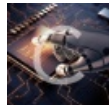


隐写术理论入门

转载

[aurora](#) 于 2019-02-20 13:41:08 发布 1828 收藏 6
分类专栏: [网络攻防 ctf](#)



[网络攻防](#) 同时被 2 个专栏收录

15 篇文章 0 订阅

订阅专栏



[ctf](#)

1 篇文章 0 订阅

订阅专栏

隐写的定义及模型——囚犯模型

隐写技术起源于Simmons在1983年提出的监狱通信问题。在该问题中隐写被定义为Alice与Bob建立一条监听者Wendy无法发现的隐蔽通信线路即Alice将秘密信息在嵌入密钥的控制下，通过嵌入算法将隐秘信息隐藏于载体中形成隐密载体,隐密载体再通过监狱通

道传输给Bob, Bob利用密钥从隐密载体中恢复出秘密信息的过程。由于隐写可以将秘密信息隐藏到任何一种正常多媒体报文中，因而报文在网上传输时不会引起监听者的注意，从而达

到麻痹监听者的目的，即使监听者预知含有秘密信息的载体也很难将信息提取和还原出来。

该隐写模型见图1:

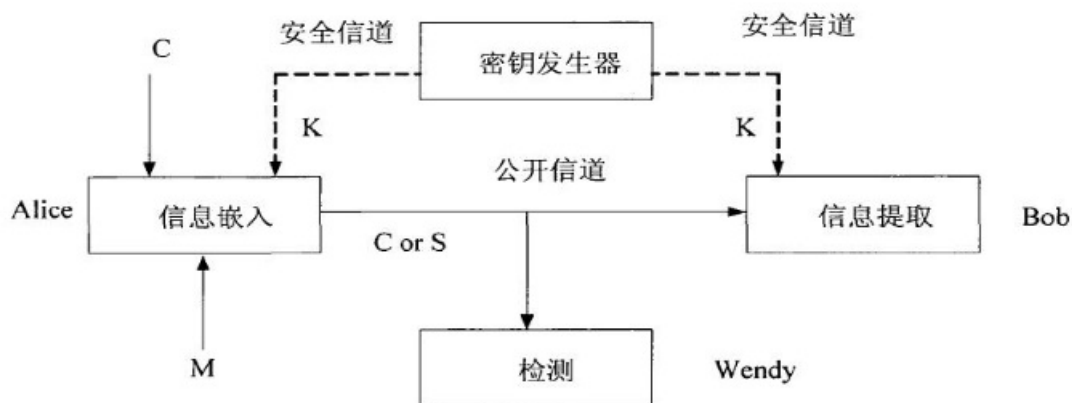


图 1 隐写的模型

https://blog.csdn.net/aurora__

<https://wenku.baidu.com/view/500d845d842458fb770bf78a6529647d272834bd.html>