AI Powered Security and Securing AI

Dr. Jimmy Su

Head of JD Security Research Center, Senior Director

Outline

- Intro of JD
- Black market in e-Commerce
- AI vs AI
- AI platform security

JD.COM Introduction

700 Million

June Sales Event **Items** Sold

Massive Scale

301.8M

Active customer accounts

160K

Active third-party vendors on JD platform

190K

Full-time employees

1.59B

Orders fulfilled in 2017

Redefining Retail Through Technology

JD.COM 京东

Our First 12 Years

- Lowering costs
- Enhancing efficiency
- Improving user experience

The Next 12 Year: Leveraging AI

Creating a truly intelligent business

- Natural Language Processing
- Smart logistics
- Smart supply chain
- Financial technologies
- Jcloud Cloud computing

How large is the black market in e-Commerce?

JD.COM 京东

- 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
- Ecosystem consists of upstream, midstream and downstream.

Upstream of the Black Market

- Verification code/image platform
  - Automate registration and login processes
- Account take-over data
  - Individually targeted high usage passwords
- Automated software
  - Timers for flash sales
- Proxy tools
  - Defeat IP based risk control strategies

Midstream of the Black Market

- Provides various accounts related services such as Instant Messaging (IM) groups or online forums.
- Fake account registration
- Account take-over
- Account washing
- Information exchange platform
- Trading platform

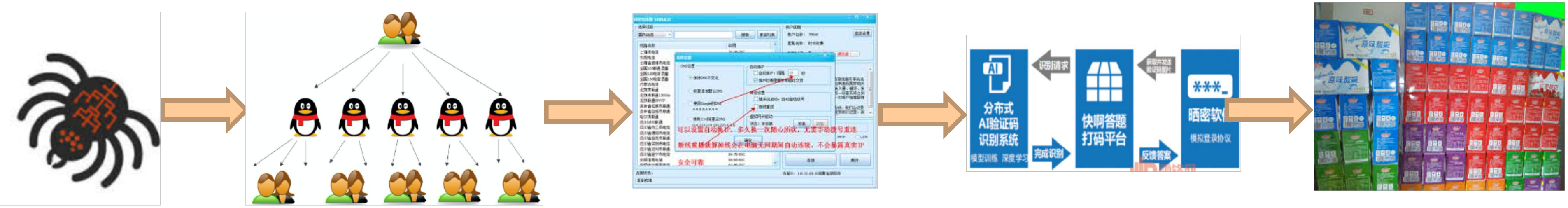
Downstream of the Black Market

- Gain profits and incur losses to normal users and e-Commerce companies
- Theft
- Fraud
- Blackmailing
- Click farming
- Scalper

Scalpers

- ❑ Scaling 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 AI based monitoring system is a strong plus to the legacy rule-based system**
  - ❑ **Accuracy of the information**
  - ❑ **New threat info acquisition never discovered before**

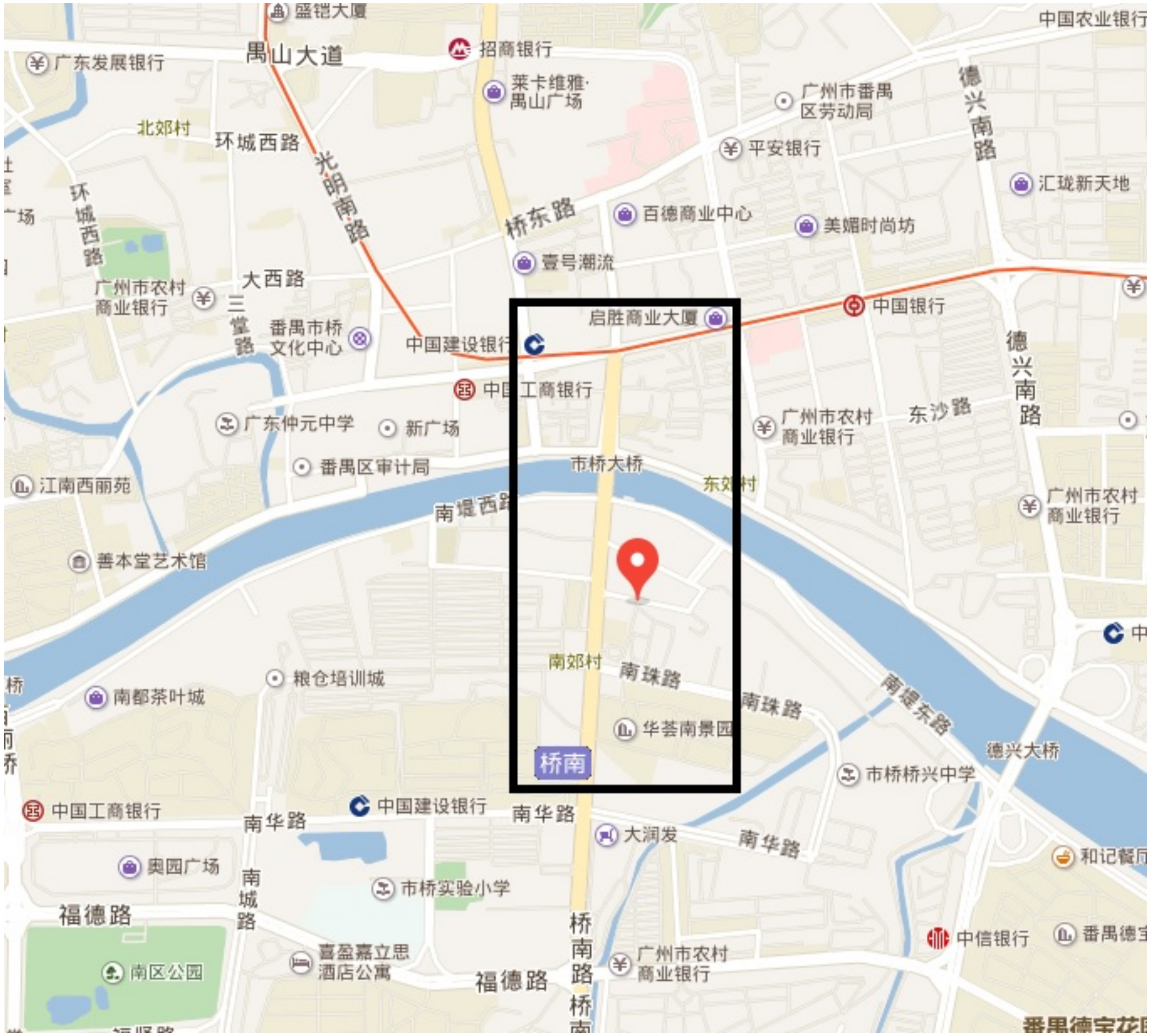
What do Scalpers do ?



Bot Detection **NLP** **Reverse Engineering** **Adversarial Machine Learning** **Address Clustering**

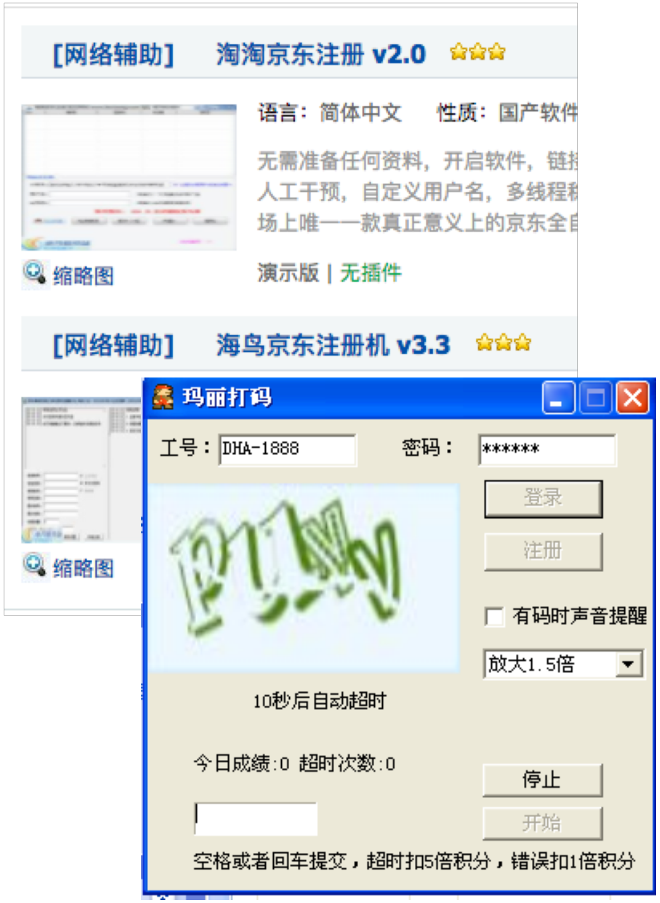
Fraudulent Cell Phone Orders

JD.COM 京东



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
人工干预，自定义用户名，多线程
场上唯一一款真正意义上的京东全

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

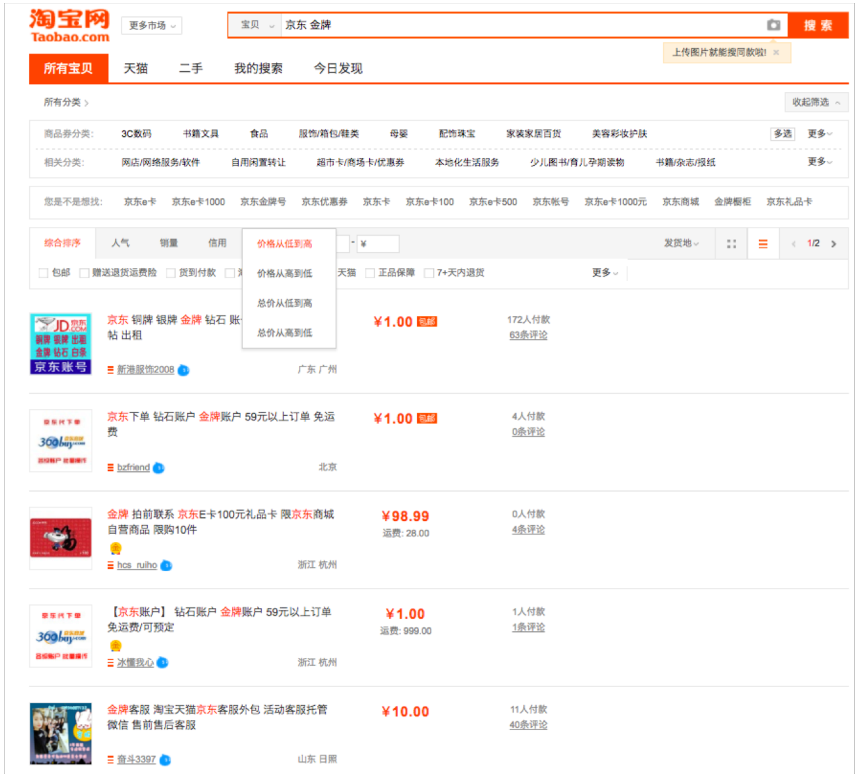
10秒后自动超时

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 金牌

商品券分类: 3C数码 书籍文具 食品 服饰/箱包/鞋类 母婴 配饰珠宝 家装家居百货 美容彩妆护肤 多选 更多

相关分类: 网店/网络服务/软件 自用闲置转让 超市卡/商场卡/优惠券 本地化生活服务 少儿图书/育儿孕期读物 书籍/杂志/报纸 更多

您是不是想找: 京东e卡 京东e卡1000 京东金牌号 京东优惠券 京东卡 京东e卡100 京东e卡500 京东帐号 京东e卡1000元 京东商城 金牌橱柜 京东礼品卡

综合排序 人气 销量 信用 价格从低到高 价格从高到低 总价从低到高 总价从高到低 ¥ 发货地 1/2

□ 包邮 □ 赠送退货运费险 □ 货到付款 □ 天猫 □ 正品保障 □ 7+天内退货 更多

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

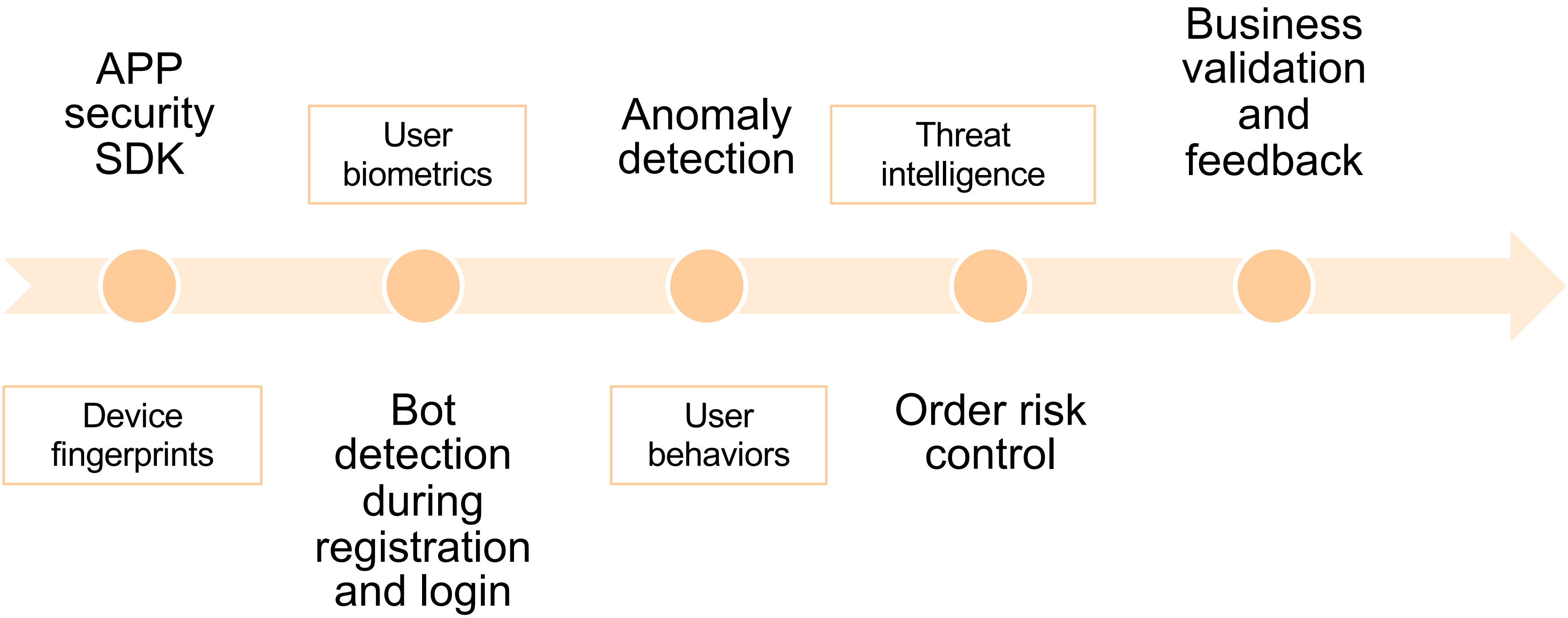
京东下单 钻石账户 金牌账户 59元以上订单 免运费 — ¥1.00 包邮 — 4人付款 0条评论 — bzfriend — 北京

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

Account Security: AI Empowered



APP security SDK

Device fingerprints

User biometrics

Bot detection during registration and login

Anomaly detection

User behaviors

Threat intelligence

Order risk control

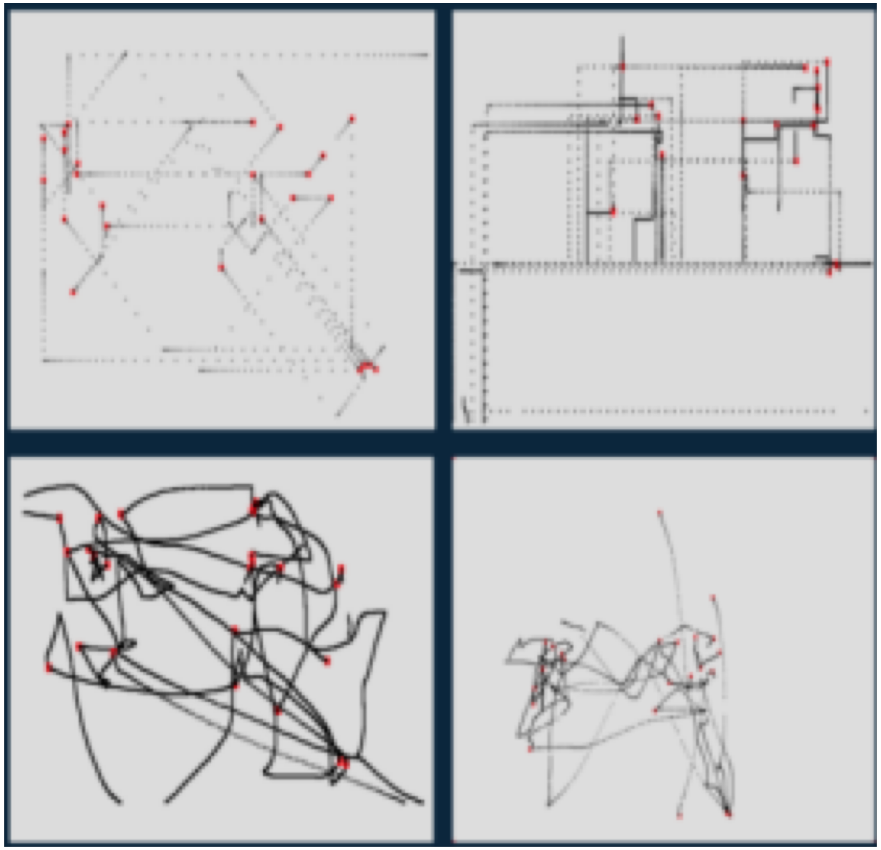
Business validation and feedback

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

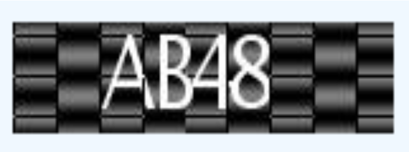
POP QUIZ: Can you identify the bot mouse movement graphs from the human ones?

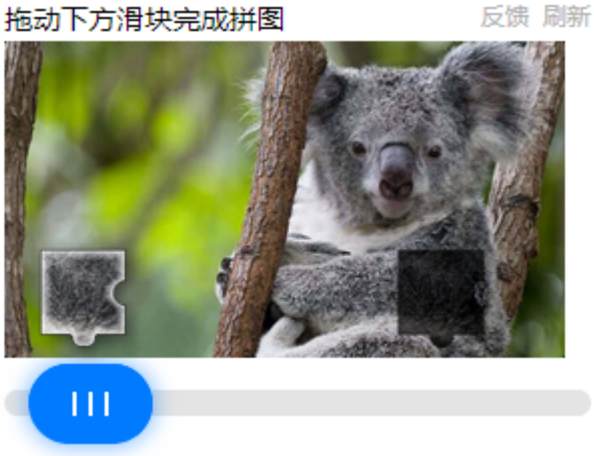
Bot Detection



Attackers using AI to Lower Costs

- **Intermediate level CAPTCHA is a solved problem in the Black Market.**




拖动下方滑块完成拼图

CAPTCHA Solving AI Platforms

JD.COM 京东

Tested on eight most popular CAPTCHA solving platforms in the Black Market

65% accuracy

71% accuracy

42% accuracy

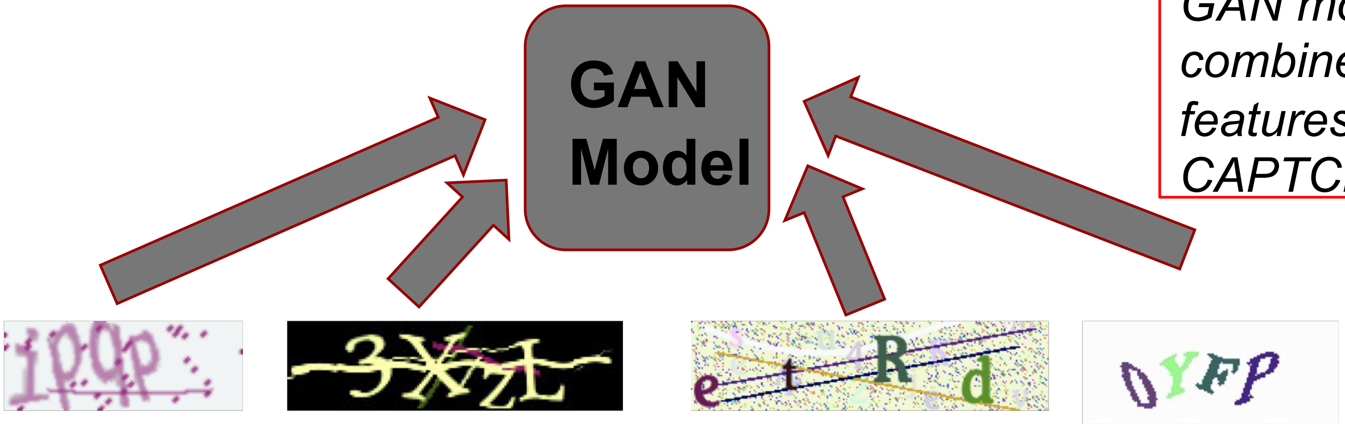
49% accuracy

76% accuracy

68% accuracy

AI Strikes Back

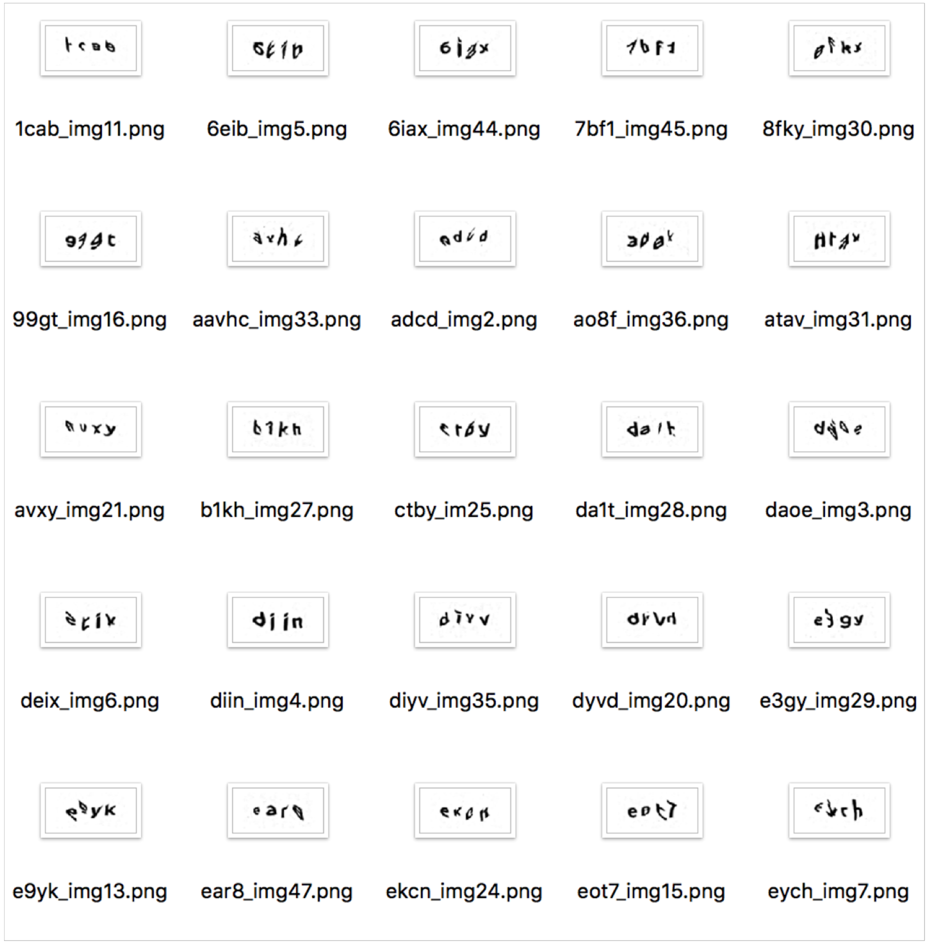
Based on CAPTCHA solving platform accuracies, we use GAN to generate adverserial samples.



GAN model combines the best features of various CAPTCHAS

GAN Adversarial Samples

- **Lower CAPTCHA platform accuracy to 12% !**
- **Must balance user experience with CAPTCHA difficulty**

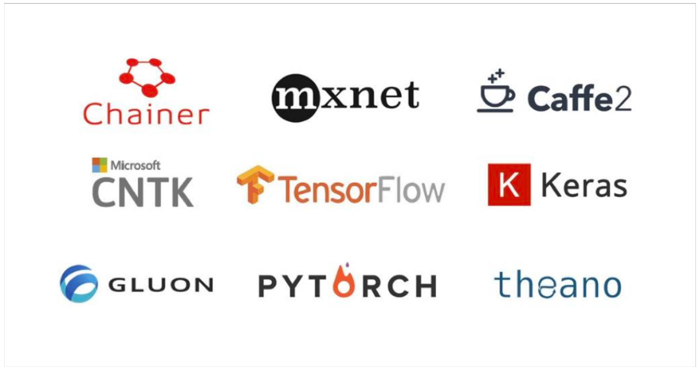


1cab_img11.png
6eib_img5.png
6iax_img44.png
7bf1_img45.png
8fky_img30.png
99gt_img16.png
aavhc_img33.png
adcd_img2.png
ao8f_img36.png
atav_img31.png
avxy_img21.png
b1kh_img27.png
ctby_im25.png
da1t_img28.png
daoe_img3.png
deix_img6.png
diin_img4.png
diyv_img35.png
dyvd_img20.png
e3gy_img29.png
e9yk_img13.png
ear8_img47.png
ekcn_img24.png
eot7_img15.png
eych_img7.png

AI平台安全隐患

恶意数据类型
(Malformed Image
Malicious PDF)

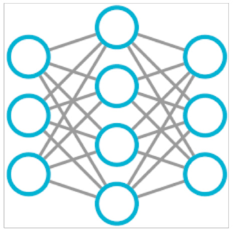
AI平台在提取特征时
需要Parse这些文件
从而引发漏洞



框架平台漏洞
(开发代码依赖库)

Tensorflow – 887K行代码 – 97个依赖库
Caffe – 127K行代码 – 137个依赖库
Torch – 590K行代码 – 48个依赖库

包含Heap Overflow, DOS, integer overflow等漏洞



模型攻击
(第三方模型
模型重用攻击)

AI平台数据隐私保护

- GDPR (Global Data Protection Regulation) 从2018/05起在EU生效
  - 对包含用户数据的训练集的使用有更加严格的限制
  - 对AI做出的决定的可解释行有更加严格的限制
  - 对数据中出现的歧视现象的限制
  - 需要相应的机制去监控这些条例没有被违反
- 原始训练数据的泄漏
  - AI平台的Attack Surface之广 包含漏洞之多 隐患很大
  - JD的隐私数据种类多 数量大 用于AI的更不少
- 挑战
  - Privacy Preserving Data Release (PPDR) vs AI/ML的矛盾
  - Differential privacy: 通过增加Noise的办法
  - RAPPOR (Google开发的)

AI平台中的BlockChain

- JD内部使用AI的部门很多 数据集重用情况复杂 追责困难
  - BlockChain记录了谁用了什么数据 做了什么model
- Trained AI Model on Blockchain
  - Model信息放到chain上, 这样保证不被attacker恶意修改

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 !