NETWORK INFORMATION HIDING

CH. 2: INTRODUCTION TO LOCAL COVERT CHANNELS

Prof. Dr. Steffen Wendzel

https://www.wendzel.de

Sample Covert Channel

- Two basic types: **storage** and **timing**.
- Consider two processes, P_1 and P_2, running within the same environment. Several possible covert channels between these processes are imaginable:

1. P_1 performs intensive computations to influence the system load (measured by P_2).
2. P_1 stops its operation at a given time t_1 or t_2 to signal a `0' or `1' bit (while P_2 monitors the process table).
3. P_1 either creates or does not create an entry in the file system known by P_2 (existence of the file signals the hidden information)

- These simple examples reveal that covert channels are usually not noise-free, need a protocol (when does a transmission start/end?) and need to detect errors in transmissions (e.g. using parity bits).
  - I will discuss such aspects in later chapters.

Sample Docker Covert Channel [1]

Docker and other container technology has been proven not to be resistant against covert channels.

- Several covert channels possible, e.g. Luo et al. [1] mention one that uses the globally used memory (GUM):

$$Bit = \begin{cases} 1, & if\ GUM\ mod\ 100\ - GUM\ mod\ 50 = 50 \\ 0, & if\ GUM\ mod\ 100\ - GUM\ mod\ 50 = 0 \end{cases}$$

- Other channels exist, too, such as Inode exhaustion [1].

[1] Luo, Y., Luo, W., Sun, X., Shen, Q., Ruan, A., Wu, Z.: Whispers Between the Containers: High-capacity Covert Channel Attacks in Docker, in Proc. TrustCom-BigDataSE-ISPA, pp. 630-637, IEEE, 2016.

Covert Channels in Android

- Plethora of research was conducted in recent years on covert channels in mobile phone environments.
- The goal is usually to establish a policy-breaking communication between two sandboxed apps.
- In Android, apps have permissions, e.g. the permission to access the contacts.

Covert Channels in Android

Many covert channels possible, here are just four we published in 2013 [1]:

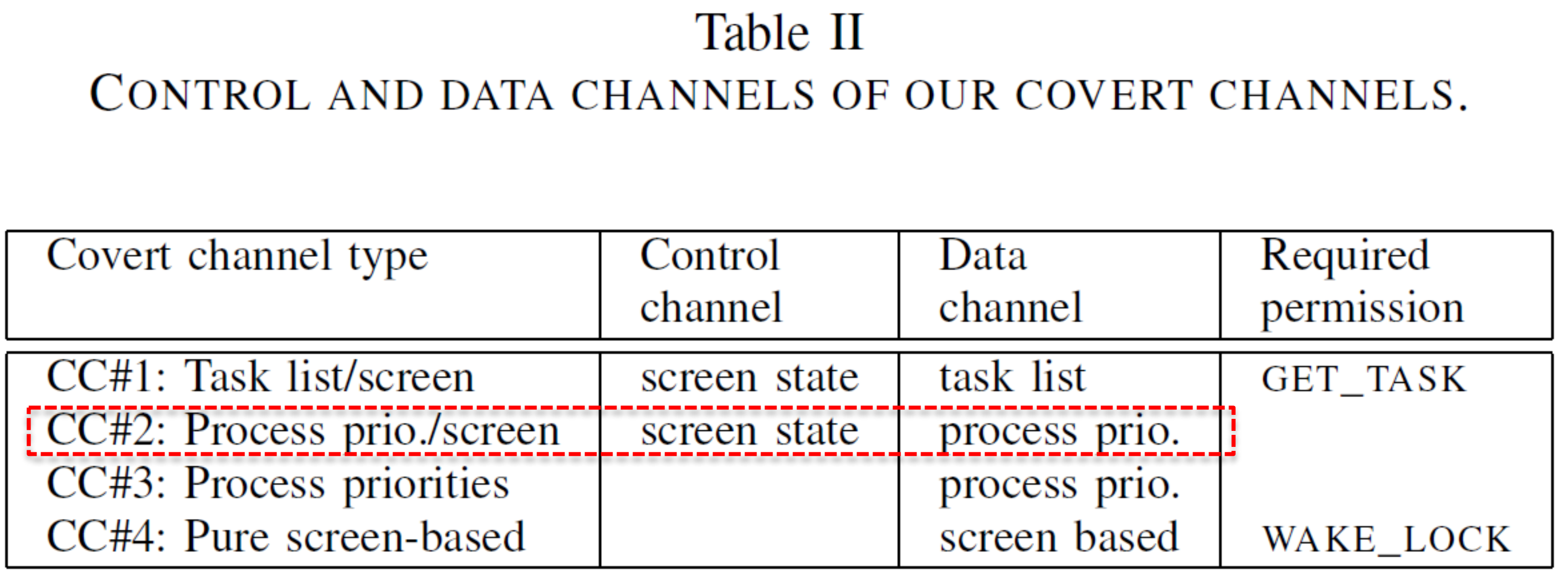


Table II
CONTROL AND DATA CHANNELS OF OUR COVERT CHANNELS.

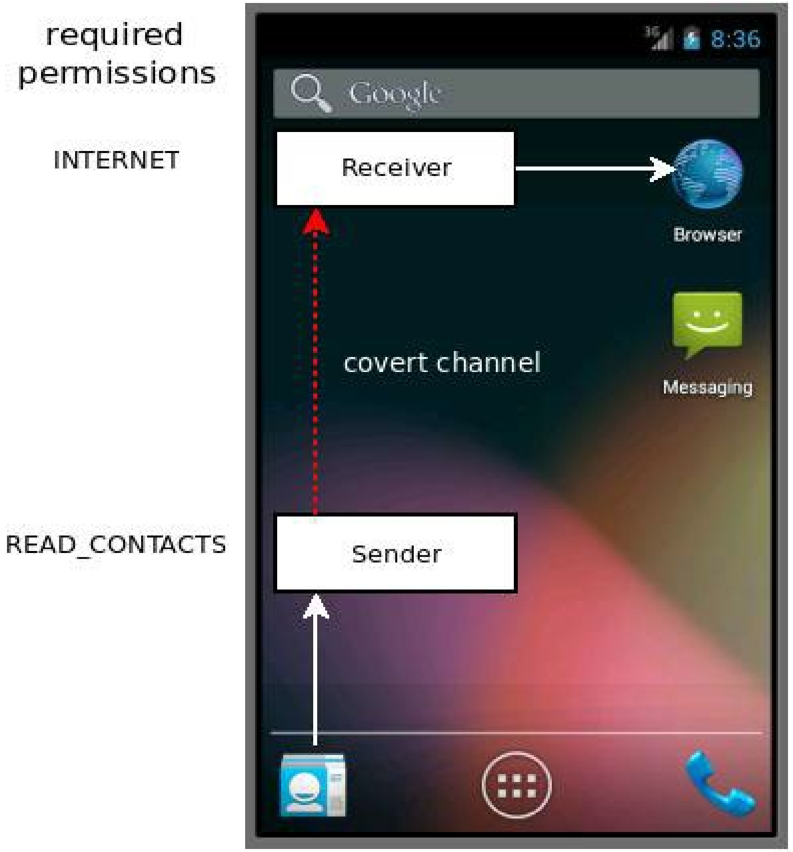
Covert channel type	Control channel	Data channel	Required permission
CC#1: Task list/screen	screen state	task list	GET_TASK
CC#2: Process prio./screen	screen state	process prio.	
CC#3: Process priorities		process prio.	
CC#4: Pure screen-based		screen based	WAKE_LOCK

[1] J.-F. Lalande, S. Wendzel: Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels, in Proc. ARES 2013, pp. 701-710, Regensburg, 2013.

Covert Channels in Android

- Example scenario using two apps (e.g. two smart home apps, one for monitoring energy consumption; one app is an energy advisor).

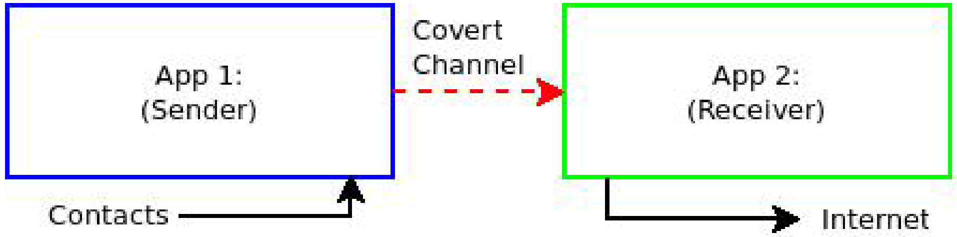
- Requirements for covert transmission:
  - Sender and receiver must run simultaneously
  - Transmission via process priority of ‚Sender'
  - Transfer process starts when user turns off the screen

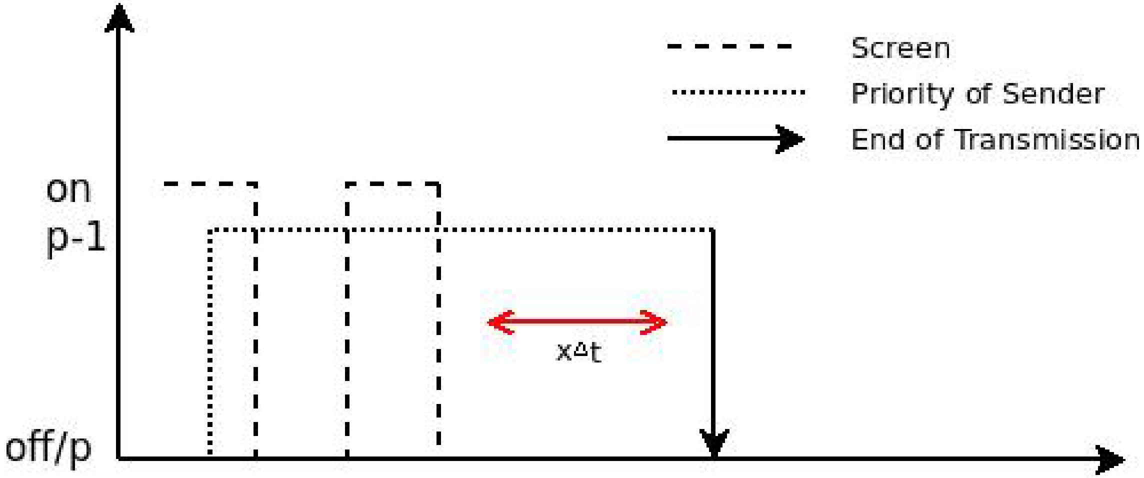


J.-F. Lalande, S. Wendzel: Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels, in Proc. ARES 2013, pp. 701-710, Regensburg, 2013.

Covert Channels in Android

How bits are transmitted:





J.-F. Lalande, S. Wendzel: Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels, in Proc. ARES 2013, pp. 701-710, Regensburg, 2013.

Covert Channels in Android (this slide is not relevant for the exam)

Video:

http://www.dailymotion.com/video/x10lcyq_ectcm-2013-hiding-privacy-leaks-in-android-applications_tech

Original slides:

http://www.wendzel.de/dr.org/files/Papers/ares13_slides.pdf