

EQUIPO 8

# MOBILE DEVICE SECURITY



# 10 PRINCIPALES RIESGOS EN DISPOSITIVOS MOBILES DE ACUERDO A OWASP.

1. USO INDEBIDO DE LA PLATAFORMA
2. ALMACENAMIENTO INSEGURÓ DE DATOS
3. COMUNICACIÓN INSEGURA
4. AUTENTICACIÓN INSEGURA
5. CIFRADO INSUFICIENTE
6. AUTORIZACIÓN INSEGURA
7. CALIDAD DEL CÓDIGO DEL CLIENTE
8. MANIPULACIÓN DE CÓDIGO
9. INGENIERÍA INVERSA
10. FUNCIONALIDAD INNECESARIA

# TIPOS DE ATAQUES EN EL DISPOSITIVO

# BASADOS EN EL NAVEGADOR

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching





## BASADOS EN EL TELEFONO Y SMS

- Baseband Attacks
- SMiShing

# BASADOS EN APLICACIONES

- Sensitive Data Storage
- No Encryption/Weak Encryption
- Improper SSL Validation
- Configuration Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges



# TIPOS DE ATAQUES



## BASADOS EN SISTEMA

- 1. No Passcode / Weak Passcode:** No establecer contraseñas fuertes o códigos de acceso hace vulnerable al dispositivo.
- 2. iOS Jailbreaking:** Significa conseguir acceso root a un teléfono y eliminar las restricciones de software.

# TIPOS DE ATAQUES

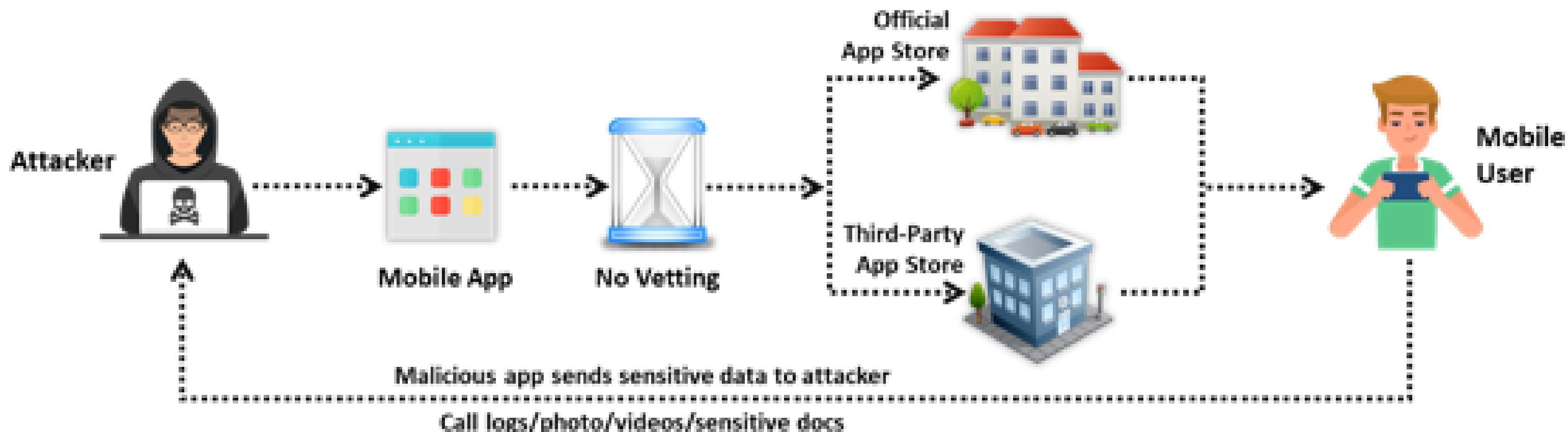


## BASADOS EN SISTEMA

**3. Android Rooting:** Es el proceso mediante el cual un usuario obtiene acceso privilegiado o "root" en un dispositivo Android.

**4. OS Data Caching:** El caché del sistema almacena datos temporales en el disco. Un atacante puede extraerlos con un sistema malicioso.

# PROBLEMAS DE SEGURIDAD POR EL SURGIMIENTO DE TIENDAS DE APLICACIONES



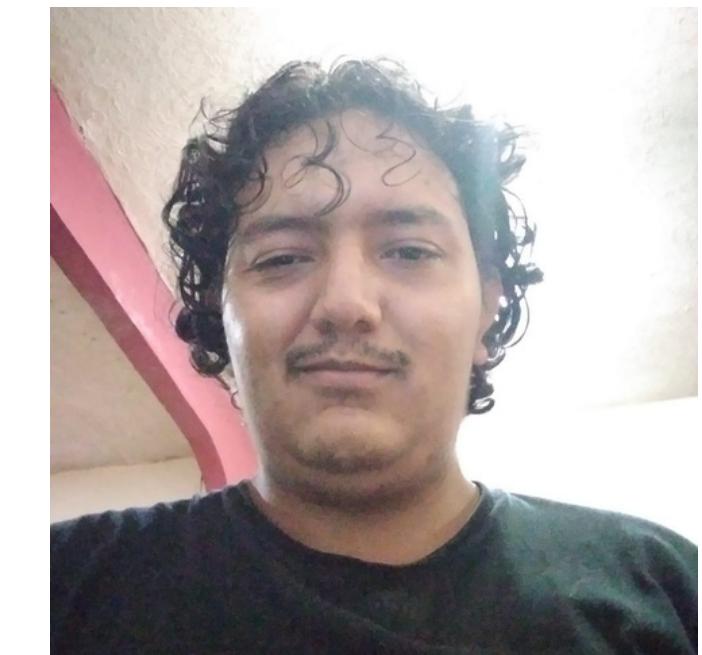
# EQUIPO 8



MARTINEZ SALGADO  
CARLOS EDUARDO



TUN DZUL ADOLFO



VAZQUEZ POMPA  
NOE

# GRACIAS