Interactive Attack on Smartphone Voice System Through Power Line

Qiben Yan

Computer Science & Engineering, Michigan State University

• Introduction

❑ Existing attacks aim at injecting the attack signals over the air, but they have several limitations:

Unauthenticated!
?
Your home address is…

❑ Vulnerable to noise

❑ Require prior knowledge of user’s voice

❑ No interaction

❑ In this work, we introduce GhostTalk, to explore the power line side-channel to launch the inaudible voice command attack. By modifying the power bank charging cable and manipulating the electric signals in the modified cable, GhostTalk successfully closes the gap between injection and eavesdropping, and performs well in noisy environments without authenticated user’s voice.

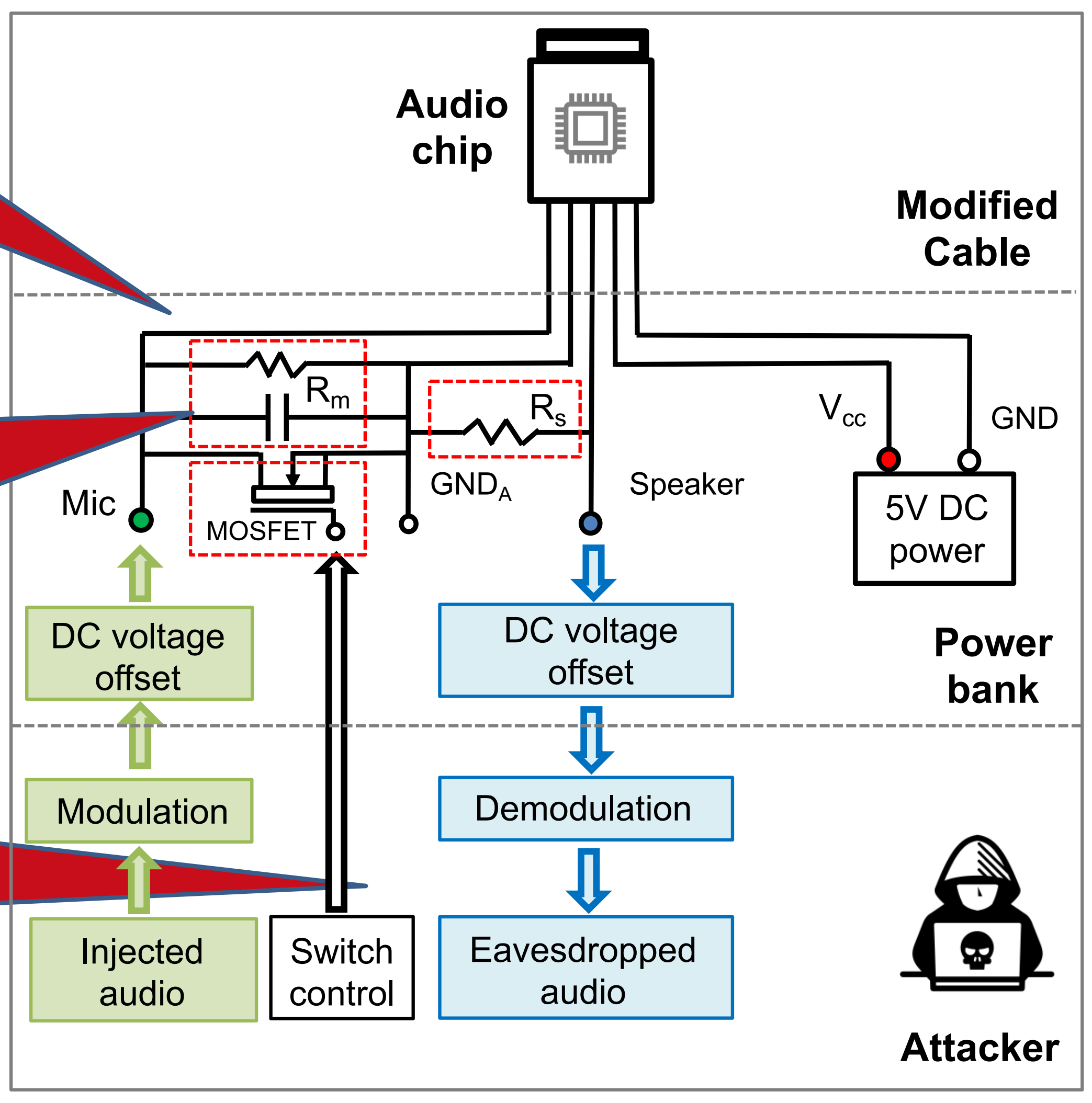
❑ Furthermore, to extend the attack scenarios, we present GhostTalk-SC (Standard Cable), to eavesdrop sensitive information from the smartphones charged by standard cables.

• GhostTalk Design

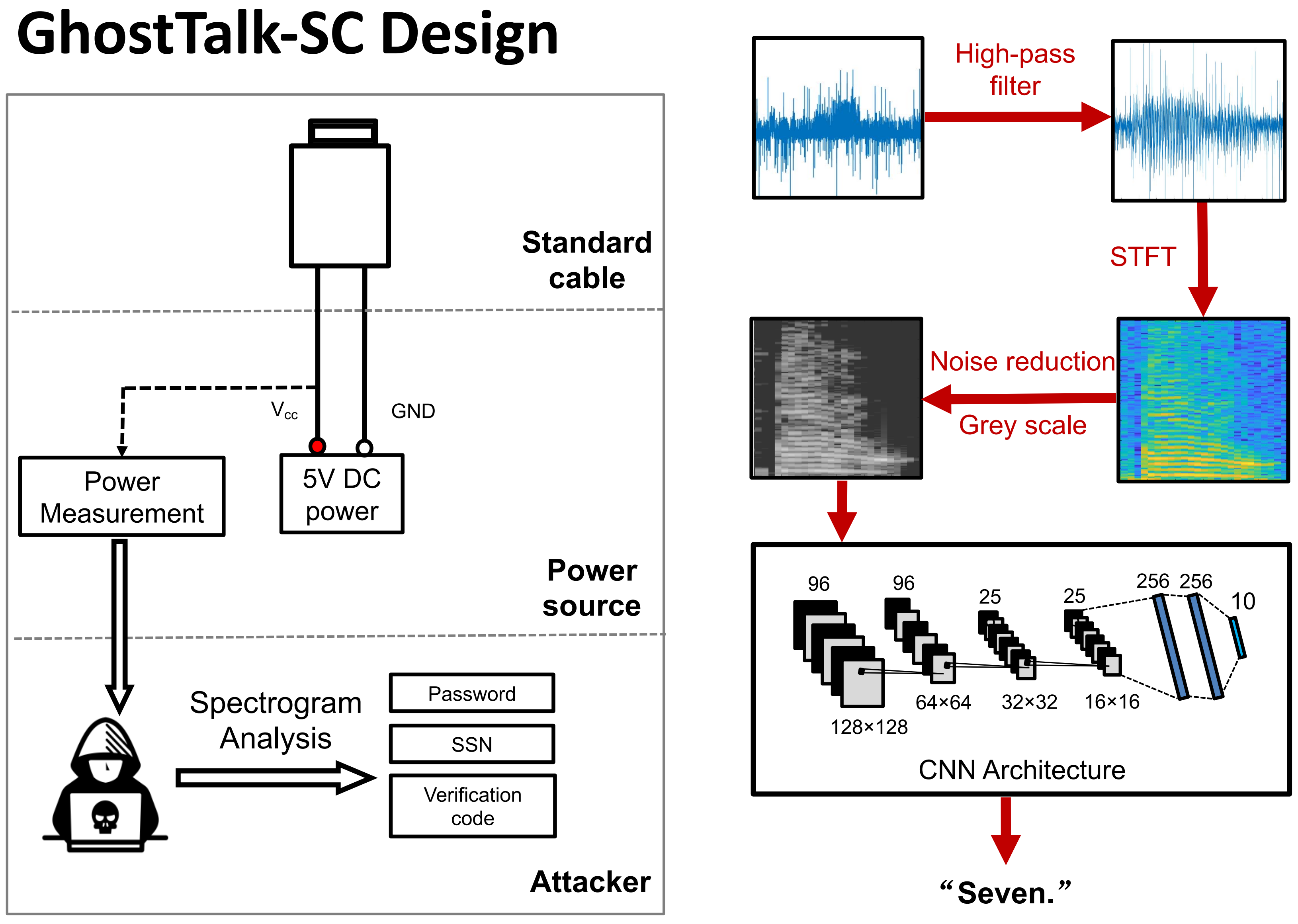
Noise Robustness: GhostTalk injects voice command through electric signals, so that environmental noise has no impact on the injection.

Interactivity: GhostTalk uses resistances to emulate a fake “headphone” and make the smartphone play audio through it. And it can hack the output audio signals by measuring the voltage on the speaker cable.

Bypass speaker recognition: GhostTalk adds a MOSFET between the microphone and ground, to emulate a fake “press button” on the headphone and activate the voice assistant.



• GhostTalk-SC Design



• Contributions

❑ GhostTalk is the first **interactive** and **inaudible** voice command attack towards smartphone voice assistants over the **charging cables**.

❑ We also propose GhostTalk-SC, an eavesdropping attack capturing audio signals from **power consumption side-channel**.

❑ We test GhostTalk and GhostTalk-SC attacks on **9 different models** of smartphones. And the evaluation results show that both attacks achieve high attack success rate and **resilient to environmental noise**.

• Countermeasures

For GhostTalk:

❑ **Disable voice assistant activation function by pressing headphone button.**

❑ **Enable headphone notification**

For GhostTalk-SC:

❑ **Stop charging your smartphone after reaching high battery level.**

• Audio attack directions

Injection attacks

❑ Replay attack

❑ Ultrasound

❑ Guided wave

❑ Light signal

❑ Charging port

Eavesdropping attacks

❑ Hidden microphone

❑ Motion sensor

❑ Wireless RF

❑ Lidar

❑ Power line

What’s the next?

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting)
June 1-2, 2022 I Arlington, Virginia