**工业控制系统抗攻击能力分析报告**

目录

[一、工业控制网络与传统IT网络的区别 3](#_Toc472584658)

[二、工业控制网络信息安全防护技术发展现状 3](#_Toc472584659)

[三、工业控制网络的脆弱性 5](#_Toc472584660)

[四、主流的几种对工业控制网络的攻击方式 6](#_Toc472584661)

[五、抗攻击策略设计 11](#_Toc472584662)

[六、抗攻击测试 19](#_Toc472584663)

[七、结束语 20](#_Toc472584664)

**关于控制系统信息安全抗攻击技术分析报告**

信息安全主要是指工业控制网络中的网络信息安全以及所连接的工业现场设备、控制设备、监控设备等的信息安全。如防止针对控制设备的非法入侵，或者破坏生产计划的正常执行顺序。

工厂安全和物理安全主要是一些不可抗拒的安全，而信息安全则大都是人为的、蓄意的破坏，而且信息安全不但可能导致生产故障的发生，而且可能危害到人员的生命安全，给企业带来经济损失，甚至危害到国家安全。传统的IT网络信息安全防护技术现在已经比较成熟，形成了比较完整的技术体系。而针对工业控制网络信息安全防护技术的研究，现在还处于起步阶段，且与传统IT网络防护技术存在着差异，本文主要分析工业控制网络信息安全防护技术。

## 一、工业控制网络与传统IT网络的区别

由于工业控制网络与传统IT网络在网络特性和安全等级上存在一定的差异，所以，针对传统IT网络的攻击防御技术并不全都适用于工业控制网络。工业控制网络在性能要求、可靠性要求、风险管理需求上与传统IT网络存在巨大差异。

1）性能要求上，工业控制网络对生产信息传递过程中的延迟要求很高，实时性要求很高，对网络中的高吞吐率要求不高。而传统IT网络确恰恰相反，对网络中的高吞吐率十分看重，而允许一定范围的网络延迟。

2）可靠性要求上，工业控制网络在生产工作中一般是要求连续不间断的，绝不允许出现突然的中断，而允许的中断也是需要提前数日进行安排和计划。在某些特殊情况下，比起生产信息因为中断而被重新传送，生产过程本身的不间断显得更加重要。而在传统IT网络中，一般系统可以自由无限制的重启，信息可以重新被发送。

3）风险管理需求上，工业控制网络关心的是工人的安危、工作流程的顺序性、产品的机密以及生产设备的损坏等问题。而传统IT网络最关注的则是数据的机密性和完整性。

## 二、工业控制系统信息安全防护技术发展现状

基于上述工业控制系统与传统IT网络系统的不同特点，其在信息安全的防护重点也有所区别。在传统IT网络系统中，有上述所提到的特点，其包括了加密、授权等技术，但是在工业控制系统中，由于其创立之初，系统处于孤岛环境中，与外界隔绝，所以没考虑此类技术。近年来，由于工业控制系统的发展变化，其开始基于传统IT网络中所用到TCP/IP协议，所以传统IT网络系统中所受到一些网络攻击，工业控制系统也会受到类似威胁，相应的防护技术，也可应用到工业控制系统中。如针对传统IT网络系统中的IP欺骗、ping of death、SYN flood、UDP flood以及各种拒绝服务攻击的抗攻击技术，工业控制系统中也可以使用。传统IT网络系统中，根据网络中流量特点或者协议特征，采用入侵检测技术或者异常检测技术。由上述提到的工业控制系统流量具有的周期性，入侵检测技术和异常检测技术也可以应用到工业控制系统中。由于工业控制系统中，采用的是如modbus、profibus等私有专用协议，一旦系统中的数据包被监听窃取或者篡改，势必产生重大威胁，因此基于协议的DPI（深度包解析）技术应运而生。

对于工业控制网络信息安全技术的研究，近年才发展起来。全球各国，不管是政府、学术界还是工业界，针对工业控制网络信息安全的研究都还不够成熟，还有很多的问题有待研究。最先开始对工业控制网络信息安全的研究国家是美国，远在1998年，便形成了信息安全的概念，并首次将其提升到国家安全层面。2002年美国政府发布《国家安全战略》以及在2003年发布《保护网络空间国家战略》明确将控制系统的安全列入战略范畴，将其作为工业控制系统信息安全的指向标，并在接下来的2004年到2011年发布了多个关于工业控制系统信息安全的政策。美国的几个国家重点实验室对工业控制网络信息安全研究颇有建树。如爱达荷国家实验室（Idaho National Laboratory）在通信协议、系统评估、漏洞减少以及系统防护上，取得了较好效果，并发表了多项研究报告。而桑迪亚国家实验室（Idaho National Laboratories）则研发出一种信任锚，其采用独立的监控与检测方法，能够发现一些蓄意的攻击。阿贡国家实验室（Argonne National Laboratory）主要针对能源控制系统的通信框架、管理软件加密以及协议分析等方面的研究。欧盟各国对工业控制网络信息安全的研究紧跟其后。在2011年，欧洲网络和信息安全局（European Union Agency for Network and Information Security）颁布《保护工业控制系统》概述了工业控制系统信息安全的现有情况。德国西门子发表了《安全概念白皮书》，针对工业网络安全提出了安全内涵、安全规章以及安全解决方案，并对西门子的工业控制系统产品，提出了详细的解决方案。加拿大的多芬诺tofino提出了工业网络安全解决方案，该方案结合多芬诺的防火墙和配置软件，应用于工业控制系统中，能够进行部分工业协议的深度解析以及访问控制的实现。

和国外相比，我国国内的针对工业控制网络信息安全的研究起步比较晚。到2010年，针对工业控制网络信息安全，我国才在法律和法规上面制定一些政策，并开始积极实施相关措施，密切关注其发展。在2011年9月，国家工业和信息化部颁布了《关于加强工业控制系统信息安全管理的通知》文件，通知中明确要求抓紧工业控制系统关键设备信息安全规范和技术标准的制定，以及明确设备安全技术要求。而接着的2012年6月底，国务院发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》文件，意见中提出加强核设施、航空航天、电力系统等重要领域工业控制系统的安全检查和风险评估，保障其系统安全。与此同时，我国电力行业也发表了《电力二次系统安全防护规定》和《电力二次系统安全防护总体要求》等相关文件。

## 三、工业控制网络的脆弱性

工业控制网络的脆弱性主要分为三大类，其中包括了安全策略与管理脆弱性、系统平台与软件脆弱性以及网络通信脆弱性。下面对以上三类脆弱性进行详细分析。

1. 安全策略与管理脆弱性

工业控制网络使用过程中一些不完整、不正确或一些根本不存在的信息安全文件，其中包括了安全策略和管理流程等。而这些安全策略和管理流程是整个控制网络的核心基础。所以，在控制网络中强制使用一体化的有效的安全策略，能够有效的确保降低工业控制网络的脆弱性。

1. 系统平台与软件脆弱性

工业控制网络中的一部分脆弱性通常是由于系统自身的缺陷，操作员站、现场设备的操作系统以及设备使用的各种软件的使用引起的。如操作员站常使用的操作系统包括了Windows系统、Linux系统以及通过特别定制的一些开放式系统。而这些系统本身存在着一些安全漏洞，使得攻击者可以利用这些漏洞进行各种攻击。而且，在这些平台上安装的一些包括如监控、数据读取以及生产过程控制的软件，都被少数的几个公司垄断着，其开发之初并没有考虑太周全，并不能完全保证自身一个漏洞也没有。如发生的“震网”事件，西门子公司的WinCC组态软件存在的漏洞就被Stuxnet病毒利用而造成攻击事件。所以系统平台与软件的漏洞和其受到的潜在威胁，也构成了工业控制网络脆弱性的一部分。

1. 网络通信脆弱性

由于在工业控制网络的设计之初，其所使用的网络环境是一个完全封闭的环境，与外界几乎是隔绝的，所以，并未过多考虑网络通信的安全问题。例如，整个控制网络缺乏保密和验证机制，特别是在一个主站和从站之间的消息发送，缺乏一个验证消息完整性的有效机制。如现场总线协议中的Modbus协议，在通信过程中，全部使用的是明文传输，其几乎没有进行强有力的认证和完整性检测。再是，在网络中缺乏对于数据流的有效控制。通常对于设备的访问，需要操作员等权限才有资格决定哪些设备可以被访问，但是一旦其攻击者被控制，攻击者非法访问某些现场设备并进行数据修改，则导致不可估量的破坏。

## 四、主流的几种对工业控制网络的攻击方式

#### 1、基于恶意数据包的攻击

在工业控制网络中，基于一般恶意数据包的攻击，主要包括的是网络中非法IP的访问，非法端口服务的访问等。该类攻击比较常见，可以发生在整个控制网络中，其危害程度较小，而且很容易被识别发现。由于在传统IT网络中，网络流量的通讯量比较大，所以其一般使用的基于黑名单的防火墙技术。但在工业控制网络中，网络通讯流量相对较小，而且可靠性要求高，对于满足基本要求的流量，才允许通过。

#### 2、基于欺骗性数据包的攻击

如图4-1所示，通常情况下，攻击者发起的一般恶意攻击，防火墙技术都能够有效的识别。但是，随着攻击手段的日益复杂化，使得传统的防护手段不一定能够提供有效的安全保障。如果在如图4-2的情况下，当攻击者采用高明的带欺骗性的攻击，可以成功躲过防火墙技术的识别，可对设备造成重大威胁。



图4-1 一般入侵示意图



图4-2 带欺骗性的入侵示意图

在工业控制网络中，基于欺骗性数据包的攻击，包括了IP欺骗攻击、中间人欺骗攻击等。其中，IP欺骗指的是攻击者向操作员站等具有控制权限的设备发送虚假的、欺骗等信息，造成操作员不能够获取正确的现场设备的信息，导致其可能做出错误判断，发送错误的操作命令等。如工作人员在操作员站不小心插入了恶意的USB，导致操作员站被感染，攻击者可以利用此机会进行欺骗攻击。而中间人攻击，如图4-3所示，该类攻击和欺骗攻击类似，攻击者利用网络中存在的完整性漏洞，截取网络中的数据包，恶意修改其中的数据信息后，再发送出去。该类攻击主要发生在监视控制层以及监视控制层与现场设备进行通信的过程中。并且该类攻击的危害程度较大。



图4-3 中间人攻击示意图

无论是IP欺骗攻击，还是中间人攻击，该类攻击都能成功的伪造数据包的IP、端口服务等数据包头的信息，通过修改数据内容的信息，或者构造恶意数据内容的数据包，混入网络通信中，给控制网络造成严重危害。即是通过修改数据包的应用层数据内容进行攻击。由于工业控制网络中的应用层通信协议是一些私有协议，如modbus协议、DNP3.0协议等。但是，一般的防火墙技术只能对IP、端口服务进行过滤，如加拿大多芬诺攻击的工业防火墙，西门子中国研究院研发的Janus安全网关，这类设备的技术更多的是针对TCP/IP网络层的防御，针对modbus协议、DNP3.0协议等工业控制协议的深度防御并不足。国内的和利时提出的针对工业安全的交换机，也只是可以帮助控制系统抵御来自二层的攻击，对三层以上的攻击无法提供防御。

#### 3、基于异常流量的攻击

基于异常流量的攻击可以分为两类。一类是间接攻击，主要包括了嗅探攻击和扫描攻击。该类攻击实际上是对现场设备的端口等进行监听、扫描等，以此探测出网络中存活的设备、设备开放的端口、设备的操作系统类型等。攻击者可以通过探测到的情况，为下一步入侵行为做准备。该类攻击可以发生在整个控制网络中，甚至整个控制系统，虽然不会直接造成危害，却是入侵的重要前兆。

另一类是直接攻击，其中包括了由欺骗性攻击进一步引发的泛洪攻击、口令攻击、拒绝服务攻击等。如SYN泛洪攻击是利用TCP协议缺陷，发送大量虚假的SYN连接请求，从而造成被攻击对象的资源被耗尽的攻击方式。拒绝服务攻击。此类攻击一般是通过非法手段来耗尽目标设备的资源，使得其网络层被阻塞，不能正常工作，甚至造成整个工业生产的停止或者严重事故。该类攻击还可以结合数据重组攻击、广播攻击、连接攻击等，给控制系统造成极大破坏。该类攻击的目标包括了整个监视控制层以及现场设备层的一部分。并且基于TCP/IP的工控私有协议，如Modbus、DNP3等都会受到严重威胁。口令攻击。该类攻击通过一定手段得到网络中设备的验证口令，非法登录网络中的系统，从而达到控制该设备的目的，对整个网络造成严重威胁。这类攻击包括了字典攻击、暴力攻击、重放攻击等。字典攻击指的是攻击者通过穷举的方式对要登录的系统进行密码破解。而暴力攻击也是通过穷举的方式，但是与字典攻击的区别在于前者使用的是预先定义的单词列表中的单个单词或者短语，而后者是使用的密码组合。重放攻击指的是攻击者不断的重复发送一个有效的数据包，其数据包可以是被攻击者拦截的登录口令。上述攻击的目标包括了监视控制层中的工程师站、操作员站等需要口令登录的设备。

表4-1 攻击划分

|  |  |  |
| --- | --- | --- |
| 攻击类型 | 危害程度 | 划分类型 |
| 非法IP访问 | 严重 | 恶意攻击 |
| 非法端口访问 | 严重 | 恶意攻击 |
| IP欺骗攻击 | 极为严重 | 欺骗性攻击 |
| 中间人攻击 | 极为严重 | 欺骗性攻击 |
| 拒绝服务攻击 | 极为严重 | 异常流量攻击 |
| SYN flood攻击 | 极为严重 | 欺骗性流量攻击 |
| IP扫描 | 轻微 | 异常流量攻击 |
| 端口扫描 | 轻微 | 异常流量攻击 |
| 口令攻击 | 严重 | 异常流量攻击 |
| 远程登录攻击 | 严重 | 异常流量攻击 |

综上所述，对各类攻击作分析，并根据其特点，划分了各类攻击的危害程度和危害类型，如表4-1所示。并且针对不同的危害类型，设计针对性的攻击防御方法。整个防御方法的框架，如图4-4所示。当数据流进入防御体系时，设计的抗攻击模块对基于恶意攻击的数据包和基于欺骗性攻击的数据包进行检测并阻止丢弃掉。而入侵检测模块则对基于异常流量的攻击进行检测，并加以报警。



图4-4 攻击防御总体方案

#### 4、flood 攻击

1、ICMP flood：ICMP flood是一种利用ICMP协议的缺陷，攻击者向目标主机长时间、连续、大量地发送ICMP数据包，使得目标主机消耗大量的CPU资源，最终导致系统瘫痪的一种攻击。其主要分为三类，一是攻击者直接利用构造数据包，对目标主机进行洪水攻击。二是攻击者伪造IP，对目标主机进行洪水攻击。三是攻击者伪造目标主机的IP，然后向其他服务器等发送ICMP报文，这些服务器收到报文后被欺骗，向目标主机返回大量的应答，使得目标主机的带宽被阻塞，从而瘫痪。针对ICMP flood的防御，目前普遍采用的方法是过滤ICMP报文，在防护端设置访问控制规则。

2、UDP flood：UDP flood是一种无连接的协议，没有拥塞控制。当一个网络主机收到一个来自IP层的报文时，UDP先检查报文中的目的端口是否正确。若不正确，则UDP就丢弃该报文，并请求ICMP发送端口不可达给源主机。若目的端口正确，UDP就将收到的报文放入队列的队尾，等待客户进程取走。若入队溢出，UDP丢弃收到的报文，但不知道源主机，UDP还请求ICMP发送端口不可达给源主机。UDP flood就是通过大的攻击数据包攻击网络带宽，阻塞网络。或者攻击目标主机，目标主机收到大量的UDP包，耗尽主机系统资源，导致拒绝服务。针对UDP flood的防御，目前没有完全的阻止方法，大都是只能起到缓解作用。主要的防御方法是增加网络带宽和限流。通过限流将链路中的UDP报文控制在合理的带宽范围之内。限流有三种：一是基于目的IP地址的限流，即是以某个IP地址作为统计对象，对到达这个IP地址的UDP流量进行统计并限流，超过部分丢弃。二是基于目的安全区域的限流，即是以某个安全区域作为统计对象，对到达这个安全区域的UDP流量进行统计并限流，超过部分丢弃。三是基于会话的限流，即对每条UDP会话上的报文速率进行统计，如果会话上的UDP报文速率达到了报警阈值，这条会话就会被锁定，后续命中这条会话的UDP报文都被丢弃。当这条会话连续3秒或者3秒以上没有流量时，防火墙会解锁此会话，后续命中此会话的报文可以继续通过。

3、SYN flood：SYN flood是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使得被攻击方资源耗尽（CPU满负荷或者内存不足）的攻击方式。传统的SYN flood方案有三种，一种是缩短等待时间（SYN timeout）并增大队列的SYN包最大容量（tcp\_max\_SYN\_backlog）。第二种是设置SYN cookie，主要是减少为维持很大数量半连接而分配的系统资源或者通过完成建立TCP连接释放更多的可分配系统资源。基本原理是客户端发送SYN请求数据包后，服务器接收到SYN数据包并不建立半连接，而是SYN 数据包中的源地址、源端口、目的地址、目的端口等信息用一种散列算法进行加密计算出一个cookie值，然后将该值作为SYN+ACK数据包中的序列号发送给客户端。当服务器端收到客户端发送的ACK数据包，重新将源地址等信息使用相同的散列算法计算出cookie值，然后与确认序号进行比较，如果两者相差为 1，服务器就为其分配资源，建立连接，否则的话就丢弃，拒绝请求。第三种是SYN proxy，SYN Proxy是设置每秒SYN片段数的阈值，当同一IP地址的SYN片段数达到这些阈值之一时，SYN Proxy 设备就开始截取连接请求并且代理回复SYN/ACK片段，并将不完全的连接请求存储到连接队列中直到连接完成或请求超时为止。当代理连接的队列被填满时，SYN Proxy拒绝来自相同安全区域中所有地址的新SYN片段，避免网络主机遭受不完整的三次握手的攻击。具体过程是SYN Proxy收到客户端发送的SYN包后，记录该状态信息并且向客户端发送SYN+ACK包，如果能够收到客户端的ACK包表明是正常访问，然后代理端向服务器发送同样的SYN报文，和服务器通过三次握手建立连接，连接建立后，SYN Proxy调整双方通信过程中的序列号和确认号，确保通信正常。SYN Proxy完成客户端和服务器端的连接，可以过滤不可用连接发往服务器，避免服务器资源的浪费。除了以上比较传统的方法外，在是对上述方法基础上进行改进，或者提出一种改进算法来实现防御。

## 五、抗攻击策略设计

安全策略的目的在于能够有效的实现对攻击的防御。本节所要进行防御的攻击主要包括的是基于IP的非法访问攻击、基于端口的非法访问攻击、欺骗性攻击以及SYN flood攻击。各个攻击的实现手段、攻击特点、攻击范围以及危害程度都存在着一定的差异。



图5-1 基于IP的非法访问

如图5-1所示，基于IP的非法访问攻击在工业控制网络中表现为，监视控制层的工程师站对控制中心定义的其不能访问的现场设备层的PLC或者控制器，进行非法的访问操作等。其攻击特点在网络通信中体现为利用非法的IP地址进行数据的发送等。而欺骗性的攻击则是攻击者利用一系列渗透手段，已经获得了在控制网络中的合法权限，然后进行伪造或者修改其他的数据信息来实现攻击。

鉴于此，本抗攻击策略设计，则是根据所要防御的攻击类型、攻击特点以及攻击的危害程度而制定。所以，本章节提出的安全策略总体框架如5-2所示。该策略总共分为了三大部分，即是针对基于IP非法访问攻击的安全域策略，针对基于端口非法访问攻击和部分欺骗性攻击的白名单访问控制策略，以及针对syn flood攻击的安全策略。



图5-2 安全策略设计总体框架

1. 安全域策略设计

安全域（security region），在传统IT网络中是指同一区域内具有相同的安全保护需求，相互信任，并且具有相同的安全访问控制和边界控制策略的子网或者网络，而且相同的网络安全域共享一样的安全策略。

在工业控制网络中，资产、设备的通信、访问以及操作并没有传统IT网络那样复杂。而且，控制网络中生产过程所涉及的控制设备与执行设备之间的关系，即是配置、组态、下发、刷新、监测等一系列的控制流程，在某种程度上都是比较固定的。如图5-3所示，工程师站A、操作员站B以及PLC三者之间共同完成一个生产项目，将其划分为安全域1。而工程师站B和控制器则一起完成另一项目，将其划分为安全域2。这样划分的意义在于，它们都工作在自己的安全域内，都有自己的一套域内安全策略，而且如果发生了跨域的非法操作行为等攻击行为，则更容易被发现以及处理。所以，制定合理的安全域策略能够更高效的、更精确的保证工业控制网络中的通信安全。



图5-3 安全域划分

通常的安全域制定主要是从网络连接、控制功能、登录访问、控制数据的存储、关联通信等角度来考虑。本小节的策略则是根据工业控制网络中资产间的通信行为、操作行为等，以及结合攻击的攻击特点来制定。具体设计方法如图5-4所示：

1. 对整个控制网络进行风险评估，并确定资产的重要等级。
2. 明确各资产所属的系统结构层次，即企业管理层、监视控制层以及现场设备层，并获取其IP地址等能够表明其所处位置的信息。
3. 根据各资产在网络中实现的功能或者操作，将完成同一控制过程或者同一环节的资产，划分在同一安全域内。
4. 标记安全域，记为，其中，表示资产设备位置信息。



图5-4 安全域设计

1. 针对IP地址欺骗的安全策略设计

欺骗性的攻击一般包括了多种欺骗类型。主要针对基于IP地址和MAC地址的欺骗性攻击来进行抗攻击策略设计。该类攻击一般分为域间IP欺骗和域内IP欺骗。所以。如图5-5所示，演示的是一个IP欺骗的全过程。由于在安全域内，所以假设攻击者X已经获得了域内的访问权限，目标设备A和被冒充设备B是信任关系。在实施欺骗前，攻击者X先通过一定手段使得设备B不能工作。然后攻击者X向设备A进行多次试探，了解ISN（初始序列号）的规律。之后，攻击者X伪造源地址为设备B、ISN为m的SYN包向设备A请求连接。设备A在收到所谓的“设备B”的请求包后，向“设备B”返回SYN+ACK包其中包括A的ISN为n，确认号为m+1，并等待“设备B”返回的ACK包。攻击者X在收到A返回的SYN+ACK后，通过某种手段估算出了应答号为n+1，并构造源IP为B的ACK包，发送给设备A。设备A收到ACK后，此时就认为自己是和设备B建立了连接。但实际上是攻击者X伪装的“设备B”。此后，攻击者X就可以对A进行更深层次的攻击了。



图5-5 IP欺骗过程分析

综上分析，IP欺骗主要利用的是设备间的信任关系，伪造IP地址以及利用三次握手的通信规则，伺机伪装发动攻击。由于MAC地址是全球唯一的，所以一般针对IP欺骗攻击的防御手段是将IP地址与MAC地址进行绑定构造一张表，然后通过匹配来实现防御。此种方法在一定程度上能够识别出IP欺骗，特别是在工业控制网络中，各个资产间的通信、访问、操作行为是比较有规律性的。但是如果攻击者同时获得了目标的IP地址和MAC地址，那么上述绑定的防御方法就失效了。而通过图5-5欺骗过程，可以发现，攻击者X在第五步返回给设备A的ACK包时，其中要返回一个n+1的应答号，而这个应答号是攻击者X自己估算的。而我们则可以通过构造出复杂的ISN，增加攻击者估算难度，使其不能够成功实现连接。鉴于此， 本小节设计一种基于IP和MAC地址绑定结合ISN重构造的安全策略，其框架如图5-6所示：



图5-6 针对IP欺骗的抗攻击策略

1. 当收到SYN包时，对其解析，并通过IP地址和MAC地址表进行IP与MAC的匹配。如果匹配失败，则丢弃此包，成功则进入下一步。
2. 通过cookie计算的方法对ISN进行重构，再载入SYN+ACK包中，并返回给发送方。
3. 下一时刻收到ACK包后，对其返回的确认号进行cookie计算，并进行验证。如果验证成功则进行连接，验证失败则不予以连接。
4. 白名单控制策略设计

在划分好安全域后，其使得各个划分好的区域之间有了一个有效的通信防护。然而，对于域内的安全防护，也需要制定相关的安全策略。如图5-6所示，在安全域内，工程师站A被允许对访问PLC1的502端口，而工程师站B被禁止。但是在某时刻，工程师站B的被感染或者工作人员恶意操作访问PLC1的502端口达到攻击目的。更有严重情况，如图5-7所发送的欺骗性攻击，攻击者通过某种手段获得安全域内合法的权限或某合法资产的信息。再伪装成合法的资产，欺骗域内其他资产，建立合法连接，发送恶意篡改的数据内容如对某PLC的线圈数据进行修改，导致工艺出差错或者严重生产事故发生。所以，针对上述攻击类型，在安全域内制定相应的安全策略显得尤为重要。



图5-6 对于端口的非法访问



图5-7 基于操作内容的欺骗性攻击

对于安全域内的安全防护，通常的模型如下所示：





其中，指的是源地址，指的是源端口，指的是目的地址，指的是目的端口，指的是对数据操作，总共包括3种操作：

：指的是对数据进行允许通过操作。

：指的是对数据进行丢弃操作。

：指的是允许数据通过，但同时发送报警。

此模型只是对网络层和传输层的数据信息设定了安全策略，但是对于上述的通过篡改应用层中操作相关的数据内容而进行的欺骗性攻击却无能为力。鉴于此，根据上述攻击在网络层、传输层以及应用层所表现出的攻击特点，提出基于白名单的安全策略，设计模型如下所示：





其中，表示源地址，表示源端口，表示目的地址，表示目的端口，表示功能码，表示操作对象起始地址，表示操作对象的数目，表示对数据的操作，而白名单策略的操作是允许，即。

基于白名单策略的设计过程如图5-8所示：

1. 在划分好的安全域中，根据安全域内各资产设备间的通信行为、访问行为、操作行为等基于数据包交换的特点，定义合法的通讯集合。
2. 将上述定义好的合法通讯集合，通过本小节设计的白名单模型予以表示出来。
3. 对其他不包括在上述合法通讯集合的数据，全部予以丢弃操作。



图5-8 白名单策略设计

1. 针对syn flood的安全策略设计

针对基于IP地址和操作内容的欺骗性攻击作了抗攻击策略的设计，但是攻击者还可以通过感染安全域的操作系统或者伪装合法的IP地址，向目标机发送大量的伪造TCP连接请求来发动syn flood攻击。如图5-9所示，是TCP三次握手正常情况下和异常情况下的syn flood攻击。在正常三次握手情况下，Host A向Host B发送SYN连接请求包，Host B接收到请求包后，向Host A返回SYN+ACK包。在Host A接收到返回的包后，再向Host B返回一个ACK包，至此表示三次握手成功。而在发动syn flood攻击时，攻击者通过某种手段获得Host A的信息后，伪装成Host A不断向Host B发送SYN包，而Host B则不断的发送SYN+ACK进行回应。与此同时，攻击者不再返回ACK包，使得握手一直处于半连接状态。而Host B的系统资源一直被积压在其连接队列中，最终Host B的资源被耗尽，甚至造成系统崩溃。此种情况若发生在工业控制网络中，将导致严重生产事故发生，后果不堪设想。所以，针对syn flood攻击的安全策略设计，也显得很有必要性。



图5-9 TCP三次握手正常与异常情况

针对syn flood攻击的防御，一般传统的方法是利用syn proxy技术，其原理是通过提高连接资源的利用率来实现防御。但是该类方法在出现攻击流量比较大时，却无法起到好的防御效果。鉴于此，根据上述攻击特点，并结合syn cookie技术，设计了一种防御syn flood的安全策略，其策略框架如图5-10所示。假设在大量SYN 包到达Host B时，针对不同IP地址来的SYN包，进行一个计数统计，并设置一个阈值。那么，当来自同一IP地址的SYN包的个数小于所设阈值时，允许再到达的SYN数据包通过，如果是大于了所设阈值，就丢弃再到达的SYN数据包。而对于到达的来自同一IP地址的ACK包，由于此类数据包是三次握手中，Host A和Host B已经建立了半连接才会收到ACK包，说明了Host A和Host B之间属于正常的连接。此时，因为已经明确了是正常的连接，所以对此ACK包对应IP地址的SYN包的计数进行减一。其他IP地址传来的SYN包和ACK包也按上述方法进行处理。当数据包到达算法模块后，在表中进行查找是否有相匹配的IP，如果没有，直接将数据包信息写入表中。如果有，则判断此数据包是什么类型的数据包，如果是SYN包，则判断表中flag（数据包个数阈值）大小，若大于n，直接丢弃此数据包，若小于或等于n，flag进行加1，并将此包转发。如果是ACK包，则对flag减1，并转发此数据包。



图5-10 针对syn flood安全策略设计框架

## 六、抗攻击测试

抗攻击测试属于安全测试的一种，是对系统安全性的一个侧面的测试和评价，是一种反向的安全测试。抗攻击测试的目的是为了测试系统的安全性，但由于系统的安全性的正向测试复杂性较高、标准不易实施、专业性较强、直观性较差，我们采用一种反向的安全测试的思路，即，通过对系统发起实际的攻击，从攻击的结果来反映和评价系统的安全性，为了测试系统在多大程度上是安全的，我们先来测试系统在多大程度上是不安全的、可以被哪些攻击所攻破、对哪些攻击的抵抗能力相对较强。抗攻击测试的测试和评价结果对系统用户和管理员来说，相对更简单和易于理解，不用具备很强的专业安全知识就可以对测试的结果有一个直观的认识，并且，抗攻击测试的测试和评价能够直接为系统的安全性改进提出针对性较强的解决方案，这种安全解决方案直接以实际的攻击测试数据为依据，为攻击测试结果中系统相对薄弱的安全性能提出相应的改进意见和方案，可以对症下药，增强安全方案的有效性和说服力。

抗攻击测试本身并不能证明系统是绝对安全的，抗攻击测试是为了直观、有说服力地证明系统是不安全的以及在多大的程度上是不安全的，并给出系统安全改进的意见。这是抗攻击测试的出发点和立足点。因此，抗攻击能力的评价是一种相对的安全评价，通过对系统实施攻击，用攻击的程度和结果来评价系统的相对的抵御攻击能力，我们通过测试和综合评价得出的系统的抗攻击能力也是一个相对的值，只能反映系统在现有攻击手段前提下，系统对各种攻击的抵御能力，即抗攻击测试只能对系统的相对安全性进行测评。

抗攻击测试的测试主要分为三个部分:模拟攻击、系统检测和抗攻击能力评价。模拟攻击阶段主要是通过组织调度攻击工具、攻击脚本对目标系统实施攻击，并将攻击的信息传递到系统检测和抗攻击能力评价部分，系统检测主要用于检测攻击前后目标系统和攻击平台系统各方面信息的变化情况，抗攻击能力评价是在模拟攻击和系统检测的基础上，对系统的抗攻击能力进行定性或定量的评价，给出系统的抗攻击能力测试结果。整个抗攻击

测试的框架结构如图4-1所示。

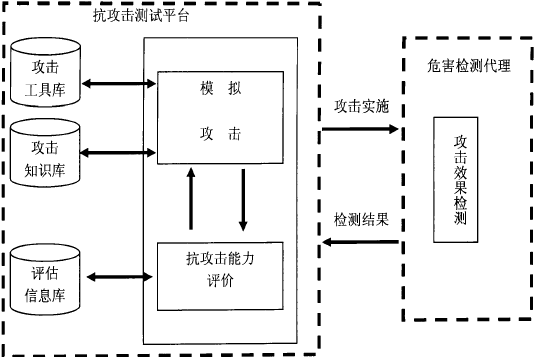


图4-1 抗攻击测试框架

在抗攻击测试中，抗攻击能力评价是整个测试中的最后一个环节，是对整个攻击测试、分析和综合的一个过程，其依据是攻击测试的过程和结果数据，目标是对抗攻击能力给出定性或定量的评价，从而对系统的抗攻击能力进行相对的评价和描述，为进一步的安全解决方案的提出奠定基础。

## 七、结束语

通过对系统的抗攻击能力进行测试，发现采用了深度包检测和访问控制技术的系统，抗攻击能力显著提高，基本能够满足工业控制系统对信息安全的要求。