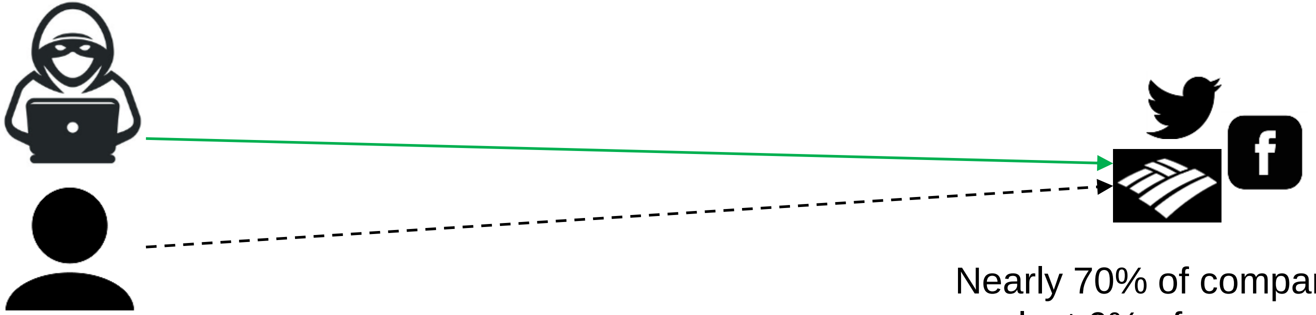
Him of Many Faces: Characterizing Billion-scale Adversarial and Benign Browser Fingerprints on Commercial Websites

Shujiang Wu, Pengfei Sun†, Yao Zhao†, Yinzhi Cao

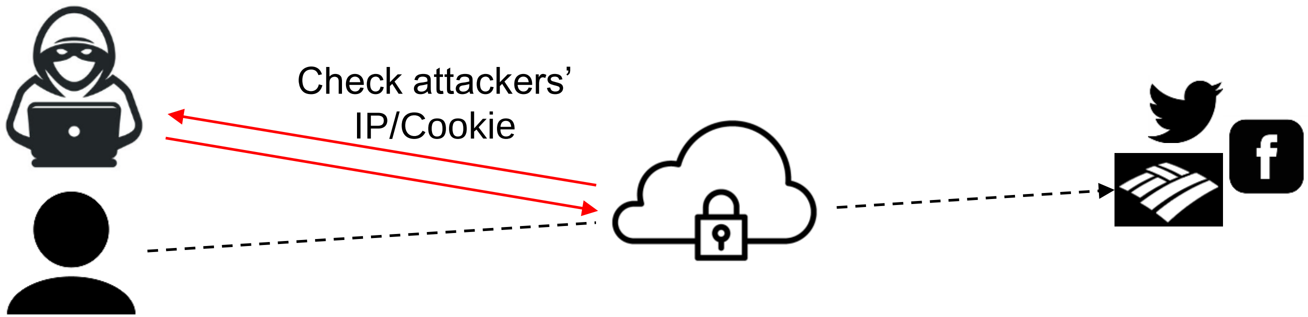
Johns Hopkins University, †F5

Bot attack and defender

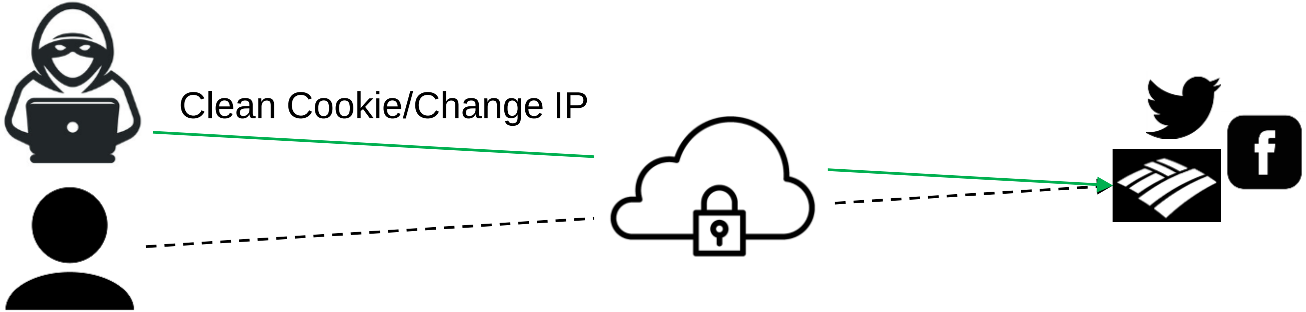


Nearly 70% of companies
lost 6% of revenue
bot-driven account fraud

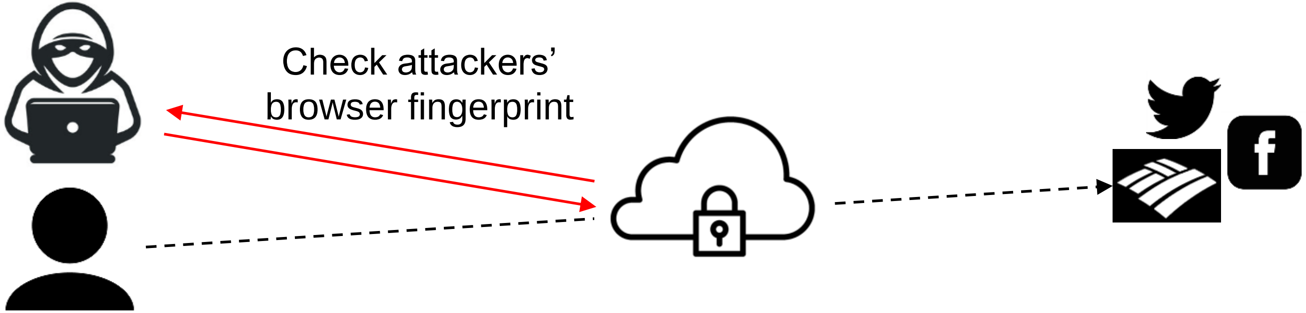
Bot attack and defender



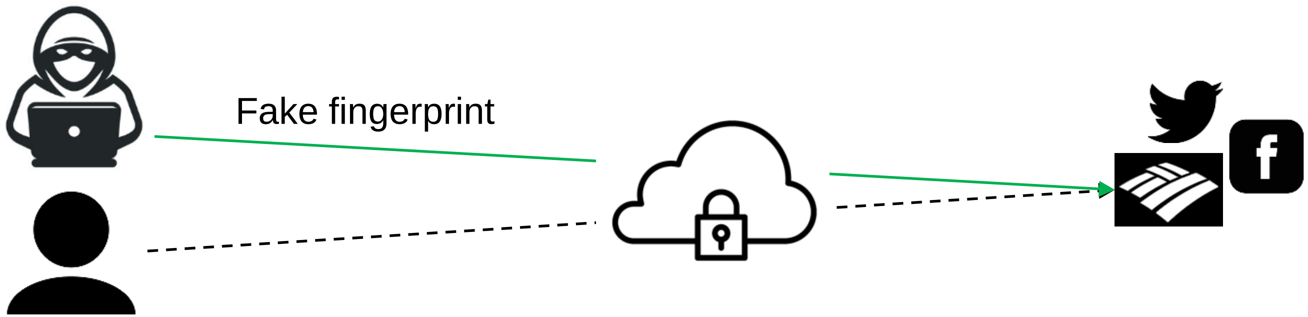
Bot attack and defender



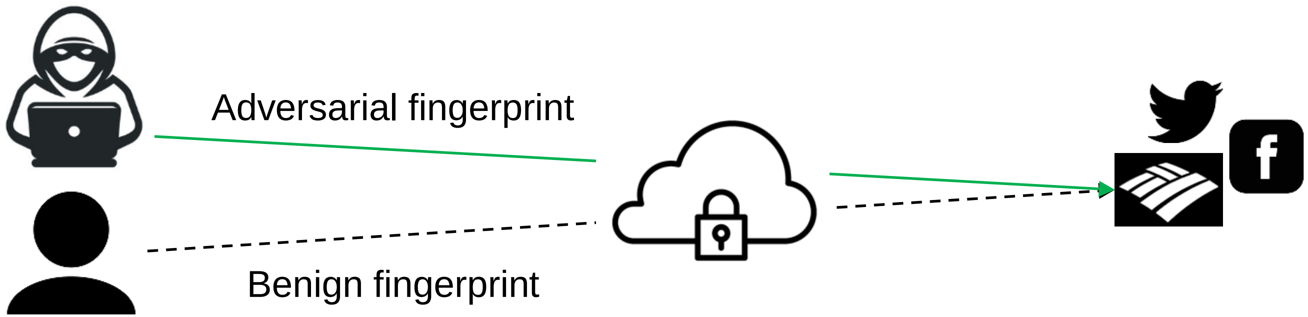
Bot attack and defender



Bot attack and defender

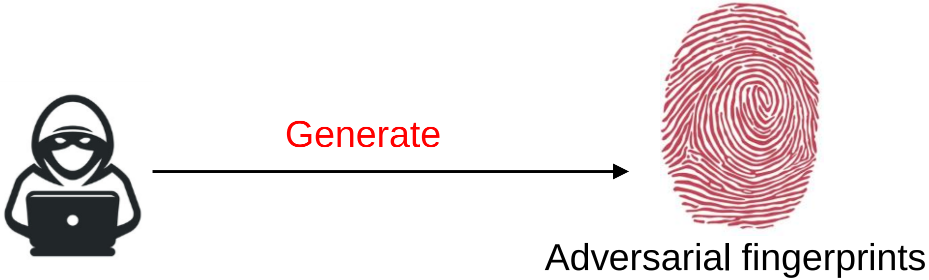


Bot attack and defender



Problem Statement

→ How to generate adversarial fingerprints



Problem Statement

→ How to generate adversarial fingerprints

→ Differences between adversarial and benign fingerprints

Benign fingerprints

Adversarial fingerprints

Outline

Measurement methodology

Step 1: Traffic Analysis

→ **Bot and Fraud Detection/Defense**

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

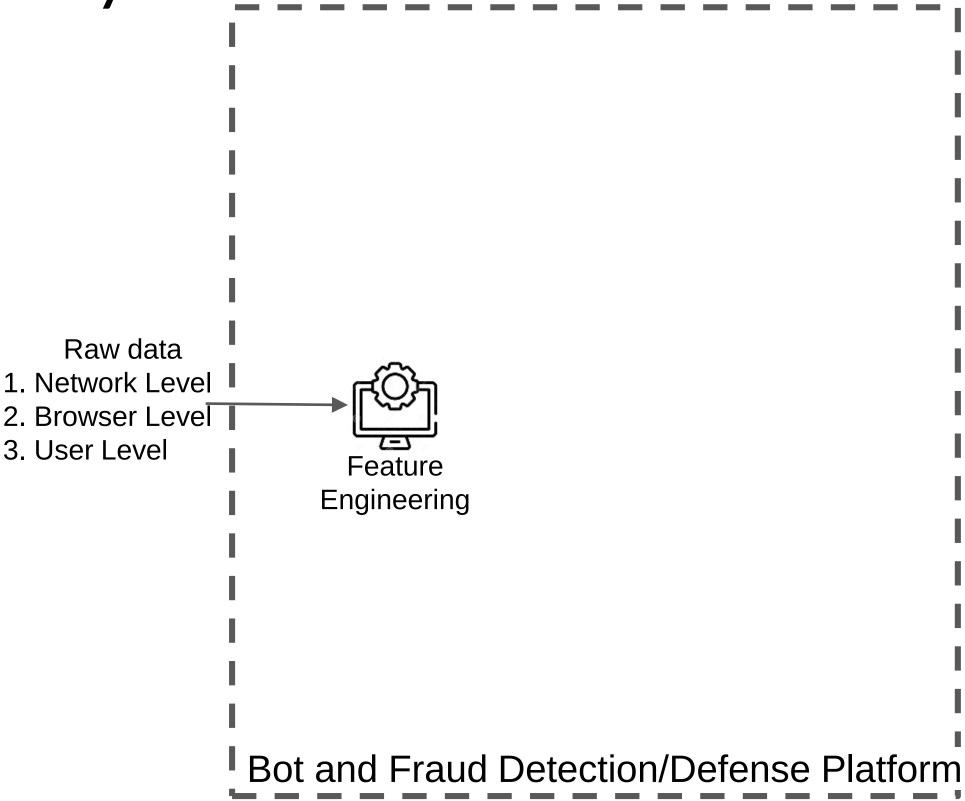
→ Generative Tool Analysis

→ Generative Strategy Analysis

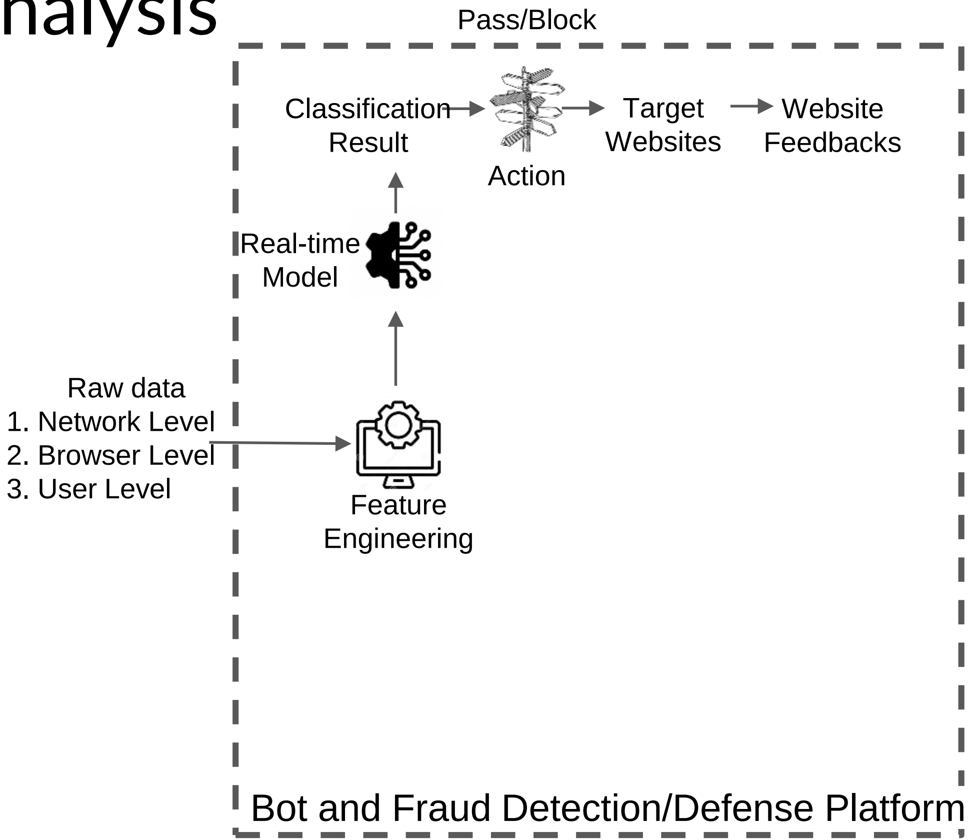
→ Statistical Analysis

Summary

Traffic analysis

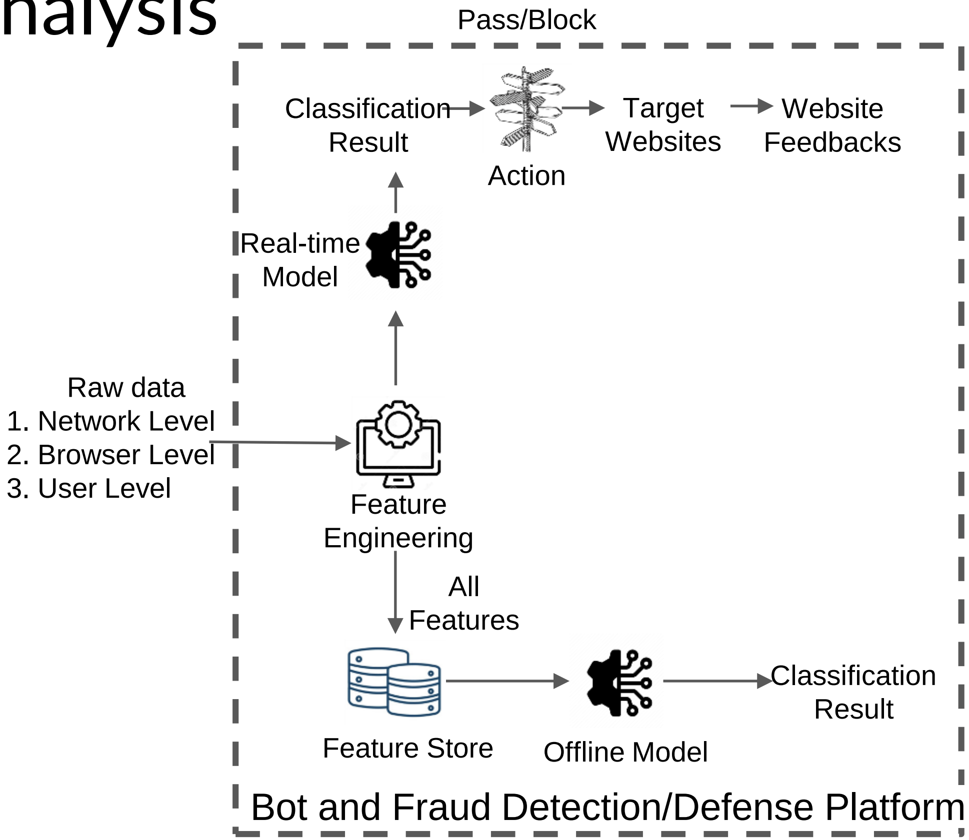


Traffic analysis



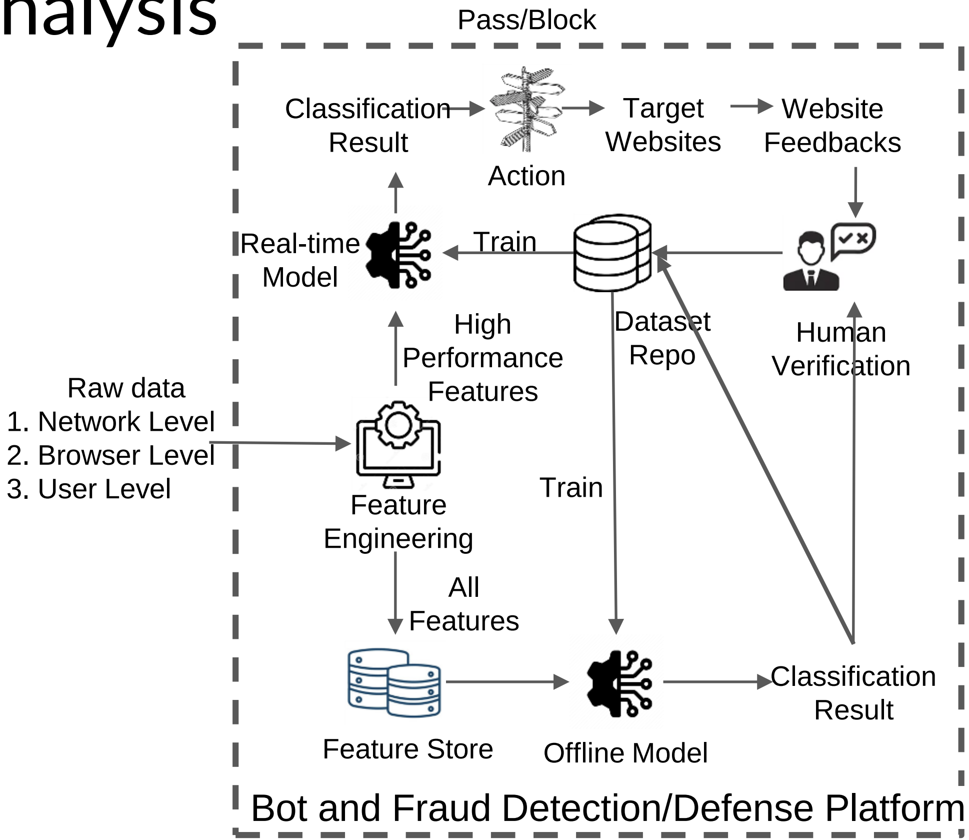
Real-time Model
1. URL
2. Cookie
3. TCP/IP FP
4. IP Address
5. ASN
6. Username
7. TLS Fingerprint
8. User Behavior

Traffic analysis



Offline Model
1. IP Reputation
2. ASN Reputation
3. User Reputation
4. Device Reputation
5. Header Reputation
6. Behavior per session

Traffic analysis



Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ **Attack Type Classification**

→ Dataset

Step 2: Fingerprint Analysis

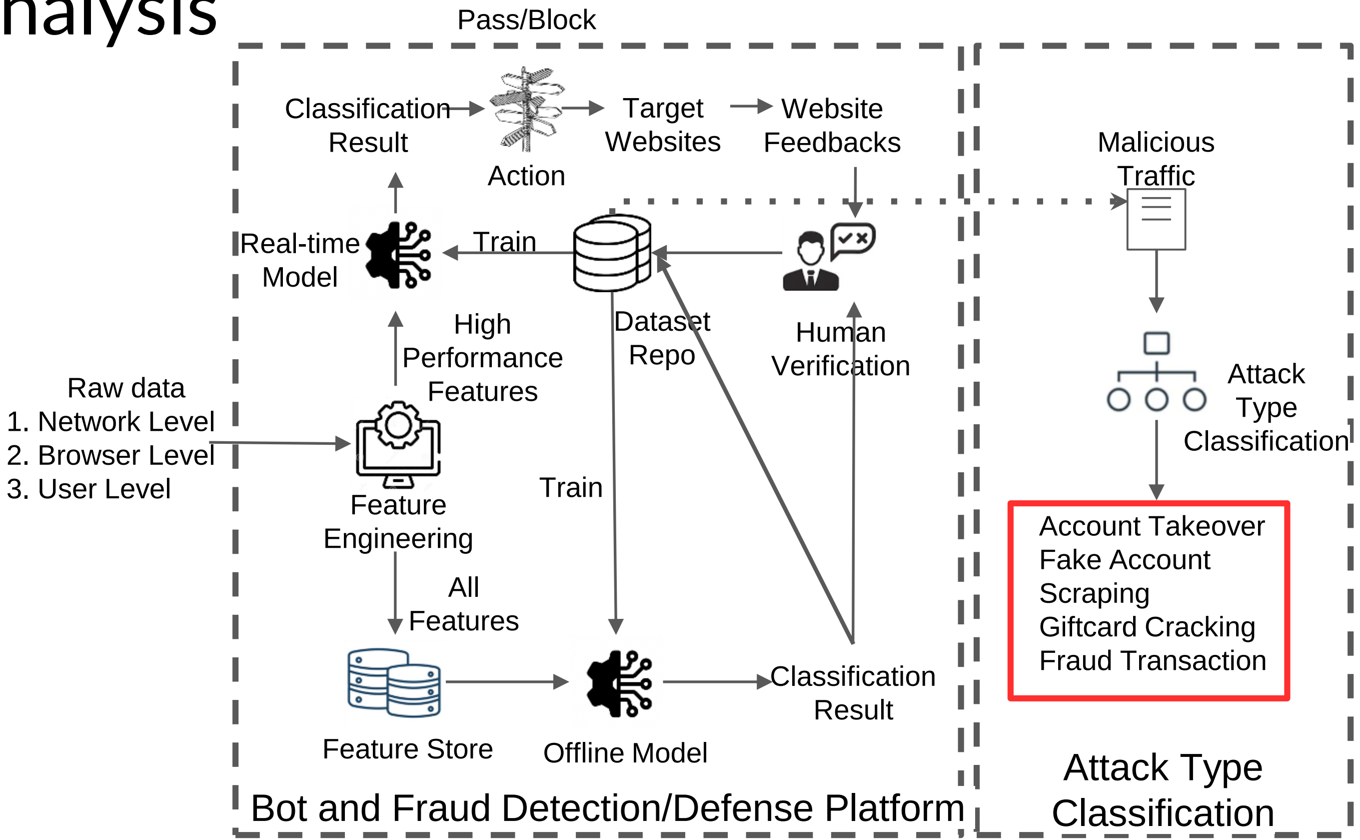
→ Generative Tool Analysis

→ Generative Strategy Analysis

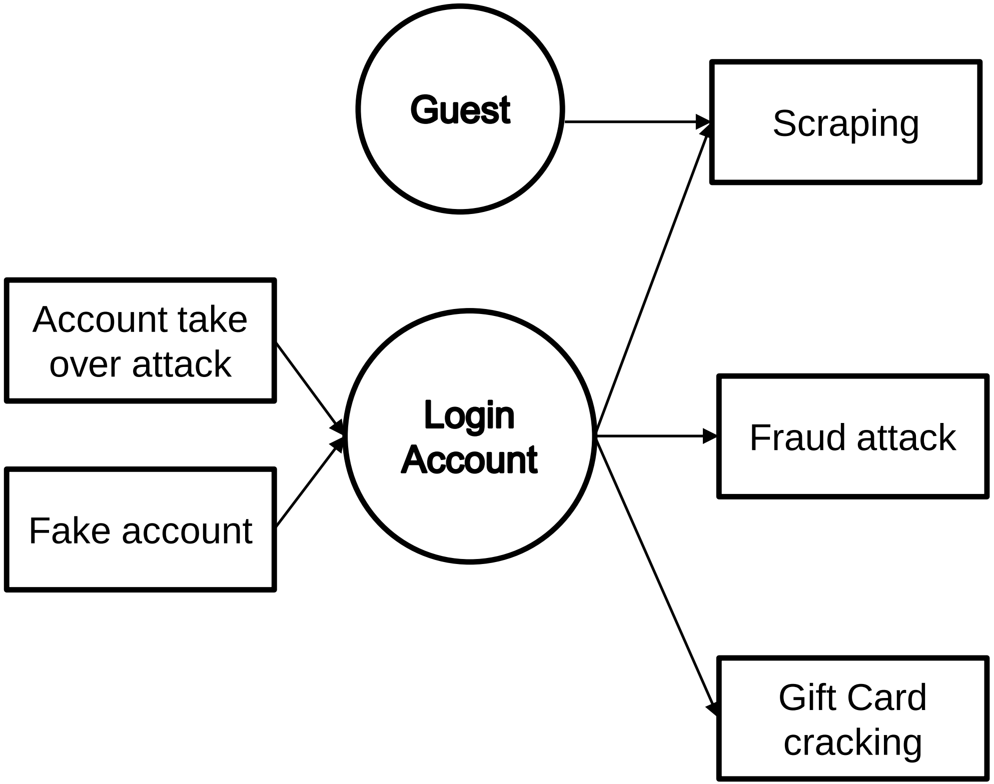
→ Statistical Analysis

Conclusion

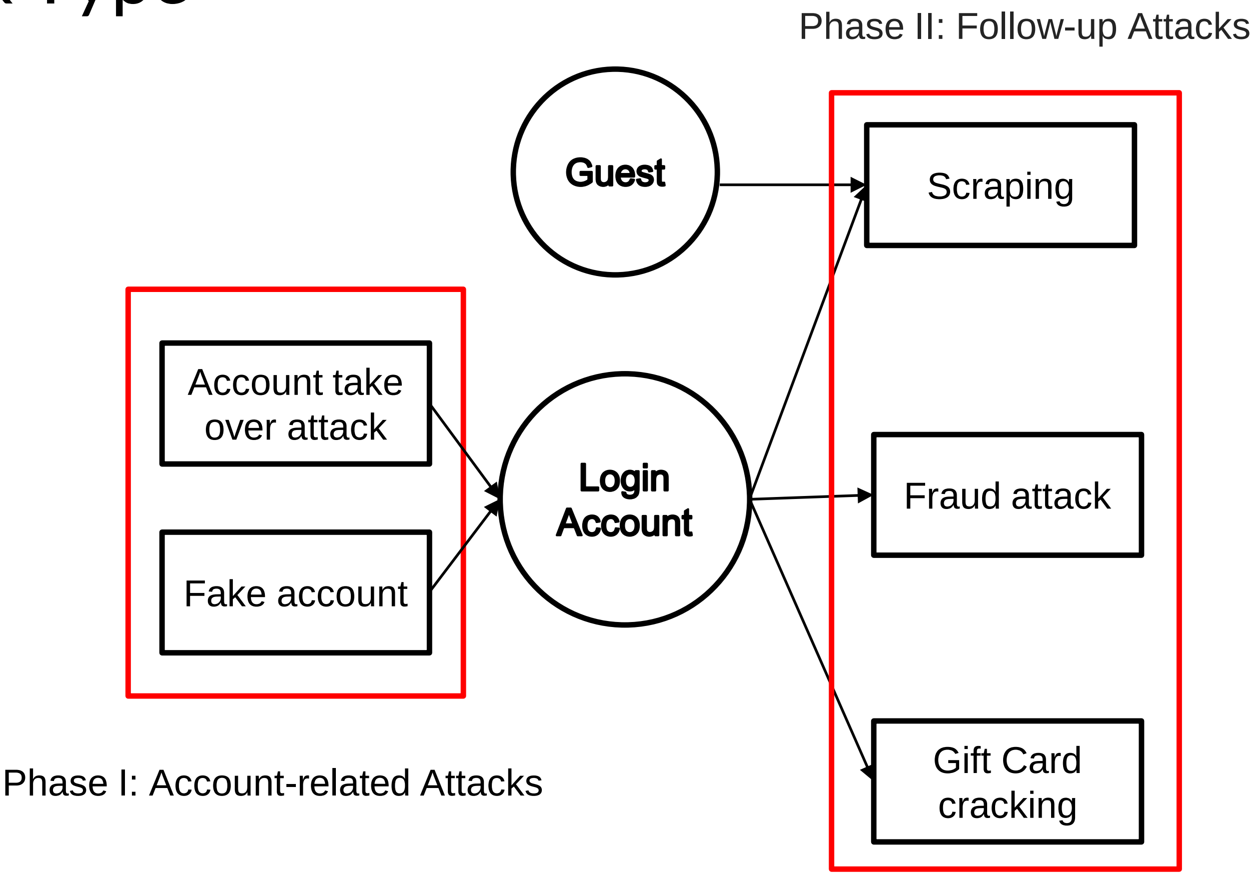
Traffic analysis



Attack Type

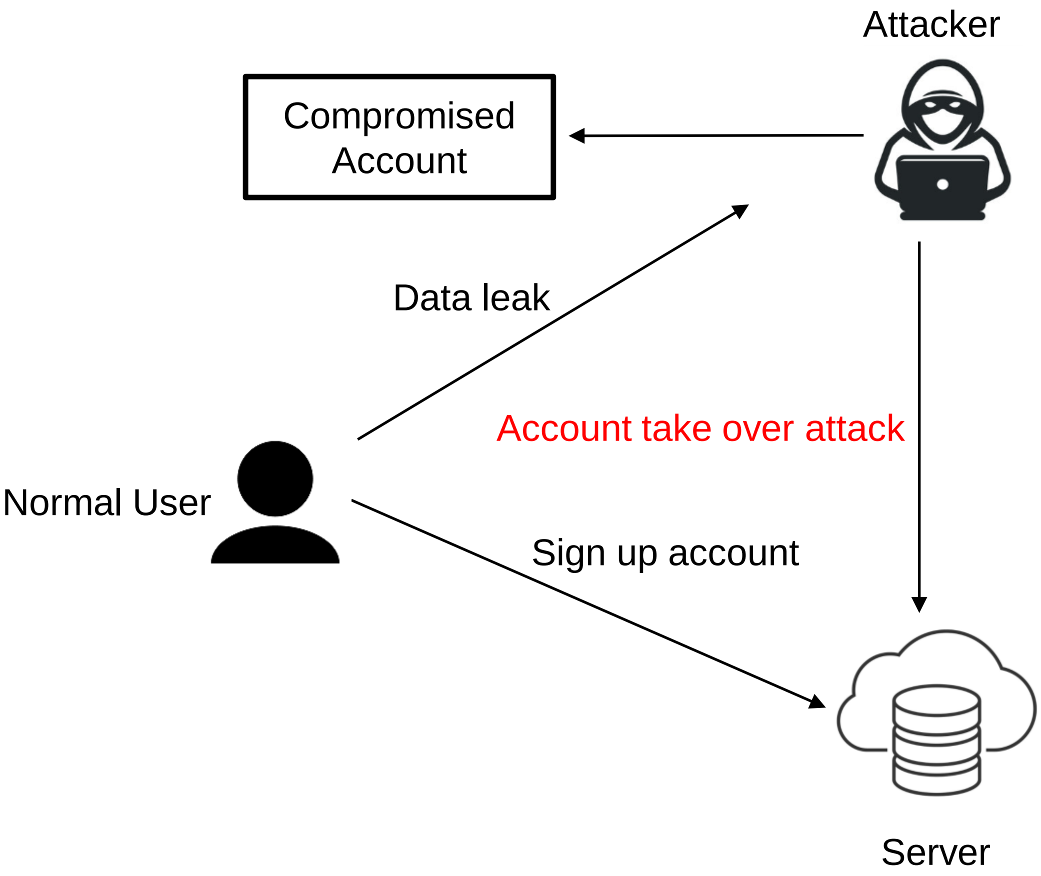

Guest
Scraping
Account take over attack
Login Account
Fraud attack
Fake account
Gift Card cracking

Attack Type

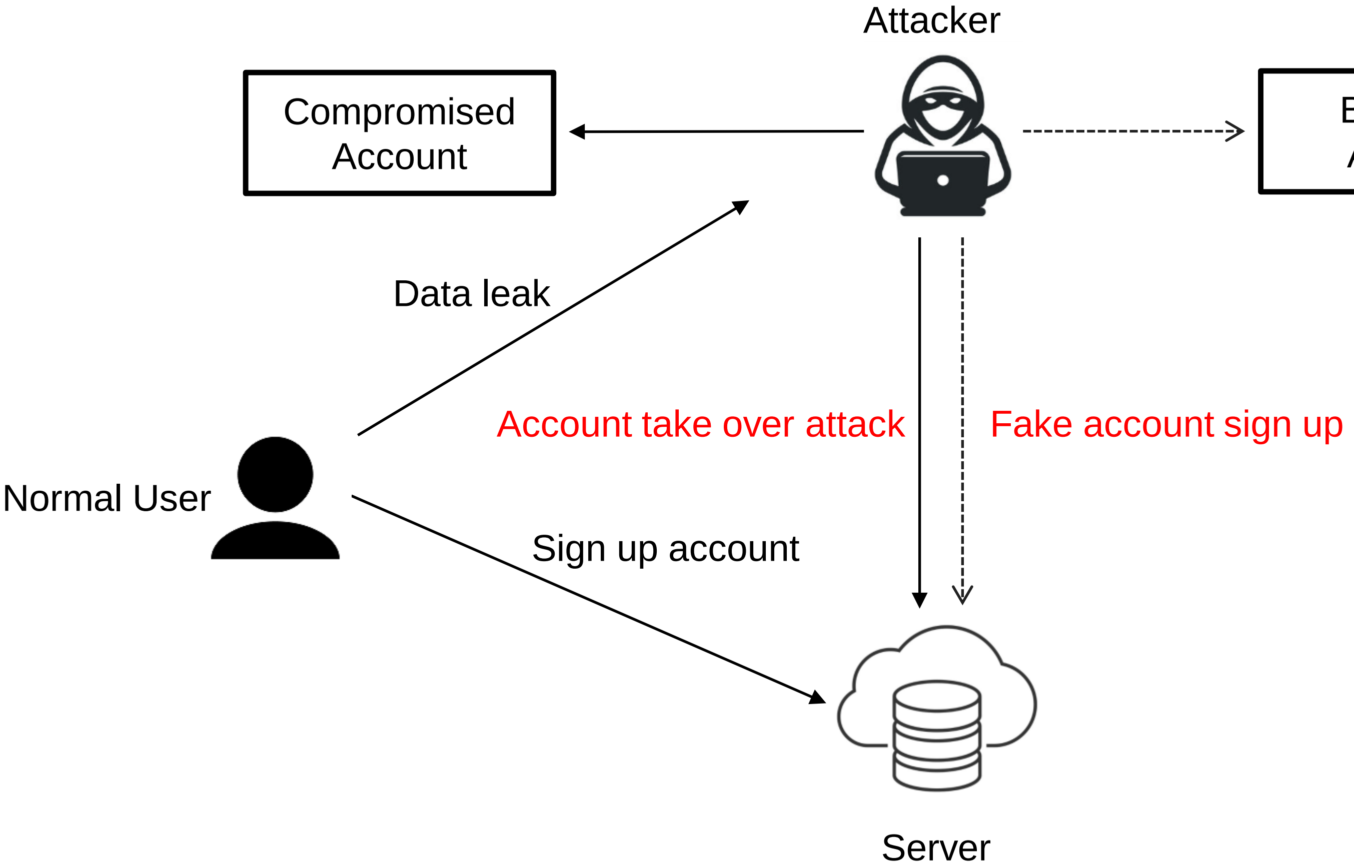


Phase II: Follow-up Attacks
Guest
Scraping
Account take over attack
Login Account
Fraud attack
Fake account
Gift Card cracking
Phase I: Account-related Attacks

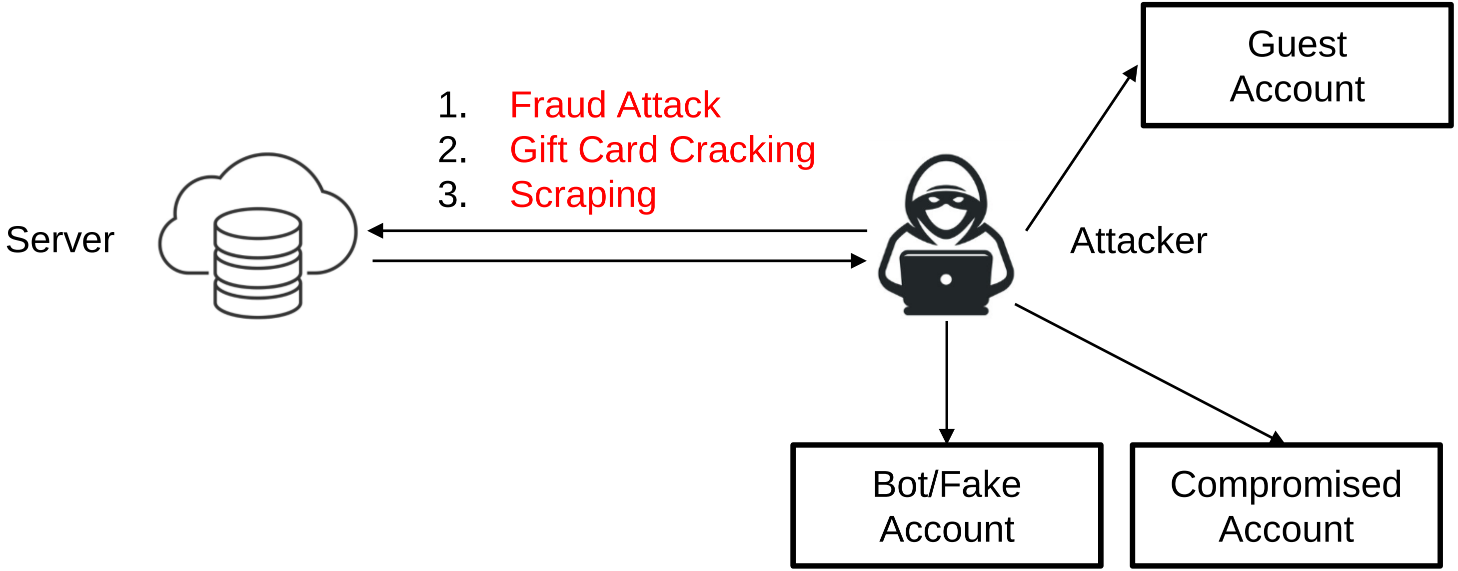
Phase I: Account-related Attacks



Phase I: Account-related Attacks



Phase II: Follow-up Attacks



Attack Type

%	Benign	Account Take Over	Fraud	Fake Account	Anonymous Scraping	Logged-in Scraping	Gift card Cracking
Rest. A	55.1	34.5	3.9	3.4	-	<0.1	3.1
Bank A	99.8	0.2	-	-	-	-	-
Bank B	46.4	52.9	<0.1	0.7	<0.1	-	-
Bank C	86.8	8.7	4.0	0.1	<0.1	0.4	-
Finance A	75.5	24.5	-	-	-	-	-
Finance B	98.7	0.1	-	-	0.5	0.6	-
Finance C	77.8	22.2	-	<0.1	-	-	-
Shop A	91.4	1.2	7.3	0.1	-	<0.1	<0.1
Shop B	48.4	0.2	1.0	-	22.5	27.8	<0.1
Airline A	79.4	0.1	-	<0.1	2.6	17.9	<0.1
Airline B	80.7	9.4	-	-	3.9	6.1	-
ISP A	99.8	0.2	<0.1	-	-	-	-
ISP B	99.5	0.5	-	-	-	-	-
ISP C	86.8	13.1	-	<0.1	-	0.1	-

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ **Dataset**

Step 2: Fingerprint Analysis

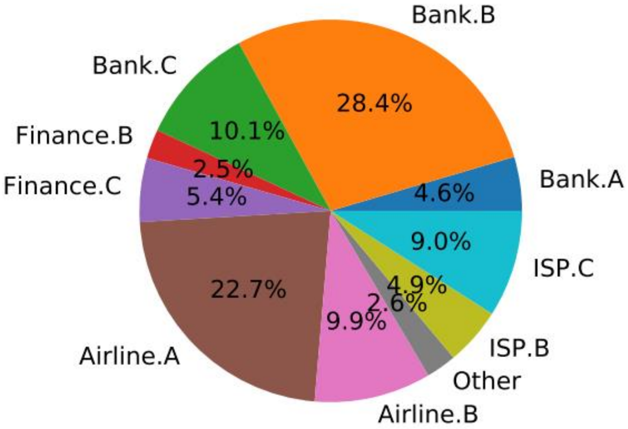
→ Generative Tool Analysis

→ Generative Strategy Analysis

→ Statistical Analysis

Conclusion

Dataset



Collected 36 billion HTTP(s) requests
Between January 2021 and June 2021
Based on 14 websites:
→ 15.3 billion (42.5% of the total) adversarial
→ 20.7 billion (57.5% of the total) benign

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ Generative Tool Analysis

→ Generative Strategy Analysis

→ Statistical Analysis

Conclusion

1. User Agent
2. Historical timestamp
3. Plugins
4. Font list
5. Canvas image
6. GPU vendor and renderer
7. Screen resolution
8. devicePixelRatio

…

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ Generative Tool Analysis

→ Generative Strategy Analysis

→ Statistical Analysis

Conclusion

Scripting tools
Emulated browsers
Virtual machines

Keep
Block
Mimic
Randomize

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ Generative Tool Analysis

→ Generative Strategy Analysis

→ Statistical Analysis →

K-L divergence
Empty rate
Unique rate

Conclusion

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ **Generative Tool Analysis**

→ Generative Strategy Analysis

→ Statistical Analysis

Conclusion

Generative Tool Analysis

1. Scripting tools
   - Simple applications (e.g., written in Python)
   - Send HTTP requests to target websites

2. Emulated browsers
   - Headless browsers, extensions, tailor-made browsers
   - Driven by automated tools like Selenium

3. Virtual machines
   - Combination with emulated browsers

Generative Tool Analysis

Attack Type	Attack tools percentage		
	Scripting	Browsers	VM
Account Takeover	82.4	15.5	0.3
Fake Account	49.2	50.6	0.1
Fraud	30.0	69.6	0.4
Scraping	93.4	6.6	<0.1
Gift card Cracking	97.5	2.2	0.3

Choose different tools according to the difficulty of operation

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ Generative Tool Analysis

→ **Generative Strategy Analysis**

→ Statistical Analysis

Conclusion

Generative Strategy Analysis

1. Keep
   - Keep the original value
   - User Agent → Requests
2. Block
   - Disable or can not support
   - Browser fingerprint → NULL-NULL-NULL-NULL
3. Mimic
   - Replace to another device's value
4. Randomize
   - Add noise or modify the value
   - WebGL render → NVIDIA GTX 1081

Adversarial Generative Strategies

Tools	Adversarial Strategy	%Request	%FP	#Req per FP
Scripting	Keep tool’s fingerprints	3.1%	<0.1%	155,552.6
	Mimicking benign fingerprints disabling JavaScript	77.6%	7.2%	657.5

Scripting tools are the most popular in practice due to its high performance.

Adversarial Generative Strategies

Tools	Adversarial Strategy	%Request	%FP	#Req per FP
Browsers	Mimic	1.0%	9.0%	7.1
	Mimic+Block	0.8%	3.5%	14.9
	Mimic+Block+Randomize	0.1%	0.2%	31.5
	Mimic+Randomize	0.2%	1.2%	8.0
	Keep	2.4%	0.4%	348.6
	Block	3.9%	<0.1%	5,151.5
	Block+Randomize	9.0%	60.3%	9.2
	Randomize	0.1%	0.1%	105.3
	Grey	1.2%	7.2%	10.3

“Randomize” and “Block” are the most popular strategies for emulated browser tools.

Adversarial Generative Strategies

Tools	Adversarial Strategy	%Request	%FP	#Req per FP
Browsers	Mimic	1.0%	9.0%	7.1
	Mimic+Block	0.8%	3.5%	14.9
	Mimic+Block+Randomize	0.1%	0.2%	31.5
	Mimic+Randomize	0.2%	1.2%	8.0
	Keep	2.4%	0.4%	348.6
	Block	3.9%	<0.1%	5,151.5
	Block+Randomize	9.0%	60.3%	9.2
	Randomize	0.1%	0.1%	105.3
	Grey	1.2%	7.2%	10.3

"Mimic" is less popular probably because adversaries need to obtain a large database of benign browser fingerprints.

Generative Strategies
Credential Stuffing Case Study

The Attacker gets thousands of account names and passwords.

Step 1: the Attacker builds a dataset linking the fake browser fingerprint and account.

	%Request	%Account	%FP	#Requests per account	#Requests per FP
Probe	2.0%	>0.1%	1.1%	112.8	46.1
Takeover Attempt	92.9%	99.8%	98.4%	1.3	1.0
Gray	5.0%	0.2%	0.5%	32.9	2.3

Generative Strategies
Credential Stuffing Case Study

The Attacker gets thousands of account names and passwords.

Step 1: the Attacker builds a dataset linking the fake browser fingerprint and account.
Step 2: The Attacker chooses a few test accounts to detect the defense system.

	%Request	%Account	%FP	#Requests per account	#Requests per FP
Probe	2.0%	>0.1%	1.1%	112.8	46.1
Takeover Attempt	92.9%	99.8%	98.4%	1.3	1.0
Gray	5.0%	0.2%	0.5%	32.9	2.3

Generative Strategies
Credential Stuffing Case Study

The Attacker gets thousands of account names and passwords.

Step 1: the Attacker builds a dataset linking the fake browser fingerprint and account.
Step 2: The Attacker chooses a few test accounts to detect the defense system.
Step 3: The Attacker deploys the account take over attack.

	%Request	%Account	%FP	#Requests per account	#Requests per FP
Probe	2.0%	>0.1%	1.1%	112.8	46.1
Takeover Attempt	92.9%	99.8%	98.4%	1.3	1.0
Gray	5.0%	0.2%	0.5%	32.9	2.3

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ Generative Tool Analysis

→ Generative Strategy Analysis

→ **Statistical Analysis**

Conclusion

Statistical Analysis

Feature Name	Kullback-Leiber Divergence		
	Adv. || Benign	Benign || Benign	Adv. || Adv.
User-Agent	1.6±1.2	0.8±1.8	1.9±1.6
Timestamp	4.2±5.6	0.5±0.6	2.0±1.5
Plugins	2.1±1.9	0.4±0.3	1.6±1.3
Font list	2.2±1.5	0.8±1.8	1.9±1.5
Canvas Image	2.7±1.5	0.9±1.9	1.9±1.5
Vendor + Renderer	5.7±2.8	0.8±1.7	2.5±2.5
Screen Resolution	5.3±3.0	0.4±0.3	2.2±1.5
devicePixelRatio	5.7±4.9	0.9±1.6	2.4±2.5
IP	1.7±0.9	0.4±1.7	1.6±2.3
ASN	3.6±1.5	2.0±1.9	3.0±1.4
FP	3.8±1.9	0.5±0.5	0.2±0.6
FP + IP + ASN	2.6±2.0	0.1±0.2	0.01±0.1

The K-L divergence
Adv./ Benign >> Adv./Adv.
Adv./ Benign >> Benign/Benign

Statistical Analysis

Feature Name	Kullback-Leiber Divergence		
	Adv. || Benign	Benign || Benign	Adv. || Adv.
User-Agent	1.6±1.2	0.8±1.8	1.9±1.6
Timestamp	4.2±5.6	0.5±0.6	2.0±1.5
Plugins	2.1±1.9	0.4±0.3	1.6±1.3
Font list	2.2±1.5	0.8±1.8	1.9±1.5
Canvas Image	2.7±1.5	0.9±1.9	1.9±1.5
Vendor + Renderer	5.7±2.8	0.8±1.7	2.5±2.5
Screen Resolution	5.3±3.0	0.4±0.3	2.2±1.5
devicePixelRatio	5.7±4.9	0.9±1.6	2.4±2.5
IP	1.7±0.9	0.4±1.7	1.6±2.3
ASN	3.6±1.5	2.0±1.9	3.0±1.4
FP	3.8±1.9	0.5±0.5	0.2±0.6
FP + IP + ASN	2.6±2.0	0.1±0.2	0.01±0.1

Adversarial fingerprint
Good at User-Agent, Plugin, Font list

Statistical Analysis

Feature Name	Kullback-Leiber Divergence		
	Adv. || Benign	Benign || Benign	Adv. || Adv.
User-Agent	1.6±1.2	0.8±1.8	1.9±1.6
Timestamp	4.2±5.6	0.5±0.6	2.0±1.5
Plugins	2.1±1.9	0.4±0.3	1.6±1.3
Font list	2.2±1.5	0.8±1.8	1.9±1.5
Canvas Image	2.7±1.5	0.9±1.9	1.9±1.5
Vendor + Renderer	5.7±2.8	0.8±1.7	2.5±2.5
Screen Resolution	5.3±3.0	0.4±0.3	2.2±1.5
devicePixelRatio	5.7±4.9	0.9±1.6	2.4±2.5
IP	1.7±0.9	0.4±1.7	1.6±2.3
ASN	3.6±1.5	2.0±1.9	3.0±1.4
FP	3.8±1.9	0.5±0.5	0.2±0.6
FP + IP + ASN	2.6±2.0	0.1±0.2	0.01±0.1

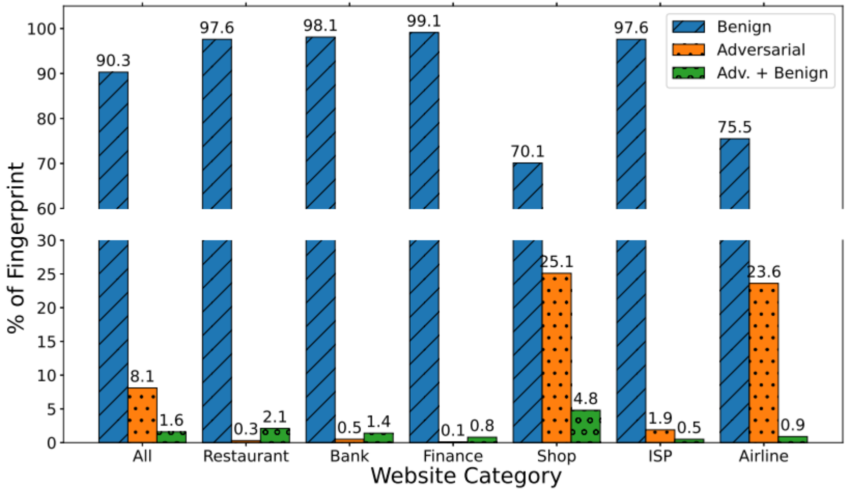
Adversarial fingerprint
Bad at Timestamp, vendor/renderer,
Screen resolution, devicePixelRatio

Statistical Analysis

Feature Name	Empty Rate %	
	Benign	Adv.
User-Agent	<0.1	<0.1
Timestamp	2.1	64.4
Plugins	4.4	46.3
Font list	11.8	50.1
Canvas Image	4.5	46.6
Vendor + Renderer	1.4	86.2
Screen Resolution	0.1	43.1
devicePixelRatio	0.0	82.4
IP	0.0	0.0
ASN	0.0	0.0
FP	0.0	<0.1
FP + IP + ASN	0.0	0.0

Adversarial fingerprints have more empty values compared with benign.

Statistical Analysis



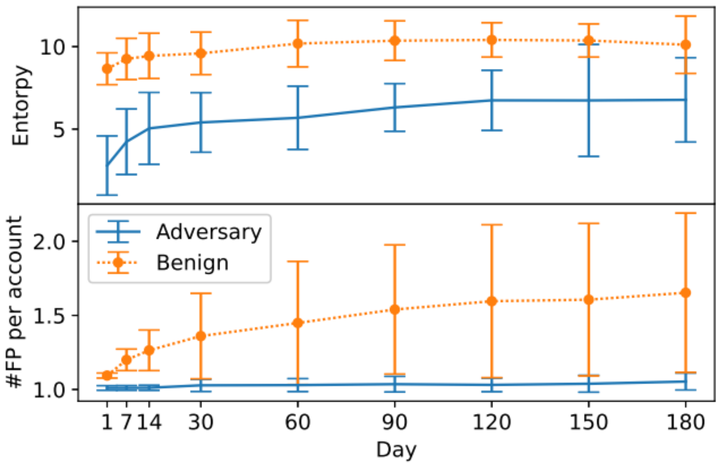
Unique browser fingerprint

1.6% shared, 8.1% are purely adversarial, 90.3% purely benign

→ Fake dataset is small

→ Create a lot of nonexistent values

Statistical Analysis



Benign fingerprints often evolve over time, while adversarial ones mostly stay stable.

Outline

Measurement methodology

Step 1: Traffic Analysis

→ Bot and Fraud Detection/Defense

→ Attack Type Classification

→ Dataset

Step 2: Fingerprint Analysis

→ Generative Tool Analysis

→ Generative Strategy Analysis

→ Statistical Analysis

Conclusion

Conclusion

--> First billion-scale measurement study of browser fingerprints

(i) adversaries are adopting various tools and strategies to generate adversarial fingerprints.

Scripting tools
Emulated browsers
Virtual machines

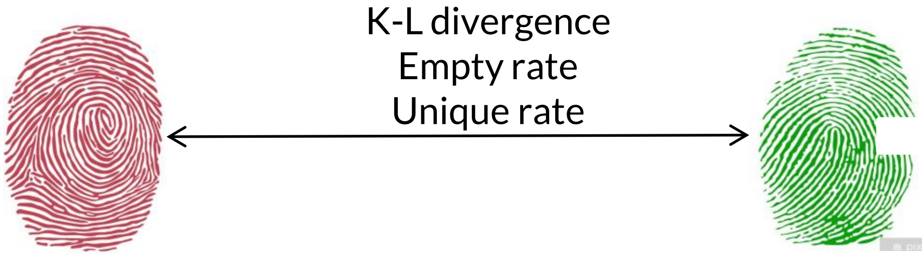
Keep
Block
Mimic
Randomize

Conclusion

--> First billion-scale measurement study of browser fingerprints

(i) adversaries are adopting various tools and strategies to generate adversarial fingerprints.

(ii) adversarial fingerprints are significantly different from benign ones in many metrics.



Conclusion

--> First billion-scale measurement study of browser fingerprints

(i) adversaries are adopting various tools and strategies to generate adversarial fingerprints.

(ii) adversarial fingerprints are significantly different from benign ones in many metrics.

(iii) adversarial fingerprints vary across different attack types.

Thanks

https://github.com/bfpmeasurementgithub/browser-fingeprint-measurement

buaasniper@gmail.com