Justin Searle <justin@utilisec.com>

RE: Smart Grid C12.22 WireShark

Martin, Van <Van.Martin@itron.com> **Wed, Nov 2, 2011 at 10:47 AM**
To: Justin Searle <justin@utilisec.com>

Justin before you share information, Please verify through us first so we do not have privacy issues

Working with someone tomorrow to get some roughly raw traffic

RFLan C12.22 is wrapped in TCP so we will get C12.22 traffic after TCP is removed

Is below snippit helpful:

From Meter saying the it is now Registered at end of Multicast

```
<AUDT-apdu>
  <called-AP-title>
    <absolute-id>2.16.124.113620.1.22.0.1.1.64.33</absolute-id>
  </called-AP-title>
  <called-AP-invocation-id>951</called-AP-invocation-id>
  <calling-AP-title>
    <absolute-id>2.16.124.113620.1.22.0.1.1.64.10001.85390</absolute-id>
  </calling-AP-title>
  <calling-AP-invocation-id>28762</calling-AP-invocation-id>
  <mechanism-name>2.16.840.1.114416.5</mechanism-name>
  <calling-authentication-value>
    A2 21 81 1F A2 1D 80 03 00 09 00 81 10 04 B5 61
    2B 2A FB 0F 46 E6 F8 B6 CA 7E 99 69 6D 83 04 49
    B0 E4 B7
  </calling-authentication-value>
  <user-information>
    <segment></segment>
  </user-information>
</AUDT-apdu>
++++++++++++++++++++++++++++++++++++++++++++++++
```

60 81 85 A2 0E 06 0C 60 7C 86 F7 54 01 16 00 01

01 40 21 A4 04 02 02 03 B7 A6 12 06 10 60 7C 86

F7 54 01 16 00 01 01 40 CE 11 85 9B 0E A8 04 02

02 70 5A 8B 08 60 86 48 01 86 FD 70 05 AC 23 A2

21 81 1F A2 1D 80 03 00 09 00 81 10 04 B5 61 2B

2A FB 0F 46 E6 F8 B6 CA 7E 99 69 6D 83 04 49 B0

E4 B7 BE 24 28 22 81 20 A1 ED 72 E1 78 BD 0D 10

DB 76 E3 07 67 3D 39 92 9E 99 80 E2 6B 16 94 FB

2C 7C 6A 78 A7 A0 5A 3A

++

HW2.0 Meter is now Registered to Application Group

{signed-unencrypted}

Itron

Van Martin

Security Test Team

O 509-891x3269

-----Original Message-----
From: Justin Searle [mailto:justin@utilisec.com]

[Quoted text hidden]

[Quoted text hidden]

2 attachments

image001.png
68K

PGP.sig
1K