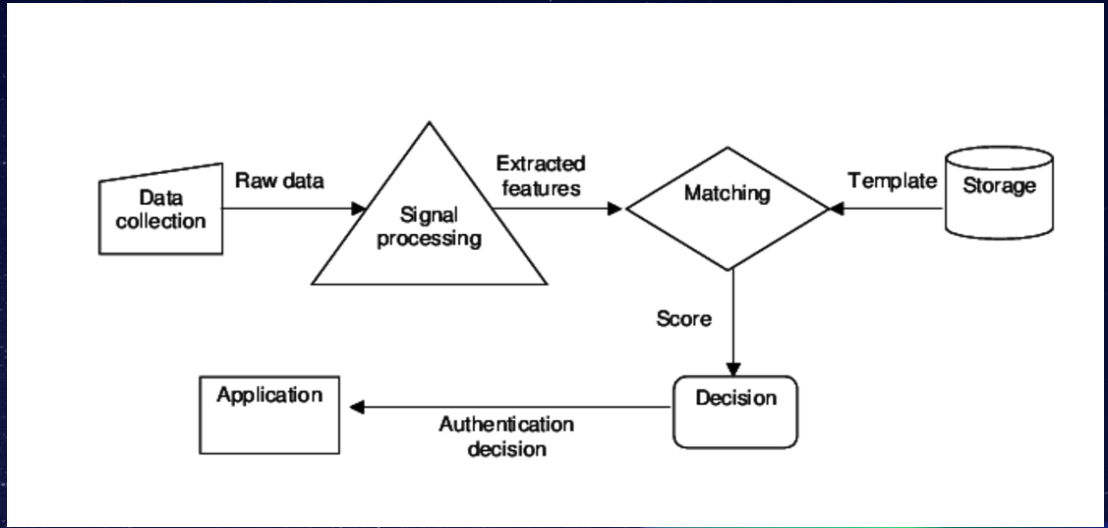
人脸识别门禁漏洞挖掘详解

王海兵 | 极棒实验室(GeekPwn Lab)总监

FIT · FREEBUF

生物识别系统通用模型



门禁系统逻辑图

HACK DEMO

分析过程

1. 拆解，取固件，逆向
2. 修改固件，回刷
3. 登入系统，debug
4. 抓取网络报文，分析结构
5. Fuzz

漏洞

1. 信息泄露（型号与序列号）
2. 逻辑错误（猜对8位密码中的1位，可获得网络响应。）

HACK DEMO

攻击

1. 抓取正常管理通讯并分析内容
2. 模拟管理端对门禁的管理，操作人脸信息的修改

HACK DEMO