下载APP

01 | 学习密码学有什么用?

2020-11-23 范学雷

实用密码学 进入课程 >

讲述：范学雷
时长 17:25 大小 15.96M

你好，我是范学雷。

从今天开始，我就和你一块儿去试着揭一揭密码学的面纱，看看里面的机关门道。

每当我们看到一个新鲜事物时，“这东西是什么，有什么用”这样的问题总是会最先浮现在我们的脑海里，诱惑着我们更进一步地去了解它。

那么，密码学是什么呢？它有什么用呢？这就是我们首先要讨论的事情。为了使问题更加直观，我们先从一个例子开始。

约个会能有多难？

我们先来做一个有趣的假设，假如马上要到七夕节了，河东的牛郎想要给河西的织女发一条信息，七夕相约鹊桥会。信息的内容是这样的：

> 织女：
>
> 七月初七晚七点，鹊桥相会。不见不散。
>
> 牛郎

可是，这封信该怎么送出去呢？银河又长又宽，两个人当然不能面对面地口头表达。这封信要想送给织女，只能通过中间媒介。传说中，有人认为这个中间媒介是喜鹊，也有人认为这个中间媒介是流星。反正不管怎么说，都没有证据表明，牛郎可以亲手把信交到织女手里。

不过，这次约会能不能成行，很大程度上就取决于这封信的送达能不能成功。特别是，银河这么长、这么宽，王母娘娘这么神通广大，这封信就更不好送了。

那么，牛郎和织女需要考虑哪些问题呢？

问题一：怎么证明双方的身份？

第一个问题，牛郎一定要确认，收信人是织女，而不是丈母娘王母娘娘。只有织女收到邀约，约会才有可能成功。换个正经的说法，就是牛郎要确认收信人的身份。

从织女的角度看，她也要确认发信人是牛郎，而不是喜欢恶作剧的少年郎，或者是其他的姊妹淘。也就是说，织女要确认发信人的身份。

可是，如果不能面对面，牛郎怎么知道收信的一定是织女；织女又怎么知道发信的一定是牛郎？

问题二：怎么能使消息不泄露？

第二个问题，牛郎一定要确认，这封信的内容王母娘娘看不到。约会的时间、地点一旦外泄，约会恐怕就会节外生枝。或者换个说法，只有牛郎和织女才能够看得到这封信的内容，其他人都不能阅读这封信。

问题是，如果织女能够看得到这封信，为什么王母娘娘就一定看不到？无论中间媒介是喜鹊还是流星，王母娘娘可是有遮天的权势，她难道就没有办法看一眼信件的内容吗？

问题三：怎么防止内容被篡改？

更坏的情况是，如果消息不仅泄露了，内容还被篡改了呢？这是牛郎织女要考虑的第三个问题。牛郎怎么才能确保，织女收到的信的内容是七夕鹊桥会，而不是分手宣言；约定的时间是晚七点，而不是早八点；约会的对象是织女，而不是嫦娥？

而织女也一定要确认，收到的信的确是牛郎写的，而且一字不多、一字不拉和一字不差。牛郎怎么做，才能确保信件的内容不被篡改呢？

问题四：怎么确保信件能收到？

事情纵有千般好，可如果织女不能及时收到信，牛郎是会被放鸽子的。这封信能不能在七夕前送到？这是牛郎织女要考虑的第四个问题。

如果是喜鹊传递信件，这个可怜的小东西会不会中途被请去喝茶吃酒，醉醺醺地忘了托付？如果是流星传递信件，织女会不会在七夕前看看流星雨，解读哪一颗流星携带了牛郎的信息？万一夜空忽然像开了万花筒，红的蓝的紫的烟花可劲地绽放，织女只有一双眼睛，可如何是好？

所以，怎么才能保证牛郎发送的信息可以被及时地送达、拆阅？

问题五：怎么防止翻脸不认账？

最后一个问题就是，牛郎一定要确认，织女收到了信，不能抵赖说没收到；织女也一定要确认，牛郎发出了约会邀请，不能抵赖说没发出邀请。

做过的事，说过的话，要有防翻脸、防撕扯机制。有什么办法防止翻脸不认账呢？

所以，你看，我们和附近的朋友打个招呼很容易：走到面前，说句你好；如果有别人，小心翼翼地问，七月初七有空没有？这信息就算是送到了。

可是，一旦我们拉开了距离，打个招呼、送一封信就变成了一件有点复杂的事情。

约会难题有现实意义吗？

在无线电技术发明之前，大部分的信息传递都是在人与人之间进行的，尤其是在熟人之间。人与人之间的信任是解决信息安全传递问题的最关键因素，信息传递的速度和半径也有很大局限。

比如说，在历史战争剧中，我们经常可以看到需要一名勇冠三军的猛将突围搬救兵的情节。作为敌方，只要能劫杀到突围的猛将，信息传递的路径就算是掐死了。

好在无线电技术发明之后，信息传递的办法就彻底改变了。即便是赵云再世，现在也没有七进七出的战争场景了。总体来说，现在的信息传递变得更迅速、更经济、几乎是无处不在了，家书值万金的场景也是一去不复返了。

无论你身在何处，只要你有一部智能手机，你就可以联系到家人和朋友。这时候你会问了，那现在都有手机了，发个微信不就全解决了吗？哪里还有什么信息传递问题？

是的，作为一款即时通信的工具，微信已经帮助我们解决掉很多问题了。那我们上面讨论的牛郎织女约会面临的问题还有现实的意义吗？有的。

因为，牛郎织女送信的障碍不独独横亘在他们之间，**它们是信息传递的普遍问题**。即使是今天看起来用户得到简单、便捷、便宜、即时的通信背后，依靠的也是复杂的现代信息技术。

现在很大一部分信息流，都是在人与机器之间进行的。无论是淘宝购物，还是银行转账，甚至发送微信，其实都是你在和机器交流。机器同意后，你的信息才有可能传递给另一个机器，或者你期望交流的具体的一个人。

既然，信息安全的问题一直和人类历史相生相伴，那我们该如何解决呢？

如果我们能够把具体的问题抽象出来，简化成易于理解的、方便表达的模型，你就能够知晓这些问题的普遍性，并且能够把它扩展到千变万化的场景里去。

那么，对于上述的这些问题，我们换个角度，换个说法，把它们表述成需求，并且放到信息系统这个虚拟的代码世界里看看，就可以找到这个具有普遍意义的模型了。

需求一：识别身份，确定牛郎就是牛郎

织女收到信，一看落款是牛郎，她就知道这个牛郎应该是孩子他爹，是董永，而不是王小二。你想一想，如果是一台机器，它该怎么解释“牛郎”这两个字。“牛郎”代表的是一个人，还是一群人？是一只蚊子，还是一盏路灯？没有更多的信息，这个机器是没有办法做进一步判断的。

这就是我们要考虑的第一个需求，就是怎样表述身份，使得这个身份可以被准确标识。这也就是所谓的**身份识别（Identification），表述的是身份如何呈现和表述，说的是身份的记号。**

扩展开来，这里的身份可以是信息的参与者，比如微信账户，也可以是资产的持有者，比如银行账户，网站域名。

需求二：认证身份，验证牛郎就是牛郎

织女收到信，看到落款是牛郎，再细看笔迹，她可能就有八分把握断定这信是孩子他爹写的。之所以还有两分疑问，那是因为对于神通广大的王母娘娘，伪造笔迹算不上是了不起的事情。

机器该怎么办？网络传递的都是二进制代码，你的键盘输入的牛郎和我的键盘输入的牛郎，并没有笔迹的差异。另外，如果只有八分把握，你敢不敢使用手机银行转账？

这就是我们要考虑的第二个需求，就是怎样认证身份，验证信里面所宣称的牛郎就是写信的那个牛郎。这也就是所谓的**身份认证（Authentication），是识别和验证身份的过程，也就是验明正身的意思。**

需求三：管理特权，授予织女看信权利

这封信为什么会送到织女的手里，而不是王母娘娘的手里？很显然，这封信的收信人是织女，所以喜鹊会把信投递给织女而不是王母娘娘。其实，这也就意味着，织女独享收信、看信的权利，而王母娘娘没有。

机器会怎么办呢？理论上，互联网的每个信息转发节点都有可能截获这封信，看到信的内容，这就破坏了看信者的独享权利。那我们怎么才能把权利授予织女，而排除其他人看信的权利？

这就是我们要考虑的第三个需求，就是怎么管理权限，使得特定的身份有特定的权限。这也就是所谓的**授权（Authorization），是指定对资源的访问权限，或者使用特权，说的是权利。**

把上面三个需求放在一起，我们就解决了**权限管理的基本问题：该怎么标识身份？该怎么验证身份？以及一个身份拥有什么样的权利？**

需求四：信息保密，没有权限不能看信

牛郎织女约会的第二个问题是，怎么能使消息不泄露？换个说法，就是怎么保密信息。**所谓的信息保密，也就是数据的“机密性”（Confidentiality），指的是数据未经授权，不得访问。授权的对象既包括个人、实体，也包括处理过程。**

如果没有授权王母娘娘拆阅信件，即使王母娘娘劫杀了送信的喜鹊，她也不能看到信件的内容。这就是信息保密的需求。

需求五：信息完整，保护内容不被篡改

牛郎织女约会的第三个问题是，怎么防止内容被篡改？换个说法，就是怎么保持信息的完整性。**所谓的“完整性”（Integrity），指的是数据未经授权，不得更改。信息的完整性，也意味着信息的准确性，信息不能残缺不全，或者来源不明、去向不明。**

如果我们能做到保护信息不被篡改，即使王母娘娘神通广大，可以请喜鹊去喝茶吃酒，她也没有办法改动信件的哪怕一个字、一个标点符号。这就是信息完整的需求。

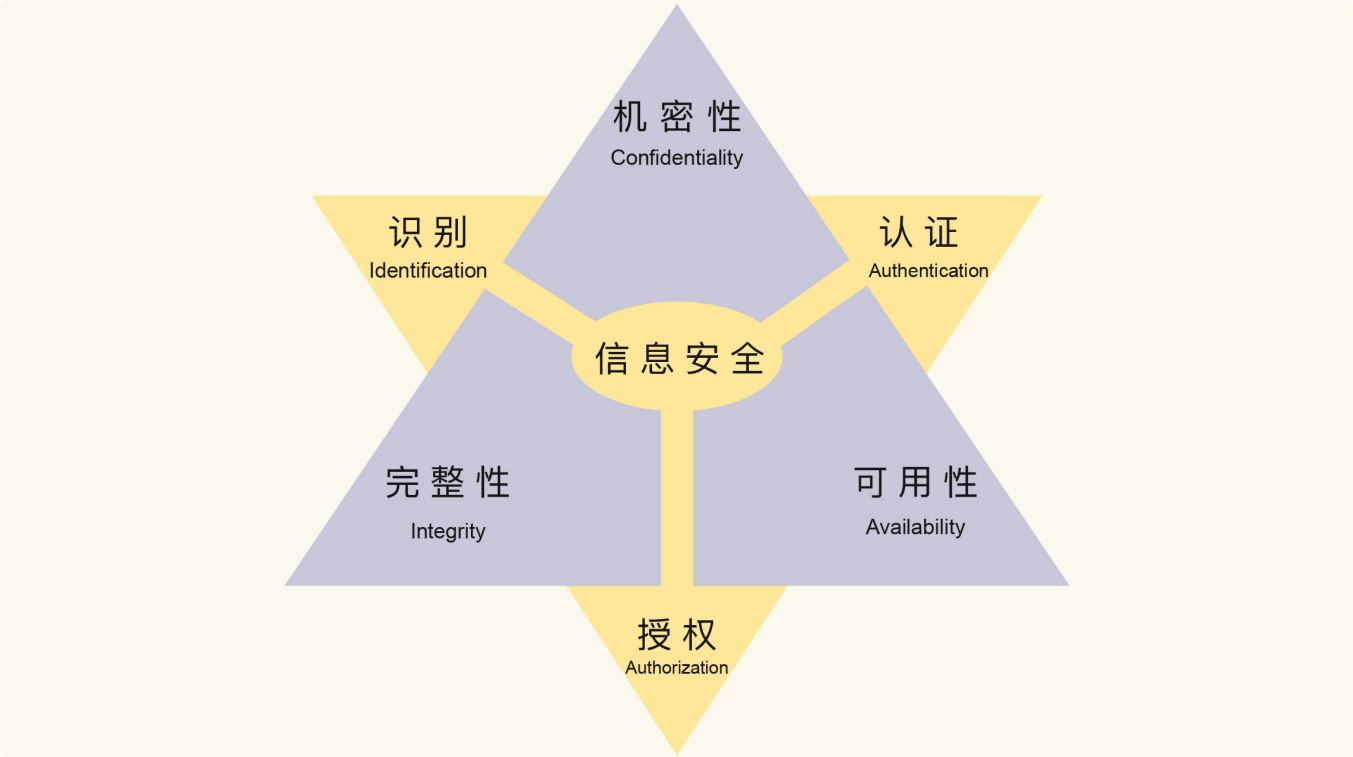
需求六：信息可用，保持信息获取能力

牛郎织女约会的第四个问题是，怎么确保信件能收到？换个说法，就是怎么保持信息的可用性。**所谓的“可用性”（Availability），指的是数据经过授权，可以访问。也就是说，需要的时候，经过授权，可以获取信息，能够获取信息。**

如果喜鹊被请去喝茶吃酒，醉醺醺地忘了托付，牛郎的信送不到，织女的信收不到，这就破坏了信息存在的意义。该发送的信息能够及时发送出去，该收到的信息能够及时收到，这就是信息可用的需求。

我们把上面三个需求放在一起，就解决了信息安全的基本问题：**信息能够完整地、秘密地传递出去和接收进来**。

在这六个需求里面，前三个需求，说的是授权的过程，后三个需求，说的是安全的要素。



哪一个需求最重要？

不知道你有没有疑问，这六个需求里，哪一个需求最重要，该优先考虑呀？这是一个好问题。

信息安全这件事，具有典型的木桶效应，安全不安全是由最短的一块木板决定的。什么意思呢？就是**每一个要素、每一个需求实现都不能有明显的弱点**。任何一个要素，如果我们没有清清楚楚地落到实处，都会带来一把鼻子一把泪的。

这六个需求就像是六个维度，就像一间屋子的长宽高（三维更便于理解）。如果很长、很宽，但是高度为零，它就没有体积。没有人能住高度为零的屋子，或者高度 10 厘米的屋子。

同样，也没有人能住长度为零或者宽度为零的屋子。一个舒适的屋子，长度、宽度、高度都要合适。这就好比，牛郎和织女约会的例子中，任何一个问题真实发生了，这场约会就会走向失败。

所以，有没有办法可以满足所有的需求呢？这时候，密码学就登场了。

密码学有办法吗？

如果放在 50 年前，这些需求理论上是没有办法完全解决的。但是现在，密码学有好几套体系办法，可以漂亮地解决掉这些问题，满足这些需求。

我们知道，信息安全是一个庞大复杂、涵盖广泛的学科，而密码学只是信息安全技术的一个小门类。也有人说密码学是信息安全的核心技术，我并不反对这样的说法。

虽然密码学只是一个小门类，但是如果你钻进了密码学领域，你就会发现，密码学也是一个大森林，枝枝蔓蔓的有很多技术、规范、协议和体系。

密码学最基础的分支有三个，第一个是单向散列函数，第二个是对称密码技术，第三个是非对称密码技术。这三项基础技术的组合运用，诞生出了丰富的安全协议和体系，比如说数字证书、安全传输、区块链、数字货币等。

回到我们上面的约会问题，如果粗陋地来看，对称密码技术可以通过加密、解密，解决“机密性”的问题；单向散列函数，可以解决“完整性”问题；非对称密码技术可以解决授权和认证的问题；通过我们对这三项基础技术的综合运用，就可以提高系统的“可用性”。

那这些密码学技术都是什么呀？是怎么解决这些问题的呀？这就是我们整个专栏要关注的重点，后面我们会接着拆解这些密码学概念和技术，开始进入密码学的细节。你准备好了吗？

Take Away（今日收获）

英文中，有一个词汇叫“Take Away”，指的是一个活动结束后，比如会议或者讨论，大家要记住的关键事实、观点或者想法。用在每篇文章的结尾，我觉得是一个很贴切的表述。但是，我没有找到合适的中文翻译，我们先使用英文词汇。谁有好的翻译，可以给我留言。

今天，通过牛郎织女这个小例子，我们探讨了牛郎织女约会信息传递的五个障碍：双方身份难以证明、消息会泄露、内容会被篡改、信件无法及时送到以及存在双方翻脸不认账的风险。

虽然在现代社会，传递一个消息已经不是一件困难的事，但这五个障碍仍是信息安全里的重要议题，我们也由此总结了信息安全的六个基本需求：

身份识别、身份认证和授权。这三个需求解决了权限管理的基本问题：该怎么标识身份？该怎么验证身份？以及一个身份拥有什么样的权利？

信息的机密性、完整性、可用性。这三个需求解决了信息安全的基本问题：信息怎么能够完整地、秘密地传递出去、接收进来？

最后，通过今天这一讲，我希望你：

理解信息安全的基本问题和基本需求；

建立起来均衡考量信息安全基本需求的意识；

明确学会用好密码学的意义。

思考题

假设牛郎织女面前都有一部电脑，电脑都是连接着互联网的。你能不能给牛郎织女一些建议，该怎么做才能摆脱上述的种种问题，把约会信息传递成功？你的建议有没有其他的缺陷？会不会带来新的问题？

这个问题现在对你来说可能有点难。不过，我就是想让你打开脑洞，尽情地发挥自己的想象力，看看有没有办法，有没有问题。专栏快结束的时候，我还会再一次问这个问题。到时候，你可以比较一下，你的想法有没有变化。

欢迎在留言区留言，记录、讨论你的想法。你的每一次发言都是思维碰撞出的火花。

也欢迎把这一讲分享给你的朋友。好的，今天就这样，我们下次再聊。

提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 开篇词 | 人人都要会点密码学

下一篇 02 | 单向散列函数：如何保证信息完整性？

精选留言 (12)

写留言

TerryGoForIt
2020-11-25

这就是 HTTPS 所解决的问题呀，即三大问题：机密性、完整性和身份校验。机密性和完整性可以由密码套件来保障（TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256）,身份验证需要有 PKI（公钥基础设施）来参与保证。

展开

作者回复: 又是一个高手哎，欣喜又紧张。

3

天蓬太帅
2020-11-29

看了一些同学写的方案，觉得可能忽略了一个前提。
如果采用非对称加密，则需要有一个对公钥确认的机制。除非双方在上次会面时一起生成了各自的密钥对，或者玉皇大帝有一个证书实名认证体系，否则相隔天河的两个人无法在没有第三方公信支持下建立认证所需的依据……

展开

作者回复: 这个理解比较深！公钥是需要查验的，也就是说要证明公钥持有者的身份需要额外的办法。同学们刚来，需要一段时间才能建立起来这个概念。

1

水蒸蛋
2020-11-23

牛郎织女用网络通信首先要建立密码本，可以用往事的点点滴滴来建立只有他们知道的密码本，这个事对称加密

展开

作者回复: 嗯，如果在多想一点：怎么保证牛郎侄女都有相同的密码本？而且可以同步使用密码本？

1

wrzgeek
2020-12-03

密码学知道的不多，现在能想到的是:在各自的电脑里应该都有证书用来验证身份的，然后双方通过非对称加密算法来交换对称秘钥，然后通过交换的对称秘钥加密传输的信息

作者回复: 嗯，这些都是密码学的范畴。

许峰
2020-11-30

又(重新)发现了一个新的世界~ 大学选修过密码学历史

展开

作者回复: 一个小学科，也是一个大世界，欢迎跟着我们一起讨论密码学。

杨杨杨
2020-11-30

老师，在怎么确保信件能收到问题中
我想到了钉钉与抖音私信 发送消息都有 已读 已发送 未读的状态
还有邮箱 发送邮件的状态 可以即时显示

作者回复: 没用过这两个的私信。不过，这的确是一个好的设计！

彩色的沙漠
2020-11-25

非对称加密交换会话秘钥，数字证书身份认证，对称加密通信

作者回复: 高手也来了，多留言探讨问题啊。-:)

任昭辉
2020-11-24

交换证书，然后签名验签，加密解密

展开

作者回复: 嗯，再问多一点：证书怎么来的呢?

2

Charlie Guo
2020-11-24

牛郎织女可以向所有人公开他们的公钥，牛郎拿到织女的公钥后可以把一个通钥用织女的公钥加密，然后发给织女，织女接到这个加密文件后可以用自己的私钥解密，得到这个通钥。之后牛郎织女只要用只有他们知道的通钥去加密解密传送文件就好了。

展开

作者回复: 调皮一点，加密数据也不用发“给织女”，满天的撒出去就行，王母娘娘收到都不怕。

Nelson
2020-11-23

老师，牛郎不是董永

展开

作者回复: 啊，闹笑话了？我怎么记得是董永呢？小时候的故事，估计是记不住细节了。

1

vcjmhg
2020-11-23

在软件选择上应该尽量选择安全的通讯软件，聊天的内容应该通过彼此熟悉的暗语进行加密

作者回复: 多想一点：该怎么使用暗语加密？

baggio
2020-11-23

牛郎生成一对非对称加密的密钥，把公钥给织女，织女使用牛郎给的公钥加密一个随机的密钥，将密文发送给牛郎，牛郎使用私钥解密密钥，并生成一个随机密钥拼接到织女密钥后边，使用织女的密钥对称加密密钥，织女收到之后使用之前保存的密钥解密，以后他们就使用这个密钥加解密所有的消息。存在的问题：公钥如何确保发送到织女那里，如果被截获并充当织女，那这所有的数据都不能正常发送到织女那里

展开

作者回复: 这个，几乎就是变形的TLS啊。公钥不是公开的吗？为什么要送到织女哪儿？满天散布行不行？

1