Covert Channel in Smart Phones

Wade C. Gasior, Li Yang

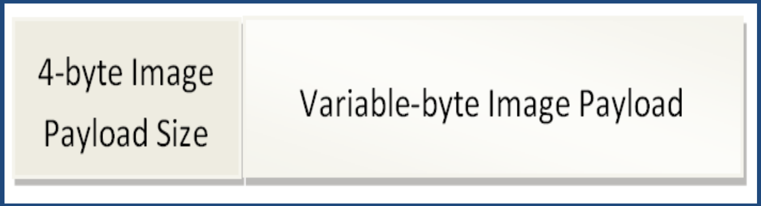
University of Tennessee at Chattanooga

THE UNIVERSITY of TENNESSEE UT
CHATTANOOGA

Implementing CC's on Android

Timing Covert Channel Design

- Timing-based
  - Need: large amount of legitimate traffic
  - Implemented IP camera application
  - Message encoded in delays between video frames (binary)



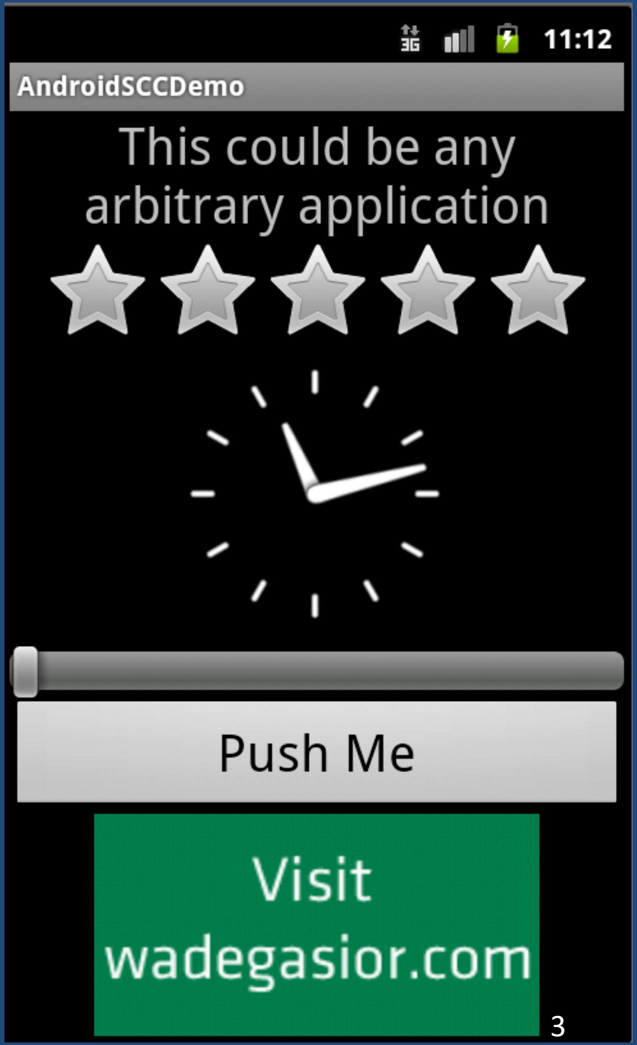
4-byte Image Payload Size	Variable-byte Image Payload

  - Server displays streamed video
  - Server decodes and displays messages

Implementing CC's on Android

Storage Covert Channel Design

- Storage-based
  - Small advertisement banner shown at bottom of app
  - App requests new banners "randomly" (http)
    - Specific ads represent specific input symbols
    - Encode messages in hex
  - Server decodes and records messages



11:12

AndroidSCCDemo

This could be any arbitrary application

Implementing CC's on Android

Challenges

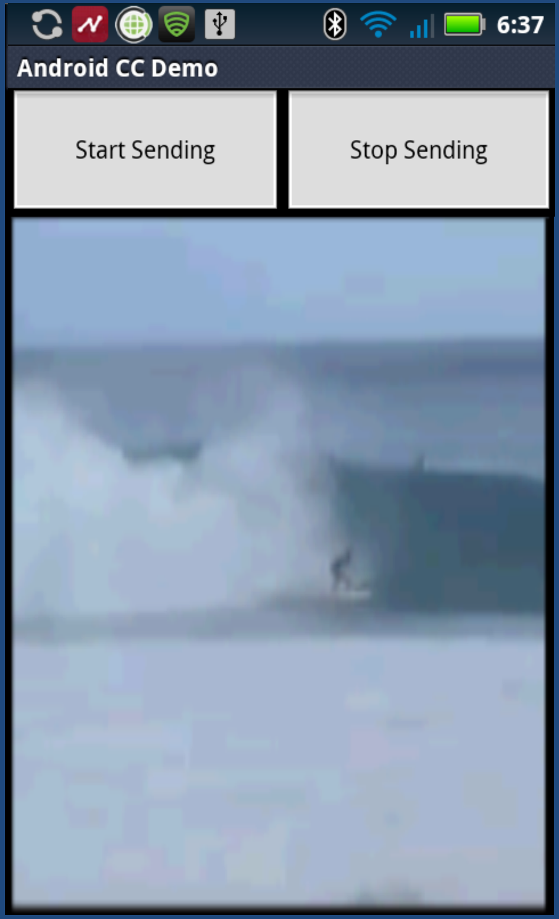
- Access to sensitive data
  - Fine-grained application permissions (suspicious if many)
  - Sandboxed runtime environment (no inter-application communication)
- No low-level packet access
  - Dalvik VM (Java)
- Cellular network
  - High jitter, high latency
  - UDP packets often dropped

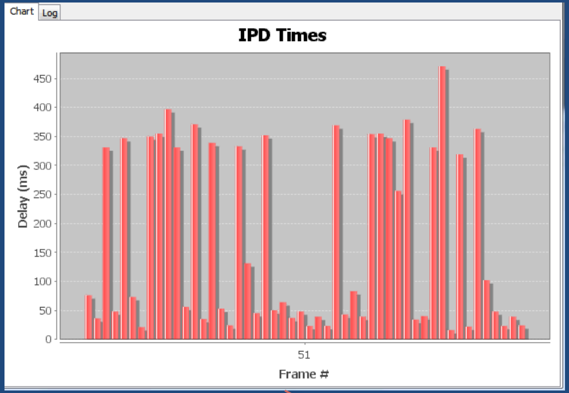
Implementing CC's on Android

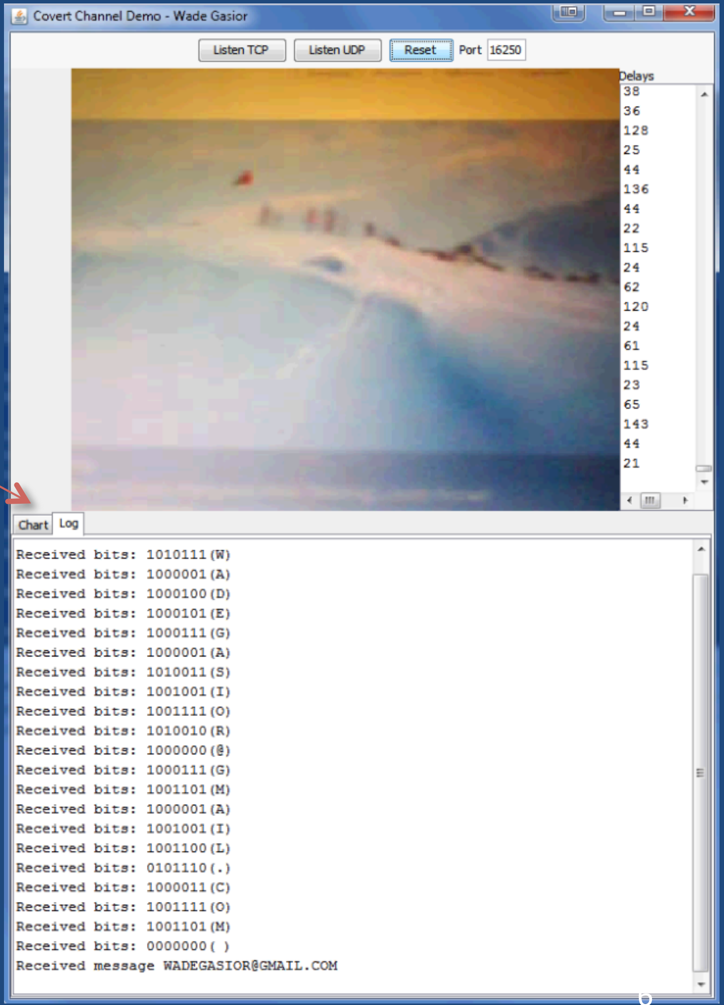
Solutions

- Access to sensitive data
  - On-device covert storage channels (Schlegel)
- No low-level packet access
  - Use timings between *events* (TCP/UDP messages) rather than packets (custom protocols)
  - Disable Nagle's algorithm
- Cellular network
  - Use larger delays
  - Use TCP only

Demo Video







```
38
36
128
25
44
136
44
22
115
24
62
120
24
61
115
23
65
143
44
21
```

```
Received bits: 1010111(W)
Received bits: 1000001(A)
Received bits: 1000100(D)
Received bits: 1000101(E)
Received bits: 1000111(G)
Received bits: 1000001(A)
Received bits: 1010011(S)
Received bits: 1001001(I)
Received bits: 1001111(O)
Received bits: 1010010(R)
Received bits: 1000000(@)
Received bits: 1000111(G)
Received bits: 1001101(M)
Received bits: 1000001(A)
Received bits: 1001001(I)
Received bits: 1001100(L)
Received bits: 0101110(.)
Received bits: 1000011(C)
Received bits: 1001111(O)
Received bits: 1001101(M)
Received bits: 0000000( )
Received message WADEGASIOR@GMAIL.COM
```