一些主流的网络安全技术

qzc

随着网络技术的迅速发展和普及，信息共享应用日益广泛而深入，但是与此同时，也带了很多网络安全问题，使经济、军事、个人隐私等领域受到黑客的严重威胁，不容忽视。

在本学期的网络安全课程中，我们学到了很多关于网络安全的知识。比如数据加密技术，身份认证技术，安全协议和防火墙技术等。

数据加密技术是网络安全的一个基础，所谓数据加密（Data Encryption）技术是指将一个信息（或称明文，plain text）经过加密钥匙（Encryption key）及加密函数转换，变成无意义的密文（cipher text），而接收方则将此密文经过解密函数、解密钥匙（Decryption key）还原成明文。密码技术是通信双方按约定的法则进行信息特殊变换的一种保密技术。根据特定的法 则，变明文（Plaintext）为密文（Ciphertext）。从明文变成密文的过程称为加密（Encryption）； 由密文恢复出原明文的过程，称为解密（Decryption）。密码在早期仅对文字或数码进行加、 解密，随着通信技术的发展，对语音、图像、数据等都可实施加、解密变换。密码学是由密码编码学和密码分析学组成的，其中密码编码学主要研究对信息进行编码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息。密码学研究密码理论、密码算 法、密码协议、密码技术和密码应用等。 随着密码学的不断成熟，大量密码产品应用于国计民生中，如USB Key、PIN EntryDevice、 RFID 卡、银行卡等。广义上讲，包含密码功能的应用产品也是密码产品，如各种物联网产 品，它们的结构与计算机类似，也包括运算、控制、存储、输入输出等部分。密码芯片是密码产品安全性的关键，它通常是由系统控制模块、密码服务模块、存储器控制模块、功 能辅助模块、通信模块等关键部件构成的。

数据加密技术要求只有在指定的用户或网络下，才能解除密码而获得原来的数据，这就需要给数据发送方和接受方以一些特殊的信息用于加解密，这就是所谓的密钥。其密钥的值是从大量的随机数中选取的。按加密算法分为专用密钥和公开密钥两种

专用密钥，又称为对称密钥或单密钥，加密和解密时使用同一个密钥，即同一个算法。如DES和MIT的Kerberos算法。单密钥是最简单方式，通信双方必须交换彼此密钥，当需给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。当一个文本要加密传送时，该文本用密钥加密构成密文，密文在信道上传送，收到密文后用同一个密钥将密文解出来，形成普通文体供阅读。在对称密钥中，密钥的管理极为重要，一旦密钥丢失，密文将无密可保。这种方式在与多方通信时因为需要保存很多密钥而变得很复杂，而且密钥本身的安全就是一个问题。

对称密钥是最古老的，一般说“密电码”采用的就是对称密钥。由于对称密钥运算量小、速度快、安全强度高，因而如今仍广泛被采用。

比如说，DES是一种数据分组的加密算法，它将数据分成长度为64位的数据块，其中8位用作奇偶校验，剩余的56位作为密码的长度。第一步将原文进行置换，得到64位的杂乱无章的数据组；第二步将其分成均等两段；第三步用加密函数进行变换，并在给定的密钥参数条件下，进行多次迭代而得到加密密文。

还有一种就是公开密钥，又称非对称密钥，加密和解密时使用不同的密钥，即不同的算法，虽然两者之间存在一定的关系，但不可能轻易地从一个推导出另一个。有一把公用的加密密钥，有多把解密密钥，如RSA算法。

非对称密钥由于两个密钥（加密密钥和解密密钥）各不相同，因而可以将一个密钥公开，而将另一个密钥保密，同样可以起到加密的作用。

在这种编码过程中，一个密码用来加密消息，而另一个密码用来解密消息。在两个密钥中有一种关系，通常是数学关系。公钥和私钥都是一组十分长的、数字上相关的素数（是另一个大数字的因数）。有一个密钥不足以翻译出消息，因为用一个密钥加密的消息只能用另一个密钥才能解密。每个用户可以得到唯一的一对密钥，一个是公开的，另一个是保密的。公共密钥保存在公共区域，可在用户中传递，甚至可印在报纸上面。而私钥必须存放在安全保密的地方。任何人都可以有你的公钥，但是只有你一个人能有你的私钥。它的工作过程是：“你要我听你的吗？除非你用我的公钥加密该消息，我就可以听你的，因为我知道没有别人在偷听。只有我的私钥（其他人没有）才能解密该消息，所以我知道没有人能读到这个消息。我不必担心大家都有我的公钥，因为它不能用来解密该消息。”

公开密钥的加密机制虽提供了良好的保密性，但难以鉴别发送者，即任何得到公开密钥的人都可以生成和发送报文。数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等问题。

数字签名一般采用非对称加密技术（如RSA），通过对整个明文进行某种变换，得到一个值，作为核实签名。接收者使用发送者的公开密钥对签名进行解密运算，如其结果为明文，则签名有效，证明对方的身份是真实的。当然，签名也可以采用多种方式，例如，将签名附在明文之后。数字签名普遍用于银行、电子贸易等。

数字签名不同于手写签字：数字签名随文本的变化而变化，手写签字反映某个人个性特征，是不变的；数字签名与文本信息是不可分割的，而手写签字是附加在文本之后的，与文本信息是分离的。

值得注意的是，能否切实有效地发挥加密机制的作用，关键的问题在于密钥的管理，包括密钥的生存、分发、安装、保管、使用以及作废全过程。

第二个很重要的技术就是身份认证技术。身份认证技术是在计算机网络中确认操作者身份的过程而产生的有效解决方法。 计算机网络世界中一切信息包括用户的身份信息都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。 如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者，也就是说保证操作者的物理身份与数字身份相对应，身份认证技术就是为了解决这个问题，作为防护网络资产的第一道关口，身份认证有着举足轻重的作用。

身份认证需要有认证的方法，在真实世界，对用户的身份认证基本方法可以分为这三种，基于信息秘密的身份认证，根据你所知道的信息来证明你的身份 (2)基于信任物体的身份认证，根据你所拥有的东西来证明你的身份 (3)基于生物特征的身份认证，直接根据独一无二的身体特征来证明你的身份。

身份认证也有几种形式，比如静态密码。举个例子就是我们很常用的密码机制。输入用户名，密码，就能登录到自己的账户。用户的密码是由用户自己设定的。在网络登录时输入正确的密码，计算机就认为操作者就是合法用户。实际上，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作为密码，或者把密码抄在纸上放在一个自认为安全的地方，这样很容易造成密码泄漏。如果密码是静态的数据，在验证过程中 需要在计算机内存中和传输过程可能会被木马程序或网络中截获。因此，静态密码机制无论是使用还是部署都非常简单，但从安全性上讲，用户名/密码方式一种是不安全的身份认证方式。

目前智能手机的功能越来越强大，里面包含了很多私人信息，我们在使用手机时，为了保护信息安全，通常会为手机设置密码，由于密码是存储在手机内部，我们称之为本地密码认证。与之相对的是远程密码认证，例如我们在登录电子邮箱时，电子邮箱的密码是存储在邮箱服务器中，我们在本地输入的密码需要发送给远端的邮箱服务器，只有和服务器中的密码一致，我们才被允许登录电子邮箱。为了防止攻击者采用离线字典攻击的方式破解密码，我们通常都会设置在登录尝试失败达到一定次数后锁定账号，在一段时间内阻止攻击者继续尝试登录。

还有 一个常用的认证形式就是智能卡。一种内置集成电路的芯片，芯片中存有与用户身份相关的数据， 智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。

智能卡认证是通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。

智能卡自身就是功能齐备的计算机，它有自己的内存和微处理器，该微处理器具备读取和写入能力，允许对智能卡上的数据进行访问和更改。智能卡被包含在一个信用卡大小或者更小的物体里（比如手机中的SIM就是一种智能卡）。智能卡技术能够提供安全的验证机制来保护持卡人的信息，并且智能卡的复制很难。从安全的角度来看，智能卡提供了在卡片里存储身份认证信息的能力，该信息能够被智能卡读卡器所读取。智能卡读卡器能够连到PC上来验证VPN连接或验证访问另一个网络系统的用户

现在我们经常要记忆很多密码，但是我们很容易忘记不常用的密码。但是服务提供方会有一种机制来保证用户可以找回密码。这就是短信验证码验证方式。通常以手机短信形式请求包含6位随机数的动态密码，身份认证系统以短信形式发送随机的6位密码到客户的手机上。客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全性。就我亲身感受而言（经常忘记密码），这种验证方式有很多好处。比如说安全性，由于手机与客户绑定比较紧密，短信密码生成与使用场景是物理隔绝的，因此密码在通路上被截取几率降至最低。还有就是普及性，只要会接收短信即可使用，大大降低短信密码技术的使用门槛，学习成本几乎为0，所以在市场接受度上面不会存在阻力。

总结完传统的这些验证方式之后，我们又了解了一种新式的验证方式，， 通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。使用传感器或者扫描仪来读取生物的特征信息，将读取的信息和用户在数据库中的特征信息比对，如果一致则通过认证。

生物特征分为身体特征和行为特征两类。身体特征包括：声纹(d-ear)、指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和DNA等；行为特征包括：签名、语音、行走步态等。目前部分学者将视网膜识别、虹膜识别和指纹识别等归为高级生物识别技术；将掌型识别、脸型识别、语音识别和签名识别等归为次级生物识别技术；将血管纹理识别、人体气味识别、 DNA识别等归为“深奥的”生物识别技术。

目前我们接触最多的是指纹识别技术，应用的领域有门禁系统、微型支付等。我们日常使用的部分手机和笔记本电脑已具有指纹识别功能，在使用这些设备前，无需输入密码，只要将手指在扫描器上轻轻一按就能进入设备的操作界面，非常方便，而且别人很难复制。

不过，这种验证方式也有一定缺陷，隐患在于一旦生物特征信息在数据库存储或网络传输中被盗取，攻击者就可以执行某种身份欺骗攻击，并且攻击对象会涉及到所有使用生物特征信息的设备。

互联网是一个面向大众，开放的网络，其实对信息的保密和系统安全的考虑并不完备，安全性之所以如此脆弱，除了使用“自由”，缺乏有效的集中式统一管理之外，根本原因是Internet上信息传输的广域性和网络协议的开放性，所以，为了增强网络的安全性，就出现了很多安全协议，这就是网络安全中另外一个很重要的模块，安全协议。

网络安全协议是营造网络安全环境的基础，是构建安全网络的关键技术。设计并保证网络安全协议的安全性和正确性能够从基础上保证网络安全，避免因网络安全等级不够而导致网络数据信息丢失或文件损坏等信息泄露问题。在计算机网络应用中，人们对计算机通信的安全协议进行了大量的研究，以提高网络信息传输的安全性。

其他的一些主流技术比如防火墙技术也在不断的发展和完善。总结了这么多纷繁复杂网络安全技术之后，个人的主机也曾被入侵过，幸亏当时没有保存很多东西。在网络攻击泛滥的今天，防御者总有一种道高一尺，魔高一丈的感觉。因为一个开放的网络，漏洞总是有的。所以我们要不断学习网络知识，不断完善网络安全。