SIPConfusion: Exploiting SIP Semantic Ambiguities for Caller ID and SMS Spoofing

Qi Wang, Jianjun Chen, Jingcheng Yang, Jiahe Zhang, Yaru Yang, Haixin Duan

What is Session Initiation Protocol (SIP)?

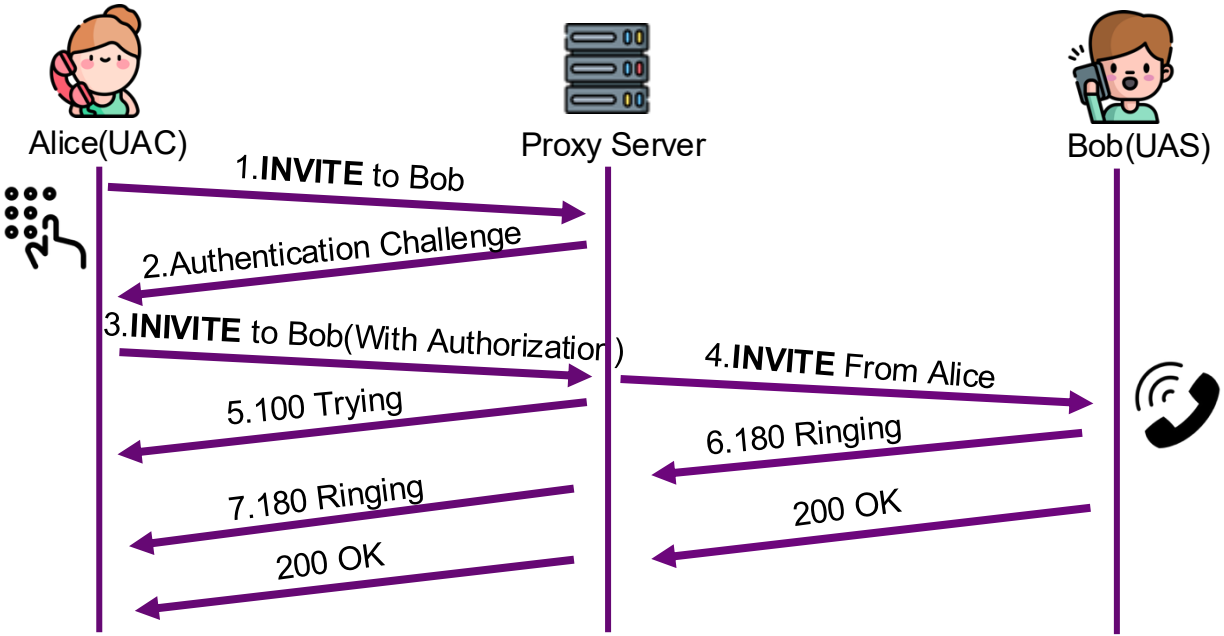
- The backbone of Modern Communication System
  - Powers nearly every business call, video conference, and message used today.
  - Coordinating the session behind the scenes.

$326.27B*

VoIP Market share Across the World By 2032

*: https://www.fortunebusinessinsights.com/voice-over-internet-protocol-voip-market-110830

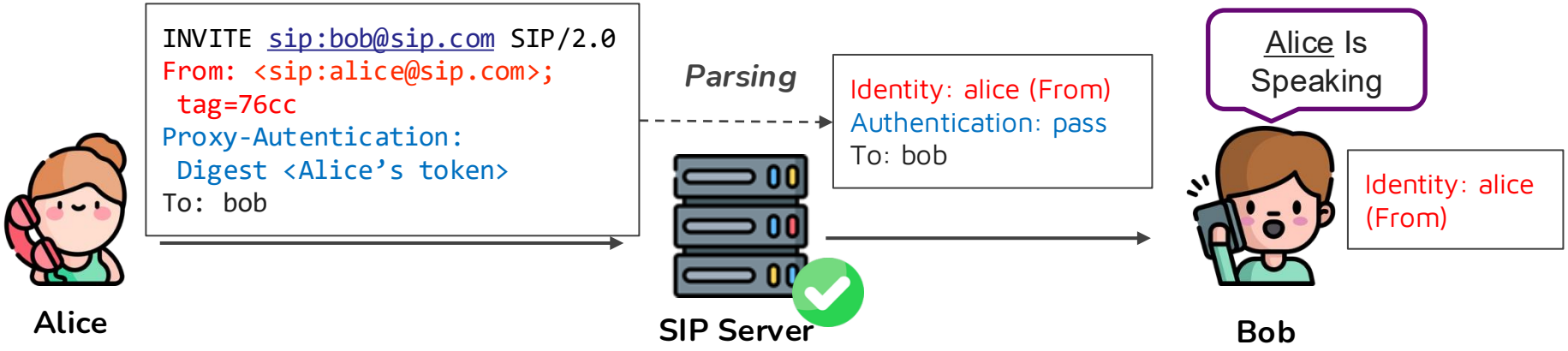
What Happens When Alice Calls Bob?



- Three Stage:
  - **Initiate call session**
  - **Authenticate call invitation**
  - **Deliver message to UAS**

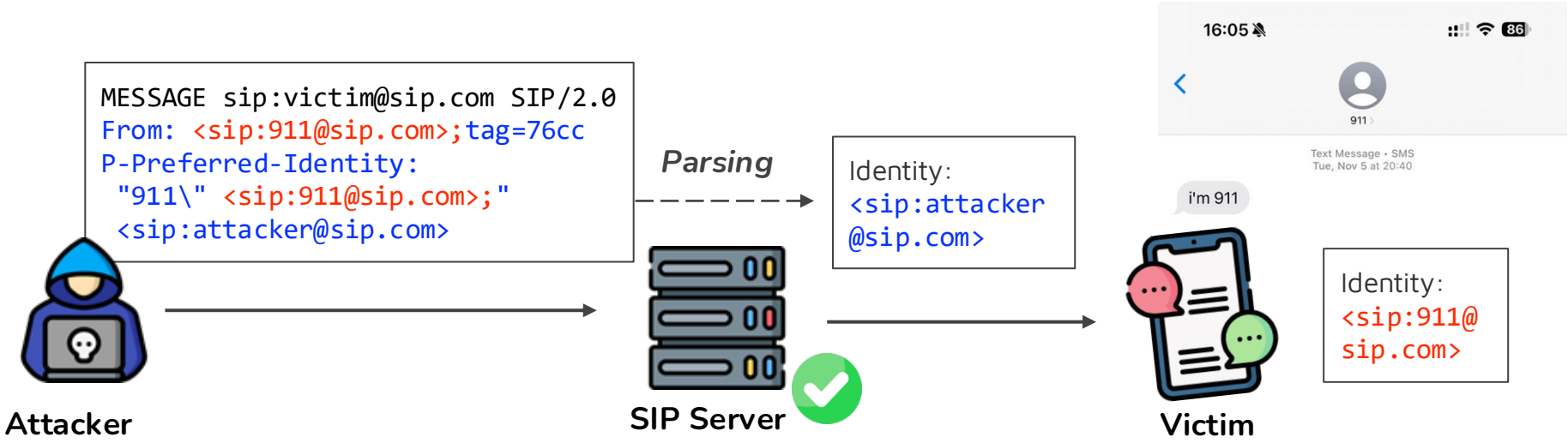
How Bob Knows It's Alice?

- Alice represent her identity with the identity header (From)
- SIP Server check whether the identity match with the authentication
- Bob's Phone show the caller **according to the identity header (From)**



How SIPConfusion Spoofs Caller Identity

- Different Implementation always had different point of view
- Victim devices may have inconsistent understanding of callers' identity
- Despite rigorous server-side checks, the client lacks equivalent validation



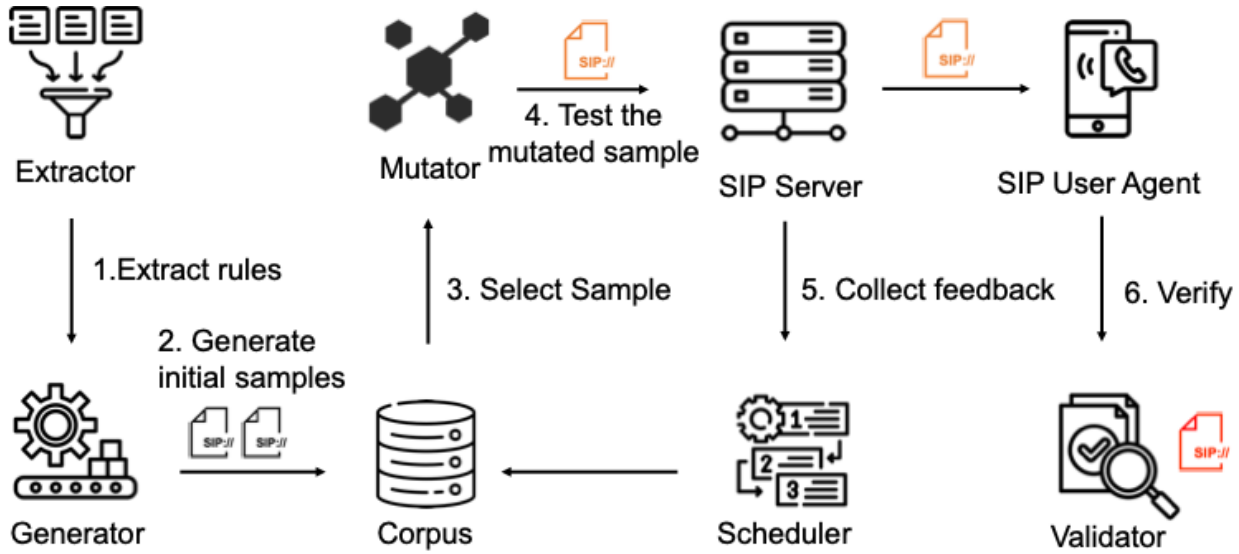
Our Motivation & Goals

- SIPConfusion attack has been rarely discussed and systematically studied.

- RQ1: How to **systematically identify** SIPConfusion in SIP implementations?
- RQ2: What **types of** SIPConfusion exist, and what is their **prevalence**?
- RQ3: What are the **real-world security implications** of SIPConfusion?

SIPChimera: Automated fuzzing Framework

- **Grammar-Guided Fuzzing:** Maximizes spec coverage with rule-based generation.
- **Spoofing Validator:** Identifies forgeries by analyzing authentic sender history.
- **Feedback-Driven Iteration:** Refines test cases using real-time server responses.



https://github.com/EkiXu/SIPChimera

Evaluation Setup

- **6** SIP Proxy Servers
  - Covers nearly all common open-source servers
- **9** SIP User Agent:
  - Popular Choices according SIP service provider rank list*
- **3** Controlled Account:
  - Admin account: send probe message
  - Victim account: receive probe/forgery message
  - Attacker account: send forgery message
    - Classified as unauthenticated attacks when authentication not trigged

TABLE I: Tested Open-source SIP Proxy Servers.

#	Name	Version	Github Stars (2025.3)
1	ejabberd[24]	24.12	6.2k
2	FreeSwitch[25]	1.10.12	3.9k
3	Asterisk[26]	22.1.1	2.4k
4	Kamailio[27]	6.0.1	2.4k
5	Opensips[28]	3.4.1	1.3k
6	Flexisip[29]	2.4.0	160

TABLE II: Tested SIP User Agents

#	Name	Version
1	Zoiper[30]	5.6.6
2	Linphone[31]	5.2.6
3	MircoSIP[32]	3.21.5
4	MizuPhone[33]	4.0.24061.97
5	Jitsi[34]	2.10.5550
6	Jami[35]	latest stable (20250304)
7	Empathy[36]	3.25.90
8	Twinkle[37]	1.10.2
9	Blink[38]	5.9.1

*VoIP.ms, “Softphones,” https://wiki.voip.ms/article/Softphones

Evaluation Result

- Most servers ensure identity headers match authenticated credentials.
  - **But Still vulnerable to SIPConfusion attacks**
- Half servers forward external domain traffic without challenges.
  - **Attacker could forgery identity even without credentials**

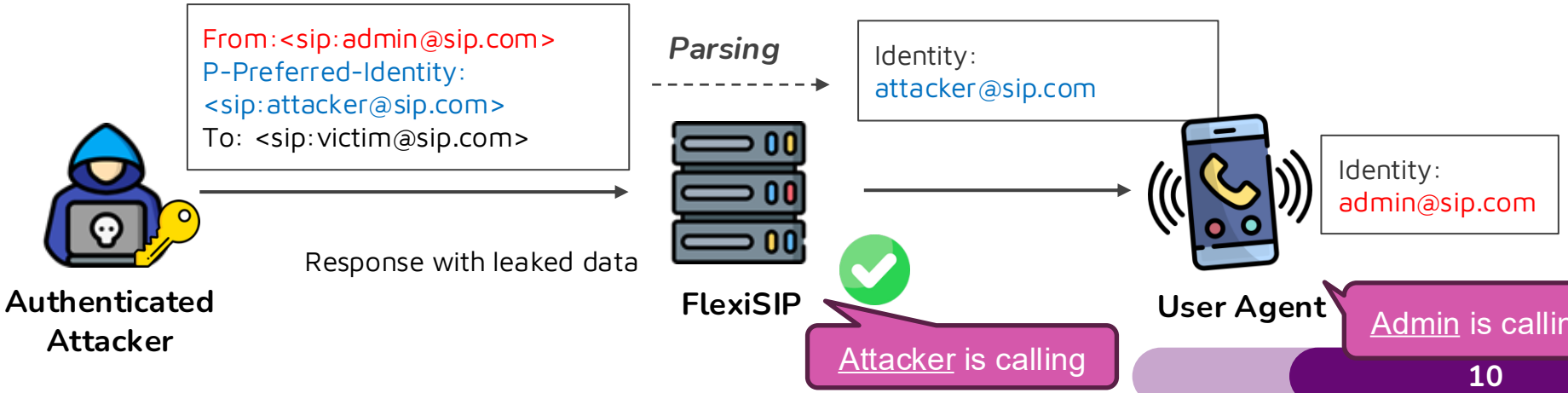
TABLE III: Spoofing Vulnerabilities between open-source SIP servers and SIP user agents.

User Agents	Method	Asterisk	FreeSWITCH	Kamailio	OpenSIPS	ejabberd	Flexisip
Linphone	INVITE						A_4
	MESSAGE	$B_{1,2}$	Not Aligned				A_4
Zoiper	INVITE			$A_{1,2}, D_{1,2}$	$A_{1,2}, C_1, D_{1,2}$	$A_{1,2}, C_1, D_{1,2}$	$A_{1,2,4}$
	MESSAGE	$B_{1,2}$	Not Aligned		$C_{1,3,4}$	C_1	A_4
Jami	INVITE				A_3, C_2, D_3	A_3, C_2, D_3	A_4
	MESSAGE	$B_{1,2}$	Not Aligned	C_2	$A_3, C_{2,3,4}, D_3$	A_3, C_2, D_3	A_4
Jitsi	INVITE						A_4
	MESSAGE	$B_{1,2}$	Not Aligned		C_3		A_4
MicroSIP	INVITE	B_3			A_3, D_3	A_3, D_3	A_4
	MESSAGE	$B_{1,2}$	Not Aligned	B_3	A_3, B_3, C_3, D_3	$A_3, B3, D_3$	A_4
Blink	INVITE				A_3, D_3	A_3, D_3	A_4
	MESSAGE	$B_{1,2}$	Not Aligned		C_4		A_4
MizuPhone	INVITE	B_3		B_3	B_3, C_1	B_3, C_1	A_4
	MESSAGE	$B_{1,2}$	Not Aligned	B_3	$B_3, C_{1,3,4}$	B_3, C_1	A_4
Empathy	INVITE				C_1	C_1	A_4
	MESSAGE	$B_{1,2}$	Not Aligned		C_1	C_1	A_4
Twinkle	INVITE				A_3, D_3	A_3, D_3	A_4
	MESSAGE	$B_{1,2}$	Not Aligned	C_2	C_2	C_2	A_4

1.Affected web framework indicates the influence of all bypass use cases for corresponding WAF

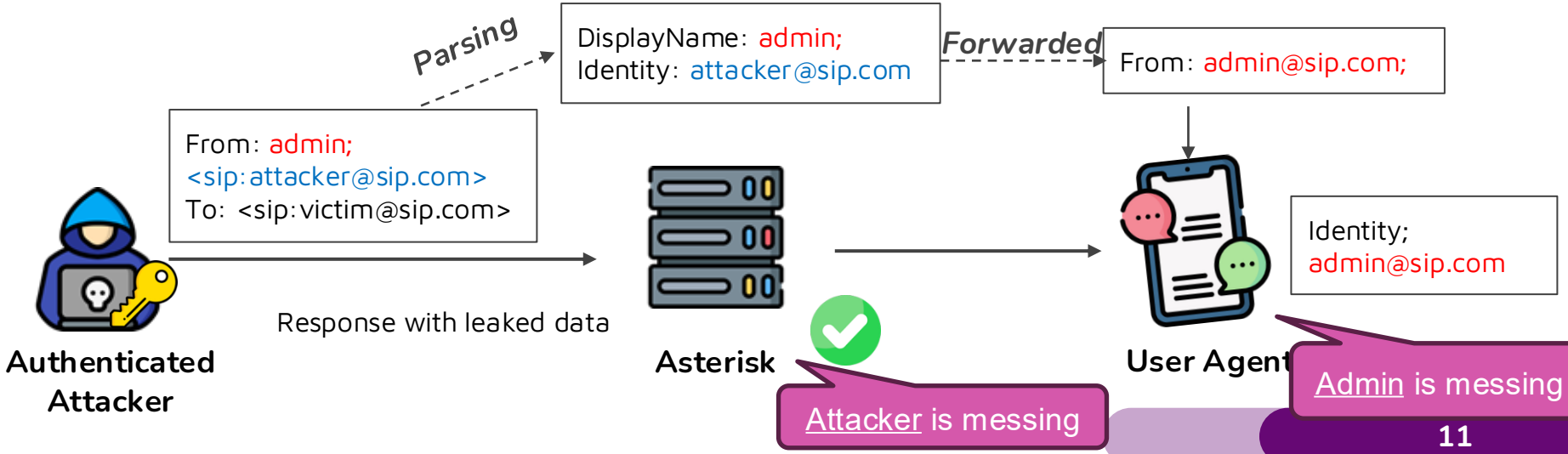
A: Identity Header Mismatch

- Multiple identity headers in standards causing the chaos
- **Case A4: P-Preferred-Identity Header Preferred Attack.**
  - FlexiSIP authenticates users using the P-Preferred-Identity header
  - The From header is not cross-validated against the authenticated identity
  - The client-controlled From header is still propagated to the callee



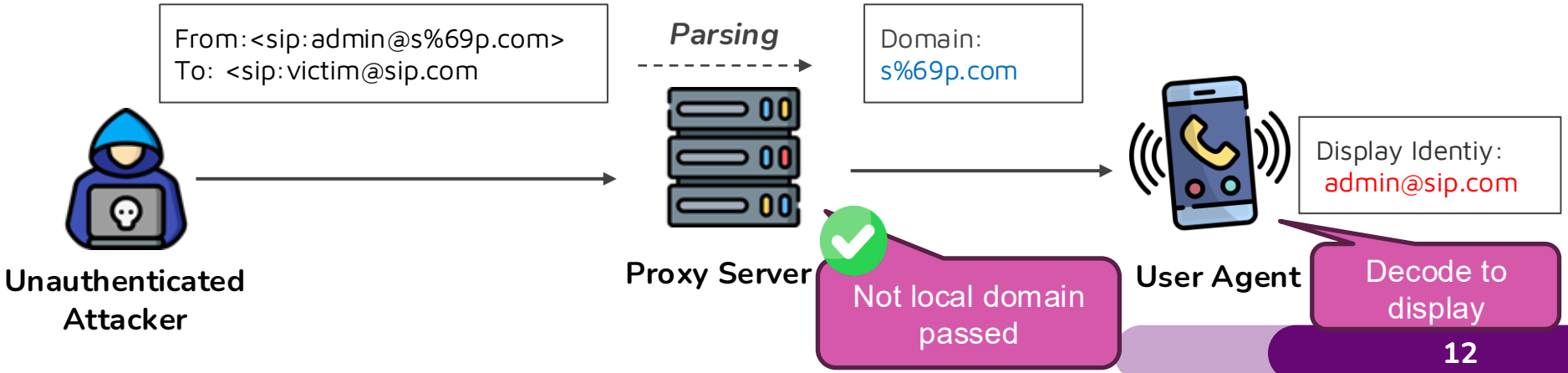
B: Malformed Identity Header

- The Complex Header component led to a potential parsing vulnerability
- **Case B1: Semicolon Truncation Attack.**
  - Semicolons are used to separate parameters in the header, but are treated as a display name
  - Unfortunately, Asterisk truncated the semicolon and rewrote the forgery of the identity



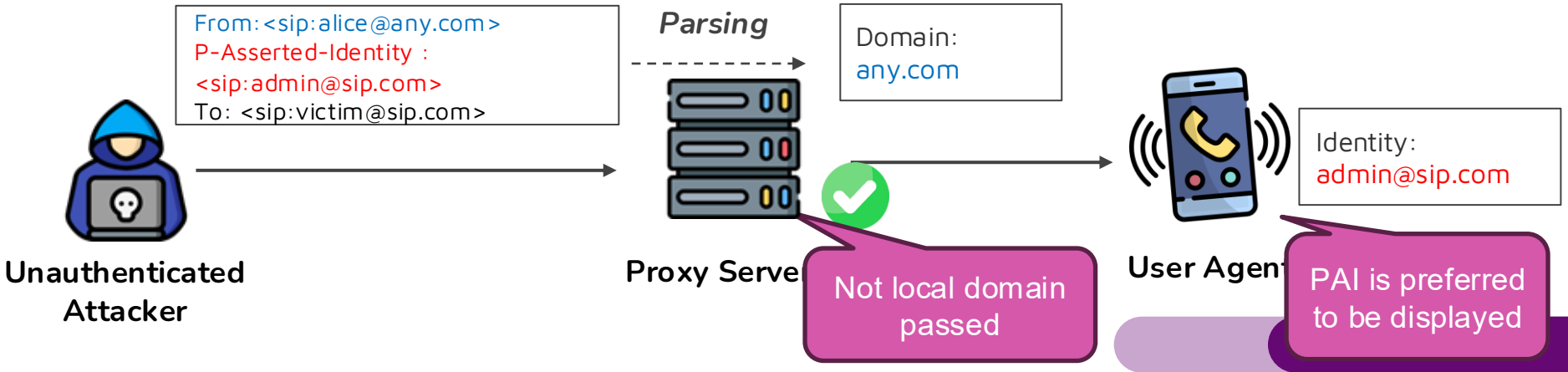
C: Domain Confusion

- SIP proxies may accept requests from non-local domains without authentication
- **Case C1: Domain Encoding Confusion Attack**
  - RFC 3261 adopts the %HEXHEX escaping mechanism, but only in the “username”
  - Some User agents fail to enforce this constraint and accidentally decode the domain



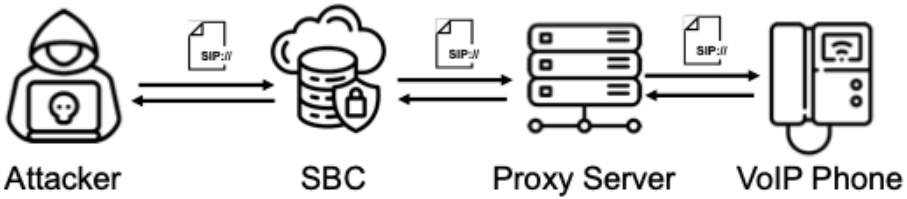
D: Header Smuggling

- Overlapping identity header standards cause inconsistent processing,
  - Enabling attackers to smuggle extra headers and bypass security checks.
- **Case D1: P-Asserted-Identity Header Smuggling Attack**
  - Using external "From" domains to bypass proxy checks and inject forged PAI headers.
  - Smuggled the P-Asserted-Identity header exploit user agents that prioritize to show PAI.



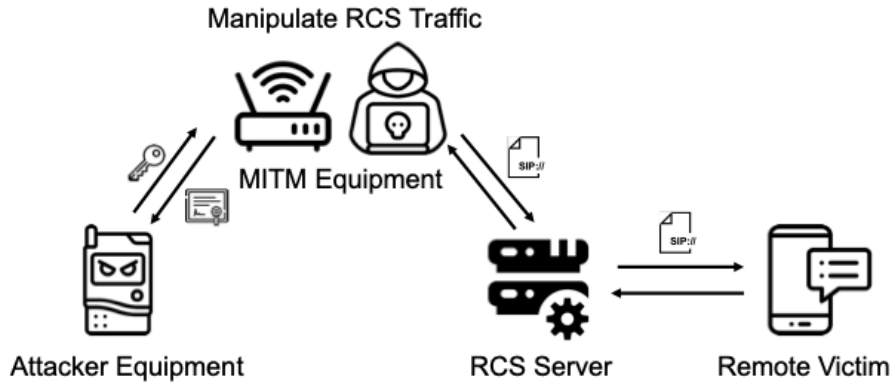
Real World Impact

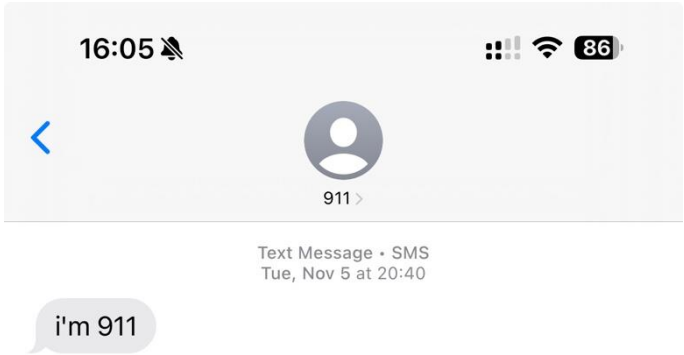
- We deployed mocked VoIP systems in our lab to test hardware.
  - All the VoIP devices are vulnerable to SIPConfusion attacks to some extent.
  - Including Yealink, Motorola and Polycom
  - Attacker could dial IP Phones with forgery identity



Real World Impact

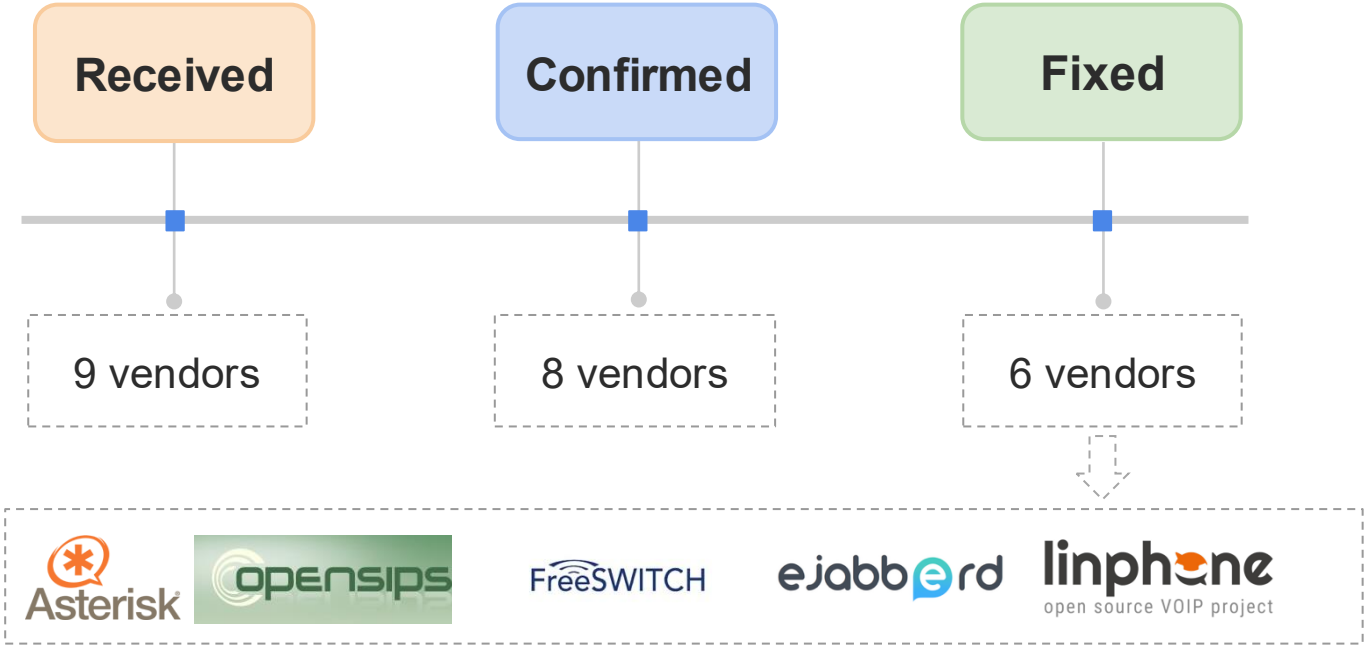
- Over 1 billion users globally utilize RCS for their daily conversations
  - All three operators will reject the naïve spoofing messages
  - While SIPConfusion attack still works.
  - Spoofed message is still delivered via traditional SMS.





Responsible Disclosure

- Response from affected Vendors



Conclusion

- **New Spoofing Tactics: SIPConfusion**
  - Leverage semantic gaps and destroy the trust boundary
- **New testing framework: SIPChimera**
  - Automated fuzzing of inconsistency vulnerabilities between SIP Server and UA.
- **New Findings:**
  - Find vulnerabilities across mainstream SIP Server and UA
  - Present real-world case studies in production VoIP and RCS-based SMS

Thank you for listening!

For more details, welcome to follow our paper

SIPConfusion: Exploiting SIP Semantic Ambiguities for Caller ID and SMS Spoofing

Qi Wang*, Jianjun Chen*✉, Jingcheng Yang*, Jiahe Zhang*, Yaru Yang*, Haixin Duan*
* Tsinghua University

***Abstract*—Session Initiation Protocol (SIP) is a cornerstone of modern real-time communication systems, powering voice calls, text messaging, and multimedia sessions across services such as VoIP, VoLTE, and RCS. While SIP provides mechanisms for authentication and identity assertion, its inherent flexibility poses the risk of semantic ambiguity among implementations that can be exploited by attackers.**

In this paper, we present SIPCHIMERA, a novel black-box fuzzing framework designed to systematically identify ambiguity-based identity spoofing vulnerabilities across SIP implementations. We evaluated SIPCHIMERA against six widely used open-source SIP servers—including Asterisk and OpenSIPS—and nine popular user agents, uncovering that attackers could spoof their identity via manipulating identity headers and circumvent authentication. We demonstrate the real-world impact of these vulnerabilities by evaluating five VoIP devices, seven commercial SIP deployments, and three carrier-grade RCS-based SMS platforms. Our experiments show that attackers can exploit these vulnerabilities to perform caller ID spoofing in VoIP calls and send spoofed SMS messages over RCS, impersonating arbitrary users or services. We have responsibly disclosed our findings to affected vendors and received positive acknowledgments. We finally propose remedies to mitigate those issues.

I. INTRODUCTION

Session Initiation Protocol (SIP) is a critical component for modern communication systems. It is the signaling standard

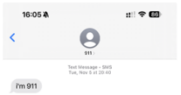


Fig. 1: A real-world example of SMS spoofing that impersonates 911 by exploiting SIP semantic ambiguities.

developed various mechanisms, such as authentication and identity assertion, to mitigate such attacks[3], [4], [5]. Both industry and regulators have rolled out countermeasures such as the STIR/SHAKEN framework, which enforces cryptographic signing of caller identities using public key infrastructure (PKI) [6]. These developments have significantly raised the bar for traditional spoofing techniques, rendering traditional methods, such as simply modifying the caller ID number, ineffective in practice.

In recent years, increasing attention has been directed toward semantic ambiguities—subtle inconsistencies among implementations that can be exploited by attackers [7], [8]. These attacks arise not from the absence of security features, but from discrepancies in interpretation. An attacker can craft malicious