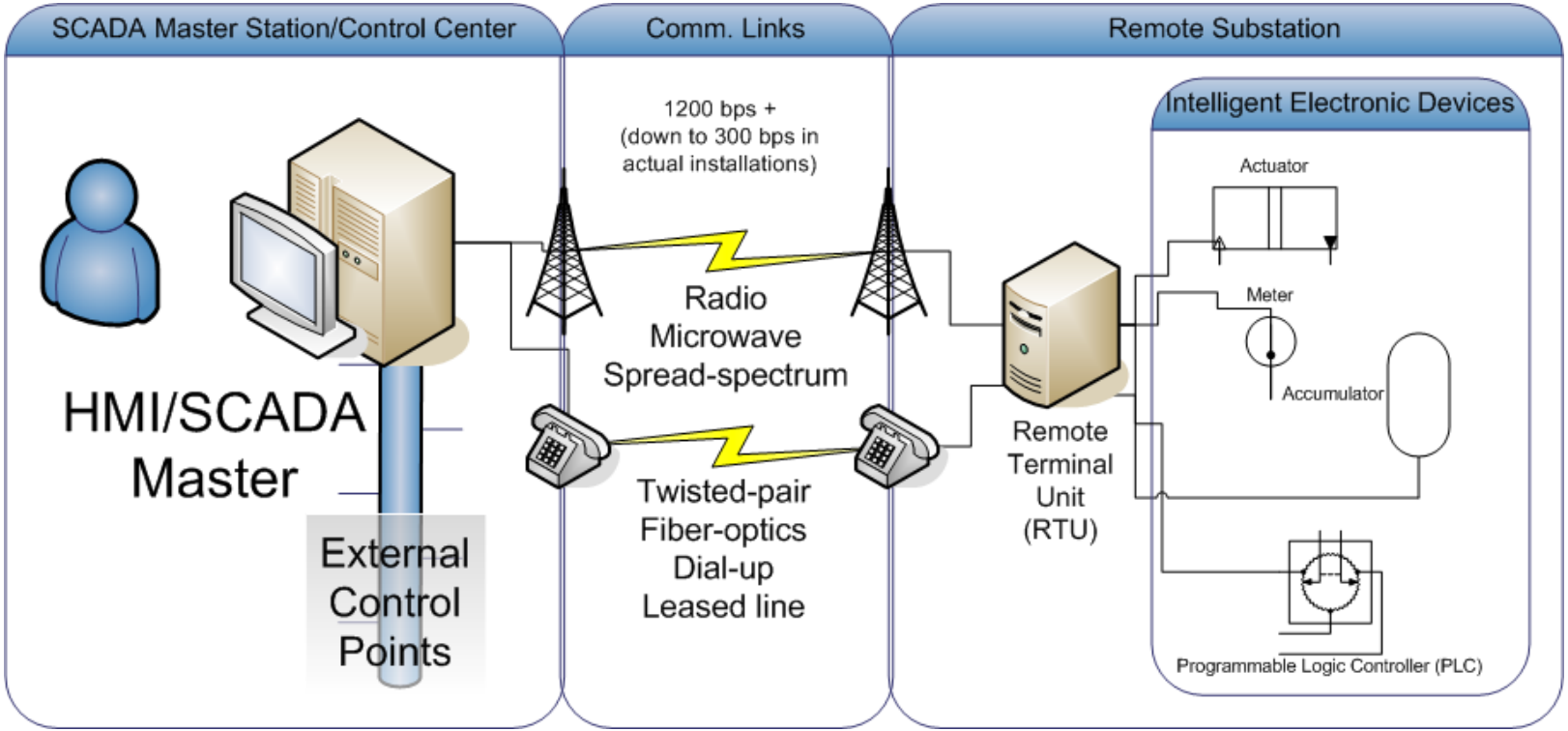
Fuzzing and protocol analysis

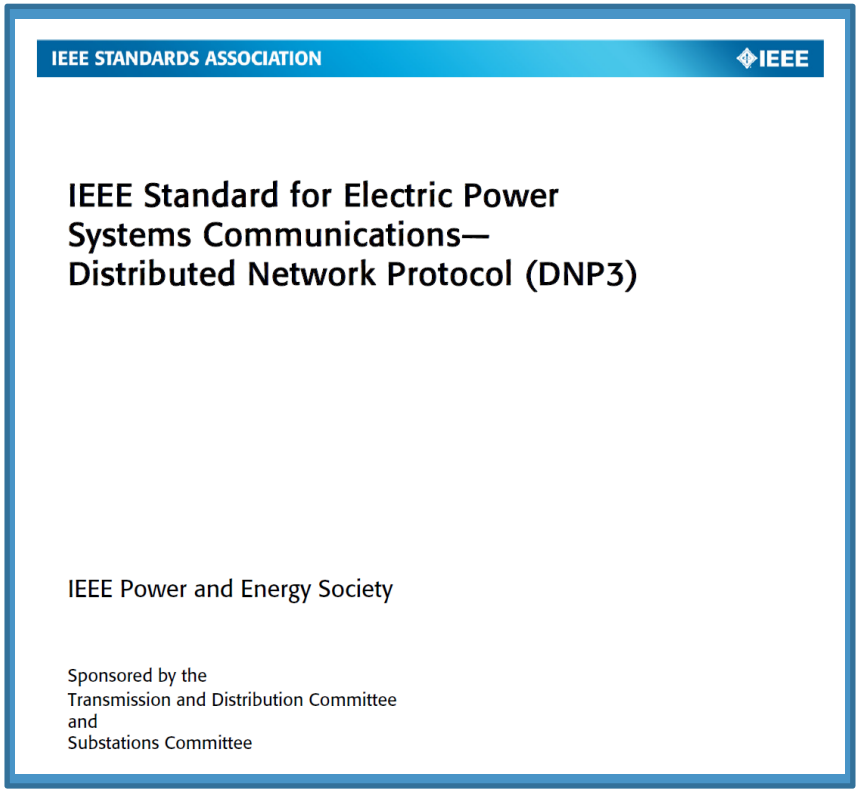
case-study of DNP3

Adam Crain, Automatak

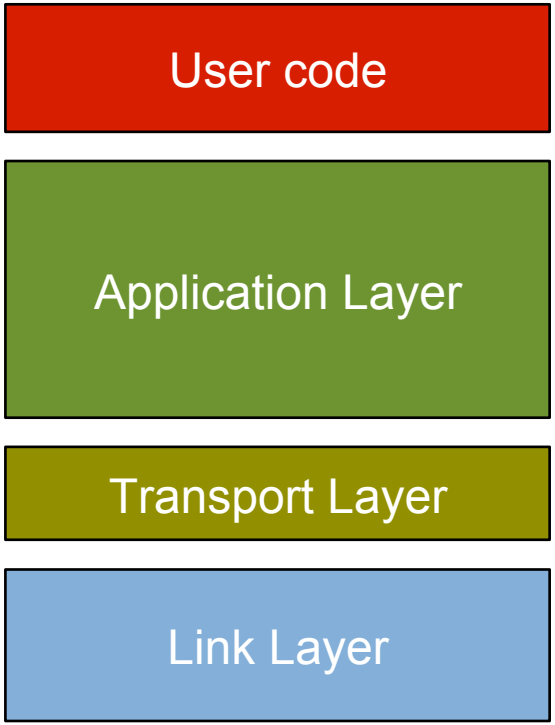

SCADA Master Station/Control Center
Comm. Links
Remote Substation
1200 bps +
(down to 300 bps in
actual installations)
Intelligent Electronic Devices
Actuator
Meter
Accumulator
HMI/SCADA
Master
Radio
Microwave
Spread-spectrum
Twisted-pair
Fiber-optics
Dial-up
Leased line
Remote
Terminal
Unit
(RTU)
External
Control
Points
Programmable Logic Controller (PLC)

Developed by Harris Corp, handed over to a vendor-neutral User Group in **1993.**

Many features have been “bolted on”, including security.



Layered Architecture



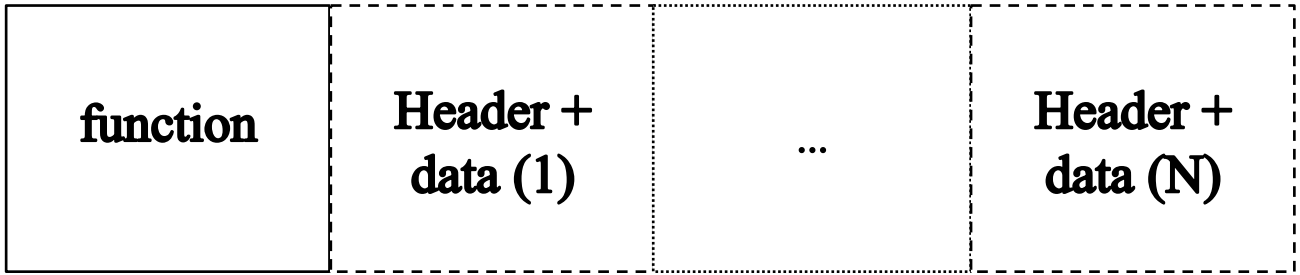
IED/RTU or your SCADA master

Application Service Data Unit (ASDU)
Typical max size of 2KB
semantics == functions + objects

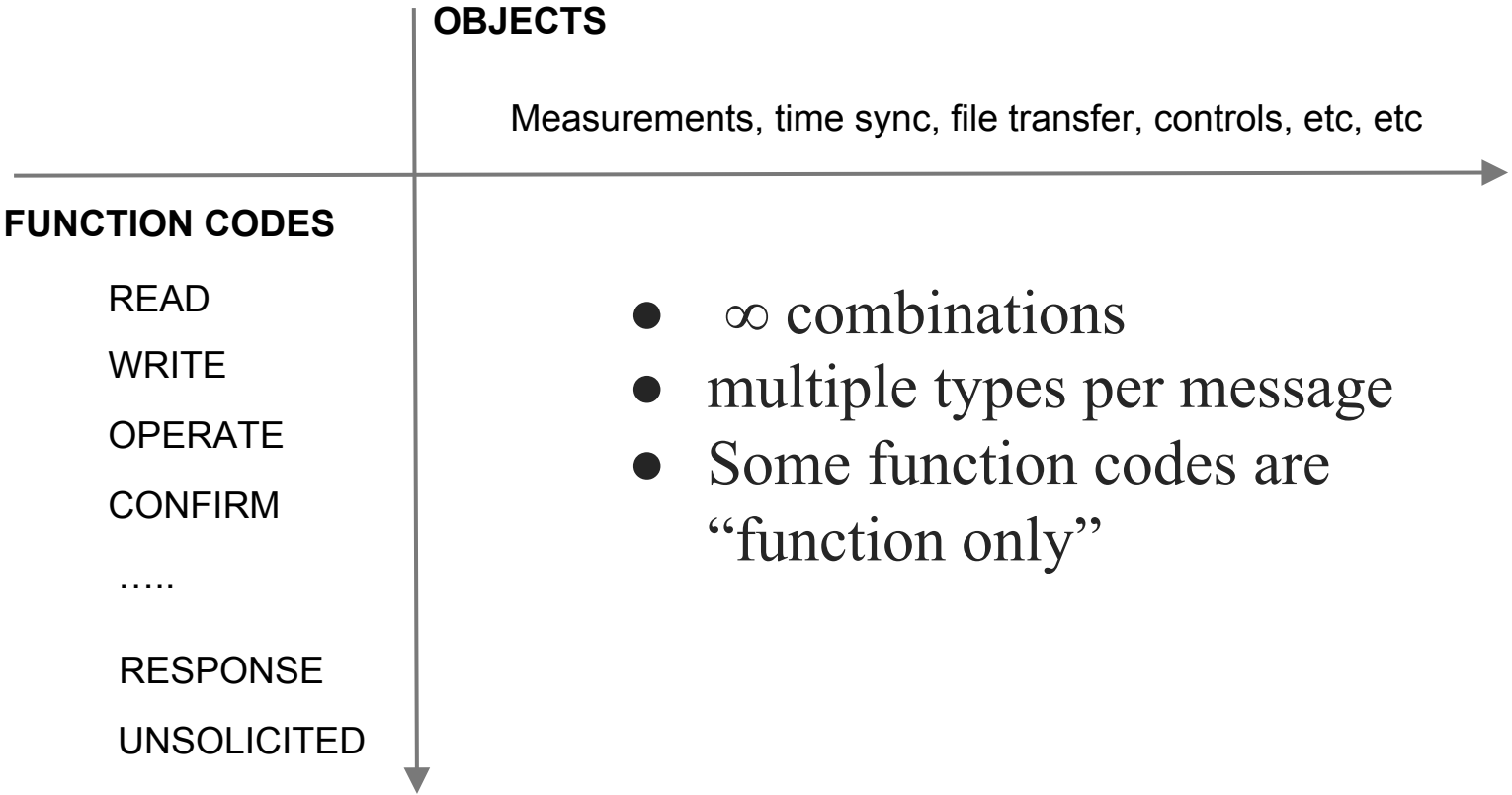
Tx segmentation
Rx re-assembly of APDUs

Adds CRCs and addressing. Error checking and (de) multiplexing.

Application layer messages



Application-layer semantics

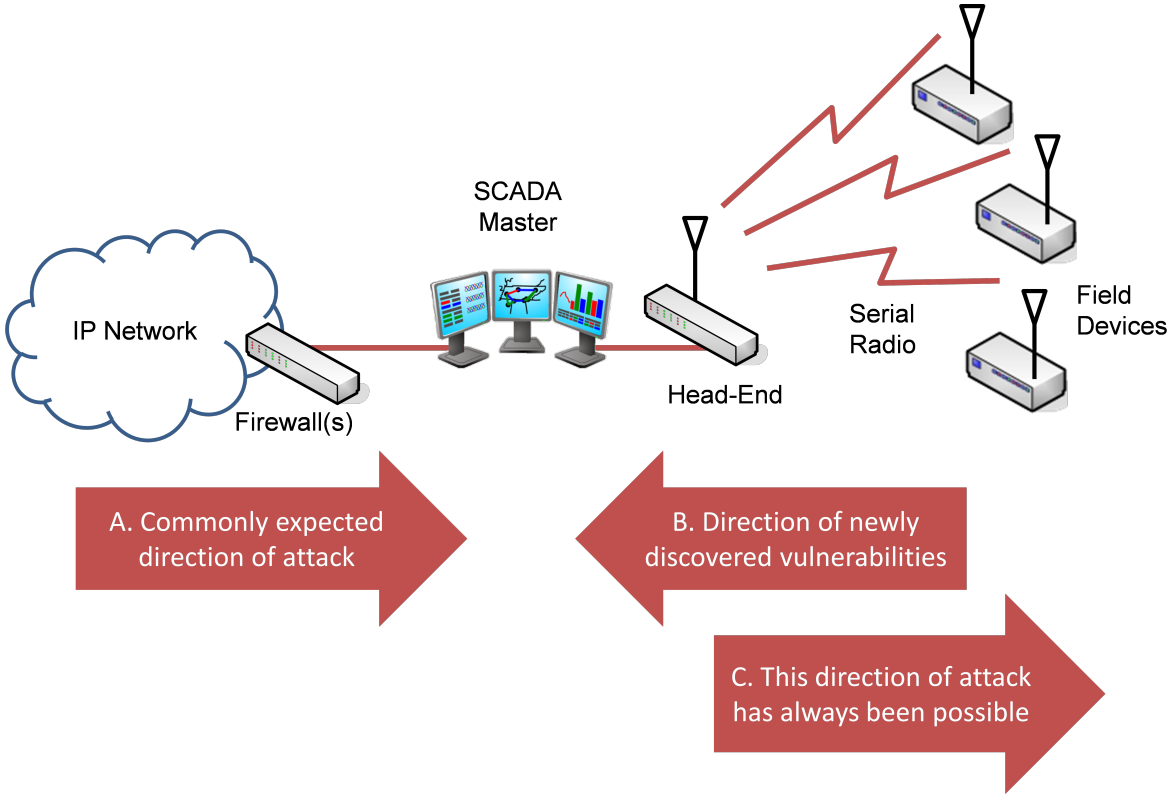


- ∞ combinations
- multiple types per message
- Some function codes are "function only"

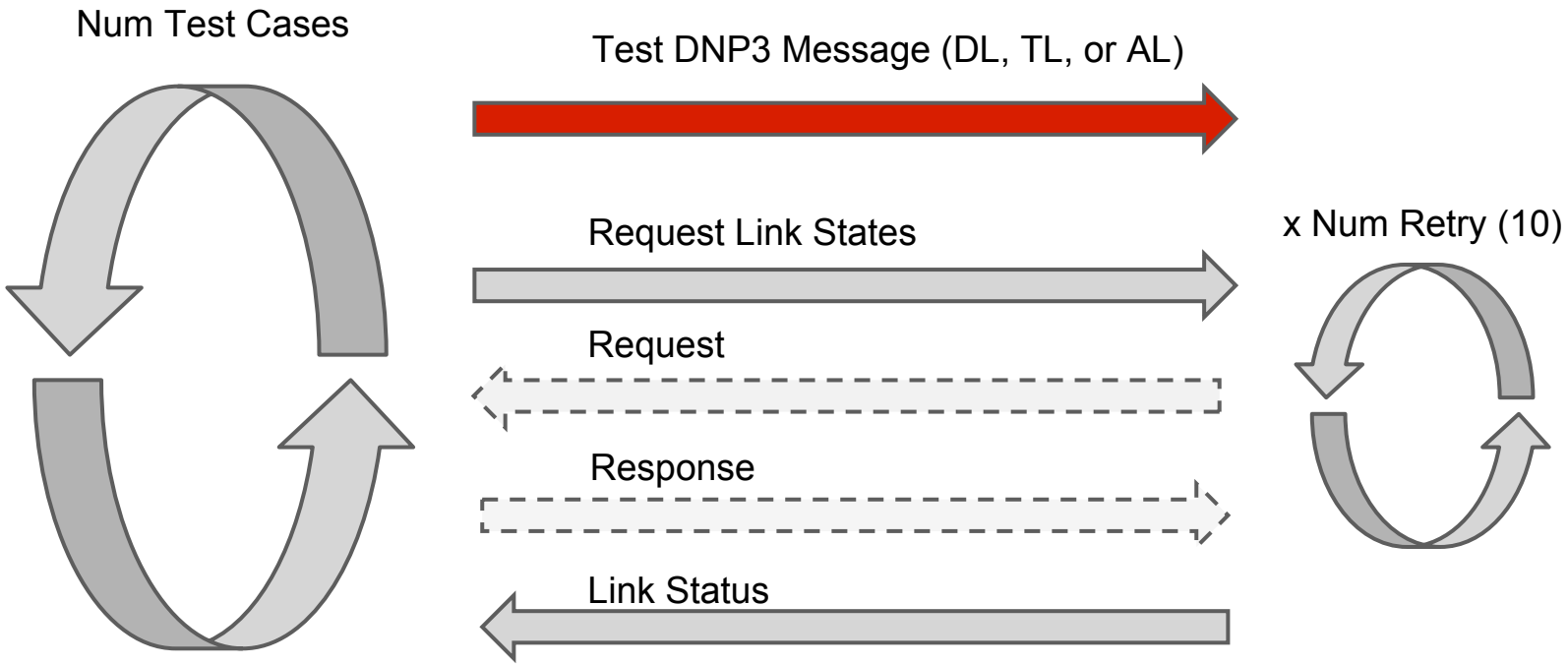
Project *Robus*

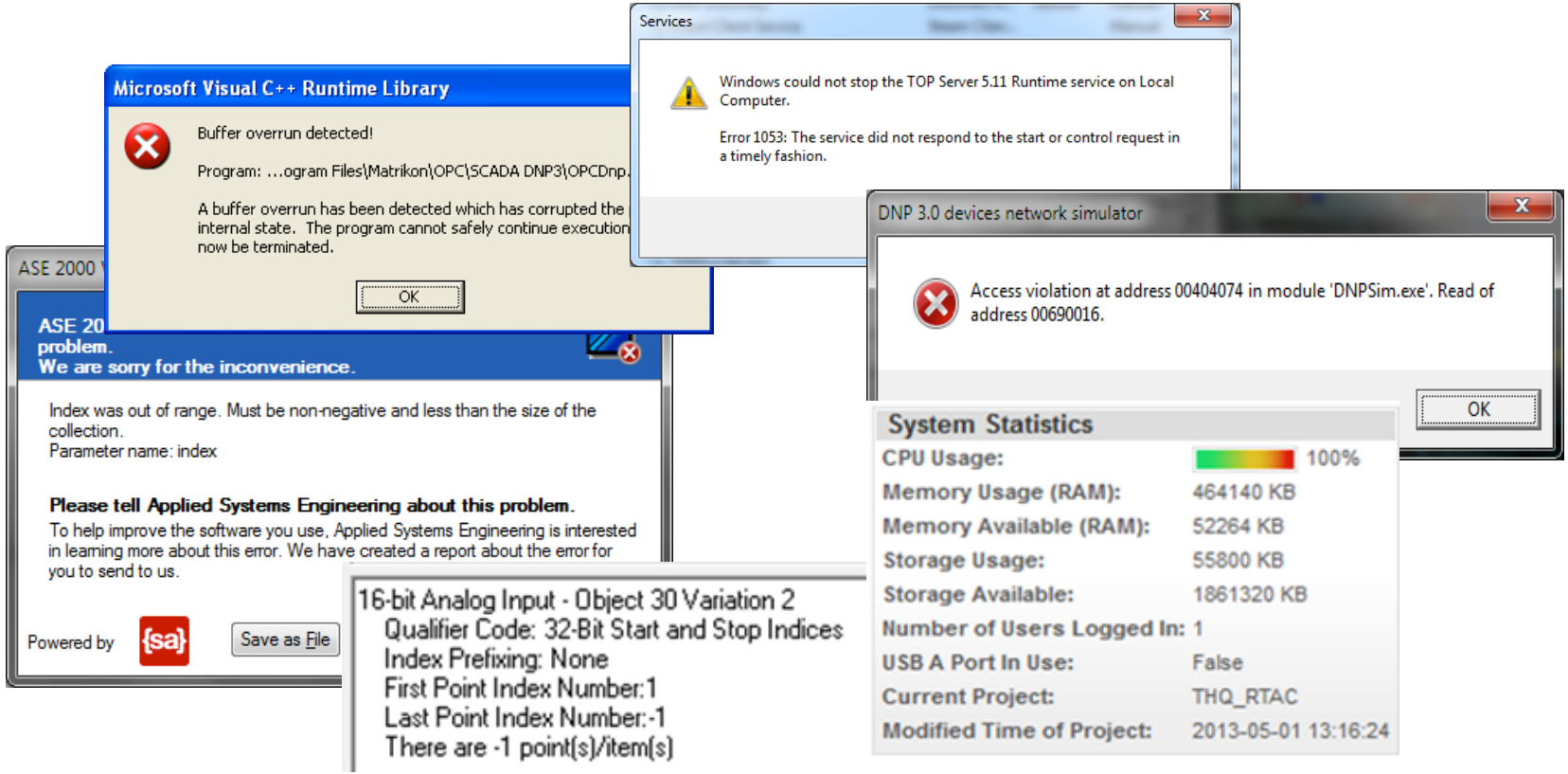
- Started in April 2013
- 30+ CVEs found via fuzzing
- Deep study of failure modes in one protocol
- automatak.com/robus

Focus on serial / masters

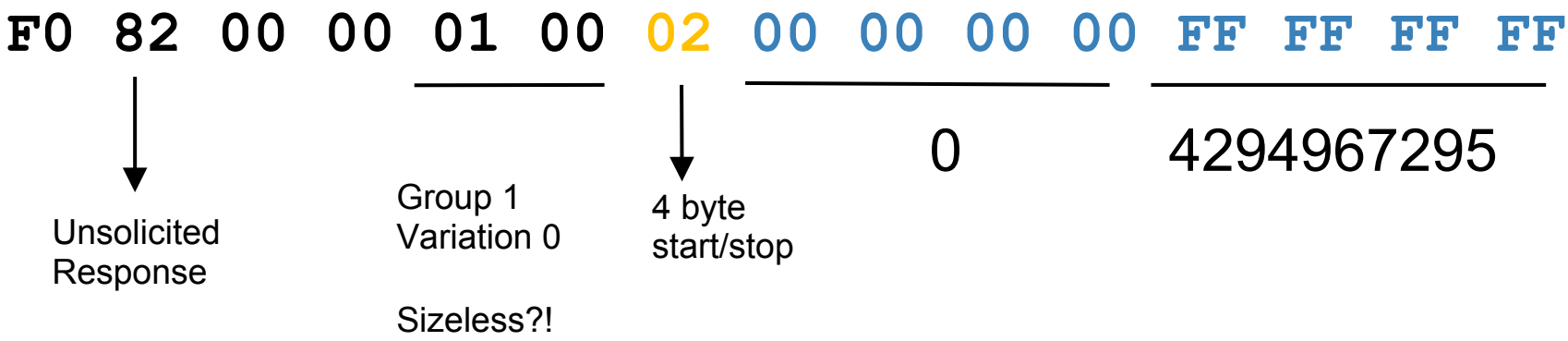


DNP3 Fuzzing




Services
Windows could not stop the TOP Server 5.11 Runtime service on Local Computer.
Error 1053: The service did not respond to the start or control request in a timely fashion.
Microsoft Visual C++ Runtime Library
Buffer overrun detected!
Program: ...ogram Files\Matrikon\OPC\SCADA DNP3\OPCDnp.
A buffer overrun has been detected which has corrupted the internal state. The program cannot safely continue execution now be terminated.
OK
DNP 3.0 devices network simulator
Access violation at address 00404074 in module 'DNPSim.exe'. Read of address 00690016.
OK
ASE 2000
ASE 20
problem.
We are sorry for the inconvenience.
Index was out of range. Must be non-negative and less than the size of the collection.
Parameter name: index
Please tell Applied Systems Engineering about this problem.
To help improve the software you use, Applied Systems Engineering is interested in learning more about this error. We have created a report about the error for you to send to us.
Powered by
{sa}
Save as File
16-bit Analog Input - Object 30 Variation 2
Qualifier Code: 32-Bit Start and Stop Indices
Index Prefixing: None
First Point Index Number:1
Last Point Index Number:-1
There are -1 point(s)/item(s)
System Statistics
CPU Usage: 100%
Memory Usage (RAM): 464140 KB
Memory Available (RAM): 52264 KB
Storage Usage: 55800 KB
Storage Available: 1861320 KB
Number of Users Logged In: 1
USB A Port In Use: False
Current Project: THQ_RTAC
Modified Time of Project: 2013-05-01 13:16:24

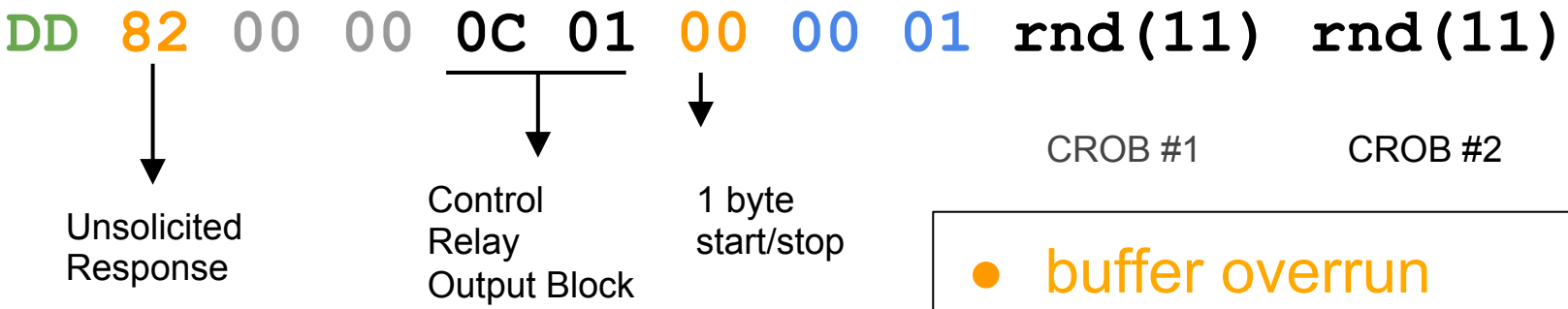
Common Faults



uint32_t count = stop - start + 1; // ← integer overflow

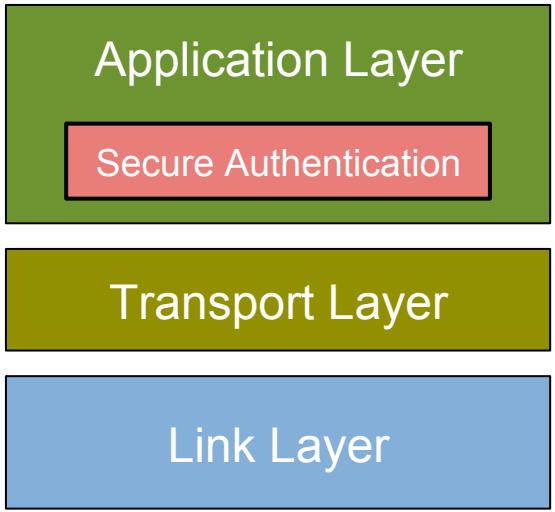
Less Common Faults

Unexpected function code / object combinations



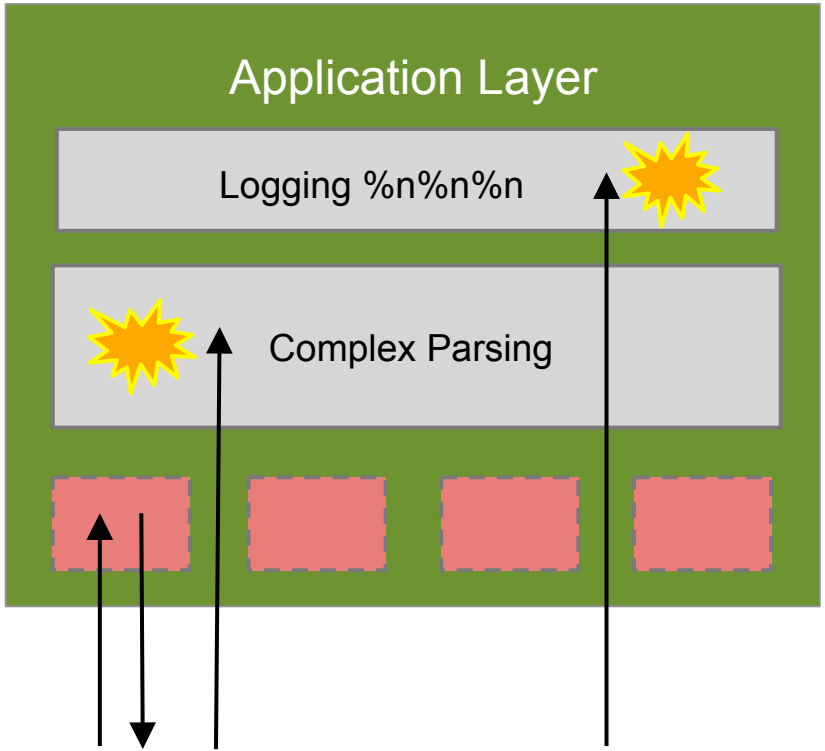
- buffer overrun
- not malformed!
- unexpected objects
- accepts broadcast

DNP3 Security



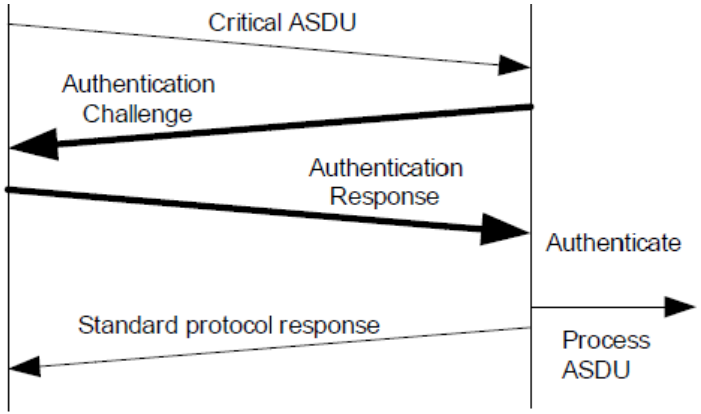
- Tightly coupled to the DNP3 application layer
- Auth-only
- New functions
- New objects
- 2 modes of authentication

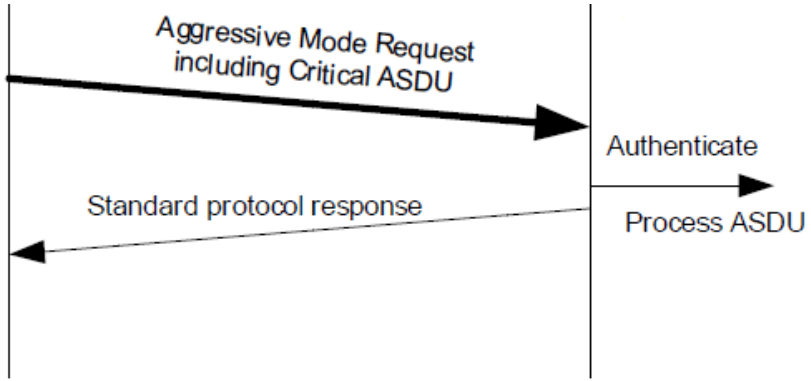
Porous Trust Boundary



- **Data is dangerous, intended function matters not.**
- **Every time you extend DNP3, you make it less secure.**
- **Optional challenges make security state machine overly complex**

2 modes of authentication

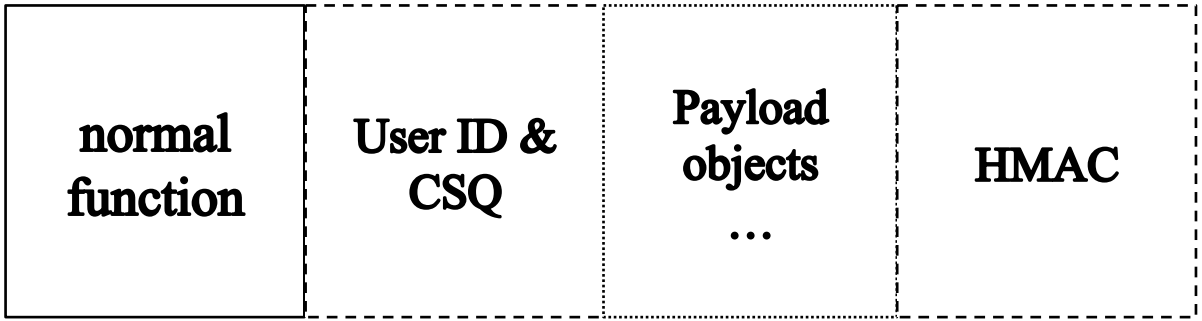




Challenge-response – 2 pass authentication

“Aggressive mode” – 1 pass authentication

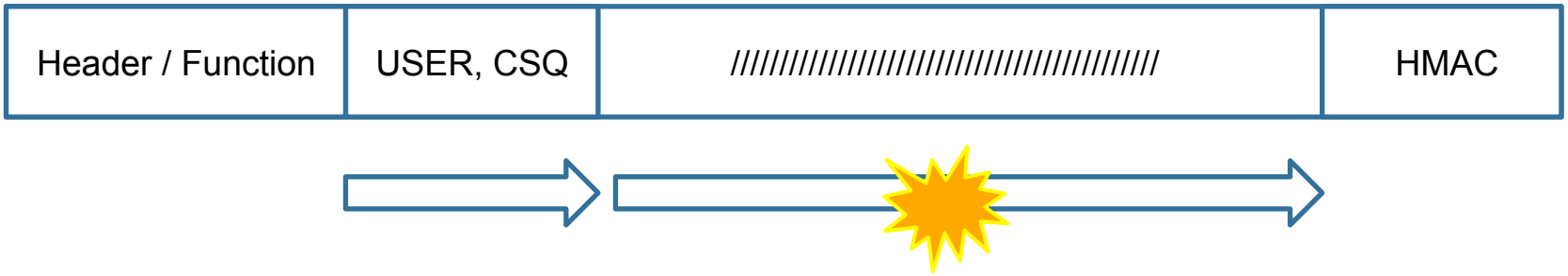
Aggressive mode message



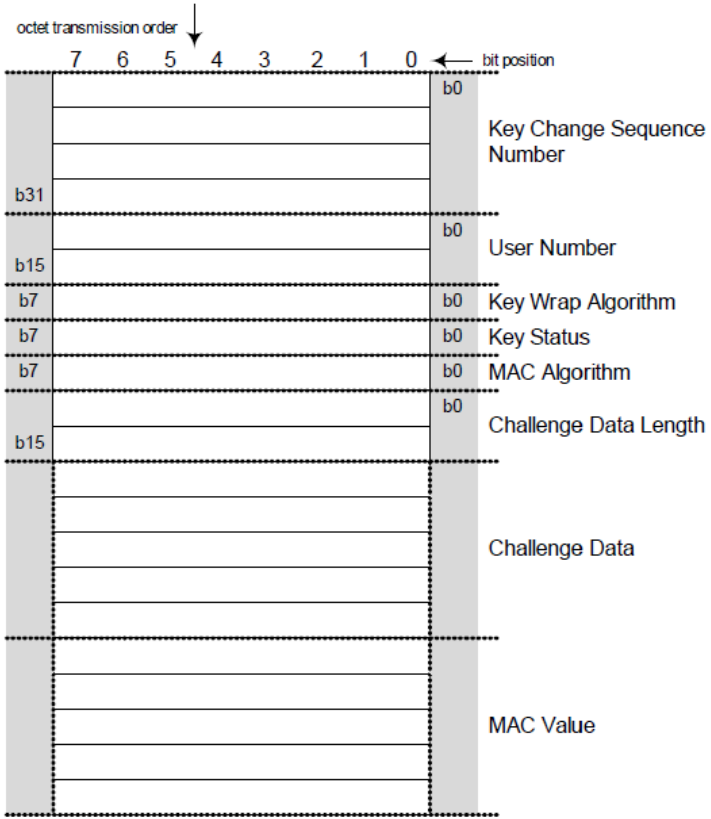
Issue #1: Aggressive-mode ambiguity

You can only tell if this is an aggressive mode request by speculatively parsing the 1st object header. Ambiguity is dangerous.

Issue #2: Lack of an envelope for HMAC



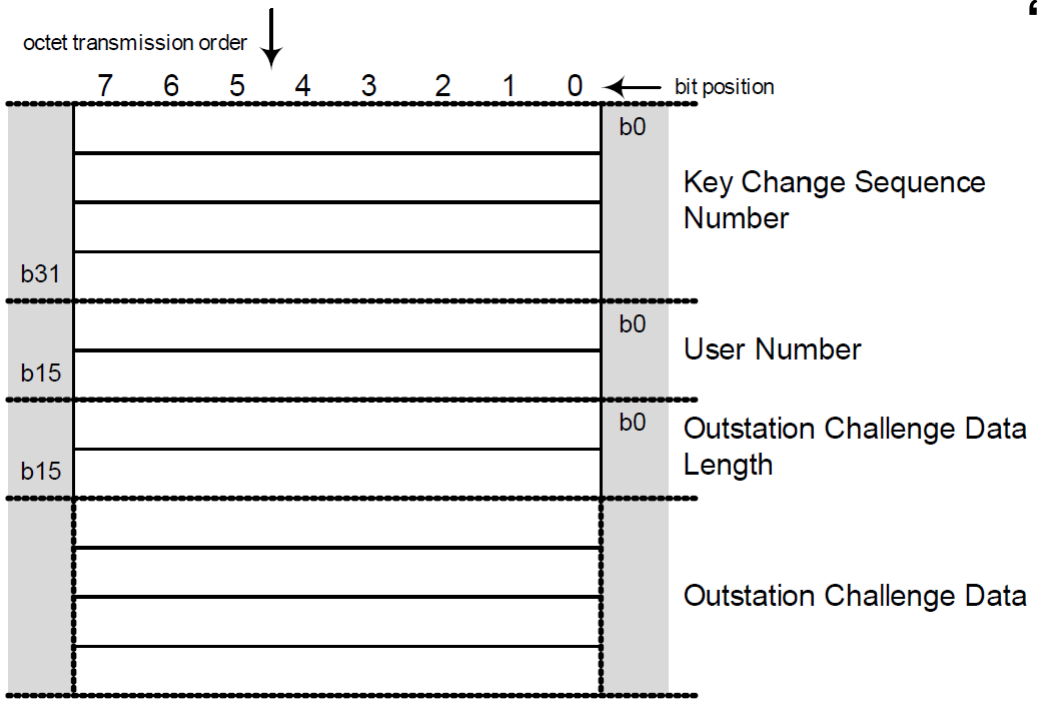
DNP3 headers cannot be “skipped”. They must be parsed sequentially (at least lightly), so that you known where the next one starts.



“Session key status object”

- Total size framed by TLV in wrapping header
- Composed of fixed-size and variable-length subfields
- Final v-length field is the remainder of the encapsulation.

“Update key change reply”



- Total size framed by TLV in wrapping header
- Composed of fixed-size and variable-length subfields
- Final v-length field is the remainder of the encapsulation **AND** a length prefix.

What does the spec have to say?

A.45.12.2.3 Notes

This object shall always be used with a Qualifier of 0x5B, indicating that the object is of variable length up to 65 535 octets, specified in the Object Prefix. The length of the Challenge Data may therefore be either calculated from the qualifier or read from the corresponding field of the object.

SA Conclusions

- Prefer a layered approach to SCADA security to that decouples legacy protocol encodings/semantics from security.
- Design security to address both function and implementation attack surface.

How can langsec help?

- Critical infrastructure vendors need better tools besides hand-rolled parsers.
- Standards bodies need the theory/guidance to produce better designs.
- Protocols need reference implementations to guide their evolution.

Questions?