山东大学 软件 学院

信息安全导论 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：201600301079 | 姓名： 崔玉峰 | | 班级： 2016级软件4班 |
| 实验题目： CA和证书 | | | |
| 实验学时：4 | | 实验日期： 2018/ | |
| 实验目的： | | | |
| 硬件环境：  PC  CPU : intel-i5  RAM: 8G | | | |
| 软件环境：  虚拟机：VMWARE  操作系统：ubuntu 18.04.5 64位 | | | |
| 实验步骤与内容：   1. **基本概念解析**   **CA:** 证书颁发机构（CA, Certificate Authority）即颁发数字证书的机构。是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。  **CA证书**： 证书的内容包括：[电子签证机关](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E7%AD%BE%E8%AF%81%E6%9C%BA%E5%85%B3/3344153" \t "https://baike.baidu.com/item/ca%E8%AF%81%E4%B9%A6/_blank)的信息、[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5/6447788" \t "https://baike.baidu.com/item/ca%E8%AF%81%E4%B9%A6/_blank)用户信息、公钥、权威机构的签字和有效期等等。目前，证书的格式和验证方法普遍遵循X.509 国际标准。  **Https：** 是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。  **SSL:**  SSL协议实现的安全机制包含：传输数据的机密性：利用对称密钥算法对传输的数据进行加密。份验证机制：基于证书利用数字签名方法对server和client进行身份验证，当中client的身份验证是可选的。消息完整性验证：消息传输过程中使用MAC算法来检验消息的完整性。通过对称加密算法（DES）为数据进行加密，非对称加密（RSA）加密对称加密的密钥。   1. **申请CA证书：**   由CA颁发的数字证书一般都是需要收费的，但是我们可以自己生成一个SSL证书，并且配置HTTPS   1. **生成SSL证书：**   Jdk中自带生成证书的软件keytool;         1. **通过Spring框架简单编写一个http接口**   访问http://localhost:/8080/say    访问https://localhost:/8080/say会报错因为没有配置证书，所以不会接受https的请求     1. **配置Https** 2. 将生成的SSL证书，放到工程文件中 3. 配置tomcat下的https相关配置      1. 访问https://localhost:/8080/say   **会提示证书验证不安全，因为毕竟是自己生成的证书，肯定不会被浏览器信任。但是可以看到可以正常进行访问**    **查看证书信息（cyf）：**       1. **申请Let`s Encrypt证书：**   Let`s Encrypt是免费的证书颁发机构，主要的特色米娜非，自动颁发，开源等特性，所以对一些小网站可以快速升级为HTTPS。   1. 直接通过git clone下载 [Certbot](https://certbot.eff.org/" \o "Certbot) 2. 生成免费证书   通过命令生成证书：  ./certbot-auto certonly --webroot --agree-tos -v -t --email 邮箱地址 -w 网站根目录 -d 网站域名  因为域名和服务器已经过期，所以暂时没有申请成功但是可以看到申请的过程还是非常简单的。 | | | |
| 结论分析与体会：    通过学习和了解Https和CA证书的知识，实现了简单的申请证书，配置HTTPS访问的过程，了解了证书的含义和目的，也学习到了HTTPS的相关知识收益匪浅。 | | | |