#### 1.1 测试环境简介



图1-1 工业控制系统信息安全实验平台的拓扑结构

如图1-1工业控制系统信息安全实验平台的拓扑结构，测试环境，包括防护模块规则配置端，模拟攻击端，PLC监控端，防护模块，以及模拟控制端。防护模块规则配置端可以实现对防护模块的访问控制规则以及深度包检测规则的配置。根据不同的工业控制协议，我们分别在模拟供给端和模拟控制端，安装基于不同工业控制协议的客户端与服务器端软件。模拟进行基于工业控制协议的通信过程。通过发送不同的数据包来观察防护模块对于不同数据包检测与防护能力。

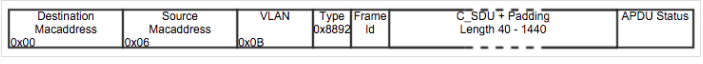
#### 1.2 基于Profinet协议的测试

试验测试通过分别在模拟攻击端和模拟控制端分别安装Profinet客户端软件与服务器软件建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。

#### 1.3 测试过程

（1）PROFINET 过程数据报结构

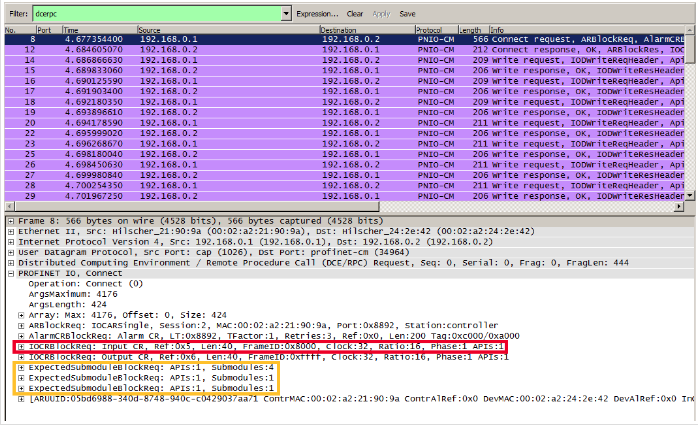
下图展示了一个 PROFINET 周期性过程数据报的一般结构：



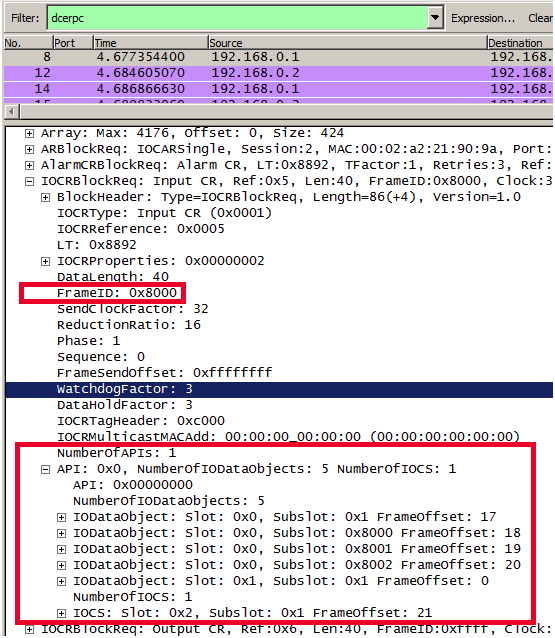
此结构基于使用 VLAN 标签的第二层以太网帧。当每个 PROFINET IO 设备和 PROFINET IO 控制器发送 VLAN 域的时候，有可能被中间的网络交换机移除掉。分析报文的时候这个需要考虑到。C\_SDU 域包含需要传输的数据。带 VLAN 的以太网帧的最小长度是 64 字节，如果 C\_SDU 域 的长度小于 40 字节会自动填补。APDU 状态域 包含周期计数和额外的状态字节。

1. 提取结构信息

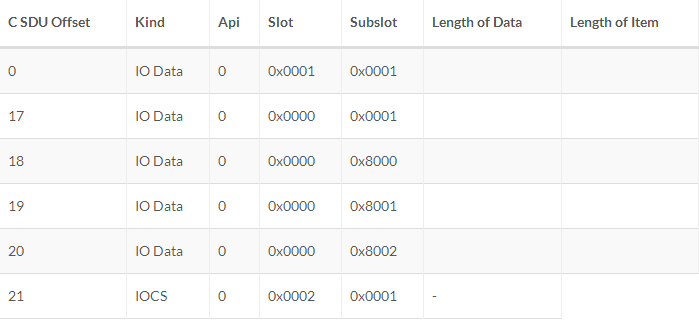
第一步要从 RPC Connect Service 中分析出需要的结构信息。通过 [WireShark](https://www.wireshark.org/) 很简单就能完成。下图展示了RPC Connect Request 和需要被用来解析一个 Input IOCR 报文的部分。红色框住的是 Input IOCR 的描述，包含了帧 ID 和在 C\_SDU 里面的数据项的偏移值。相关的过程数据能从黄色框中的 Submodule Requests提取。



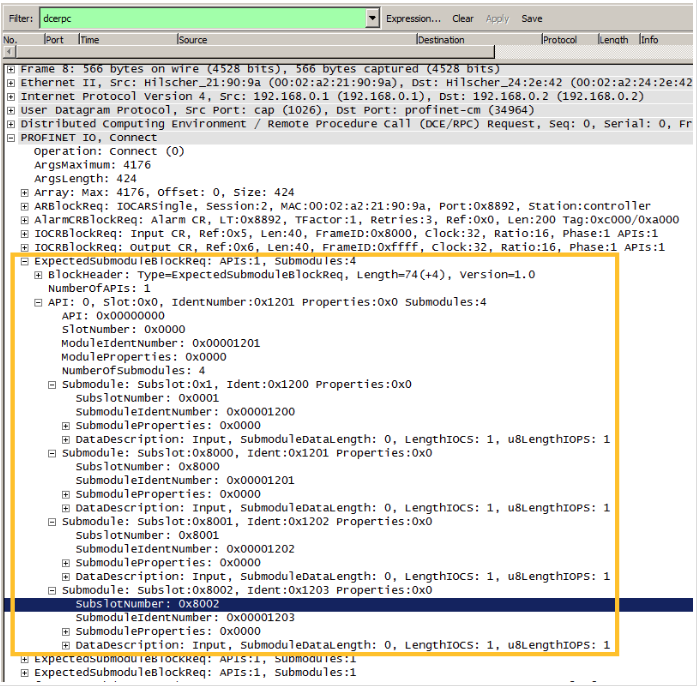
开始解析需要创建一个包含所有数据项偏移值的列表。这些信息从 IOCR Block Request 中提取。在本例中我们主要关注 Input IOCR。帧中帧 ID 是 0x8000。Output  Output IOCR 帧 ID 必须从 RPC Connect Response 帧中提取出来IOCR 帧 ID 由设备分配。下图展示了期望的 Input IOCR 的 IOCR Block Request。



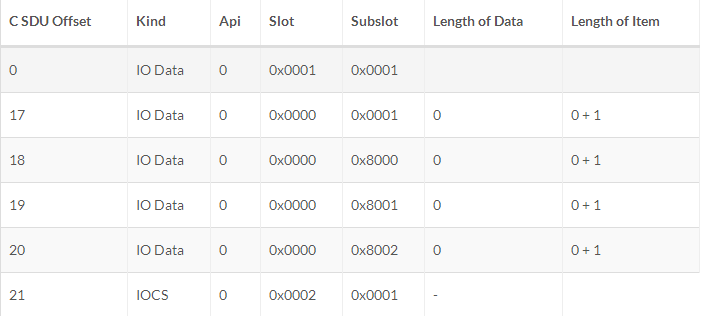
1. 根据（2）的信息创建表



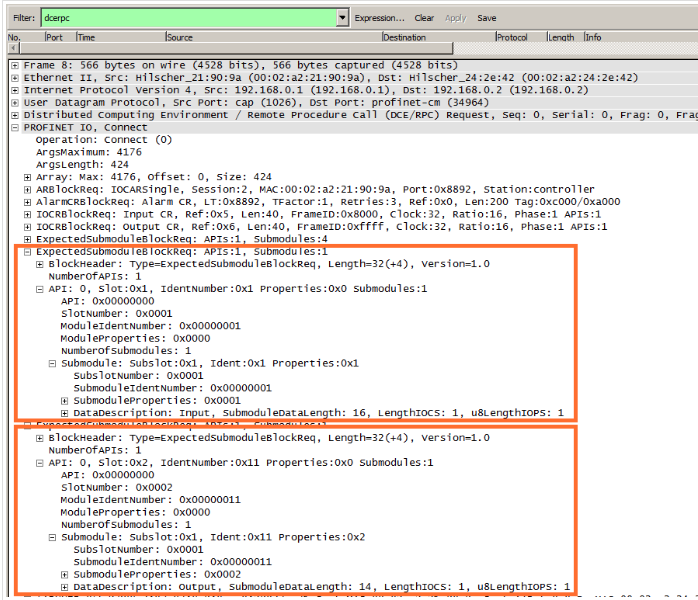
现在所有的偏移值都知道了。下一步就是提取各项的大小。这些长度能从 Expected Submodule Blocks 描述的子模块中提取出来。第一个 Expected Submodule Blocks 由下图展示：



从这些信息中得到 API 0 和 Slot 0 数据项的长度。这边导入指针是为了检查正确的数据描述元素。每个子模块都能分配一个输入数据描述 Input-Data Description 和一个输出数据描述 Output-Data Description。对于 Input IOCR 来说 Input Data Description 和 IO Data 有关， Output Data Description 和 IOCS 项 有关。Output IOCR 反之亦然。在示例中所有的第一个 Expected Submodule Block 的子模块有 0 个输入数据，1 字节 IOPS 和 1 字节 IOCS。（IOPS/IOCS 长度通常为 1 字节。）

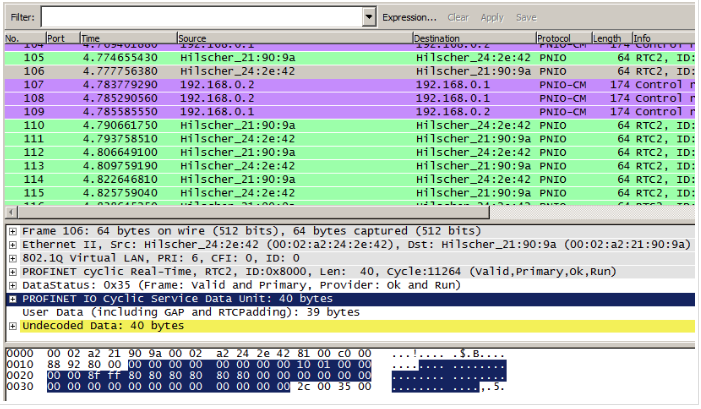


用剩下的 Expected Submodule Blocks 信息完善表格



（4）解析过程数据报

最后一步是用上文创建的表格解析过程数据报。下图展示了一个 Input IOCR 的特定数据报。为了正确的选择解析不仅 Frame ID 需要加入计算，而且数据报的 Mac 地址 也要加入计算，因为在 RT Mode 下同样的 Frame ID 可能被不同的设备用到。下图中，帧 ＃106 被选择用来分析。



蓝色标记的部分是包含实际过程数据的 C\_SDU部分（包括填充）。基于表格可以提取到如下数据：



状态值 0x80 表示相关的过程数据对于 IO Data 对象是有效的。对于 IOCS 对象，它表明相关过程数据的 “消费者” 在使用这个数据。（这个相关的过程数据发送方向相反，因此不是 IOCR 的一部分。换句话说，这个例子中 Slot 0x1 Subslot 0x1 是一个输入子模块 Input Submodule， Slot 0x2 Subslot 0x1 是一个输出子模块 Output Submodule。）

#### 1.4 总结

通过实验测试可知，该防护模块基于Profinet进行深度包解析，实现访问控制和通信管理,从而有效的实现防护功能。