第 3 章

远程用户认证

CHAPTER 3


视频讲解

3.1 概述

用户认证是计算机系统用于核实用户身份的一种安全技术。它是计算机防御体系的重要组成部分,也是防御系统入侵的主要防线。用户认证涉及识别(identification)和认证(authentication)两项功能。识别是指用户向系统呈现一个凭证(如用户名)以申明其身份,认证是指系统通过用户提供的认证信息(如用户口令)以核验用户的身份。

根据用户连接系统的方式,用户认证可分为本地用户认证和远程用户认证。在本地用户认证中,用户与系统的物理距离很近,如使用个人计算机、通过门禁系统等。在远程用户认证中,用户一般通过网络向系统提供凭证和认证信息,如用户通过互联网登录某个网站。本书主要介绍远程用户认证技术。此外,用户认证不同于消息认证。消息认证是通信各方验证消息源真实性和消息内容未被篡改的技术。本章仅关注用户认证,关于消息认证的介绍可参见 2.3 节。

本章首先对远程用户认证技术进行概述,然后分别介绍基于口令、公钥体制和生物特征的远程用户认证技术。

3.1.1 用途与挑战

远程用户认证技术在网络安全中具有广泛的应用,以下列举几项常见用途。

1) 身份记录

许多应用需要记录远程用户的身份,并且要求对用户身份进行核实。例如,一个在线会议系统要记录有哪些用户参加了会议,它可以利用人脸识别技术对用户身份进行认证。另一个常见的应用是网络日志,在将用户记录写入日志之前,它必须首先保证用户身份的真实性。

2) 访问控制

访问控制的目标是防止非法用户进入系统或者防止合法用户对资源的非法使用。简单来说,身份认证解决“一个用户是否拥有其声称的身份”的问题,而访问控制技术解决“一个身份有什么权利”的问题,因此访问控制的实现通常要基于身份认证技术。例如,当用户使用一个 Web 应用提供的服务时,系统先通过用户名和口令进行用户认证,然后根据该身份拥有的系统权限判断其可以访问哪些子系统、能够进行哪些操作。

3) 网络协议

许多网络协议的安全性建立在身份认证的基础上。例如位于网络层的 IPSec 协议、位于传输层的 SSL 协议首先会利用数字证书进行用户身份认证,认证通过后再提供后续服务。

当前,远程用户认证在技术和应用方面仍面临着诸多挑战。

1) 认证系统面临不断发展的安全威胁

远程用户认证系统从技术原理、系统设计与实现到系统使用都面临着不断发展的攻击技术的威胁。例如,在认证技术中使用的加密算法在原理上存在潜在的安全风险。一个典型的例子是广泛用于电子商务等领域的 MD5 和 SHA-1 哈希算法被发现存在安全缺陷,即

使采用的认证技术未发现缺陷，系统在设计和实现时引入的安全漏洞也可能被攻击者利用。最后，若用户不能正确配置和使用系统，则会提高认证系统的风险。例如，用户在应用 SSL 协议时，若选择简单模式，可能受到中间人的攻击。

2）认证方式难以兼顾安全性和便利性

对于系统而言，安全性与便利性通常是矛盾的。由于远程身份认证的频繁使用，这一矛盾更加突出。例如，出于提高安全性的考虑，远程系统一般要求用户使用复杂的口令，这增加了用户记忆和使用口令的难度，促使用户趋向于将同一个口令用于不同的应用服务中，由此增加了安全风险。又例如，某些银行要求用户使用便携式的动态口令设备实现用户认证，这提高了系统的安全性，但却给用户带来不便。

3）身份认证的“孤岛”问题

目前市场上存在多种用户认证方式，如数字证书、人脸识别、虹膜识别、指纹识别、短信验证码等。在一个综合应用中，不同的子系统可能采用不同的认证方式，以满足多样化的场景和应用需求。但是这些认证方式相互独立，采用不同认证方式的子系统各自为政，类似于一个个“孤岛”。当子系统不断扩充时，认证方式不断增加，系统难以管理，且用户体验较差。

3.1.2　远程用户认证方式

远程用户认证主要基于三种因素，即用户知道的信息、用户拥有的物品和用户的生物特征，下面分别介绍。

1）基于用户知道的信息

用户知道的信息指用户可以用大脑记忆的信息，例如口令、个人识别码（Personal Identification Number，PIN）、预先设定的问题的答案等。随着个人移动设备的普及，图像口令和手势口令也被用作用户认证。其中，图像口令向用户呈现一张数字图像，要求用户以正确的顺序点击图片中的几个位置；手势口令通常用于触屏设备，要求用户按正确的轨迹在屏幕上移动手指。

用户知道的信息以记忆的形式存放在用户大脑里，使用时不需要额外的设备支持，因此一直是最常使用的用户认证方式之一。然而，个人识别码、预先设定的问题、图片口令、手势口令等方式容易猜测，安全性较低，不适合用于远程用户认证。如果使用口令作为远程用户认证，一般要求口令有足够高的复杂度，并且应定期更新。针对口令的攻击和防御方法将在 3.2.1 节介绍。

2）基于用户拥有的物品

用于身份认证的物品一般指智能卡和 USB（Universal Serial Bus，通用串行总线）电子钥匙等小型物件。能用于身份认证目的的便携式智能设备，如平板电脑、智能手环、智能手表、智能手机，也可归为此类。数字证书本质上是一串二进制数据而非实体物品，但是数字证书难以记忆，一般存储在用户拥有的移动设备或计算机上，因此本书将基于数字证书的认证也归于此类。有的应用将用于认证的这些物品称为令牌，将基于令牌的认证方式简称为令牌认证。

令牌认证在涉及个人财产的场景中被广泛应用。如银行卡、公交卡、校园卡等具有支付功能的工具一般采用 IC（Integrated Circuit，集成电路卡）卡，其内置的集成电路能保存用户身份相关的数据。USB 电子钥匙是一种含有 USB 接口且具有存储功能的硬件设备，一般

存储了用户的密钥或数字证书,利用密码算法实现对用户身份的认证。动态口令令牌是银行系统常用的一种认证设备,它使用密码算法动态产生随机口令。

令牌认证方式不需要用户记忆复杂的口令,但也有不足之处。首先,令牌需要随身携带,这给用户带来不便。其次,令牌可能遗失或被他人窃取。当 USB 电子钥匙连接计算机后,攻击者可以通过木马程序盗取已读入计算机内存中的密钥。动态口令令牌不需要连接计算机,但攻击者可以通过伪造的钓鱼网站骗取动态口令,然后在口令改变之前登录真实的网站。此外,基于数字证书的令牌认证如果使用不当(参见 3.3.1 节),也存在认证漏洞。

3) 基于用户的生物特征

生物特征指相对稳定且难以伪造的用户私人特征,包括静态生物特征和动态生物特征两类。其中,典型的静态生物特征有指纹、虹膜、人脸等,动态生物特征有步态特征、语音模式、笔迹模式等。生物特征也常被用于多因素认证系统。例如在门禁系统、线上支付系统等安全认证应用中,在要求用户输入口令的同时进行人脸识别或指纹识别。

生物特征认证具有不会遗忘、难以窃取的优点,但该方式也存在一些缺点。首先,它的可靠性不如其他方式,通常伴有一定概率的误报和漏报。当用户因受伤、生病等原因不能提供正常的生物特征时无法进行认证;其次,生物特征认证一般需要特殊设备支持,使用不太方便;再次,生物特征被攻击者窃取后用户无法修改其认证信息,因此该方法风险性较高;最后,生物特征属于个人隐私信息,用户可能拒绝使用该方式。


视频讲解

3.2　基于口令的远程用户认证

口令认证具有使用方便且实施成本低的优点。它是目前最常见的认证方式之一,在远程用户认证中被广泛使用。用户使用远程服务之前,一般需要向系统提供身份标识和对应的口令。若身份标识与口令匹配,则身份认证成功,否则认证失败,系统拒绝向用户提供服务。由于口令使用的广泛性,针对口令的攻击方法层出不穷。

口令可以有多种表现形式,如字符口令、图像口令、手势口令等,本节针对最常用的字符口令,首先介绍常见的口令攻击方式,然后讨论加强口令安全性的几种主要方法。

3.2.1　常见的口令攻击方式

口令一般是静态的,因此一旦攻击者窃取或者截获口令,便能冒充用户。凡是用户拥有权限的操作,攻击者都可以实施。因此获取口令对于攻击者有很大的诱惑力,针对口令的攻击方法也很多。下面介绍几类常见的口令攻击方式。

1) 利用用户疏漏窃取口令

有的用户安全意识不够强,在使用口令时由于操作不当,导致口令被窃取。利用用户疏漏窃取口令的攻击方法主要分为两类。

(1) 偷看:用户有时会将复杂的口令记录在便利贴或本子上,这种方式容易被其他人看到。另一种常见的方式是“肩窥”(shoulder surfing),即当用户在输入口令时被周围的人偷看。例如,用户在取款机上输入口令时,周围的人有可能看到口令。此外,在安装了摄像头的场所输入口令,也存在被偷看的可能性。

(2) 社会工程学(social engineering)：攻击者冒充合法用户或用户信任的人获取用户口令。例如，攻击者在电话中冒充政府或用户所在单位的工作人员，询问其口令。另一种常见方式是钓鱼网站攻击。攻击者构造一个假冒网站，如某个银行的网站，骗取用户输入用户名和口令，这些信息实际发送给了攻击者。

防御以上两种攻击方法的关键是增强用户的安全防范意识，提高口令使用的警觉性。

2) 暴力破解攻击和字典攻击

猜测口令最直接的方法是尝试所有可能的口令，这种方法称为暴力破解。例如，如果知道用户的口令为 6 位数字，则需要尝试的可能性为 100 万种。若攻击者编写程序逐一尝试所有口令，则可能在较短的时间内发现正确的口令。

如果口令的结构比较复杂，可能的口令数量很多，攻击者会尝试最有可能的那些口令，这种攻击称为字典攻击。攻击者利用一般用户最常使用的口令，结合当前用户的个人数据，如姓名、生日等信息构造一个最有可能的口令列表，该列表被称为口令字典。攻击者从字典中逐一取出口令进行尝试。

防御暴力破解和字典攻击的有效方法是提高口令的复杂性，具体方法将在 3.2.2 节介绍。

3) 特定账户攻击和常用口令攻击

在特定账户攻击中，攻击者针对某个固定账户，通过尝试不同口令，直到找到正确的口令为止。特定账户攻击的一种变体是常用口令攻击，即使用某个常用口令对不同账户进行攻击，直到找到使用该口令的账户。

防御这两种攻击的方法包括禁止选择常用口令、限制口令尝试的频率、尝试失败次数过多则锁定账户等。

4) 电子监视

攻击者利用电子窃听手段获取用户口令。例如攻击者窃听无线通信、监听局域网数据包，或者在用户的计算机植入恶意程序监听用户的键盘输入。

防御电子监视的主要方法包括恶意程序扫描和通信加密两种方法。为了预防键盘监听，有的应用会显示一个随机产生的非标准键盘，并让用户通过触屏输入。

尽管口令认证面临多种攻击的威胁，但仍然是目前最常见的远程用户认证技术之一。这是因为口令认证具有简单、方便和低成本的优点，而其他认证技术也有其自身的缺点。如果使用口令认证，则应提高口令安全性，例如要求用户选择合适的口令。

3.2.2　口令选择策略

理论上，足够复杂的口令可以确保口令在一定时间内难以被破解。但过于复杂的口令很难记忆，降低了口令的实用性。为了在便于记忆和保留一定复杂度之间取得平衡，可以制定和实施合理的口令选择策略。常用的口令选择策略包括用户教育、计算机生成口令、后验口令检查和先验口令检查等。

1) 用户教育

用户教育策略是指对用户进行培训，告知复杂口令对于安全的意义，并给出正确设置口令的建议。例如，用户可选择有特殊意义的短语或句子，将首字母连成口令，同时在口令中加入一些特殊的数字和符号。然而，用户教育策略有其局限性，用户可能会忽视非强制性的

建议,或在理解和实施这些建议时出现错误。

2) 计算机生成口令

计算机生成口令策略是指由计算机生成复杂性较高、足够安全的口令。当用户使用口令时直接从计算机中提取。该策略已在部分网络浏览器中应用。例如,当用户在某个网站上注册并填写口令时,浏览器自动生成一个高强度口令,然后保存到计算机中。当用户登录该网站时,浏览器从计算机中提取口令并自动填写到口令栏中。由计算机生成口令的方式需要确保存储在计算机上的口令不被攻击者窃取。此外,当用户在其他计算机上使用该口令时,应有一套解决方案支持用户获取其口令。

3) 后验口令检查

后验口令检查策略类似于一种安全测试。该策略在口令设置后周期性地尝试破解用户口令,然后告知用户口令的脆弱性。该策略有两个主要缺点:一是系统用于破解口令的资源有限,而攻击者往往能调用更多的资源对口令进行破解,因而未被系统破解的口令不一定能抵抗真实攻击;二是后验检查结果可能滞后,脆弱的口令在被系统发现前可能已被攻击者破解。

4) 先验口令检查

先验口令检查是目前使用最广泛的口令选择策略。该策略在用户设置口令时对其安全性进行检查,若不满足安全要求,则拒绝该口令。规则实施和口令检查器是目前常用的两种先验口令检测方法。

(1) 规则实施。

该方式类似于一种强制性的用户教育,当用户设置的口令不满足安全规则时则拒绝口令。例如,要求用户在设置口令时,口令长度必须在八位以上,且口令应同时包含数字、大小写字母和标点符号等。若不满足此规则,则不能成功设置口令。相比用户教育,规则实施具有强制性,实际效果通常更好。然而,满足规则的口令也可能是脆弱的。

(2) 口令检查器。

这种方式类似于使用一个脆弱口令字典,若用户的口令在该字典中则拒绝其口令。这种策略的主要缺点在于需要占用计算机较多的时间和空间资源。随着越来越多的脆弱口令加入字典,字典将占用很大的存储空间,同时在字典中搜索口令的时间也会变长。

在实践中,可以将规则实施结合起来,要求口令既满足安全规则,同时也不在脆弱口令字典中。先验口令检测策略的不足是用户口令被拒绝的概率较高,可能导致用户体验下降,甚至不再使用系统。

3.2.3 安全散列函数与“盐值”

系统在保存口令时一般不会直接存储口令的内容,而是对口令进行某种处理,然后保存处理后的结果。采用这种方式有两个原因,一是用户可能不希望系统知道自己的口令;二是攻击者有可能入侵系统获得保存在系统中的数据。系统应确保即使攻击者获得了口令处理后的结果,也难以恢复出口令。

一种简单的处理方式是采用散列函数。2.3 节对散列函数进行了介绍,它可将任意长度的消息压缩为固定长度的消息摘要。假设用户的口令为 p,散列函数为 H,则系统计算 p 的散列值 h,即 $h=H(p)$,然后将 h 存储到系统中。系统验证用户输入的口令 q 时,首先计

算 q 的散列值 $r=H(q)$，然后比较 h 与 r。若两者相等，说明用户输入的口令正确。

在口令存储中使用的散列函数必须是安全散列函数，它具有不可逆性和防碰撞特性。不可逆性确保用户即使获得了口令的散列值 h，也难以恢复出实际的口令 p。防碰撞特性确保当攻击者输入错误口令时，其散列值与正确口令的散列值不同。

仅使用安全散列函数会带来一种安全缺陷，即相同口令的散列值相同。攻击者可以利用这一缺陷发动攻击。一是弱口令出现的频率较高，同一个弱口令的散列值也相同，因此出现次数较多的散列值很可能是弱口令；二是同一个用户在不同的系统中可能使用相同的口令，攻击者可以利用这一关联性降低口令破解的难度。

为了弥补这一缺陷，在处理口令时通常还会引入盐值(salt)。盐值是以随机或伪随机方式生成的一段字符串，通过参与口令散列值的计算来增强口令的安全性。假设某个用户的盐值为 s，口令的散列值计算方式可表示为 $h=H(p,s)$。然后系统同时保存 h 和 s，便于后续验证用户输入的口令是否正确。通过引入盐值，相同口令的散列值一般是不同的，从而增强了口令存储的安全性。

尽管安全散列函数和盐值提高了口令的安全性，但仍然面临暴力破解或字典攻击的威胁。若攻击者获得了散列值 h 和盐值 s，则可通过多次尝试猜测到口令。对系统而言，应防止攻击者窃取散列值和盐值，并禁止对口令认证的高频猜测；对用户而言，应对该威胁最有效的方法是设置足够复杂的口令。

3.2.4　验证码

当攻击者通过网络猜测用户口令时，可能会采用暴力破解攻击或字典攻击，企图在较短时间内尝试所有可能的口令。防御此类攻击的一种思路是降低口令猜测的频率。验证码是实现该目的的一种常用方法。

验证码的英文名称为 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart，全自动区分计算机和人类的公共图灵测试)，最早由卡内基梅隆大学的路易斯·冯·安等提出。对于互联网上的一些特殊功能，如注册、支付、投票等，一些恶意用户可能会利用计算机开展大批量的自动化操作，这偏离了此类功能的初衷。验证码的引入就是要区分机器和自然人，从而防止短时间内的大量访问请求。验证码常见的使用情景如下。

(1) 注册：通过验证码防止虚假账户注册。

(2) 短信接口保护：减少非法用户对短信接口的高频调用。

(3) 投票：减少用户虚假投票，提高投票的公平性。

(4) 口令找回：用于口令相关的安全操作，对操作者进行身份核实。

(5) 支付验证：当金额交易较大时保障资金安全。

由于验证码可以防止计算机发起高频请求，因此也可以用于缓解口令暴力破解攻击。常用的验证码类型包括识别型验证码、行为式验证码、短信验证码和语音验证码。

1) 识别型验证码

识别型验证码以图片的形式展示给用户，用户观察图片内容后输入识别结果，若输入正确则通过验证。最早的识别验证码主要显示数字、字母等简单的字符。有的网站采用了中文字符以提高识别难度。但 OCR(Optical Character Recognition，光学字符识别)技术的成

熟使字符型验证码不再安全。有的网站要求用户识别出图像中的物体,如楼梯、交通灯。这类识别码相比字符型验证码更难破解。近年来,随着图像识别技术的快速发展,识别型验证码用于区分人和机器的有效性严重降低。

2) 行为式验证码

由于识别型验证码的不足,越来越多的 Web 网站开始采用行为式验证码。此类验证码利用人的行为特征区分人和机器。常见的行为式验证码主要有拖动式验证码和点触式验证码。

(1) 拖动式验证码:要求用户根据提示,把图像中缺失的滑块拖曳到正确位置。

(2) 点触式验证码:要求用户根据文字提示,单击图像中符合要求的一种或者多种物品。

3) 短信验证码

系统通过短信接口将字母或数字类型的验证码发送到用户手机,用户在系统中填写验证码以完成验证操作。

4) 语音验证码

系统向用户播放一段音频,用户根据音频的指示输出正确的答案。与短信验证码相比,该方式需要的等待时间更短。

3.3 基于数字签名的远程用户认证

3.3.1 使用数字签名实现远程用户认证

2.2 节提到公钥密码体制有三类应用,即非对称加密、数字签名和对称密钥分发,其中,数字签名具有身份认证、消息完整性验证和防签名抵赖的功能。这里重点关注身份认证功能,特别是如何使用数字签名技术实现远程用户认证。利用数字签名技术实现用户认证的基本假设是只有用户本人拥有其私钥。由于没有用户的私钥无法伪造其数字签名,当一个数字签名被证实确实由用户的私钥产生时,用户的身份也得到确认。

如图 3.1 所示为使用数字签名技术实现远程用户认证的基本过程。假设 Bob 需要向 Alice 证明自己身份,需要首先生成一个消息 M,然后用自己的私钥 R 对 M 进行数字签名,生成签名结果 S。接下来 Bob 通过网络将 M 和 S 发送给 Alice。Alice 找到 Bob 的公钥 U,然后利用数字签名验证算法对(M,S)进行计算。如果计算表明 S 确实是 Bob 对 M 的签名结果,则用户认证通过,否则用户认证失败。

然而,以上方法用于用户认证时可能受到重放攻击(replay attack)。假设攻击者 Eve 窃听到 Bob 发送给 Alice 的数据(M, S),若他向 Alice 再次发送(M, S),则用户认证成功,从而让 Alice 误以为自己是 Bob。

该基本方案的缺陷在于 Alice 没有判断 M 是否为重发的消息。几种可防御重放攻击的改进方法如下。

方法 1:将 M 改为唯一识别号 I。当 Alice 收到(I, S)后,首先检测之前是否收到过 I,若收到过则说明该消息是重放攻击。该方法要求 Alice 存储收到的所有消息的识别号。

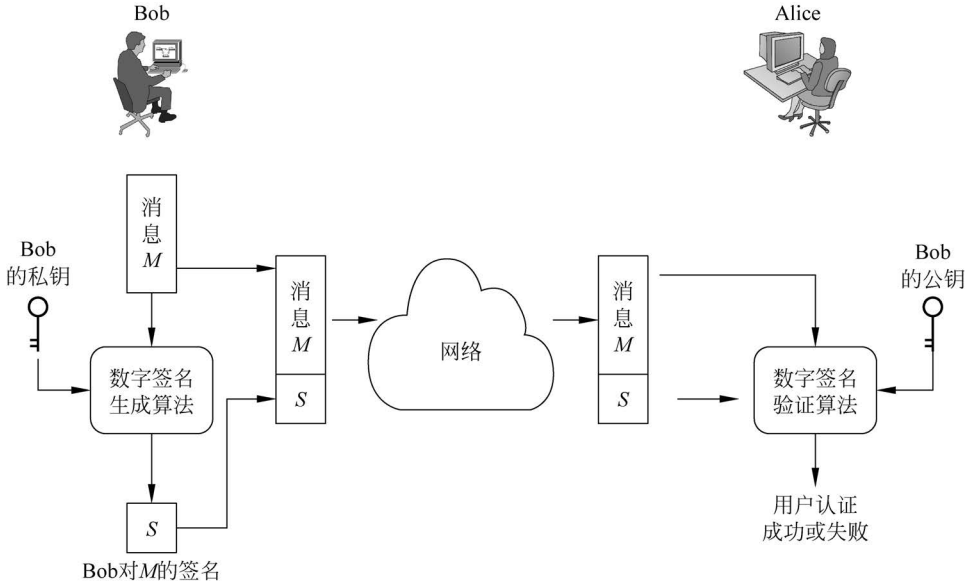

图 3.1　使用数字签名实现远程用户认证的简单流程

方法 2：将 M 改为时间戳 t。当 Alice 收到(t，S)后，首先检测 t，如果 t 距离当前时间超过一个阈值 T，说明该消息是重放攻击，从而拒绝认证。该方法要求 Bob 和 Alice 双方要时间同步，且 T 值的选取很重要。若 T 太大，则 Eve 的重放攻击可能会通过认证；若 T 太小，由于网络延迟，Bob 的正常请求可能被拒绝。

方法 3：同时使用唯一识别号 I 和时间戳 t。Alice 收到(I，t，S)后，首先检测 t，如果 t 距离当前时间超过一个阈值 T，则拒绝认证。若未超过，则检测在过去的 T 时间内是否收到过 I。该方法允许系统选择一个合理的阈值，且只需要保存较少的数量。

方法 4：Alice 随机生成一个随机数 r 发给 Bob，Bob 计算 r 的数字签名 S。Alice 收到(r，S)后，首先检查 r 是否为自己发给 Bob 的随机数。该方法要求双方进行半双工通信。

为了验证数字签名，Alice 事先需获得 Bob 的公钥。假设公钥存储在某台服务器上，若该服务器已被 Eve 入侵，当 Alice 向服务器请求 Bob 的公钥时，Eve 可以控制服务器向 Alice 发送自己的公钥。接下来 Eve 利用自己的私钥产生数字签名并发送给 Alice。由于 Alice 保存的公钥实际是 Eve 的，因此 Eve 的数字签名将验证成功，从而使 Alice 误以为发送消息的用户是 Bob。该攻击的出现是因为公钥与用户身份之间未建立绑定，可通过数字证书解决。

3.3.2　数字证书

1) 数字证书的结构与生成原理

数字证书的目的是建立公钥与用户身份间的绑定。数字证书一般包含用户身份、用户公钥及第三方的数字签名。第三方通常是用户信任的认证中心(Certificate Authority，CA)，如政府、金融和电信机构。用户通过安全渠道将其基本信息及公钥提交给认证中心，认证中心对这些信息进行数字签名运算以生成数字证书。需要用户公钥的人可以从各种公共渠道获得该用户的数字证书，并通过证书中包含的数字签名验证其有效性。如图 3.2 所

示为数字证书的基本结构和生成过程。

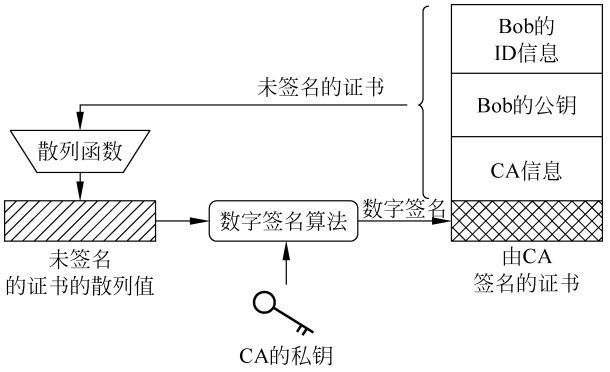

图 3.2　数字证书的基本结构与生成过程

用户申请并获得数字证书的流程如下。

(1) 用户利用程序创建一个密钥对,即一个公钥和一个私钥。

(2) 用户通过安全渠道将个人公钥等信息提交给 CA。提交可以是面对面的线下方式,也可以是带有安全机制支持的网页、邮件或软件等线上方式。

(3) CA 为未签名的证书生成数字签名。图 3.2 对该过程进行了描述。未签名的证书包含用户信息、CA 信息和用户公钥等数据。CA 首先利用某个散列函数计算未签名证书的散列值,然后使用自己的私钥和数字签名算法生成该散列值的数字签名。

(4) CA 将数字签名添加到未签名证书的末尾,组成一个完整的数字证书。

(5) CA 将数字证书交给用户。

用户获得证书后,可发给其他实体,以告知自己的公钥。其他实体也可以向 CA 查询,获得某个用户的数字证书。要验证某个用户的数字证书是否有效,首先从证书中提取未签名部分的数据,然后计算其散列值,最后使用 CA 的公钥和签名认证算法验证数字签名。如果该签名确是 CA 的签名,且该 CA 是可信的,则数字证书有效,即数字证书中的公钥属于证书用户。

2) X.509 数字证书格式

X.509 是目前使用最广泛的公钥证书格式。X.509 证书被用于各种互联网安全应用,包括位于网络层的 IPSec 协议、位于传输层的 SSL 协议、TLS 协议,位于应用层的安全电子交易 SET 协议、电子邮件协议 S/MIME。RFC 5280 对 X.509 进行了详细描述。

如图 3.3 所示为 X.509 证书第三版的格式,包括以下元素。

(1) 版本号:第三版证书的版本号取值为 3。

(2) 证书序列号:一个用于区分证书的整数值,对同一 CA 中该值是唯一的。

(3) 签名算法标识符:对未签名证书进行签名时采用的算法标识符和参数。该项与签名域中的信息相同。

(4) 发放者名称:颁发此证书的 CA 的名称。

(5) 有效期:包括开始日期和结束日期,在此期间外此证书无效。

(6) 用户名称:证书持有者的名称,与用户公钥绑定。

(7) 用户公钥信息:包括公钥,通常是一个二进制串,以及使用此公钥的加密算法的标

识符及参数。

(8) 发放者唯一标识符：一个可选项，发放者重名时，用于唯一确定证书发放者。

(9) 用户唯一标识符：一个可选项，用户重名时，用于唯一确定用户。

(10) 扩展：用于记录扩展信息。

(11) 签名：对证书的签名结果，是一个二进制串。此域包含签名算法标识符及算法参数。

证书颁发后可能被撤销。当用户的私钥泄露，用户名称改变或用户的管理单位发生改变时用户可向 CA 申请撤销证书。若 CA 的私钥泄露或签名算法不再安全时，则所有发布的证书均应撤销。因此在验证数字证书之前，首先应判断该证书是否在有效期内，以及是否已被撤销。X.509 标准定义一个证书撤销列表(Certificate Revocation List，CRL)实现此功能。该列表包含若干证书撤销记录，每个记录给出了证书序列号和撤销日期。

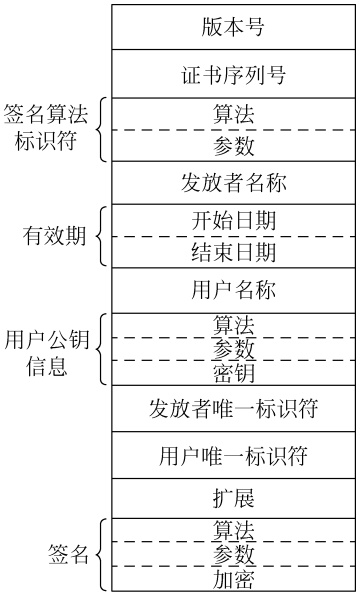

图 3.3　X.509 证书第三版格式

如果所有的证书均为同一个 CA 颁发，则该 CA 将面临巨大的访问压力，会成为通信的瓶颈。为解决这一问题，多个 CA 可以组成一种层次化结构。例如，假设用户 a 的证书由 CA_1 颁发，用户 b 的证书由 CA_2 颁发，CA_1 和 CA_2 的证书均由 CA_0 颁发，且所有用户都知道 CA_0 公钥，则三个 CA 组成一个层次结构，根节点为 CA_0。当用户 b 收到 a 的证书时，发现其证书由 CA_1 颁发，但用户 b 没有 CA_1 的公钥。它可以利用 CA_0 的公钥验证 CA_1 的数字证书，从而得到可信的 CA_1 的公钥。对于更高的层次结构，用户可逐层回溯，直到某层 CA 的数字证书为可信 CA 颁发。这一方案要求任意两个用户共享同一个根节点，现实中往往没有这样的根节点，此时可通过 CA 间的交叉认证解决。如果两个用户没有共享同一个根节点，但这两个根节点相互进行了认证，并给对方颁发了证书，则这两个用户仍可相互验证数字证书。

如上所述数字证书的使用涉及注册、撤销、交叉认证等多种功能，过程比较复杂，因此需要专门的规范进行管理。

3) 公钥基础设施

公钥基础设施(Public Key Infrastructure，PKI)是基于公钥密码体制的一套软硬件设施和规范，其目标是帮助用户安全高效地获取公钥，实现数字证书的生成、管理和撤销等功能。下面介绍 PKIX 模型，它由互联网工程任务组(IETF)基于 X.509 证书提出。

PKIX 模型包含三个关键部分。

(1) 端实体：证书的持有者，可以是用户、机构、服务器和路由器等实体，对应数字证书中的用户字段。

(2) CA：证书的发放者。CA 支持多种管理活动，如证书注册和撤销。

(3) 存储库：用于存储和检索数字证书和 CRL。

PKIX 还包含两个可选部分。一个是注册中心(Registration Authority，RA)，它可为

CA 承担注册功能；另一个是 CRL 发放者，它可为 CA 承担 CRL 发布的功能。

在 PKIX 中，CA 可提供以下管理功能。

(1) 注册：在 CA 向端实体颁发数字证书之前，端实体向 CA 登记其身份。根据 CA 的要求，注册可采用线上或线下的方式进行。RA 可代理 CA 提供注册功能。

(2) 初始化：CA 向端实体提供必要的信息，帮助其为接收数字证书做好准备。

(3) 认证：CA 为端实体颁发数字证书。

(4) 密钥对恢复：当端实体的密钥对(主要指私钥)无法访问时，CA 为其恢复密钥对。

(5) 密钥对更新：当证书过期或证书被撤销时，需要更新密钥对。CA 负责生成新的密钥对，并为其颁发新证书。

(6) 撤销证书：当端实体提出撤销证书的申请时，CA 对证书进行撤销。

(7) 交叉认证：两个 CA 相互认证并互换交叉证书的过程。交叉证书是一个 CA 给另一个 CA 颁发的数字证书。

(8) 证书和 CRL 发布：CA 将数字证书或 CRL 存入存储库。这两项功能也可分别由 RA 和 CRL 发放者提供。

3.4 基于生物特征的远程用户认证

生物特征认证系统利用个人独有的生理特征实现用户认证。生物特征认证可分为静态生物特征认证和动态生物特征认证。生物特征是人体固有的特征，不需要记忆，也不用担心遗失，且很难伪造。因此，生物特征认证具有较强的安全性与便利性。但是生物特征认证一般需要额外的检测设备，且存在一定的误检率和漏检率。此外，用户的身体状态和所处环境的变化也可能影响认证结果。

本节将简要介绍常用的生物特征，以及利用生物特征进行远程用户认证的典型过程，然后介绍在生活中经常使用的指纹识别技术和人脸识别技术。

3.4.1 生物特征及远程认证过程

1. 生物特征

生物特征可分为静态和动态两类。静态生物特征是指在一段时间内保持稳定的生理特征，如人的指纹特征、人脸特征、虹膜特征等；动态生物特征是随时间变化的特征，如人的声音特征和步态特征等，通常可用一个信号序列表示。

1) 静态生物特征

(1) 指纹特征：指尖皮肤因凹凸不平而形成的纹路模式。

(2) 人脸特征：脸的几何特征，一般指脸形及面部关键器官，如眼睛、眉毛、鼻子、嘴唇、下颚的形状和位置。有的技术将人脸内部的血管分布也视为人脸特征的一部分，可利用红外热成像技术进行识别。

(3) 手形特征：手的几何特征，包括手的形状、手指和指关节的长度及宽度等。

(4) 人眼特征：包括虹膜和视网膜特征。虹膜是位于人眼中部的圆盘状血管膜，俗称“黑眼球”。虹膜包含斑点、条纹、褶皱等丰富的细节特征，其图像可用相机进行捕捉。视网

膜是位于眼球壁内层的一层薄膜，视网膜特征是指视网膜下的血管分布形成的数字图像特征，可通过低强度的可见光或红外线扫描获得。

2）动态生物特征

（1）声音特征：每个人的声音也具有一定的独特性，如发音的频率等。声音可通过麦克风等设备方便地进行采集。

（2）步态特征：每个人在体型、体重、肌肉力量、骨骼长度、协调能力、走路风格等方面都存在细微差异，要伪装走路的姿态非常困难。步态特征可从摄像头等设备采集的视频图像中提取。

（3）签名轨迹：每个人的签名具有其独特性。签名可分为离线和在线两类。离线签名图像不随时间变化，属于静态生物特征。在线签名则属于动态生物特征，在线签名通过写字板和输入笔对签名轨迹进行采样，形成一系列的采样点。

2. 基于生物特征的远程用户认证

利用生物特征进行远程用户认证包括注册和认证两个阶段。

注册是将用户身份与其生物特征进行绑定的过程。系统对用户的生物特征进行采集，利用特征提取算法从中提取特征，并与用户的身份（如用户 ID）关联起来。

认证是根据用户提供的身份信息和生物特征，判断生物特征是否属于对应用户，据此给出认证成功或失败的结论。下面给出利用生物特征进行远程用户认证的一个简单例子。

（1）用户将 ID 发给远程主机；

（2）远程主机发送随机数 r 和加密函数标识符 E 给用户，r 用于防止重放攻击；

（3）生物特征采集系统采集用户生物特征，利用特征提取算法从中提取出特征 B；

（4）生物特征采集系统生成 $E(r', D, B)$ 并发送给远程主机，其中 $r' = r$，D 为采集系统的 ID 号；

（5）远程对 $E(r', D, B)$ 进行解密。当以下条件均满足时，认证通过，否则认证失败。

① r' 与 r 相等；

② D 是合法设备的 ID 号；

③ B 与用户注册时保存的特征相似度超过规定的阈值。

基于生物特征进行用户认证的核心技术是生物特征识别技术。接下来介绍两种常见的识别技术。

3.4.2　指纹识别技术

指纹是指尖皮肤因凹凸不平而形成的纹路。指纹识别具有以下特点。

（1）独特性：每个指纹都是独一无二的，即使双胞胎的指纹、同一人的左右手指也不相同。

（2）稳定性：除非受到较严重的物理伤害，每个人的指纹形态终生不变。

（3）便利性：指纹采集方便，采集成本较低。

指纹的一个明显的结构特征是交错的脊线和谷线。经过光学处理后，指纹图像一般用黑色表示脊线，用白色表示谷线。脊线的细节可分为以下三个层次描述。

第一级：代表指纹的总体特征，主要包括指纹的纹型和全局特征点，一般肉眼可直接辨

识。纹型可分为弓形、箕形、斗型三大类。全局特征点主要指中心点和三角点等。

第二级：代表指纹的局部特征，最常见的二级特征是端点和分叉点。端点是一条脊线终止的细节点，分叉点则是一条脊线分裂成两条的细节点。

第三级：代表指纹的高分辨细节特征，如脊线上的汗孔、纹线边缘特征、疤痕等。第三级特征更为细致，但稳定性不如第二级特征。随着高精度指纹采集器的应用，第三级特征也开始受到重视。

指纹识别用于犯罪鉴定已有100多年的历史。早期的指纹使用油墨和纸记录，依靠肉眼进行识别。目前采用的指纹自动识别系统(Automated Fingerprint Identification System，AFIS)则采用数字图像记录，利用计算机算法进行自动识别。AFIS的典型工作过程可分为四个阶段。

(1) 图像采集：利用各种传感器将指纹信息转换成数字图像。常见的传感器有光学传感器、电容传感器、射频传感器、超声波传感器等。

(2) 图像增强：采集到的指纹图像一般是灰度图像，需要进一步处理，以减少噪声干扰，增强脊线和谷线的对比度，便于下一步提取指纹特征。图像增强一般包括平滑处理、二值化和细化等操作。

① 平滑处理：目的是消除采集设备、外部环境及手指异常等原因引入的噪声，一般可通过数字滤波算法实现。

② 二值化：目的是将灰度图像转换为二值图像，剔除噪声与毛刺，突出脊线分布。

③ 细化：目的是将脊线宽度减少到一个像素点，得到指纹的骨架图像。

(3) 特征提取：从指纹的骨架图像中提取全局特征点及端点和分叉点等普通特征点。

(4) 特征匹配：通过旋转平移等几何变换将待检测指纹与模板指纹的特征点对齐，计算两个指纹特征的相似度。若相似度超过一个阈值，则匹配成功，否则匹配失败。

随着指纹识别技术的成熟，对于高质量的指纹图像，现有的AFIS一般能达到极高的准确率。然而，目前也出现了许多针对指纹识别的攻击。例如攻击者利用硅胶等材料模拟指纹纹路，欺骗指纹识别系统。2019年，部分智能手机上的指纹识别模块错误地将硅胶材料的纹路识别为真实指纹图案，使攻击者得以解锁手机并完成手机支付。该事件迫使国内多家电子支付机构紧急关闭了该系列手机的指纹支付功能。因此，利用活体检测技术发现伪造指纹，是提高指纹认证安全性的必要手段。

3.4.3 人脸识别技术

人脸识别技术是一种利用计算机算法根据视频或者图片中的人脸特征确定人的身份的技术，是当前最常用的生物特征识别技术之一。自20世纪70年代以来，人脸识别技术不断发展，目前已基本成熟，在信息安全、公共安全、金融、媒体等领域广泛应用。

与其他生物特征识别技术相比，人脸识别技术具有以下优势。

(1) 自然性。人脸识别技术利用脸部特征确定人的身份，符合人类的习惯，容易被用户理解和接受。指纹、虹膜、视网膜等生物特征的识别不符合人类习惯，不具备自然性。

(2) 方便性。人脸信息采集设备可以是常见的摄像头、照相机、手机，成本较低且容易获得。采集过程简单方便，不需要专门的技术人员。

(3) 非强制性。人脸识别技术通过摄像头、相机等设备方便地采集到人脸图像信息。

用户不需要主动接触采集设备，甚至察觉不到采集设备的存在。而对于指纹等生物特征，用户需要接触采集设备，并主动配合采集过程才能完成。

由于人脸识别技术的以上优势，它在许多领域均获得了成功的应用。

（1）信息安全领域。主要用于用户认证，例如，在使用智能手机前进行的屏幕解锁验证，在移动支付应用中进行的用户身份验证，在电子政务应用中进行的用户身份确认等。

（2）安保领域。主要用于门禁管理，例如，在银行部门、军事重地等重要场所，通过人脸识别技术对用户的身份进行识别和验证，以确定是否让用户进入。

（3）公共安全领域。主要用于智能监控，例如，在人口流动密集区如机场、车站、景点等重要出入口布置摄像头，通过人脸识别技术发现公安部门发布的黑名单人员。

（4）媒体行业。主要用于视频检索，从海量的视频文件中找到需要的信息。传统的视频检索采用人工方式进行，往往需要大量的成本和时间。利用人脸识别技术可以自动地、快速地实现视频检索，从而降低人工成本，提高工作效率。该技术还可帮助公安人员快速检索监控视频。

在实践中，人脸识别技术需要解决多个难题，包括如下问题。

（1）光照问题。在采集人脸图像时，由于人脸的三维形态和环境光线的复杂性，人脸的图像表示会随之改变。严重情况下，人脸图像会产生曝光或阴影，导致人脸部分特征消失，使识别准确率急剧下降。

（2）姿态问题。许多应用在采集人脸图像时，不强制要求被识别者主动配合，因此人脸姿态可能差别很大。例如用户可能低头，或者只采集到一侧脸等。对于姿态变化过大的情况，人脸识别的准确率可能大幅降低。

（3）表情问题。当脸部表情变化时，面部肌肉和五官都会产生一定程度的扭曲，使得人脸识别的识别率降低。

（4）遮挡问题。在许多情况下，人脸可能被外界事物遮挡，例如围巾、墨镜、帽子等饰物，或者用于防止疾病传染的口罩，甚至是人的头发。严重的遮挡使采集到的人脸图像丢失重要的脸部信息，从而影响了特征提取。

（5）图像质量问题：由于采集设备或采集人员的问题，采集到的图像可能图像模糊、分辨率太低，导致人脸识别困难。

（6）小样本问题：大量样本对于提高识别准确率非常重要。实际情况中，很难为一个人采集到多个样本。例如公安系统中的人脸库可能只有身份证中的一张正面照。

自 20 世纪 70 年代开始，为解决以上难题，人脸识别技术不断发展，许多研究成果已在真实世界中应用。根据其基于的人脸特征，人脸识别技术可分为以下四类方法。

1）基于几何特征的方法

基于几何特征的方法出现在人脸识别技术发展的早期阶段。该方法利用人脸各器官（如眼睛、鼻子、嘴巴）的几何形状及相互之间的位置关系来表示人脸特征。例如，使用向量描述眼睛、鼻子、嘴巴之间角度、距离。将该向量与模板库中的向量进行对比，找到相似度最高的向量。几何特征方法具有算法简单、计算速度快、不易受光照影响等优点。然而该方法容易受表情影响，且该方法只利用了人脸的小部分特性，而无法利用更为丰富的人脸整体外观和细节信息，导致其识别度不高。基于几何特征的方法目前仍在某些人脸识别系统中使用，但其主要用途不再是识别人脸，而是在预处理阶段用于提取人脸中的关键点。

2) 基于全局特征的方法

基于全局特征的人脸识别方法于20世纪90年代初提出。它对整幅人脸图像进行处理,从中提取出代表整个人脸图像的特征向量,该特征向量可以反映人脸的全局结构信息。该方法通常利用降维技术(如主成分分析、独立成分分析、线性判别分析、流形学习等)将高维的人脸图像映射为一个低维向量,并保存为一个模板。进行人脸识别时,则将待测人脸图像的映射结果与模板库中的向量进行比较。在外界环境和拍摄要求严格受控的条件下,基于全局特征的人脸识别方法对于正面人脸的识别效果较好。然而在非受控环境下,特别是伴随着姿态、光照、表情等变化,该方法的准确率显著降低。

3) 基于局部特征的方法

基于局部特征的人脸识别方法在20世纪末和本世纪初得到快速发展。该方法选择人脸图像中的具有较强区分能力的多个区域,分别提取出特征,再合并为人脸特征。与全局特征提取方法相比较,局部特征对姿态、光照、表情等变化有比较好的鲁棒性。具体来说,该方法首先使用人脸关键点检测算法定位人脸中的关键位置,然后在每个关键位置上使用手工设计的特征提取算法分别提取出不同的特征。这些算法经特殊设计,因此对环境、表情和几何变换等干扰有较强的鲁棒性。最后,通过串联或向量编码等方法将各位置上提取的特征融合为人脸特征。该方法的缺点是计算较为复杂,且需要手工设计特征提取算子。

4) 基于深度学习的方法

深度学习是利用人工神经网络的分层结构来处理复杂的高维数据。人工神经网络由多层网络构成,每层网络由多个人工神经元组成,本层神经元的输出作为下一层神经元的输入。利用这种结构实现对输入信息的分层处理,使每层网络从上一层的输出中提取出更抽象、更具区分性的特征。一般而言,神经网络的层数越深,其表达能力和区分能力越强。深度学习技术的提出使该目标成为可能。

基于深度学习的人脸识别方法以整张人脸图像为输入,经过多层神经网络的计算,输出最终的人脸特征。从表面来看,基于深度学习的方法重新回到了基于全局特征的人脸识别,事实上,该方法在提取特征时是由局部到整体逐渐过渡的。网络的前几层以提取局部特征为主,之后这些局部特征逐渐融合为全局特征。因此,基于深度学习技术的方法同时利用了局部特征和全局特征。

2012年以来,深度学习进入飞速发展阶段,人脸识别领域也因此受益。2014年,在实验条件下,基于深度学习技术的人脸识别技术在准确率上已经超过人类。目前,市场上大多数的人脸识别系统采用了深度学习技术。

与指纹识别类似,使用人脸识别进行用户认证时,也需要两个阶段,即注册和认证。

注册是从用户的人脸图像中提取脸部特征保存起来,并与用户身份进行绑定。

利用人脸识别进行用户认证的过程一般可分为以下四个阶段。

(1) 人脸检测。人脸检测是检测输入的图像中是否存在人脸,如果存在人脸,则将人脸部分从输入图像中分割出来。

(2) 预处理。预处理的主要目的是改善图像质量,对图像进行规范化,便于后续提取出人脸特征。预处理包括图像增强、人脸扶正、归一化等工作。图像增强的目的是改善图像质量。例如,降低外界环境引入的噪声、光照和遮挡的影响。人脸扶正的目的是获得端正的人脸图像。例如,可先识别出人脸的特征点,再通过旋转变换实现人脸扶正。归一化是将人脸

图像转换为尺寸和灰度取值范围相同的标准化图像。

(3) 特征提取。特征提取是将预处理后的标准化人脸图像转换为具有区分性的人脸特征,便于后续识别出人的身份。人脸图像一般用像素值矩阵表示,矩阵包括大量元素,因此原始人脸图像是高维的。此外,姿态、光照、表情也会降低人脸图像信息的有效性,使同一人脸的不同样本间的差别很大。特征提取就是要将原始的高维图像转换成低维向量,并降低各种外界因素对特征表示的影响。

(4) 特征匹配。将提取的特征与模板特征进行对比,计算两者的相似度。若相似度超过一个阈值,则匹配成功,否则匹配失败。

5) 人脸识别技术面临的挑战

在严格受控的条件下,人脸识别目前已能达到极高的准确率。但在真实应用中,特别是在非受控条件下,人脸识别技术仍面临许多挑战,例如前面提到的遮挡、图像质量、样本数目对识别准确率的影响。此外,人脸识别还会受到年龄变化、化妆、疾病等问题的影响。当人脸识别技术用于公共安全和信息安全领域时,还需要解决主动逃避和图像伪造问题。

主动逃避是指被识别人故意不让系统识别其脸部特征。被识别人的主动逃避,加上现有识别系统的不足可能会导致严重的安全问题。例如 2013 年美国波士顿马拉松爆炸案造成上百人受伤。警方从现场视频中提取的嫌犯人像,在身份库中不能成功搜索匹配。人脸识别专家对其人脸识别系统进行了评估,认为光照、姿态、遮挡和图像质量等问题造成了搜索嫌犯的失败。根据 2019 年美国 NIST 机构发布的评估报告,在环境不可控、用户不配合的条件下,人脸识别技术错误识别率要比受控条件下高出一个数量级。

图像伪造是指攻击者通过假的脸部图像或视频欺骗识别系统,从而通过用户认证。为了提高人脸识别系统的安全性,需要使用人脸防伪技术,也称活体人脸检测技术。一种常用的人脸防伪技术,要求被检测人根据系统指示做出相应的动作,如张嘴、转头、眨眼等。使用三维人脸识别技术也可提高防伪检测效果。该技术利用二维或三维摄像头构建用户头部的三维模型,从而识别出图像或视频欺骗。

3.5　远程用户认证中的对抗

随着深度学习技术的成功,人脸识别已经成为用户认证的最常用的方式之一。本节重点介绍人脸识别的攻击技术和防御方法。尽管基于深度学习技术的人脸识别达到了极高的准确率,目前也存在多种攻击方法,如重放攻击(replay attack)、对抗样本攻击(adversarial attack)和人脸融合欺骗攻击(morphing attacks)。

人脸识别中的重放攻击思路类似于网络通信中的重放攻击,攻击者将窃取到的人脸信息发送给检测器,从而通过人脸识别验证。重放攻击又可分为欺骗攻击(spoofing attack)和面具攻击。欺骗攻击主要通过图片或视频伪造脸部信息。例如,攻击者将打印的人脸图像置于摄像头前,或者利用显示设备播放窃取的人像视频。欺骗攻击的检测方法主要包括基于动作的方法和基于特征分析的方法。基于动作的方法要求用户根据检测系统的提示做出相应的动作,如眨眼、张嘴、转头等。基于特征分析的方法则对视频或图像中的人脸特征进行分析,以判断摄像头获取的信息是否来自真实的人。此外,三维人脸识别技术也被用于检测欺骗攻击,它通过构建人脸的三维模型发现伪造的人脸。

在面具攻击中,攻击者使用硅胶、乳胶等软性材料来制造面具,当佩戴好面具后,攻击者有可能骗过人脸识别系统。面具攻击能在一定程度上应对人脸识别系统对欺骗攻击的检测。例如,攻击者佩戴面具后能够按系统提示做出相应动作,从而应对基于动作的检测。面具攻击的缺点是攻击成本高,一般需要昂贵的材料且制作工艺难度较高、制作时间较长。此外,佩戴面具的攻击者容易被人类检查员发现。

2014 年,研究者发现了深度学习技术的一个缺陷。如果向图像添加一些噪声,即使修改后的图像对于人眼而言并没有多大的变化,但神经网络却无法正确识别图像中的物体。这类修改后的图像样本被称作对抗样本,用对抗样本攻击神经网络被称作对抗攻击。如今,对抗攻击已经成为人脸识别系统面临的重要威胁。针对人脸识别的对抗攻击可分为数字攻击(digital attack)和物理攻击(physical attack)两类。数字攻击的攻击过程发生在数字域,攻击者通过访问和直接干扰数字输入图像使人脸识别系统失效。物理攻击的干扰对象则位于物理世界,攻击者通过可穿戴物品使人脸识别系统失效。例如,研究者表明,攻击者通过佩戴眼镜、帽子,或者在人脸上贴纸,都可以使人脸识别系统输出错误的识别结果。对抗攻击的防御方法主要包括对抗训练和预处理方法。对抗训练将对抗样本加入到训练数据中,使得神经网络可以学习到对抗样本的特征,从而降低识别错误。然而,使用对抗训练方法更新后的神经网络可能无法检测出新的对抗样本。预处理方法对输入的人脸图像进行预处理。这些预处理方法通常是一个数据转换模块,以消除人脸图像中的对抗扰动,从而降低对抗样本干扰神经网络的概率。

人脸融合欺骗攻击是一种针对人脸识别的新型攻击。攻击者将自己及协助者的真实人脸图像融合成一张人脸照片,该照片中的人脸与攻击者和协助者都存在较高的相似度。接下来,协助者向注册机构提交融合照片,并获得身份证件。最后,攻击者使用协助者证件假冒其身份。由于攻击者与注册的照片高度相似,因此有可能骗过人脸识别系统。鉴于融合人脸图像与真实图像之间存在纹理差异,可以利用这一点检测融合欺骗攻击。例如,有的检测系统使用人脸图像的二值化统计图像特征表示人脸图像的纹理模式,再利用机器学习技术判断图像是否由多个图像融合生成。

3.6 验证码破解对抗项目

1. 项目概述

本项目要求对抗双方模拟针对验证码的攻击及防御过程。对抗分为三轮:第一轮,双方搭建模拟环境,利用工具开展简单的验证码破解活动;第二轮,双方编写程序实现三种类型的验证码攻击与防御活动;第三轮,双方查阅参考资料、提出新想法,实现对一种难度较高的验证码系统的破解。

2. 能力目标

(1) 能够实现多种类型的验证码。
(2) 能够对多种类型的验证码进行破解。
(3) 能够检索和学习参考资料并据此设计新的验证码破解或防御方法。

（4）能够编写程序将设计的方法用于实践。

（5）能够撰写项目报告详细描述对抗过程和技术细节。

3. 项目背景

A 公司是一家提供金融资讯服务的公司，客户登录系统后可通过 A 公司的网站获取相关的金融资讯。最近 B 组织使用网络爬虫技术频繁地抓取 A 公司网站的资讯。为了应对这一情况，A 公司决定采用验证码区分网络爬虫和正常用户。

4. 评分标准

学生的项目成绩由三部分构成：

（1）对抗得分。由每一轮的对抗结果决定。

（2）能力得分。根据学生在对抗过程中展现的专业能力决定。

（3）报告得分。由项目报告的质量决定。

5. 小组分工

项目由两个小组进行对抗，各组人数应大体相当，每组可包含 1～4 人。分工应确保每个组员达到至少 3 项能力目标。

两个小组可分别扮演 A、B 双方，或者同时扮演 A、B 双方。

6. 基础知识

项目需要的基础知识包括：

（1）Web 网站的基本知识。

（2）常见的验证码类型，如图形验证码、滑动验证码、旋转验证码等。

（3）程序编写知识。

7. 工具准备

（1）操作系统，用于搭建目标网站，推荐使用 Linux。

（2）Web 服务器，用于提供 Web 服务，推荐使用 Apache。

（3）编程语言，用于开发网站、攻击程序和防御程序，常用的有 Python、Java、PHP 等。

8. 实验环境

本项目需要至少两台计算机，一台为 A 方所有，用于安装 Web 服务器，可放置在互联网上；另一台为 B 方所有，用于访问 A 方的 Web 服务器。

9. 第一轮对抗

第一轮的任务是搭建模拟环境，并开展简单的字符型验证码攻击和防御活动。

1）对抗准备

A 方搭建网站并上传至服务器提供访问，网站实现了简单的字符型验证码功能。B 方准备好验证码的破解程序或工具。

2) 对抗过程

(1) A 方展示验证码的正常使用过程。

(2) B 方访问 A 方网站,利用攻击程序或工具破解 A 方网站的字符型验证码。

(3) 多次重复第(2)步,统计 B 方成功破解验证码的次数。

3) 对抗得分

达到以下要求,对应方可获得积分:

(1) A 方环境配置正确。

(2) A 方成功破解 B 方验证码的次数。

(3) B 方成功防御 A 方验证码攻击的次数。

以上各项的具体分值可由双方在对抗前商议确定。

10. 第二轮对抗

在第二轮对抗中,双方针对更多类型的验证码开展验证码攻击和防御活动。

1) 对抗准备

A 方编写程序实现三种类型的图形验证码。

(1) 滑动验证码:用户将拼图块拖动至图形中正确的地方。

(2) 旋转验证码:用户旋转图像至正确的角度。

(3) 点选验证码:用户根据提示从多个图像中选择正确的一个。

B 方编写程序对以上三种图形验证码进行破解。

2) 对抗过程

(1) A 方展示三种验证码的正常使用过程。

(2) B 方使用攻击程序破解 A 方网站的验证码。

(3) 统计 B 方破解每种验证码的成功率。

3) 对抗得分

对抗得分由以下部分构成:

(1) B 方破解滑动验证码的成功率。

(2) B 方破解旋转验证码的成功率。

(3) B 方破解点选验证码的成功率。

以上各部分的具体分值可由双方在对抗前商议确定。第二轮的总分值应高于第一轮。

11. 第三轮对抗

在第三轮对抗中,A、B 双方均担任攻击者角色。双方协商选择一种当前被广泛采用的、有挑战性的验证码类型进行破解。

1) 对抗准备

双方查阅相关资料,开发或选择一个具有较高难度的验证码系统。双方学习新的验证码破解方法,设计并编写破解程序。

2) 对抗过程

双方针对选择的验证码系统开展破解活动,记录破解的时间和成功率。

3）对抗得分

对抗得分由以下部分构成：

（1）破解成功率。

（2）破解时间。

以上各部分的具体分值可由双方在对抗前商议确定。第三轮的总分值应高于第二轮。

3.7　参考文献

[1]　王平，汪定，黄欣沂. 口令安全研究进展[J]. 计算机研究与发展，2016，53(10)：2173-2188.

[2]　童永清. 口令攻击与防范[J]. 计算机安全，2004(01)：66-67.

[3]　张晋源，袁丽欧. 探析关于图形验证码的安全性[J]. 电脑编程技巧与维护，2017(12)：76-77.

[4]　张立新. 多种类型验证码的研究与分析[J]. 福建电脑，2016，32(10)：76＋125.

[5]　胡健，柳青，王海林. 验证码安全与验证码绕过技术[J]. 计算机应用，2016，36(S1)：37-41＋57.

[6]　王刚刚. 图片验证码的识别与研究[D]. 南京：南京邮电大学，2018.

思考题

1. 识别和认证的区别是什么？请提供两个例子辅助你的解释。
2. 说明本地用户认证和远程用户认证之间的区别。
3. 列出并简要说明三种远程用户认证技术。
4. 远程用户认证技术常见的几种用途是什么？
5. 远程用户认证技术面临的挑战分别有哪些？
6. 简要说明基于三种因素的远程用户认证方式。
7. 常见的口令攻击方式有哪些？
8. 列举并简单描述设置和选择口令的四种常用方法。
9. 列出并简要说明常用的验证码类型。
10. 简述用户申请并获得数字证书的流程。
11. 基于生物特征的用户认证原理是什么？
12. 列举并简要描述生物特征认证方法所使用的主要身体特征。
13. 简述基于生物特征的远程用户认证的两个阶段。
14. 总结人脸识别技术面临的挑战。