ESYA centre

MOBILE SECURITY - AN ASSESSMENT OF CYBER SECURITY THREATS IN THE INDIAN ECOSYSTEM

NOVEMBER 2023 | ISSUE NO. 037

Mobile Security - An Assessment of Cyber Security Threats in the Indian Ecosystem

November 2023

Esya Centre
B-40 First Floor
Soami Nagar South,
New Delhi - 110017, India

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at www.esyacentre.org

Attribution: Karnal Singh and Lalantika Arvind. *Mobile Security - An Assessment of Cyber Security Threats in the Indian Ecosystem.* November 2023, Esya Centre.

About the Author: Karnal Singh is the former Chief of Enforcement Directorate, a cyber security expert and a lawyer specializing in white collar crimes and cyber crime investigations.

Contributor: Lalantika Arvind

CONTENTS

ABBREVIATIONS

AI	ARTIFICIAL INTELLIGENCE
API	APPLICATION PROGRAMMING INTERFACE
APP	APPLICATION
BIS	BUREAU OF INDIAN STANDARDS
CERT-In	COMPUTER EMERGENCY RESPONSE TEAM - INDIA
CVV	CARD VERIFICATION VALUE
ENISA	EUROPEAN UNION AGENCY FOR CYBERSECURITY
EU	EUROPEAN UNION
EU GDPR	EUROPEAN UNION GENERAL DATA PROTECTION REGULATION
IoT	INTERNET OF THINGS
IT Act, 2000	INFORMATION TECHNOLOGY ACT, 2000
IT Rules, 2021	INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021
MaaS	MALWARE AS A SERVICE
Malware	MALICIOUS SOFTWARE
MeitY	MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
NSCS	NATIONAL SECURITY COUNCIL SECRETARIAT
OEM	ORIGINAL EQUIPMENT MANUFACTURER
OS	OPERATING SYSTEM
OSOS	OPEN SOURCE OPERATING SYSTEM
OTP	ONE TIME PASSWORD
OWASP	OPEN WORLDWIDE APPLICATION SECURITY PROJECT

PII	Personal Identifying Information
RaaS	Ransomware as a Service
RBI	Reserve Bank of India
UPI	Unified Payments Interface

EXECUTIVE SUMMARY

Cyber security is of growing concern as India universalises digital access relying especially on public infrastructure. Cyber attacks can compromise critical infrastructure and personal data, diminishing trust in digital systems, and hampering growth across segments of the digital economy. Cyber threats from state or non-state actors, criminal organisations, hackers, and emerging threats AI and immersive technologies, pose a growing risk to financial, biometric, personal and state security. Almost a billion smartphones are connected in India, and it is reasonable to consider mobile security a national security priority.

Mobile security depends on two factors: device security and user awareness. The first includes measures adopted by handset manufacturers, operating system providers, and application developers. Given the pre-eminence of mobile internet use in India, mobile device vulnerabilities and low user awareness of security risks are the main threats to mobile system security.

Mobile device ecosystem is susceptible to operating system (OS) security concerns, untrusted third-party application (app) stores, and unchecked API sharing. These vulnerabilities can be mitigated to make it more difficult for attackers to exploit mobile systems. **Therefore, the domestic regulatory frameworks and discourses must prioritise system security and preventing device vulnerabilities.**

To minimise vulnerabilities and strengthen mobile ecosystem security, policymakers, legislators, regulators, and the courts adequately consider the implications of their decisions on cybersecurity outcomes. For instance, if a regulator is unsure whether a decision would have repercussions for cybersecurity, it should consult a relevant cybersecurity authority. The Bureau of Indian Standards can also issue mandatory standards for mobile OS and app stores to ensure more layers of security in the system, and data protection norms, such as data minimisation and purpose limitation, should be followed in API sharing.

Further, as user awareness and security literacy are critical pillars of mobile ecosystem security, public-private initiatives (such as collaborations between OS providers and CERT-In for user awareness campaigns) would also foster trust in digital systems.

CHAPTER 1: INTRODUCTION

India is well on its way to universalising digital access, with mobile penetration (including smartphone and other mobile users) growing to 76.6% in 2022.[1] The country had around 800 million mobile subscribers in March 2023,[2] and is expected to have a billion smartphone users by 2026.[3] At the same time, the World Economic Forum estimates that **cybercrime will amount to half the global digital economy by 2025, with much of it targeted at mobile users.**[4] Growing exposure to cyber threats is a natural corollary to the rapid growth in digital adoption in India as well. In 2022, data breaches cost Indian companies INR 17.6 crore,[5] and 30 crore people were vulnerable to cyber attacks in the country.[6]

By compromising critical infrastructure and the data privacy of individuals, cyber attacks have the potential to damage digital trust and hamper growth in the digital economy across market segments. It is reasonable therefore to consider mobile security a national security priority. The nodal legislation for India's digital economy, the Information Technology (IT) Act, 2000, addresses cybersecurity threats from a national security perspective. It defines cyberterrorism[7] as the intention to threaten the security of India and strike terror by the denial of access, or unauthorised access, to computer resources, including mobile devices. It also defines cyberterrorism to include the introduction of any computer-resource contaminant that causes death, disrupts essential services, or adversely affects critical information infrastructure.[8]

The IT Act also authorises the Union Government to take down any apps or websites that threaten the security of the State.[9] The Ministry of Electronics and Information Technology (MeitY) has used this provision to ban Chinese apps in the past,[10] and most recently to ban encrypted messaging apps in the Kashmir Valley.[11] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 also include provisions for blocking access to online games that threaten state security,[12] and the IT Act empowers the government to monitor, intercept or decrypt information in any computer resource in the interest of national security,[13] or to prevent cyber attacks.[14]

The IT Act is also the genesis for the Indian Computer Emergency Response Team (CERT-In) and the sectoral CERTs.[15] CERT-In is the national agency for cyber-incident response, and the IT Act empowers it to mandate emergency measures to ensure cybersecurity, and to issue guidelines and procedures for preventing cybersecurity incidents, including for mobile devices.

Further, the National Security Council Secretariat (NSCS) is the apex agency overseeing cybersecurity threats in India, and assists the National Security Council in advising the Central Government. It is headed by the National Security Advisor, who reports directly to the Prime Minister, advising them on all security matters, including pertinent cybersecurity issues. The National Cyber Security Coordinator also serves on the NSCS, and coordinates with various agencies at the national level on matters of cybersecurity, enabling information exchange.[16] In the event of mobile security risks or vulnerabilities, such as app misuse or the threat of Indians' sensitive data being accessed by untrusted governments, the NSCS can weigh in as its mandate includes intelligence assessments and analyses pertaining to internal and national security. In these institutions and laws, India has recognised the relationship between a secure mobile ecosystem and national security.

However, the security of the mobile ecosystem is dependent on two additional factors: overall device security, and the security awareness of mobile users. Device security comprises the security measures taken by handset manufacturers, operating system (OS) providers, and app developers. **Given the predominance of mobile internet connectivity over other forms of digital connectivity in India, device vulnerabilities or a lack of security awareness can gravely impact people's financial and personal data security.**[17] **They can also compromise critical infrastructure, endangering individual, economic, and national security.** Therefore,

domestic regulatory frameworks and discourses must prioritise building secure systems and preventing device insecurity.

This paper highlights the need to focus on mobile security so as to ensure overall cybersecurity, by examining the interplay between consumer protection and specialised regulatory frameworks. The second chapter provides a taxonomy of cybersecurity threats, and the third on the threats posed by unsecured mobile devices. The fourth chapter concludes the paper with recommendations for regulatory steps and first-principles that can foster a secure and robust digital ecosystem.

CHAPTER 2: TAXONOMY OF CYBERSECURITY THREATS

There has been an increase in cybersecurity attacks globally in recent years, especially on critical infrastructure. According to Microsoft's Digital Defense Report 2022, cyber attacks on companies in IT and financial services, transportation, and communications infrastructure accounted for 40% of total IT activities, from July 2021 to June 2022. Such attacks only accounted for 20% of activities in the preceding year.[18]

India is no exception. It witnessed 13.91 lakh cybersecurity incidents in 2022, according to CERT-In.[19] The attack on its premier medical institute, the All India Institute of Medical Sciences, was among the most prominent.[20] The perpetrators corrupted patient files stored on the hospital IT system, and held to ransom the sensitive health data of 4 crore patients, including senior government officials and ministers.

The growth in cyber attacks is of special concern to India, as it is in the midst of a digital transformation. Indian IT services exports amounted to USD 157 billion in 2021-22,[21] and it has become the first country[22] to develop the three foundational digital public infrastructures (of digital identity,[23] real-time payments via the Unified Payments Interface (UPI), and data sharing[24] – on India Stack, a set of open APIs and digital public goods. The government has also successfully implemented several service delivery platforms such as CoWIN (for Covid vaccine registration), the Ayushman Bharat Digital Mission (integrated digital healthcare infrastructure), DIKSHA (a learning platform for teachers and students), e-RUPI (person and purpose-specific digital vouchers for direct benefit transfers), and UMANG (for unified access to public services).[25] In fact, UPI transactions amounted to INR 126 lakh crore in 2022, growing by over 50% over the previous year.[26] The government has also rolled out DigiLocker, a secure cloud-based app enabling access to important documents such as driving licences and digital identity cards.

The government has also invested in internet and digital access through the Digital India Mission, with schemes like BharatNet, which aims to provide rural internet connectivity at affordable prices and has helped bring 846.6 million people online,[27] 812 million of them mobile subscribers, as of March 2023,[28] and has enabled the manufacture of affordable smartphones.[29] These efforts in digital transformation have led to rapid mobile adoption, and as a consequence, mobile dependence.

Mobile phones have come to be used for everything, from payments to healthcare, and even the use of drones.[30] It is evident that Indian users trust mobile technology, but this trust is a double-edged sword, as it increases the risk and potential impact of security vulnerabilities. A compromised smartphone may lead to financial and data loss for individuals, but it may also compromise national security and critical infrastructure. Thus, fostering mobile security is integral to maintaining people's trust in digital systems, and it is important to understand what makes these systems vulnerable. The next section provides a taxonomy of cybersecurity risks.

The digital economy contributes 15% to global GDP,[31] and is growing at twice the rate of the remainder. Festering cybersecurity risks may harm user trust and hinder overall economic growth. A taxonomy of such risks allows us to understand the role played by institutional actors in mitigating them, and how the relevant institutions can deepen their focus on preventing these risks.

2.1. Modus operandi of cyber attacks[32]

Cybercriminals can compromise communication networks or computer systems via friendly entry or hacking. These are elaborated below.

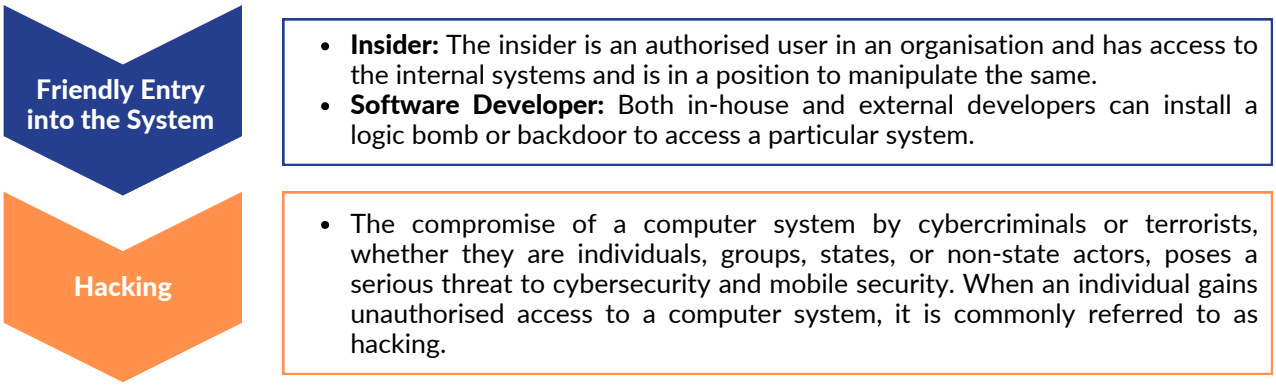

Figure 1: Modus Operandi of Cyber Attacks

Vulnerabilities, threats, exploits, and associated risks are the four fundamental dimensions of security. Understanding each of these is important in developing effective security measures to protect against an attack or breach.

A. Vulnerabilities

In cyberspace, vulnerabilities are structural weaknesses or flaws in hardware, software or network systems that can be exploited by hackers or other actors to gain unauthorised access, steal data, disrupt operations, or otherwise cause damage. Vulnerabilities may emanate from errors in design, coding or configuration, or from outdated or unpatched software, misconfigured systems, or human error. The common vulnerabilities in digital systems can be divided into hardware, software, network and human vulnerabilities, outlined below.

HARDWARE VULNERABILITIES	SOFTWARE VULNERABILITIES	NETWORK VULNERABILITIES	HUMAN VULNERABILITIES
• Weaknesses in hardware devices or components that can be exploited by attackers to gain access or control over a system. • Examples include firmware vulnerabilities, etc.	• Weaknesses in software code or applications that can be exploited by attackers to gain access or control over a system. • Examples include buffer overflow, SQL injection, and cross-site scripting vulnerabilities. Many of these vulnerabilities are detected and exploited by hackers. After the developer is made aware of these vulnerabilities, the developer modifies the code and issues patches to the users. • Manufacturers in some countries deliberately leave security holes while exporting the systems to other countries so their countries can exploit it for spying or bringing down the systems of the other country at will.	• Weaknesses in network infrastructure or protocols that can be exploited by attackers to intercept or manipulate data, or to gain access to a network. • Examples include weak passwords, unsecured Wi-Fi networks, and unpatched routers.	• These are weaknesses in human behaviour or decision-making that can be exploited by attackers to gain access or trick users into divulging sensitive information. • Examples include phishing attacks, social engineering, and weak passwords.

Figure 2: Common Vulnerabilities

B. Threats

A cyber threat is something with the desire and capacity to infiltrate cyber systems and cause damage. A cyber threat may emanate from external factors – state or non-state actors, criminal organisations, terrorists, hackers – or internal factors, such as former or current employees.

External Threat Factors

State and Non State Actors

- State and non-state actors are increasingly resorting to cyber warfare since physical wars are costly and result in huge loss of life. Cyber weapons are cheaper, readily available and enable repositioning (i.e malware can be injected into crucial spots and activated whenever desired).
- Non-state actors may also carry out cyberattacks on behalf of nations.

Cybercrime Organizations or Cyber criminals

- These criminals seek commercial gains by hacking banks, financial institutions and through phishing scams and ransomware.

Terrorist Organizations

- Terrorist groups aim to penetrate and attack critical assets and national infrastructure in order to cause disruption, chaos, and fear. Their goals may be political, ideological, or religious, and they may use cyberattacks to achieve their objectives.
- For example a terrorist group may launch a cyberattack on a power grid or a transportation system to cause widespread disruption and create fear among the population.

Hackers or Hacktivists

- These are individuals or groups who use their technical expertise to gain unauthorised access to computer systems for various reasons, such as political, social or personal agendas. Groups such as 'Anonymous' are well-known examples of hacktivists who use hacking as a means to raise awareness and draw attention to various issues.
- However, there are also malicious hackers who exploit vulnerabilities in computer systems for personal gain or to cause harm to individuals or organisations.

Threat of Harassment

- Cyberattacks committed with the intention of harassment are commonly referred to as cyberstalking or online harassment. This type of behaviour can take many forms, including attempts to gain unauthorised access to personal accounts or devices.

Figure 3: External Threat Factors

C. Exploits

Exploits are the tools or techniques used to breach security and infect a targeted system. They include code that takes advantage of software bugs, malicious scripts that exploit vulnerabilities in a web application, and social engineering attacks that exploit human weaknesses. Exploits can be created by the attackers themselves or purchased on the dark web, making them easily accessible both to novice and experienced cybercriminals.

D. Risk

In the context of cybersecurity, risk is the likelihood of a vulnerability being exploited, and the potential damage caused by such an exploit. The risk associated with a cyberattack depends on several factors, including the value of the information or assets targeted, the motivation and ability of the attacker, and the effectiveness of the security measures in place to prevent, detect and respond to such an attack. Effective risk management involves identifying and prioritising risks, implementing appropriate security controls, and continuously monitoring and assessing their effectiveness, to minimise the impact of a cyberattack.

Some specific and significant cyberattacks associated with mobile systems are briefly described below, with details in the Annexure.

CYBERATTACK	DESCRIPTION
Malware (short for malicious software)	Any software created deliberately to perform an unauthorised, often harmful, action, including to damage or disrupt a system or attack its confidentiality, integrity, or availability.[33] From 2020-21, India witnessed an 845% increase in mobile malware attacks, with 12,719 attacks per day in 2021.
Malicious Apps	Apps that contain malware, and can cause harm to users, including through stealing and collecting user data. Mobile malware can be used to mount targeted attacks against mobile device users, and smartphones and tablets are susceptible to worms, viruses, trojans and spyware similar to desktops.[34]
Malvertising	The use of online advertisements to distribute malicious programs. Malicious actors embed a special script in a banner or redirect users who click on an ad to a special page that executes code for downloading malware.
Ransomware	Malicious software that encrypts data or otherwise blocks access to it, unless the user pays to unlock or decrypt the data. Ransomware can also be used to access an individual's private data, such as photos and videos, with the attackers demanding money in exchange for not leaking it. India ranked at 10 globally in the number of ransomware attacks in 2021, and 42% of complaints were from Maharashtra.
Phishing	Social engineering tools used to trick users into revealing personal information, such as passwords or credit card numbers, by using fraudulent emails, messaging apps, or phone calls. Socially engineered prompts are also used to entice users into downloading malicious apps that steal personal identifying information (PII). Phishing has overtaken malware as the foremost form of online attack, and India witnessed over 17 lakh phishing attacks per day between April and June 2022.
Financial fraud	Besides phishing and malicious apps, the Reserve Bank of India (RBI) has noted that fraudsters are also scamming people in India into downloading screen-sharing apps. They use these apps to gain remote access to a user's mobile phone or computer, gaining access to sensitive information like a one-time password (OTP) or bank card verification value (CVV) number.

2.2. Tools exploiting emerging technology

While there is extensive documentation of the aforementioned threats , the use and misuse of emerging technologies also poses significant cybersecurity concerns.

Artificial intelligence (AI), for example, is a great tool for enhancing human productivity. However, its misuse can lead to increasingly sophisticated attacks. The ChatGPT tool has been used by malicious actors to create code that can steal sensitive information, download malware and run decryption functions.[35] AI models pose a further risk due to their lack of design and development transparency, which can make it difficult to identify vulnerabilities.[36] AI and machine learning tools can also be used to conduct largescale, automated cyber attacks.[37] The forthcoming Digital India Act is likely to overhaul the IT Act and build guardrails around emerging technologies such as AI.[38] It presents an important opportunity to enact regulations to protect against AI cybersecurity concerns, such as design transparency and content moderation requirements.

In the realm of emerging technologies, the interconnected nature of **Internet of Things** (IoT) devices also poses a cybersecurity risk. Vulnerabilities in device software can be exploited to access sensitive personal information in breach of privacy. In the Verkada attack,[39] for instance, attackers exploited vulnerabilities in cloud-based video surveillance facilities to access footage from 150,000 CCTV cameras in hospitals, schools, and other facilities, and the personal information of those surveilled. The growing adoption of IoT devices also compounds existing vulnerabilities, as malware or a virus in one device can go on to infect others on the network.[40] As **5G and subsequent technologies** (6G and beyond) enable wider use of IoT devices, the vulnerabilities associated with mobile networks will increase.[41] This is a grave concern, as an untrusted 5G supply chain increases the risk of software/network tampering by malicious actors.[42]

The next stage of mobile technology, **immersive technology**, includes virtual reality, mixed reality and augmented reality, which offer an interactive, immersive user experience, but also increase the risk of a cybersecurity breach. Devices such as smart headsets or smart glasses are susceptible to hacking by threat actors,[43] putting sensitive biometric information such as iris scans and fingerprint information at risk. Hackers are also able to access data such as facial expressions and speech patterns, and replicate them for identity theft. Further, virtual reality simulations of terrorist attacks may be used by malicious threat actors to radicalise individuals or cause widespread panic.[44] Interpol is preparing against the risks posed by immersive technologies such as the “metaverse”, given that they can facilitate largescale cyber attacks.[45]

While it is positive that Indian users currently trust mobile technology and are fostering its use, it is important to maintain and strengthen their trust. This will require empowering users through digital literacy initiatives, and mandating standardised security protocols for all connected devices, including IoT and mobile devices. We expand on these in the following chapter.

Cybersecurity threats have adverse implications for the security of financial information, biometric and personal information, and the state. The evidence shows grave threats on the horizon that need to be addressed by focusing on mobile security.

The mobile device ecosystem is also susceptible to harm from OS security concerns and untrusted third-party app stores. These risks can be mitigated if the vulnerabilities in mobile systems are closed, to make it more difficult for attackers to exploit these systems. The next chapter is a deep dive into mobile security concerns, the root causes of common vulnerabilities, and the need to ensure mobile security at multiple layers.

CHAPTER 3: ANALYSIS OF MOBILE SECURITY VULNERABILITIES

Mobile ecosystem intermediaries play an important role in building trust in digital systems, and regulations on intermediaries (such as India's IT Rules, 2021 and the EU's Digital Services Act) have been instituted at the global level. Regulators have also created mobile security guidelines with differentiated obligations for various actors in the ecosystem. App developers, for instance, must follow the secure app obligations and directions in the EU's 2016 Smartphone Secure Development Guidelines, and in India the draft Mobile Device Security Guidelines place security obligations on app developers, OS creators, and device manufacturers. In the United States, the Federal Trade Commission has brought privacy enforcement actions against mobile manufacturers,[46] app developers,[47] and mobile advertising networks.[48]

The worldwide recognition that different actors in the mobile ecosystem play a crucial role in securing the ecosystem as a whole is because vulnerabilities in mobile systems can emanate from hardware as well as software. This chapter discusses the most common sources of software vulnerabilities, including mobile operating systems (OS), application software (including third-party apps), and the unchecked sharing of application programming interfaces (APIs).

3.1. Mobile operating systems (OS)

Mobile OS is the software enabling a mobile device to run programs, tasks and functions. **A mobile OS is also responsible for ensuring the device is protected at the software layer,**[49] which is why OS developers issue frequent software updates to close vulnerabilities. Conversely, an insecure OS fails to prevent[50] attacks on the software layer of a mobile phone. For instance, tampering with the API design causes a breach that is exploited by attackers to gain control of the system and access the personal and sensitive data stored on the phone. Such vulnerabilities can also be installed by malicious apps that also spread the malware to other apps installed on the phone. The Bureau of Indian Standards (BIS) considers verifiable OS protection (ensuring that the OS and application updates come from a valid source) an integral part of device security and integrity safety.[51]

There are three kinds of mobile OS, closed source or entirely proprietary OS, partially proprietary OS, and open-source OS (OSOS).

Closed source OS, such as Apple's iOS, is entirely proprietary, and its source code is available only to the development team. Others can only access the object code, which is in machine language and cannot be modified or researched further.

Open-source OS (such as in the Android Open Source Project) is one made available to the public for research and modification. To use the Android logo and brand name along with its source code on mobile devices, original equipment manufacturers (OEMs) are required to sign a compatibility licence agreement with its proprietor Google.

An open-source OS with a robust developer ecosystem offers many security benefits, such as faster and continuous vulnerability checks. Android has multiple stakeholders, including researchers, software developers, ethical hackers, Google employees, and teams of various Android licensees, constantly working to identify and close vulnerabilities.

Google's compatibility agreement with OEMs further requires licensees to undertake certain baseline security measures. As a result, wherever Android is used on a mobile device, user trust is maintained, given

the security offered by the compatibility agreement. In fact, the so-called zero-day bounties for ethical researchers to identify vulnerabilities are highest for Android devices, as it is difficult to identify Android vulnerabilities that are not already well known.[52]

Others believe, however, that closed-source software is more secure, as its code can be viewed by fewer actors. This is a misconception. While the number of vulnerabilities identified by third-party researchers may be lower because the source code has not been made public, the number of zero-day vulnerabilities in the code may in fact be higher. This is because the OSOS is constantly scrutinised by OEMs, researchers and developers, in addition to the dedicated development team. Thus, many OSOS vulnerabilities are detected and plugged in the development phase. During the early development stages of Apple iOS and Google Android, iOS did have fewer zero-day vulnerabilities.[53] This was partly due to a lack of research into iOS vulnerabilities, according to experts.[54] Comparing the vulnerabilities today, the extensive investment by numerous stakeholders has paid off, and Android has fewer vulnerabilities.[55]

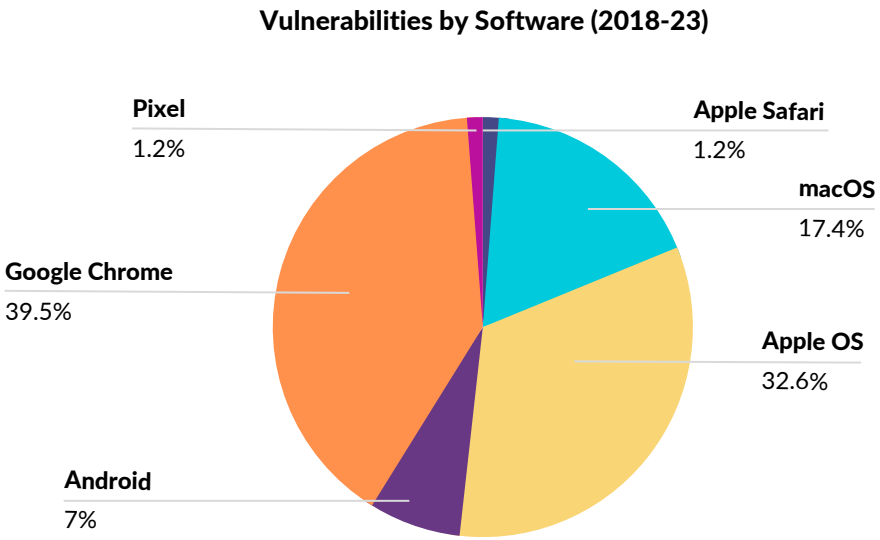

Figure 4: Vulnerabilities by Software (2018-2023);
Source: Zero Day, 2023

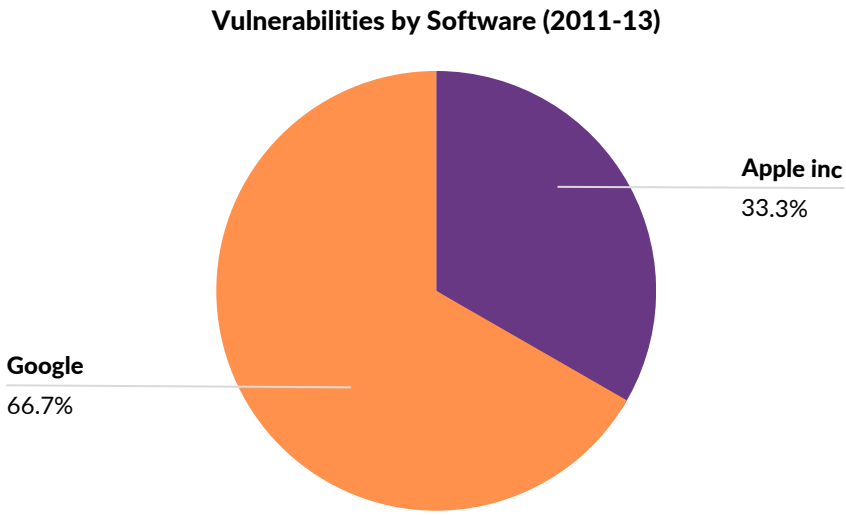

Figure 5: Vulnerabilities by Software (2011-2013),
Source: Zero Day, 2023

This does not mean that iOS is particularly vulnerable to security breaches. Both iOS and Android have achieved a mature software development lifecycle stage, enabling improved efficient security features for users.[56] As with Android, Apple also has a dedicated team constantly monitoring for vulnerabilities and releasing software patches periodically. In the indicative list below, we show the common security features employed by most mobile operating systems, regardless of the nature of their source code.

The common security features across secure OS include:[57]

- **Data encryption:** Helps protect data from unauthorised access.
- **App sandboxing:** Isolates each app from other apps, making it harder for malware to spread.
- **App permissions:** Let users control which apps have access to their data and device features.
- **Software updates:** Include security patches that can help protect devices from known vulnerabilities.

These security features are implemented by mobile OS designers and device manufacturers to protect users and their data from unauthorised access, modification or destruction. For example, Russian hackers used a popular cash-earning app to install malware inside Indian phones that gave them access to the microphone, location, camera, biometric sensors and WiFi controls, in 2022.[58] Criminals also misused Apple's Enterprise Developer Programs to trick users into installing apps that defrauded them of money.[59] **OS features like application sandboxing can help prevent this type of malware from spreading.**

Further, OS features like app permissions do not grant an app permission to use the camera, microphone, or other device resources by default. Thus, malware developers must trick the user into giving the app such permissions, above all by exploiting people's lack of awareness about such threats to security. It is for this reason that user awareness is a crucial aspect of OS and mobile security. Users must also install OS updates regularly, since even if the malicious app is removed from the device, certain malware can re-install itself by exploiting OS vulnerabilities.[60] This highlights the importance of OS security updates and user awareness for ensuring device security.

A. Security risks of incompatible software

Incompatible OS is a key risk vector in digital security. For instance, an Android fork is a modified version of the Android OS created by a third party. Amazon Fire OS is an example of an incompatible Android fork, which is partially proprietary in nature. While it is based on Android, it lacks the security compatibility features installed on Android devices. Incompatible Android forks such as Fire OS are not inherently insecure, but they are more vulnerable to security issues than Android OS.[61] Their lack of baseline compatible security features can result in inadequate ability to offer security checks and regular security updates. Thus an increase in incompatible Android forks may lead to an increase in vulnerable devices on the market.

However, Android forks cannot completely be avoided or "banned" since they act as an OS entry gateway for many smaller companies, especially because Apple does not license its OS. In such a scenario, harmonising and mandating baseline security requirements for OSes (such as through BIS standards) may improve baseline security in mobile operating systems.

3.2. API sharing risks

An application programming interface (API) is software that lets two apps communicate with each other and enables user interaction with an app. This requires data sharing, and APIs facilitate the transfer and harvesting of user data.[62] The data is essentially used to scale app development for a particular platform. For instance, a social network might share its API with developers to facilitate in-app features such as games.[63]

Given the volume and kind of data accessed by APIs, they are a key target for security breaches.[64] An API data

breach can occur due to data exposure, where user data has been shared with the front end without enabling any filters (which would restrict the shared data only to that required by the developer, or would encrypt or tokenise the data). In such a case it is easy for attackers to bypass the front end that receives unfiltered data, and access the personal identifiable information of app users. Unsecured APIs can be exploited by malicious actors, including foreign threat actors, to facilitate malware attacks,[65] data breaches and surveillance activities, given the easy availability of the relevant code. A data breach in Twitter's API in 2021 allowed hackers to gain access to user email IDs and contextual information that was used to launch social engineering attacks in 2023.[66]

An absence of data protection obligations in API sharing agreements also allows malicious actors to exploit data without users knowing. The Cambridge Analytica data breach of 2018 is an example of this.[67] Facebook's GraphAPI let third-party applications extract user data (including login details such as email IDs) and integrate it with their applications.[68] Moreover, the API permitted access to the data of users of the third-party app *and* to the data of their Facebook friends. The third party, a quiz offered by data scientist Dr Aleksandr Kogan, had access to user email IDs, locations, photos, status updates and check-ins. This data was profiled and sold to the consulting company Cambridge Analytica, enabling access to the data of nearly 50 million users.[69] This highlights the importance of data protection obligations under API sharing agreements.

The EU General Data Protection Regulation (GDPR) requires that user data be shared with a third party only within the contours of a data-sharing agreement. It also requires that data protection principles[70] such as data minimisation (wherein data is collected for specified, explicit and legitimate purposes and not processed further in a manner incompatible with those purposes) and purpose limitation (wherein the data processed is relevant and limited only to what is necessary in relation to the processing purposes) be followed. Thus, any application sharing APIs would share and process personal information in a limited, specific manner, that has been consented to, in a valid contract. In this regard, India has taken a significant step in enacting the Digital Personal Data Protection Act, of 2023, to ensure the protection of personal data from breaches of security, including through API sharing. At times, even in the absence of data protection legislation, the proprietary nature of APIs has been used to enforce data protection measures and security obligations.

As APIs allow developers to scale and foster rapid innovation, regulators might mandate their unconditional sharing.[71] As documented in this chapter, there are serious security and privacy consequences to unregulated and unchecked API sharing that must be assessed before making any such mandates. Chapter 4 provides recommendations for the same.

3.3. Third-party app stores

To expand consumer choice and foster the growth of smaller developers, many OS providers let users download apps from third-party app stores, or directly via web browsers. The latter is known as *sideloading*. As discussed in the previous chapter, malicious apps are a key means for threat actors to attack mobile devices. The Maharashtra police caught a racket of predatory loan apps used for ransomware attacks with links to China and the UAE in 2022.[72] The apps gained access to private data such as photos and contact lists, and the non-repayment of loans resulted in morphed images of users being shared with their contacts.

User safety and consumer benefits go hand in hand, and to ensure security, OS providers like Android display warnings to users who undertake sideloading. This prevents users who are less aware of the security risks from potentially installing malicious applications and risking their data privacy.[73] Such disclaimers are a crucial aspect of device and OS integrity. In fact, the IT Rules 2021 require intermediaries to prevent users from publishing content that contains software that can limit or destroy the functionality of a computer device.[74] Because app stores are intermediaries, they have an obligation to ensure user security under the IT Rules. Even an OS, when facilitating third-party interactions,[75] such as an app downloaded from a third-party resource (such as sideloading), is an intermediary, and has the same obligation under the regulations.

One of the largest drivers of mobile phone attacks are unverified third-party app stores. The details of 20 million users, including their personal information and sensitive passwords, were leaked by hackers of a third-party app store, Aptoide, in 2020.[76] It has been found that third-party app stores are five times riskier to use than verified app stores,[77] and they can also facilitate cybercrime by hosting[78] prohibited content such as gambling apps or pornography.[79] In fact, fraudulent copies of well-known app stores have been used by malicious actors to steal information and blackmail users.[80]

However, security features of Android OS such as 'Play Protect' also work when the device is offline.

To deal effectively with the risks posed by app stores, organisations such as the EU Agency for National Cybersecurity (ENISA) and the Open Worldwide Application Security Project (OWASP) have published security guidelines for mobile app developers. These are discussed in the next chapter as effective measures to enforce app security in the system.

Cybersecurity frameworks that do not consider the diverse array of risks presented here may endanger the mobile ecosystem. The next chapter recommends specific regulatory steps and first-principles for enhancing the security of mobile ecosystem.

CHAPTER 4: RECOMMENDATIONS

It is important to strike a balance in ensuring national security, consumer protection (including consumer choice) and the rights of manufacturers and developers. A step toward this would be to distinguish those elements of mobile OS and app store design, access requirements, and prohibitions that ensure cybersecurity from those that restrict consumer benefits and choices.[81]

Due diligence

A key metric for adjudicating whether a legislation or regulatory decision carries cybersecurity implications is the test of proportionality.[82] It is critical to ensure that any legislation or regulatory decision is well-reasoned and does not *reduce* existing security standards of an ecosystem.[83] Policymakers, lawmakers, regulators and the courts must adequately consider the cybersecurity implications of their actions. If a regulator is unsure whether a particular decision has repercussions for cybersecurity, it should consult a relevant cybersecurity authority.

Standardisation

Technical differences in the kinds of mobile OS available in the market can lead to varying levels of security across the mobile ecosystem. To ensure greater security, the BIS can mandate OS providers and hardware manufacturers to undertake a set of baseline security practices, which may include app sandboxing, data encryption, and app permissions.

To reduce the risk posed by third-party app stores, standards like the OWASP's Verification Guide for Secure Mobile Applications can aid in securing app stores.[84] This is done by verifying the security of an app's data storage, inter-app communication, the use of cryptographic APIs, and secure network communication. The United Kingdom has also released a voluntary Code of Practice for app stores and app developers,[85] which requires these entities to prioritise security practices including baseline privacy measures, obligations for vulnerability disclosure and data protection, ensuring that apps are up to date, and providing security information to users.

Despite standardisation requirements, malicious actors may wilfully disregard them. Thus to ensure maximum device security, it is important to isolate app stores and prevent instances of "app stores within an app store" that happen without the knowledge or consent of both parties.

Data protection and data sharing

To effectively counter the risks of unchecked API sharing, data protection norms must be adhered to. The Indian Digital Personal Data Protection Act, 2023 (DPDP) requires that steps be taken to prevent personal data breaches and that any data processing be done for a consented purpose. Principles such as data minimisation and purpose limitation underpin the legislation since data can only be collected and processed for a consented purpose.

On the software protection layer, OWASP's technical standards for app and OS security also require developers to limit access to the data shared while sharing APIs to ensure maximum security. The BIS too can consider implementing such technical specifications for API sharing and app developers.

Self-regulation

According to the ENISA, protections for securing users from app store vulnerabilities[86] include app review (app stores must review apps and their security features before making them available on their platform), reputation mechanism (users and the app store rate and review an app based on the level of security it provides to users), app revocation/ kill-switch (the ability of app stores to remotely revoke apps), and application sandboxing. ENISA also recommends "wall-gardening" app stores (to ensure users can only download apps from specified app stores), but acknowledges this must be done in a manner that does not hinder competition. Given that sideloading and third-party app stores are important for smaller entities, adhering to the four other security measures would help reduce the adverse impact of sideloading and third-party app stores.

User awareness

While the above measures can be taken by ecosystem entities, user awareness and security literacy are also crucial pillars of mobile ecosystem security. The Indian Cyber Crime Coordination Centre under the Ministry of Home Affairs runs user awareness programs to inform people of threats related to cybercrime, how to protect their devices, and what to do if they are targeted in such crimes. The process can be strengthened by partnering with mobile ecosystem players such as smartphone makers and app stores to run awareness campaigns through videos, informative emails, and by creating awareness resources like handbooks.

Similarly, CERT-In under MeitY is responsible for the constant monitoring of threats, and it regularly notifies vulnerabilities in popular apps like internet browsers, encouraging users to update to the latest versions to ensure maximum security.[87] Public-private initiatives such as collaborations between OS providers and CERT-In on cybersecurity awareness campaigns for users can also foster trust in digital systems and improve cybersecurity literacy.

ANNEXURE 1 : TAXONOMY OF CYBERSECURITY THREATS

- *Malware* (short for malicious software): Any software created deliberately to perform an unauthorised, often harmful, action, including damaging or disrupting a system and attacking its confidentiality, integrity, or availability.[88] For example, malware like SQL Injections exploit vulnerabilities in the code to gain access to valuable information. SQL is a query language used in programming to access, modify, and delete data stored in relational databases, and most websites and web applications rely on SQL databases.

  The emergence of the MaaS (malware as a service) business model, where the owners of MaaS servers offer paid access to a software and hardware botnet that distributes malware for carrying out cyber attacks, has reduced the costs of such attacks and made them more prevalent. From 2020 to 2021, India witnessed an 845% increase in mobile malware attacks, with 12,719 attacks per day in 2021.

- *Malicious apps:* Apps that contain malware, and can cause harm to users, including by stealing and collecting user data. Mobile malware can be used to mount targeted attacks against mobile device users and smartphones or tablets that are susceptible to worms, viruses, trojans and spyware similar to desktops.[89] Users may unknowingly access harmful cloud-based apps where they sync their data, giving the app access to private and sensitive information, where it may create copies of it. Vulnerabilities in the code of existing apps can also be exploited by malicious actors to listen in on calls or perform remote code execution.[90] CERT-In has recognised the threat posed by malicious apps and it is mandatory to report such incidents to the agency. Google banned 36 malicious apps that could spy on users' GPS location, collect lists of the applications installed on a phone, and gather a history of Wi-Fi and Bluetooth device information in April 2023.

- *Malvertising:* The use of online advertisements to distribute malicious programs. Malicious actors embed a special script in a banner or redirect users who click on an ad to a special page containing code for downloading malware. Special methods are used to bypass large ad network filters and place malicious content on trusted sites. In some cases, visitors do not even need to click on a fake ad – the code executes when the ad is displayed. For example, Goldoson is a prevalent mobile malware that loads web pages without the user's consent or knowledge.

- *Ransomware:* Ransomware is malicious software that encrypts or otherwise blocks access to data, unless the user pays to unlock or decrypt it. Ransomware can also be used to access individuals' private data, like photos and videos, with the attackers demanding money in exchange for not leaking it. Varieties of malware target both desktop systems and mobile devices. Increasingly, malicious actors are participating in the RaaS (Ransomware-as-a-Service) business model, whereby malware developers lease out ransomware and its control infrastructure to other cybercriminals. The RaaS ecosystem has proliferated through the darknet, where there are specialised marketplaces selling malware and other tools.

  India ranked 10th worldwide in the number of ransomware attacks in 2021, with 42% of the complaints from Maharashtra. The Maharashtra police caught a racket of predatory loan apps used for ransomware with links to China and UAE in 2022. The apps received access to private data such as photos and contact lists, and the non-repayment of loans would result in morphed images being shared with user contacts.

- *Phishing:* These are techniques used to trick users into revealing personal information, such as passwords or credit card numbers, by using fraudulent emails, texts, or phone calls. Phishing has overtaken malware as the foremost form of attack, and India witnessed over 17 lakh phishing attacks every day from April to June 2022.

- *Spear phishing:* This is a type of phishing targeted at a specific individual or organisation. Generally intended to steal data, it can also be used to install malware. Spear phishing was notably used to target employees of the US Department of Defense, with more than 10,000 tweets tailored to the employees being shared during the 2016 presidential elections. More recently, the United Kingdom issued an advisory against Iranian and Russian spear-phishing attacks earlier in 2023.

- *Financial fraud:* In the Indian context, besides malware and phishing, the Reserve Bank of India has noted that fraudsters are frequently scamming people into downloading screen-sharing apps. They use these apps to gain remote access to a user's mobile phone, giving them access to sensitive information like one-time passwords (OTPs) and bank card verification value (CVV) numbers. CERT-In has also warned users of a rise in banking trojan malware attacks, wherein malware hidden inside apps disguised as legitimate browsers or other tools is used to capture login credentials when users log into net banking applications.

ENDNOTES

1 "India: Mobile Phone Penetration Rate 2026." *Statista*, https://www.statista.com/statistics/1373584/india-mobile-phone-penetration-rate/. Accessed 3 Aug. 2023.

2 Telecom Regulatory Authority of India. *Highlights of Telecom Subscription Data as on 31st March, 2023.*, https://www.trai.gov.in/sites/default/files/PR_No.46of2023_0.pdf. Accessed 3 Aug. 2023.

3 Press Trust of India, "India to have 1 billion smartphone users by 2026: Deloitte report". Business Standard. 22 Feb. 2022. https://www.business-standard.com/article/current-affairs/india-to-have-1-billion-smartphone-users-by-2026-deloitte-report-122022200996_1.html. Accessed 3 Aug. 2023.

4 "Why Digital Trust Is Key to Building Thriving Economies." *World Economic Forum*, 17 Aug. 2022, https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/. Accessed 3 Aug. 2023.

5 Lele, Sourabh. "India sees sharp rise in cyber attacks as internet base continues to widen". Business Standard, 7 Aug. 2022. https://www.business-standard.com/article/technology/india-sees-sharp-rise-in-cyber-attacks-as-internet-base-continues-to-widen-122080700773_1.html. Accessed 3 Aug. 2023.

6 Press Trust of India. "Around 5 Lakh People Potentially Fall Victim to Phishing Scams in India: Report." The Economic Times. 3 Mar. 2023. https://economictimes.indiatimes.com/tech/technology/around-5-lakh-people-potentially-fall-victim-to-phishing-scams-in-india-report/articleshow/98393025.cms. Accessed 3. Aug. 2023

7 Section 66F. Information Technology Act, 2000. Ministry of Electronics and Information Technology.

8 Section 66F. Information Technology Act, 2000. Ministry of Electronics and Information Technology.

9 Section 69A. Information Technology Act, 2000. Ministry of Electronics and Information Technology.

10 "Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order.", *Press Information Bureau*, 29 Jun. 2020, http://pib.gov.in/PressReleseDetail.aspx?PRID=1635206. Accessed 3 Aug. 2023.

11 ANI News. "Centre Blocks 14 Apps in Jammu and Kashmir for Spreading Terror". 1 May 2023. https://www.aninews.in/news/national/general-news/centre-blocks-14-apps-in-jammu-and-kashmir-for-spreading-terror20230501095505/. Accessed 3 Aug. 2023.

12 Rule 4C, Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf

13 Section 69. Information Technology Act, 2000. Ministry of Electronics and Information Technology.

14 Section 69B. Information Technology Act, 2000. Ministry of Electronics and Information Technology.

15 Section 70B. Information Technology Act, 2000. Ministry of Electronics and Information Technology.

16 "Cyber Security", *Ministry of Home Affairs*, 18 Dec. 2018. *Press Information Bureau*, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474. Accessed 3 Aug. 2023.

17 India has transformed itself as a mobile-first consumer economy: InMobi report". *Exchange4Media*, 19 Jan. 2021, https://www.exchange4media.com/digital-news/india-has-transformed-itself-as-a-mobile-first-consumer-economy-inmobi-report-110341.html. Accessed 3 Aug. 2023.

18 Microsoft Security. *Digital Defense Report 2022*. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022. Accessed 3 Aug. 2023.

19 Thathoo, Chetan. "India Witnessed 13.9 Lakh Cybersecurity Incidents In 2022: Govt." *Inc42 Media*, 11 Feb. 2023, https://inc42.com/buzz/india-witnessed-13-9-lakh-cybersecurity-incidents-in-2022-govt/. Accessed 3 Aug. 2023.

20 Srivastava, Ashish. "AIIMS Delhi: Held to Ransom by Cyber Attack." *The New Indian Express*, 28 Nov. 2022, https://www.newindianexpress.com/cities/delhi/2022/nov/28/aiims-delhi-held-to-ransomby-cyber-attack-2522960.html. Accessed 3 Aug. 2023.

21 Digitalizing India: a force to be reckoned with'", Ernst and Young, 2023, at page 9, https://www.ey.com/en_in/india-at-100/digitalizing-india-a-force-to-reckon-with. Accessed 3 Aug. 2023.

22 Saran, Samir and Sharad Sharma. *Digital Public Infrastructure – lessons from India'*, available at < https://www.orfonline.org/research/digital-public-infrastructure-lessons-from-india/ >

23 "Unique Identification Authority of India." *Government of India*, https://uidai.gov.in/en/. Accessed 3 Aug. 2023.

24 Ministry of Finance, Government of India. "Know all about Account Aggregator Network - A Financial Sharing System". *Press Information Bureau*, 10 Sep. 2021, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713. Accessed 3 Aug. 2023.

25 Ernst and Young, *'Digitalizing India: a force to be reckoned with'*, 2023, at page 10, available at < https://www.ey.com/en_in/india-at-100/digitalizing-india-a-force-to-reckon-with >

26 Das, Basudha. "UPI dominated digital transactions in 2022, payments worth Rs 126 lakh crore recorded, says report". *Business Today*, 19 Apr 2023. https://www.businesstoday.in/industry/banks/story/upi-dominated-digital-transactions-in-2022-payments-worth-rs-126-lakh-crore-recorded-says-report-377991-2023-04-19. Accessed 3 Aug 2023.

27 Telecom Regulatory Authority of India. *Highlights of Telecom Subscription Data as on 31st March, 2023*., https://www.trai.gov.in/sites/default/files/PR_No.46of2023_0.pdf. Page 2. Accessed 3 Aug. 2023.

28 Telecom Regulatory Authority of India. *Highlights of Telecom Subscription Data as on 31st March, 2023*., https://www.trai.gov.in/sites/default/files/PR_No.46of2023_0.pdf. Page 2. Accessed 3 Aug. 2023.

29 Garg, Ankita. "Budget 2023 Impact: Mobile Phones Expected to Get Cheaper in India". *India Today*, 1 Feb. 2023. https://www.indiatoday.in/technology/news/story/budget-2023-impact-mobile-phones-expected-to-get-cheaper-in-india-2329258-2023-02-01. Accessed 3 Aug. 2023.

30 Kundu, Rhik. "Liberalized Drone Rules, 2021 to usher in growth of drone ecosystem: Industry". *The Mint*, 27 Aug 2021, https://www.livemint.com/industry/manufacturing/liberalized-drone-rules-2021-to-usher-in-growth-of-drone-ecosystem-industry-11630070249070.html. Accessed 3 Aug. 2023.

31 "Why Digital Trust Is Key to Building Thriving Economies." *World Economic Forum*, 17 Aug. 2022, https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/. Accessed 3 Aug. 2023.

32 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 12

33 *Mobile Device Standards (Part 1)*, Bureau of Indian Standards at Paragraph 2.17, and Kaspersky Encyclopedia

34 *Mobile Device Standards (Part 2)*, Bureau of Indian Standards at Paragraph 5.1.4

35 "OPWNAI: Cybercriminals Starting To Use ChatGPT". CheckPoint, 6 Jan. 2023, https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/. Accessed 3 Aug 2023.

36 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 14

37 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 14

38 BL New Delhi Bureau. "Draft Digital India Act will regulate emerging technologies to protect citizens: Rajeev Chandrasekhar". *BusinessLine*, 12 Jun. 2023, https://www.thehindubusinessline.com/info-tech/draft-digital-india-act-will-regulate-emerging-technologies-to-protect-citizens-rajeev-chandrasekhar/article66960829.ece. Accessed 3 Aug. 2023.

39 Gartenberg, Chaim. "Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more". The Verge, 10 Mar 2021, https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals. Accessed 3 Aug. 2023.

40 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 14

41 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 14

42 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 14

43 Abdullahi, Khullani M. "Cybersecurity Threats In Virtual Reality (VR) And Augmented Reality (AR) — Challenges Organizations May Encounter & Tips On How To Overcome Them". *Medium*, 17 Apr. 2021, https://medium.com/immers-space/cybersecurity-threats-in-virtual-reality-vr-and-augmented-reality-ar-challenges-41435b6b5d88. Accessed 3 Aug. 2023.

44 Singh, Karnal. *Internal Security*, Unique Publishers, 2023 at Chapter 14

45 Kartit, Dina and Elizabeth Howcroft. "Interpol says metaverse opens up new world of cybercrime". *Reuters*, 28 Oct. 2022, https://www.reuters.com/technology/interpol-says-metaverse-opens-up-new-world-cybercrime-2022-10-27/. Accessed 3 Aug. 2023.

46 HTC America, Inc., No. C-4406, F.T.C. June 25, 2013, available at < https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf >

47 Fed. Trade Comm'n v. Equiliv Investments, No. 2:2015 cv 04379 D.N.J., June 24, 2015, available at < https://www.ftc.gov/system/files/documents/cases/1604vulcundo.pdf >

48 Turn, Inc., No. C-4612 (F.T.C. Apr. 6, 2017), https://www.ftc.gov/system/files/documents/cases/152_3099_c4612_turn_decision_and_order.pdf *See also:* United States. v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf

49 "Updating Your Smartphone Operating System". *Federal Trade Commission*, https://www.fcc.gov/consumers/guides/updating-your-smartphone-operating-system. Accessed 3 Aug. 2023.

50 "What is Mobile Security?". *CheckPoint*, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/. Accessed 3 Aug. 2023.

51 *Mobile Device Standards (Part 2)*, Bureau of Indian Standards at Table 3 Security Control (page 6)

52 "Payouts for Mobiles", *Zerodium*, 2023, https://zerodium.com/program.html. Accessed 3 Aug. 2023. *Zerodium is a leading exploit acquisition platform for advanced zero-day research and cybersecurity vulnerabilities. Their bounty programme for Android Mobile OS vulnerabilities is USD 250,000.*

53 "Zero-Day Vulnerabilities by Software 2011-13", *Zero-Day*. Accessed 3 Aug. 2023.

54 Kleidermacher, Dave. "Open vs closed source: which wins for security?", 8 Nov. 2022, https://davek.substack.com/p/open-vs-closed-source-which-wins. Accessed 3 Aug. 2023. The author explains that once researchers started assessing iOS code, many vulnerabilities, including zero-day vulnerabilities were discovered.

55 "Zero-Day Vulnerabilities by Software 2018-23", *Zero-Day*. Accessed 3 Aug. 2023.

56 Kleidermacher, Dave. "Open vs closed source: which wins for security?", 8 Nov. 2022, https://davek.substack.com/p/open-vs-closed-source-which-wins. Accessed 3 Aug. 2023.

57 "Improve Your Threat Protection Efficacy Using Built-In OS Security". *Forrester*, 2020. Accessed 3 Aug. 2023. *See Also: "*Mobile Security Scorecard". *Omdia*, 2022, https://omdia.tech.informa.com/OM014286/Omdia-mobile-security-scorecard-puts-the-focus-on-features-enterprises-value. Accessed 3 Aug. 2023.

58 Verma, Shubham. "Your Android Phone May Be the Next Target of Malware Associated with Russia". *India Today*, 5 Apr. 2022, https://www.indiatoday.in/technology/news/story/your-android-phone-may-be-next-target-of-new-malware-associated-with-russia-1933723-2022-04-05. Accessed 3 Aug. 2023.

59 Wuerthele, Mike. "Thieves abused Apple's enterprise app programs to steal $1.4 million in crypto". *Apple Insider*, 14 Oct. 2021,https://appleinsider.com/articles/21/10/14/thieves-abused-apples-enterprise-app-programs-to-steal-14-million-in-crypto. Accessed 3 Aug. 2023.

60 "Prevent and Remove Viruses and Other Malware". *Microsoft Support*. Accessed 3 Aug. 2023

61 Lele, Saurabh. "The trouble with Android 'forks': Experts fear security, privacy breaches". *Business Standard*, 22 Jan. 2023, https://www.business-standard.com/article/technology/the-trouble-with-android-forks-experts-fear-security-privacy-breaches-123012200610_1.html. Accessed 3 Aug. 2023.

62 Ziolkowski, Dawid. "API Data Breaches: How to Prevent". *Traceable AI*. Accessed 3 Aug. 2023.

63 Mitra, Ronnie. "How the Facebook API led to the Cambridge Analytica Fiasco". *API Academy*, 15 June. 2018, https://apiacademy.co/2018/06/how-the-facebook-api-led-to-the-cambridge-analytica-fiasco/. Accessed 3 Aug. 2023.

64 Romeo, Chris. "OWASP Top 10 API Breaches". *Tech Beacon*, https://techbeacon.com/security/owasp-api-security-top-10-get-your-dev-team-speed. Accessed 3 Aug. 2023.

65 Pell, Stephanie K and Bill Baer. "Protecting national security, cybersecurity and privacy while protecting competition". *Brookings*, 19 Jan. 2022, https://www.brookings.edu/articles/protecting-national-security-cybersecurity-and-privacy-while-ensuring-competition/. Accessed 3 Aug. 2023.

66 Keary, Tim. "Twitter data breach shows APIs are a goldmine for PII and social engineering". *Venture Beat*, 6 Jan. 2023, https://venturebeat.com/security/twitter-social-engineering/. Accessed 3 Aug. 2023.

67 Wong, Julia Carrie. "The Cambridge Analytica scandal changed the world – but it didn't change Facebook". *The Guardian*, 18 Mar. 2019, https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook. Accessed 3 Aug. 2023.

68 Wagner, Kurt. "Here's how Facebook allowed Cambridge Analytica to get data for 50 million users". *Vox*, 17 Mar 2018, https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data. Accessed 3 Aug. 2023.

69 Rosenberg, Matthew, Nicholas Confessore and Carole Cadwalladr. "How Trump Consultants Exploited the Facebook Data of Millions". *The New York Times*, 17 Mar. 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed 3 Aug. 2023.

70 Article 5, European Union General Data Protection Regulation, 2018.

71 "OWASP API Security Project". *OWASP*. https://owasp.org/www-project-api-security/. Accessed 3 Aug. 2023.

72 "Maharashtra: MCOCA invoked against accused in latest 'Loan App' case". *Indian Express*, 8 Oct. 2022, https://indianexpress.com/article/cities/pune/maharashtra-mcoca-invoked-against-accused-in-latest-loan-app-case-8196554/. Accessed 3 Aug. 2023.

73 Chertoff, Michael. "To protect consumers, Congress should secure the app store supply chain". *TechCrunch*, 15 Feb. 2022, https://techcrunch.com/2022/02/15/to-protect-consumers-congress-should-secure-the-app-store-supply-chain/. Accessed 3 Aug. 2023.

74 Rule 3(1)(b)(viii), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

75 The Information Technology Act, 2000 defines an intermediary as *"with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;]*. Accordingly, when an OS is facilitating a user's interaction with an app for sideloading, it is doing so on behalf of the app developers and is thus an intermediary.

76 Cimpanu, Catalin. "Details of 20 million Aptoide app store users leaked on hacking forum". *ZDNET*, 17 Apr. 2020, https://www.zdnet.com/article/details-of-20-million-aptoide-app-store-users-leaked-on-hacking-forum/. Accessed 3 Aug. 2023.

77 Kotzias, Platon, et al. "How Did That Get In My Phone? Unwanted App Distribution on Android Devices." *ARXIV*, Oct. 2020, https://arxiv.org/pdf/2010.10088.pdf. at page 2. Accessed 3 Aug. 2023.

78 Grant, Connor. "Fraud and abuse are still common in Google and Apple app stores". *The Hustle*, 13 Feb. 2019, https://thehustle.co/apple-google-apps-saudi-arabia/. Accessed 3 Aug. 2023.

79 "Sexually Explicit Material Used as Lures in Recent Cyber Attacks". *Trend Micro*, 18 Feb. 2015, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks?linkId=12425812. Accessed 3 Aug. 2023.

80 Paganini, Pierluigi. "Yanbian Gang steals millions from mobile banking customers of South Korea". *Security Affairs*, 18 Feb. 2015, https://securityaffairs.com/33709/cyber-crime/yanbian-gang-mobile-banking.html. Accessed 3 Aug. 2023.

81 Pell, Stephanie K and Bill Baer. "Protecting national security, cybersecurity and privacy while protecting competition". *Brookings*, 19 Jan. 2022, https://www.brookings.edu/articles/protecting-national-security-cybersecurity-and-privacy-while-ensuring-competition/. Accessed 3 Aug. 2023.

82 As evidenced in *Epic Games Inc v/s Apple Inc*, United States District Court, Northern District of California, Case No. 4:20-cv-05640-YGR. https://storage.courtlistener.com/recap/gov.uscourts.cand.364265/gov.uscourts.cand.364265.812.0_3.pdf.

83 *Epic Games Inc v/s Apple Inc*, United States District Court, Northern District of California, Case No. 4:20-cv-05640-YGR. https://storage.courtlistener.com/recap/gov.uscourts.cand.364265/gov.uscourts.cand.364265.812.0_3.pdf.

84 "Mobile AppSec Verification Standard". *Open Web Application Security Project*, https://owasp.org/www-pdf-archive/OWASP_Mobile_AppSec_Verification_Standard_v0.9.2.pdf. Accessed 3 Aug. 2023

85 “Code of Practice for app store operators and app developers”. *Information Commissioner’s Office*, Dec 9. 2022, https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers. Accessed 3 Aug. 2023.

86 “Appstore Security: 5 Lines of Defence Against Malware”. *European Union Agency for Cybersecurity*, 12 Sept. 2011, https://www.enisa.europa.eu/publications/appstore-security-5-lines-of-defence-against-malware. Accessed 3 Aug. 2023.

87 Sinha, Parakh. “India's cybersecurity watchdog tells users update Google Chrome and Microsoft Edge immediately”. *CNBC TV 18*, 23 May. 2023, https://www.cnbctv18.com/technology/cert-in-google-chrome-microsoft-edge-vulnerabilities-update-now-16737351.htm. Accessed 3 Aug. 2023.

88 Mobile Device Standards (Part 1), *Bureau of Indian Standards* at Paragraph 2.17, and Kaspersky Encyclopedia

89 Mobile Device Standards (Part 2), *Bureau of Indian Standards* at Paragraph 5.1.4

90 “OPWNAI: Cybercriminals Starting To Use ChatGPT”. CheckPoint, 6 Jan. 2023, https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/. Accessed 3 Aug 2023.

www.esyacentre.org