eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem

Maryam Motallebighomi[1], Jason Veara[1], Evangelos Bitsikas[1], and Aanjhan Ranganathan[1]

[1]Northeastern University, Boston, USA

Abstract

eSIM (Embedded Subscriber Identity Module) technology is rapidly reshaping mobile connectivity by enabling users to activate cellular services without a physical SIM card. While the flexibility of remote provisioning improves convenience and scalability, particularly for international travelers, it also introduces complex and underexplored privacy and security risks. This paper presents an empirical investigation of how eSIM adoption affects user privacy, focusing on routing transparency, reseller access, and profile control. We first show how travel eSIMs often route user data through third-party networks, including Chinese infrastructure, regardless of user location. This raises concerns about jurisdictional exposure. Second, we analyze the implications of opaque provisioning workflows, documenting how resellers can access sensitive user data, proactively communicate with devices, and assign public IPs without user awareness. Third, we validate operational risks such as deletion failures and profile lock-in using a private LTE testbed. In addition to these empirical contributions, we reflect on the evolving threat landscape of eSIM technology and analyze the shifting trust boundaries introduced by its global provisioning architecture. We conclude with actionable recommendations for improving eSIM transparency, user control, and regulatory enforcement as the technology becomes widespread across smartphones, IoT deployments, and private networks.

1 Introduction

eSIM technology is redefining how devices connect to cellular networks. Unlike traditional SIM cards, which require physical distribution and manual activation, eSIMs are embedded into hardware and enable remote provisioning of cellular profiles. This shift simplifies connectivity for mobile phones, wearables, and IoT devices and is rapidly gaining traction. eSIM adoption is accelerating, with GSMA projecting that 50% of all smartphones will be eSIM-enabled by 2028 [75, 77]. The launch of eSIM-only devices, such as the iPhone 14 in the US, reflects this industry shift. A key driver of this adoption is the enhanced flexibility, convenience, and scalability of remote SIM provisioning (RSP). This adoption is enabled by GSMA's Remote SIM Provisioning (RSP) architecture [70], which allows eSIM profiles to be downloaded and activated over the air. Unlike physical SIMs, which often require in-person activation, travel eSIMs can usually be purchased and installed online. This has fueled a global marketplace of online eSIM resellers [54], operating across borders with minimal regulatory oversight. These services are typically marketed through web stores and mobile apps, with providers operating across borders and often facing minimal regulatory oversight.

While this flexibility simplifies mobile connectivity, it also introduces new privacy and security risks. First, many travel eSIMs route user traffic through third-party infrastructure, often located in foreign jurisdictions. This may expose user metadata and content to networks outside the user's country, raising concerns about jurisdictional control and surveillance. Second, the ease of online distribution lowers the barrier for unregulated or opaque eSIM providers to enter the market. These entities may access sensitive user data or offer features such as remote provisioning or static IP assignment without clear user awareness or consent. Third, eSIM profile management is often abstracted away by mobile platforms, leaving users with limited visibility or control. Users may be unaware of whether a profile remains active or whether deletion was successful—especially when offline or in edge-case states. Fourth, the digital provisioning model creates new opportunities for phishing and spoofing. Malicious actors can distribute fake eSIM profiles via fraudulent QR codes or websites, tricking users into installing unauthorized configurations. Finally, the adoption of eSIMs in private networks (e.g., hospitals and industrial settings), introduces additional risk. These deployments rely on local infrastructure and administrative policies, which may not follow operator-grade security practices.

In this paper, we explore how the design and deployment of eSIMs reshape traditional trust boundaries and expand the mobile attack surface. We identify where risks are amplified

by architectural shifts, and where new vulnerabilities emerge due to provisioning complexity, lack of transparency, or inconsistent enforcement of user control. Specifically, we make the following contributions:

- **Routing and jurisdictional exposure analysis.** We analyze IP assignment and traceroute paths from dozens of travel eSIM profiles and find that user traffic is frequently routed through foreign networks, including those operated by Chinese and European telecom providers. This occurs even when the user is physically located in the United States, raising concerns about surveillance, location inference, and access to region-locked services.
- **Reseller ecosystem evaluation.** We analyze multiple eSIM reseller platforms and their management dashboards, documenting the types of sensitive operations exposed to unregulated entities including metadata access (EIDs, ICCIDs), lifecycle controls, static IPs, and remote management.
- **Proactive communication and silent behavior.** Using a programmable eUICC (sysmoEUICC1) and SIMtrace2 hardware interface, we observe proactive STK behavior in live travel eSIMs. We capture silent open/send/close data sessions and unsolicited SMS retrieval initiated by profiles, demonstrating user-invisible communication embedded in the provisioning layer.
- **Profile lifecycle failure modes.** Through controlled experiments using a private LTE testbed and commercial SM-DP+ infrastructure, we demonstrate that profile deletions may silently fail when devices are offline. As a result, users are unable to reinstall the same profile, creating denial-of-service-like behavior that can only be resolved through manual intervention.
- **Risks in private eSIM-based networks.** We explore the eSIM's use in private LTE/5G environments and highlight how reduced visibility, permissive profile policies, and local administrator access may introduce additional risks. These risks stem from control redistribution in custom deployments, not the eSIM technology itself.

To support transparency and reproducibility, we will release all datasets and captured logs on GitHub upon publication. This includes eSIM installation traces, deletion logs, and network traffic collected during our experiments.

2 eSIM Architecture and Threat Landscape

2.1 Physical SIM vs eSIM

The Subscriber Identity Module (SIM) has evolved significantly from a removable physical chip to an integrated digital solution. Traditional SIM cards are physical chips stored within a Universal Integrated Circuit Card (UICC), a secure hardware module that manages a single SIM profile [76]. While traditional SIMs are portable and require a dedicated SIM slot in devices, their inability to support multiple profiles and reliance on physical handling have driven the development of eSIM technology. An eSIM represents the next generation of SIM technology. Unlike physical SIM cards, an eSIM is a digital version of the SIM that is embedded directly into a device. eUICC (embedded Universal Integrated Circuit Card) is a secure, programmable hardware module integrated into devices such as smartphones, smartwatches, or IoT devices, capable of storing multiple eSIM profiles. Each profile includes its own International Mobile Subscriber Identity (IMSI) and Integrated Circuit Card Identifier (ICCID), allowing the device to connect to different networks without requiring a physical swap [69].

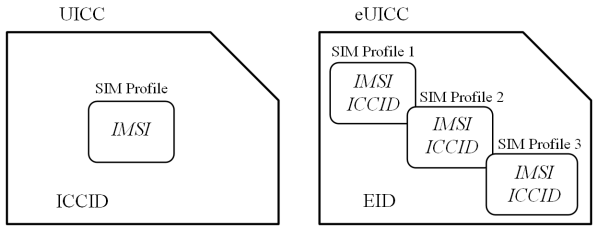

Figure 1: Comparison between the UICC architecture of physical SIM cards and the eUICC architecture of eSIMs

Figure 1 illustrates the structural differences between traditional UICC and eUICC. While a traditional SIM (UICC) contains a single SIM profile limited to one network operator, an eUICC can store multiple SIM profiles, each with its own ICCID and IMSI. This shift enables seamless profile switching, eliminates the need for a physical SIM slot, and supports more compact IoT devices and wearables [95]. To manage multiple profiles within a single eUICC, a unique identifier called the eUICC Identifier (EID) [73] was introduced to provide global traceability and simplify operator management. However, the centralized generation and reliance on global uniqueness introduce privacy concerns if the EID is exposed or misused by malicious entities.

2.2 Remote SIM Provisioning Protocol

RSP is a process that enables eSIM profiles to be remotely installed and managed. Unlike traditional physical SIM cards, which connect to a mobile network upon insertion, an eSIM requires installation and activation to establish connectivity [51]. The RSP process begins when the provider sends a profile order to the Subscription Manager Data Preparation (SM-DP+) server, which prepares the eSIM profile and makes it available for download to the user's device. Users can download eSIM profiles using three methods: scanning a QR code, using the provider's app, or manually entering the server address and ac-

tivation code [5]. Secure communication during this process is ensured by the Local Profile Assistant (LPA) running on the device, which uses TLS protocols to prevent interception. Figure 2 illustrates the RSP architecture, including the roles of the Mobile Network Operator (MNO), the end user's device (UE), the LPA, the eUICC, the SM-DP+ server, and the eUICC Manufacturer (EUM). Trust within the RSP ecosystem is maintained through a hierarchical chain of certificates issued by a GSMA Certificate Issuer (CI). These certificates authenticate SM-DP+ servers and eUICC manufacturers, ensuring a secure provisioning process [57, 68, 72]. The RSP specification assumes that all entities in the ecosystem—including the SM-DP+ server, eUICC, and MNO—are trusted and secure, with robust mechanisms to protect their secret keys. The LPA on the user's device is also trusted not to leak sensitive information. While the RSP protocol is designed to secure communication against network-based adversaries, it assumes all participants are trusted, making certificate management and secure implementation critical to its security.

2.3 eSIM Threat Landscape

2.3.1 Legacy Threats, Amplified

While eSIM technology offers numerous benefits, its implementation introduces several challenges and risks. Some risks are specific to the technical design of eSIMs, while others apply to both traditional SIMs and eSIMs. However, these risks are amplified within the eSIM ecosystem due to features like remote provisioning, reduced user visibility, and introducing opaque intermediaries. As an example, the use of eSIMs has the potential to make SIM swapping easier for an attacker. Unlike physical SIMs, which require possession and deliberate user action, eSIMs can be installed by simply scanning a QR code or tapping a URL sent via SMS. This removes friction, much like QR-based phishing versus manual URL entry, making attacks easier to execute and harder for users to detect or question. While the underlying threats may not be entirely new, the increased feasibility, scalability, and convenience introduced by eSIMs mean that attack scenarios are now more practical and widespread.

Private networks, such as those used in hospitals and warehouses, present unique challenges and opportunities for eSIM technology. However, the trust models in these networks are critical. Mismanagement of eSIM profiles or inadequate provisioning security could allow attackers to intercept communications, track user activity, or disrupt critical operations. The flexibility and scalability of eSIM technology, powered by RSP, have redefined how users connect to mobile networks.

2.3.2 New Actors, New Risks

The issues that apply to both SIMs and eSIMs are further exacerbated due to evolving business models that have introduced new commercial entities into the market. Unlike physical SIM

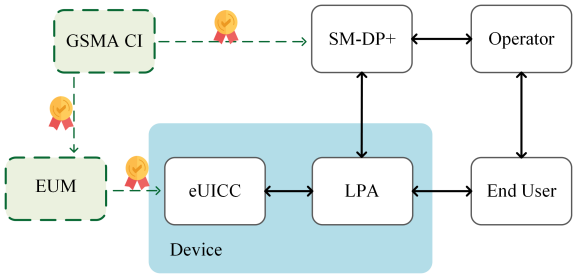

Figure 2: Remote SIM Provisioning System Architecture

cards, where MNOs directly manage connectivity, the rise of eSIMs has led to a significant increase in eSIM resellers and white-label service providers [55]. The travel eSIM industry has change drastically. Airports, travel companies, and even small organizations are now able to become eSIM resellers. This means that users may purchase an eSIM from a recognizable brand without realizing that the underlying network provider or data handling entity might be completely different. The sheer number of travel eSIM companies operating today makes it challenging for users to understand who is actually managing their data. There are most certainly some issues unique to the eSIM ecosystem, such as eSIM deletion and reinstallation. Unlike physical SIMs, where users can simply swap the card between devices, eSIMs involve more complex processes that can introduce new risks. For example, we show that if a phone is offline during profile deletion, the SM-DP+ server may not register the deletion, leading to a situation where the user cannot reinstall the profile, effectively resulting in a denial-of-service (DoS) scenario. Such issues did not exist with traditional SIM cards, where physical possession directly correlated with control.

In the following section, we examine the privacy implications of data flow in the eSIM ecosystem, focusing on vulnerabilities such as untrusted resellers, data routing through third-party countries, and the lack of transparency in handling user information. These findings form the foundation for a broader discussion on security challenges, user control, and regulatory gaps addressed later in the paper.

3 Data Flow and Privacy Risks

3.1 Motivation and Goal

Recently, there has been a surge in providers offering eSIM solutions tailored especially towards the travel industry. Many brands now compete in this space, offering diverse options and attractive pricing [78], including affordable plans tailored to specific regions and needs. In general, a customer seeking access to mobile services can purchase directly from a mobile network operator (MNO), from a mobile virtual network operator (MVNO), or from an eSIM reseller. MNO's own and operate the network infrastructure and ensure subscriber

Table 1: Details of IP addresses, Geolocation of the IPs, and ISPs associated with various eSIM providers

Provider	Company Origin	Public IP	Geolocation of the IP	ISP
Airalo [1]	US/Singapore	206.0.71.14	Texas, US	WEBBING USA, INC.
AIRSIMe [2]	Hong Kong	38.86.196.203	Texas, US	Telecom North America Inc
Alosim [3]	Canada	147.28.187.8	Texas, US	Equinix Services, Inc.
Better Roaming [6]	UK	146.88.208.55	NY, US	Truephone Inc
BNESIM [7]	Hong Kong	38.86.196.254	Texas, US	Telecom North America Inc
BreatheSIM [8]	Isle of Man	195.10.99.99	Isle of Man	Manx Telecom
CMLink eSIM [9]	China	223.118.51.111	China	China Mobile International Limited
DENT [11]	British Virgin Islands	37.248.246.98	Poland	SPARKS
eSIM Access [13]	China	206.0.69.143	Texas, US	WEBBING USA, INC.
Eskimo [15]	Singapore	111.65.35.51	Singapore	SingTel Mobile
Flexiroam [16]	Malaysia	206.0.69.106	Texas, US	Webbing USA
Gigsky [17]	US	193.88.50.248	Denmark	TDC NET
GoogleFi [18]	US	172.56.199.56	Real Location of User	T-Mobile
Holafly [19]	Ireland	223.118.51.96	China	China Mobile International Limited
Maya Mobile [22]	US	38.86.196.229	Texas, US	Telecom North America Inc
MTX Connect [23]	Luxembourg	45.153.104.4	Oslo, Norway	Nexthop AS
Nomad [25]	US	192.178.240.193	VA, US	Google LLC
Numero [26]	Spain	154.54.12.114	Germany	Cogent Communications
RedTeaGo [31]	China	91.223.100.68	England	O2 (UK)
Saily [32][1]	Lithuania	94.156.229.223	NY, US	Saily Inc.
T-mobile [38]	US	172.59.9.77	US	T-Mobile
Ubigi [40]	France	140.174.33.144	NY, US	Transatel
USIMS [41]	Switzerland	140.174.33.128	NY, US	Transatel
Voye [43]	Israel	206.0.69.170	Texas, US	WEBBING USA, INC.
Yesim [45]	Switzerland	37.248.248.86	Poland	SPARKS

identity using both physical and embedded SIM technologies. Consumers can purchase long-term contracts for cellular voice and data or prepaid data-only plans. Cellular data plans can also be purchased from an MVNO. These operators provide cellular data and voice services without actually owning the infrastructure. Instead, they enter into a commercial agreement with the MNO and provide access to consumers [79]. The adoption of eSIM technology allowed MVNOs to expand their customer base through focused marketing and ease of provisioning [88]. A customer also has the option to acquire voice or data cellular plans from an eSIM reseller. The eSIM reseller is an entity whose focus is to purchase eSIM profiles from either an MVNO or MNO at wholesale prices and resell directly to consumers. An eSIM reseller does not own or operate the infrastructure, nor do they have any sort of commercial agreement with MNOs. Consequently, dedicated websites [14] exist that help users compare eSIM options, features, and prices for different locations. The business models of these companies vary significantly as well. Some are direct resellers that rebrand eSIM services from established providers, while others are linked to MVNOs. This diversity has driven intense competition, making it more convenient for users to find options that suit their needs.

With such a wide array of eSIM providers, our goal is to experimentally determine how user data flows through mobile networks when using an eSIM profile purchased from an eSIM reseller. Our goal is to identify any privacy risks associated with the use of eSIM profiles purchased from eSIM resellers. Specifically, we answer the following questions:

1. What path does the user's data take when using an eSIM marketed for international travel?
2. What are the implications to user privacy and connectivity when using an eSIM marketed for international travel?
3. What are the privacy and security risks associated with using an untrusted or unverified eSIM provider?
4. What user information can an eSIM reseller access?

3.2 Evaluation Methodology

To address the above questions, it is necessary to develop a methodology that systematically tests mobile service connectivity across a variety of providers. Our experimental setup

[1] Saily allows users to select their virtual location from 82 available options within the application.

consists of eSIM profiles purchased from a variety of domestic and international network providers (see Table 1), and then installed on our testing devices; Google Pixel 4 XL and iPhone 13. The initial list of eSIM providers was sourced from Apple's official website [53]. This resource offers a comprehensive listing of global eSIM providers that are most likely to offer reliable consumer eSIM services. Regardless of the eSIM provider, purchase, activation, and usage are conducted within the United States, unless noted otherwise.

Our experimentation falls into two main efforts. First, we examine the flow of user data when using a travel eSIM. We are mostly interested in IP address assignment and the end-to-end path of user data. To identify the origins of the IP addresses used during the test, we use IPinfo [20]; an online tool that provides detailed information about IP address ownership and geographic location. We selected IPinfo as it is one of the most well-known databases for IP geolocation, offering ease of integration and consistent country-level resolution, which aligned with our goal of identifying cross-border data routing patterns rather than precise location.

We cross-checked the geolocation results with MaxMind [21] and DBIP [10], two other well-known databases for IP geolocation. For certain IPs (e.g., 146.88.208.55), geolocation databases provided differing results: IPinfo and DBIP placed the IP in the U.S., while MaxMind listed it in the UK. MaxMind's result may reflect the registered Autonomous System Number (ASN) or organization origin, while IPinfo or DB-IP may better capture the actual data exit point. Also, some IP-to-ISP mappings can vary over time due to reassignments or changes in MVNO infrastructure. We present the geolocation and ISP data as resolved via IPinfo at the time of writing this paper and note updates where applicable.

Next, we use a variety of publicly available network tools to analyze the flow of user data. In the case of devices using an Android, we used the application *PingTools* [29]. In the case of iOS, we use the applications *Net Analyzer* [24] and *Ping Traceroute* [28]. These allow the use of the traceroute diagnostic command to determine the path data packets take as they travel between the phone and the destination servers.

Due to platform constraints on mobile devices, we were unable to run advanced measurement tools such as Paris Traceroute [27], which are specifically designed to reduce artifacts caused by load balancing and multipath routing (ECMP). Instead, multiple sessions per provider were monitored using network diagnostic tools available on Android and iOS. While IP addresses changed, country-level and ASN-level routing remained consistent. To mitigate common traceroute artifacts, such as asymmetric paths, silent hops, and ECMP-induced variability, we repeated measurements and focused on higher-level routing patterns rather than individual hop-level accuracy. Our approach of repeated measurements and higher-level aggregation enabled us to identify consistent and meaningful routing behaviors across different eSIM providers.

We conducted all experiments from a single geographic location in the United States over 4 months. In this study, using a consistent location, we did not consider the potential impact of dynamic IMSI switching by eSIMs across countries. Some travel eSIMs may change their IMSI when moving between regions to leverage local network agreements, which can alter data routing paths and affect the consistency of geolocation results. As a result, the traceroute data we collected may not fully capture the complexity of dynamic IMSI switching [44].

We evaluate the privacy risks associated with using travel eSIM providers and, more broadly, eSIM resellers. For this analysis, we first compiled a list of eSIM resellers that offered platforms designed to simplify operations for resellers. We then created our own reseller platform using tools available to resellers subscribed to these platforms. By leveraging this setup, we 'sold' eSIM profiles to our testing devices (Google Pixel 4 XL and iPhone 13) to analyze the level of access resellers have to user data. Additionally, we tested whether any safeguards were in place by attempting to retrieve data associated with the active eSIM profiles.

3.3 Data Flow in International eSIM Usage

After purchasing and installing a targeted set of eSIMs, we observed that in almost all cases the device's public IP address did not correspond to its physical location. Instead, most of the assigned IPs were associated with third-party countries. Specifically, through IPinfo, we confirmed that many of the IP addresses belonged to telecommunications providers located in different countries. This data helped us map the flow of information and understand how connections are being routed. Table 1 provides an overview of commercial eSIM providers that we tested, including their company origins, the public IP addresses assigned to users, the geolocation of IPs, and the Internet Service Providers (ISPs) associated with the IPs.

For instance, the purchase of an eSIM from Holafly, a European company headquartered in Ireland, might result in the connection being routed through the China Mobile network. This means the IP address assigned to the device belongs to China Mobile Network, which is a Chinese telecommunications provider. On top of that, by disabling the GPS on the phone, the IP geolocation shows that the device is physically located in China. As a result, this observation has significant implications for access to location-based services. As a control, we conducted the same test using an eSIM purchased from the US service provider T-Mobile. The results showed assignment of a US-based IP address.

Using the eSIMs, we were also able to access services and content restricted to specific regions. For example, we could stream videos from ViuTV [42], an entertainment platform that is typically unavailable in the United States, without the need for a VPN. This behavior highlights how the assigned IP address affects access to geographically restricted content. Additionally, we observed that for Holafly eSIM, the SMDP+ (Subscription Manager Data Preparation) address used for

Table 2: Overview of Traceroute Data Showing IP/Host, Geolocation, and Network Information

#	IP/Host	Geolocation	Additional Info
1	10.91.31.81	Private	–
2	10.91.31.2	Private	–
3	223.118.51.27	China	China Mobile Network
4	223.120.2.113	Hong Kong	China Mobile Network
5	223.120.2.88	Hong Kong	China Mobile Network
6	223.120.2.118	Hong Kong	China Mobile Network
7	223.119.17.154	Hong Kong	China Mobile Network
8	108.170.232.110	Hong Kong	Google LLC
9	142.250.59.20	Hong Kong	Google LLC
10	74.125.245.2	Hong Kong	Google LLC
11	142.251.226.63	Hong Kong	Google LLC
12	142.250.225.151	Taiwan	Google LLC
13	142.250.225.148	Taiwan	Google LLC
14	108.170.238.142	Taiwan	Google LLC
15	209.85.242.125	Taiwan	Google LLC
16	tsa01s11-in-f14.1e100.net	-	Google LLC

installing the eSIM (`rsp1.cmlink.com`) also belonged to the China Mobile Network, granting the network significant control over user data and connectivity. To further investigate the data flow, we used the *traceroute* command on the phone. The results revealed multiple IP addresses involved in the routing process, many of which belonged to networks in third-party countries. Table 2 presents the detailed results of this analysis, including the IP addresses, their geolocation information, and additional network information. These findings provide a clearer picture of how user data travels across international networks when using a travel eSIM.

The travel eSIMs that we tested utilize roaming to provide internet connectivity. Roaming involves connecting to a Visited Public Land Mobile Network (VPLMN) while the user's subscription remains managed by the Home Public Land Mobile Network (HPLMN) [71] as shown in Figure 3. Key network components in this process include the Serving Gateway (SGW), which facilitates data transfer within the visited network, and the Packet Gateway (PGW), typically located in the home network, which assigns IP addresses and connects the device to external networks like the internet. The Home Subscriber Server (HSS) in the home network authenticates users and manages their subscription details, while the Mobility Management Entity (MME) in the visited network oversees user mobility and session setup [71, 83].

What are the consequences? How user data is routed during roaming depends largely on the agreement between the user's provider and the visited network. Many travel eSIMs we tested utilize Home-Routed Roaming (HRR), a roaming arrangement where all data traffic and signaling from a roaming user's device are routed back to their home network (i.e., original carrier) for processing. In HRR, the home network authenticates users through its HSS and keeps track of when and where they connect [80]. To validate the user's subscription,

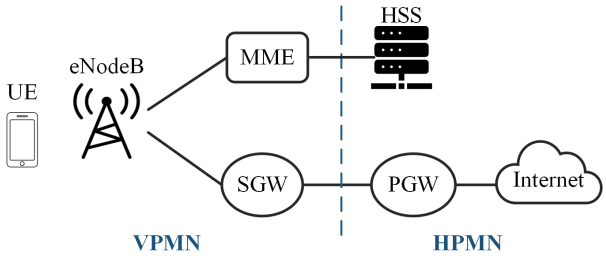

Figure 3: LTE Roaming Architecture

the visited network must communicate with the HSS. The PGW in the home network then routes and manages the user's internet traffic. This gives the home network visibility into all active data sessions, including the services and websites accessed by the user.

Interactions between the visited network's MME and the home network's HSS also allow the home network to determine the user's approximate location, such as the region of the visited network where the connection is occurring. Additionally, since the PGW processes all the traffic, the home network can potentially analyze the user's online behavior, including browsing history and app usage. This significant level of access that home networks have to user data during roaming raises serious privacy concerns with travel eSIMs. The home network is often operated by a third-party entity in a country that the user may not even be aware of.

An alternative to HRR is Local Breakout (LBO), where user traffic is routed directly from the visited network to the internet rather than being tunneled back to the home network [52]. In LBO, SGW in the visited network terminates the user plane traffic locally, while only control plane functions, such as authentication, still involve the home network. This approach reduces latency and minimizes the home network's ability to monitor user data, as internet traffic does not pass through the home PGW [86]. However, implementing LBO requires substantial collaboration between the home and visited networks. It is less common among travel eSIM providers, especially those offering white-label services, because it demands dedicated partnerships with local MNOs [80]. Since we conducted our testing entirely from the United States, we are confident that travel eSIMs whose IP addresses are located outside the US are using HRR. This is consistent with our observation that user traffic was routed through foreign providers (e.g., China Mobile), resulting in an IP address from the provider's country rather than the user's current location. However, identifying LBO is non-trivial. The presence of a US-based IP address does not indicate that eSIM uses LBO. For instance, data may be routed through a US-based proxy or gateway server, while actual network control remains with a foreign provider. Additionally, roaming configuration may vary by region, providers could use HRR in one region and LBO in

another, depending on local infrastructure and regulations.

Although global privacy laws such as the GDPR in Europe and other consumer privacy laws impose restrictions on data usage [48, 63], users are often unaware of the extent of data access or how their information is being handled. GDPR, for example, requires telecom providers to handle personal data securely and obtain user consent. However, the enforcement of these laws varies significantly across regions. In Europe, eSIM deployments must comply with GDPR, which ensures that users retain direct control over their personal data [62, 91]. More importantly, this process requires ongoing effort, including regular security audits and vulnerability assessments, to maintain compliance and ensure user protection. Policymakers must develop and enforce clearer rules for travel eSIM providers to ensure adherence to privacy standards. Travel eSIM providers must also adopt greater transparency regarding their data handling practices, including identifying the networks involved and the extent of data access.

As travel eSIMs grow in popularity, prioritizing user privacy through robust regulations and user education is critical. By implementing clear and enforceable privacy standards, users can remain informed and protected while enjoying the convenience that travel eSIMs offer. Additionally, the growing number of brands, providers, and business models in the market makes it increasingly difficult for users to navigate and evaluate these options, further underscoring the need for clear guidance and strong privacy protections.

Implications of Local Breakout (LBO) on Privacy: While our testing focused on observable behaviors, such as IP routing paths and traceroute hops, we also acknowledge that roaming architecture (HRR vs. LBO) plays a critical role in shaping privacy risk. While our measurements confirm widespread use of HRR among travel eSIMs, we also consider how our findings would be affected if LBO were used. Under LBO, user data does not pass through the home network's core infrastructure, which would reduce the ability of the home provider or its partners to inspect traffic or infer user behavior. This mitigates some surveillance and tracking concerns. However, LBO also shifts the trust boundary: the visited network and its intermediaries now have control over the user's traffic, and their privacy and regulatory posture may be unknown or unverified. Importantly, LBO only affects the routing path of user data; it does not impact other risk surfaces such as initial profile provisioning or how eSIM profiles behave on the device. In summary, LBO changes who can see or manipulate the user's traffic, but it does not eliminate privacy risks, only redistributes them. While LBO may improve data sovereignty in some contexts, it does not fundamentally alter the broader concerns raised in this paper.

3.4 Proactive communication in Travel eSIMs

Proactive communication refers to the ability of the SIM or eSIM profile to initiate actions or transmit data without direct user input [58]. Traditionally, SIM cards could perform such actions through a set of commands defined in the SIM Application Toolkit (STK), allowing the SIM to initiate communication with the network, send SMS messages, or trigger data sessions. These features have supported legitimate use cases such as service configuration and network diagnostics. In the context of eSIMs, especially travel eSIMs provisioned by third-party resellers, the presence of proactive communication warrants closer analysis. Because eSIM provisioning is typically remote and may involve opaque intermediaries, users have limited visibility into what kinds of STK commands are embedded in the profile. This opens the door for proactive behaviors such as location updates, telemetry data sharing, or background SMS communication to occur without the user's awareness or explicit consent.

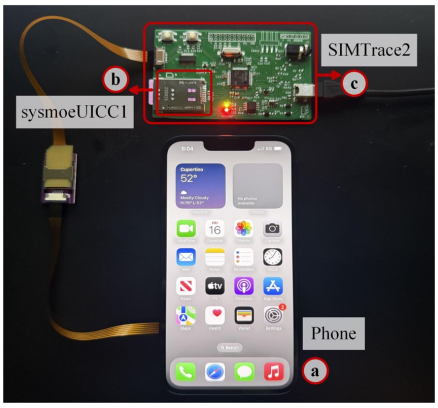

Figure 4: Setup for capturing proactive communication: (a) iPhone 13, (b) sysmoEUICC1 for downloading the eSIM, (c) SIMtrace2 for capturing communication between the phone and the eSIM profile.

Experimental Methodology: Previous works [58] have conducted experiments to investigate the proactive behavior of physical SIMs. However, we wanted to investigate the proactive behavior of travel eSIMs to better understand the privacy risks. To observe proactive behavior, it is necessary to monitor the communication channel between the eUICC and the mobile device. However, because the eUICC is soldered onto the UE's circuit board, such monitoring is difficult with off-the-shelf hardware. To overcome this limitation, we used a Sysmocom eUICC for consumer eSIM(sysmoEUICC1) [34] to host eSIM profiles we wanted to test. Paired with SIMtrace2 [33], this setup allowed us to install the profiles on an iPhone 13 and monitor the communication between the device and the eUICC for any proactive behavior [49], as demonstrated in Figure 4.

Observations: We tested several travel eSIM profiles from different providers, including eSIM Access, Holafly, and Numero, to explore the range of proactive behaviors. The eSIM profiles were downloaded and activated on the sysmoEUICC1

Table 3: Overview of eSIM resellers

Provider	NDA	API Access	White Label	Origin
eSIM Card	Yes	Yes	Yes	USA
Monty	No	Yes	No	UK
Mobimatter	Yes	Yes	Yes	UAE
eSIMGo	No	Yes	Yes	UK
eSIMaccess	No	Yes	Yes	China
Telnyx	No	Yes	No	USA
Maya Mobile	Yes	Yes	Yes	USA

to be used with SIMtrace2. The experimental conditions included phone startup, initial network registration, and periods of idle connectivity. Among our test profiles, the Numero eSIM did not exhibit any proactive communication during our tests. In contrast, both eSIM Access and Holafly demonstrated proactive behaviors. In the case of eSIM Access, we observed that the eSIM profile opened a channel to an IP address (18.138.95.198) registered in Singapore. This connection was established without any explicit user action, suggesting that the profile may be configured to periodically communicate with a remote server for purposes such as phone status updates or network configuration checks. Notably, although the user's public IP address assigned via the mobile network was geolocated in the United States, the proactive communication still targeted a server in Singapore. This highlights the complexity and opacity of the eSIM ecosystem, where backend entities involved in profile management may operate across jurisdictions and remain invisible to end users. For Holafly, we detected a different form of proactive communication. The eSIM retrieved an SMS that originated from the number +8526765671903, indicating that it was sent from Hong Kong. This highlights how the eSIM can silently download information without user intervention. These findings demonstrate that such behaviour, especially when endpoints span multiple countries, raises concerns about transparency, user consent, and the enforceability of regional privacy expectations.

3.5 Risks Associated with eSIM Resellers

The barrier for entry to become an eSIM reseller is surprisingly low. Several platforms provide "turnkey" solutions to potential eSIM resellers. They often target their services to travel agents who can provide a value-added service to their customers traveling abroad. They are even provided with white label eSIM mobile applications [13], which are developed by companies that sell eSIM profiles at wholesale prices. The applications are meant to be further customized by the eSIM reseller, and then delivered to customers to facilitate financial transactions, targeted marketing campaigns, and many more features. These potential eSIM resellers can leverage these services to develop an eSIM reselling marketplace with custom branding. Once potential resellers are established, they can also take advantage of a custom application programming interface (API) queries to purchase eSIM profiles at wholesale rates which can then be re-sold to customers at a recommended MSRP (Manufacture's Suggested Retail Price). This system is analogous to new car dealerships that purchase cars directly from the manufacturer and sell to consumers. In the case of a car dealership, the car manufacturer has a serious stake in ensuring that dealerships operate according to strict policies and procedures to avoid tarnishing the brand reputation. In the case of eSIM reselling, users are unlikely to give any consideration to who is managing and operating the eSIM profile they have just downloaded to their mobile device. MNOs and MVNOs appear to be willing to allow any party the opportunity to re-sell access to their networks. The opportunity exists for virtually anyone to establish their own online presence, selling cellular data plans to anyone with an internet connection. This scenario has serious implications for user data privacy.

In an effort to better understand the risks of using an eSIM reseller, we first compiled a list of eSIM reseller platform providers. Table 3 provides an overview of the providers we reviewed. Some of these providers list their services specifically as eSIM resale provider's while others indicate they cater toward eSIM distributors. For the purpose of this analysis, there is no distinction between a reseller or distributor. Each company can be analyzed through their eSIM offerings listed on their website. While the branding and marketing of each reseller varies, there are several key features they seem to have in common. Most notably, all resellers provide some sort of reseller dashboard that can be used to monitor eSIM profiles that have been purchased wholesale, and that have been sold to a user. However, some vendors add additional support for integration into other custom websites or even provide a white label application or website that can be rebranded according to the individual reseller. One point to note is that many of these companies require the signature of some form of a non-disclosure agreement. Retrieving information on eSIM resale attributes was not possible as publication of these results would likely violate these NDA's. Most of these vendors publish claims of providing resale services to notable partners. For instance, eSIMaccess states that its partners include major companies such as Google and Apple [13]. The nature of these partnerships are not clear, yet they add to the appearance of legitimacy of the reseller platform.

After this initial analysis, we decided to investigate further a selected number of eSIM reseller platforms. We subscribed to both eSIMaccess and Telnyx resale platforms to create our own eSIM reseller service. Our goal was to assess the extent of access an eSIM reseller could have to a user's private data. Additionally, we wanted to develop a better understanding of any safeguards that may or may not be in place when it comes to access to user data. We chose these resellers primarily due to the lack of NDA required for sign-up. All that was needed to become an eSIM reseller in both cases was a valid email

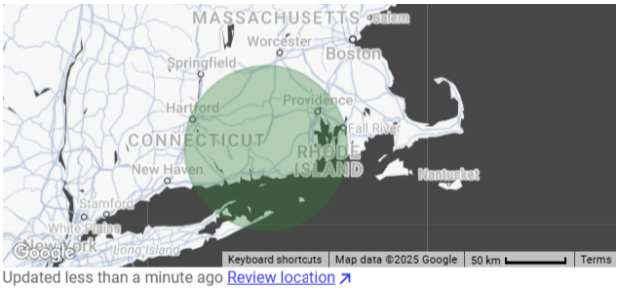

Figure 5: Device location information provided by Telnyx reseller dashboard

address and method of payment.

eSIMAccess - eSIMAccess is a subsidiary of Readtea Mobile, a Chinese based telecommunications company [30]. The main webpage entices potential resellers with claims like "Your Brand, Our Plans". The entire ecosystem is designed to make it extremely easy for anyone to begin reselling cellular data and voice plans with *No commitments*. Once registered a reseller can quickly view eSIM plans, previous purchases, billing, and profile information from a partner dashboard. eSIM profiles can be purchased for use in 265 different countries around the globe. Plans are purchased based on their intended usage location, amount of data, and use duration (days). Additionally, regional plans can be purchased for use in multiple countries. For example, 1 GB of data for use in the United States for a single day has a wholesale price of $1.30 with a suggested retail price of $2.60. Once plans have been purchased by the reseller, a QR is generated and can then be sent to customers once purchased from the reseller. The eSIMaccess dashboard allows a reseller to maintain an inventory of eSIM profiles ready for sale. Once these eSIM profiles are activated by users, the resellers can maintain constant observation of the status of the profile (New, Installed, In-Use, Deleted), how much data is left according to the profile limits, how much time is left on the profile time limits, and the ICCID of each profile.

Every reseller on the eSIMAccess platform receives an API key and access to API documentation. The API queries can be used for the following actions: Get All Data Packages (list available profiles), Order Profiles (use account credit), Query All Allocated Profiles (retrieve user profile info), Cancel Profile (refund inactive profiles), Suspend/Unsuspend Profile (pause/restart profile), Revoke Profile (remove eSIM plan), Balance Query/Top Up (manage account balance), Set Webhook (automated notifications), and Send SMS (to eSIM users). The most notable privacy concern relates to the data provided as a result of the 'Query All Allocated Profiles' request. This API query returns (among other things) the IMSI, MSISDN, and eSIM PIN for any activated eSIM profile in use. The items are of course normally available to MNOs, which in of itself is not necessarily a privacy concern. The eSIM pin, for example, is set by the profile provider as an added layer of security against unauthorized access to profile data. Physical SIM cards have similar capabilities, and users can reset the SIM pin. Our experiments also showed that if a user updated their eSIM pin, the new pin was not disclosed to the eSIM reseller. However, this data is now exposed to parties outside the MNO, notably an untrusted eSIM resale vendor. The 'Send SMS' action allows the reseller to send SMS messages directly to their users. Again, this capability has been engineered into the design of mobile networks to enable network operators to communicate with their users. However, this capability is now in the hands of an unverified reseller, offering a delivery mechanism for binary SMS attacks against mobile devices.

Telnyx - Telnyx is a global telecommunications company providing a diverse set of solutions to a variety of industries [36]. Most notably they offer custom connectivity solutions in the form of an eSIM resale platform. This platform is advertised to provide global connectivity to IoT devices, as well as a means to provide private connectivity to corporate or private networks. Telnyx does not provide custom white label solutions to its resellers. Instead, it provides a much deeper level of technical customization and detail. It seems that the eSIM reseller platform is geared towards customers that need a finer level of control on profile usage. It does provide all the same API functionality that eSIMaccess and more. Resellers can access this information on the "Mission Control Portal" or through API queries. Most notably, Telenyx provides device location information for any active eSIM profile. An example of the location information Telnyx provided on the "Mission Control Panel" is depicted in Figure 5. Telnyx provides limited insight into how this location information is generated. For its physical SIM solutions, they indicate that:

"An estimate of your SIM card location ... is acquired based on the location of the cell tower to which the SIM is connected to....The more powerful the cell tower is, the larger the error rate of the SIM's location will be due to the strength of the signal coming off of that tower." [37]

It is likely that the location information for an eSIM user is generated via similar methods. However, the location information refresh period is variable. We conducted several experiments with mobile devices using Telnyx eSIMs. Traveling across major cities over the course of several hours did not show real-time changes. However, device location upon eSIM activation was always within the error circle presented. In some cases however, the reported location of the user was within a 0.5 mile of the actual location. Further testing to understand exactly the extent to which a user location could be tracked is not necessary to determine that user privacy is in fact compromised. Again, user location is always disclosed to major network operators. In the US, mobile device location must be provided to emergency services and law enforcement when proper conditions are met. The differentiating factor in this scenario is that this location information is not available

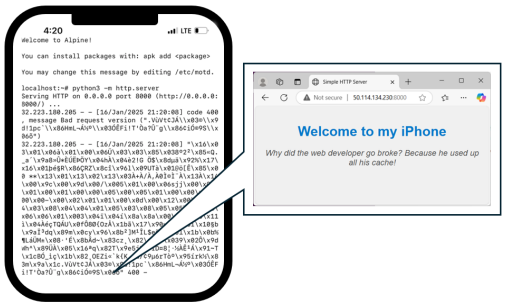

Figure 6: Mobile Device Web Server

to the eSIM reseller without the knowledge of the eSIM user.

Telnyx also provides the ability to assign a public IP address to an eSIM profile. Experimental results showed that an iPhone using a Telnyx eSIM with a public IP enabled, responded to ICMP ping requests making it accessible from anywhere on the internet. To further demonstrate this scenario we configured a test device, in this case an iPhone 13, with a Telnyx eSIM configured with a static public IP address. The device was then configured to run a simple HTTP server so that any device could browse to the webpage. A demonstration is shown in Figure 6. Additionally, the iPhone was able to display the HTTP requests as other clients connected to the web server. The ability to assign a user's mobile device a static public IP (potentially without their knowledge or consent) presents a significant security risk. This potentially allows direct communications with devices globally to deliver malware or sustain prolonged command and control operations with malicious software that exists on the device.

4 eSIM Deployment and Usability Challenges

The adoption of eSIM technology has introduced new security, usability, and regulatory challenges. This section focuses on evaluating the implications of Remote SIM Provisioning (RSP) in real-world scenarios, the risks associated with eSIMs in private networks, and the limitations users face in managing eSIM profiles. By addressing these challenges, we aim to identify gaps in security and regulation while highlighting opportunities to enhance trust in eSIM technology.

This section seeks to investigate these challenges by addressing the following questions:

1. Are there implications or risks in Remote SIM Provisioning (RSP) in real-world scenarios, considering the security parameters outlined in GSMA standards?

2. What security and privacy challenges arise from the reduced control users have over eSIMs compared to physical SIMs, particularly in managing, deleting, and transferring profiles?

3. What specific threats do private network eSIM deployments (e.g., hospitals, warehouses) introduce, including potential for malicious profile installations, unauthorized access, or communication interception?

4. Have regulations kept pace with the rapid growth of eSIM technology to address its challenges?

Together, these research questions address four key areas of the eSIM ecosystem: the technical risks of Remote SIM Provisioning (RSP), user-centric challenges around profile management and control, vulnerabilities introduced by emerging use cases like private networks, and the adequacy of current regulatory frameworks.

4.1 Evaluation Setup and Methodology

To answer these questions, we conducted some experiments, including tests on a private network and a prominent eSIM provider as a case study. To analyze the RSP protocol in practice and test real-world user challenges, we used a three-month prepaid plan from Mint Mobile , a well-known eSIM provider in the United States. By monitoring the installation, activation, and usage processes, we captured detailed logs and assessed potential vulnerabilities in real-world conditions. Specifically, we conducted controlled experiments in a private network environment using the Amarisoft Callbox [4], a comprehensive LTE/5G testing solution. An eSIM provided by Amarisoft was provisioned via a commonly used SM-DP+ server, "consumer.rsp.world." This server is also employed by other travel eSIM providers, such as Ubigi [40] and Transatel [39]. When the eSIM profile was successfully downloaded and activated, the device was able to connect to our private network. During the connection process, the device (i.e., User Equipment) sent an attach request to MME. The MME initiated authentication using information in the eSIM profile, such as the IMSI and authentication keys. If the eSIM profile's settings align with the private network's configurations, then the authentication and connection establishment conclude successfully.

During our experimentation, we captured detailed logs from the network-side infrastructure and a rooted phone to observe the full sequence of events during the attachment, activation, deactivation, and deletion. This involved firmware logs from the device, internet related traffic (e.g., HTTPS), and cellular-based traffic from the Amarisoft (e.g., Non-Access Stratum (NAS) and Access Stratum (AS) messages), providing us with complete insights into the operational mechanisms of eSIMs in private networks. These experiments demonstrated that eSIMs can streamline connectivity in private networks, provided the configuration parameters, like keys and authentication settings, are correctly matched. However, the ease of deploying eSIMs also raises concerns about potential misuse, such as malicious profile installations or unauthorized access in less secure environments.

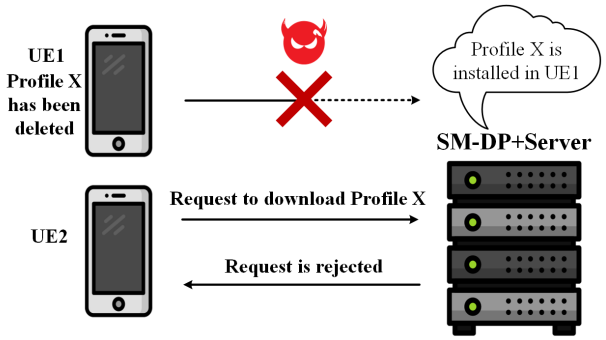

Figure 7: An attacker intercepting the internet connection during profile deletion prevents the notification from reaching the SM-DP+ server, thereby blocking reinstallation

4.2 Managing eSIM Profiles

Disabling and Deleting eSIMs. Managing eSIM profiles presents unique challenges not typically encountered with physical SIM cards. While physical SIMs can be inserted or removed at will, eSIMs depend on digital workflows governed by multiple entities, each with its own policies and infrastructure (e.g., SM-DP+ servers). As a result, profile lifecycle operations such as disabling, deleting, or transferring an eSIM involve more complex processes with usability and operational implications. To understand these dynamics, we used our Amarisoft-based private LTE testbed to observe how devices behave during profile disablement and deletion. When an eSIM is disabled, the device (UE) sends a detach request to the network, disconnecting it from the network. Simultaneously, the UE notifies the SM-DP+ server of the change in status. Even though disabling the eSIM disconnects the phone from the network, the profile remains stored in the eUICC and can be re-enabled by the user. To verify that disabling the eSIM effectively disconnected the device from the network, we sent an emergency message through Amarisoft's Public Warning System (PWS). As expected, the device did not receive this message, confirming complete network detachment.

In contrast, the deletion process proved more fragile. When connected to the internet, the device successfully informed the SM-DP+ server that the profile was deleted, allowing it to be reinstalled using the same QR code. However, if deletion occurred while offline (e.g., with WiFi disabled), the notification failed to reach the server. As a result, the SM-DP+ server continued to treat the profile as active, preventing reinstallation and triggering an "already installed" error (Figure 7). Furthermore, according to GSMA specifications [66, 67], profiles can include policy rules that restrict deletion or deactivation.

This behavior is not necessarily a security flaw. GSMA specifications assume the availability of a secure connection during profile state changes, but in practice, it introduces a user experience failure mode that could result in unnecessary downtime or user support escalation. This risk becomes particularly problematic if a device is lost, damaged, or network-disconnected during deletion, leaving the user unable to recover or reinstall the profile without provider assistance. This scenario was observed in our case study with a commercial eSIM provider, Mint Mobile When the profile was deleted while the device was offline, the server failed to receive the deletion notification due to a TLS handshake error. Wireshark logs confirmed that the user equipment could not establish a secure connection with the SM-DP+ server, leaving the profile marked as active. As a result, reinstallation attempts using the original QR code were blocked. The issue was only resolved after the provider issued a new profile.

Provider-Imposed Restrictions. Several eSIM providers enforce limitations that reflect design choices rather than vulnerabilities. For example, many eSIM profiles are configured for single-use installation, or are bound to a device's unique EID. These restrictions help prevent unauthorized sharing or reuse of profiles, especially in scenarios involving data resellers or travel plans. During our evaluation, we encountered several common provider warnings:

`Flexiroam`: "Most eSIMs can only be installed once; if removed, they cannot be reinstalled."

`GigSky`: During installation, GigSky notifies users that "The eSIM cannot be moved to another device".

`Nomad eSIM`: "DO NOT Remove this eSIM! This eSIM can only be installed once. Please do not remove it from your phone once installed."

While these behaviors align with GSMA standards and operator policies, they limit user flexibility and may create confusion or friction—particularly when users are unaware of the implications of deletion. The ability to re-use a QR code is not guaranteed and depends on whether the SM-DP+ server receives the correct profile status updates.

eSIM Profile Persistence and Size Implications. eSIM profiles can also carry additional policy rules that govern deletion or deactivation. These settings are often legitimate—for example, used in enterprise device management to enforce compliance or provisioning controls. However, if exploited by untrusted resellers or in low-regulation environments, such policies could theoretically be misused to prevent users from removing a profile entirely, effectively locking the profile in place. Additionally, profile size may pose indirect risks. Larger profiles (e.g., for 5G or multi-network configurations that include additional encryption and authentication mechanisms) [12] are common and usually intentional. We speculate that a malicious or poorly designed provider could exploit this feature by installing an unusually large or bloated profile. Given the limited memory capacity of eUICCs, this could exhaust available storage and prevent additional profiles from being installed. Although we did not observe this behavior in the wild, it represents a plausible DoS-like scenario in constrained or low-end hardware deployments.

4.3 Risks in Private Networks

The deployment of eSIMs in private networks is expanding rapidly as organizations such as hospitals, conferences, and event venues are increasingly adopting eSIMs for connectivity [50]. For example, hospitals may deploy private networks with eSIMs to enable authorized personnel to securely access patient data. Similarly, conferences and venues may issue eSIM profiles via QR codes to provide participants with internet access instead of relying on WiFi. While these applications highlight the versatility of eSIM technology, they also raise significant security and privacy concerns. Users must be aware of the potential risks before installing an eSIM profile, particularly in private network scenarios.

One of the most alarming security risks is the potential for a malicious private network to gain unauthorized access to a user's device through an eSIM profile. Consider a scenario where an attacker distributes tampered QR codes at public venues such as conferences, airports, or other gatherings, promising free internet access. Some individuals might scan the QR code and install the eSIM profile without fully understanding the potential consequences. An attacker might also target specific victims using social engineering techniques to persuade them to install a malicious eSIM profile. We discovered that once an eSIM profile is installed, the network provider gains a significant degree of control over the device's connectivity. For example, (a) a malicious network can exploit the installed eSIM profile to monitor user activities, such as tracking their location and intercepting communications, without the user's consent, and downgrading security in NAS and AS communications, and (b) once connected to the malicious network, the operator may send binary SMS messages to the user's device. These messages could modify device settings, extract sensitive information, or install harmful payloads without the user's knowledge [94]. Such scenarios are harder to execute with physical SIMs due to the need for physical distribution and greater user control over installation. Consequently, the ease of installing eSIM profiles and the ability to store multiple eSIM profiles simultaneously significantly increase the risk of such attacks.

In addition to these risks, the eSIM profile itself could be inherently malicious. For instance, it might contain harmful configurations, introduce vulnerabilities, or expose the user to further attacks. In theory, malicious eSIM profiles, especially those distributed outside vetted channels, could be configured to exfiltrate data or enable location tracking. Once installed, these profiles may grant attackers persistent access to the device's network communications, making it difficult for users to detect or remove the threat without technical expertise. The dynamic and remote nature of eSIM provisioning further intensifies these risks. Users may unknowingly install malicious profiles through tampered QR codes, fake provisioning apps, or phishing campaigns, putting their devices and data at significant risk. To mitigate these risks, users should exercise caution when scanning QR codes for eSIM installation. They should regularly review installed eSIM profiles on their devices and ensure they only install profiles from trusted and reputable sources.

4.4 Standardization and Regulatory Gaps

The security of the eSIM ecosystem relies heavily on robust protocols, user authentication measures, and regulatory oversight. However, even with secure protocols in place, the human factor remains a critical vulnerability. For instance, poor customer service practices can undermine the overall security of eSIM management, making it susceptible to attacks like SIM swapping. To understand the practical implications of eSIM provisioning, during the profile installation process in our Mint Mobile case study, we captured logs and observed encrypted communication between the UE and the SM-DP+ server. This communication involved certificate exchanges to establish mutual trust, followed by the secure download of the eSIM profile. We evaluated the protocol's resilience by attempting a man-in-the-middle (MITM) attack using MITMProxy [60], a tool capable of intercepting HTTPS traffic. We noticed that the TLS handshake between the UE and the SM-DP+ server failed since the UE did not trust the proxy's certificate, preventing the download process. While the protocol itself was secure, our interactions with Mint Mobile customer service revealed deficiencies in their authentication/identification process. For example, an attacker with basic information about a victim (such as their account number or phone number) could potentially request an eSIM transfer. This highlights the urgent need for stricter authentication measures, such as mandatory Multi-Factor Authentication (MFA), to mitigate these risks.

Moreover, we compared the regulatory landscapes of the United States and Europe regarding eSIM implementation. European network providers enforce stringent identity verification measures before issuing SIM cards. For instance, some European providers require users to be physically present in the country in order to install and activate an eSIM, ensuring tighter control over the provisioning process. In contrast, providers in the United States adopt more relaxed regulations regarding user identification.

While the RSP protocol has been proven secure so far when implemented correctly, social engineering attacks that previously targeted physical SIM cards remain a significant concern for eSIMs. The ease of remote management makes eSIMs particularly susceptible to attacks like SIM swapping. SIM swapping involves an attacker impersonating the victim to convince the mobile network operator's customer support to transfer the victim's eSIM profile to the attacker's device. These attacks often exploit weaknesses in authentication/identification processes, leveraging publicly available information or bypassing insufficient protections like the absence of MFA. Notable real-world examples underscore these

vulnerabilities. In one case, a scammer remotely gained control of a victim's phone number by applying for an eSIM, granting access to the victim's bank account [87]. Similarly, "The Sun" reported another incident [92] where an attacker impersonated the victim, hijacked their eSIM, and took over banking apps linked to the phone number. These cases highlight the urgent need for authentication protocols and more rigorous identification requirements.

Finally, it should be clarified that the RSP also facilitates secure over-the-Air (OTA) updates for SIM profiles, enabling MNOs and eSIM platform providers to deploy security patches, bug fixes, and configuration updates remotely. However, this extensive control also introduces risks. Some users have reported that certain travel eSIM providers installed additional apps without their consent. These concerns highlight the assumed trustworthiness of entities like MNOs (or MVNOs) and SM-DP+ providers and must be carefully scrutinized to ensure the security and integrity of the eSIM ecosystem.

5 Discussion and Recommendations

5.1 eSIM Transfer Challenges and Security

Transferring an eSIM is significantly more complex than moving a physical SIM card, as eSIMs are embedded within devices and cannot be physically transferred. This poses challenges when a device becomes inoperable, lost, or damaged, requiring users to rely on their mobile network operator or eSIM provider to transfer or re-provision the eSIM profile. Additionally, some eSIM profiles are bound to the EID of the original device, further complicating the transfer process. While this improves security, it introduces delays and inconvenience for users, especially when multiple profiles are installed on a single device. Apple and Google have implemented their own eSIM transfer solutions to simplify this process. Apple's eSIM transfer feature supports a limited subset of carriers and requires devices running iOS 16 or later, signed into the same Apple ID, and in close proximity with active WiFi and Bluetooth. Users initiate the transfer on the new device, select the eSIM to transfer, and authorize the process on the old device. In our experiments with a T-Mobile eSIM on iPhone 13 models, traffic captured using Aircrack-ng [46] and Ubertooth-One [47] revealed the exchange of "Nearby Information" messages over Bluetooth [84] and TLS-encrypted communication with Apple and T-Mobile servers. Bluetooth proximity ensures the devices are physically controlled by the user during the transfer, requiring manual authorization on both devices. TLS encryption safeguards profile data during transmission, making interception highly unlikely.

Google's eSIM transfer method simplifies moving profiles between devices but requires carrier support, limiting universal compatibility. The process involves generating a QR code on the old device, which the new device scans to download and activate the eSIM profile. During testing, the QR code contained a URL[1] and a key managed by Google for secure transfers. The process relies on certificates and encrypted communication for security, similar to RSP. Unlike Apple's approach, Android's method does not require shared account authentication, which may reduce security. While encrypted communication protects data, the absence of recipient device verification introduces potential risks.

5.2 Limited Access to eSIM Infrastructure

Improving transparency and fostering research in the eSIM ecosystem requires addressing the significant limitations in accessing and experimenting with RSP infrastructure. Much of the Remote SIM Provisioning (RSP) implementation, particularly the SM-DP+ functionality, operates as a "trusted black box," creating significant barriers for researchers. For instance, setting up an SM-DP+ server requires certified components and digital certificates issued by GSMA [56], making it nearly impossible for independent researchers to study these systems comprehensively. Currently, no commercial products offer customizable eSIM solutions tailored for research, small private networks, or laboratory use. Unlike programmable physical SIM cards, such as the sysmoISIM-SJA5 [35], there are no comparable tools available for eSIM technology. This gap restricts researchers from gaining full control over eSIM profiles or studying their behavior, thereby hindering advancements in the field. In short, there is an urgent need to develop open, research-friendly eSIM platforms to allow controlled experimentation with provisioning, activation, and deletion.

5.3 Improving eSIM Ecosystem Security

Accountability of eSIM Resellers. A major challenge in the eSIM ecosystem is the lack of clear accountability when mobile services are resold by third-party resellers. Unlike MNOs, resellers may not be subject to the same regulatory standards, creating a gap in data and privacy compliance. When mobile network services are packaged as wholesale commodities, there is a risk of user data being mishandled. The responsibility for protecting this data is often unclear: does it lie with the reseller, the MNO, or the wholesale provider? Our findings reveal that resellers often have access to sensitive user data, and this level of access varies greatly depending on agreements with wholesale providers.

To mitigate these risks, the roles and responsibilities of resellers and wholesale providers must be clearly defined. At a minimum, the following measures should be implemented. Wholesale providers should proactively vet resellers and ensure continued compliance with data protection regulations. Resellers must adhere to transparent data handling practices and provide clear information to users about IP routing methods and data usage. In the interim, users should prioritize

[1] https://simtransfer.goog/esim/

selecting eSIM services from resellers that are transparent in their data practices and compliant with applicable regulations.

eSIM Usability and Transparency. To improve the user experience and security within the eSIM ecosystem, several key measures are necessary. Establishing standardized policies across all eSIM providers would reduce user confusion and ensure consistent functionality, creating a more seamless experience for users. Reliable notification mechanisms should be developed to ensure that delete notifications consistently reach SM-DP+ servers, even during network disruptions, preventing potential errors and inconveniences. Transparency is another critical factor—providers must clearly communicate their data handling practices, reinstallation policies, and device compatibility, enabling users to make informed choices. Finally, enhanced user education is essential to raise awareness about potential risks, such as malicious profiles, fraudulent QR codes, and insecure networks, empowering users to make safer decisions and better manage their eSIM profiles. These steps collectively aim to create a secure and user-friendly eSIM ecosystem.

Other eSIM Security Measures. The European Union Agency for Cybersecurity (ENISA) has provided valuable guidance [64], which can serve as a foundation for further research and implementation. Regulatory bodies must enforce stricter rules requiring eSIM providers to disclose data handling practices and guarantee secure provisioning processes. Regular security audits, compliance with international GSMA standards [74], and the use of certified components are critical for maintaining the integrity of the RSP ecosystem. Providers must also adopt stronger authentication mechanisms, such as multi-factor authentication (MFA), to prevent SIM swapping and social engineering attacks. Device manufacturers should incorporate safeguards to prevent unauthorized profile installations or updates, requiring explicit user consent for any changes to profiles or configurations.

6 Related Work

Research into the security of Subscriber Identity Modules (SIMs) has uncovered a range of significant vulnerabilities in their design and implementation [97]. For example, SIMURAI [82] demonstrated how malicious SIM cards can exploit device and baseband vulnerabilities, enabling advanced attacks. Similarly, empirical studies [81] have shown how weaknesses in carrier authentication processes facilitate SIM swap attacks, which allow adversaries to hijack accounts by fraudulently transferring phone numbers to unauthorized SIM cards. The transition to eSIM technology builds upon these challenges while introducing unique risks due to its digital, remotely managed nature. For example, Walvekar et al. [93] explored security concerns and highlighted key vulnerabilities related to the use of eSIMs . However, their work lacked experimental validation of real-world implementations or practical mitigation techniques.

Similarly, Ding et al. [61] conducted a formal security analysis of the embedded SIM remote provisioning (RSP) protocol using SPIN model checking. Their study focused solely on formal verification without evaluating these issues in practical settings. Ahmed et al. [57] analyzed the Consumer RSP protocol. Their work primarily concentrated on protocol-level issues, leaving broader risks such as privacy violations and user-targeted threats unaddressed. In contrast, Gaber and Kaluza [65] examined the challenges arising from the distribution of responsibilities among stakeholders in the eSIM adoption. They argued that the lack of clarity in roles creates usability concerns. Chitroub et al. [59] focused on theoretical security challenges in next-generation SIM cards, analyzing vulnerabilities in authentication and communication protocols. SecureSIM [96] proposed a novel framework for rethinking authentication and access control in SIM and eSIM environments. While the approach offered an innovative design, it did not evaluate feasibility in large-scale deployments. Similarly, Samanvita et al. [89] addressed challenges in eSIM profile management testing but focused exclusively on ensuring correct eSIM behavior. Dhameliya et al. [85] analyzed potential threats and protection mechanisms related to eSIMs, discussing theoretical attack vectors and mitigation strategies. Additionally, Maluleka [90] studied the adoption of eSIM technology by South African users for international roaming, exploring user perceptions and adoption barriers. While this work offered insights into usability challenges, it did not delve into specific security or privacy risks.

Our work expands upon these efforts by comprehensively analyzing the eSIM ecosystem from provisioning to deletion. We examine practical security and privacy challenges, including threats posed by travel eSIM providers and resellers, malicious networks, and user practices. Our efforts fill the gap left by prior research that predominantly focuses on theoretical or protocol-level vulnerabilities.

7 Conclusion

This paper underscores the critical importance of addressing the security and privacy challenges in the rapidly expanding field of eSIM technology. Although the eSIM ecosystem has the potential to simplify the lives of users, it could also have a negative affect on user privacy. Our findings reveal risks such as location tracking, data interception, and vulnerabilities during eSIM provisioning and management. The ease of use offered by eSIMs increases the likelihood of users unknowingly falling victim to malicious activities or misconfigurations, emphasizing the urgent need for greater awareness of these risks. By raising awareness among users, implementing additional security controls to compensate for the lack of physical SIMs, and addressing regulatory gaps, stakeholders can enhance privacy and security while fostering trust in this evolving technology.

Acknowledgement

The authors gratefully acknowledge the support of NSF Grant 2144914, Google PhD Fellowship, and the United States Coast Guard Academy. The views expressed in this publication are those of the authors and do not necessarily represent the views of the United States, the Department of Homeland Security, or the United States Coast Guard.

Ethical Considerations

- **Data Privacy:** We ensured that no personally identifiable information (PII) or sensitive user data was collected, stored, or disclosed during our testing process. Any data analyzed or referenced in this work pertains solely to the behavior and functionality of the eSIM services, without involving real users' accounts or profiles.
- **Testing Boundaries:** All tests conducted were limited to controlled environments, such as our lab devices and private networks, to avoid interfering with the operation of live commercial networks or the experience of other users.
- **Fair Representation:** The results presented in this paper aim to provide an unbiased evaluation of the tested eSIM services. We refrained from endorsing or disparaging specific providers without clear evidence. Any identified vulnerabilities were documented to highlight potential risks to users, with recommendations for improvement.
- **Engagement with Stakeholders:** As part of our ethical considerations, we have reached out to the GSMA to seek guidance on how they perceive the identified issues, particularly the challenges surrounding data flow and jurisdiction. This step ensures that we address the broader implications of our findings within the context of industry standards and regulations. However, we have not yet contacted individual eSIM resellers as there are currently no explicit regulations or frameworks.

Compliance with Open Science Policy

In alignment with Open Science Policy and to foster transparency and reproducibility in eSIM-related research, we have made all artifacts associated with this study publicly available. These include datasets, captured logs of eSIM installations, activations, and deletions, as well as relevant network captures and protocol interactions observed during our experiments. By releasing these resources, we aim to support the validation of our findings and enable other researchers to build upon our work efficiently. Our artifact is available through Zenodo and can be accessed at: https://doi.org/10.5281/zenodo.15587623

References

[1] Airalo. https://www.airalo.com.

[2] AIRSIMe. https://www.airsime.com/.

[3] alosim. https://alosim.com.

[4] Amarisoft Callbox: LTE/5G Testing Solution. https://www.amarisoft.com/callbox/.

[5] Android Open Source Project, eSIM Overview. https://source.android.com/docs/core/connect/esim-overview.

[6] BetterRoaming. https://www.betterroaming.com.

[7] BNESIM. https://www.bnesim.com.

[8] BreathesSIM. https://www.breathesim.com.

[9] CMLink eSIM. https://esim.cmlink.com.

[10] DBIP - IP geolocation API and database. https://db-ip.com/.

[11] Dent eSIM. https://www.dent-app.com.

[12] eSIM Profile Database. https://osmocom.org/projects/sim-card-related/wiki/ESIM_profile_database. Osmocom Project.

[13] eSIMaccess. https://esimaccess.com/.

[14] eSIMDB, eSIM Database - Compare eSIM Providers Worldwide. https://esimdb.com/.

[15] Eskimo. https://www.eskimo.travel.

[16] FlexiRoam. https://www.flexiroam.com.

[17] GigSky. https://www.gigsky.com.

[18] Google Fi. https://fi.google.com.

[19] Holafly. https://esim.holafly.com.

[20] IPinfo - IP Address Details and API. https://ipinfo.io/.

[21] MaxMind - GeoIP Databases. https://www.maxmind.com/.

[22] Maya Mobile. https://maya.net/.

[23] MTX Connect. https://www.mtxc.eu.

[24] Network Analyzer. https://apps.apple.com/us/app/network-analyzer-net-tools/id562315041. Technet.

[25] Nomad. https://www.getnomad.app.

[26] Nomero eSIM. https://www.numeroesim.com.

[27] Paris Traceroute. https://paris-traceroute.net/.

[28] Ping & Traceroute. https://apps.apple.com/us/app/ping-trace-route/id1134394314. Loopbots Technology.

[29] PingTools Network Utilities App. https://play.google.com/store/apps/details?id=ua.com.streamsoft.pingtools. PingTools Network Utilities.

[30] Red Tea Mobile. https://www.redteamobile.com/resource/pdf/CompanyProfile.pdf.

[31] RedteaGo. https://esim.redteago.com.

[32] Saily. https://saily.com.

[33] SIMTrace2. https://osmocom.org/projects/simtrace2/.

[34] sysmoEUICC1 eUICC for consumer eSIM RSP. https://sysmocom.de/products/sim/sysmocom-euicc/.

[35] sysmoISIM-SJA5: A Versatile SIM/USIM/ISIM Card. https://www.sysmocom.de/products/sysmoisim-sja5. sysmocom - systems for mobile communications GmbH.

[36] Telnyx. https://www.telnyx.com/solutions.

[37] Telnyx SIM card location and device details. https://support.telnyx.com/en/articles/5812302-sim-card-location-and-device-details.

[38] Tmobilel. https://www.t-mobile.com/.

[39] Transatel. https://www.transatel.com.

[40] Ubigi eSIM. https://cellulardata.ubigi.com.

[41] USIMS. https://usims.com.

[42] Viutv. https://viu.tv/.

[43] Voye. https://voyeglobal.com.

[44] What is IMSI switching, and how does it work? https://telnyx.com/resources/imsi-switching.

[45] yesim. https://yesim.app.

[46] Aircrack-ng: A complete suite of tools to assess wifi network security. https://www.aircrack-ng.org/, 2006.

[47] Ubertooth one: An open source bluetooth sniffer. https://greatscottgadgets.com/ubertoothone/, 2011.

[48] Protecting Subscriber Privacy in 5G. Tech. rep., Trusted Connectivity Alliance, July 2020.

[49] Capturing SIM to modem communication using Osmocom SIMtrace2. https://docs.eseye.com/Content/Resources/Files/8825-Osmocom-SIMtrace-Instructions.pdf, 2022.

[50] eSIM Sponsorship for Events. https://esimaccess.com/esim-sponsorship-for-events/, 2023. eSIM Access.

[51] eUICC Profile Package: Interoperable Format Technical Specification. Tech. rep., Trusted Connectivity Allience, July 2023.

[52] Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 18). Tech. Rep. TS 23.401 V18.8.0, 3GPP, 2024.

[53] Worldwide Service Providers, 2024. https://support.apple.com/en-us/101569.

[54] Embedded sim (esim) technology market report. https://www.fortunebusinessinsights.com/industry-reports/embedded-sim-esim-technology-market-100372, 2025. Fortune Business Insights.

[55] eSIMstatisticstelecomserviceprovidersneedtoknowin2025. https://www.mobiliseglobal.com/50-esim-statistics-in-2023/, 2025.

[56] ABDOU, B. A. Commercializing esim for network operators. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (2019), IEEE, pp. 616–621.

[57] AHMED, A. S., PELTONEN, A., SETHI, M., AND AURA, T. Security analysis of the consumer remote sim provisioning protocol. *ACM Transactions on Privacy and Security 27*, 3 (2024), 1–36.

[58] BURGESS, D. A. More Proactive SIMs. https://medium.com/telecom-expert/more-proactive-sims-f8da2ef8b189, 2021.

[59] CHITROUB, S., ZIDOUNI, N., AOUADIA, H., BLAID, D., AND LAOUAR, R. Sim card of the next-generation wireless networks: Security, potential vulnerabilities and solutions. In *2018 2nd European Conference on Electrical Engineering and Computer Science (EECS)* (2018), IEEE, pp. 502–509.

[60] CORTESI, A., HILS, M., KRIECHBAUMER, T., AND CONTRIBUTORS. mitmproxy: A free and open source interactive HTTPS proxy, 2010–. [Version 11.0].

[61] DING, Z., HU, Y., LUO, W., HUANG, Z., ZHANG, L., AND QIN, Z. Security analysis of embedded sim remote provisioning protocol using spin. In *Proceedings of the 2021 11th International Conference on Communication and Network Security* (2021), pp. 43–48.

[62] EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). Guidelines on the Protection of Personal Data Processed by Mobile Applications Provided by European Union Institutions, 2016.

[63] EUROPEAN UNION. General Data Protection Regulation (GDPR), 2016. A regulation concerning data protection and privacy in the European Union and the European Economic Area.

[64] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). Embedded SIM Ecosystem, Security Risks and Measures, March 2023.

[65] GABER, C., AND KALUZA, P. esim adoption: essential challenges on responsibilities repartition. In *2022 1st International Conference on 6G Networking (6GNet)* (2022), IEEE, pp. 1–4.

[66] GSMA. RSP Architecture Specification. Standard SGP.21, 2016.

[67] GSMA. RSP Technical Specification. Standard SGP.22, 2016.

[68] GSMA. eSIM Whitepaper. https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf, 2018.

[69] GSMA. Embedded SIM Remote Provisioning Architecture. Standard SGP.01, 2020.

[70] GSMA. Remote Provisioning of Embedded UICC Technical Specification. Standard SGP.02, 2020.

[71] GSMA. Eps roaming guidelines. Tech. rep., 2021.

[72] GSMA. Security Evaluation of Integrated eUICC. Standard SGP.08, 2021.

[73] GSMA. EID Definition and Assignment Process, Version 1.1. Standard SGP.29, 2024.

[74] GSMA. RSP Compliance Process, Version 3.1. Standard SGP.24, 2024.

[75] GSMA INTELLIGENCE. eSIM: Market Progress, Consumer Behaviour and Adoption to 2030.

[76] GSMA INTELLIGENCE. Understanding SIM Evolution, 2015.

[77] GSMA INTELLIGENCE. The Mobile Economy, 2024.

[78] HOSEIN, P., PACK, S., ET AL. Pricing esim services: Ecosystem, challenges, and opportunities. *IEEE Communications Magazine 61*, 7 (2023), 18–24.

[79] KIISKI, A., AND HÄMMÄINEN, H. Mobile virtual network operator strategies: Case finland. In *ITS 15th Biennial conference* (2004).

[80] LANGE, S., GRINGOLI, F., HOLLICK, M., AND CLASSEN, J. Wherever i may roam: Stealthy interception and injection attacks through roaming agreements. In *European Symposium on Research in Computer Security* (2024), Springer, pp. 208–228.

[81] LEE, K., KAISER, B., MAYER, J., AND NARAYANAN, A. An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth symposium on usable privacy and security (soups 2020)* (2020), pp. 61–79.

[82] LISOWSKI, T. P., CHLOSTA, M., WANG, J., AND MUENCH, M. {SIMurai}: Slicing through the complexity of {SIM} card security research. In *33rd USENIX Security Symposium (USENIX Security 24)* (2024), pp. 4481–4498.

[83] MANDALARI, A. M., LUTU, A., CUSTURA, A., SAFARI KHATOUNI, A., ALAY, Ö., BAGNULO, M., BAJPAI, V., BRUNSTROM, A., OTT, J., MELLIA, M., ET AL. Experience: Implications of roaming in europe. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (2018), pp. 179–189.

[84] MARTIN, J., ALPUCHE, D., BODEMAN, K., BROWN, L., FENSKE, E., FOPPE, L., MAYBERRY, T., RYE, E. C., SIPES, B., AND TEPLOV, S. Handoff all your privacy: A review of apple's bluetooth low energy continuity protocol. *arXiv preprint arXiv:1904.10600* (2019).

[85] MATHEW, A. Threats and protection on e-sim. *International Journal of Recent Technology and Engineering 9* (09 2020), 184–186.

[86] NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL (NPSTC). Broadband Network Requirements Task Force: Technical Working Group Report, 2012.

[87] NEWS.COM.AU. Sydney man wakes up to find he had lost $52,000 in terrifying phone hack, 2022. https://www.news.com.au/finance/money/costs/sydney-man-wakes-up-to-find-he-had-lost-52000-in-terrifying-phone-hack/news-story/3ffd94e41142776b5ac336c55f09dd06.

[88] RAMNEEK, R., HOSEIN, P., AND PACK, S. Secure and scalable esim service provisioning framework for mobile virtual network operators. In *2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS)* (2023), pp. 381–384.

[89] SAMANVITA, S., TRIVEDI, S. P., AND JAYANTHI, P. Testing of esim profile management. In *2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)* (2021).

[90] SINGH, S. Adoption of embedded subscriber identity module (esim) technology services by south african smartphone users for international roaming.

[91] SRDJAN GOMBAR . Cyber Management Alliance, Security Benefits of eSIMs Over SIM Cards for International Travel, 2024. https://www.cm-alliance.com/cybersecurity-blog/security-benefits-of-esims-over-sim-cards-for-international-travel.

[92] THE SUN. Phone hack warning as scam costs man his life savings. https://www.thesun.co.uk/tech/17114889/phone-hack-life-savings-sim-scam/, 2021.

[93] WALVEKAR, H., CHANDAK, M., AND KANADE, A. esim: Security aspects for privacy and protection of users.

[94] WEN, H., PORRAS, P. A., YEGNESWARAN, V., AND LIN, Z. Thwarting smartphone sms attacks at the radio interface layer. In *NDSS* (2023).

[95] YUAN, H., BALOIAN, A., JANAK, J., AND SCHULZRINNE, H. esim technology in iot architecture. *arXiv preprint arXiv:2401.04302* (2024).

[96] ZHAO, J., DING, B., GUO, Y., TAN, Z., AND LU, S. Securesim: rethinking authentication and access control for sim/esim. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking* (2021), pp. 451–464.

[97] ZHOU, Y., YU, Y., STANDAERT, F.-X., AND QUISQUATER, J.-J. On the need of physical security for small embedded devices: a case study with comp128-1 implementations in sim cards. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17* (2013), Springer, pp. 230–238.

A Amarisoft Callbox Used as a Private Network

Figure 8 shows the Amarisoft callbox, which was used as a private network to connect an eSIM. Amarisoft provided the eSIM for the callbox that we purchased. It is important to note that the server is not an Amarisoft product; instead, Amarisoft partners with a third-party service provider for the SM-DP+ server. We configured the keys and parameters on the callbox and downloaded the default eSIM profile. Since access to the SM-DP+ servers and the necessary certificates is restricted, it is not possible to design custom eSIM profiles. However, as we investigated, some providers claim to allow users to design eSIM profiles tailored for private networks.

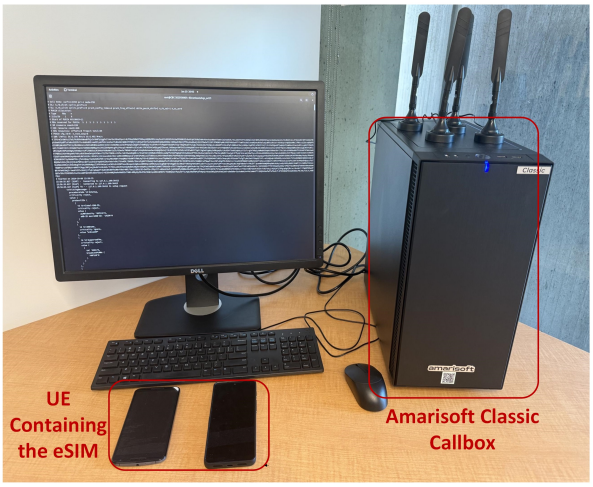

Figure 8: An eSIM was connected to our private network to capture logs and conduct experiments.

B Examining Network IP Assignments in Travel eSIMs

This screenshot serves as an example from one of the travel eSIMs we tested. As shown, the public IP address 223.118.51.96 is assigned through the connection to China Mobile's network and is visible when querying 'what is my IP' or similar services. Additionally, the addresses 10.118.87.179 and 10.118.87.180 are private IPs used within the carrier's internal network. These private IPs facilitate local communication, while the public IP 223.118.51.96 is used for internet access and represents the device's identity to external servers and services.

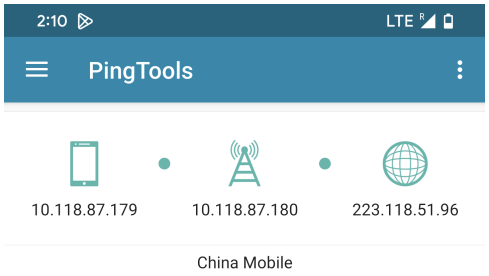

Figure 9: Network IP Assignments in Travel eSIMs

C eSIM Security Threats and Contributing Factors

Table 4 outlines the key security threats within the eSIM ecosystem, highlighting the primary risk factors associated with each threat. Specifically, each threat is characterized by the primary capabilities required by an adversary, the associ-

ated threat category, and the underlying issue type. The table highlights how eSIM adoption can produce unique threats to the ecosystem, that are not present in the traditional SIM deployments.

D Proactive Communication in Travel eSIMs

Figure 10 displays a portion of the captured communication in Wireshark for eSIM access, including commands for opening a channel, sending data, and closing the channel.

Table 4: eSIM-Specific Security Threats and Their Characteristics

Threat	Attacker Capabilities	Threat Category	Issue Type
eSIM Swapping	Social Engineering Operator Coercion	Identity & Account Takeover	Operational / Procedural
Untrusted Networks	Network, User Location and Data Control (e.g., MVNOs)	Surveillance & Traffic Interception	Ecosystem / Trust Model
Untrusted eSIM Providers	Profiles Injection and User Information Collection (e.g., eSIM resellers)	Privacy Breach Provisioning Abuse	Ecosystem / Policy
Malicious Profiles	SM-DP Infrastructure Access Malicious Profile Design	Remote Provisioning Injection	System Design & Implementation
Intercepting eSIM Deletion	Profile Deletion Request Interception (e.g., MitM)	Lifecycle Manipulation Protocol Tampering	System Design

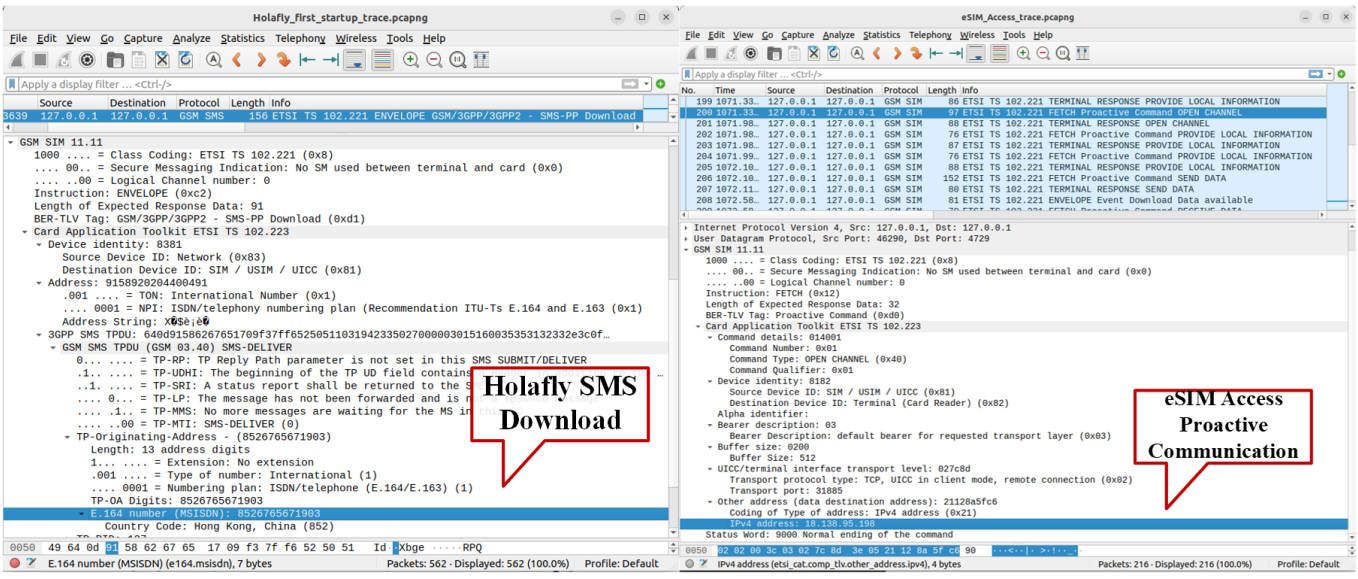

Figure 10: Wireshark showing the captured proactive communication for eSIM Access and Holafly.