MIT 6.829: Computer Networks Fall 2017

Lecture 11: Network Security

Scribe: Rotem Hemo, Utsav Banerjee

Today

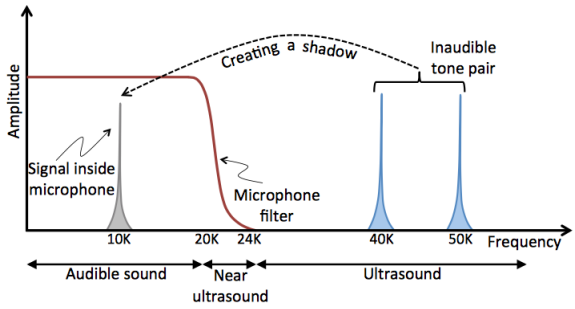
1. Backdoor
2. Acoustic communication

Overview

This lecture is on acoustic communications and physical layer security. Cryptographic techniques can be used to provide confidentiality and integrity of transmitted messages, however they can not prevent physical layer attacks such as jamming. This is a real concern in devices, such as medical implants (e.g., pacemakers), which do not use any encryption. In such scenarios, attackers can not only query data but also send commands over the unencrypted channel.

1 Backdoor

1.1 objectives



There are few problems with near ultrasound range (20KHz – 24KHz) that backdoor needs to overcome-

1. Near ultrasound frequencies are audible by babies and pets
2. The bandwidth is low (about $4KHz$)

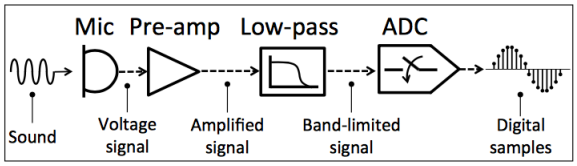
1.2 Backdoor Benefits and functionality

1. Establish a communication channel with any receiver that has a microphone
2. Attacks on security, such as evading access control, denial of service (jamming) and establishing covert channels
3. Providing security, such as preventing a private communication from getting recorded

2 Acoustic Communication

2.1 How does a microphone work?

Microphones consist of an amplifier that is expected to have linear input-output characteristics, but is non-linear in practice.



2.1.1 Low Pass Filter

Removes anything about a threshold (say 20KHz)

2.1.2 Amp

The input-output relationship can be written as

- $V_{out} = AV_{in} + A_2V_{in}^2 + \underbrace{A_3V_{in}^3 + \dots}_{\text{negligible factors}}$ where A is a the amplifying factor.
- Backdoor exploits the 2nd ($A_2V_{in}^2$) factor.

2.2 Basic idea

2.2.1 Leverage the non-linearity of the signal.

For example, suppose the input is the sinusoid $v_{in} = \sin \omega_0 t$ with frequency ω_0. Then, the output is:

$$v_{out} = A_1 \sin \omega_0 t + A_2 \sin^2 \omega_0 t = \frac{A_2}{2} + A_1 \sin \omega_0 t - \frac{A_2}{2} \cos 2\omega_0 t$$

that is, the output contains a scaled version of the input sinusoid at base frequency ω_0, along with an additional DC component and another sinusoid with frequency $2\omega_0$, called the second order harmonic.

2.2.2 Transmit 2 sinusoid $\rightarrow$ inter-modulation

Let us consider a signal which is the sum of two sinusoids $v_{in} = \sin \omega_1 t + \sin \omega_2 t$. Then, the output is:

$$v_{out} = A_2 + A_1(\sin \omega_1 t + \sin \omega_2 t) - \frac{A_2}{2}(\cos 2\omega_1 t + \cos 2\omega_2 t) + A_2(\cos(\omega_1 - \omega_2)t - \cos(\omega_1 + \omega_2)t)$$

that is, we not only get higher frequency harmonics at $2\omega_1$, $2\omega_2$ and $\omega_1+\omega_2$, but also a low frequency harmonic at $\omega_2-\omega_1$ (assuming $\omega_2>\omega_1$). Even if ω_1 and ω_2 are in the ultra-sound range, $\omega_2-\omega_1$ can be in the audible range (i.e. pass the LPF).

2.3 Challenges

1. Non-Linearity in speakers
2. Choosing an appropriate modulation for communication signal
3. Jamming without excessive power

2.4 Modulation

2.4.1 Amplitude Modulation (AM)

$$
\begin{aligned}
S_{AM} &= a\cdot \underbrace{\sin(\omega_m t)}_{\text{message}}\cdot \underbrace{\sin(\omega_c t)}_{\text{carrier}} \\
S_{AM}^2 &= A_2\Big(a\sin(\omega_m t)\cdot(\omega_c t)\Big)^2 \\
&= -A_2\frac{a^2}{4}\cos(2\omega_m t) + \text{some higher frequency}
\end{aligned}
\tag{1}
$$

That is, there are no low-frequency harmonics. Also, None linearity at the speaker can create harmonics in the audible range (i.e. would cause the message to be heard in the room). Therefor, we can't use AM for this system.

2.4.2 Frequency Modulation (FM)

$$S_{FM} = sin\Big(\omega_c t + \beta\sin(\omega_m t)\Big)$$

When FM gets squared it **doesn't** generate any audible signal.

$$S_{FM}^2 \sim 1+\cos(2\omega_c t + \text{ other terms })$$

New problem: It won't produce sound at the microphone as well.
Solution: Add **another speaker** and use it to produce the sound. This would generate the (f_c-f_s) components.

2.5 Ringing effect

The piezoelectric ("Shadow" from old transmissions) in the microphone's diaphragm has a characteristic of the form $h(t)=k_0\delta(t)+k_1\delta(t-1)+k_2\delta(t-2)+\cdots\approx k_0\delta(t)+k_1\delta(t-1)$

Therefore, for an input signal $s(t)$, the output is $h(t)\star s(t)=k_0 s(t)+k_1 s(t-1)$, that is, we have a sum of two sinusoids. This creates the same undesirable effects as using amplitude modulation.

BackDoor solves this problem by characterizing the microphone to determine $h(t)$. The input to the microphone is $s'(t) = h^{-1}(t) \star s(t)$, so that the output of the diaphragm is $h(t) \star s'(t) = h(t) \star h^{-1}(t) \star s(t) = s(t)$.

2.6 Jamming

BackDoor achieves signal jamming by sending occasional full-amplitude spikes to re-calibrate the microphone ADC to full range and making the message signal fall only in the first bit of the ADC.

References

[1] Nirupam Roy, Haitham Hassanieh, and Romit Roy Choudhury. 2017. BackDoor: Making Microphones Hear Inaudible Sounds. In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '17). ACM, New York, NY, USA, 2-14. DOI: https://doi.org/10.1145/3081333.3081366