© Weiss

“Smartphone Honeypots”

SPRING 2011

Collin Mulliner, 21-22 March 2011
collin@sec.t-labs.tu-berlin.de

Agenda

- Introduction
- Honeypots
- Smartphone Challenges
- Flavors
- Project Idea
- Conclusions

Smartphone (in)Security

- Smartphone technology moves fast
  - New software features every few month (about every 6 month with Android)

- New attacks all the time
  - Trojans
  - botnets
  - 0-day bugs

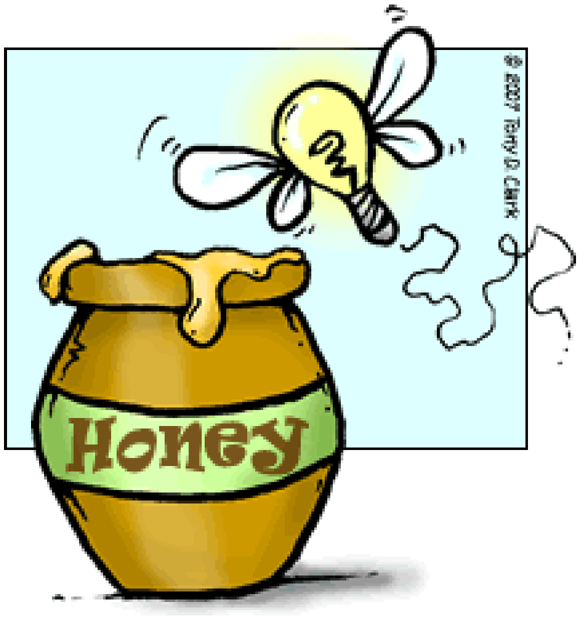
- **→ Build a Smartphone Honeypot to catch new attacks**

Honeypot

- **A computer system that is meant to be attacked**
  - Are there attacks at all
  - Distract attackers from real systems
    - Use of honeynets
  - Study the attacker's behavior
    - Kind of attack used to break into the honeypot
    - Activity after break in
- Honeypot vs Honeynet
  - Single computer
  - Whole network of fake machines (honeynet)

Project Goal : Build a Smartphone Honeypot

- What are the challenges?



Smartphone Honeypot : Challenges

- System Design/Setup
- Monitoring
- Containment
- Visibility

Smartphone Honeypot: System Setup

- **How to design a smartphone honeypot**

- What platform / OS?
  - Can we emulate OSes? (see *Provos honeyd*)

- Real hardware vs. Emulator?

  - Do we want to support/catch telephony based attacks?
    - SMS, MMS, ...

vs

Smartphone Honeypot: Monitoring

- **Monitoring is one of the main components of a honeypot**

- Need to record all interaction with the honeypot
  - IP traffic
  - GSM / 3G traffic
  - Changes to the file system
  - Syscalls

- This highly depends on the system setup, of course
  - Probably easy with emulator and hard with hardware

Smartphone Honeypot: Containment

- **Hijacked honeypot must not be used for further attacks!**
- Highly depends on system setup
  - Emulator → easy
    - Use host OS to build protection framework
  - Real Hardware → hard
    - ???

Smartphone Honeypot: Visibility

- **Honeypot needs to be attacked otherwise it is useless!**
- Get phone/emulator a public IP of an mobile network operator
  - Wait for IP-scan by attacker and/or worm
- Install apps from AppStore/Market
  - Automate use of apps (probably a lot of work)
  - Use unofficial AppStores
- Spread mobile phone number
  - SMS, MMS attacks
- This will be very interesting!

Honeypots Flavors

- Low-interaction: just sit and wait to be attacked
  - e.g. just simulate/emulate network services
- High-interaction: do something in order to get attacked
  - e.g. a real system
  - Could also proactive “use” apps. such as a web browser
- Smartphones have few network services → High-interaction
- Investigate if “Shadow Honeypots” are useful for smartphones

Project Idea

- Build Smartphone Honeypot
- Platform: Android
  - Openness and Market share
- Honeypot flavor: high-interaction
  - Install apps from Market
- Monitoring and Containment
  - TODO still under investigation
- Visibility
  - TODO still under investigation (1 part = install apps)

Conclusions

- Smartphones are an interesting target for attacks
- Desktop/Server honeypots have shown to be effective
- Smartphone Honeypots look promising
  - Many challenges
  - ➔ Interesting topic
  - ➔ Work In Progress

Questions?

Thank you!