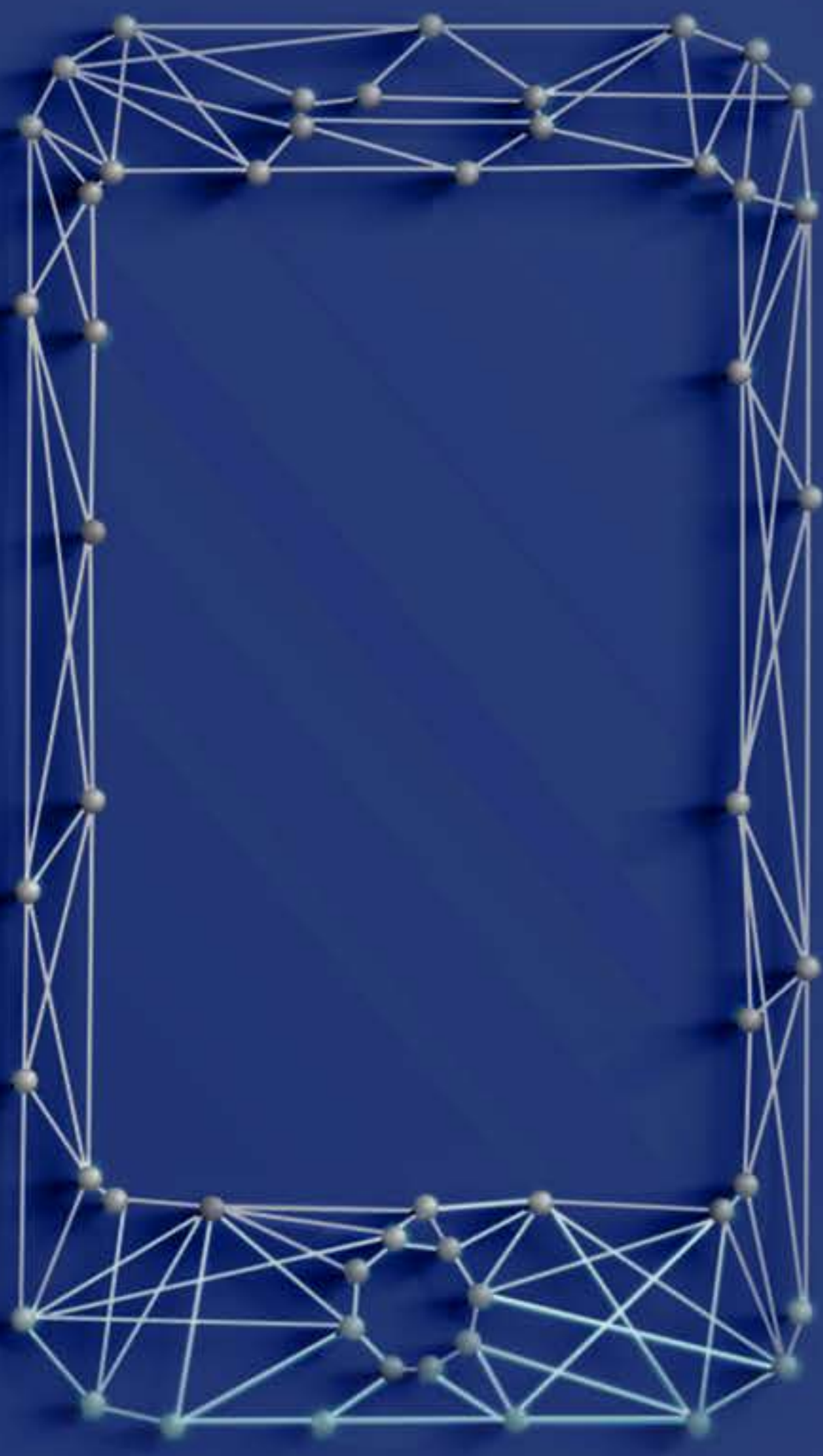
TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE



MOBILE APPLICATIONS

Intensifying Risks to Data Security & Privacy

Mobile applications are now surfacing as a new feeble link when it comes to user's information security and privacy. Threat actors are utilizing advanced techniques to evade detection while deploying malicious applications on official app stores. This constantly rising complexity of associated cyber threats, accompanied by growing data breach incidents is keeping CISOs up at night. We have also seen nations prohibiting several mobile applications for infringing data security and privacy regulations.

Impact of COVID-19

The risk of privacy breach has increased manifolds with the growing popularity of mobile applications in the current pandemic when people are asked to self-isolate and work remotely. Mobile devices have become a core tool to play down stress, manage daily tasks, access business-critical data, etc. Video conferencing and collaboration applications like Zoom, Skype, Microsoft Teams, Google Meet, etc. observed a massive surge in usage across the web and mobile platforms.

As per App Annie, a trusted mobile data and analytics platform, users spent around 1.6 trillion hours on mobile devices in the first half of 2020 with a 220% increase in time spent on business applications.

Besides popularity, the COVID-19 outbreak has contributed phenomenally in letting threat actors capitalize the global disruptions through new cyber threat campaigns. They are distributing fake mobile applications embedded with trojans or virus, which upon execution steal host device's information that may include (but not limited to) contact information, financial details, username and passwords, device details, etc.

Third-party App Stores

Google Play and App store are the two leading distribution channels for mobile applications. This fact is not concealed from cybercriminals. Hence, they have started focusing on third-party stores that lie outside the boundaries of official app stores. According to the Symantec's report, third-party app stores host 99% of discovered mobile malware. There are more than 300 third-party app stores across the globe, and the number is still growing.

Users who download mobile apps from such stores face increased security risks as third-party stores do not have stringent application review processes in place like official app stores. According to the 2020 Mobile Threat Report by Wandera, 5.8% and 1.1% of iOS and Android devices, respectively, have at least one sideloaded apps installed.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Increased Mobile Apps Usage – A Sign of Digital Transformation or Cyber Risk

Certainly, mobile apps have supported organizations to speed up their digital transformation and deliver a great experience to employees and customers. However, on the contrary, cybersecurity is still a major concern when it comes to mobile applications. We often see mobile applications asking for more than sufficient permissions, which are not required for them to function. These permissions pose a huge risk to users' privacy as they allow an application to access users' sensitive information.

Let's go through both dimensions of mobile applications usage i.e. the digital transformation and cybersecurity risk.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Some recent findings highlighting the risks related to mobile applications:

- High-risk vulnerabilities were found in 38% of iOS applications and 43% of Android applications.
  (Source: Positive Technologies)

- The percentage of fraudulent transactions originating from a mobile application increased from 13% in Q4 2019 to 26% in Q1 2020.
  (Source: RSA Fraud Report Q1 2020)

- Rogue mobile apps were accounted for 15% of fraud attacks in Q1 2020.
  (Source: RSA Fraud Report Q1 2020)

- The average value of a fraudulent payment transaction in the mobile channel has increased by 60% (from USD 480 to 767) in Q1 2020.
  (Source: RSA Fraud Report Q1 2020)

Need For Stringent Obligations

As the world is constantly updating its digital footprints, the need for data protection has become more crucial than ever. For developing countries, the growing volume of personal data and adoption of smartphones is continually increasing the demand for a strict and firm data protection obligations that can regulate the use of data collected by mobile applications and give users a sense of security.

As a user, we need to be more vigilant while installing applications and granting permissions keeping in mind the task for which the app is downloaded. We can follow the practice of reading terms and conditions before logging onto any mobile applications to reduce the chances of getting compromised.

Get in touch with us to know more about the potential cyber threats and explore a wide portfolio of security solutions intended to minimize the risk.

Write to us: contactcs@tataadvancedsystems.com