A Nationwide Census on WiFi Security Threats: Prevalence, Riskiness, and the Economics

Di Gao, Hao Lin, Zhenhua Li, Feng Qian, Qi Alfred Chen
Zhiyun Qian, Wei Liu, Liangyi Gong, Yunhao Liu

清華大學 Tsinghua University
University of Minnesota
UCI University of California, Irvine
UC Riverside

Outline

1. Background
2. Methodology
3. Key Findings
4. Attack Ecosystem
5. Summary

Outline

1. Background

2. Methodology

3. Key Findings

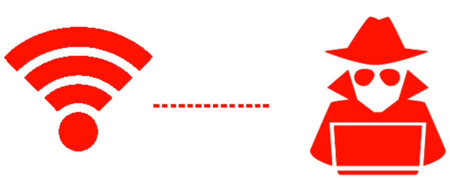
4. Attack Ecosystem

5. Summary

1.1 WiFi & Security Threats

☐ WiFi: An Enticing Target for Security Threats

- WiFi carries over 75% of the last-mile mobile Internet traffic
- Vulnerabilities of WiFi access points (APs) have been exploited
  - Traffic eavesdropping
  - Phishing attack
  - Cryptojacking …
- Various attack vectors in the wild



Compromised AP

Malicious AP

1.2 WiFi Security Today

WiFi-based Attacks: Nationwide Security Threats

Affecting Hundreds of Millions of End Users

Outline

1. Background
2. Methodology
3. Key Findings
4. Attack Ecosystem
5. Summary

2.1 Large-Scale Measurement

Collaborative Study

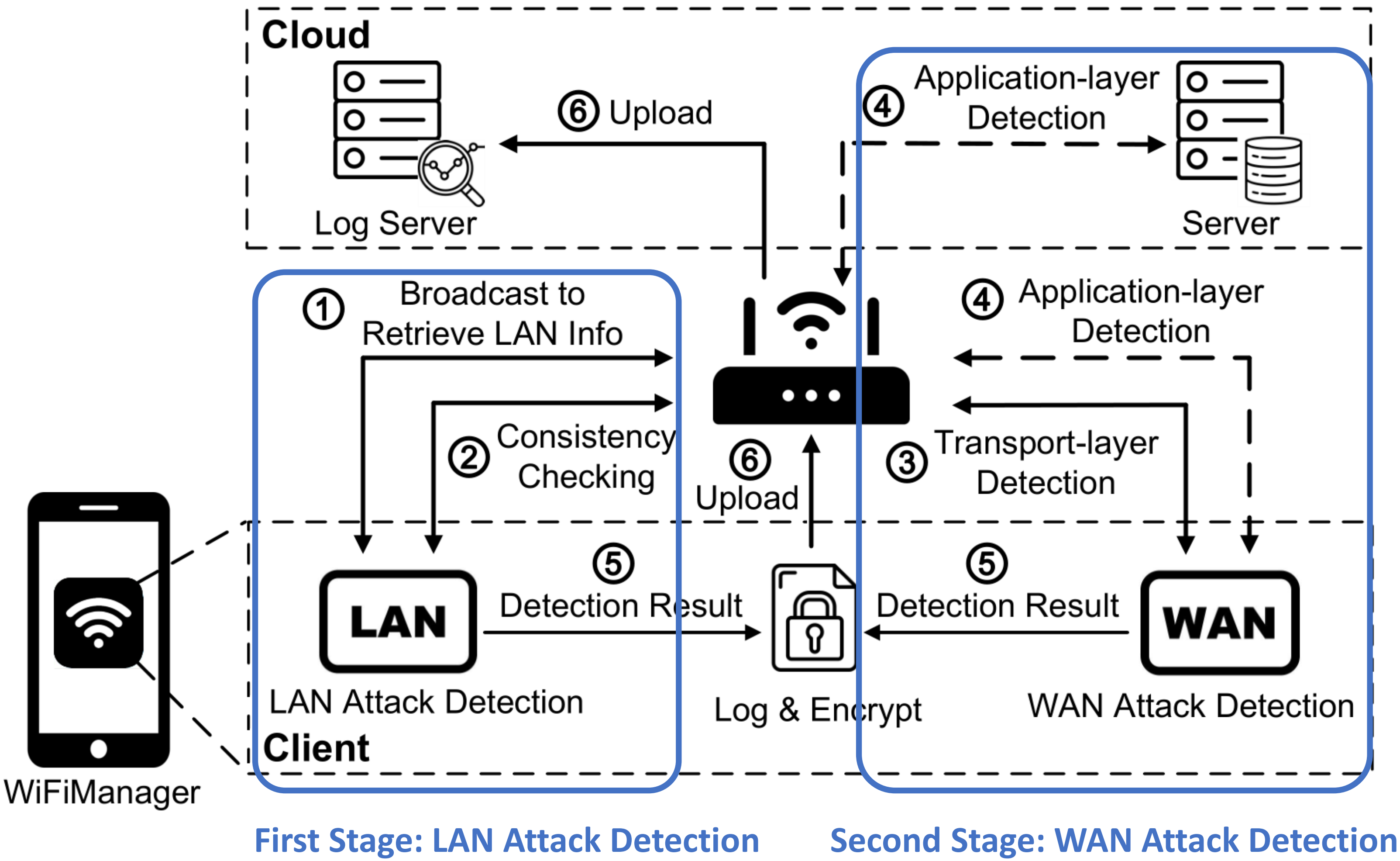
- In collaboration with WiFiManager, a WiFi management service
- WiFiManager serves 800M+ Android users in 200+ countries
- User devices as testers for WiFi APs

WiSC: A WiFi Security Checking System inside WiFiManager

Requirements		Challenges
User-space App	→	No Root Access
In-depth Understanding	→	Good Coverage & Precision
Low Resource Consumption	→	No Long-Term Monitoring

2.2 WiSC Architecture

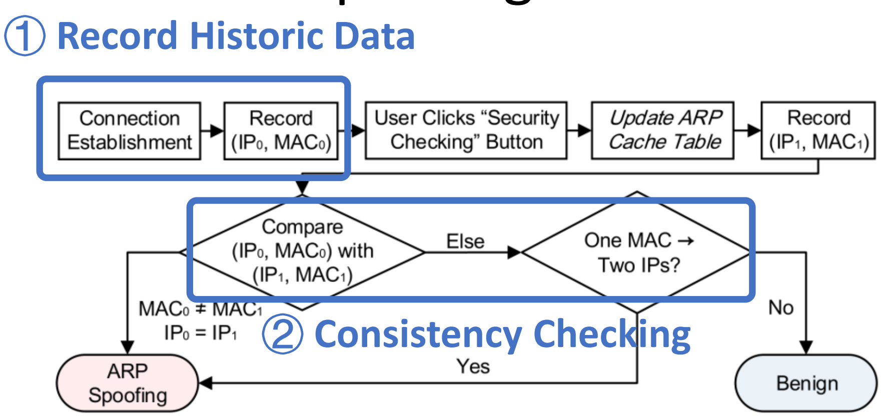
System Overview: A Two-Stage Pipeline

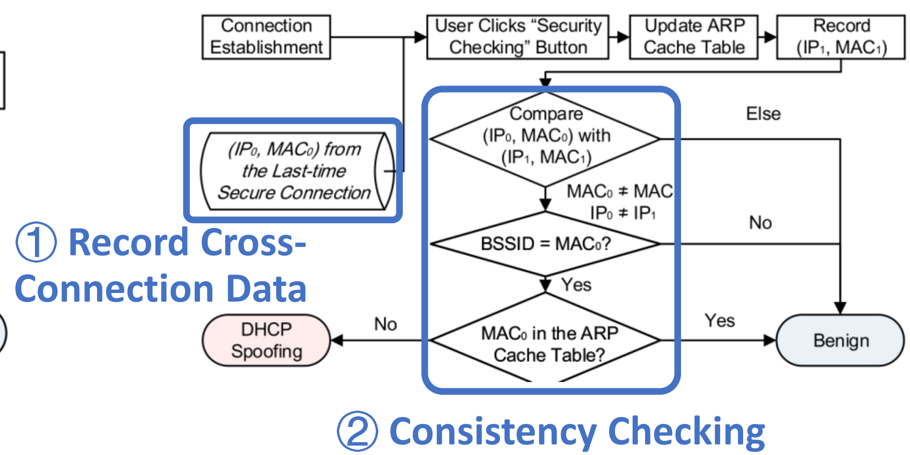


2.3 LAN Attack Detection

Cross-Connection Gateway-Consistency Detection

- Threat model: ARP spoofing and DHCP spoofing
- Broadcast **ARP Requests** to retrieve LAN info & configurations
- Run consistency checking with **cross-connection & historic data**
- ARP Spoofing Detection
- DHCP Spoofing Detection



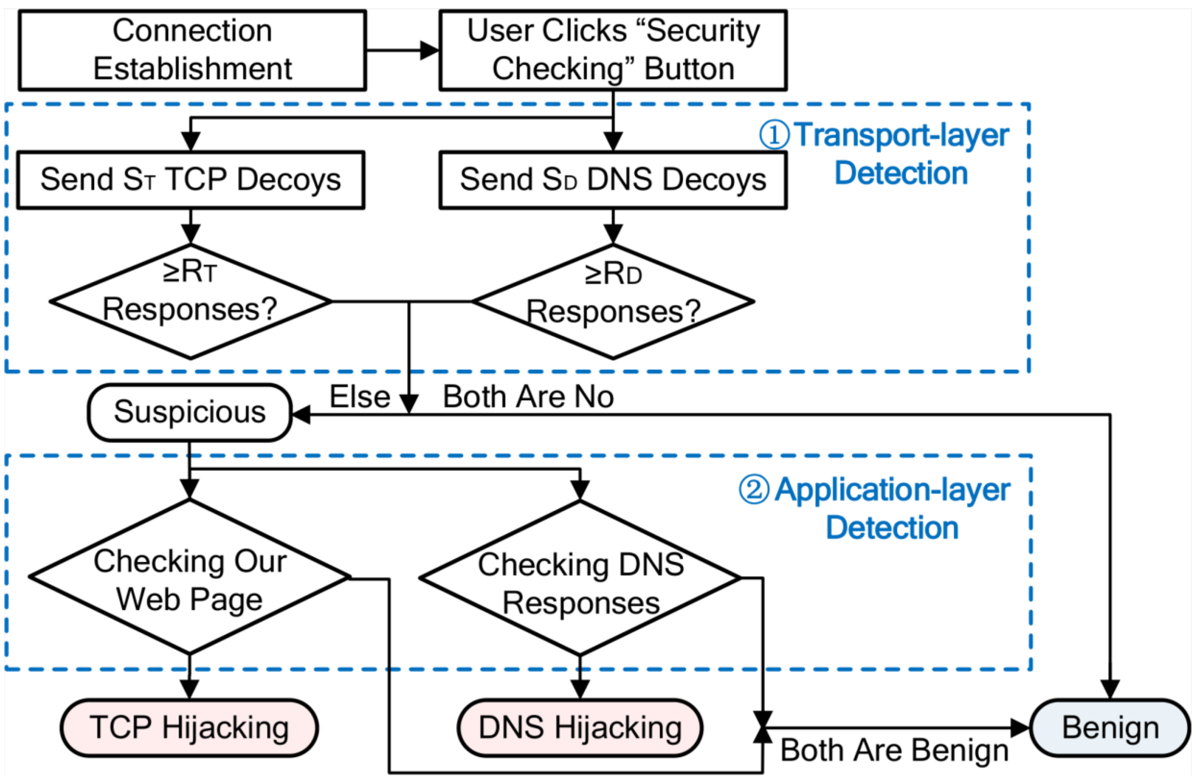


Rule out various false positives that traditional methods may fall into

2.4 WAN Attack Detection

☐ Cross-Layer Decoy-Based Detection

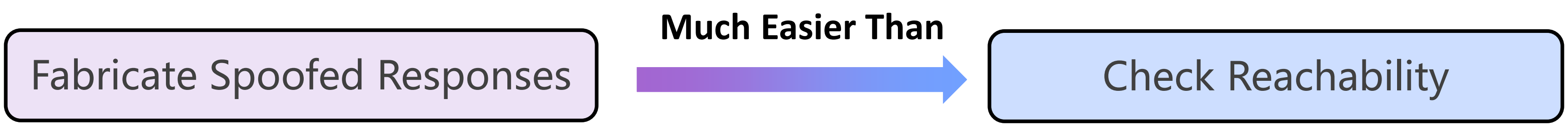
- Thread Model: TCP hijacking and DNS hijacking
- Transport-layer detection & application-layer detection



2.4 WAN Attack Detection

☐ Transport-Layer Detection

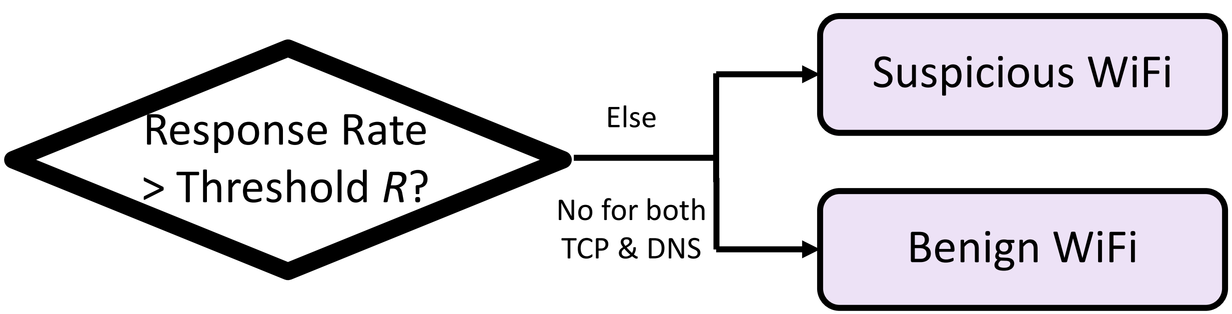
- Key insight: even packets with **unreachable destination IP addresses** are highly likely to trigger the hijacking behavior



Packets with unreachable destination IP addresses

- Send decoy packets to the WiFi AP and check response rate

Carrying web-like TCP/DNS traffic

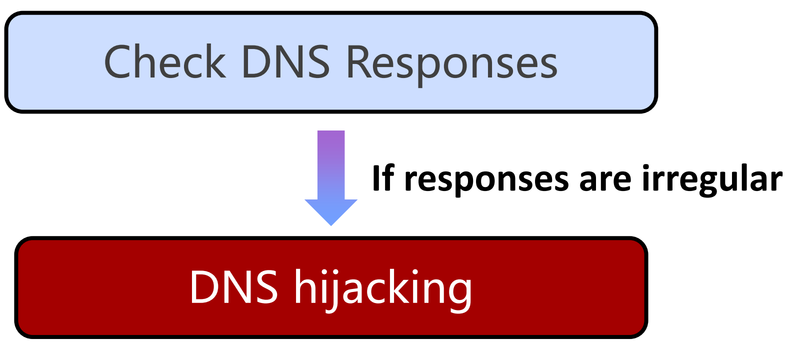


- Threshold *R* is determined with data-driven statistical modeling

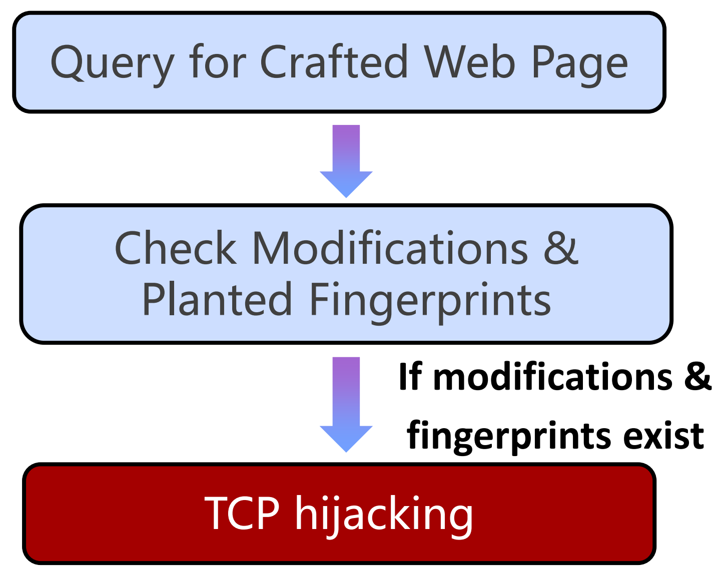
2.4 WAN Attack Detection

Application-Layer Detection

- For the APs deemed as suspicious by transport-layer detection
- Rule out false positives such as ISPs' DNS interception
- DNS hijacking detection



- TCP hijacking detection



2.5 Real-World Deployment

- We implement WiSC as an optional function of WiFiManager
- Users can opt in by clicking the "Security Checking" button
- Period: From 10/22/2018 to 04/03/2019 (**6 months**)
- Record a total of **14M opt-in users** and **19M WiFi APs**
- Involve 178 countries/regions, mostly located in China

Outline

1. Background

2. Methodology

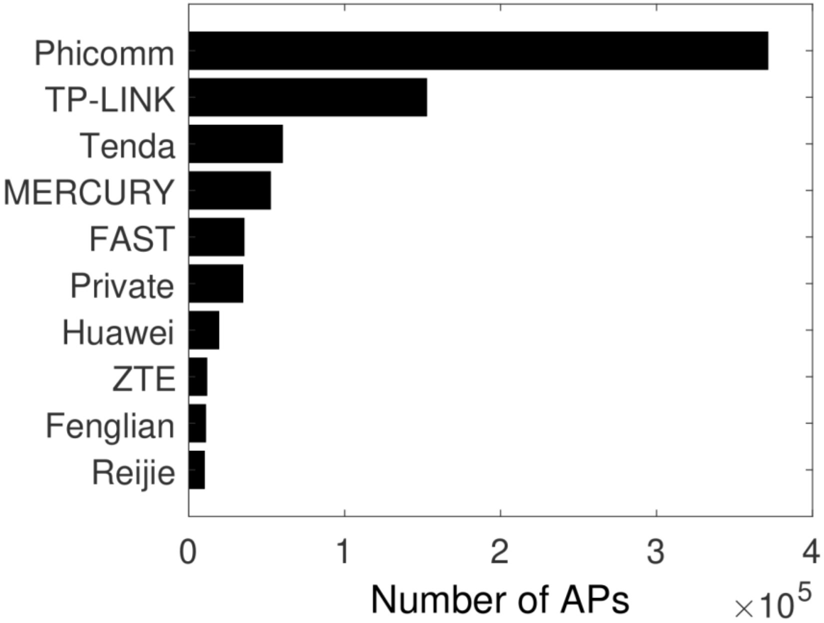
3. Key Findings

4. Attack Ecosystem

5. Summary

3.1 Prevalence of Attack

- Attacks are detected on **3.92%** of the APs (1.5% in previous study)
- Among all the malicious APs, top 10 brands account for 98.48%
- Some countries exhibit even higher prevalence of attacks than China



Country	# of APs	Prevalence	Major Attack Technique
China	19,119,764	3.92%	TCP hijacking (57.6%)
Burma	7148	4.48%	TCP hijacking (53.1%)
Vietnam	4288	1.8%	DHCP spoofing (40.2%)
Russia	3169	8.93%	DNS hijacking (43.8%)
South Korea	2701	2.07%	ARP spoofing (91.1%)
Cambodia	2213	2.17%	ARP spoofing (47.9%)
Laos	1530	1.05%	DHCP spoofing (43.7%)
Thailand	1350	4.15%	DNS hijacking (53.5%)
Malaysia	1317	2.89%	DNS hijacking (44.7%)
Japan	1315	2.59%	ARP spoofing (67.6%)
Singapore	1133	1.5%	ARP spoofing (50%)
Philippines	840	2.86%	DNS hijacking (45.8%)
Indonesia	796	22.36%	TCP hijacking (91%)
United States	608	1.01%	ARP spoofing (66.6%)
Pakistan	523	1.53%	ARP Spoofing (62.5%)

3.2 Attack Techniques (WAN)

Attack Techniques	Ratio
TCP Hijacking	**57%**
DNS Hijacking	17%
ARP Spoofing	16%
DHCP Spoofing	12%

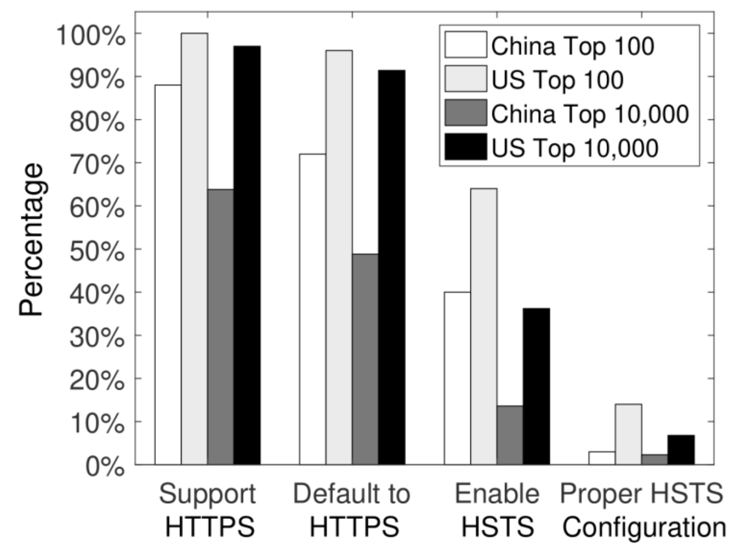
- TCP hijacking accounts for 57% of attacks

Why is TCP hijacking still rampant when there is HTTPS?

- We measure HTTPS deployment for top Alexa ranking sites

A staggering lack of effective HTTPS adoption!

- Quite a few do not use HTTPS by default
- **60% China & 36% US** top 100 sites do not enable HSTS
- **92.5% China & 78.1% US** top 100 sites do not properly configure HSTS

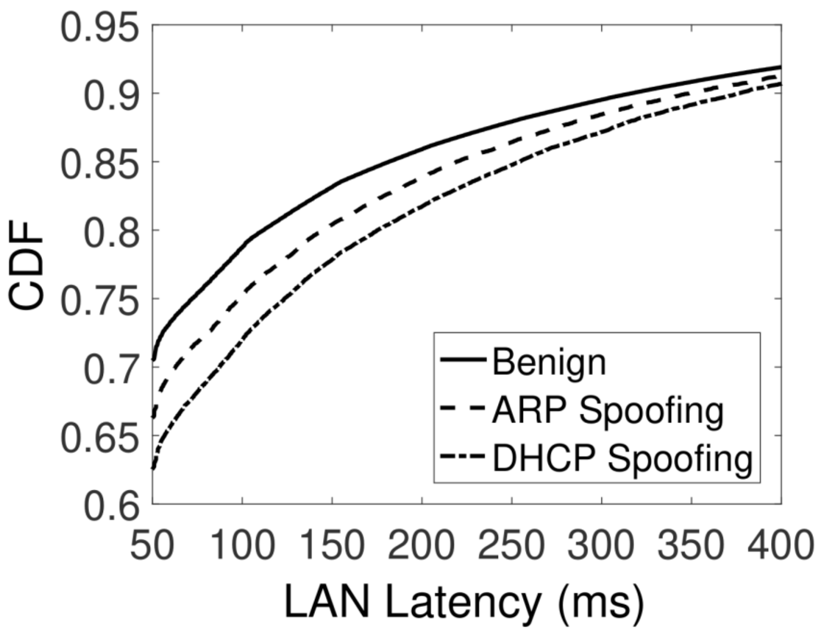


3.3 Attack Techniques (LAN)

Attack Techniques	Ratio
TCP Hijacking	57%
DNS Hijacking	17%
ARP Spoofing	16%
DHCP Spoofing	**12%**

- DHCP spoofing was previously hypothetical
- We make real-world observations of DHCP spoofing
- Spoofing is more detected on APs with poorer LAN connectivity
- Poor LAN environment can slow down legitimate responses' delivery

Adversaries may adopt response flooding to increase success rate



3.4 Malicious Behaviors & Objectives

- **55%** of the attacks involve **web pages being injected with ads**
- 26% are typical **DoS and passive traffic monitoring** by spoofing
- Potential phishing attacks through DNS hijacking
- HTTPS-targeted attacks such as SSLStrip are identified

} < 8%

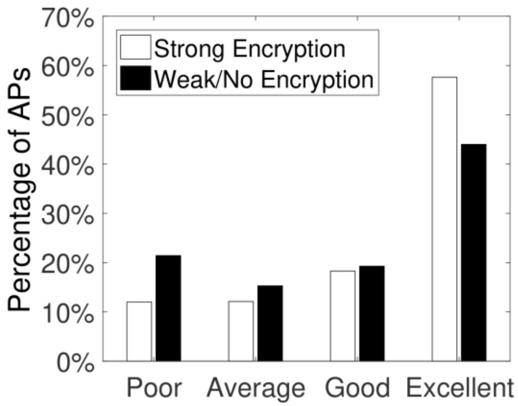
- Ad injection is detected on

Better encryption seems to aggravate the problem?

2.33% APs with strong encryption (WPA/WPA2) ⟷ 1% APs with no or weak encryption (WEP)

- Strong encryption leads to better Internet connectivity, and thus higher success rate

Solely relying on link-layer cryptography may not suffice

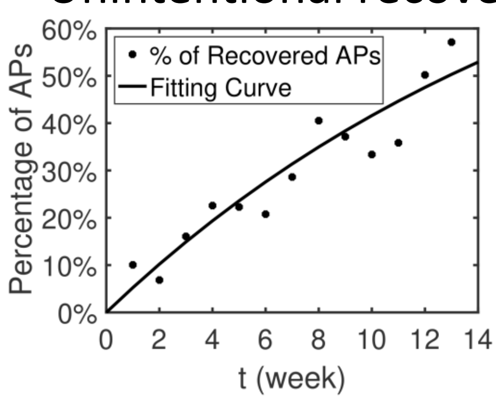


3.5 Fundamental Motives of Ad Injection

- Evasive techniques are adopted (domain altering, code obfuscation)
- **A malicious AP does not compromise all intercepted web pages!**
- We analytically model the economy behind ad-injection attacks

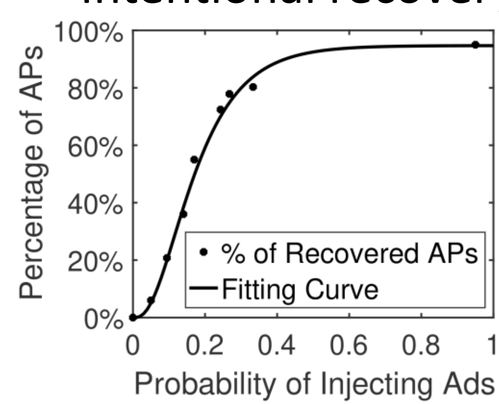
Ad injection probability P_{ad} ⟷ ? ⟷ Ad injection profit $Profit(P_{ad})$

- Key insight: malicious APs can gradually recover over time
  - Unintentional recovery



$$\mathbb{P}_F(t) = 1 - e^{-0.054t}$$

  - Intentional recovery



$$\mathbb{P}_L(P_{ad}) = 0.95 * (1 - 1.99e^{-10.12P_{ad}-0.67})^3$$

3.5 Fundamental Motives of Ad Injection

- With the recovery probability of malicious APs:

Recovery probability → Number of malicious APs → Estimated profit

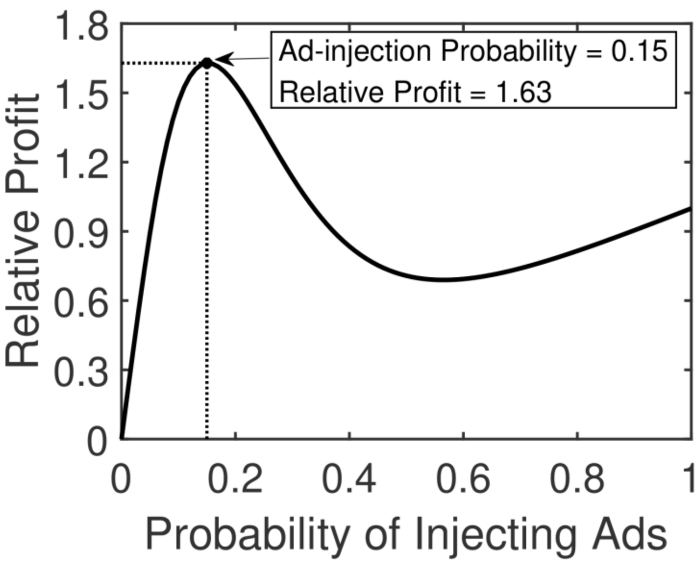
- Estimated profit

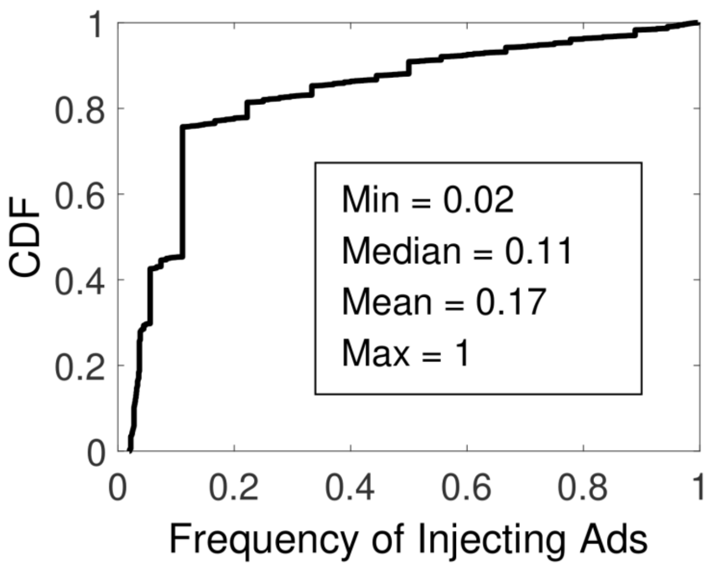
Maximized at P_{ad} = **0.15**

Very close!

- Actual injection probability

Averaging at P_{ad} = **0.17**





Adversaries may have carefully tuned their behaviors to achieve maximum profit in the long run

Outline

1. Background

2. Methodology

3. Key Findings

4. Attack Ecosystem

5. Summary

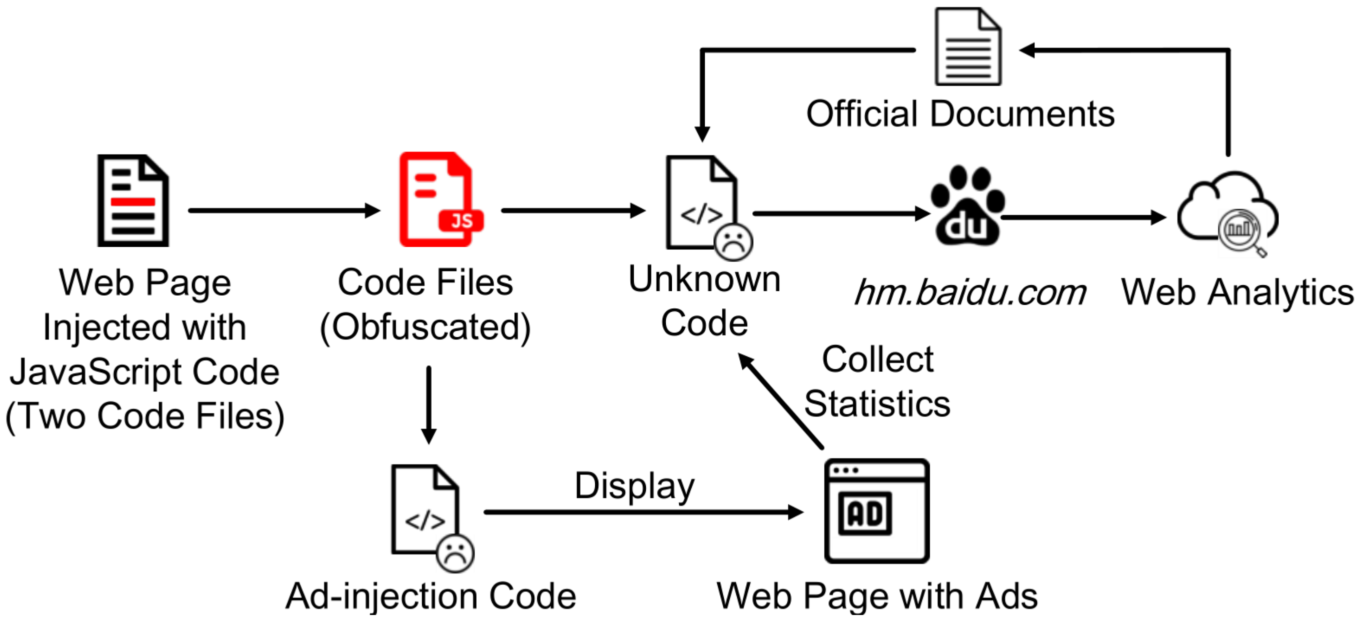
4.1 Uncovering the Ecosystem

- We examine adversaries’ code inserted into the web page
- Injection code consists of two components

e.g., hm.baidu.com
Web analytics service!

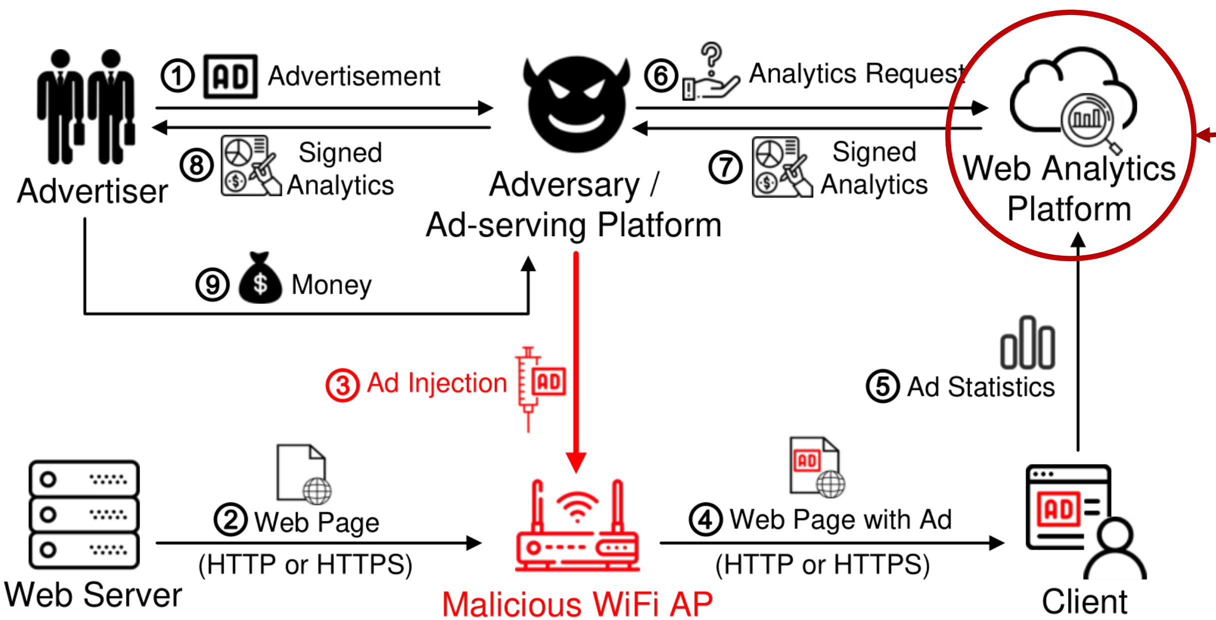
  - Code for injecting ads
  - **Code from legitimate domains?**

Adversaries use web analytics service to prove their advertising effects!



4.1 Uncovering the Ecosystem

- Adversaries act as ad-serving platforms
- Advertisers outsource advertising to these platforms
- Ad-serving platforms inject ads through malicious APs
- **Ad-serving platforms prove advertising effects to advertisers**



Done through legitimate analytics services

4.2 Undermining the Ecosystem

- Adversaries heavily rely on web analytics platforms for monetization
- Web analytics platforms are **the bottleneck of the ecosystem**!
- We have reported our findings to the four identified platforms
- Baidu Analytics stopped serving **67% of the reported ad links**, leading to **49.8% of decrease** of ad injections as of August 2020

Adversary	% of All Ads	Entity We Report to
t.7gg.cc	35.8%	Baidu Analytics
5myr.cn	8.9%	OeeBee
agtsjb.com	8.7%	UMeng/Adblock Plus
103.49.209.27	1.2%	360zlzq/Adblock Plus
withad.com	0.4%	UMeng/Adblock Plus
zfkmw.com	0.3%	UMeng/Adblock Plus
js.union-wifi.com	0.06%	360zlzq/Adblock Plus
172.81.246.180	0.05%	360zlzq/Adblock Plus

5 Conclusion

■ We conduct the first large-scale measurement study of WiFi security threats of 19M WiFi APs based on 14M end user devices.

■ We present a lightweight WiFi threat detection system called WiSC that takes advantage of active probing and cross-layer information.

■ We comprehensively analyze WiFi attacks in the wild, the adversaries' profit-driven motives, the WiFi attack ecosystem.

■ We discover that the web analytics platforms are the bottleneck of the underground economy and leverage it to effectively combat the preponderant ad injection attacks at the national scale.