SIEMENS华南区广东省汕头市西门子(授权)一级总代理

产品名称	SIEMENS华南区广东省汕头市西门子(授权)一级总代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子变频器:西门子触摸屏 西门子伺服电机:西门子PLC 西门子直流调速器:西门子电缆
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房
联系电话	18475208684 18475208684

产品详情

01.实验数据惊人：PLC设备频频"罢工"

在实验中，我们选择了5台普通计算机作为攻击主机，针对三台不同的PLC设备（西门子s7-300、施耐德M340、PAC RX3i）进行了UDP泛洪和SYN泛洪攻击。每台攻击主机分别攻击10次，记录了每次攻击后PLC设备的拒绝服务次数并计算了拒绝服务的概率。

实验结果显示，三个PLC设备，普通洪水攻击均能轻松造成拒绝服务。攻击主机数量越多，拒绝服务的概率越高，造成的危害也越大。这充分暴露了PLC设备在洪水攻击面前的脆弱性。

在泛洪攻击下，通过监控软件与PLC通信，判断PLC是否拒绝服务，在图中，制造的峰值取消，观测到拒绝服务点。

02.实验环境

实验环境包括五台攻击主机、三台PLC设备以及一个监控软件。攻击主机使用Go语言编写UDP泛洪和SYN泛洪攻击程序，PLC设备为西门子s7-300、施耐德M340、PAC RX3i，监控软件负责实时监测PLC设备的通信状态。所有设备均在同一局域网内运行。

工控设备与编程软件：

实验环境包括三台不同型号的工业控制器（PLC）以及它们对应的下位编程软件：

03.泛洪攻击实现

在系统配置了5台攻击者主机（普通电脑），每台主机都具备能力发动不同类型的攻击，例如UDP泛洪（UDP flood）或SYN泛洪（SYN flood）攻击。这些攻击者主机旨在向目标PLC发起大量恶意网络请求，通过占用其网络带宽、资源和处理能力，以干扰或阻止PLC正常运行，可能导致通信中断或系统崩溃等问题。泛洪攻击可以分为多种类型,常见类型网络层攻击、传输层攻击、应用层攻击、资源消耗攻击等。从攻击原理上拒绝服务攻击分为两类，网络带宽攻击和连通性攻击。

3.1、网络带宽攻击-UDP泛洪攻击

这种类型的攻击旨在通过向目标系统发送大量的数据流量，使其网络带宽耗尽，导致网络拥塞。攻击者的目标是使目标系统无法处理正常的网络流量，从而使其服务不可用。典型的代表是UDP Flood攻击。

这段代码是一个用Go编写的网络工具，用于执行UDP泛洪攻击（UDP Flooding Attack）。攻击使用UDP协议发送消息"UDP Flooding Message"。代码通过创建大量的并发goroutines来模拟攻击，最多允许同时运行的goroutines数目为10,000。每个goroutine都执行sendUDP函数，该函数负责建立UDP连接并发送消息。通过这种方式，攻击者可以向目标工控设备发送大量UDP请求，占用其带宽和系统资源，可能导致性能下降或服务不可用。

3.2、连通性攻击-SYN泛洪攻击

连通性攻击的目标是消耗目标系统的资源，使其无法建立新的连接或处理连接请求。这种类型的攻击不一定需要大量的数据流量，而是专注于使用各种方式消耗目标系统的连接资源。SYN Flood攻击、ACK Flood攻击以及其他基于TCP连接的攻击都可以归类为连通性攻击。

这段代码是一个使用Go编写的网络工具，旨在执行SYN泛洪攻击（SYN Flooding Attack）。攻击的目标IP地址和端口在代码中指定为特定值。代码允许创建大量并发的goroutines，该函数负责创建原始套接字（raw socket）并发送构造好的TCP头部，模拟TCP连接请求。这种行为可能导致目标服务器处理大量连接请求，占用其带宽和系统资源，最终可能导致性能下降或服务不可用。

04.监控环境实现

为了实时监测PLC设备的运行状态，本实验采用了力控监控软件。该软件能够实时采集PLC设备的运行数据，并在发现异常时监测及时发出警报。在实验过程中，我们通过该软件实时监测PLC设备的通信状态，以判断其是否受到攻击并发生拒绝服务。

原理：

通过PLC组态编程，负责对指定中间变量进行累加器峰值跳变编程，制造规律数据。组态软件趋势图组态，监控数据齿装变化。上位机采集这个变量的值，将其可视化为趋势图。通过监测这个趋势图的正常运行，我们可以进行PLC联通性的测试。这个测试方法使得我们能够验证PLC是否正常工作，确保其能够按预期执行任务并提供准确的数据。

05.实验步骤

1.将5台攻击主机和3台PLC设备连接在同一局域网内。

2.配置攻击主机，分别针对3台PLC设备进行UDP泛洪和SYN泛洪攻击。每台攻击主机分别攻击10次。

3.利用监控软件实时监测PLC设备的通信状态，记录每次攻击后PLC设备的拒绝服务次数。

4.分析实验数据，计算每次攻击后PLC设备的拒绝服务概率。

5.汇总实验数据，形成实验报告。

06.实验结论

通过对三台不同型号的PLC进行实际的DOS攻击测试，我们得出了以下结论：

1.攻击类型和成功率：我们使用了两种主要的DOS攻击类型，即UDP Flood和TCP SYN Flood。在不同的PLC上，它们的成功率会有所不同。攻击成功率的差异可能取决于PLC的硬件、通信能力和配置。

2.PLC抵抗能力：不同PLC在面对DOS攻击时表现出不同的抵抗能力。一些PLC可能在攻击下表现得更加稳定，而另一些可能更容易受到影响。这表明在工业控制系统中，选择和配置PLC对于网络安全至关重要。

3.DOS攻击的成功概率通常相对较低，因为它需要攻击者发送大量请求以超过目标设备的处理能力。然而，随着攻击流量的增加，攻击成功的概率也会显著提高。尤其是在DDOS（分布式拒绝服务攻击）攻击中，涉及多个攻击者同时发动攻击，对工控设备的影响更加破坏性。

4.工控设备通常难以承受DDOS攻击，因为它们的硬件和网络资源有限，难以应对大规模攻击造成的网络拥塞和资源耗尽。DDOS攻击可能导致工控设备的通信中断、系统崩溃或性能下降，从而对生产环境造成严重影响。

5.为了防止类似攻击事件的发生，我们需要采取一系列措施来加强PLC设备的安全性。例如，限制PLC设备的网络访问权限、定期更新设备的固件和软件、部署防火墙等。只有这样，才能确保工业生产的安全稳定运行。