

[工控系统]

基于协议解析的工控安全威胁监测

文/北京中电普华信息技术有限公司 李明维 张传远 杨夏祎 齐永忠

通过对工控通信协议安全性的分析，研究了协议解析关键技术，并设计了工控安全威胁监测的方案，及时监测工控系统产生的安全威胁。

工业控制系统（以下简称工控系统）是国家基础设施的重要组成部分，也是工业基础设施的核心。近年来工控系统安全事件频发，尤其是“震网”“火焰”“毒区”等 APT 攻击的出现，充分反映出工控系统信息安全所面临形势的严峻性。

通过对工控网络通信数据包进行深度解析，然后根据预先设定的策略产生告警事件，实时将告警信息等数据上报至综合分析处理中心，实现对威胁工控安全的行为进行监测。

数据采集

为了构建面向工业控制系统的综合数据采集能力，需要针对工业控制系统的设备特点、网络特点和应用特点进行综合分析，根据采集数据的类型、数据源与数据接口研发集成多种数据采集技术，并具有可扩展的综合数据采集矩阵。

（1）网络流量采集

工业控制系统网络流量采集需要利用加载高速流量，采集分析引擎的网络流量，采集现场监测装置进行流量捕获。流量采集主要是在集散控制网络的汇聚节点或关键位置根据网络的特性把现网的流量发送到集散控制网络流量采集器中，采集方式如图1所示。

采集方式主要包括如下方式：

（1）流量分流器

对于普通的千兆/百兆电口工业控制以太网，可

以通过部署流量分流设备把工业控制以太网中的原始流量复制后传输到工业流量采集器中，如图1所示。

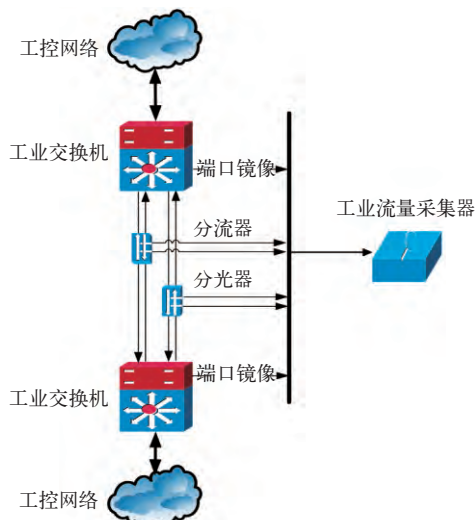


图1 网络流量采集方式

网络流量采集现场监测装置的高速流量，进行采集分析和引擎采用模块化设计，可以通过加载新的协议分析引擎，支持识别新的集散控制网络协议的流量。

（2）配置采集

集散控制的控制设备、服务器设备、网络设备、工程师站和操作站等的配置的采集主要通过配置管理接口进行采集，根据不同设备提供的接口，需要基于相应的协议进行配置采集，对于提

供WEB管理接口的PLC的配置，可以通过HTTP/HTTPS协议访问PLC设备进行配置采集。对于提供命令行访问接口的网络设备、服务器设备可以通过Telnet/SSH管理接口协议访问目标设备，通过命令行方式采集相关的配置。

(3) I/O状态采集

工业控制系统的控制设备输出的I/O状态在时间上是有顺序的，同时尝试改变控制时序或控制逻辑的攻击在I/O状态上面就有可能表现出异常的状态，因此需采集I/O状态并进行安全分析。

工业控制系统的控制设备输出的I/O状态的采集需要采用专用的设备采集I/O输出的电信号，并经过信号整形后识别I/O输出的逻辑关系，为后续的控制逻辑分析提供原始的I/O数据。

(4) 日志采集

日志采集主要通过采集工业控制系统中的各类设备的系统安全事件、用户访问记录、系统运行日志及系统运行状态等各类信息，经过原始日志标准化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统日志的全面审计。

通过日志分析可以监测整个工业控制系统的运行情况，及时发现系统异常事件；通过日志分析和审计功能，可以方便高效地对工业控制系统进行有针对性的安全审计。遇到特殊安全事件和系统故障，可以通过信息提取或关联分析进行故障快速定位，并提供原始的信息支撑安全事件应急处理或系统恢复。

日志的采集可以根据目标设备的特点，提供Syslog或SNMP方式，可以通过文件提取的方式，获得日志文件后传输到大数据存储库进行保存与统一的解析与分析。

数据分析

针对工业控制系统的攻击通常更加隐蔽，目的性也更强，一个设备遭到木马攻击或控制，往往整个网络都有可能被攻击，从而产生大量的异常连接，通过网络流量统计、分类技术，可以在监测正常流量统计特征的基础上，发现异常的攻击行为产生的非法流量，从而从流量分类统计的角度发现可疑的异常攻击连接。该方法区别于传统的基于特征码的入侵检测方法，基于攻击源和攻击目标以及攻击流量进行分析，无需进行内容

匹配，可以高效进行安全检测。

流量统计与分析可以利用如下技术进行正常流量的统计并用于异常流量的检测：地址分析技术、端口分析技术、频率分析技术、连接时间分析技术、协议分析技术、带宽分析技术及流量图分析技术。如图2所示。

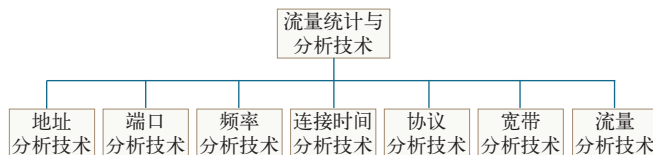


图2 流量统计与分析技术功能图

监测告警

通过分析获取的数据，对工控协议进行深度解析，实现对电力工控系统安全威胁的监测，及时发现潜在的异常，并产生告警，主要包括基于基线的异常告警，畸形报文告警以及非法应用层协议的告警。

(1) 基于基线的异常告警

工控系统具有特定的生产目标，为达到此目标制定了明确的生产逻辑，并在实际运行中严格遵守。在工控系统中各个设备需按照业务逻辑在固定时间完成特定动作，不能有丝毫差错，否则将威胁设备、系统的正常运行，甚至对物理世界产生破坏。通过对工控网络中的数据流进行监控，形成工控系统日常通信行为基线，对于偏离基线情况及时进行预警。

(2) 畸形报文告警

工控系统中的工控协议报文都有严格定义，不容易被利用，但是由于工控协议承载在TCP/IP协议之上，通过伪造TCP/IP报文进行攻击，也是一种常用的入侵手段。系统针对工控网络中TCP/IP报文进行各种典型违规的检测，及时发现伪造的畸形报文，同时对工控协议报文进行检测，发现不符合规约规定畸形工控协议报文，并进行告警。

(3) 非法应用层协议告警

工控系统的业务相对固定，工控网络中使用的工控协议也相对固定，通过对工控网络中的通信协议进行实时识别与分析，检测工控网络通信行为的规范性，及时发现非法应用层协议的违规使用，如HTTP、FTP、SSH、Telnet和DNS等，并进行告警。EA

(收稿日期：2018.09.11)

(编辑：白文亭)