Practical Security Evaluation of an Audio-based Ad Hoc Device Pairing Scheme

David Rieger
Karlsruhe Institute of Technology, Germany
Stephan Sigg and Yusheng Ji
National Institute of Informatics, {sigg, kei}@nii.ac.jp

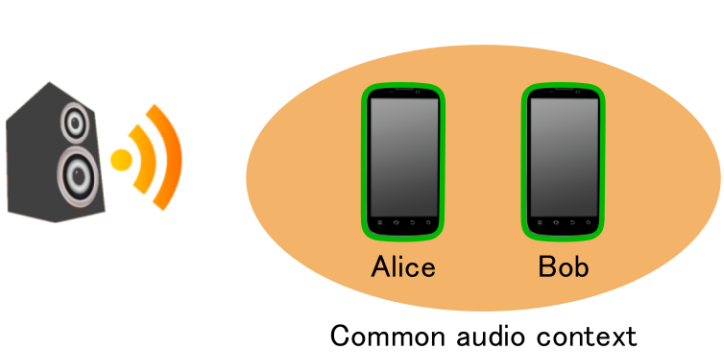
Background

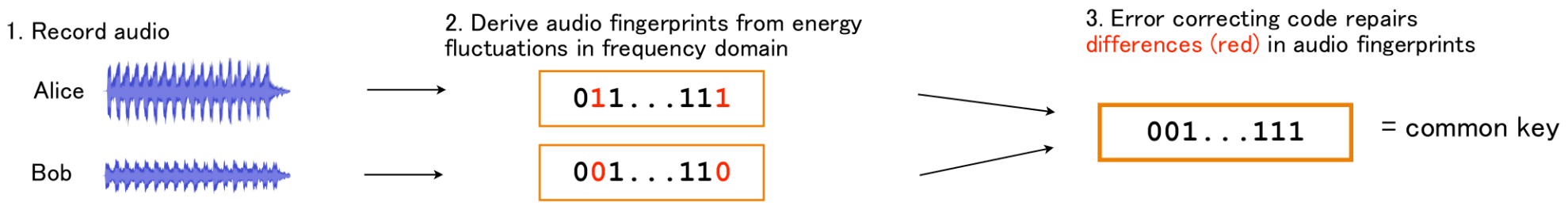
I am evaluating the security of a device pairing scheme based on ambient audio allowing users to unobtrusively pair their mobile devices. Authentication is achieved by recording audio in a common audio context relieving users of the hassle of entering passwords.

Motivation

What kinds of attacks is this protocol vulnerable to? Sound waves can be heard and recorded by everyone in the vicinity. In which way can an attacker outside Alice's and Bob's audio context guess their common key or distort the protocol?

Generating a common key between mobile devices from ambient audio



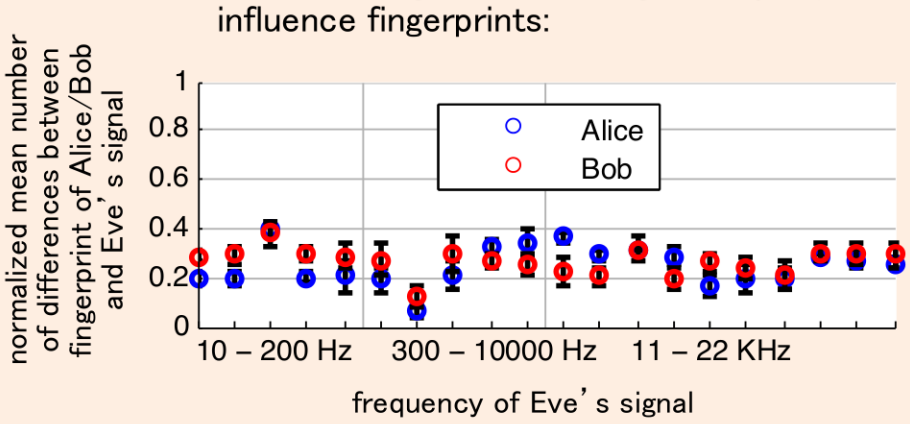


Attack scenarios and Evaluation

Active Attacks

▪Eve can influence the key Alice and Bob generate by playing audio signals. Certain types of attack signals might not attract Alice's and Bob's attention. Ringing cell phones are common e.g.

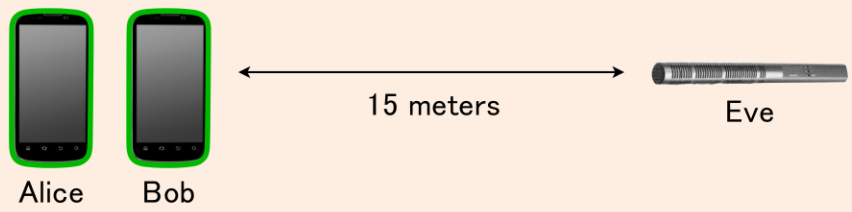
▪Eve can play audio signals on frequencies outside the human hearing range and attack Alice and Bob without them noticing. Yet these signals equally influence fingerprints:



To alleviate this kind of threat, a bandpass filter can be applied.

Passive Attacks

▪Can Eve use directional microphones to "sneak into" Alice's and Bob's audio context from a distance? Yes, even at 15 meters distance!



The fingerprints of Alice and Bob as well as Alice and Eve (Bob and Eve respectively) differ in approx. 30 % of their bits regardless of this distance.

▪Inconspicuous and invisible microphones present everywhere might not be noticed by Alice and Bob. This could include a boundary layer microphone on a conference table or a lavalier microphone used by someone standing close to Alice and Bob:

Collaboration:
Matthias Budde and Michael Beigl, TECO, Karlsruhe Institute of Technology, Karlsruhe, Germany
Tatsuo Nakajima, Distributed and Ubiquitous Computing Laboratory, Waseda University, Tokyo, Japan