

#XIVJORNADASCCNCERT

Contadores inteligentes y ciberseguridad

Estado del escenario español



Gonzalo José Carracedo Carballal

Tarlogic Security SL

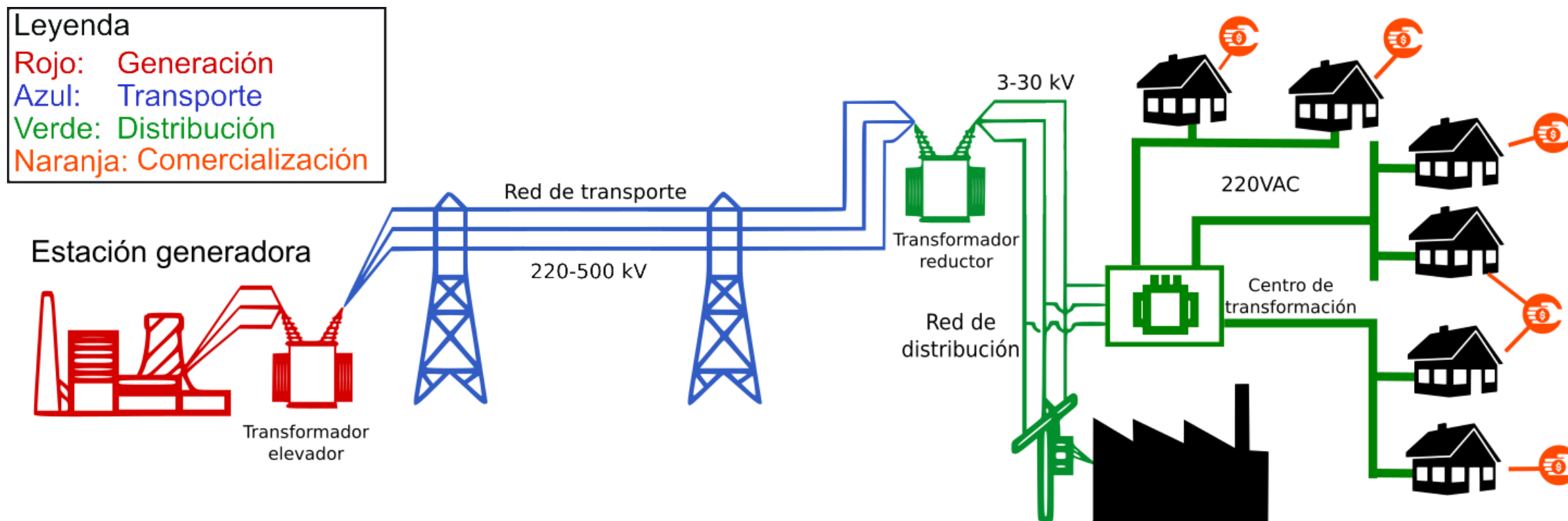
gonzalo.carracedo@tarlogic.com

La investigación hasta marzo de 2020

Contexto de partida

El sistema eléctrico en pocas palabras

Conceptos básicos



Contadores inteligentes y telegestión

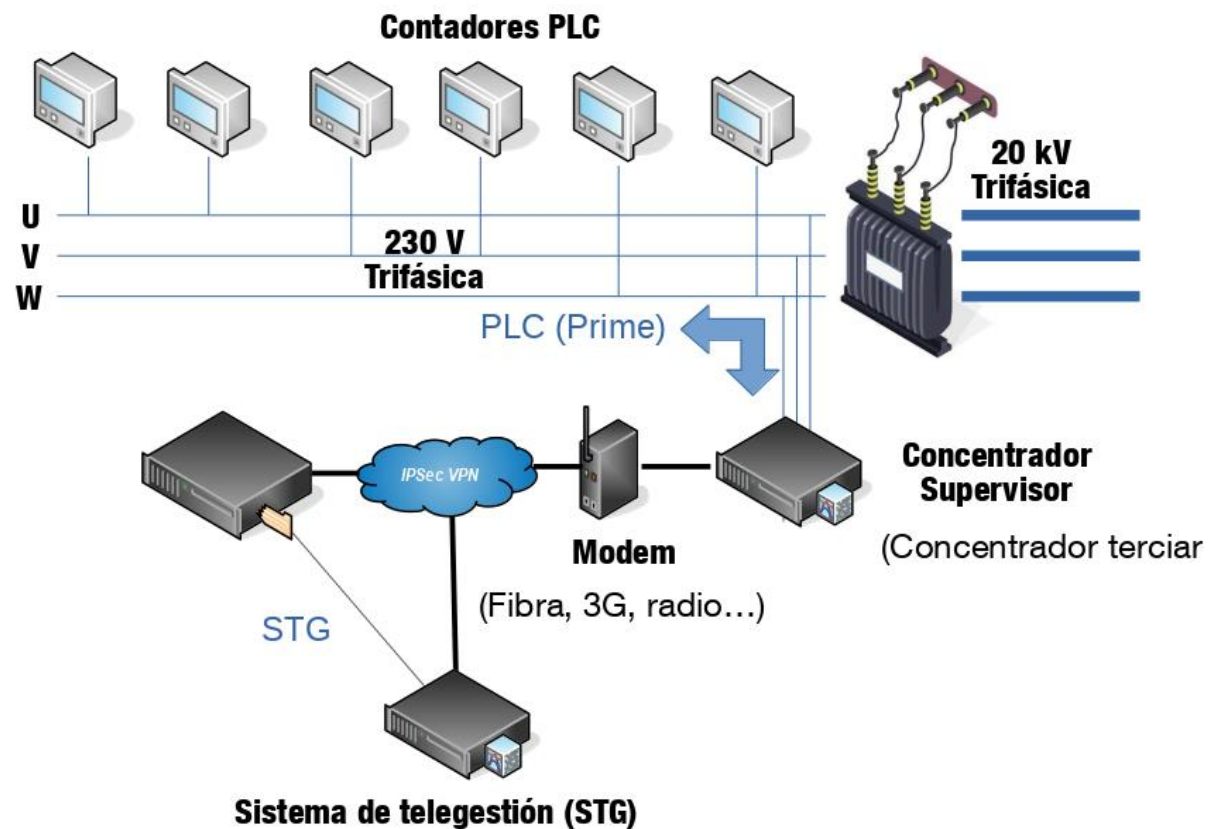
Más allá de la mera lectura de datos

- Desde enero de 2019, todos los contadores eléctricos instalados en puntos de suministro de baja potencia en España deben ofrecer funcionalidades de **telegestión**.
 - Lectura remota de medidas
 - Cambio de parámetros (potencia máxima, períodos tarifarios, relación de transformación, etc)
 - Interacción con el interruptor de control de potencia (ICP)
- Comunicación remota a través de **comunicaciones en línea de corriente (PLC)**
 - Los contadores en los puntos de suministro se comunican con la distribuidora mediante un dispositivo llamado concentrador de datos ubicado físicamente en los distintos centros de transformación.



Contadores inteligentes y telegestión

Un vistazo a las redes PLC



La problemática de PLC

- Las redes PLC (sea cual sea la tecnología específica subyacente) se aprovechan de un medio que no ha sido pensado para las comunicaciones de datos
 - Ruido impulsivo
 - Acoples inductivos entre líneas
 - Acoples entre redes a través del neutro
 - Pérdidas entre contador y concentrador
 - Visibilidad mutua entre redes diferentes
 - Visibilidad mutua entre contadores en la misma fase
- Lógicamente es una red en estrella, en la práctica recuerda más a una red inalámbrica.
- Los protocolos de comunicaciones son responsables de su buen funcionamiento.

Protocolos de comunicaciones PLC

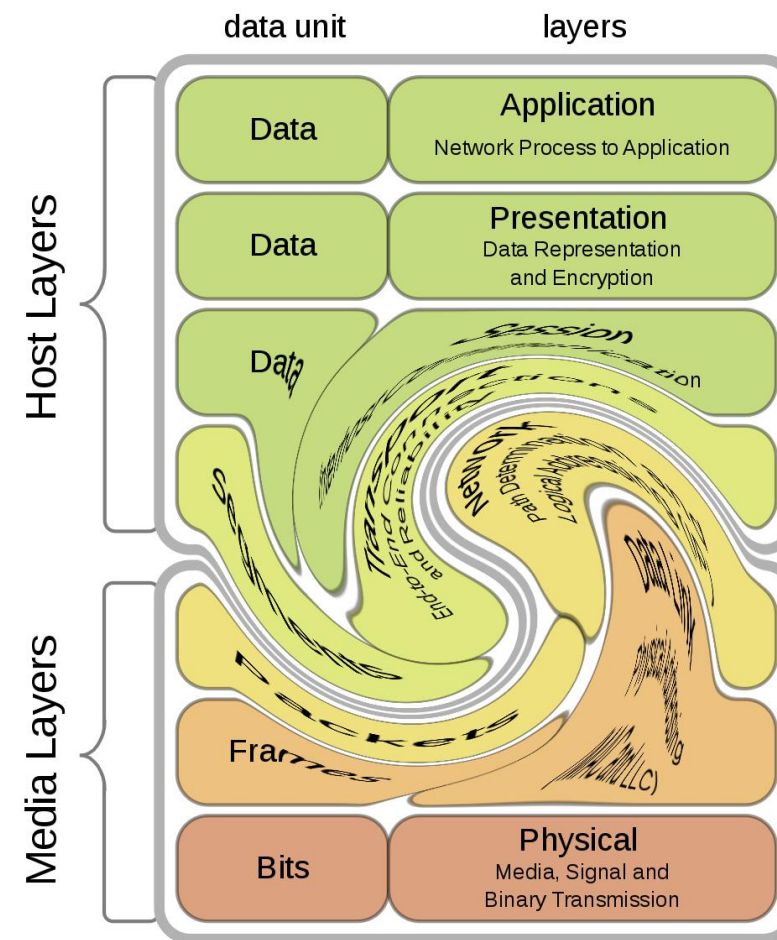
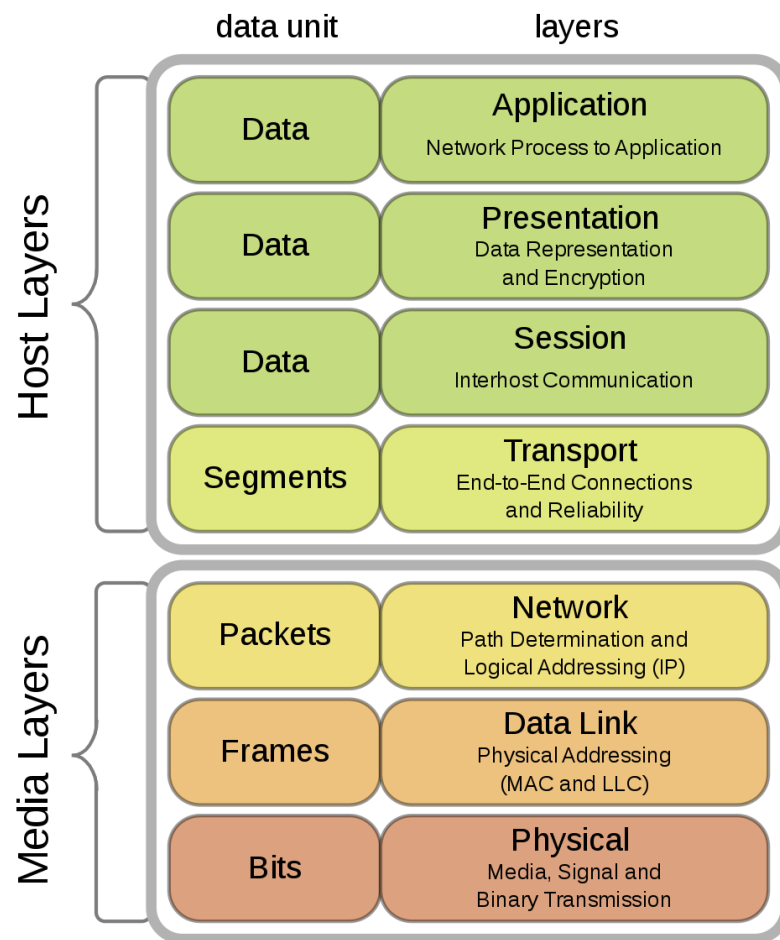
El caso español

- Dos grandes pilas de comunicaciones en el parque de contadores español, con una extensión cada una cercana al 50%.
- **Meters and More (e-distribución)**
 - Describe tanto una capa de enlace, como de aplicación y de modelo de datos
 - También ofrece una capa opcional de compatibilidad con DLMS/COSEM
- **PRIME (todas las demás)**
 - PRIME per se (capa física y de enlace)
 - DLMS (capa de aplicación)
 - COSEM (modelo de datos)

meters
AND more
OPEN TECHNOLOGIES

PRIME
ALLIANCE®

El estándar PRIME



PRIME y las limitaciones de PLC

¿Cómo gestiona PRIME las limitaciones de este medio?

- **Ruido impulsivo y acoples**
 - Misma trama se suele enviar varias veces
 - Contadores de secuencia, mecanismos ARQ
- **Pérdidas entre contador y concentrador**
 - Promoción automática de repetidores (switches)
- **Visibilidad mutua entre redes diferentes**
 - Listas negras de contadores
- **Visibilidad mutua entre contadores en la misma fase**
 - Autenticación
 - Autorización
 - Cifrado

Seguridad PRIME

Protegiendo las comunicaciones PLC

- Dos estándares PRIME: 1.3.6 y 1.4
- **PRIME 1.3.6** ofrece dos configuraciones de seguridad denominadas **perfiles**
 - **Perfil 0**: no seguridad. La información se transmite en claro.
 - **Perfil 1**: seguridad parcial. Cifrado y autenticación (via HMAC) en algunas tramas.
 - Investigadores españoles demostraron que **perfil 1** es esencialmente vulnerable.
- **PRIME 1.4** corrige las vulnerabilidades de 1.3.
 - Además, introduce un perfil adicional de seguridad (**perfil 2**) que cifra más mensajes.

Seguridad DLMS/COSEM

Protegiendo la capa de aplicación

- **DLMS** es un protocolo de paso de mensajes entre objetos.
- **COSEM** es el modelo de clases, objetos y propiedades/métodos de los mismos, describiendo las funcionalidades del contador.
- **Autenticación**
 - NS (no security): el usuario solicita datos al contador libremente.
 - LLS (Low level security): autenticación mediante usuario y contraseña
 - HLS (High level security): autenticación mutua en cuatro pasos mediante un intercambio de retos criptográficos.
- **Autorización**
 - Durante la asociación se indica qué acciones se desean realizar contra el contador.
- **Cifrado**
 - Varias suites criptográficas, mensajes específicos en función del alcance de las claves.

Conclusiones preliminares

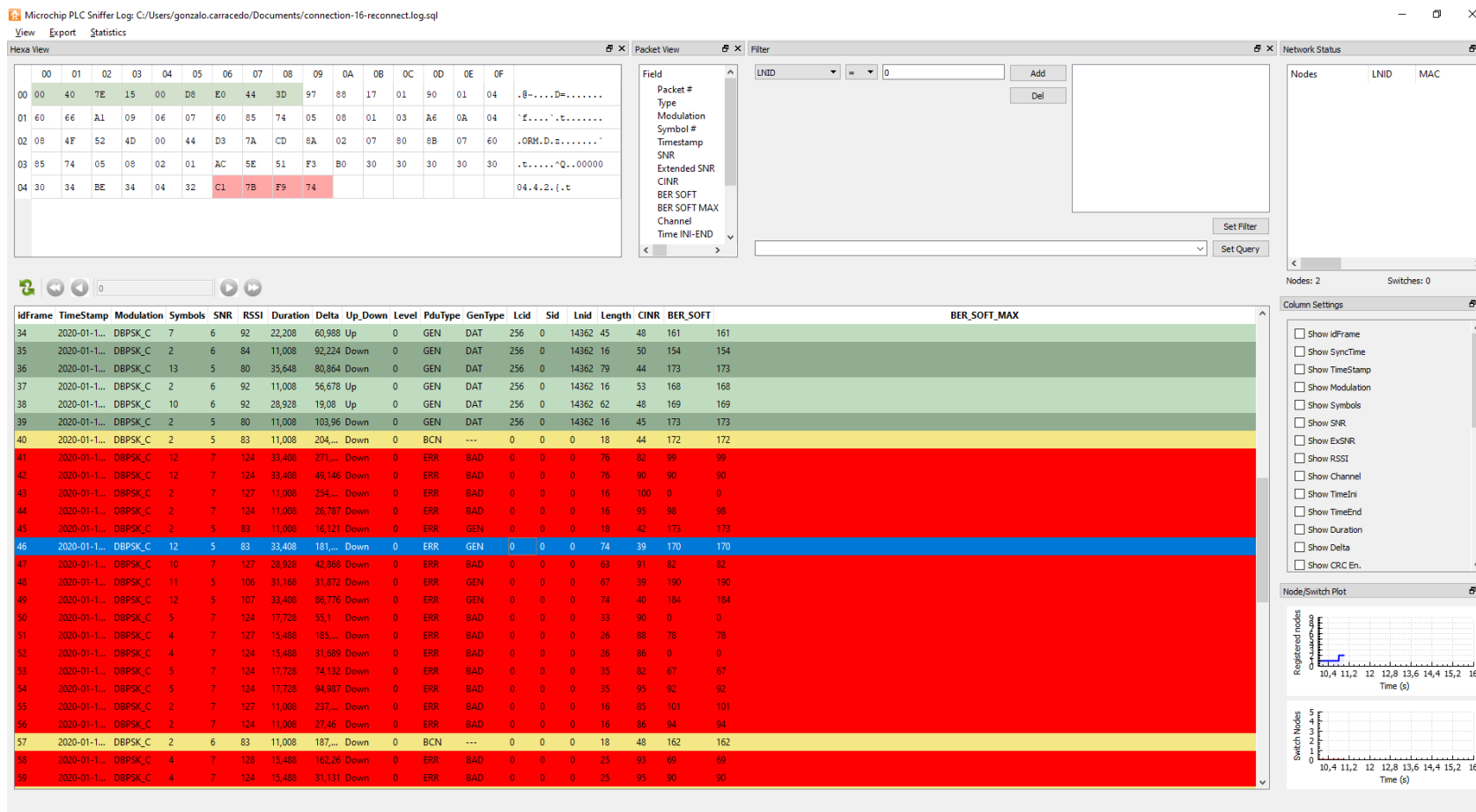
Un vistazo a la red PLC

- Análisis de tráfico mediante placas de evaluación PLC de Microchip: **PL360EK**
- Pruebas realizadas en la oficina de Tarlogic en Las Tablas
- Se ha observado tráfico **PRIME 1.3.6** en **perfil 0** (sin cifrar)
- Se ha observado tráfico DLMS/COSEM cifrado (mensajes tipo GLO/DED) **pero en su mayoría sin cifrar**
- Se ha observado autenticación DLMS/COSEM en modo **baja seguridad** con la misma contraseña al menos en modos de lectura: "00000001"
- **Esta configuración sugiere varios ataques.**



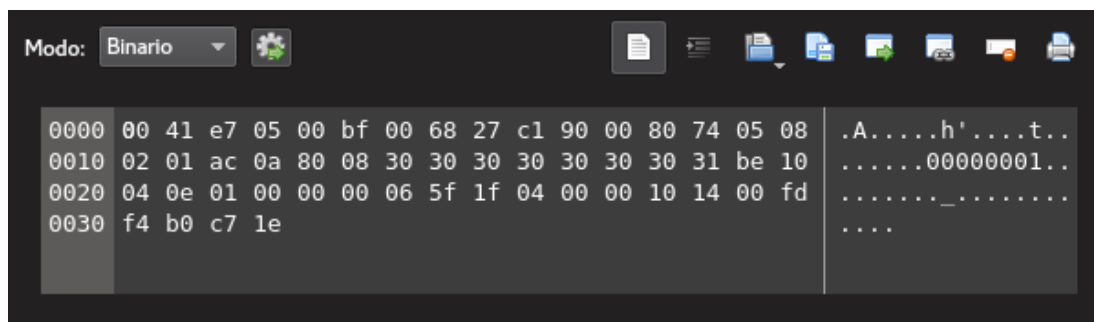
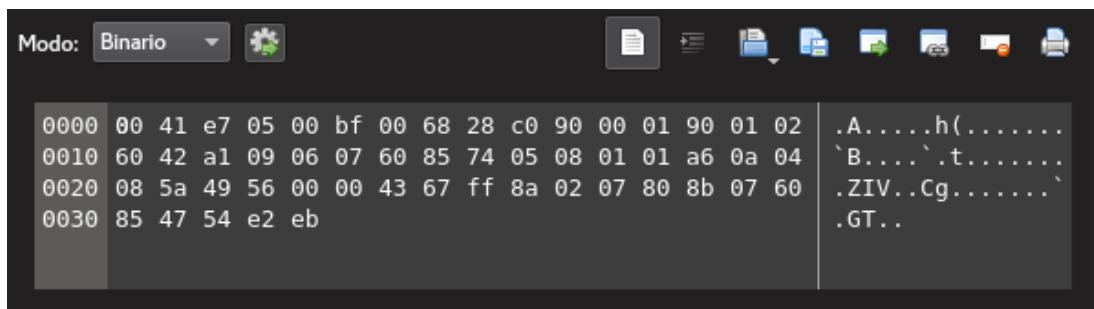
Conclusiones preliminares

Un vistazo a la red PLC



Conclusiones preliminares

Un vistazo a la red PLC



```
<AssociationRequest>
  <ApplicationContextName Value="LN" />
  <CallingAPTitle Value="5A495600004367FF" />
  <SenderACSERequirements Value="1" />
  <MechanismName Value="Low" />
  <CallingAuthentication Value="3030303030303031" />
  <InitiateRequest>
    <ProposedDlmsVersionNumber Value="06" />
    <ProposedConformance>
      <ConformanceBit Name="SelectiveAccess" />
      <ConformanceBit Name="Get" />
      <ConformanceBit Name="BlockTransferWithGetOrRead" />
    </ProposedConformance>
    <ProposedMaxPduSize Value="00FD" />
  </InitiateRequest>
</AssociationRequest>
```

Ataques reales a la red

Planteamiento y pruebas de laboratorio

- Esta pobre configuración de seguridad planteó una serie de ataques a la red. Entre ellos:
 - Captura de credenciales
 - Identificación de contadores
 - Análisis de las medidas
 - Secuestro de comunicaciones
 - Suplantación de identidad
 - Ejecución de órdenes privilegiadas
- Despliegue de un pequeño laboratorio PLC con un concentrador y cuatro contadores PRIME



Resultados

Control remoto del ICP

- Prueba de concepto en directo realizada en RootedCON
 - Ver charla online "*The Joy of Bugging Smart Meters*"
<https://www.youtube.com/watch?v=UsVDI8oRYrA>
- Precondiciones:
 - Perfil **PRIME 0**, autenticación **DLMS** en **baja seguridad**, tráfico **DLMS** en **claro**
- No es un resultado inmediato debido a la poca fiabilidad de la red, **pero el secuestro del tráfico se ha probado posible.**
- Pequeña herramienta de consola (PLCHack) para la ejecución de estos ataques.



<https://www.youtube.com/watch?v=HBv24UJUK3I>

Continuación de las investigaciones

Sistematización de las pruebas, herramientas y resultados

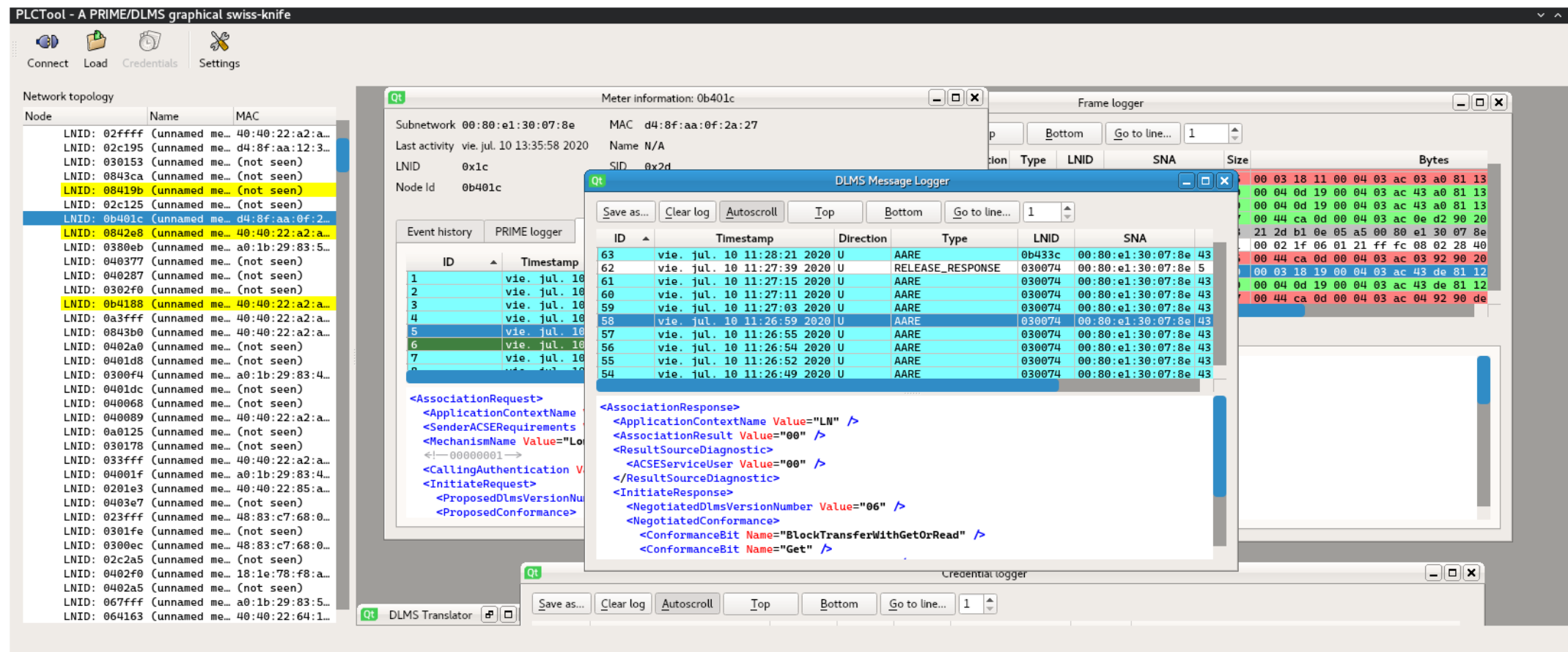
Limitaciones de la investigación anterior

Yendo más allá

- Análisis de tráfico real restringido a un solo enchufe (una única distribuidora)
 - Gran limitación respecto del tráfico observado.
 - Visión extremadamente parcial de la configuración de las redes.
- La mayor parte del funcionamiento real de la red PRIME ha sido deducido desde el laboratorio
 - Cuestiones meramente prácticas: no se perdían paquetes, se podían generar órdenes a voluntad para su posterior análisis y no existía riesgo de interferir con un contador real.
- Funcionalidades básicas de PRIME/DLMS como la configuración del cifrado o la actualización del firmware no se pudieron observar.
- PLCHack era una herramienta demasiado rudimentaria.

PLCTool

La navaja suiza del análisis de redes PLC



PLCTool - A PRIME/DLMS graphical swiss-knife

Connect Load Credentials Settings

Network topology

Node	Name	MAC
LNID: 02ffff	(unnamed me...	40:40:22:a2:a...
LNID: 02c195	(unnamed me...	d4:8f:aa:12:3...
LNID: 030153	(unnamed me...	(not seen)
LNID: 0843ca	(unnamed me...	(not seen)
LNID: 08419b	(unnamed me...	(not seen)
LNID: 02c125	(unnamed me...	(not seen)
LNID: 0b401c	(unnamed me...	d4:8f:aa:0f:2...
LNID: 0842e8	(unnamed me...	40:40:22:a2:a...
LNID: 0380eb	(unnamed me...	a0:1b:29:83:5...
LNID: 040377	(unnamed me...	(not seen)
LNID: 040287	(unnamed me...	(not seen)
LNID: 0302f0	(unnamed me...	(not seen)
LNID: 0b4188	(unnamed me...	40:40:22:a2:a...
LNID: 0a3fff	(unnamed me...	40:40:22:a2:a...
LNID: 0843b0	(unnamed me...	40:40:22:a2:a...
LNID: 0402a0	(unnamed me...	(not seen)
LNID: 0401d8	(unnamed me...	(not seen)
LNID: 0300f4	(unnamed me...	a0:1b:29:83:4...
LNID: 0401dc	(unnamed me...	(not seen)
LNID: 040068	(unnamed me...	(not seen)
LNID: 040089	(unnamed me...	40:40:22:a2:a...
LNID: 0a0125	(unnamed me...	(not seen)
LNID: 030178	(unnamed me...	(not seen)
LNID: 033fff	(unnamed me...	40:40:22:a2:a...
LNID: 04001f	(unnamed me...	a0:1b:29:83:4...
LNID: 0201e3	(unnamed me...	40:40:22:85:a...
LNID: 0403e7	(unnamed me...	(not seen)
LNID: 023fff	(unnamed me...	48:83:c7:68:0...
LNID: 0301fe	(unnamed me...	(not seen)
LNID: 0300ec	(unnamed me...	48:83:c7:68:0...
LNID: 02c2a5	(unnamed me...	(not seen)
LNID: 0402f0	(unnamed me...	18:1e:78:f8:a...
LNID: 0402a5	(unnamed me...	(not seen)
LNID: 067fff	(unnamed me...	a0:1b:29:83:5...
LNID: 064163	(unnamed me...	40:40:22:64:1...

Meter information: 0b401c

Subnetwork 00:80:e1:30:07:8e MAC d4:8f:aa:0f:2a:27

Last activity vie. jul. 10 13:35:58 2020 Name N/A

LNID 0x1c SID 0x2d

Node Id 0b401c

Frame logger

Position	Type	LNID	SNA	Size	Bytes
1	AARE	0b433c	00:80:e1:30:07:8e	43	00 03 18 11 00 04 03 ac 03 a0 81 13
2	RELEASE_RESPONSE	030074	00:80:e1:30:07:8e	5	00 04 0d 19 00 04 03 ac 43 a0 81 13
3	AARE	030074	00:80:e1:30:07:8e	43	00 04 0d 19 00 04 03 ac 43 a0 81 13
4	AARE	030074	00:80:e1:30:07:8e	43	00 44 ca 0d 00 04 03 ac 0e d2 90 20
5	AARE	030074	00:80:e1:30:07:8e	43	21 2d b1 0e 05 a5 00 80 e1 30 07 8e
6	AARE	030074	00:80:e1:30:07:8e	43	00 02 1f 06 01 21 ff fc 08 02 28 40
7	AARE	030074	00:80:e1:30:07:8e	43	00 44 ca 0d 00 04 03 ac 03 92 90 20
8	AARE	030074	00:80:e1:30:07:8e	43	00 03 18 19 00 04 03 ac 43 de 81 12
9	AARE	030074	00:80:e1:30:07:8e	43	00 04 0d 19 00 04 03 ac 43 de 81 12
10	AARE	030074	00:80:e1:30:07:8e	43	00 44 ca 0d 00 04 03 ac 04 92 90 de

DLMS Message Logger

ID	Timestamp	Direction	Type	LNID	SNA
63	vie. jul. 10 11:28:21 2020	U	AARE	0b433c	00:80:e1:30:07:8e
62	vie. jul. 10 11:27:39 2020	U	RELEASE_RESPONSE	030074	00:80:e1:30:07:8e
61	vie. jul. 10 11:27:15 2020	U	AARE	030074	00:80:e1:30:07:8e
60	vie. jul. 10 11:27:11 2020	U	AARE	030074	00:80:e1:30:07:8e
59	vie. jul. 10 11:27:03 2020	U	AARE	030074	00:80:e1:30:07:8e
58	vie. jul. 10 11:26:59 2020	U	AARE	030074	00:80:e1:30:07:8e
57	vie. jul. 10 11:26:55 2020	U	AARE	030074	00:80:e1:30:07:8e
56	vie. jul. 10 11:26:54 2020	U	AARE	030074	00:80:e1:30:07:8e
55	vie. jul. 10 11:26:52 2020	U	AARE	030074	00:80:e1:30:07:8e
54	vie. jul. 10 11:26:49 2020	U	AARE	030074	00:80:e1:30:07:8e

Event history PRIME logger

ID	Timestamp
1	vie. jul. 10 11:28:21 2020
2	vie. jul. 10 11:27:39 2020
3	vie. jul. 10 11:27:15 2020
4	vie. jul. 10 11:27:11 2020
5	vie. jul. 10 11:27:03 2020
6	vie. jul. 10 11:26:59 2020
7	vie. jul. 10 11:26:55 2020
8	vie. jul. 10 11:26:54 2020
9	vie. jul. 10 11:26:52 2020
10	vie. jul. 10 11:26:49 2020

DLMS Translator

Save as... Clear log Autoscroll Top Bottom Go to line... 1

Credential logger

Save as... Clear log Autoscroll Top Bottom Go to line... 1

Ampliando el estudio de la red

Algo más que tramas sueltas

- Extensión limitada debido a la pandemia global. Dos puntos de análisis:
 - Domicilio particular en el barrio de **Hortaleza (Madrid)**
 - Domicilio particular en **O Barco de Valdeorras (Ourense)**
- Ampliación de objetivos:
 - **Identificación** de redes y contadores
 - **Asociación** de tráfico a cada contador
 - **Registro** de direcciones MAC, identificadores, contraseñas y tipos de acceso
 - **Análisis** de la robustez de las contraseñas capturadas
 - **Captura** de tráfico no DLMS (actualizaciones de firmware)

Tráfico PLC en Hortaleza (Madrid)

PRIME 1.3.6, perfil 0 (sin cifrar)

Qt Frame logger

Save as... Clear log Autoscroll Top Bottom Go to line... 1

ID	Timestamp	Direction	Type	LNID	SNA	Size	Bytes
1564	lun. sept. 21 14:32:18 2020	U	DATA	0021dd	40:40:22:02:85:f0	26	00 00 27 19 00 18 87 74 0d c4 81 05 00 90 02 01 c...
1565	lun. sept. 21 14:32:19 2020	U	BEACON	ffffff	40:40:22:02:85:f0	18	26 10 88 00 01 a4 40 40 22 02 85 f0 04 04 8e e1 b...
1566	lun. sept. 21 14:32:19 2020	D	DATA	0021dd	40:40:22:02:85:f0	33	00 41 e7 05 00 18 87 74 14 c5 90 05 00 90 01 02 c...
1567	lun. sept. 21 14:32:19 2020	U	Corrupt	ffffff	40:40:22:02:85:f0	16	00 00 27 11 00 18 87 74 03 85 81 06 91 30 ad 03
1568	lun. sept. 21 14:32:19 2020	U	DATA	0021dd	40:40:22:02:85:f0	26	00 00 27 19 00 18 87 74 0d c5 81 06 00 90 02 01 c...
1569	lun. sept. 21 14:32:19 2020	D	DATA	0021dd	40:40:22:02:85:f0	33	00 41 e7 05 00 18 87 74 14 c6 90 06 00 90 01 02 c...
1570	lun. sept. 21 14:32:19 2020	U	DATA	0021dd	40:40:22:02:85:f0	26	00 00 27 19 00 18 87 74 0d c6 81 07 00 90 02 01 c...
1571	lun. sept. 21 14:32:19 2020	D	DATA	0021dd	40:40:22:02:85:f0	33	00 41 e7 05 00 18 87 74 14 c7 90 07 00 90 01 02 c...
1572	lun. sept. 21 14:32:20 2020	U	DATA	0021dd	40:40:22:02:85:f0	72	00 00 27 19 00 18 87 74 3b c7 81 08 00 90 02 01 c...
1573	lun. sept. 21 14:32:20 2020	D	DATA	0021dd	40:40:22:02:85:f0	33	00 41 e7 05 00 18 87 74 14 c8 90 08 00 90 01 02 c...
1574	lun. sept. 21 14:32:20 2020	U	DATA	0021dd	40:40:22:02:85:f0	29	00 00 27 19 00 18 87 74 10 c8 81 09 00 90 02 01 c...

PRIME headers Hexdump

```

frame->PDU.AKV.NACKID.resize(0);
frame->PDU.SAR.TYPE = 0; // FIRST
frame->PDU.SAR.NSEGS = 0x0;

frame->PDU.CL.TYPE = 0x90;
frame->PDU.CL.SRC = 1; // DC
frame->PDU.CL.DEST = 2; // METER;

frame->PDU.DATA = hexStrToVector("c001c5004600015e2214ff0300");
// 00000000 c0 01 c5 00 46 00 01 5e 22 14 ff 03 00 | ....F...^"....
// 0000000d

```

Tráfico PLC en Hortaleza (Madrid)

DLMS sin cifrar

DLMS Message Logger							
Save as... Clear log Autoscroll Top Bottom Go to line... 1							
ID	Timestamp	Direction	Type	LNID	SNA	Size	PDU
121	mar. sept. 22 00:51:42 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
122	mar. sept. 22 00:51:44 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
123	mar. sept. 22 00:51:45 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
124	mar. sept. 22 00:51:47 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
125	mar. sept. 22 00:51:48 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 02
126	mar. sept. 22 00:51:49 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 02
127	mar. sept. 22 00:51:50 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 02
128	mar. sept. 22 00:51:52 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 02
129	mar. sept. 22 00:51:52 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 03
130	mar. sept. 22 00:51:54 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 03
131	mar. sept. 22 00:51:54 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 03
132	mar. sept. 22 00:51:54 2020	D	GET_REQUEST	08a025	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 04


```

<GetRequest>
  <GetRequestForNextDataBlock>
    <InvokeIdAndPriority Value="C1" />
    <BlockNumber Value="00000002" />
  </GetRequestForNextDataBlock>
</GetRequest>
  
```

Tráfico PLC en Hortaleza (Madrid)

Totalidad de autenticaciones DLMS en baja seguridad

Qt DLMS Message Logger

Save as... Clear log Autoscroll Top Bottom Go to line... 1

ID	Timestamp	Direction	Type	LNID	SNA	Size	PDU
142	mar. sept. 22 00:52:41 2020	U	RELEASE_RESPONSE	00226a	40:40:22:02:85:f0	5	63 03 80 01 00
143	mar. sept. 22 00:54:08 2020	D	AARQ	18e300	40:40:22:02:85:f0	68	60 42 a1 09 06 07 60 85 74 05 08 01 01 ...
144	mar. sept. 22 00:54:12 2020	D	AARQ	18e300	40:40:22:02:85:f0	68	60 42 a1 09 06 07 60 85 74 05 08 01 01 ...
145	mar. sept. 22 00:54:12 2020	D	GET_REQUEST	18e300	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
146	mar. sept. 22 00:54:15 2020	D	GET_REQUEST	18e300	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
147	mar. sept. 22 00:54:19 2020	D	GET_REQUEST	18e300	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 01
148	mar. sept. 22 00:54:24 2020	D	GET_REQUEST	18e300	40:40:22:02:85:f0	7	c0 02 c1 00 00 00 04
149	mar. sept. 22 00:54:25 2020	D	RELEASE_REQUEST	18e300	40:40:22:02:85:f0	2	62 00
150	mar. sept. 22 00:54:27 2020	U	RELEASE_RESPONSE	18e300	40:40:22:02:85:f0	5	63 03 80 01 00
151	mar. sept. 22 00:54:27 2020	U	RELEASE_RESPONSE	18e300	40:40:22:02:85:f0	5	63 03 80 01 00
152	mar. sept. 22 00:54:28 2020	D	RELEASE_REQUEST	18e300	40:40:22:02:85:f0	2	62 00
153	mar. sept. 22 00:54:30 2020	U	AARE	02a790	40:40:22:02:85:f0	43	61 29 a1 09 06 07 60 85 74 05 08 01 01 ...

```

<AssociationRequest>
  <ApplicationContextName Value="LN" />
  <!-- ZIV (00004367ff) -->
  <CallingAPTitle Value="5A495600004367FF" />
  <SenderACSERequirements Value="1" />
  <MechanismName Value="Low" />
  <!-- 00000001 -->
  <CallingAuthentication Value="30303030303031" />
  <InitiateRequest>
    <ProposedDlmsVersionNumber Value="06" />
    <ProposedConformance>
      <ConformanceBit Name="BlockTransferWithGetOrRead" />

```

Tráfico PLC en Hortaleza (Madrid)

Contraseñas simples o fácilmente crackeables

Credential logger							
Save as... Clear log Autoscroll Top Bottom Go to line... 1							
Id	Timestamp	Meter name	NID	MAC	SNA	Password	Contexts
35	mar. sept. 22 05:23:09 2020	ZIV (0...	06203f	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get
34	mar. sept. 22 05:23:08 2020	ZIV (0...	06203f	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get
33	mar. sept. 22 05:22:54 2020	ZIV (0...	0621dd	18:1e:78:fa:7d:83	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
32	mar. sept. 22 05:22:48 2020	ZIV (0...	0621dd	18:1e:78:fa:7d:83	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get
31	mar. sept. 22 05:22:17 2020	ZIV (0...	06203f	N/A	40:40:22:02:85:f0	ZHJyAAEH	BlockTransferWithSetOrWrite, Set
30	mar. sept. 22 05:22:10 2020	ZIV (0...	0621dd	18:1e:78:fa:7d:83	40:40:22:02:85:f0	ZHFzAAEH	BlockTransferWithSetOrWrite, Set
29	mar. sept. 22 03:09:00 2020	ZIV (0...	0621dd	18:1e:78:fa:7d:83	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
28	mar. sept. 22 02:57:45 2020	ZIV (0...	0623cd	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
27	mar. sept. 22 02:57:44 2020	ZIV (0...	0623cd	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
26	mar. sept. 22 02:57:42 2020	ZIV (0...	0623cd	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
25	mar. sept. 22 02:57:11 2020	ZIV (0...	06203f	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
24	mar. sept. 22 02:54:20 2020	ZIV (0...	062614	d4:8f:aa:24:b3:2c	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
23	mar. sept. 22 02:54:20 2020	ZIV (0...	062614	d4:8f:aa:24:b3:2c	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
22	mar. sept. 22 02:54:07 2020	ZIV (0...	062701	d4:8f:aa:23:70:57	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
21	mar. sept. 22 02:53:44 2020	ZIV (0...	0621f0	d4:8f:aa:22:fa:19	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
20	mar. sept. 22 02:52:37 2020	ZIV (0...	06275b	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
19	mar. sept. 22 02:46:13 2020	ZIV (0...	0625cd	40:40:22:a3:e1:d2	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
18	mar. sept. 22 02:41:45 2020	ZIV (0...	08a025	N/A	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess
17	mar. sept. 22 02:17:58 2020	ZIV (0...	0667a9	d4:8f:aa:23:4b:5a	40:40:22:02:85:f0	00000001	BlockTransferWithGetOrRead, Get, SelectiveAccess

Tráfico PLC en Hortaleza (Madrid)

¡Actualizaciones no autenticadas de firmware!

PLCTool - A PRIME/DLMS graphical swiss-knife - [Frame logger]

Connect Load Credentials Settings

Network topology

Node	Name	MAC
▶ SNA: 4040220285f0	(unnamed DC)	40:40:22:02:85:f0

Save as... Clear log Autoscroll Top Bottom Go to line... 1

ID	Timestamp	Direction	Type	LNID	SNA	Size	Bytes
83381	lun. ago. 3 12:04:17 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 64 00...
83382	lun. ago. 3 12:04:20 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 6c 00...
83383	lun. ago. 3 12:04:20 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 6d 00...
83384	lun. ago. 3 12:04:21 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 71 00...
83385	lun. ago. 3 12:04:21 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 71 00...
83386	lun. ago. 3 12:04:23 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 75 00...
83387	lun. ago. 3 12:04:23 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 76 00...
83388	lun. ago. 3 12:04:24 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 77 00...
83389	lun. ago. 3 12:04:26 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 7b 00...
83390	lun. ago. 3 12:04:28 2020	U	BEACON	ffffff	40:40:22:02:85:f0	18	22 6a 88 00 01 15 40 40 22 02 85 f0 04 04 0e c4 fa 69
83391	lun. ago. 3 12:04:28 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 81 00...
83392	lun. ago. 3 12:04:28 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 83 00...
83393	lun. ago. 3 12:04:30 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 85 00...
83394	lun. ago. 3 12:04:30 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 86 00...
83395	lun. ago. 3 12:04:31 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 88 00...
83396	lun. ago. 3 12:04:31 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 88 00...
83397	lun. ago. 3 12:04:31 2020	U	BEACON	ffffff	40:40:22:02:85:f0	18	22 d3 88 00 01 45 40 40 22 02 85 f0 04 04 ba 52 0c 0a
83398	lun. ago. 3 12:04:32 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 8d 00...
83399	lun. ago. 3 12:04:33 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 8f 00...
83400	lun. ago. 3 12:04:34 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 91 00...
83401	lun. ago. 3 12:04:34 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 92 00...
83402	lun. ago. 3 12:04:35 2020	D	DATA	003ffe	40:40:22:02:85:f0	86	00 42 ee 0c 00 62 ff f8 49 00 11 85 60 00 00 01 9d 00...

PRIME headers Hexdump

```

frame->PDU.PKT.ID = 0x00;
// frame->PDU.PKT.NID = 0x18bffe;

frame->PDU.ARQ.PKTID = 0;
frame->PDU.ARQ.WINSIZE = 0x0;
frame->PDU.ARQ.ACKID = 0;
frame->PDU.ARQ.NACKID.resize(0);
frame->PDU.SAR.TYPE = 0; // FIRST
frame->PDU.SAR.NSEGS = 0x11;

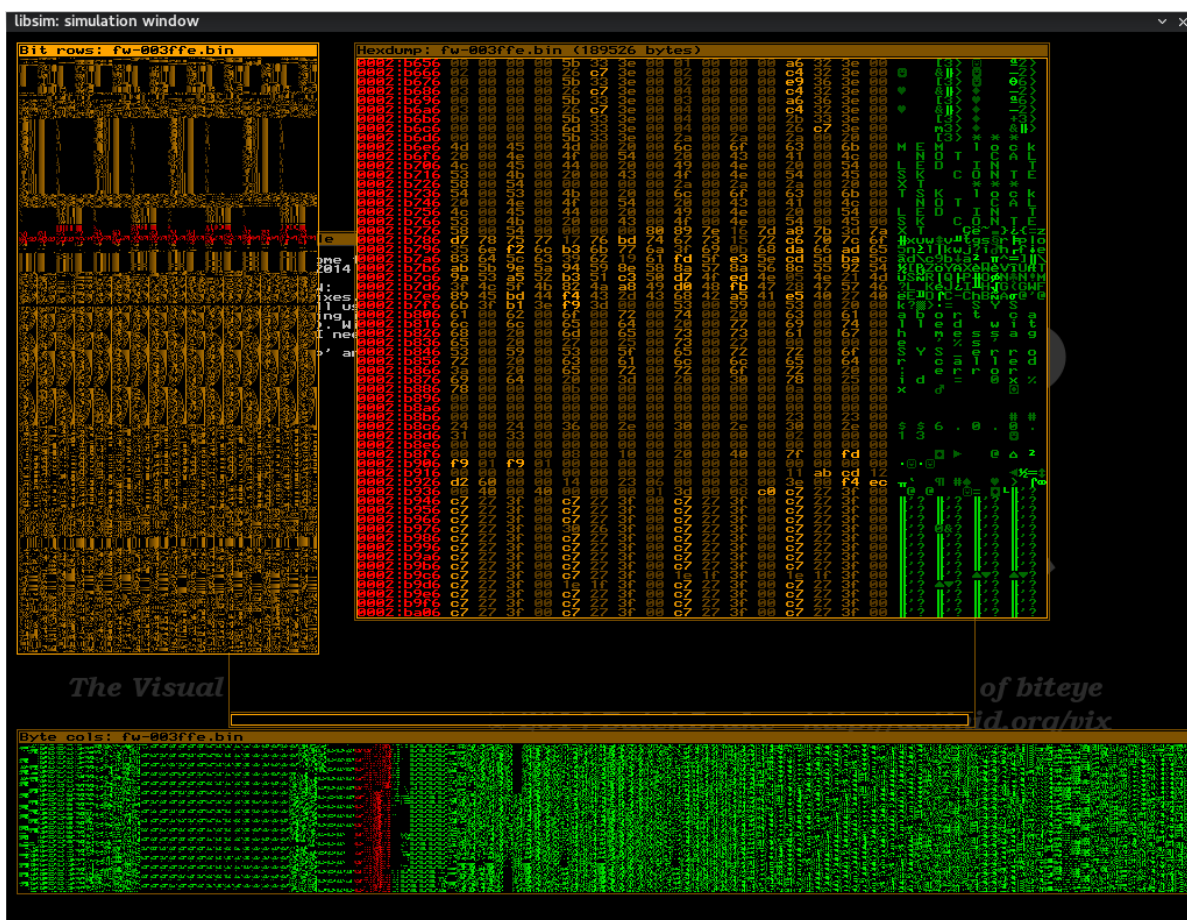
frame->PDU.CL.TYPE = 0x85;
frame->PDU.CL.SRC = 96; // METER
frame->PDU.CL.DEST = 0; // METER;

frame->PDU.DATA =
hexStrToVector("00016d003d7ec8346b02fd7ebf8783721a3bb0ba38ba1a58eaf9f4296a5711e2b1ea61bb9e532d0925d9dc62a2b5335d92c756824aea152803ee9b2dbaf5d28c21dc6f9");
// 00000000 00 01 6d 00 3d 7e c8 34 6b 02 fd 7e bf 87 83 72 | ..m-..4k...r
// 00000010 1a 3b b0 ba 38 ba 1a 58 ea f9 f4 29 6a 57 11 e2 | ;..8..X...jw..
// 00000020 b1 ea 61 bb 9e 53 2d 09 25 2d 9d c6 2a 2b 53 35 | ;a..5-..%..*+5
// 00000030 d9 2c 75 68 24 ae a1 52 80 3e e9 b2 db af 5d 28 | ;..uh$.R>....[
// 00000040 c2 1c d6 f9 | ....
// 00000044

```

Tráfico PLC en Hortaleza (Madrid)

¡Actualizaciones no autenticadas de firmware!



Tráfico PLC en O Barco de Valdeorras

PRIME 1.3.6, perfil 0 (sin cifrar)

Qt Frame logger Save as... Clear log Autoscroll Top Bottom Go to line... 1

	Timestamp	Direction	Type	LNID	SNA	Size	Bytes
...	lun. jul. 13 13:55:06 2020	U	DATA	000a69	00:80:e1:30:07:8e	60	00 03 18 05 00 0d 29 a4 2f d5 90 05 42 06 00 00 00 20...
...	lun. jul. 13 13:55:08 2020	U	DATA	000a69	00:80:e1:30:07:8e	60	00 03 18 05 00 0d 29 a4 2f 99 90 06 40 00 00 00 00 06...
...	lun. jul. 13 13:55:08 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:09 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:09 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:09 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:11 2020	U	Corru...	ffffff	00:80:e1:30:07:8e	16	00 03 18 05 00 0d 29 a4 03 de 90 06 d2 ab ab e6
...	lun. jul. 13 13:55:12 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:13 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:15 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:17 2020	U	DATA	000a69	00:80:e1:30:07:8e	56	00 03 18 05 00 0d 29 a4 2b dd 90 06 84 0f 00 00 00 80...
...	lun. jul. 13 13:55:17 2020	U	DATA	000a69	00:80:e1:30:07:8e	60	00 03 18 05 00 0d 29 a4 2f da 90 06 41 00 00 00 00 06...

PRIME headers Hexdump

Tráfico PLC en O Barco de Valdeorras

DLMS sin cifrar

Qt DLMS Message Logger

Save as... Clear log Autoscroll Top Bottom Go to line... 1

ID	Timestamp	Direction	Type	LNID	SNA	Size	PDU
4919	lun. jul. 13 12:20:11 2020	U	EXCEPTION_RESPONSE	034a1d	00:80:e1:30:07:8e	3	d8 02 01
4920	lun. jul. 13 12:20:12 2020	U	EXCEPTION_RESPONSE	034a1d	00:80:e1:30:07:8e	3	d8 02 01
4921	lun. jul. 13 12:20:15 2020	U	EXCEPTION_RESPONSE	034a1d	00:80:e1:30:07:8e	3	d8 02 01
4922	lun. jul. 13 12:20:49 2020	U	EXCEPTION_RESPONSE	034a1d	00:80:e1:30:07:8e	3	d8 01 02
4923	lun. jul. 13 12:20:50 2020	U	EXCEPTION_RESPONSE	034a1d	00:80:e1:30:07:8e	3	d8 01 02
4924	lun. jul. 13 12:29:08 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
4925	lun. jul. 13 12:29:16 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
4926	lun. jul. 13 12:29:17 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
4927	lun. jul. 13 12:29:19 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
4928	lun. jul. 13 12:29:19 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
4929	lun. jul. 13 12:29:20 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
4930	lun. jul. 13 12:29:20 2020	U	AARE	010883	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...

Tráfico PLC en O Barco de Valdeorras

Totalidad de autenticaciones DLMS en baja seguridad

Qt DLMS Message Logger

Save as... Clear log Autoscroll Top Bottom Go to line... 1

ID	Timestamp	Direction	Type	LNID	SNA	Size	PDU
3077	dom. jul. 12 00:03:58 2020	U	AARE	00866d	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
3078	dom. jul. 12 00:03:58 2020	U	AARE	00866d	00:80:e1:30:07:8e	43	61 29 a1 09 06 07 60 85 74 05 08 01 01...
3079	dom. jul. 12 00:03:59 2020	D	AARQ	00866d	00:80:e1:30:07:8e	56	60 36 a1 09 06 07 60 85 74 05 08 01 01...
3080	dom. jul. 12 00:03:59 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	18	c4 01 c1 00 09 0c 07 e4 07 0c 07 00 03...
3081	dom. jul. 12 00:04:00 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	18	c4 01 c1 00 09 0c 07 e4 07 0c 07 00 03...
3082	dom. jul. 12 00:04:01 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	18	c4 01 c1 00 09 0c 07 e4 07 0c 07 00 03...
3083	dom. jul. 12 00:04:01 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	18	c4 01 c1 00 09 0c 07 e4 07 0c 07 00 03...
3084	dom. jul. 12 00:04:02 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	16	c4 01 c1 00 09 0a 30 30 34 30 31 31 32...
3085	dom. jul. 12 00:04:03 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	16	c4 01 c1 00 09 0a 30 30 34 30 31 31 32...
3086	dom. jul. 12 00:04:04 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	16	c4 01 c1 00 09 0a 30 30 34 30 31 31 32...
3087	dom. jul. 12 00:04:04 2020	U	GET_RESPONSE	00866d	00:80:e1:30:07:8e	16	c4 01 c1 00 09 0a 30 30 34 30 31 31 32...
3088	dom. jul. 12 00:04:04 2020	D	GET_REQUEST	00866d	00:80:e1:30:07:8e	13	c0 01 c1 00 01 00 00 60 01 00 ff 02 00

```

<AssociationRequest>
  <ApplicationContextName Value="LN" />
  <SenderACSERequirements Value="1" />
  <MechanismName Value="Low" />
  <!-- 00000001 -->
  <CallingAuthentication Value="3030303030303031" />
  <InitiateRequest>
    <ProposedDlmsVersionNumber Value="06" />
    <ProposedConformance>
      <ConformanceBit Name="BlockTransferWithGetOrRead" />
      <ConformanceBit Name="BlockTransferWithSetOrWrite" />
      <ConformanceBit Name="Get" />

```

Tráfico PLC en O Barco de Valdeorras

¡La contraseña 00000001 da control total del contador!

Qt Credential logger				
Save as...	Clear log	Autoscroll	Top	Bottom
Go to line...	1			
NID	MAC	SNA	Password	Contexts
050a3b	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
00866d	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0084a4	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0084c2	a0:1b:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0084c2	a0:1b:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
00845e	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
008626	48:83:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
008559	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0086bb	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0086bb	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
008405	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
008405	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0c42e4	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0383c5	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0383c5	N/A	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0b4188	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0b4188	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action
0b4188	40:40:...	00:80:e1:30:07:8e	00000001	BlockTransferWithGetOrRead, BlockTransferWithSetOrWrite, Get, Set, SelectiveAccess, EventNotification, Action

Conclusiones

Un panorama poco alentador

La configuración mínima de seguridad es la norma

- **PRIME en modo perfil 0 es lo único que se observa**
- **DLMS sin cifrar es extremadamente popular**
 - No se han vuelto a ver tráfico DLMS cifrado desde el inicio de las capturas
- **DLMS en baja seguridad es extremadamente popular**
 - No se ha encontrado ninguna autenticación de alta seguridad
- **¡Las actualizaciones de firmware no están autenticadas!**
 - Actualizaciones multicast (NID: 003ffe)
 - El DC lo solicita, y los contadores simplemente lo aceptan
 - Parece ser así por estándar (ver anexo correspondiente en las especificaciones de PRIME 1.3.6)
- **Evaluación preliminar de la seguridad: muy pobre.**

Contrastando resultados

Buscando una perspectiva diferente

- Principios de responsable disclosure de cara a publicar estos resultados
 - En coordinación con organismos oficiales.
 - Disponibles en el blog de Tarlogic
- Nos hemos puesto en contacto con varias distribuidoras
 - Resultados dispares
 - Hemos apoyado a alguna distribuidora proporcionando las herramientas hardware y software mencionadas para ayudar en el proceso de identificación y remediación de riesgos.
- Correo electrónico a la **PRIME Alliance** con nuestras conclusiones.
 - "No habéis descubierto nada nuevo."
 - **"No se puede concluir que los sistemas instalados por los vendedores sean inseguros."**
 - "Ponemos en copia a nuestro abogado. Esperamos que reflejéis el estado real de la situación (no de vuestro laboratorio) y respetéis nuestros derechos."

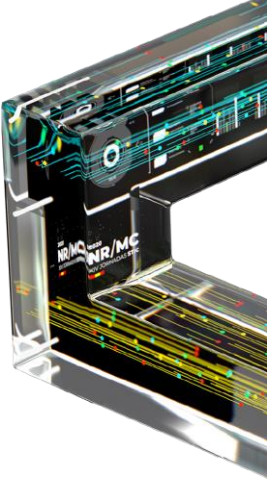
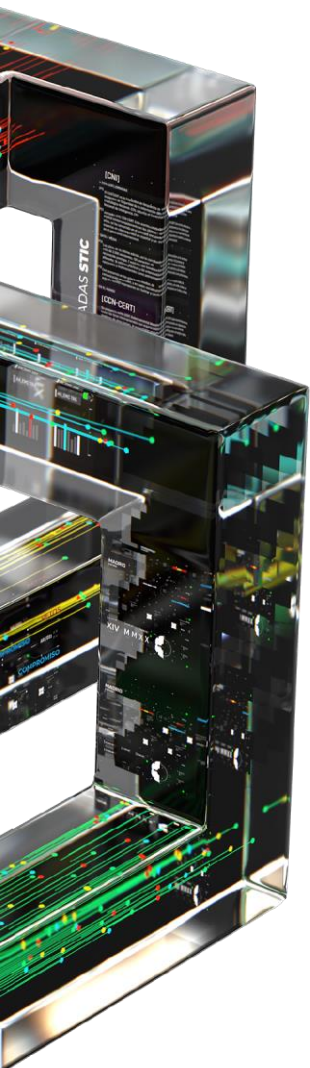
Nuestra perspectiva

Abriendo la investigación

- La respuesta por parte de las partes implicadas nos permite concluir que:
 - Ni la captura de tráfico, ni de las medidas, ni de las contraseñas, ni la ejecución de métodos (e.g. corte del ICP) ni la actualización no autenticada del firmware suponen una amenaza a la seguridad.
 - Un poco decepcionante, pero a este respecto debemos ser humildes y aceptar la realidad.
- **El compromiso del departamento de Innovación de Tarlogic con la divulgación del conocimiento es total.**
 - Hemos indagado en el funcionamiento de este tipo de redes un poco más allá de la teoría: **valor didáctico.**
 - Uno de nuestros objetivos es que los resultados de esta investigación sirvan para facilitar el proceso de aprendizaje de todos aquellos interesados en las tecnologías PRIME y DLMS/COSEM

Calendario de publicaciones

- **1 de diciembre de 2020**
 - Liberación de **PLCTool** y firmware para PL360EK para el estudio y análisis del tráfico PRIME y DLMS/COSEM visible desde los enchufes de un domicilio.
 - Publicación en el GitHub de Tarlogic: <https://github.com/TarlogicSecurity>
- **A lo largo de 2021**
 - Liberación de framework de ataque para PLCTool
 - Algunos ataques predefinidos
 - Modificación de parámetros
 - Control remoto del interruptor de control de potencia de los contadores
 - Destinado a formación en entornos controlados de laboratorio



MUCHAS GRACIAS

#XIVJORNADASCCNCERT