网络与系统安全大作业

靳宗明

网络空间安全学院,南开大学,天津,中国, zongming_jin@mail.nankai.edu.cn

目录

1 引言

在设计 TCP/IP 网络协议和 OSI 标准通信模型的初期，网络设计者关心的问题是如何将数据从一台计算机有效和可靠的传输到另外一台计算机上去。数据的安全性在当时并没有提到议事日程。因此，TCP/IP 通信协议和 OSI 标准通信模型没有内置的安全机制。当人们逐渐意识到这个设计缺陷之后，便想方设法在现有的框架内加入各种安全机制。但是由于网络架构最初的设计并没有加入安全设计，所以后期加的各种安全机制也会存在各种各样的问题。

无论是有意的攻击还是无意的误操作，都会给系统带来不可估量的损失，攻击者可以窃听网络上的信息，窃听用户的口令、数据库的信息；还可以篡改数据库的内容，伪造用户身份，更严重的是，攻击者还可以删除数据库的内容，摧毁网络节点，释放计算机病毒。

所以本文从现有的问题出发，分析传统网络架构的安全问题，然后根据不同的问题设计一种新的网络架构,能在系统设计上解决目前的安全问题。不仅如此，

本文在最后一部分还会引人区块链的使用，因为这一部分和我本人的研究方向相关，我本人上一段的研究方向是异构物联网安全，为了使各种异构网络、异构终端可以接入物联网系统，我采用了区块链的方法进行作为网络的中间层向上层进行屏蔽，这样可以使网络更加安全，动态，屏蔽底层差异。

2 背景介绍

（1）传统网络架构

这一部分会简单介绍一下传统的网络结构，如图 1 是传统的 OSI 和 TCP/IP 协议簇图示。

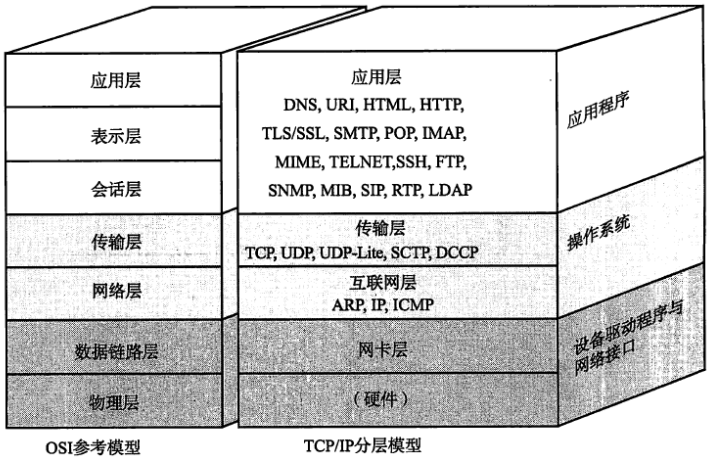

图 1 传统网络结构

链路层下面还有物理层，指的是电信号的传输方式，比如常见的双绞线网线，光纤，以及早期的同轴电缆等，物理层的设计决定了电信号传输的带宽，速率，传输距离，抗干扰性等等。在链路层本身，主要负责将数据跟物理层交互，常见工作包括网卡设备的驱动，帧同步（检测什么信号算是一个新帧），冲突检测（如果有冲突就自动重发），数据差错校验等工作。

网络层的 IP 协议是构成 Internet 的基础。该层次负责将数据发送到对应的目标地址，网络中有大量的路由器来负责做这个事情，路由器往往会拆掉链路层和网络层对应的数据头部并重新封装。IP 层不负责数据传输的可靠性，传输的过程中数据可能会丢失，需要由上层协议来保证这个事情。

网络层负责的是点到点的协议，即只到某台主机，传输层要负责端到端的协议，即要到达某个进程。典型的协议有 TCP/UDP 两种协议，其中 TCP 协议是一种面向连接的，稳定可靠的协议，会负责做数据的检测，分拆和重新按照顺序组装，自动重发等。而 UDP 就只负责将数据送到对应进程，几乎没有任何逻辑，也就是说需要应用层自己来保证数据传输的可靠性。

应用层位于计算机网络体系结构的最上层，前面四层做的所有事情就是为了他服务，他也是设计和建立计算机网络的最终目的，通俗的讲，就是我们开发的应用软件，就处于这一层，比如，QQ，浏览器访问网页，等等你看得到的应用软

件都是在这一层，但是这些软件在运行的过程中，也需要依靠一些特定的协议才能完成相应的功能。

（2）网络安全的需求

从上述网络架构中可以发现，传统的网络设计并没有特殊的考虑安全因素，目标就是为了更好的更快的更简单的实现两台计算机或两个端节点之间的传输和通信。为了设计一种新型安全的网络架构，其实就是为了保护联网计算机系统不被入侵，保证存储在计算机系统中的数据以及在网络上传输的数据不被窃取、篡改和伪造。简单来说，就是为了达到如下四种要求特性。

1、数据机密性(Confidentiality)

保证存储和传输中的数据不被第三者读取

2、数据完整性(Integrity)

保证存储和传输中的数据不被第三者篡改

3、数据和服务的可用性(Availability)

保证计算机系统资源不会被第三者通过漏洞阻碍合法用户使用

4、数据的不可否认性

保证数据的合法拥有者无法向他人抵赖自己是该数据的拥有者

3 新型网络架构设计

为了设计新型的安全的网络架构，我将会利用课上学的四个点优化现有的 TCP/IP 网络架构，这四个点分别是：密码系统（Cryptosystem），防火墙(Firewall)，抗恶意软件(AMS software)，入侵检测系统(IDS)。

如图 2 就是新型安全网络架构的层级图示。

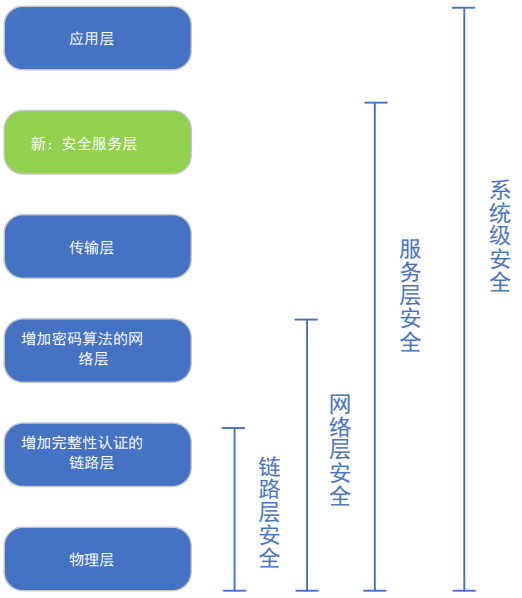

图 2 新型安全网络架构层级图示

相比于传统的 TCP/IP 网络架构，我在其中的几层进行了一定的修改优化，在传输层和应用层之间添加了一层，命名为服务层，下面自底向上介绍这种新型安全网络架构。

（1）链路层安全

为了保证链路层的安全，我优化了链路层的传输结构，尤其是添加了链路层的完整性认证，因为传统的链路层没有只有简单的 CRC 校验，只能保证接收数据的正确性，且恶意攻击简单，只需附上修改后的 CRC 校验和即可，我使用了密码系统中的散列函数来保证链路层数据传输的真实完整性，具体方法可以使用 hash，如果有更高的安全性要求，也可以使用更加安全一些的 HMAC 来保证数据传输的真实有效性。

（2）网络层安全

为了使网络层变得更加安全，我设计了一种面向用户的网络层安全模型。

传统的 IPSec 协议主要包括安全关联 SA、安全关联数据库 SAD、安全策略数据库 SPD、安全协议 AH/ESP、网络安全关联和密钥管理协议(ISAKMP)、网络密钥交换协议(IKE)和相关的 IPSec 协议方式(包括隧道模式、传输模式或通配符模式)等要素。其中的 IKE 协议是 ISAKMP、SKEME 和 Oakley 三种协议的混合体。它主要负责为需要安全网络通信的任意两个网络节点建立信任关系，并在此基础上协商它们今后进行安全通信所必需的各种安全连接 SAs。

不论是 IPSec 协议本身，还是诸如 FreeS/WAN 这样的具体协议实现，它们都有一个共同的不尽如人意的地方，那就是它们本质上只为网络中任意两个网络节点间提供安全通信服务。而在很多的网络应用中，真正需要的是面向用户的网络安全通信服务。另外，IPSec 协议本身也没有考虑通信安全策略和信任管理问题，这使得 IPSec 协议在一个实际的网络安全应用中还显得不够完备。

面向用户的网络层安全通信模型的结构如图 3 所示。其中的 NN 代表所有可信的网络节点。这些网络节点可以属于一个分布在网络上的安全网络会议系统，也可以属于一个企业/事业单位的内部信息网。面向用户的网络层安全通信模型就是要为这些网络应用在网络层构建一个通用的、面向用户的安全通信环境。这个安全通信环境对其上的网络应用和网络应用中的用户来说，应该是透明的。用户不必了解该安全通信环境的实现细节，唯一需要做的就是在登录上述网络应用系统时，向所在网络节点提供自己的私有信息(包括用户身份信息和个人私钥等)。

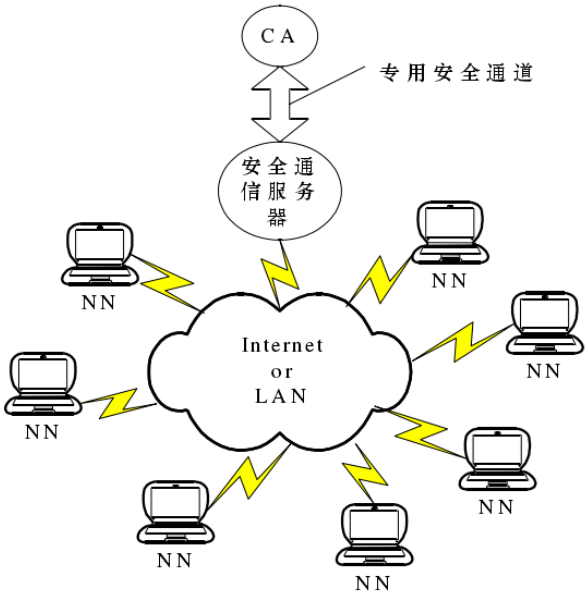

图 3 面向用户的网络层组网结构

（3）服务层安全

我在传输层和应用层之间添加了一层叫做安全服务层，这一层向上层提供安全服务，屏蔽下层网络变化，简单工作流程设计如 4 图所示

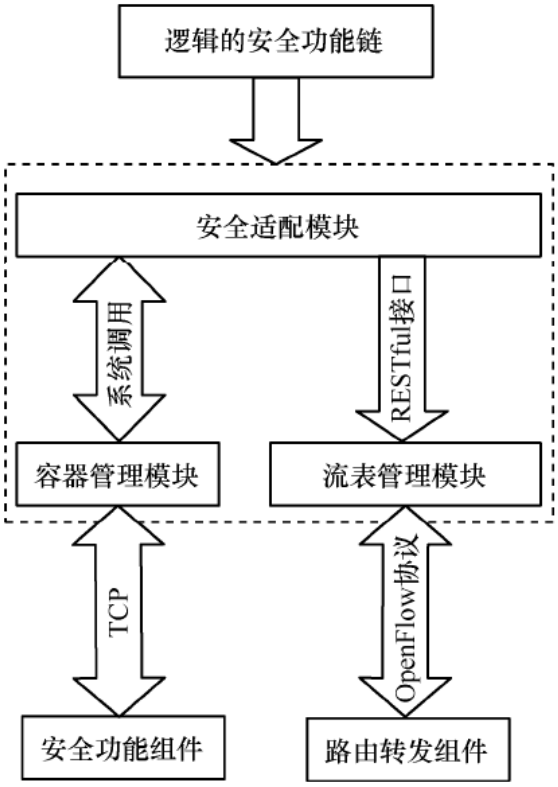

图 4 服务层安全功能链

（1）网络管理员通过安全需求配置界面定制所需的安全服务，生成逻辑的安全功能链。

（2）安全适配模块采用系统调用的方式向容器管理器请求提供相应的安全功能实例，后者基于当前的资源信息，选择已有的安全功能实例或创建新的安全功能实例，并返回所选实例的网络信息。

（3）安全适配模块调用 RESTful 接口向流表管理模块通告该安全功能链的转发配置。

（4）流表管理模块利用 OpenFlow 协议向数据转发层中的安全感知组件和路由转发组件下发流表配置。

（4）系统级安全

我将包含应用层的系统的安全抽象成系统级安全，在此我将加入防火墙、抗恶意软件(AMS software)，入侵检测系统(IDS)在系统高层来保证网络架构的安全。

防火墙是一种高级访问控制设备，置于不同网络安全域之间的一系列部件的组合，它是不同网络安全域间通信流的唯一通道，能根据企业有关的安全政策控制（允许、拒绝、监视、记录）进出网络的访问行为。简单来说，防火墙就是根据访问控制规则决定进出网络的行为的一种设备。如图 5 所示，对于没有防火墙存在的一条网络路线中，主机 A 发送给主机 B 的任何一个数据包，主机 B 都会照单全收，即使是包含了病毒、木马等的数据也一样会收。

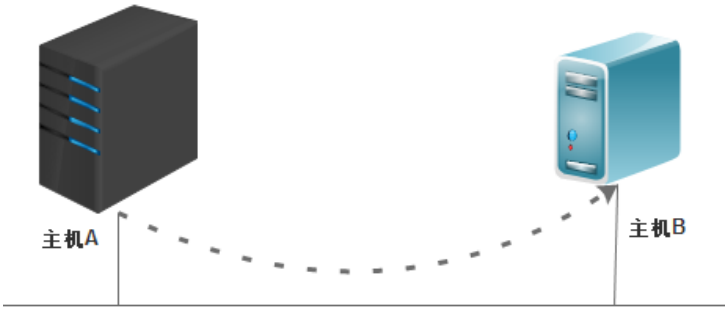

图 5 无防火墙系统

如图 6 所示，有了简单的防火墙之后，在数据传输的过程中就会接受"入关"检查，能通过的数据包才继续传输，不能通过的数据包则拒绝或者直接丢弃。

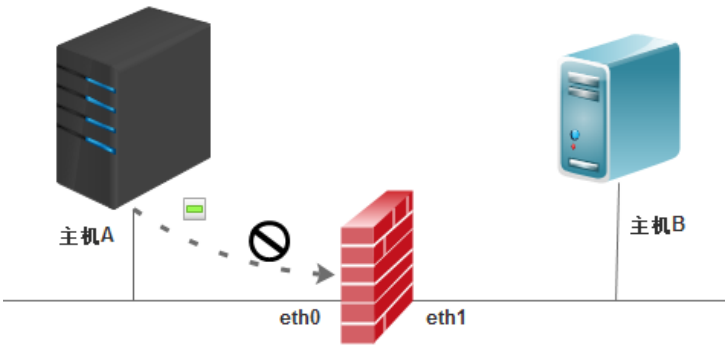

图 6 有防火墙系统

抗恶意软件指的是能抵抗各种恶意攻击的安全软件，能够进行各种恶意代码、程序、行为的检测，包括病毒，蠕虫，木马，攻击的检测。在系统级安装特定的

抗恶意软件，进行周期性标准化扫描，进而保证系统级的安全。

传统上，防火墙作为第一道防线能够进行一定程度上系统级安全防护，然而，随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多变，单纯的防火墙策略已经无法满足对安全高度敏感的系统需要，在这种环境下，入侵检测系统便不得不作为第二道防线深入的进行入侵检测。

入侵检测，就是对入侵行为进行发觉，它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析。从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。具体来说，入侵检测系统的主要功能有：检测并分析用户和系统的活动，核查系统配置和漏洞，评估系统关键资源和数据文件的完整性，识别已知的攻击行为，统计分析异常行为，操作系统管理，并识别违反安全策略的用户活动。

4 基于区块链的网络结构介绍

下面是我上一段时间做的基于区块链的一点研究，其应用场景虽然是物联网，但是完全可以将其扩展到整个互联网络架构中去，然后这个研究点的目的就是基于区块链的物联网安全，在这其中我采用区块链作为一个中间层来实现网络中信息的安全存储，整合，传输，然后在上层添加一些异常检测算法，保证最终应用层的安全运行。

（1）区块链介绍

区块链技术，可以理解为由多方参与共同维护的一个分布式数据库，也称为分布式账本技术。区块链数据存储在点对点（P2P）网络中的分布式节点中，每个参与者都要维护一个账本副本，其特性就是只能单方向增加，而不能修改或者删除之前添加的交易信息，并且每一笔交易或者账本信息都被独一无二地由相应的参与方进行签名。随着比特币的提出以及盛行，使得区块链技术也进入人们视野。比特币是中本聪提出的一种电子支付系统，其的特点就是分布式，去中心化，利用密码学的方法保证交易的正确性和完整性。由于其如上的特性，自 2009 年应用以来，比特币一直正确地运行，并且从来没有发生一笔错误的交易。随着人们对区块链技术的认识逐渐加深，其应用范围不断扩大，从金融领域逐渐扩展到物联网、车联网领域，虽然实际的应用还没有落地，但是其作为一种分布式的、防篡改的、透明且安全的技术已经在学术领域广泛应用，由于其天然的特性，在未来将会应用于生活的方方面面。

（2）基于区块链的网络架构

基于区块链的网络架构从下到上分别是设备层，边缘层，服务层，应用层。在边缘层我应用了区块链网络进行资源的安全存储，收集，如图 7 所示。

图 7 基于区块链网络的层级结构

设备层是各种各样的终端设备，它们具有在运行过程中会产生各种各样的安全问题，然而局限于其较低的计算力和较弱的安全防御能力，需要将各种安全相关日志上传，然而在日志信息上传存储也是不安全的，这就变得更加棘手和难以解决。

所以在边缘层我使用了区块链作为一种安全的组网手段向上层屏蔽了终端设备层的异构特点，同时也能保证数据存储的安全和完整。

然后就是服务层，服务层我增加了一些智能的异常的检测算法，包括简单的异常分类器算法还有一些复杂的高计算力的 AI 异常检测算法，所以在这一层就已经在服务上保证了应用的安全。

如上就是对基于区块链的一种安全网络架构的简单介绍，主要是将区块链引入网络中的一种尝试，由于区块链良好的密码学安全架构，其可能在未来会得到更广泛的引用，但是不得不解决目前区块链技术还存在的各种各样的问题，尤其是扩展性差的问题，这也是阻碍区块链得到广泛应用的一个最大的阻碍。

5 总结与展望

目前的网络架构还是遵循传统的 OSI 和 TCP/IP 的设计方式，然而 OSI 和 TCP/IP 架构的设计初期并没有考虑过多的安全问题，主要原则就是为了保证数据能传输到对方节点，然而随着恶意攻击数量和水平不断提高，传统网络架构的安全问题变得越来越严重，虽然在后来的网络架构发展中添加了各种安全方案来保证网络的安全，例如 IPsec、SSL 等，但是其只能保证当前层数据传输的安全和有效，无法形成统一的安全架构体系。虽然目前相关研究人员提出了各种各样新型的网络安全架构模型，但是也都很难再现实中应用。所以优化传统网络架构，增加安全方案，保证数据传输的安全和完整，更具有现实意义。

区块链技术从中本聪提出比特币以来就进入人们的视野，但是我认为，区块链的思想对我们的影响远大于区块链技术对我们的影响，其提供了一种达到大规模分布式共识的新方案，为我们现实中的网络设计提供了新的借鉴。