The Importance of Testing Smart Grid IEDs against Security Vulnerabilities

Eroshan Weerathunga, Anca Cioraca

GE Grid Solutions

2016 Texas A&M Relay Conference

Topics

- **Vulnerabilities and Attacks**
- Assessment and Attack Simulation
- Regulatory Standards
- Secure Software Development

Vulnerabilities

- Unchanged default passwords
- Bad designs and coding practices
- Test and debug features left in the production build
- Unencrypted / Unsigned sensitive information
- No limit conditions in incoming packet rates
- Weak password policies and no limit in number of authentication failed attempts
- Vulnerabilities from third party software components and operating systems

Attacks

- Passive - Monitoring of communications sent over public media
- Active - Attempts to circumvent or break security features, introduce malicious code
- Close -in – An unauthorized individual gains close physical proximity through clandestine entry, open access, or both
- Insider– Attacks by an authorized person
- Distribution - Malicious modification before installation

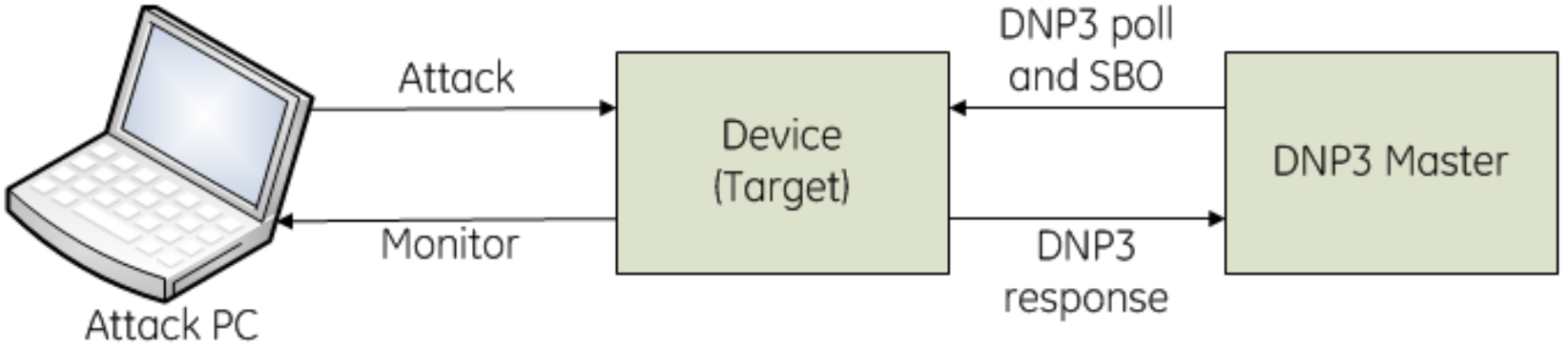
Topics

- Vulnerabilities and Attacks
- **Assessment and Attack Simulation**
- Regulatory Standards
- Secure Software Development

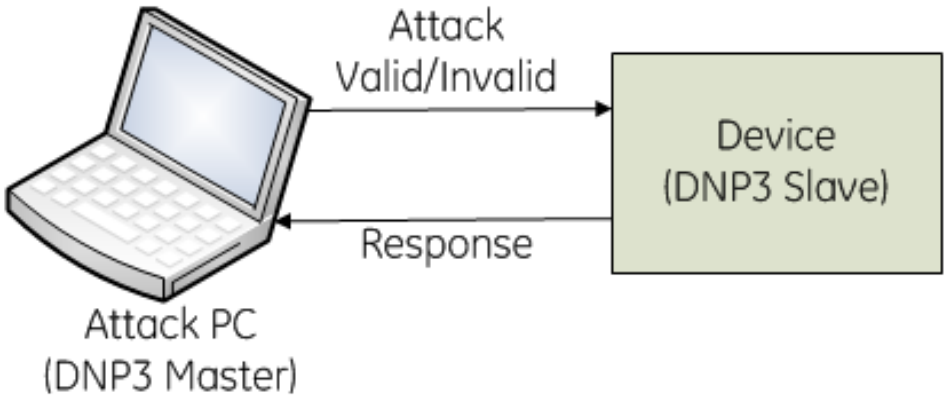
Vulnerability Assessment

- Scan– Probe a device to find open ports
- Storm - Sending packets in a higher rate to a target device to execute a denial of service attack
- Fuzzer - Injecting malformed, unexpected, or random data
- Grammar - Iterate over each field and choose fuzz values in a predetermined way

Attack Simulation



Test setup for attack simulation



Test setup for DNP3 attack

Port Scans

- TCP Scan

  A SYN packet is sent (as if we are going to open a connection), if the target host responds with a SYN+ACK, this indicates the port is listening

- UDP Scan

  Sends empty UDP datagrams. If the port is closed, device send back an “ICMP Port Unreachable” message

ARP Tests

- ARP request storm
- ARP host reply storm
- ARP Cache saturation storm
- ARP grammar

40	1.07681300	4a:ec:29:cd:ba:ab	SbsTechn_0b:72:d2	ARP	60 10.100.3.1 is at 4a:ec:29:cd:ba:ab
41	1.07784200	f2:fb:e3:46:7c:c2	SbsTechn_0b:72:d2	ARP	60 10.100.3.2 is at f2:fb:e3:46:7c:c2
42	1.07784300	54:f8:1b:e8:e7:8d	SbsTechn_0b:72:d2	ARP	60 10.100.3.3 is at 54:f8:1b:e8:e7:8d
43	1.07883000	76:5a:2e:63:33:9f	SbsTechn_0b:72:d2	ARP	60 10.100.3.4 is at 76:5a:2e:63:33:9f
44	1.07981600	c9:9a:66:32:0d:b7	SbsTechn_0b:72:d2	ARP	60 10.100.3.5 is at c9:9a:66:32:0d:b7
45	1.07993100	31:58:a3:5a:25:5d	SbsTechn_0b:72:d2	ARP	60 10.100.3.6 is at 31:58:a3:5a:25:5d
46	1.08096300	05:17:58:e9:5e:d4	SbsTechn_0b:72:d2	ARP	60 10.100.3.7 is at 05:17:58:e9:5e:d4
47	1.08196900	ab:b2:cd:c6:9b:b4	SbsTechn_0b:72:d2	ARP	60 10.100.3.8 is at ab:b2:cd:c6:9b:b4
48	1.08196900	54:11:0e:82:74:41	SbsTechn_0b:72:d2	ARP	60 10.100.3.9 is at 54:11:0e:82:74:41
49	1.08295900	21:3d:dc:87:70:e9	SbsTechn_0b:72:d2	ARP	60 10.100.3.10 is at 21:3d:dc:87:70:e9

ARP Cache saturation storm

IP Tests

- IP unicast storm
- IP broadcast storm
- IP fragmented storm

2052	19.0730910	107.181.39.110	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=001f)
2053	19.0854850	90.190.79.81	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=001f)
2054	19.0977660	144.237.104.76	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=001f)
2055	19.0991270	10.100.3.100	10.100.3.50	ICMP	98 Echo (ping) request id=0x0db9, seq=30253/11638, ttl=64 (
2056	19.0993580	10.100.3.50	10.100.3.100	ICMP	98 Echo (ping) reply id=0x0db9, seq=30253/11638, ttl=64 (
2057	19.1101790	60.206.190.69	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=4440, ID=001f)
2058	19.1225770	104.212.96.22	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=5920, ID=001f)
2059	19.1349660	161.203.144.118	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=7400, ID=001f)
2060	19.1472260	211.95.188.124	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=8880, ID=001f)
2061	19.1595870	48.100.7.25	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=10360, ID=001f)
2062	19.1719360	196.245.133.43	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=11840, ID=001f)
2063	19.1844460	57.9.210.68	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=13320, ID=001f)
2064	19.1968020	96.169.118.18	10.100.3.50	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=14800, ID=001f)
2065	19.1990960	10.100.3.100	10.100.3.50	ICMP	98 Echo (ping) request id=0x0dba, seq=60514/25324, ttl=64 (
2066	19.1992000	10.100.3.50	10.100.3.100	ICMP	98 Echo (ping) reply id=0x0dba, seq=60514/25324, ttl=64 (

IP fragmented storm

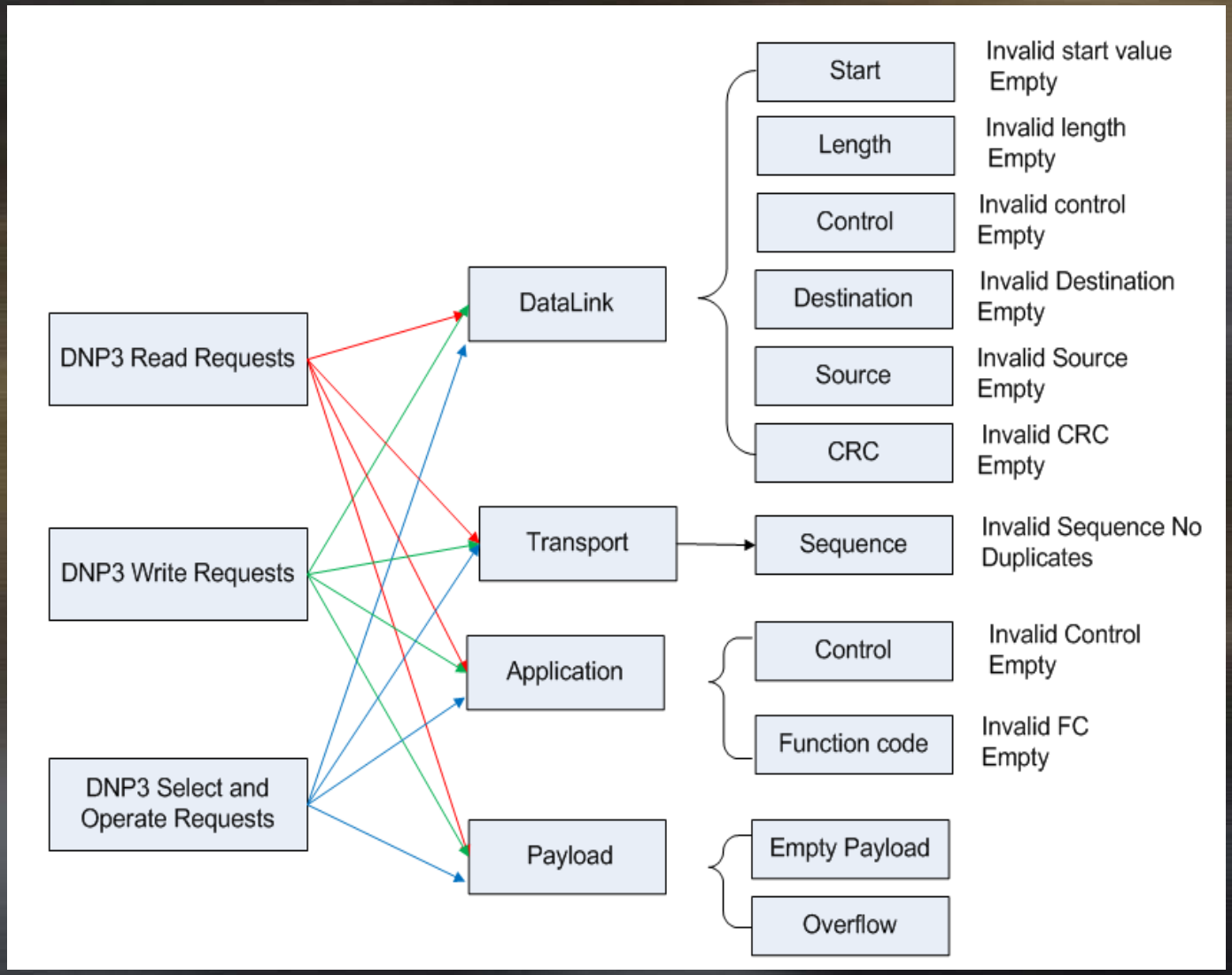
TCP/IP Tests

- TCP/IP Land attack
- TCP SYN storm

77	1.42252100	10.100.3.1	10.100.3.50	TCP	60 40218→21 [SYN] Seq=0 Win=5000 Len=0
78	1.42370900	10.100.3.1	10.100.3.50	TCP	60 37883→21 [SYN] Seq=0 Win=5000 Len=0
79	1.42371000	10.100.3.1	10.100.3.50	TCP	60 46546→21 [SYN] Seq=0 Win=5000 Len=0
80	1.42462900	10.100.3.1	10.100.3.50	TCP	60 37915→21 [SYN] Seq=0 Win=5000 Len=0
81	1.42564300	10.100.3.1	10.100.3.50	TCP	60 45619→21 [SYN] Seq=0 Win=5000 Len=0
82	1.42574800	10.100.3.1	10.100.3.50	TCP	60 41782→21 [SYN] Seq=0 Win=5000 Len=0
83	1.42676100	10.100.3.1	10.100.3.50	TCP	60 38396→21 [SYN] Seq=0 Win=5000 Len=0
84	1.42787000	10.100.3.1	10.100.3.50	TCP	60 41282→21 [SYN] Seq=0 Win=5000 Len=0
85	1.42787100	10.100.3.1	10.100.3.50	TCP	60 47028→21 [SYN] Seq=0 Win=5000 Len=0
86	1.42877000	10.100.3.1	10.100.3.50	TCP	60 43592→21 [SYN] Seq=0 Win=5000 Len=0
87	1.42975600	10.100.3.1	10.100.3.50	TCP	60 43067→21 [SYN] Seq=0 Win=5000 Len=0

TCP SYN storm

DNP3 Fuzzer/Grammar



DNP3 protocol fuzzing

DNP3 Fuzzer/Grammar – cont.

```
Distributed Network Protocol 3.0
  Data Link Layer, Len: 11, From: 1, To: 2, RES, Unknown function (0x0c)
      Start Bytes: 0x0564
      Length: 11
    Control: 0x2c (RES, Unknown function (0x0c))
        0... .... = Direction: Not set
        .0.. .... = Primary: Not set
        ...0 .... = Data Flow Control: Not set
        .... 1100 = Control Function Code: Unknown (12)
      Destination: 2
      Source: 1
      CRC: 0x3859 [correct]
  Transport Layer: 0xc1 (FIR, FIN, Sequence 1)
      1... .... = Final: Set
      .1.. .... = First: Set
      ..00 0001 = Sequence: 1
    Application data chunks
        Application Chunk 0 Len: 6 CRC 0x76b5
  Application Layer: (FIR, FIN, Sequence 1, Read)
    Control: 0xc1 (FIR, FIN, Sequence 1)
        1... .... = First: Set
        .1.. .... = Final: Set
        ..0. .... = Confirm: Not set
        ...0 .... = Unsolicited: Not set
        .... 0001 = Sequence: 1
      Function Code: Read (0x01)
    READ Request Data Objects
      Object(s): Class 1 Data (Obj:60, Var:02) (0x3c02)
        Qualifier Field, Prefix: None, Code: No Range Field
            .000 .... = Index Prefix: None (0)
            .... 0110 = Qualifier Code: No Range Field (6)
          Number of Items: 0
```

Invalid datalink control

```
Distributed Network Protocol 3.0
  Data Link Layer, Len: 10, From: 1, To: 2, DIR, PRM, Unconfirmed User Data
      Start Bytes: 0x0564
      Length: 10
    Control: 0xc4 (DIR, PRM, Unconfirmed User Data)
      Destination: 2
      Source: 1
      CRC: 0x9164 [correct]
  Transport Layer: 0xf8 (FIR, FIN, Sequence 56)
      1... .... = Final: Set
      .1.. .... = First: Set
      ..11 1000 = Sequence: 56
    Application data chunks
  Application Layer: (FIR, Sequence 7, Unknown function (0xbf))
    Control: 0x87 (FIR, Sequence 7)
        1... .... = First: Set
        .0.. .... = Final: Not set
        ..0. .... = Confirm: Not set
        ...0 .... = Unsolicited: Not set
        .... 0111 = Sequence: 7
      Function Code: Unknown function (0xbf) (0xbf)
```

Unknown function code

Topics

- Vulnerabilities and Attacks
- Assessment and Attack Simulation
- **Regulatory Standards**
- Secure Software Development

Regulatory Standards

- NERC CIP v5
  - Section 004, requirement 4.1 “process to authorize based on need, as determined by the Responsible Entity”
  - Section 007, requirement 4.1 regarding Security Event Monitoring
  - Section 007, requirement 1.1,“enable only logical network accessible ports that have been determined to be needed by the Responsible Entity”

Regulatory Standards – cont.

- IEEE 1686 – 2013
  - Provides a set of features, functions, and practices for IEDs and IED configuration software
  - Communications port access
  - Authorization using role-based access control (RBAC)
  - Audit trail

Topics

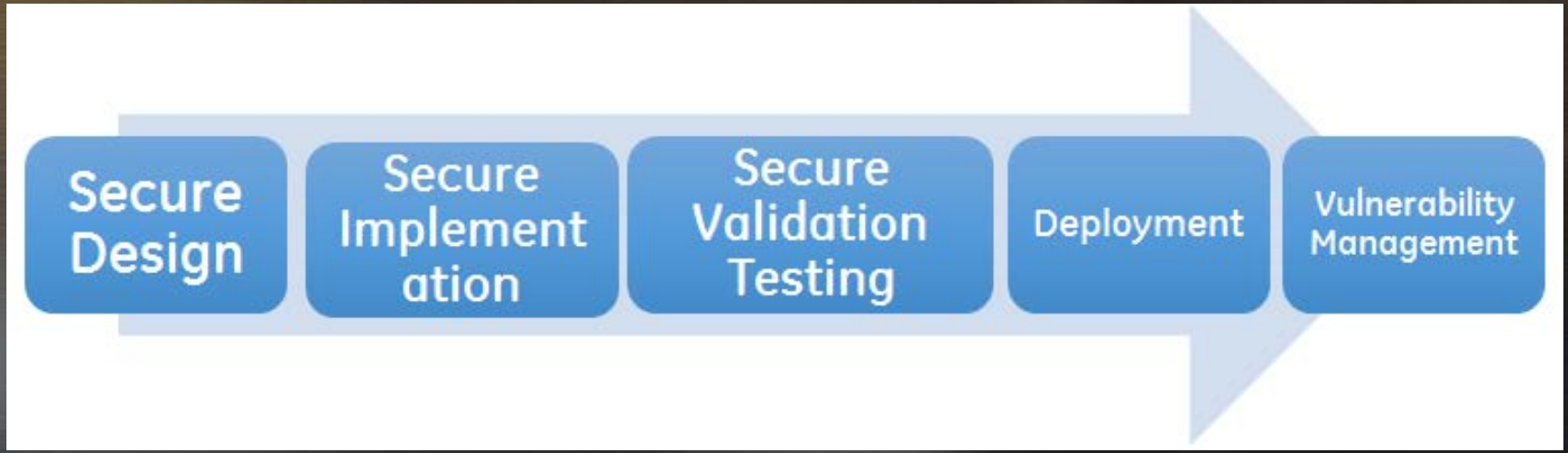
- Vulnerabilities and Attacks
- Assessment and Attack Simulation
- Regulatory Standards
- **Secure Software Development**

Secure Software Development

- Problem analysis
- Requirements
- Design
- Implementation
- Testing
- Deployment
- Maintenance

Secure Software Development –cont.

- Secure coding practices
  - Static analysis, peer review, unit testing
- Secure validation testing
  - Final step before product released



Conclusions

- Importance of security testing
  - Standard compliance
  - Customer satisfaction
  - Avoid damages to brand reputation
- Vulnerability product assessment
- Secure software development

Thank You

Questions?