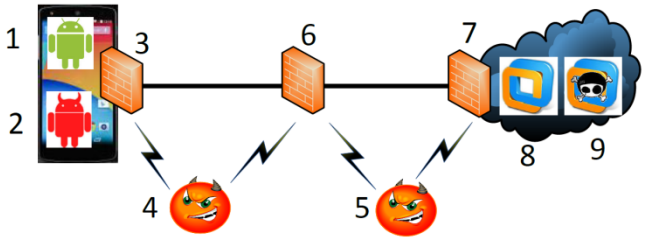
Modern TCP Security Vulnerabilities and Defenses

Challenge:

- TCP is a complex protocol that is still evolving to this date
  - For example, new RFCs are being introduced, new features are being added
- Multiple threat models and participating parties are involved. Difficult to reason about the security properties of TCP
- Many types of side channels exist in TCP and it is unclear how they are introduced and in what ways they can be exploited

Scientific Impact:

- Systematically understand the weaknesses in both TCP design and implementation
- Demonstrates that new and subtle TCP vulnerabilities (such as side channels) exist and can be serious
- Develop methodology to systematically discover important classes of vulnerabilities such as side channels
- Gain an understanding of what security guarantees are desired of TCP and how they can be achieved



Solution:

- We will focus on shared resources between the victim and legitimate connections to identify possible side channels
- We will apply model checking as a rigorous approach to systematically identify side channels and be able to construct examples of exploitations
- We will reason about the desired security properties and propose defenses
- So far, we have discover one serious instance of side channel vulnerability, CVE-2016-5696, in the Linux TCP stack

Broader Impact:

- Our work exposes subtle and serious TCP security flaws that are difficult to discover
- CVE-2016-5696 allows an off-path attacker to
  - Infer if any two arbitrary hosts on the Internet are communicating or not
  - Infer The sequence number used in both sides
  - Reset the connection and inject malicious payload
- The vulnerability is patched in Linux kernel and it raises the awareness of this class of side channel vulnerabilities that has been largely overlooked today

Zhiyun Qian, Award Number: 1464410, Institution: University of California, Riverside, Contact: zhiyunq@cs.ucr.edu