计算机网络中的安全

网络安全概念

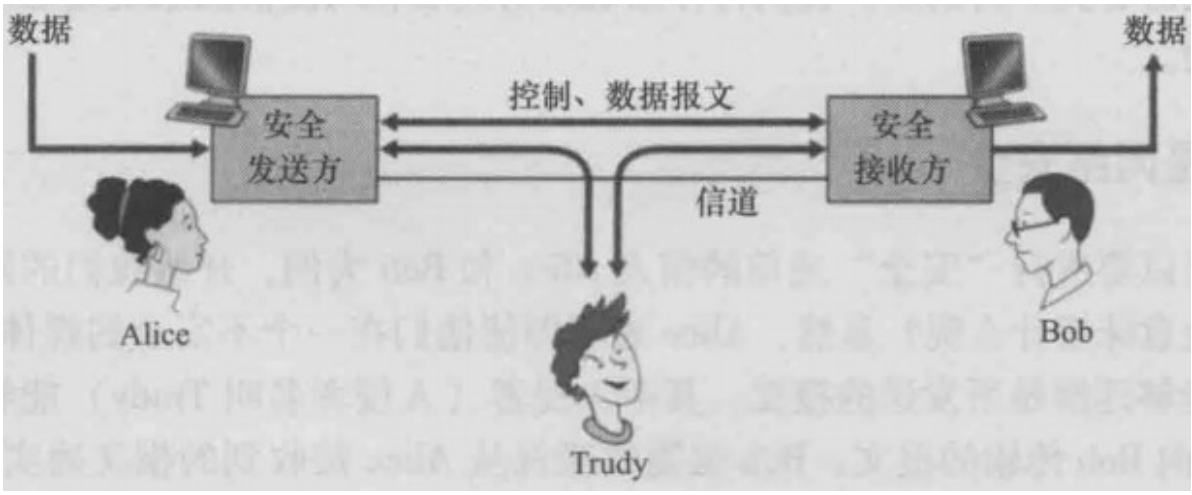
安全通信（secure communication):

- **机密性（confidentiality）**：仅有发送方和希望的接收方能够理解传输报文的内容。因为窃听者可以截获报文，这必须要求报文在一定程度上进行**加密（encrypted)**,使截取的报文无法被截获者所理解。机密性的这个方面大概就是通常意义上对于术语安全通信的理解。
- **报文完整性（message integrity）**：确保其通信的内容在传输过程中未被改变（恶意篡改或意外改动）。我们在可靠传输和数据链路协议中遇到的检验和技术在扩展后能够用于提供这种报文完整性。
- **端点鉴别（end- point authentication）**：发送方和接收方都应该能证实通信过程所涉及的另一方确实具有他们所声称的身份。人类的面对面通信可以通过视觉识别轻易地解决这个问题。当通信实体在不能看到对方的媒体上交换报文时，鉴别就不是那么简单了。当某用户要访问一个邮箱，邮件服务器如何证实该用户就是他或她所声称的那个人呢?
- **运行安全性（operational security）**：几乎所有的机构（公司、大学等）今天都有了与公共因特网相连接的网络。这些网络都因此潜在地能够被危及安全。攻击者能够试图在网络主机中安放蠕虫，获取公司秘密，勘察内部网络配置并发起 DoS 攻击。诸如**防火墙**和**入侵检测系统**等运行设备正被用于反制对机构网络的攻击。防火墙位于机构网络和公共网络之间，控制接人和来自网络的分组。入侵检测系统执行"深度分组检查"任务，向网络管理员发出有关可疑活动的警告。

入侵者的行为

明确了我们所指的网络安全的具体含义后，我们接下来考虑入侵者可能要访问的到底是哪些信息，以及入侵者可能采取哪些行动。Alice（发送方）想要发送数据给 Bob（接收方）。为了安全地交换数据，即在满足机密性、端点鉴别和报文完整性要求的情况下，Alice 和 Bob 将交换控制报文和数据报文（以非常类似于 TCP 发送方和接收方双方交换控制报文和数据报文的方式进行）。通常将这些报文全部或部分加密。
人侵者能够潜在地执行下列行为:

- **窃听**——监听并记录信道上传输的控制报文和数据报文。
- **修改、插入或删除**报文或报文内容。

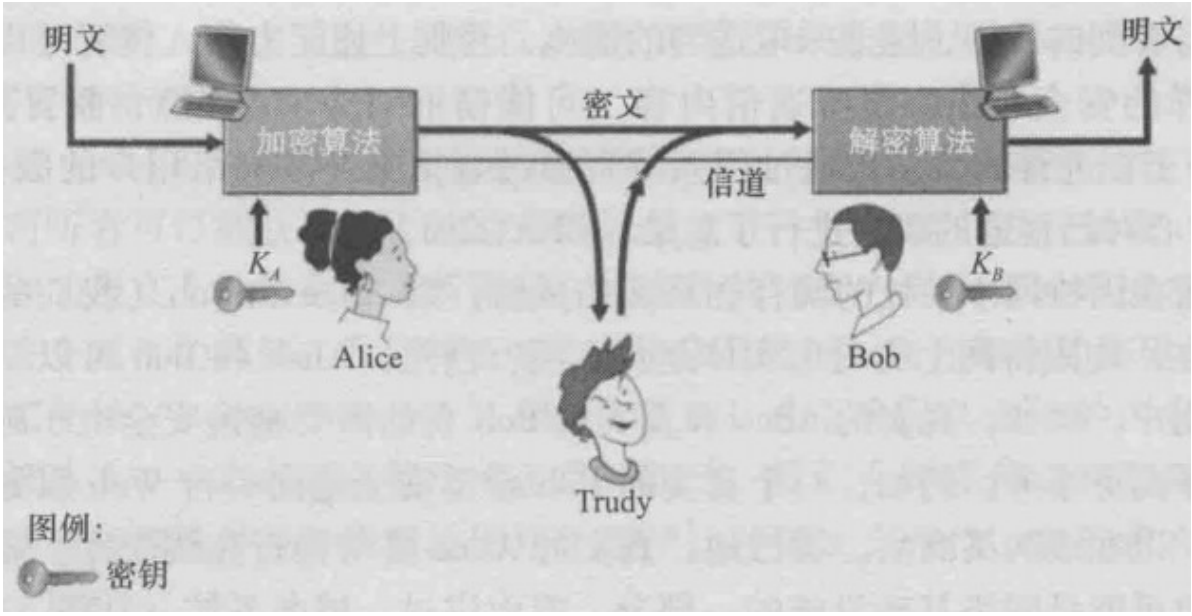


发送方、接收方和入侵者（Alice、Bob 和 Trudy)

密码学概念

初等概念

现在假设 Alice 要向 Bob 发送一个报文。 Alice 报文的最初形式（例如，“ Bob, I love you. Alice" ）被称为**明文（ plaintext, cleartext ）** 。 Alice 使用**加密算法（ encryption algorithm）**加密其明文报文，生成的加密报文被称为**密文（ ciphertext ）**，该密文对任何人侵者看起来是不可懂的 。 有趣的是在许多现代密码系统中，包括因特网上所使用的那些，加密技术本身是已知的，即公开发行的、标准化的和任何人都可使用的，即使对潜在的人侵者也是如此！显然，如果任何人都知道数据编码的方法，则一定有一些秘密信息可以阻止入侵者解密被传输的数据 。 这些秘密信息就是密钥。



密码学组成部分

Alice 提供了一个**密钥（ key ）** K_A，它是一串数字或字符，作为加密算法的输入 。 加密算法以密钥和明文报文 m 为输入，生成的密文作为输出 。 用符号 $K_A(m)$ 表示（使用密钥 K_A 加密的）明文报文 m 的密文形式。 使用密钥 K_A 的实际加密算法显然与上下文有关。 类似地， Bob 将为**解密算法（ decryption algorithm ）**提供密钥 K_B ，将密文和 Bob 的密钥作为输入，输出初始明文 。 也就是说，如果 Bob 接收到一个加密的报文$K_A(m)$ ，他可通过计算 $K_B(K_A(m)) = m$ 进行解密。

- **对称密钥系统（ symmetric key system ）**： Alice 和 Bob的密钥是相同的并且是秘密的 。
- **在公开密钥系统（非对称加密）（ public key system）**：使用一对密钥：一个密钥为实际上为全世界所知，另一个密钥只有 Bob 或 Alice 知道（而不是双方都知道）。

对称密钥密码

- 凯撒密码
- 单码代替密码
- 根据入侵者所拥有的信息区分破解加密方案的难易程度 。
    - 唯密文攻击
    - 已知明文攻击
    - 选择明文攻击。
- 多码代替密码
- 块密码与流密码
- 密码块链接

非对称加密（公开密钥加密）