2017年度浙江大学学术进展

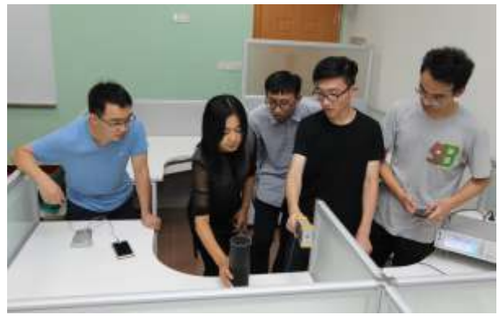
“海豚音攻击”基于麦克风非线性作用的硬件漏洞发现与防护

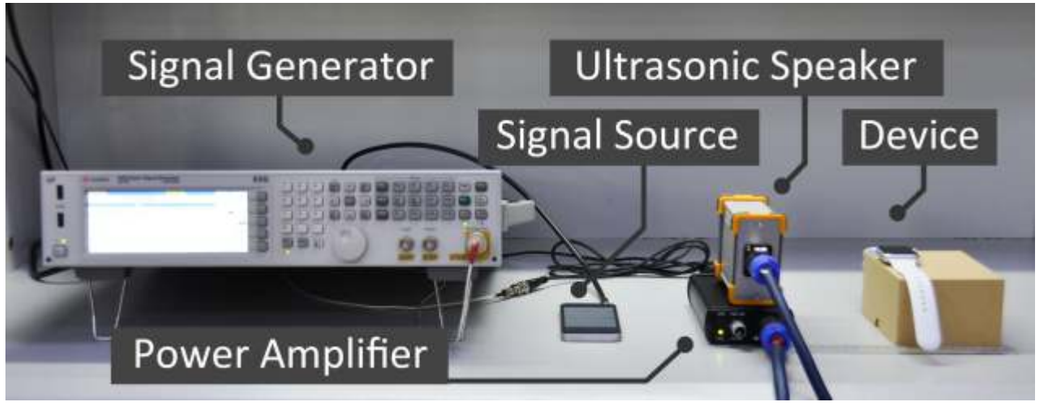
★ ★ ★ ★ ★ 〈入选年度十大学术进展〉

针对智能设备的麦克风传感器，首次发现了由于硬件耦合带来的系统漏洞，并给出了相应的防护和解决方案。在语音系统日益普遍的今天，DolphinAttack作为一个启发性和标志性的成果，在物联网安全领域具有重要意义。

项目负责人：徐文渊

语音助手系统让人通过最自然的语音输入方式和现代计算系统交互，它已经在手机、电脑、音箱、智能家居、汽车等智能设备上得到了广泛应用。作为一种便捷的重要人机交互方式，可以预见语音助手将在越来越多的设备系统中运用，为保护这些带有语音助手功能的系统，语音助手本身的安全性至关重要。该项研究针对语音助手系统进行安全分析，研究发现并对安全问题进行防护。其中研究成果包括两方面，（1）立足于语音助手依赖的声音传感器（麦克风），首次发现了





Manuf.	Model	OS/Ver.	SR System	Attacks Recog.	Attacks Activ.	Modulation Parameters f_c (kHz) & [Prime f_c]	Modulation Parameters Depth	Max Dist. (cm) Recog.	Max Dist. (cm) Activ.
Apple	iPhone 4s	iOS 9.3.5	Siri	√	√	20–42 [27.9]	≥ 6%	175	110
Apple	iPhone 5s	iOS 10.0.2	Siri	√	√	24.1–26.2 27 29.1 [26.1]	100%	7.5	10
Apple	iPhone SE	iOS 10.3.1	Siri	√	√	22–28 31 [24.6]	≥ 45%	30	25
			Chrome	√	N/A	22–26 29 [22.6]	≥ 37%	19	N/A
Apple	iPhone SE+	iOS 10.3.2	Siri	√	√	23–29 31 33 [22.4]	≥ 45%	25	24
Apple	iPhone 6s+	iOS 10.2.1	Siri	√	√	26 [26]	100%	6	12
Apple	iPhone 6 Plus	iOS 10.3.3	Siri	5	√	— [24]	—	—	5
Apple	iPhone 7 Plus	iOS 10.3.1	Siri	√	√	21 24–28 [25.3]	≥ 30%	19	32
Apple	watch	watchOS 3.2	Siri	√	√	26–37 [22.3]	≥ 5%	11.1	14.6
Apple	iPad mini 4	iOS 10.2.1	Siri	√	√	23–46 [29.8]	≥ 25%	91.6	50.3
Apple	MacBook	macOS Sierra	Siri	√	N/A	20-22 24-25 27-37 38 [22.8]	≥ 76%	35	N/A
LG	Nexus 5X	Android 7.1.1	Google Now	√	√	30.5 [30.7]	100%	4	11
Asus	Nexus 7	Android 6.0.1	Google Now	√	√	24–29 [24.1]	≥ 5%	10	87
Samsung	Galaxy S6 edge	Android 6.0.1	S Voice	√	√	28–38 [29.4]	≥ 17%	36.1	91.2
Huawei	Honor 7	Android 6.0	HiVoice	√	√	29–37 [29.6]	≥ 17%	19	16
Lenovo	ThinkPad T440p	Windows 10	Cortana	√	√	23.8–25 [23.6]	≥ 35%	50	8
Amazon	Echo	5589	Alexa	√	√	23-24 25-31 33-34 [24]	≥ 25%	105	165
Audi	Q3	N/A	N/A	√	N/A	21–23 [21]	100%	18	N/A

[2] Prime f_c is the carrier wave frequency that exhibits highest baseband amplitude after demodulation. — No result
[3] Another iPhone SE with identical technical spec.
[4] Experimented with the front/top microphones as device.

由于硬件耦合带来的系统漏洞，并利用此漏洞在20多种智能设备上实施了“海豚音攻击”，该攻击可通过人耳不可听的方式实现有声语音指令的注入，从而以隐秘的方式控制智能设备拨打电话、发送信息、访问网页、购物等，威胁用户安全和隐私。（2）该研究成果同时包括相应的硬件和软件层面防护方案，通过麦克风硬件改进和基于SVM的分类器对攻击进行防护和检测，可提高语音交互方式的安全性。

该成果发现在麦克风中广泛存在非线性作用。非线性作用是指信号在通过设备时，输入与输出表现出非线性关系，这一现象主要源于硬件设备本身。通过利用这一现象，该成果成功将语音指令以人耳听不到的频率发送给智能设备，通过麦克风的非线性解调后，恢复出语音信号有效。此时，语音助手识别到该有效语音指令，并控制智能设备执行恶意操作。

针对这一硬件漏洞，该成果首次提出基于硬件和基于软件的防御方案。其中，基于硬件的防御方案是重新设计麦克风，通过抑制麦克风的高频响应，使得麦克风无法“听”到人类无法听的高频声音，避免了无声指令耦合进麦克风电路的可能。在软件上，通过分析正常语音和通过海豚音攻击产生的语音，发现两者在较高频段的信号有较大差异。基于此发现，该成果提出了基于机器学习的防御无声指令控制语音助手的方法，并达到理想的效果，因此，各大生产厂商只需要更新智能设备的系统就可以解决这个安全隐患。