



核心摘要

这是一个要求你们**小组合作**完成的**技术论文和编程项目**。核心任务是**研究、实现、攻击并防御**两种最重要的密钥交换协议：**Diffie-Hellman (D-H)** 和 **RSA**。你们需要像一个安全研究员一样，不仅理解它们如何工作，还要理解它们如何被攻破，以及如何加固它们。

任务详细分解

你的项目必须包含以下八个部分：

1. 解释一种对D-H的攻击技术

- **要求**：选择一个针对Diffie-Hellman协议的攻击方法，并详细解释其原理。
- **可能的攻击**：中间人攻击是最经典和最容易理解的。你也可以选择其他如：小子群攻击、无效曲线攻击等。
- **内容**：解释攻击者是如何利用协议的弱点或实现上的缺陷来窃听或篡改通信的。

2. 解释一种对RSA的攻击技术

- **要求**：选择一个针对RSA密钥交换或签名的攻击方法，并详细解释其原理。
- **可能的攻击**：定时攻击是一个很好的选择，因为它侧重于旁道攻击。其他选择包括：因式分解攻击（如果使用弱密钥）、填充预言攻击等。
- **内容**：解释攻击者是如何在不直接破解数学难题的情况下，通过分析时间等旁道信息来恢复私钥的。

3. 实现D-H和RSA

- **要求**：编写程序代码，分别实现基础的Diffie-Hellman密钥交换和RSA加密/密钥交换过程。
- **目的**：这证明了你们对协议底层数学和流程的真正理解。你不需要实现工业级的强度，但要能正确演示协议的核心步骤。

4. 应用攻击技术攻击D-H和RSA

- **要求**：使用你在第3步中实现的协议，然后编写攻击代码，对你实现的协议发起在第1步和第2步中描述的攻击。
- **目的**：这是“实践出真知”的部分。你需要成功演示攻击是如何在现实中发生的。例如，在你的D-H实现中成功插入一个中间人，或在你的RSA实现中通过计时分析获取密钥。

5. 解释如何防御这些攻击

- **要求：**从理论和最佳实践的角度，解释有哪些方法可以防御你在第1步和第2步中描述的攻击。
- **内容：**例如，防御D-H的中间人攻击需要使用认证（如数字证书）；防御RSA的定时攻击需要使用常数时间算法。

6. 应用防御技术保卫D-H和RSA

- **要求：**修改你在第3步中实现的代码，将第5步中提到的防御措施应用进去。
- **目的：**证明你不仅知道如何攻击，也知道如何修复。你需要展示加固后的协议能够成功抵御你之前演示的攻击。

7. 比较和对比对D-H和RSA的攻击

- **要求：**分析并讨论这两种协议所面临攻击的异同点。
- **思考方向：**
 - 攻击目标是什么？（是窃听会话密钥，还是直接获取长期私钥？）
 - 攻击的根源是什么？（是协议本身的设计缺陷，还是实现上的疏忽？）
 - 攻击的难度和成本如何？

8. 比较和对比防御D-H和RSA的方法

- **要求：**分析并讨论保护这两种协议的方法的异同点。
- **思考方向：**
 - 防御的核心思想是什么？（认证、使用安全参数、防止信息泄漏）
 - 哪种协议的防御更复杂或成本更高？
 - 在现实世界中（如TLS协议中），它们是如何被结合使用以相互弥补弱点的？