<<信息安全综合实践>>

图书基本信息

书名：<<信息安全综合实践>>

13位ISBN编号：9787302213536

10位ISBN编号：7302213534

出版时间：2010-2

出版时间：清华大学出版社

作者：李建华　等编著

页数：351

<<信息安全综合实践>>

前言

信息安全学科是一门新兴的综合性交叉学科，涉及通信学、计算机科学、密码学、信息学、数学、安全工程、法律、管理等诸多学科，也关系到国家社会信息化的推进、国家基础信息系统的安全保障工作、电子政务和电子商务的应用以及国家安全。
本书编者积极探索和建设以主干专业课为基础，以实习实践为主线，面向工程应用的实践教学模式。依托在国家863重大项目“信息安全工程实践综合实验平台研究与集成”等滚动支持下建设的国内首个信息安全综合实践平台，教学团队开设了“信息安全综合实践”、“信息安全科技创新”等课程，通过基础性实验、拓展性实验和创新性实验，深化学生专业理论知识的掌握和应用，培养学生的实践能力和创新精神，也形成了由信息安全认证类、信息安全综合管理类、信息安全攻击与防护类以及无线网络安全等部分组成的教材体系。
为了更好地与国内外信息安全工作者进行学术和教学交流，推动国内信息安全工程实践人才的培养，教学团队将所形成的教材整理成书，抛砖引玉。
对于书中的不足之处恳请读者批评指正。
参与本书编写的人员有李建华、陈恭亮、陆松年、薛质、孟魁、蒋兴浩、张爱新、龚洁中、杜海波、吴越、范磊、张宝稳、刘功申、马进等。
本书在编写过程中得到了上海交通大学信息安全工程学院许多教师以及本科生和研究生的支持和帮助，在此向他们表示衷心感谢。

<<信息安全综合实践>>

内容概要

本书系统地介绍了信息安全所涉及的信息安全认证类、信息安全综合管理类、信息安全攻击与防护类以及无线网络安全等实验，这些实验分成基础性实验、拓展性实验和创新性实验，有些可独立实施，有些则要借助于信息安全综合实践平台来实现。

本书可作为信息安全专业、通信专业、计算机专业、信息专业的本科生和研究生的教科书，也可以供从事信息安全工作的科研和工程技术人员参考。

<<信息安全综合实践>>

书籍目录

章节摘录

插图：1.1.4 密码分析学密码分析学就是研究密码破译的科学。
如果能够根据密文系统确定出明文或密钥，或者能够根据明文密文对系统确定出密钥，则称这个密码系统是可破译的。
常用的密码分析方法主要有3种。
（1）穷举攻击：对截获的密文，密码分析者试遍所有的密钥，以期得到有意义的明文；或者使用同一密钥，对所有可能的明文加密直到得到的密文与截获的密文一致。
穷举攻击也称强力攻击或完全试凑攻击。
（2）统计分析攻击：密码分析者通过分析明文与密文的统计规律，得到它们之间的对应关系。
（3）数学分析攻击：密码分析者根据加密算法的数学依据，利用数学方法（如线性分析、差分分析及其他一些数学知识）来破译密码。
根据密码分析者可利用的数据，可将常见的密码分析攻击分为4类，由弱到强分别是唯密文攻击、已知明文攻击、选择明文攻击和选择密文攻击。
（1）唯密文攻击：密码分析者有一些用同一密钥加密的密文，他们试图恢复出尽可能多的明文，或者推算出加密密钥以解出更多的密文。
（2）已知明文攻击：密码分析者不仅得到了一些明文，而且也知道相应的密文，他们的任务是据此推出加密密钥或算法，而该算法可以对用同一密钥加密的任何密文进行解密。
（3）选择明文攻击：密码分析者不仅可得到一些消息的密文和相应的明文，而且也可选择被加密的明文。
通过选择特定的明文进行加密，有可能产生更多的关于密钥的消息，这比已知明文攻击更有效。
如果分析者不仅能选择被加密的明文，还能基于以前的结果修正这个选择，那么就是自适应选择明文攻击。
（4）选择密文攻击：密码分析者可选择不同的密文，并可得到对应的明文。
这种攻击主要用于公钥算法。
一个密码系统，如果无论密码分析者截获多少密文和用什么技术方法进行攻击都不能被攻破，则称为绝对不可破译的。
绝对不可破译的密码在理论上是存在的，这就是著名的“一次一密”密码。
但是，由于密钥管理上的困难，“一次一密”密码是不实用的。
从理论上来说，如果能够拥有足够多的资源，那么任何实际使用的密码都是可以破译的。

<<信息安全综合实践>>

版权说明