AI vs AI: Uncover the Billions of Black Market in e-Commerce

Bin Zhao, Ph.D.   Jin Yang, Ph.D.

Security Architect, JD Silicon Valley R&D Center

Outline

- Intro of JD
- Black market in e-Commerce
- AI-based defense system
- Deployment and Evaluation
- AI security and future

JD.COM Introduction

700 Million

June Sales Event **Items** Sold

Massive Scale

301.8M

Active customer accounts

150K

Active third-party vendors on JD platform

160K

Full-time employees

1.59B

Full-time orders fulfilled in 2016

Redefining Retail Through Technology

- A+B+C
- AI
- Big Data
- Cloud Computing

How large is the black market in e-Commerce?

- 51.8% of the network traffic are bot traffic
- 28.9% of them are malicious bot traffic
- Billions of dollars lost for companies
- Many cases: DIDI, Uber, even Apple iOS has been targets in this black market
- E-Commerce companies have been largely targeted
  - Large promotions
  - Many coupons
  - Flash sales

Overview of This Black Market

- Traditionally, the black market full of manual labor and low technology.
- Now it is a complete industrial chain with AI driven technology and automated tools.
- Greatly undermines the reputation of e-Commerce companies
- Impact normal customers' shopping behaviors
- A complete industrial chain consists of upstream, midstream and downstream.

Upstream of the Black Market

- Verification code/image platform
- Social Engineering Data
- Automated software
- Proxy tools

- Provides raw materials for producing accounts and identification information.
- Platform doing verification on code, image, voice, text message, question solving, etc., ranging from a couple of cents to $2, depending on whether or not real-name authentication is required.

Midstream of the Black Market

- Provides various accounts related services and exchanging platforms, such as Instant Messaging (IM) groups or online forums.
- Fake accounts registration
- Accounts stealing
- Accounts washing
- Information exchange platform
- Trading platform

Downstream of the Black Market

- Gain profits and costs losses to normal users and e-Commerce companies.
- Theft
- Fraudulence
- Blackmailing
- Click farming
- Scalper

Fraudulent Behaviors

- Bulk Registration
- Ranking boost via fake transactions
- Scalping orders placing
- Fake reviews
- Account trading
- Etc.

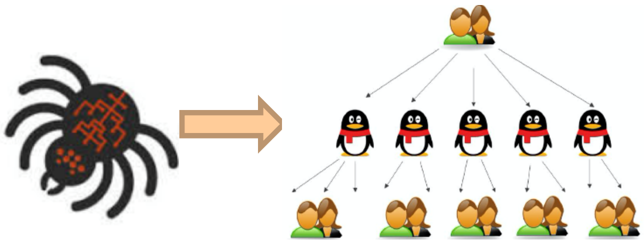
AI Security Overview

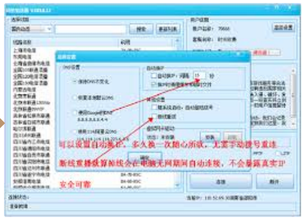
- AI is used throughout security analytics at JD
  - Different to traditional security : account security
  - Target special activities of special group of people
- It is the only way for us to operate efficiently at scale
- Arms race between the attackers and defense
  - Combination of non-traditional security forces:
  - Business analysis, linguist, AI tech, computer system
- AI security
  - From understand tech to understand human
  - From understand one group of people to understand another group of people

Anti Scalpers

- ❑ Scalping is a common threat to E-Commerce Platforms in China
  - ❑ Huge promotions
  - ❑ Alibaba, VIP, Suning, etc
  - ❑ User experience
- ❑ Monitoring Scalper activities and notify their activities in advance
- ❑ **New monitoring system is a strong plus to the current rule-based system**
  - ❑ **Accuracy of the information**
  - ❑ **New threat info acquisition never discovered before**

What do Scalpers do ?

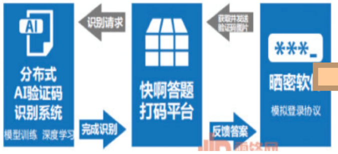




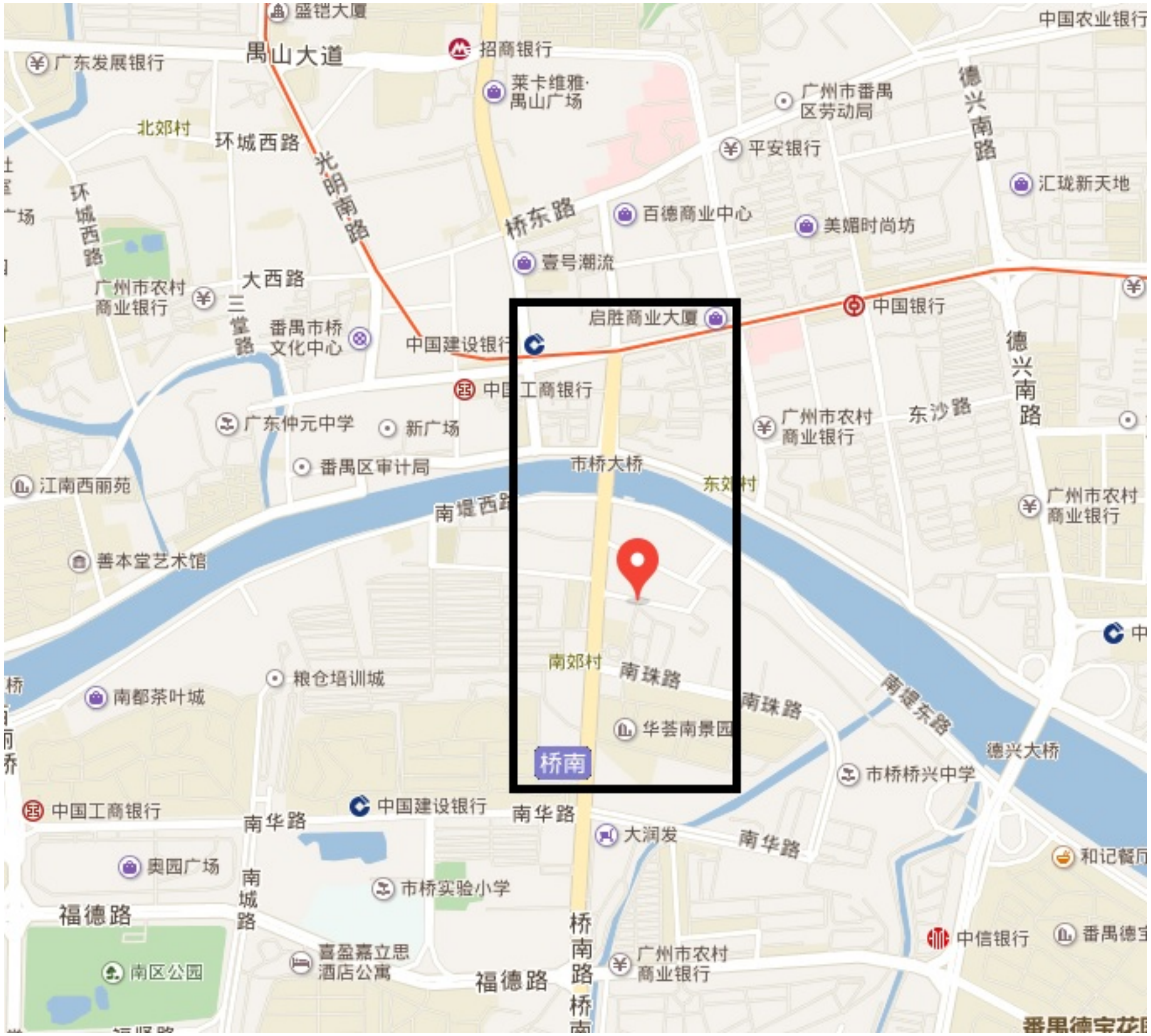
可以设置自动换IP，多久换一次随心所欲，无需手动拨号重连

断线重播就算断线会在电脑无网期间自动连接，不会暴露真实IP

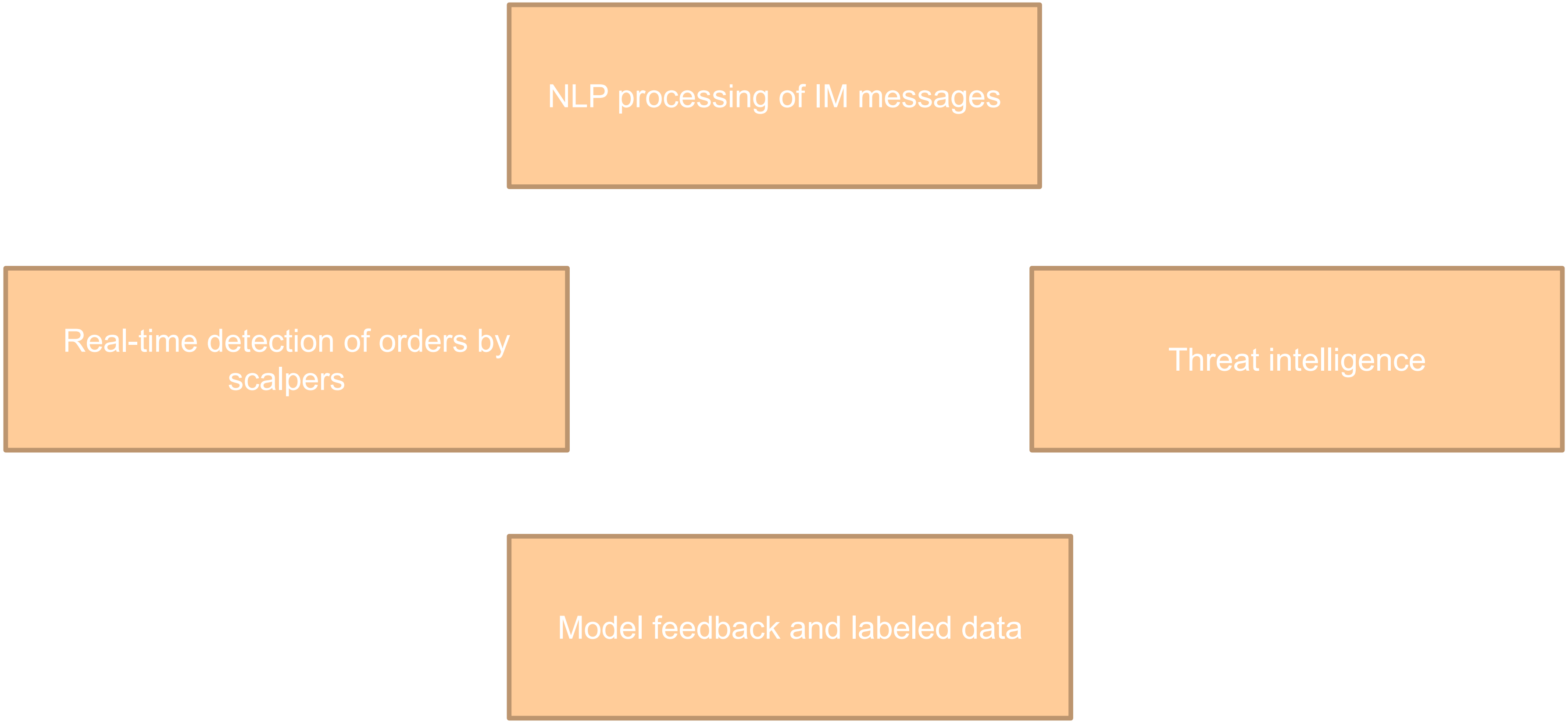
安全可靠



Fraud Cell Phone orders Taken Down



Steps against Scalper



NLP processing of IM messages

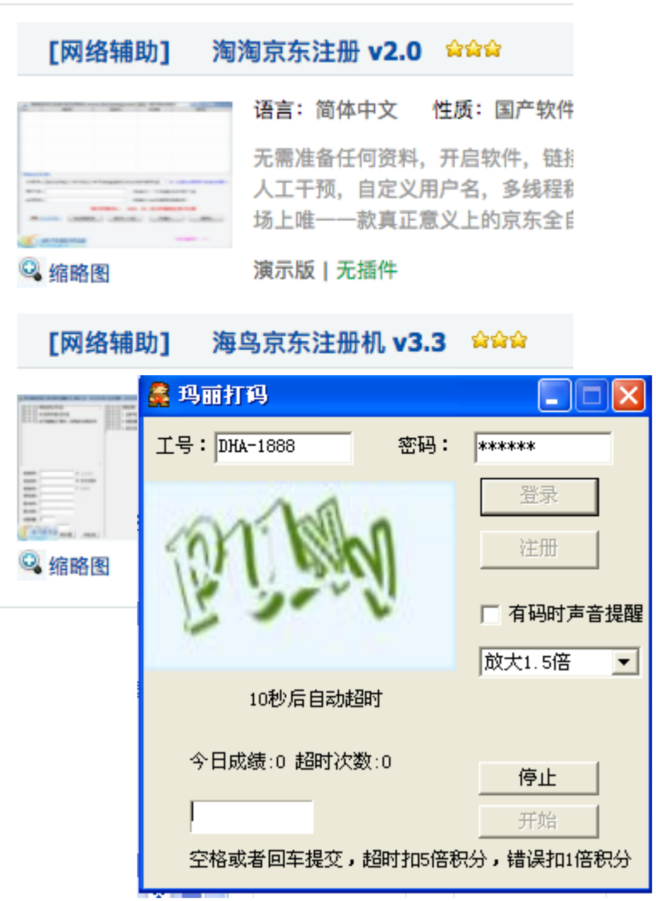
Real-time detection of orders by scalpers

Threat intelligence

Model feedback and labeled data

Bulk Registration

- Using tools or simulators
- Underground economy chain
  - Access code service
  - SMS verification service
  - Fake ID
- Features to detect
  - Behaviors of bots
  - Rush registration
  - Fake information



[网络辅助] 淘淘京东注册 v2.0

语言：简体中文 性质：国产软件

无需准备任何资料，开启软件，链掛
人工干预，自定义用户名，多线程利
场上唯一一款真正意义上的京东全自

演示版 | 无插件

[网络辅助] 海鸟京东注册机 v3.3

玛丽打码

工号：DHA-1888 密码：******

□ 有码时声音提醒

放大1.5倍

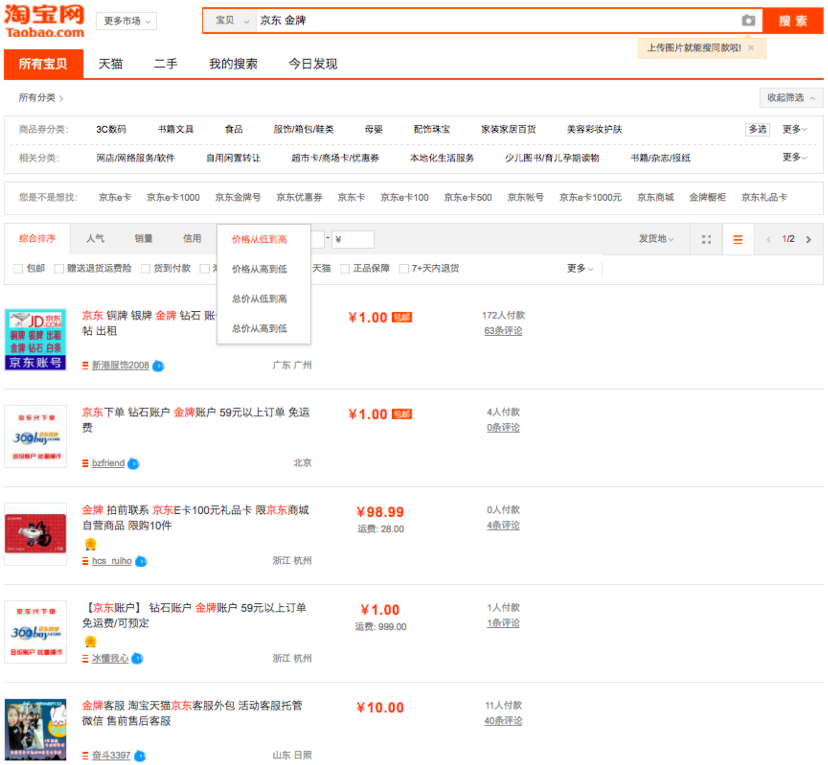
10秒后自动超时

今日成绩:0 超时次数:0

空格或者回车提交，超时扣5倍积分，错误扣1倍积分

Account Trading

- Price by account types
- Trading platform
  - E-commercial websites
  - IM Groups (QQ，Wechat)
  - Personal Websites



京东 铜牌 银牌 金牌 钻石 账
帖 出租
¥1.00 包邮
172人付款
63条评论
新港服饰2008
广东 广州

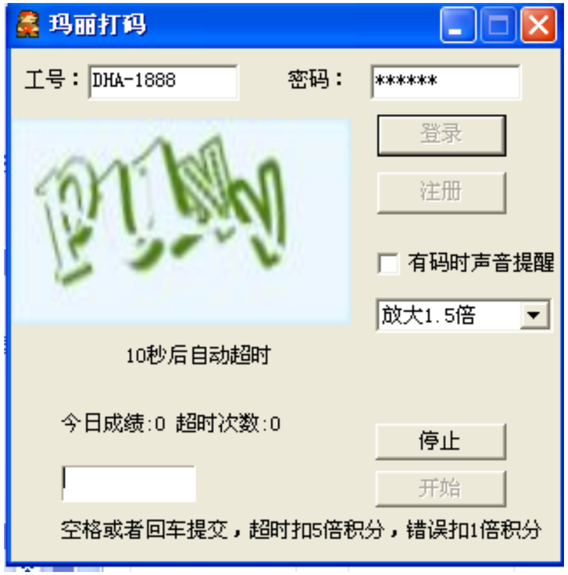
京东下单 钻石账户 金牌账户 59元以上订单 免运费
¥1.00 包邮
4人付款
0条评论
bzfriend
北京

金牌 拍前联系 京东E卡100元礼品卡 限京东商城自营商品 限购10件
¥98.99
运费: 28.00
0人付款
4条评论
hcs_ruiho
浙江 杭州

【京东账户】 钻石账户 金牌账户 59元以上订单免运费/可预定
¥1.00
运费: 999.00
1人付款
1条评论
冰懂我心
浙江 杭州

金牌客服 淘宝天猫京东客服外包 活动客服托管微信 售前售后客服
¥10.00
11人付款
40条评论
奋斗3397
山东 日照

AI-based Distributed Captcha Solver



工号：DHA-1888 密码：******

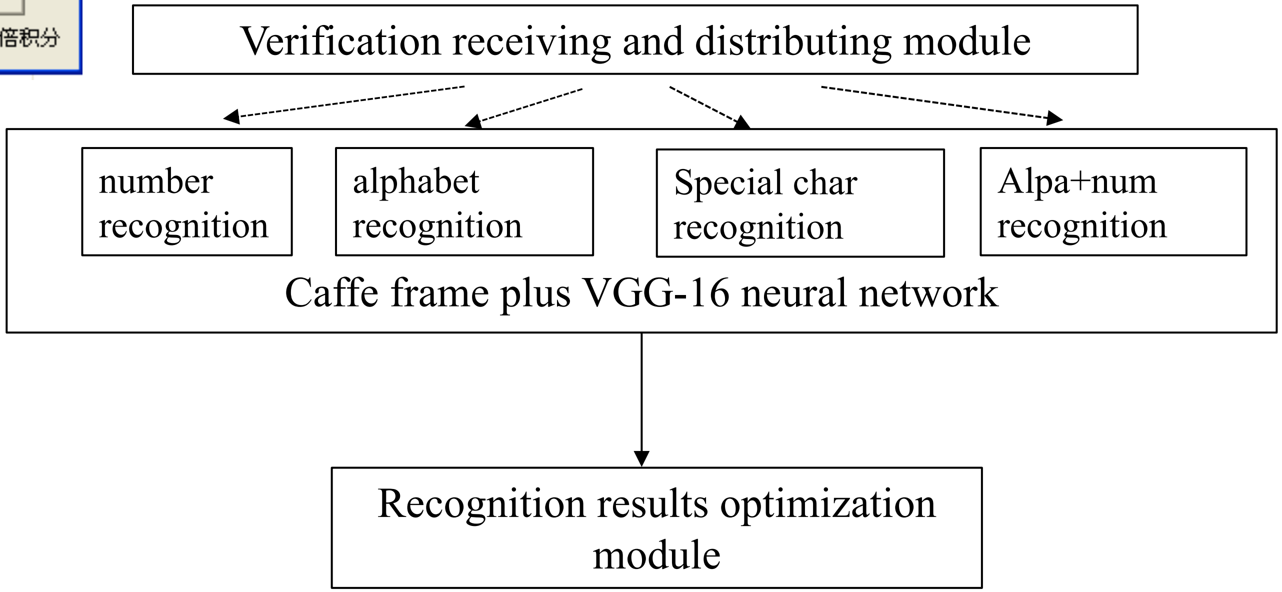
□ 有码时声音提醒

放大1.5倍

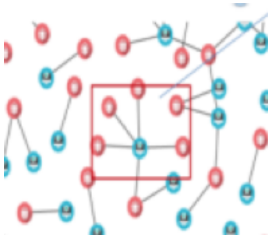
10秒后自动超时

今日成绩:0 超时次数:0

空格或者回车提交，超时扣5倍积分，错误扣1倍积分


Verification receiving and distributing module
number recognition
alphabet recognition
Special char recognition
Alpa+num recognition
Caffe frame plus VGG-16 neural network
Recognition results optimization module

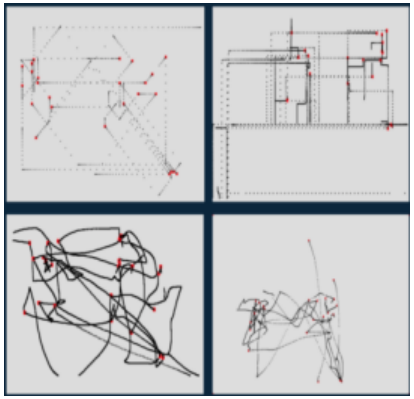
JD Registration Anti-Fraud

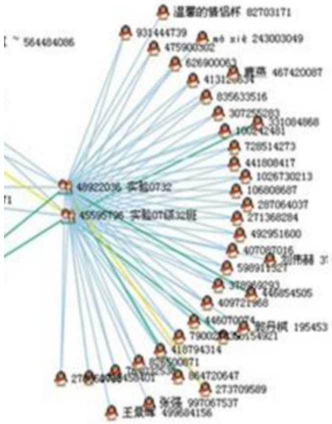


Device Analysis

Cluster Analysis

User Behavior





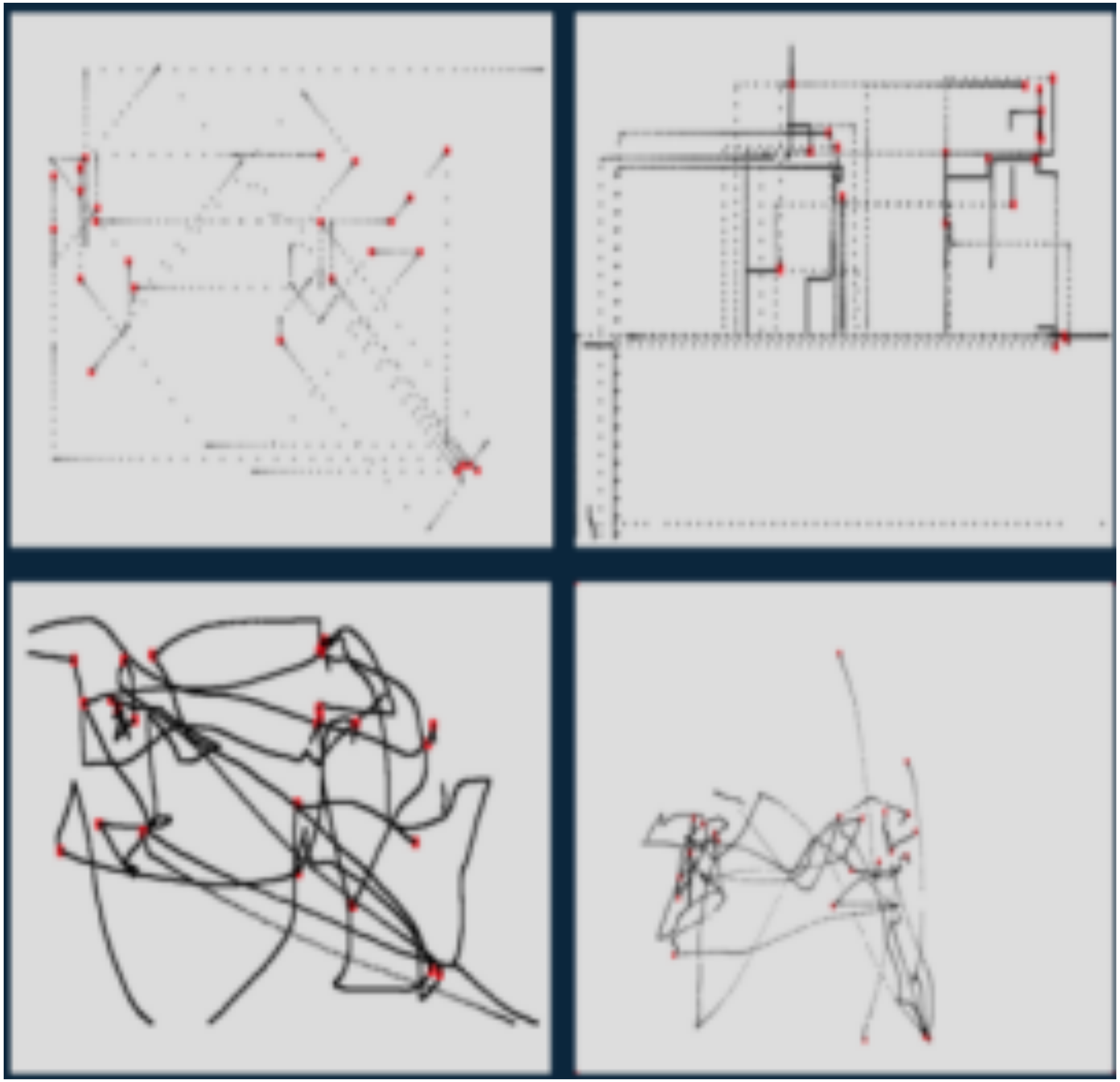
Bot Detection Using Biometrics

- Many scenarios at JD would benefit from distinguishing between bot and human

  Bot account registration
  Bot placing an order
  Bot crawling our site to extract pricing info
- Exploring biometrics features including mouse movement and keyboard

POP QUIZ: Can you identify the bot mouse movement graphs from the human ones?

Bot Detection



AI Security Future

- Black market in e-Commerce in China is one scenario of AI vs. AI

- More AI security problems to solve
  - Openness and collaboration

Thank you !