This is a trap!

校园一卡通系统

by 第六组

周京汉 2015011245 沈俊贤 2015011258 李睿燮2015080062

1

BACKGROUND

事情要从大秦历8102年说起

背景

重要性、必要性

M1卡

可读可写

安全

多功能

意义

不言而喻

重点、难点

如何形成一套完整的系统

子系统直接如何协作

如何开发一套用户友好的系统

如何保证用户的安全性

2

TECHNIQUE

孔乙己显出极高兴的样子，将两个指头的长指甲敲着柜台，点头说，“对呀对呀！十六个字节有六十四种加密方法，你知道么？”

整体架构

门禁

门禁实行联网/断网机制
断网时在本地判断规则
联网时额外检查学生信息

注册

注册中心要求全程联网
注册新卡
注销旧卡
延长卡的有效期限

零钱

零钱包要求全程联网
充值
消费
查询消费记录

我们的 逻辑 系统

pyserial

串口通信

http request

服务器与接口通信

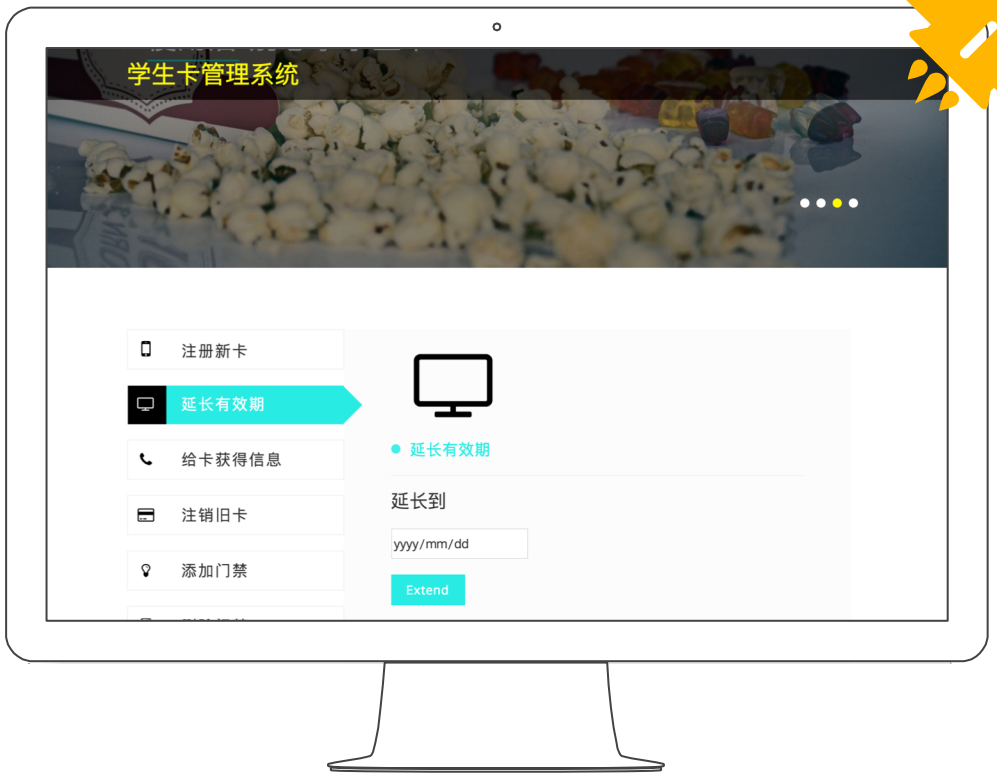
zerorpc

Electron与接口通信

electron 强大 而 轻巧

虽然npm炸了一万次

但是我们还是 接上了



Arduino
掌握 核心 科技

读写？

串口？

认证？

一个ino就搞定！

+

- 存储学生信息
- 注册中心同步
- 失效卡信息抓取

AES-128

——我们有AES-128，你有量子计算机吗？

——16位进16位出，只需要一个python module

3

IMPLEMENTATION

[数据删除]剑每出一把，我们的github上就多一个milestone

实验过程中遇到的难点

M1卡
压力 读取

卡一直放在读卡器上怎么办？

Arduino部分的硬件模块在每次loop循环的时候都会检测是否是新卡

卡连续短暂拿开放回怎么办？

这会导致arduino发送的“检测到新卡”和“检测卡移开”信号重叠，为此引入了延迟，强制这两个信号相距0.5s

卡在读/写一半的时候拿开怎么办？

两侧的串口会监测串口中发送的内容，当卡移开的时候arduino会向客户端发送关闭信号，两侧都停止工作 ，等待下一次检测到卡的活动

卡刚放上去就拿开怎么办？

和上一种情况并没有分别

门禁连续读卡怎么办？

门禁的特点要求能够连续读卡，为此在遇到上述读卡异常的时候，我们处理的方式和注册机/零钱包有所不同

M1卡存取 中文

- 不在 0-128的 范围内，没有办法简单通过ord和chr转换
- utf-8中一个汉字占三个字节，对于字节对齐不友好
- 由于格式要求，只能操作单一字节

经过调研，我们发现unicode是通过\uxxxx的形式存储，我们将其从中间截取，分别存入不同的位置。

zerorpc 交互

- 不能直接在electron添加相关依赖
- 和submit发生冲突
- 经常发生莫名丢包问题

可移植性

M1卡技术细节

- 监视串口
- 解析命令
- 执行读写、认证

客户端技术细节

- 三个模块：注册中心、零钱包、门禁
- 被动监视串口
- 命令的封装

服务器技术细节

- 创建与注册
- 数据库存储
  - 基本信息: 学号，姓名，院系，性别，类别，有效日期
  - 钱包信息: 余额
- 访问对应url发送请求

安全技术细节

- M1卡的安全机制

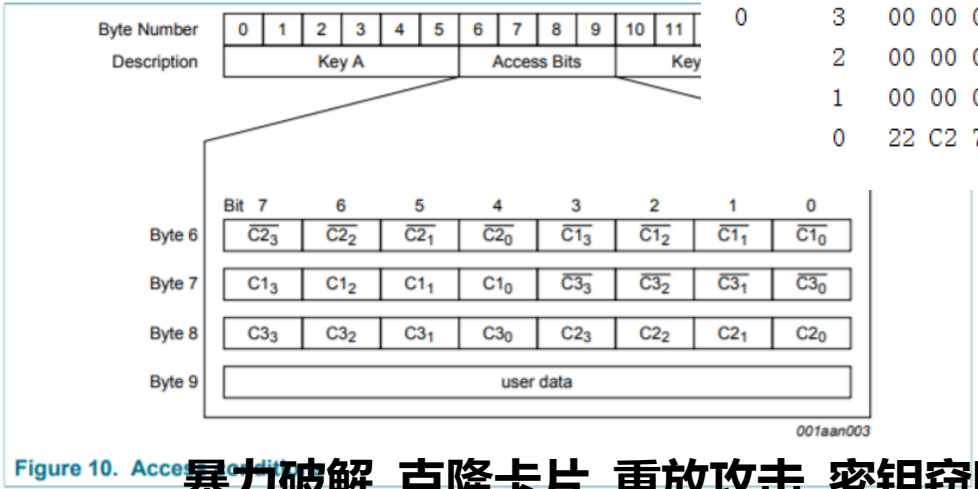


Figure 10. Acces

urrent data in sector:

0	3	00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	[0 0 1]
	2	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	1	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[0 0 0]
	0	22	C2	73	0D	9E	08	04	00	62	63	64	65	66	67	68	69	[0 0 0]

暴力破解, 克隆卡片, 重放攻击, 密钥窃听, 验证漏洞,

安全技术细节

- 断网盗刷
  - 未存储在卡中的信息（从根本上杜绝 ！）
  - 信息差
- 加密M1卡
- 克隆卡

4

RESULT

我们的结果就和悲嘆の怠惰一样显然

最终 结果

- 在shell模式下，能够流畅且鲁棒地完成：制作新卡、注销旧卡、学生注册（即更新卡的有效期）、门禁控制、零钱包（小额的储值与消费）
- 完成了后端对学生信息的存储
- 基本完成了前端

展示!

I am Huangpei

这个系统如此安全，以至于我把我的个人信息存在这里

5

SUMMARY

Congratulation, This is a trap!

实验 感想

- 各个部分的实现都不难，但是形成一套流畅的系统难
- M1卡安全不容忽视

Thanks!

Any questions?