



2016 中国互联网安全大会  
China Internet Security Conference

协同联动 共建安全+命运共同体

# 移动终端交互行为分析的身份主动认证与安全感知

**沈超**

西安交通大学副教授  
智能网络与网络安全教育部重点实验



中国互联网安全大会



360互联网安全中心

身份安全、身份认证？  
不就是密码、指纹吗？

# 身份安全得到极大关注



中国互联网安全大会



360互联网安全中心

各种智能计算终端（传统PC、云终端、移动终端等）已进入到各行各业，能够存储并访问越来越多的安全和隐私信息，**内部人员攻击、密码泄漏、隐私侵犯、身份盗用**等造成的**国家及各级企业隐密信息泄漏及财产损失**已引起各国政府和企业的**极大关注**。



内部人员攻击



密码泄漏



身份安全



隐私侵犯



身份盗用

# 棱镜门等事件的频发带来的挑战



中国互联网安全大会



360互联网安全中心

- “棱镜”、“颞颥”事件再次说明由于**终端安全信息泄露**给国家造成的重大损失
- 需要对**终端操作行为进行持续监控**，并对**操作者身份进行认知**
- 需要**主动式的身份安全分析方法**
  
- **DARPA在2013年12月支持4年期的交互行为测定&主动认证计划**
  - 在用户使用计算终端的过程中进行**主动式行为监控和身份认知分析**
  - 强调**不需要用户的配合**



# DARPA Active Authentication - Continued

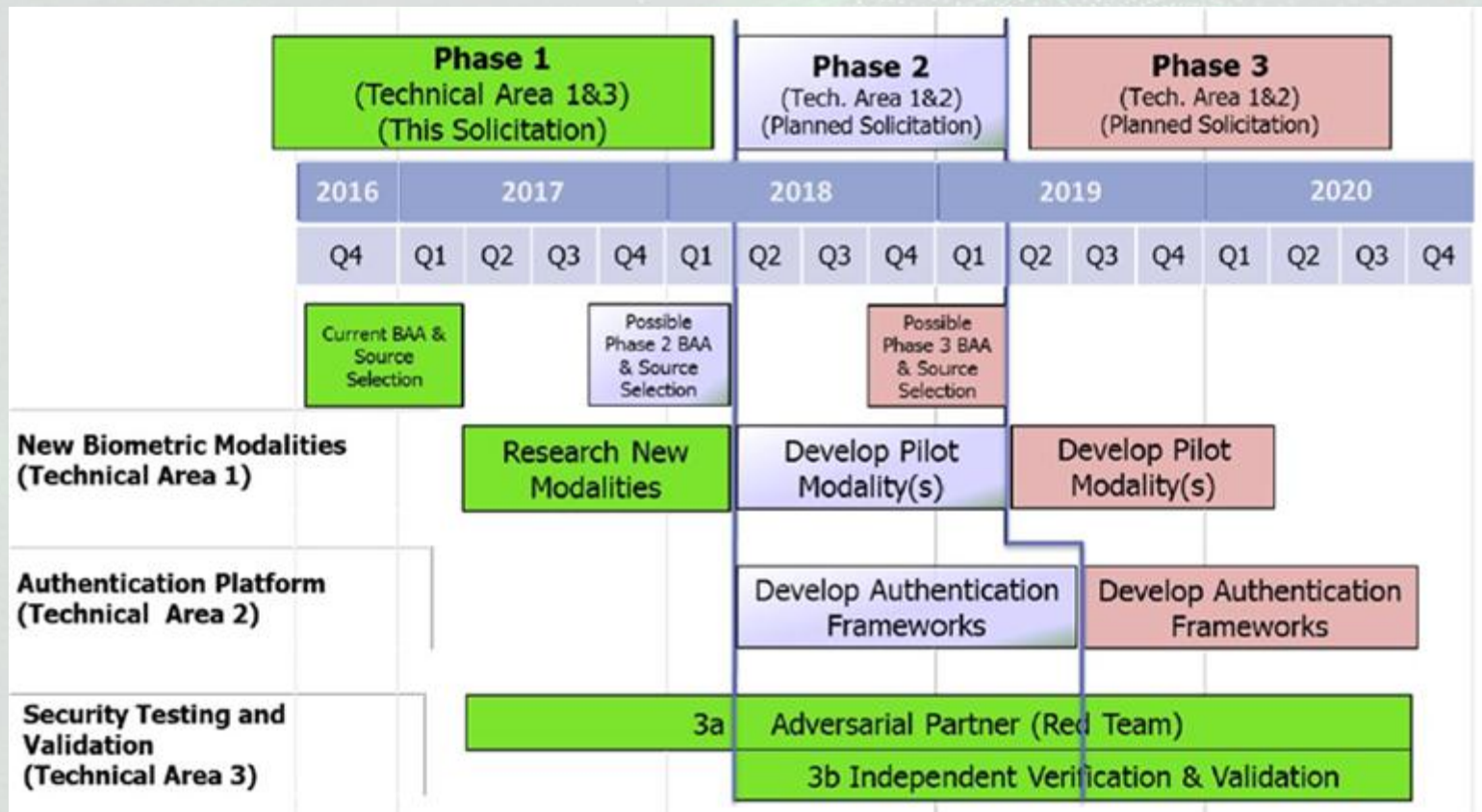


中国互联网安全大会



360互联网安全中心

- 新的动机：在个人强身份认证信息丢失或被复制（2013年底德国国防部长指纹泄漏）的情况下，能够通过行为分析的方法进行身份的动态识别。
- “斯诺登事件” -> 第二个4年期研究（从2016开始）





中国互联网安全大会



360互联网安全中心

终端交互行为是什么？  
进行**主动式**身份认证和监控？

## □ 生物特征

✓ 生理特征（虹膜、指纹等）

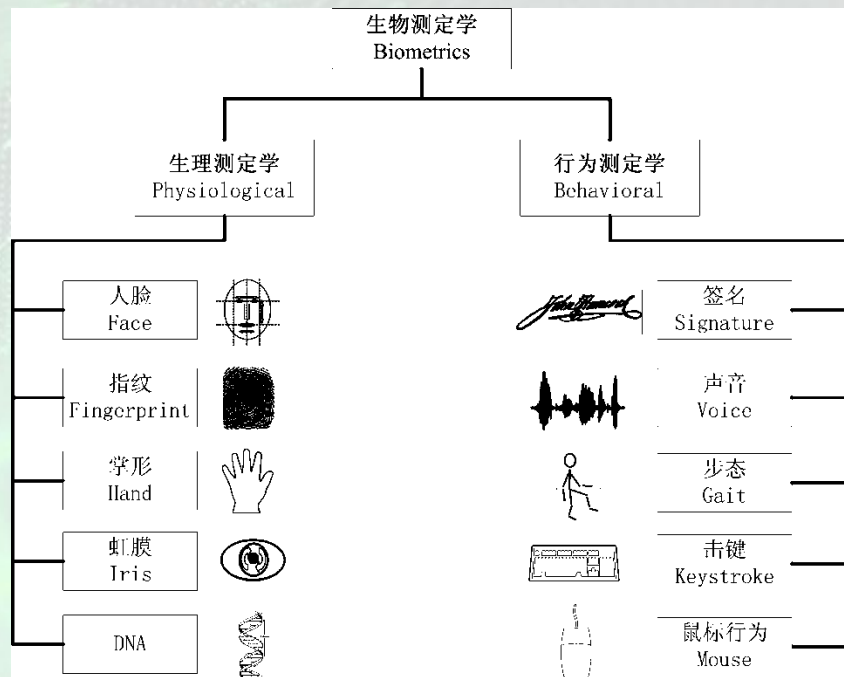
✓ 行为特征（步态等）

✓ 终端交互行为：

- 鼠标 – 移动模式，曲线特征
- 键盘 – 敲击节奏
- 触摸屏&触摸板 – 触摸模式
- 穿戴传感器 – 交互模式
- 软生物特征 – 衣服、发型、肤色
- 可视交互的人脸特征

### 优点：

- ❖ 终端交互行为直接从人机交互过程中提取
- ❖ 无需记忆或携带，不需要额外的硬件
- ❖ 可无缝融入用户与智能计算终端的交互过程



# 终端交互行为主动身份认证和认知



中国互联网络安全大会



360互联网安全中心

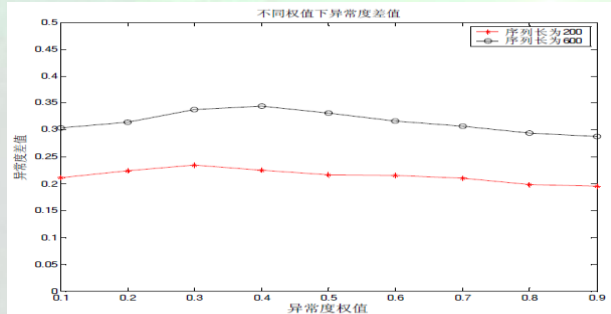
- 终端交互行为安全监控和身份认知
  - ✓ 静默式捕获终端用户操作人机交互设备时所产生的交互行为数据
  - ✓ 结构化描述交互行为并提取稳定的行为表征特征
  - ✓ 监控操作者的身份安全（监控用户的交互行为、持续分析用户的真实身份）
  - ✓ 认知用户的物理身份信息（操作者的性别、年龄、左右手使用习惯等信息）

## 终端交互数据

	subject	sessionIndex	rep	H.period	DD.period.t	UD.period.t	
1	s002	1	1	0.1491	0.3979	0.2488	0.1069
2	s002	1	2	0.1111	0.3451	0.2340	0.0694
3	s002	1	3	0.1328	0.2072	0.0744	0.0731
4	s002	1	4	0.1291	0.2515	0.1224	0.1059
5	s002	1	5	0.1249	0.2317	0.1068	0.0895
6	s002	1	6	0.1394	0.2343	0.0949	0.0813
7	s002	1	7	0.1064	0.2069	0.1005	0.0866
8	s002	1	8	0.0929	0.1810	0.0881	0.0818
9	s002	1	9	0.0966	0.1797	0.0831	0.0771
10	s002	1	10	0.1093	0.1807	0.0714	0.0731
11	s002	1	11	0.0887	0.1660	0.0773	0.0876
12	s002	1	12	0.0911	0.1525	0.0614	0.0824
13	s002	1	13	0.1114	0.1620	0.0506	0.0900
14	s002	1	14	0.0903	0.1871	0.0968	0.0805
15	s002	1	15	0.1169	0.2562	0.1393	0.0739
16	s002	1	16	0.1270	0.1839	0.0569	0.0911
17	s002	1	17	0.1016	0.1799	0.0783	0.0792
18	s002	1	18	0.1056	0.1755	0.0699	0.0781

## 安全监控

2013年5月18日 13:45: 当前为第16次, 当前主动认证的用户身份可靠性为77.42%  
2013年5月18日 13:50: 当前为第17次, 当前主动认证的用户身份可靠性为82.43%  
2013年5月18日 13:55: 当前为第18次, 当前主动认证的用户身份可靠性为75.32%  
2013年5月18日 13:60: 当前为第19次, 当前主动认证的用户身份可靠性为78.97%  
2013年5月18日 14:05: 当前为第20次, 当前主动认证的用户身份可靠性为88.24%  
2013年5月18日 13:10: 当前为第21次, 当前主动认证的用户身份可靠性为89.45%  
2013年5月18日 13:15: 当前为第22次, 当前主动认证的用户身份可靠性为62.42%  
2013年5月18日 13:20: 当前为第23次, 当前主动认证的用户身份可靠性为76.42%



## 身份认知分析

操作者的性别为：男

年龄为：20-30

左右手使用习惯：右手

身高：约为170~180

.....



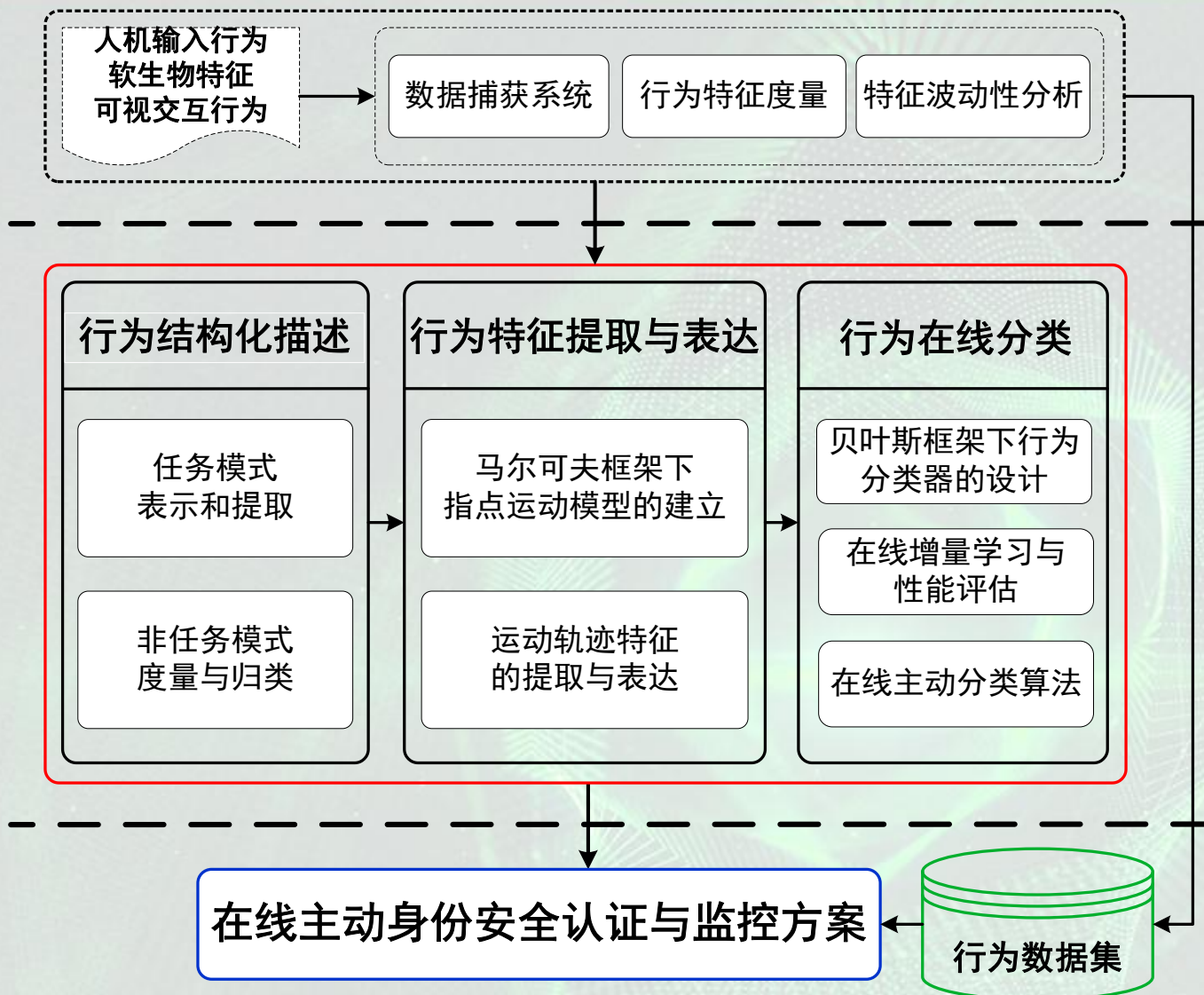
# 技术框架



中国互联网安全大会



360互联网安全中心





中国互联网安全大会



360互联网安全中心

在PC端、网页端、移动端  
上都能用吗？

# 技术方案



中国互联网安全大会



360互联网安全中心

## 智能终端交互行为监控和身份认知

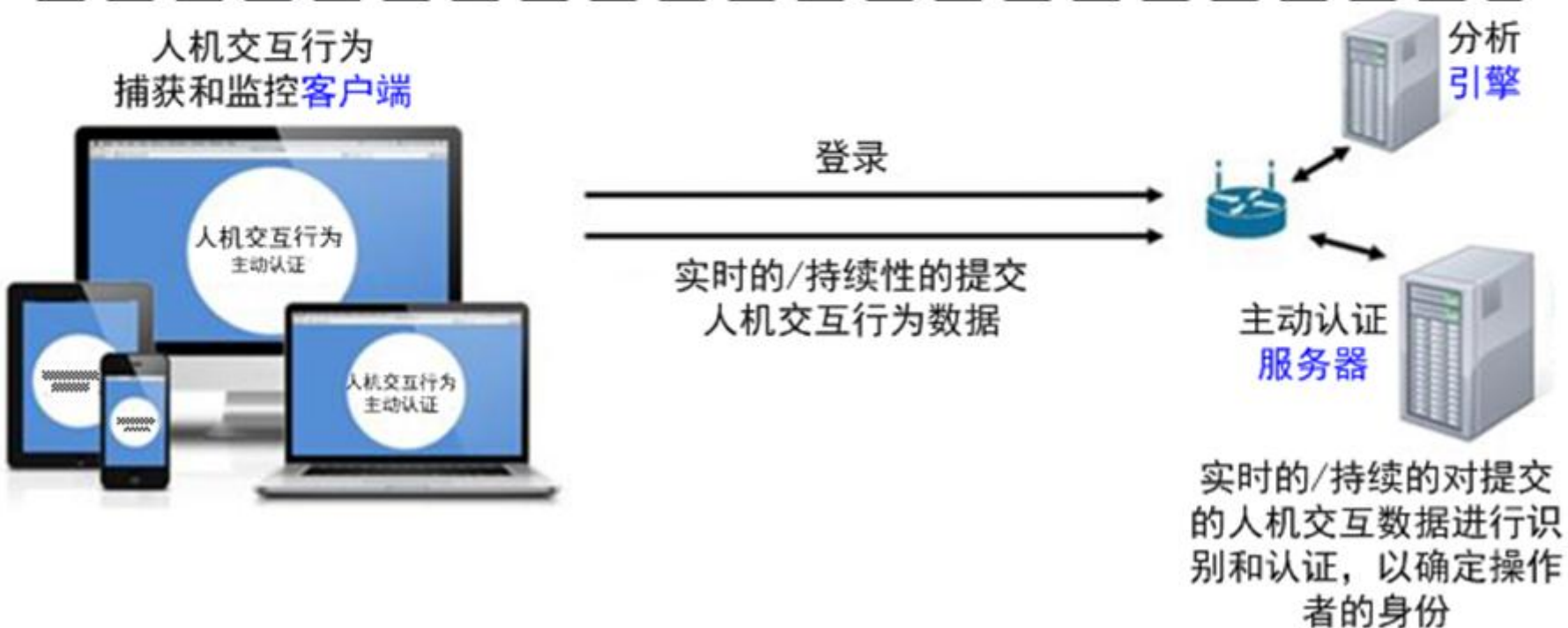
传统终端

网页终端

移动终端

Services

API



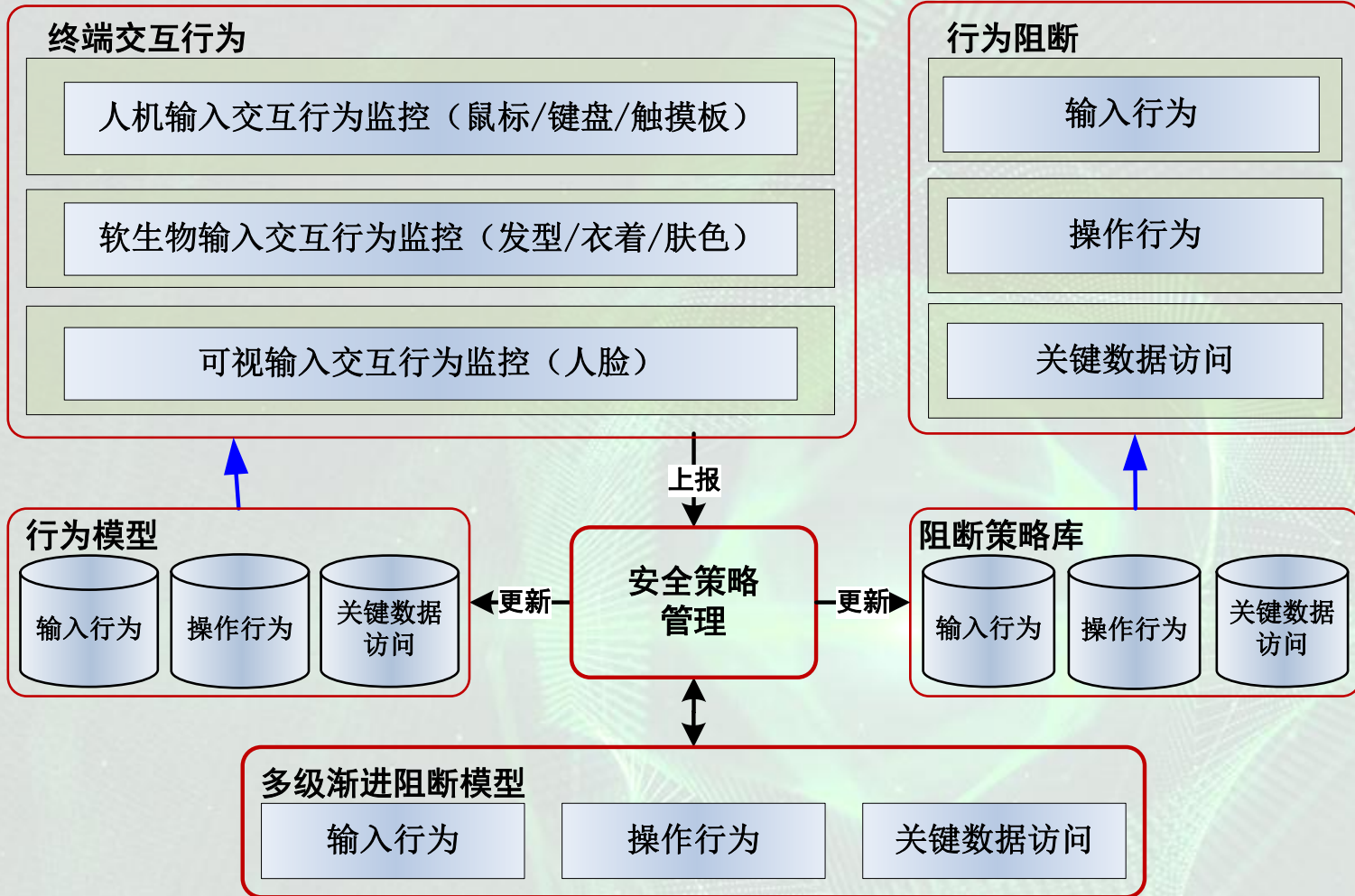
# 逻辑方案



中国互联网安全大会

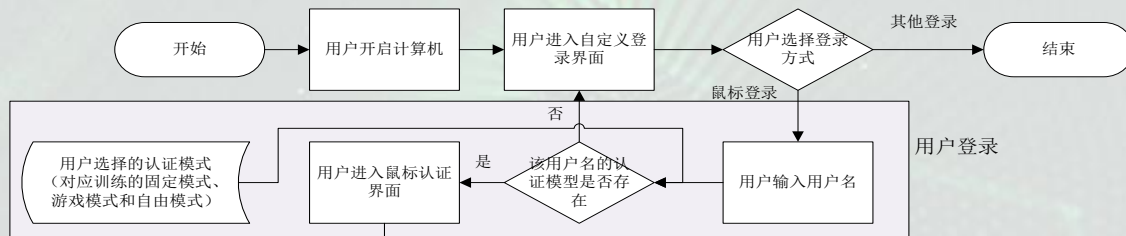


360互联网安全中心



# 传统终端交互行为的身份认证

## 系统设计



## 系统实现



# 传统终端交互行为的身份监控

## 系统设计



## 系统实现

基于鼠标动力学的身份认证及监控! 通过下面的操作可以进行鼠标行为训练集监控 未启用鼠标认证

鼠标训练

固定状态  游戏状态  自由状态

鼠标监控

全局监控  Office监控  聊天监控

状态信息

固定状态 未创建

请尽快创建!

游戏状态 已创建

创建时间 2010-4-29 12:53:01

自由状态 已更新

更新时间 2010-4-28 12:33:22

未开启监控

日志信息

类型	日期时间	用户名	结果

鼠标行为

击键行为

身份认证

数据采集

监控结果日志

阻断用户操作

结束

# 传统终端交互行为认证与监控



中国互联网安全大会



360互联网安全中心

### 终端交互行为监控

实时监测 | 行为监控 | 监测阻断 | 系统设置

## BehaviorCog

行为认知&终端保护

登陆用户：张赫 | 身份合法度：95.3415 | 监控结果：合法

#### 输入交互行为

- 监测状态：已关闭
- 监测结果：正常
- 监测模板：已建立
- 日志记录：已开启

#### 可视交互行为

- 监测状态：已开启
- 监测结果：正常
- 监测模板：已建立
- 日志记录：已开启

#### 软生物特征交互行为

- 监测状态：已开启
- 监测结果：正常
- 监测模板：已生成
- 日志记录：已开启

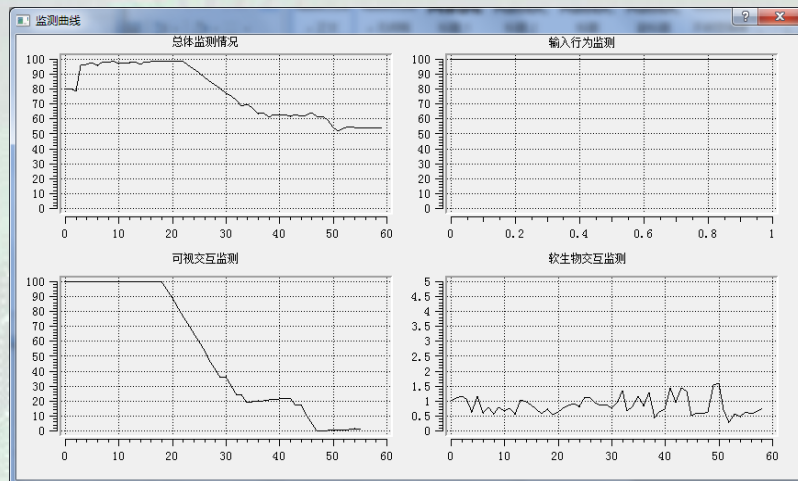
#### 监测曲线

#### 监测日志

5日20:55:43	终端交互监测	正常	得分为：95.4252
5日20:55:46	终端交互监测	正常	得分为：95.3396
5日20:55:49	终端交互监测	正常	得分为：95.4765
5日20:55:52	终端交互监测	正常	得分为：95.3958
5日20:55:55	终端交互监测	正常	得分为：95.3735
5日20:55:58	终端交互监测	正常	得分为：95.3466
5日20:56:1	终端交互监测	正常	得分为：95.3135
5日20:56:4	终端交互监测	正常	得分为：95.465
5日20:56:7	终端交互监测	正常	得分为：95.4218
5日20:56:10	终端交互监测	正常	得分为：95.3415

版本号：v2.1 | BehaviorCog已保护您 10 天 | 已连接到服务器：127.0.0.1 : 4000

## 客户端



## 分析引擎

### MainWindow

控制台 | 当前连接用户

```
得分为：0.766438#7,张赫,,0.0.766438#9,张赫,,0,9月15日20:54:35 终端交互监测 异常 得分为：50.7671#
收到信息127.0.0.1 : 8,张赫,,0,50.7671#
收到信息127.0.0.1 : 3,张赫,,0,9月15日20:54:38 可视交互监测 异常 得分为：0.050143#
收到信息127.0.0.1 : 6,张赫,,0,0.050143#4,张赫,,0,9月15日20:54:38 软生物交互监测 正常 得分为：1.12052#7,张赫,,0,1.12052#
收到信息127.0.0.1 : 6,张赫,,0,0.050143#4,张赫,,0,9月15日20:54:38 软生物交互监测 正常 得分为：1.12052#7,张赫,,0,1.12052#
收到信息127.0.0.1 : 6,张赫,,0,0.050143#4,张赫,,0,9月15日20:54:38 软生物交互监测 正常 得分为：1.12052#7,张赫,,0,1.12052#
收到信息127.0.0.1 : 9,张赫,,0,9月15日20:54:38 终端交互监测 异常 得分为：50.0815#8,张赫,,0,50.0815#
收到信息127.0.0.1 : 9,张赫,,0,9月15日20:54:38 终端交互监测 异常 得分为：50.0815#8,张赫,,0,50.0815#
```

端口 4000 | 服务器已开启

## 服务器端

# 加强版-传统终端交互行为的安全认证



中国互联网安全大会



360互联网安全中心

DBAS-桌面安全认证系统

行为监控 安全阻断 系统设置 帮助

## DBAS 桌面行为认证

基本状态 输入行为 文件行为 注册表行为 网络行为 进程行为

### 输入行为状态

<b>鼠标行为</b>	<b>键盘行为</b>	<b>输入行为认证登陆:</b>
鼠标监控 <input type="checkbox"/> 开启	键盘监控 <input type="checkbox"/> 开启	已关闭 <input type="checkbox"/> 开启
鼠标阻断 无	键盘阻断 无	<a href="#">查看开放式数据集</a>

### 资源访问行为状态

<b>文件访问状态:</b>	<b>注册表访问状态:</b>	<b>网络访问状态:</b>
文件监控 已关闭 <input type="checkbox"/> 开启	注册表监控 已关闭 <input type="checkbox"/> 开启	网络监控 已关闭 <input type="checkbox"/> 开启
监控磁盘 C:\	注册表阻断 已关闭 <input type="checkbox"/> 开启	监控网卡
文件阻断 已关闭 <input type="checkbox"/> 开启		监控结果

### 进程访问状态

进程监控 已关闭 <input type="checkbox"/> 开启	当前监控进程 <u>csrss.exe</u>
进程阻断 已关闭 <input type="checkbox"/> 开启	阻断策略 中
	<a href="#">详细信息</a>



# 传统终端双因素强化认证



中国互联网安全大会



360互联网安全中心

MainWindow

BehaviorCog.  
行为认知&终端防护v1.2

账号

密码

设置  注册新用户

客户端

MainWindow

请至少输入密码5次  
增大模板数量可提高效果

请输入密码

已输入密码 1 次

20%

注册模块

MainWindow

BehaviorCog.  
行为认知&终端防护v1.2

服务器

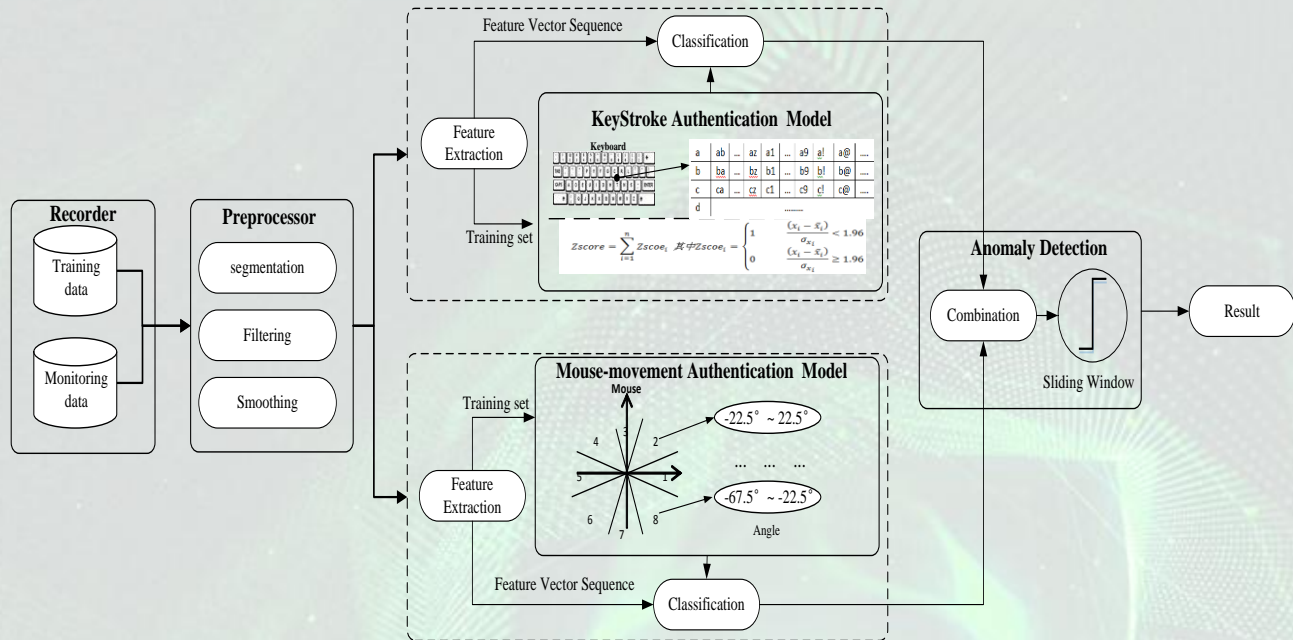
端口

服务器端

认证精度在200人的测试集上高达99.99% !

# Web交互行为的身份确认与追踪

## 系统设计



## 系统实现



# Web交互行为认证与监控（银行）

My JSP 'include.jsp' start... x My JSP 'include.jsp' start... x  
202.117.61.37:8080/mouseservlet/4.jsp  
Apps Gligoo 学术搜索\_谷... Microsoft Academic... Coursera Mining of Massive D... NS Next Scientist - Digit... Other bookmarks  
关闭窗口

ICBC 中国工商银行 金融专家 个人网上银行

欢迎页面 我的账户 定期存款 通知存款 公益捐款 转账汇款 私人银行 网上贷款 银医服务  
工行理财 网上基金 账户商品 账户外汇 网上贵金属 网上债券 结售汇 银证业务 网上期货  
网上预约 缴费站 信用卡服务 网上汇市 工银e支付 工银信使 电子银行注册 银行卡服务 安全中心

转账

收款人姓名:   
收款人身份证号:   
收款人账号:   
转账金额:   
留言:   
密码:   
确定

转帐页面的认证

关闭窗口

ICBC 中国工商银行 金融专家 个人网上银行

欢迎页面 我的账户 定期存款 通知存款 公益捐款 转账汇款 私人银行 网上贷款 银医服务  
工行理财 网上基金 账户商品 账户外汇 网上贵金属 网上债券 结售汇 银证业务 网上期货  
网上预约 缴费站 信用卡服务 网上汇市 工银e支付 工银信使 电子银行注册 银行卡服务 安全中心

缴费

缴费项目:  水费  电费  天然气费  手机费  
单位名称:   
手机号码:   
缴费金额:   
密码:   
确定

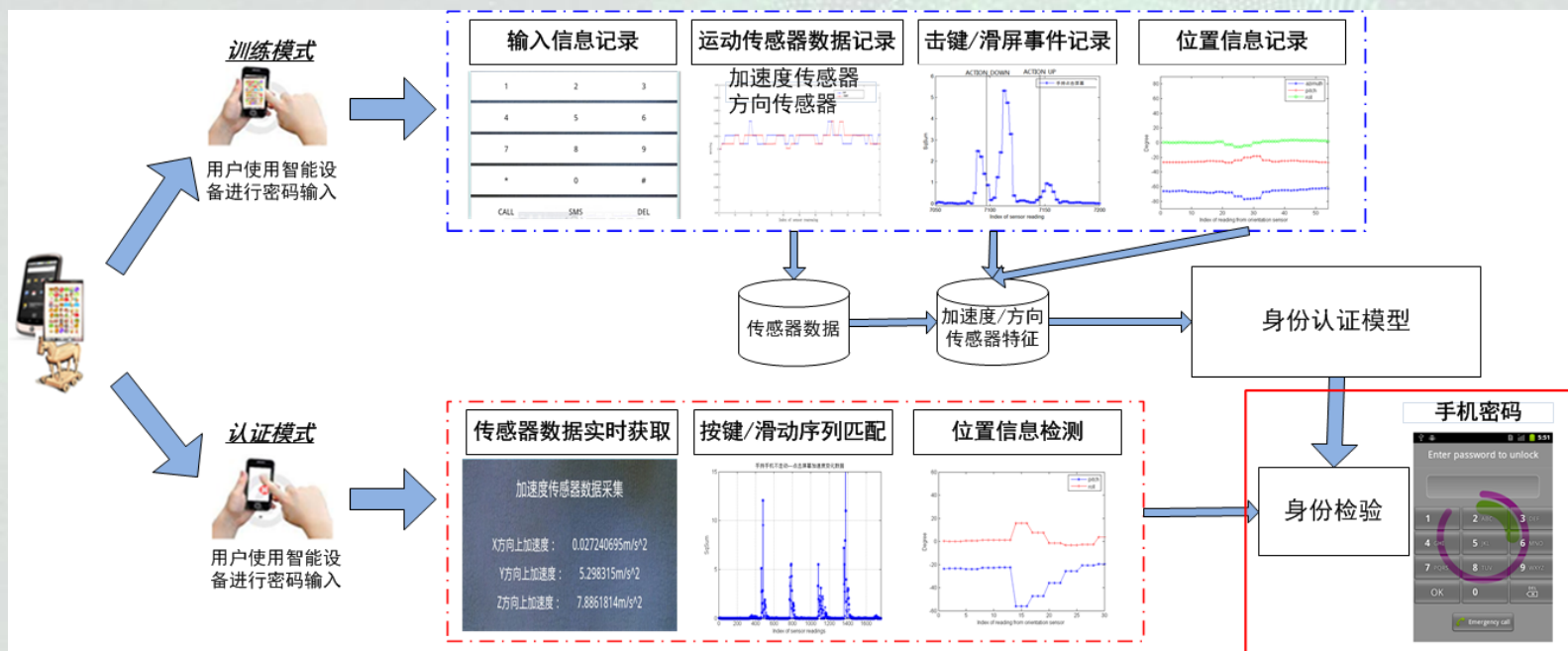
缴费页面的认证

# 移动端交互行为/传感器的双因素认证

## 关键技术

- 输入序列和运动传感器数据的融合技术
- 传感器的结构化表示技术 & 运动传感器的特征分析与提取
- 在线学习、认证和更新技术

## 研究框架



# 移动端双因素强化认证（手机&平板）



# 移动端交互行为/传感器的主动监控



中国互联网安全大会

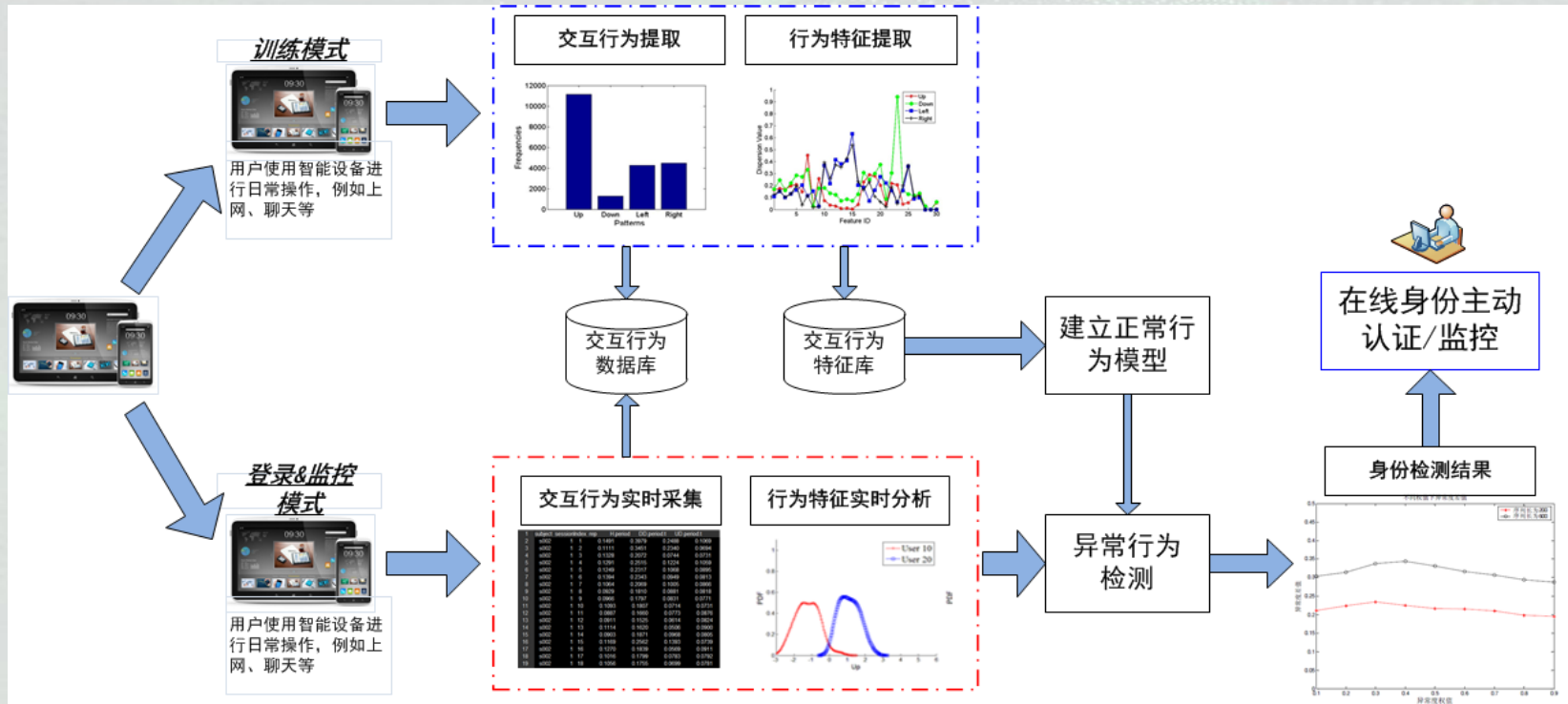


360互联网安全中心

## ■ 关键技术

- 异构数据的结构化表示和融合技术 & 多源数据的融合建模技术
- 交互行为的半监督增量学习技术 & 在线主动认证技术

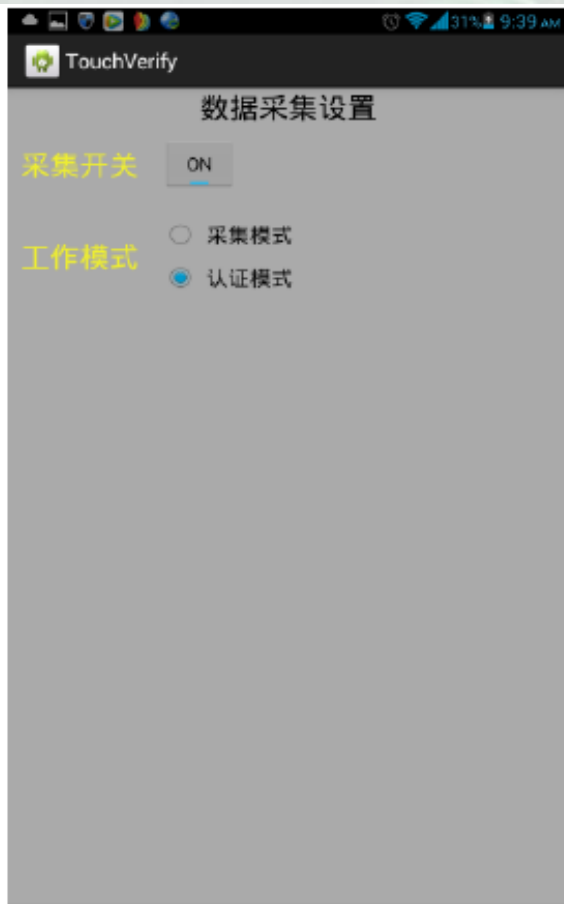
## ■ 研究框架



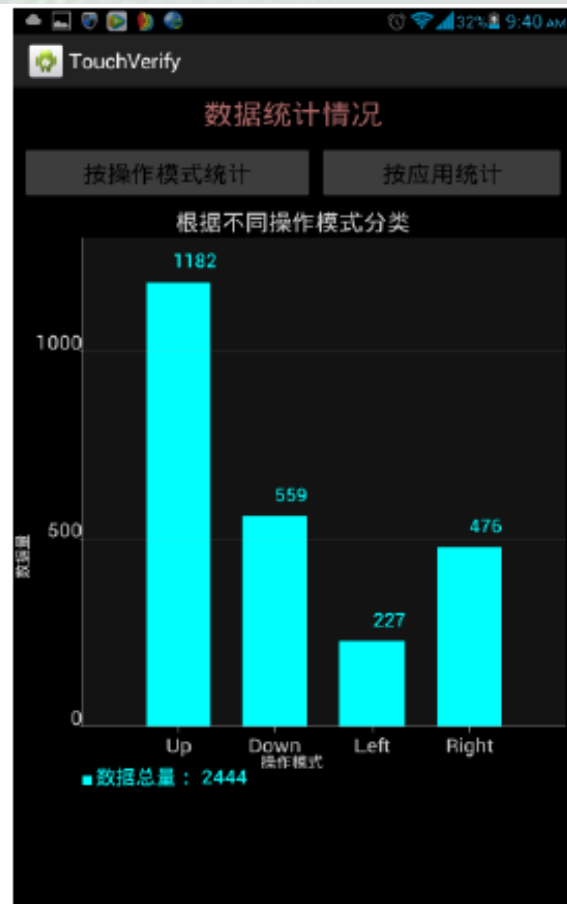
# 移动端交互行为/传感器的主动监控



(a) 主界面



(b) 数据采集界面



(c) 数据统计界面

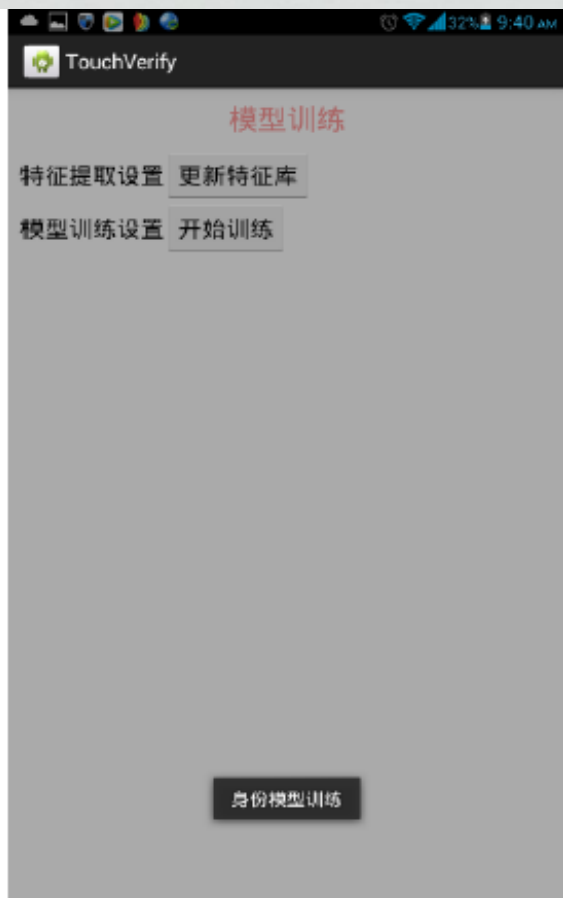
# 移动端交互行为/传感器的主动监控



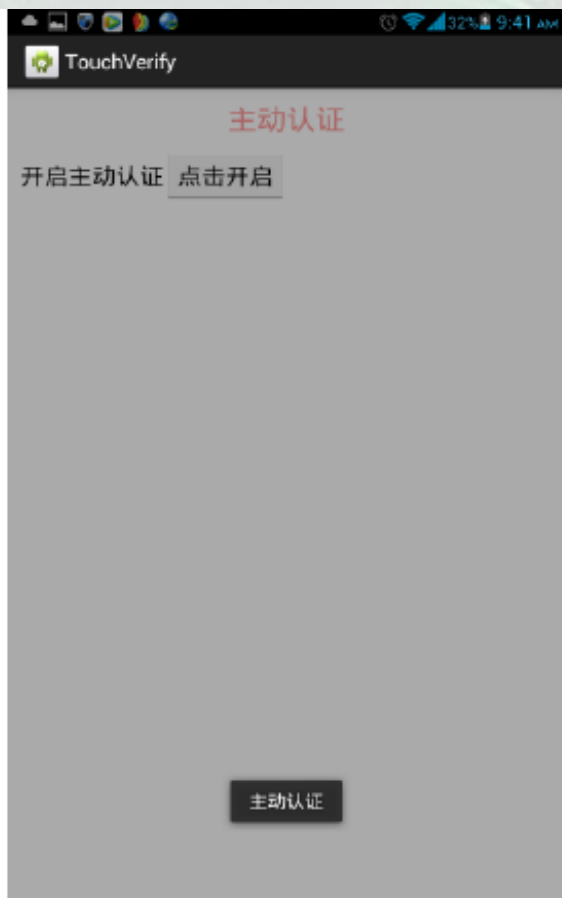
中国互联网安全大会



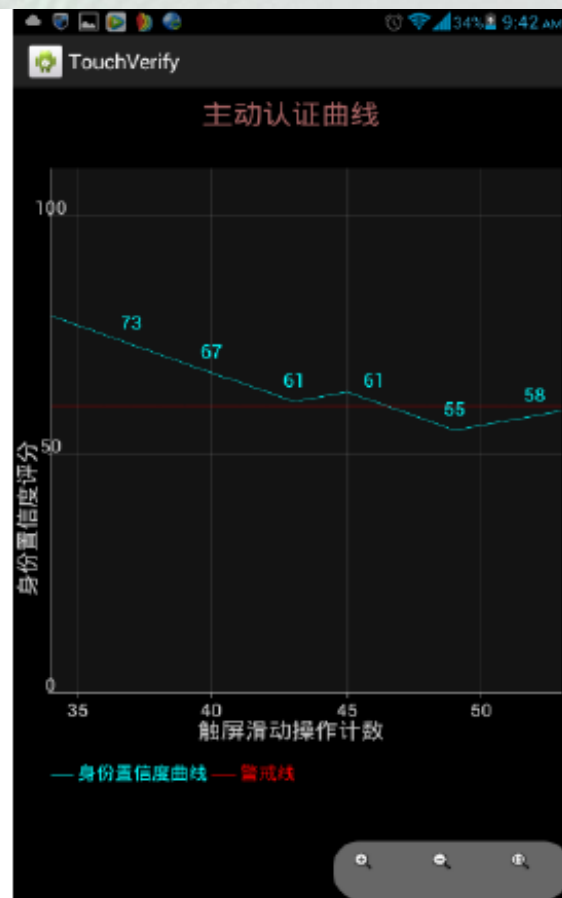
360互联网安全中心



(d) 模型训练界面



(e) 主动认证界面



(f) 主动认证曲线界面

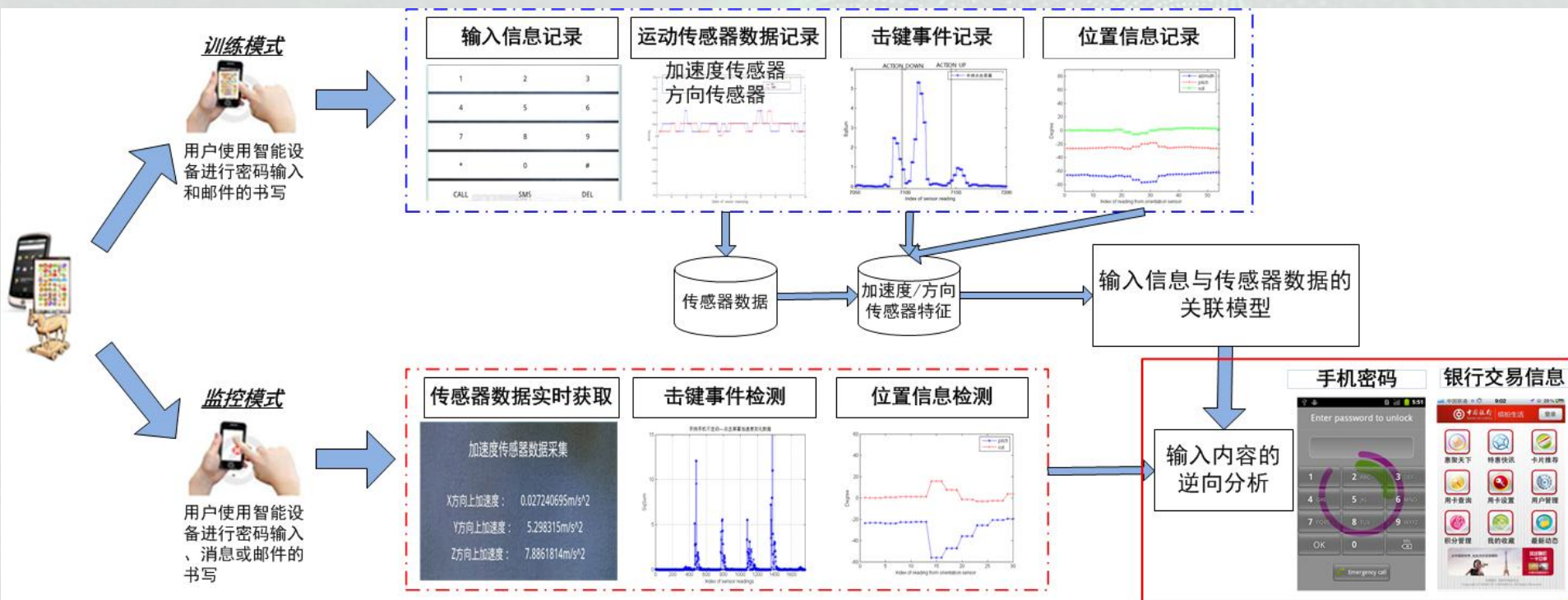


# 移动端交互输入行为的逆向分析

## ■ 关键技术

- 基于加速度传感器的输入行为检测技术 & 基于方向传感器的位置感知技术
- 多源传感器数据的融合表示技术 & 智能终端输入行为的逆向推理技术

## ■ 研究框架



# 谢 谢



中国互联网安全大会



360互联网安全中心