DroidHook: Detecting Data EXfiltration

Aisha Ali-Gombe
Irfan Ahmed
Golden Richard III

(University of New Orleans)
Data EXfiltration

- Unauthorized transfer of data.
- Permissions are complicated.
- Most Android malware go after user sensitive data.
- Performance overhead using traditional tainting.
• 93% use either Service or Broadcast Receiver or both for Data Exfiltration
How Bad is “Bad”?  

- SMS  
- Contacts  
- Wifi Services  
- Browser History  
- Call Logs  
- Account Info  
- Phone State  

SMS Hijacking  

Data Theft  

Affects not only user  

BUT  

also friends family and other contacts
Exit Channels

- Telephony Network: SMS & MMS
- IP Network
- Hardware
DroidHook

• IP Network
  • Hook “Read API Calls”
  • Store process information and return value
  • Check payload and against known value
  • Using similarity hashing
DroidHook Architecture
Cont.

• SMS and MMS:
  • `sendsmsmmessage()` **must** be triggered by user event for third party apps
  • Can only be called from App’s main UI thread
  • User preview
Conclusion

- **DroidHook:**
  - Low performance overhead
  - Protect user sensitive data
  - Can detect modified data