The graduate acoustic attack:
“The sound of silence” °

Jean-Jacques Quisquater (UCL-Crypto)
Moti Yung (Google, Columbia)

° Thanks to Garfunkel and Simon
Tuesday August 19, 2014, 2pm, CRYPTO-UCSB:
3 set-ups of acoustic attacks against a long RSA key (Genkin-Shamir-Tromer)
Acoustic attack: the model

Your COMPUTER with RSA key to be attacked
→ At some distance vibrating OBJECT (MICROPHONE) connected to another computer
→ signal and cryptographic processing
→ RSA key in the hand of enemy
We want more: attacking from outside such an computer put in a sound-proof room ...

• We want to expand our knowledge of **Acoustical Intelligence** (**ACOUSTINT**, sometimes **ACINT**): it is an intelligence gathering discipline that collects and processes acoustic phenomena.

• Here is a possible set-up for the computer (and the user 😊) ...
Acoustic attack: new model

Your COMPUTER with RSA key to be attacked
→ At some distance some vibrating OBJECT (which one?)
→ Full-proof-sound room and window
→ Signal and cryptographic processing
→ RSA key in the hand of enemy

Is it possible?
By the way how old are acoustic attacks?
A Century Old Invention: the photophone.

April 26th, 1880 – Alexander Graham Bell & Sumner Tainter announce their invention - the Photophone. Sound is transmitted on reflected light-rays a distance of 213 meters. They also claim, “it can transmit songs with great purity of tone.” This is the forerunner of CDs, DVDs, fiber optic telephone transmission, and remote eavesdropping.

The idea:
Other old projects (acoustic locators)
More about active acoustic attacks:
1. replacing sun by remote laser in the photophone


The configuration includes projection of laser beam and observation of the movement of the secondary speckle pattern that are created on top of the target (diffusive object). The speckles are self interference random patterns and have the remarkable quality that each individual speckle serves as a reference point from which one may track the changes in the phase of the light that is being scattered from the surface. The sensor is a fast expensive camera (7800 fps) used in defocused mode.
Then taping a cellular phone or listening from the back of the neck! Possible range is 100 meters or more using a telescope.
2. A new passive acoustic attacks: the visual microphone (SIGGRAPH 2014, last week) by Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham Mysore, Frédo Durand, William T. Freeman

- Replacing the sensor (classical microphone) by any familiar vibrating object close to the sound then using a remote comescope: they then amplify a lot these vibrations from the object using an algorithm (Eulerian Video Magnification). Then they recover the sound.
Final model and set-up

- RSA "sound" from a computer to be attacked,
- corresponding vibrations of a familiar object close to the computer,
- (mirror and) sound-proof window and room,
- external camescope (using a trick: the rolling shutter) with zoom for the attack,
- translation of the images into "sound" using Eulerian Video Magnification,
- if necessary "deblurring" of the sound thanks to the equivalent method for images (using several sources), see http://users.soe.ucsc.edu/~milanfar/ (March 2014 in recent news)
- then using the ideas from the CRYPTO 2014 paper.
Gyrophone: Recognizing Speech from Gyroscope Signals

Authors:
Yan Michalevsky and Dan Boneh, Stanford University; Gabi Nakibly, National Research & Simulation Center, Rafael Ltd.

Open Access Content
Papers are restricted to registered attendees until the event begins. Once the event begins, the content becomes free and open to everyone. Journal articles are open to everyone upon publication. If available, video, audio, and/or slides of this presentation will be posted here after the event.

Abstract:
We show that the MEMS gyroscopes found on modern smart phones are sufficiently sensitive to measure acoustic signals in the vicinity of the phone. The resulting signals contain only very low-frequency information (<200Hz). Nevertheless we show, using signal processing and machine learning, that this information is sufficient to identify speaker information and even parse speech. Since iOS and Android require no special permissions to access the gyro, our results show that apps and active web content that cannot access the microphone can nonetheless eavesdrop on speech in the vicinity of the phone.