

SHANGHAI JIAO TONG UNIVERSITY

本科生毕业设计（论文）中期检查报告



论文题目： 针对ARM架构微控制器的故障注入攻击研究

学生姓名: 王屿轩

学生学号: 518030910138

专 业: 信息安全

指导教师: 谷大武

学院 (系): 电子信息与电气工程学院

|  |
| --- |
| 课题进展情况：  由于疫情影响，学校和宿舍相继封闭，我无法前往实验室进行实验。而且，由于疫情对于物流的影响，实验用的嵌入式设备暂时未能到货。所以这一阶段的进展主要集中在文献阅读上，尽可能为之后的实验进行准备。  在文献阅读的过程中，我熟悉了故障注入攻击的流程，对攻击的前期准备工作，攻击参数的尝试和选择，以及攻击可能的应用场景都有了深入的了解。同时我经过调研，发现电磁故障注入攻击和电压故障注入攻击有很多共同点，都通过硬件手段对芯片进行攻击，可以改变内部寄存器的值，或跳过指令，可以用于获取芯片调试访问权限，威胁加密硬件的安全等。相较于电磁故障注入攻击，电压故障注入攻击需要的硬件实验较少，达成的条件不如电磁故障注入攻击严苛。所以为了顺利完成毕业设计，我将毕业设计题目由“针对ARM架构程序控制流的电磁故障注入攻击”改为“针对ARM架构微控制器的故障注入攻击研究”。  很多文献都表明了故障注入攻击对于bootloader以及密码算法的威胁是切实存在的，而且通过实验证实了攻击的可行性。Rivire, Lionel等人实现了精确的且故障注入攻击，他们的实验设备利用信号发生器和放大器实现了5ps的抖动。他们实现了四条指令的跳过和重播，该漏洞可以用于对很多密码算法，如AES，进行差分故障分析。Van den Herrewegen等人演示了针对几种商用微控制器的嵌入式bootloader的实际攻击，并提供了一系列反模式，可以帮助指导安全实现的设计。Lennert Wouters等人的工作通过电压故障注入攻击，获得了完全的调试访问权限，并对AES加密硬件实施攻击，通过差分故障分析成功恢复密钥。  电压故障注入攻击通过改变芯片供电电压的方式进行攻击。可以瞬间将核心电压电源短接至地，使得输入电压短暂归零，称为撬杆电压故障。也可以使用外部电源来提供自己的电压，使得输入电压短暂升高。这样可以使得一些内部寄存器的值发生改变，进而让正在执行的代码进入攻击者想要的分支，实现攻击。  由于暂时无法进行硬件实验，我进行了一些软件方面的准备工作。我进行了串口通信相关的实验，编写了从嵌入式开发板提取ROM bootloader的python程序。同时我还对后续用到的一些工具，例如Ghidra逆向工具，unicorn模拟进行了初步的了解。 |

|  |
| --- |
| 课题研究已取得的阶段性成果：  实现了与嵌入式设备的串口通信，并通过串口通信获取芯片内部寄存器的值。该成果可以在后续的实验中有两个用途。一是可以通过UART与bootloader的串行接口进行通信，进而提取bootloader的二进制文件。二是读取内部寄存器的值可以用于验证攻击是否生效。  值得说明的是，该部分成果并非在最终的德州仪器的CC2640上进行，而是在STM32103上进行。二者操作比较接近，可以较为轻易地移植。  此外，编写了从嵌入式开发板提取ROM bootloader的python程序。该程序可以通过UART通讯的方式提取bootloader的二进制文件，用于逆向分析。 |

|  |
| --- |
| 存在的问题及解决思路：  最初我的毕业设计题目是“针对ARM架构程序控制流的电磁故障注入攻击”。该毕业设计题目大部分工作都需要实验室的硬件设备进行实验。由于疫情影响，学校封闭，我无法前往实验室进行实验，毕业设计难以推进。上海疫情形势仍然严峻，学校解封时间还不能确定，这给我的毕业设计带来了很大的困难。  在前期调研中我了解到，故障注入攻击不止有电磁故障注入攻击一种，还有电压故障注入攻击等形式。这些攻击都是针对嵌入式设备的物理攻击，都有较大的威胁。然而相较于电磁故障注入攻击，电压故障注入攻击需要的硬件实验相对较少。所以为了顺利完成毕业设计，我将毕业设计题目由“针对ARM架构程序控制流的电磁故障注入攻击”改为“针对ARM架构微控制器的故障注入攻击研究”。  目前疫情期间购买的实验用的板子不能配送，需要等待配送才能开始进行提取bootloader，逆向分析等工作。至于故障注入的实验还是需要去实验室完成。 |

|  |
| --- |
| 下一阶段的工作计划和研究内容：  在实验用的嵌入式开发板到货之前，继续进行调研，阅读文献和相关工作，为实验进行准备。  在实验用的嵌入式开发板到货后，提取和分析bootloader，对其进行逆向。通过UART与bootloader的串行接口进行通信。读取内存，包括bootloader本身的ROM。通过读取从地址0x10000000开始的数据来提取ROM。使用unicorn引擎对bootloader进行模拟，获得bootloader执行的操作和流程，确定攻击需要的执行路径，并初步确定故障注入的时机。  在可以去实验室之后，对硬件进行电压故障注入攻击实验。首先对攻击目标进行修改，移除连接到重置引脚的电容器和连接到DCOUPL引脚的去耦电容器。并在DCOUPL引脚上添加了一个10欧姆的分流电阻器和一个SMA连接器。SMA连接器可连接至芯片窃听器，用于故障注入和侧通道分析。接下来确定故障注入的时间和宽度，确定攻击参数。尝试通过攻击获得完全的调试访问权限。尝试使用JTAG调试器连接到目标，以验证故障是否成功。或者通过侧信道分析，观察电压或功率的变化，证明故障成功注入。此外，尝试对AES硬件进行故障注入攻击引入故障，并通过差分故障分析尝试恢复密钥。 |

|  |
| --- |
| 指导教师意见：  指导教师签名：  年 月 日 |
| 学院（系）意见：    审查结果： □ 同 意 □ 不 同 意  学院（系）负责人签名：  年 月 日 |