期末复习提纲 – 信息安全技术

一、概述

1. 安全基本目标有哪些？其含义分别是什么？
2. OSI 安全框架定义了哪三个方面？其中安全攻击被分成哪两个类别，有什么特点？分别有哪些实例？

二、信息加密技术和信息隐藏技术

0. 对加密信息的攻击类型有哪些？
3. 现代密码学算法按照密钥的使用方式分主要有哪两类？
4. 对称密码算法按照对明文的处理方式不同可以分成哪两类？对称密码算法有哪些？基本的参数（明密文分组长度，密钥长度）？
5. 分组密码的工作方式有哪些?这些工作方式的缩写是什么？特点是什么？
6. 公钥密码有哪些算法，主要的应用是什么？主要指公钥的加解密、密钥分配和数字签名等方法的应用/作用。
7. 公钥算法安全性的数学基础有哪些？
8. 理解模幂运算，包括: $C=M^e \bmod n$，则 $M=C^d \bmod n$。

如果 $M=AB \bmod n$，则 $M^e \bmod n=(AB \bmod n)^e \bmod n =A^eB^e \bmod n$。

9. RSA 算法的计算过程？针对 RSA 算法有哪些类型的攻击？
10. DH 算法的实现过程？针对 DH 算法的中间人攻击是如何发生的？
11. ~~ElGamal 算法的计算过程？~~
12. 作为保密通信的一种方式，信息隐藏和数据加密的主要区别是什么？

三、消息认证技术

13. 什么是消息认证？为什么需要消息认证？如何实现消息认证（或消息认证函数的实现方式）？
14. 散列函数可被应用于哪些方面？密码学散列函数需哪些安全性需求？常见的散列函数有哪些？基本参数（输入、输出长度、安全性等）？
15. 什么是消息认证码？消息认证码的实现方式有哪两种？~~常见的算法有哪些~~?
16. 消息认证和加密的关系（同时提供认证和加密的通用方案有哪些）

四、数字签名技术

17. 什么是数字签名？数字签名的作用是什么？常见的数字签名算法有哪些？如何理解 RSA 私钥加密实现数字签名?

五、密钥分配和管理技术

18. 对称密钥的分发方式有哪些（如何实现）？
19. 什么是公钥证书？如何生成？CA 的作用包括哪些？PKI 包括哪些关键元素？

六、身份认证技术

20. 什么是身份认证？身份认证的原理是什么？身份认证的常用工具有哪四种？
21. 认证中如何抗重放？
22. 简述基于挑战应答的身份认证方式？

23. Kerberos v4 认证系统是如何实现的？（仅做了解）

七、访问控制和审计技术

24. 对访问控制和审计的最基本的理解

八、网络安全与 Internet 安全

25. 按照协议分层，各层安全网络协议有哪些？

26. 建立在传输层之上的安全协议有哪些？

27. Web 安全威胁有哪些？（从 web 通信中涉及的浏览器、web 服务器和通信信道的角度来讨论 web 安全威胁）

28. SSL/TLS 提供哪些服务？SSL/TLS 协议层次实现？

29. 基于 wireshark 的数据包捕获结果分析。

其他：

30. 基于 openssl 的程序设计实验的代码分析。

31. windows 下常见的命令行命令、常见端口

32. 基础的网络知识，主要涉及 web 应用相关的 http、tcp 等内容，见上课补充的 ppt

0. 常见攻击形式：钓鱼、重放、劫持、洪泛、拒绝服务、欺骗、穷举

结合每次的作业和 ppt 进行复习。