|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 班级：信息安全 3班 | 学号：201978030321 | | 姓名：袁航 | | 第 5 周： |
| 实验环境类型：  Ubantu16.0.4 | | Linux版本：ubantu16.0.4 | | 内核版本：uname-a | |
| **1、实验任务：**  可信计算课程本实验使用TPM模拟器搭建的实验环境进行实验，模拟器为IBM推出的TPM2.0模拟器。软件栈采用Intel推出的TSS相关组件，同时可能还要安装Openssl相关库。参照资料或根据自己电脑系统的需求，下载相应版本的软件，在安装好的虚拟机上搭建可信计算模拟环境，为后续实验打好基础。  参考资料：[TPM模拟器和TPM2-TSS安装\_jianming21的博客-CSDN博客\_tpm2-tss](https://blog.csdn.net/jianming21/article/details/107942585?utm_medium=distribute.pc_aggpage_search_result.none-task-blog-2~aggregatepage~first_rank_ecpm_v1~rank_v31_ecpm-1-107942585.pc_agg_new_rank&utm_term=tpm%E6%A8%A1%E6%8B%9F%E5%99%A8&spm=1000.2123.3001.4430)  **2、实验流程：**  （要求：利用文字和截图描述自己的实验过程）  1.安装配置所需依赖  sudo apt install lcov pandoc autoconf-archive liburiparser-dev libdbus-1-dev libglib2.0-dev dbus-x11 libssl-dev \  autoconf automake libtool pkg-config gcc libcurl4-gnutls-dev libgcrypt20-dev libcmocka-dev uthash-dev    2.从官网下载TPM模拟器程序ibmtpm1332.tar.gz  wget https://jaist.dl.sourceforge.net/project/ibmswtpm2/ibmtpm1332.tar.gz    3.创建安装目录并将源码解压到对应目录  mkdir ibmtpm1332  cd ibmtpm1332/  tar zxvf ../ibmtpm1332.tar.gz    4.进入解压的目录，执行安装命令  cd src/  sudo make    5.将tpm服务器添加到Linux系统执行目录下  sudo cp tpm\_server /usr/local/bin/    6.在ubuntu中配置TPM服务(创建tpm.server.service文件和配置服务)：  sudo leafpad /lib/systemd/system/tpm-server.service  在文件中添加以下内容  [Unit]  Description=TPM2.0 Simulator Server Daemon  Before=tpm2-abrmd.service  [Service]  ExecStart=/usr/local/bin/tpm\_server  Restart=always  Environment=PATH=/usr/bin:/usr/local/bin  [Install]  WantedBy=multi-user.target    7.测试TPM配置情况，启动TPM服务  systemctl daemon-reload  systemctl start tpm-server.service  service tpm-server status    TPM2-tss安装   1. 添加tss用户   sudo useradd --system --user-group tss     1. 从官网下载tpm-tss-2.1.0.tar.gz   wget <https://github.com/tpm2-software/tpm2-tss/releases/download/2.1.0/tpm2-tss-2.1.0.tar.gz>  解压tpm-tss源码：  tar zxvf tpm2-tss-2.1.0.tar.gz  1  进入软件目录并进行配置查询。  为了测试各种TCTI、SAPI和ESAPI api等接口，通过定制配置构建来测试单个和整体接口情况，并利用check来构建出目标。  cd tpm2-tss-2.1.0/  ./configure --enable-unit --enable-integration  sudo make check    5.执行安装并配置动态链接  sudo make install  sudo ldconfig    Tpm2\_abrmd安装   1. 从官网下载tpm2\_abrmd安装包   Wget https://github.com/tpm2-software/tpm2-abrmd/releases/download/2.0.2/tpm2-abrmd-2.0.2.tar.gz  tar zxvf tpm2-abrmd-2.0.2.tar.gz  cd tpm2-abrmd-2.0.2/  sudo ldconfig   1. 设置安装配置   ./configure --with-dbuspolicydir=/etc/dbus-1/system.d --with-systemdsystemunitdir=/lib/systemd/system   1. 执行安装make   sudo make install  5.添加tpm2-abrmd进入系统服务  sudo cp /usr/local/share/dbus-1/system-services/com.intel.tss2.Tabrmd.service /usr/share/dbus-1/system-services/  6.重启DBUS  sudo pkill -HUP dbus-daemon  7.修改tpm2-abrmd.service服务配置  在启动服务时加载tss动态库并将服务启动到本地2321端口。  将“ExecStart=/usr/local/sbin/tpm2-abrmd”修改为“ExecStart=/usr/local/sbin/tpm2-abrmd --tcti=“libtss2-tcti-mssim.so.0:host=127.0.0.1,port=2321””  8.测试服务  systemctl daemon-reload  systemctl start tpm2-abrmd.service  service tpm2-abrmd status    Tpm2\_tools安装  1.从官方下载tpm2\_tools，由于版本需要与tp2-tss以及tpm2-abrmd，下载版本为tpm2-tools 3.x    2.进入目录中：    3.执行bootstarp、config和make    4.测试tpm2-tools工具连接abrmd服务是否正常    5.执行安装  **6.**打印pcr情况，查看输出是否正常    **3、实验总结（很重要）：**  （要求：对本次实验进行总结，发现不足，寻找后续改进的办法）  从这次实验中我学到了很多东西。第一，我在前期准备上的不足导致我自己花了许多时间在解决ubantu版本这一问题上。我也认识到自己有许多不足。第二，我认识到自己在Linux知识上有许多不足，这也提醒我平时要多多学习相关知识。 | | | | | |
|  | | | | | |