



SECURE CHANNEL

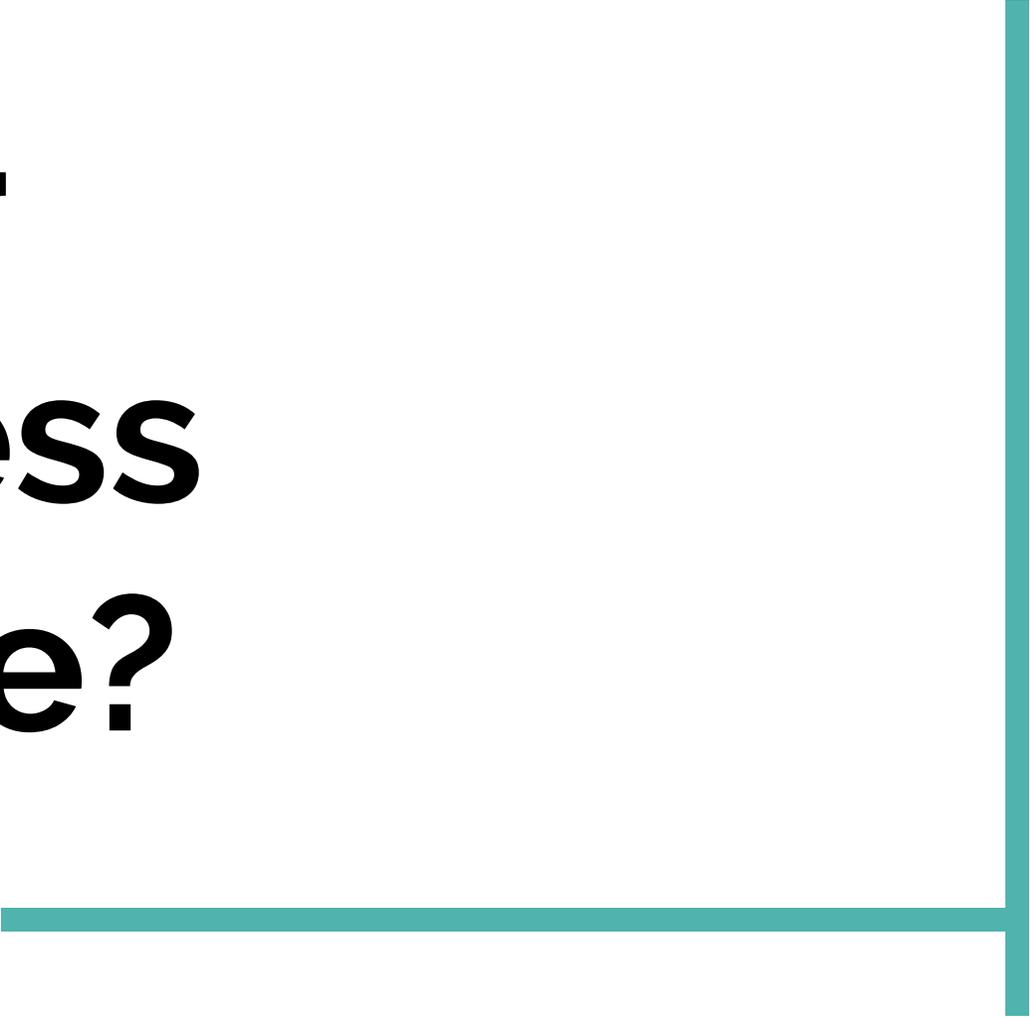
THE ONLY INTEGRATED TOTAL SECURITY SOLUTION
Looking Beyond Future...

Cybernet Security Solutions LLP

Rogue Mobile App Threat – An Uncontrollable Lethal Threat

www.cybernetsecurityinc.com

**Can
your
business
survive?**

A teal-colored L-shaped graphic element consisting of a vertical line on the right side and a horizontal line at the bottom, meeting at a right angle in the bottom right corner of the slide.

By 2022, API abuses will be **the most frequent attack vector** resulting in data breaches for enterprise applications – ***The Gartner Group***

“If it starts happening then we have to **close down** the banking system” - **RBI**

WhatsApp CEO has given up on cloned apps

CERT-IN warning of **banking virus** stealing credentials using **fake Android apps**

Google Pay reached out to 3 crore users in India, in just a month when launched, offering just Rs. 100/- for a download and Rs. 100/- for each referral.

Guess, how many of your users may download, if Rs. 1000/download and Rs. 1000/referral are offered?

What if Rs. 10,000 for a new registration is offered?

Guess, how many rogue apps can float around targeting your organization, say in six months, if one can be created in days?

This offer will also make web users and inactive users shift to mobile app.

Many new users will register.

The Base Vulnerability

→ The base vulnerability is **API Exploitation**.

→ Rogue app is just an user interface exploiting APIs. **Nothing** do with the original app.

→ Look alike feel is given just to **deceive** users.

→ A rogue app **need not** have any app-level security of the original app.

→ Any server side security based on an app-provided data can be **easily broken** by sending the right data through APIs.

→ Once broken, **ALL** users become victim.

✓ User-id, password, can be phished.

✓ OTP can be obtained from SMS

✓ Other 2FAs, including biometric can be phished

✓ Other data like Credit Card#, Acct #. etc. can be phished

Your Strong Security – Hacker's Child's Play



Certificate Pinning

Get cert. from the original app



Encryption

Get key from the original app



Anti-Tampering

Get hash from the original app



OTP/2FA

Get OTP from SMS. 2FA can be locally stored.



App Monitoring

Mark the app private



Playstore Checks

Upload on an external site



Biometric

Biometric value stolen from app



Confirmation SMS

App can delete SMS



Location Tracking

Steal geo location using app



App Hardening / RASP

Decrypted code available



Mobile SDK

Simply ignore



Obfuscation

Public objects are not Obfuscated



All app initiated security checks can always be broken

Do you know how to bypass all security checks in one shot ?

Just use the organization website in built-in app browser (WebView)

Here programmatically code can be modified, data can be substituted, pages can be navigated, etc.



Not supported in web app

- SSL/Certificate Pinning
- Encryption
- Anti-tampering
- Device Authentication
- Mobile SDK
- App Hardening/RASP
- Location Tracking
- Obfuscation
- Emulator detection
- Rooting detection
- Debug detection
- Digital Signatures



Simply bypassed

- Captcha
- O-Auth
- Source Identifier



Thank You

Email - sales@cybernetsecurityinc.com

Web - www.cybernetsecurityinc.com

SECURECHANNEL