# 网络安全

**Priyank Sanghavi, Kreena Mehta\*, Shikha Soni\*\***  
EXTC, D.J Sanghvi College of Engineering  
 IT, Sardar Patel Institute of Engineering  
EXTC, D.J Sanghvi College of Engineering

**摘要-**网络安全对于个人计算机用户，组织和军队变得越来越重要。随着互联网的出现，安全问题成为一个主要的关注点，有关安全的历史能够使我们更好的理解网络安全技术。因特网因为它自身的结构允许了安全威胁的出现。如果因特网的结构能够改变，就可以减少通过网络发送的可能攻击。了解网络攻击的方式能让我们在一定程度上避免受到攻击。许多企业通过防火墙和加密机制保护自己免受网络攻击。企业创建一个“内联网”，在保持连接到互联网的同时,防止可能的安全威胁。保证整个网络的安全是一项巨大的任务,它正处在一个领域进化阶段。为了了解今天的研究进度，有关因特网的背景知识，缺陷，通过网络攻击的方法以及安全技术都是至关重要的因此要再次被提及。

**索引词**-数据安全，因特网结构，IPv4，网络安全

## I.前言

由于因特网的存在和网络技术的发展，世界变得更加互联化。在全球网络基础设施

上有大量的个人、商业、军事和政府信息。网络安全正在变得越来越重要,因为知识产权通过互联网,可以很容易地获得，违背知识产权的行为也会发生。

有两种完全不同的网络:数据网络和交换机组成的同步网络。因特网被认为是一种数据网络，因为当前的数据基于地理网络由计算机路由器组成，信息可以通过特殊的程序获取,如植入到路由器中的“木马”。同步网络,由交换机不缓冲数据,因此不受到攻击者的威胁。这就是为什么在网络安全上总是强调网络上的数据,例如因特网和其他的接入因特网的网络。

通过下面的几点研究可以对网络安全这个话题进行分析：

1. 网络安全方面的架构和互联网的脆弱性
2. 网络攻击的类型和防护方法
3. 网络接入互联网的安全性
4. 当前网络硬件和软件的发展

## II. 网络安全

系统和网络技术是各种各样的应用程序的关键技术。网络和应用都得保证安全。尽管网络安全是至关重要的，但明显缺乏容易实现的防护方法。

在安全技术人员和网络开发者之间存在一个“沟通差距”。基于开放式系统接口（OSI）模型的网络设计是一个很好的方法。不同层次的协议可以很好的协作来创建一个允许模块化开发的堆栈。个别层次的实现可以在后面更改而不需要进行其他另外的调整，这样能使开发更加的灵活。和网络设计相反，网络安全的设计就没有做到很好的扩展。没有一个可行的方法来管理网络安全的需求。安全网络的设计没有和网络设计的那些优点。网络的安全性并不是确保终端计算机的安全。当我们通过信道传输数据时应尽量避免收到攻击。黑客能够攻击特定的信道，获取加密了的数据并解密然后插入一些错误的信息。保证中间网络的安全和保证计算机的安全及加密信息同样重要。

当我们开发一个安全的网络时，以下几点需要被考虑到[1]：

1. 可访问性-通过认证的用户可以通过特定的网络进行通讯
2. 机密性-网络上的信息仍然是私有的
3. 真实性-确保网络上的用户是他本人
4. 完整性-确保消息在传送过程中没有被修改
5. 非否认性质-确保用户不会拒绝使用网络

正是因为对安全问题，对潜在攻击者，对所需的安全级别以及对能使网络易遭受攻击的因素的理解，一个有效的网络安全计划才能被发展。有很多安全产品可以使我们的计算机受到尽量少的攻击。比如信息加密，防火墙，入侵检测，身份验证等。世界上使用比较普遍的产品是它们的混合产品。企业内部网络不仅能够连接到互联网并且还能起到很好的保护作用。因特网的自身架构导致了他在网络安全方面的缺陷。了解互联网的安全问题大大有助于开发安全的解决方案。

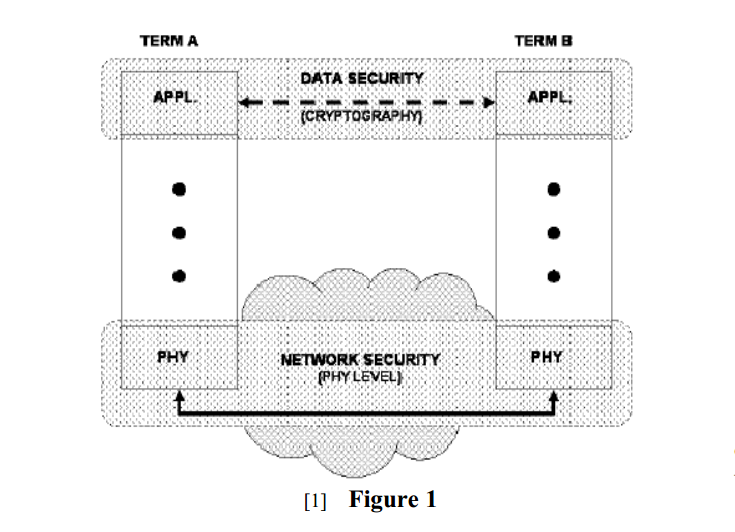
通过互联网攻击的类型也是需要研究的并且能够检测和防范，入侵检测系统是基于最常用的攻击类型建立的。网络入侵的数据包能引起问题的原因如下：

* 毫无原因的消耗资源
* 利用系统资源的预留函数来进行干扰
* 获取系统的信息如密码登录信息等这些可以用来进行后续的攻击

III. 区分数据安全和网络安全

数据安全是安全的方面,允许一个客户的 数据转换为我们无法理解的数据来进行传输。即使这些无法理解的数据被拦截，也需要密钥来进行解码。这种方法在一定程度上是有效的。过去比较健壮的加密方法在现在可以很容易的被破解。由于黑客的技术的不断进步，加密方法需要发展的更快一步才行。

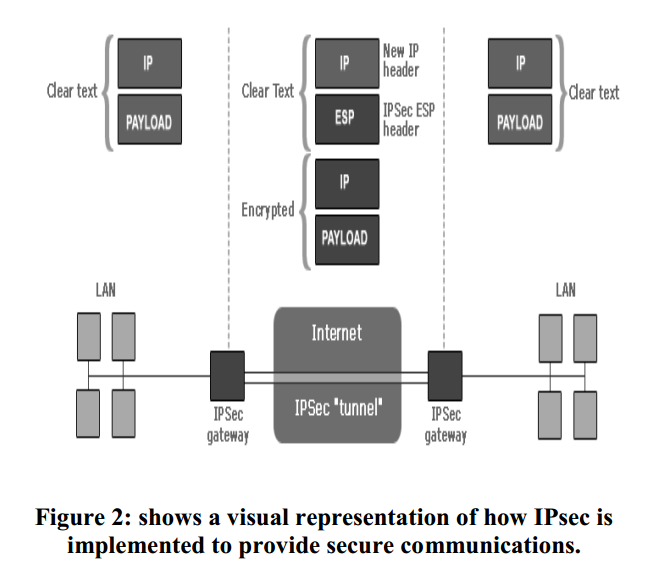
当在网络上翻译一段密文，一个私有的网络是行之有效的。这就能使密文能够得到很好的保护，所以对大多数来说尝试对它进行破坏是不太可能的。一个安全的网络也将阻止某人 从未经授权的消息插入网络。因此，硬编码也硬性攻击网络都是必需的。



在OSI模型中，数据安全和网络安全的关系如图1所示。可以看出机密主要出现在应用层；因此应用层的开发人员应当意识到它的存在。用户可以选择不同的方法来保证数据的安全。网络安全主要包含于物理层中。物理层上面的其他层也可以用来完成网络安全的需求。身份认证通常在物理层之上的某一层来完成。在物理层网络安全需要进行故障检测、攻击检测机制和智能的反测量策略[2]。

## IV. 互联网体系结构和安全性的脆弱方面

对网络漏洞的恐惧导致组织普遍采用受到保护的私有网络或企业内部网络。互联网工程任务组(IETF)引入了安全机制在各层网络协议套件[4]。这些安全机制允许逻辑保护通过网络传输的数据单位。对当前的版本和新版本的互联网协议进行分析来确定安全的影响。尽管安全可能存在于协议中,并不是所有的攻击都是严格的被防护。对这些攻击进行分析来确定其他安全机制可能是必要的。互联网协议的安全体系结构被称为IP安全是网络安全的标准化。IP安全、ip安全协议，涵盖了新一代的IP(IPv6)以及当前版本(IPv4)。尽管新技术,如ip安全协议最好地安全克服了互联网的已知量不足, 但他们似乎还不够[5]。



IP安全协议是一个点对点的协议，一方加密, 另一方解密,双方共享单个密钥或多个密钥。IPsec可以 用于两种模式,即传输模式和隧道模式。

## V. 通过当前的网络攻击IPV4协议

### 1.常见的网络攻击方法

常见的网络攻击方法被分解成不同的类别。一些攻击获得系统的信息或个人信息,如窃听和网络钓鱼攻击。攻击同样会干扰系统的预定功能，如病毒、蠕虫和木马。其他形式的攻击可以使系统的资源白白消耗，这些可以通过拒绝服务(DoS)攻击。其他形式的网络 入侵也存在,如land攻击,surf攻击，teardrop攻击。这些攻击并不像DoS攻击一样出名,但它们用于某种形式的攻击,即使没有提到它们的名字。

1.1窃听

拦截通讯中未经授权的信息叫窃听。消极窃听是只偷偷听网络消息，而消极窃听则是将其他的信息插入到信息流中。这可能导致信息被扭曲。敏感信息可以通过这种方式来获取。

1.2 病毒

病毒自我复制的程序使用文件感染和传播[8]。一旦打开一个文件,病毒将在系统中被激活。

1.3蠕虫

蠕虫和病毒很相似，因为他们都是自我复制,但蠕虫不需要文件来进行传播[8]。有两种主要类型的蠕虫,邮件批量转发蠕虫和网络蠕虫。邮件转发蠕虫使用电子邮件作为一种手段来感染其他电脑。网络自适应蠕虫是网络的一个主要问题。一旦它访问目标主机, 它可以通过木马或其他方式进行感染。

1.4木马

木马似乎是良性的用户程序,但实际上会有一些恶意的目的。木马通常携带一些载体，如病毒[8]。

1.5网络钓鱼

网络钓鱼是为了从个人、团体或组织获取机密信息 [9]。钓鱼者通过欺骗用户来透露个人信息,如信用卡号网上银行凭证和其他敏感信息。

1.6 IP欺骗攻击

欺骗IP是计算机的地址的镜像,它可以伪装成可信计算机的地址以访问其他电脑。入侵者身份被隐藏了，这意味着检测和预防更加困难。利用当前的IP协议技术、IP欺骗数据包不能被消除[8]。

1.7拒绝服务

拒绝服务攻击是当系统接收过多的请求，而不能对相应进行响应[9]。然后系统消耗资源等待着握手操作的完成。最终,系统不能回应，请求呈现不服务。

### 网络安全技术

互联网威胁在全球仍是一个重大的问题，只要世界上有信息通过访问互联网和传输。不同的防御和检测机制被开发出来用来处理这些攻击。

2.1加密系统

今天密码学是一个有用的安全的和广泛使用的工具。它使用代码和密文将信息转换为不可理解的数据。这些无法理解的数据可在网络上安全的传输。

2.2防火墙

防火墙是一个典型的边界控制机制或周边防御机制。防火墙的目的是将流量阻止在外面，但它也可以用来阻止内部通讯。防火墙是抵御入侵者的前线防御机制。它的设计是一个系统,以防止未经授权的访问或一个私人网络。防火墙可以在硬件和软件中实现,或两者的结合[8]。

2.3入侵检测系统

入侵检测系统（IDS）是一个额外的保护措施,帮助抵御电脑入侵。IDS系统可以用来检测一个软件和硬件设备的攻击。IDS产品用于监控连接来确定攻击是否成立，一些IDS系统监控和预警攻击,而其的则尝试阻止攻击。

2.4反恶意软件和扫描器

病毒、蠕虫和木马都是恶意软件,所以用来检测和治疗受感染系统的工具被称之为反恶意软件工具。

2.5安全套接字层(SSL)

安全套接字层(SSL)是一套协议一种标准的方式来实现一个好的网络之间的安全级别浏览器和一个网站。旨在web浏览器和web服务器之间创造一个安全的SSL 通道或隧道。所以任何信息交换可以在隧道中获得保护。SSL提供了身份验证的客户端服务器证书的使用。客户端提供一个证书服务器证明自己的身份。

## VI. IP协议IPV6的安全问题

IPv6是人人都在谈论未来的事情。从安全的角度来看,IPv6相比IPV4也是一个相当大的进步，尽管IPV6也有安全机制，它仍然很容易受到威胁。一部分的IPv6协议仍然构成了潜在的安全问题。新的互联网协议并不保护配置 服务器、糟糕的应用程序设计,或不受保护的网站。

可能出现由于以下原因导致的安全问题：

1. 头处理问题
2. 洪泛问题
3. 流动性问题

由于IPSec嵌入式的功能头处理的问题逐渐显现，正是因为头处理，扩展头可以阻止一些常见的攻击来源。问题是扩展头需要处理栈,这可以导致扩展头链特别长。大量的扩展头可以超过一个节点的大小,如果是故意这么做的话，这也是一种攻击。IP欺骗在IPV6上仍然是一个威胁，当整个网络的部分扫描发现潜在目标提供开放服务时一种被叫做端口扫描的攻击出现了，IPv6协议的地址空间是巨大的,但该协议仍然不能避免收到此种类型的攻击。流动性是一个纳入IPv6新功能。这个功能需要特别的安全措施。网络管理员需要意识到这些安全需要在使用IPv6的流动性特性。

## VII. 不同网络的安全性

今天的企业使用防火墙的组合, 加密和认证机制,创建“内部网” 连接到互联网的同时对它进行保护。内部网是一个使用互联网协议的私人计算机网络。内部网与外部网的区别在于前者一般都局限于员工的组织而后者通常可以被消费者，供应商或者其他获准的党派访问到。

从组织的内部网络不一定非得访问到因特网，当提供这样的访问时通常是通过一个网关和防火墙, 伴随着用户身份验证、加密的消息和频繁利用虚拟专用网络(vpn)。

虽然可以在可以控制环境的环境中建立内部网来快速共享数据，数据仍然是有风险的除非有严密的保安措施。一个封闭的内部网的缺点是至关重要的数据可能不进入那些需要的人的手中，内部网在机构内部还有一席之地。但对于更广泛的数据共享,在下列的保障下最好还是保持网络的开放性:

1.防火墙,入侵检测和报告

2.具有复杂的病毒检查功能的防火墙

3.规范化员工邮件中的附件

4.加密所有的连接和数据转换

5.通过同步定时密码或安全证书进行身份验证

如果内部网需要访问互联网，那么虚拟专用网络（VPN）会被用到。存在跨多个地点通常运行在独立的租赁行或VPN可以利用的新方法。VPN是一个私有网络使用公共网络(通常是因特网) 连接远程站点或用户。不是使用专用的现实地理世界的连接,如专线,VPN的用途 “虚拟”连接的路由通过互联网公司的私人网络远程站点或员工。

## VIII. 网络安全的发展现状

网络安全领域还是一样的路线。同样的方法被用作生物识别。生物识别技术提供了一个比密码的身份验证更好的方法。这可能会大大减少安全系统的未经授权的访问。软件方面的网络安全是非常动态的。新防火墙和加密方案正在实施。研究有助于了解当前的发展和预测未来的发展。

1。硬件的发展

硬件的发展并不是很迅速，生物识别系统和智能卡是唯一新的有广泛影响的硬件安全技术。生物识别最明显的用处是工作站登录到网络时。每个工作站都需要一些软件支持生物识别,这取决于生物正在使用的一些硬件设备。这些设备在每台计算机上都实现将会花费更多的代价。

1. 软件的发展

网络安全的软件方面是非常巨大的。它包括防火墙、防病毒、VPN、入侵检测等更多。所有安全软件的研究开发和可行的研究。我们的目标是获得一个基于安全软件在今天所处的位置的一个宏图。

## IX. 未来安全的发展趋势

驱动着网络安全向前发展的正是一些列的应用程序。未来可能会出现类似于免疫系统的安全网络。免疫系统能够抵抗攻击并且能够不断完善自己以对抗强悍的敌人。类似的，网络安全可以像免疫系统一样来运作。

生物识别的潮流已经发生了一段时间了，但是好像没有引起太大的反响。现在正在发展中的安全技术和现在正在用的安全技术几乎一样只是做了一些轻微的调整。

## X. 结论

随着互联网扩展，网络安全是一个越来越重要的领域，并且获得了越来越多的注意力。通过分析安全威胁和网络协议来决定在安全技术上是否需要做一些改变。安全技术大多数是基于软件的，但是许多常见的硬件设备也被应用进来。当前网络技术的发展并没有给人留下什么深刻的印象。

最初人们认为由于网络安全领域的重要性，新的网络安全的方法不管时硬件还是软件都需要进行积极的研究，当我们发现现在许多的发展都发生在已经正在使用的技术上这很让人感到意外。与IPV6结合使用的安全工具，例如防火墙，入侵检测，身份验证机制在未来都能够很好的保护我们的知识产权不受到侵犯。为了应对未来的网络安全的威胁，网络安全领域将不得不发展的更加迅猛。

## 参考文献

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it

seriously," Computer, vol.31, no.9, pp.24‐28, Sep 1998

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security,"

Communications, 2008. ICC '08. IEEE International Conference on,

pp.1469‐1473, 19‐23 May 2008

[3] “Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL‐4‐

Manual/security‐guide/ch‐sgs‐ov.html.

[4] Molva, R., Institut Eurecom,“Internet Security Architecture,” in Computer

Networks & ISDN Systems Journal, vol. 31, pp. 787‐804, April 1999

[5] Sotillo, S., East Carolina University, “IPv6 security issues,” August 2006,

www.infosecwriters.com/text\_resources/pdf/IPv6\_SSot illo.pdf.

[6] Andress J., “IPv6: the next internet protocol,” April 2005,

www.usenix.com/publications/login/2005‐04/pdfs/andress0504.pdf.

[7] Warfield M., “Security Implications of IPv6,” Internet Security Systems

White Paper, documents.iss.net/whitepapers/IPv6.pdf

[8] Adeyinka, O., "Internet Attack Methods and Internet Security Technology,"

Modeling & Simulation, 2008. AICMS 08. Second Asia International

Conference on, vol., no., pp.77‐82, 13‐15 May 2008

[9] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3,

no.6, pp. 68‐72, Nov.‐Dec. 2005