

Forum:[Hack Forums](#)

Thread: [Hacking Audio 4096-bit encryption beatten](#)

DrPanda - September 9, 2014, 3:18 pm

ok this really isn't a relatively new thing, but in recent years it has been on a new level of OH HOLY JEBUS, WHERE IS MY TIN FOIL HAT...

What im talking about is Acoustic Hacking, and No im not talking about what you seen Matthew Broderick doing with a Tape Recorder in "WarGames" to get trough a door or what you seen the "Freak" use in "Hackers" to get free long distance, even tho as cool as Matthew Broderick was and Freaks phreaking skills, its not the point

No what im talking about is actually hacking audio signals and using the to capture important information us as passwords, names even documents (in a far future), ok yes using your granddads hearing aid to listen for button presses on keypads is pretty LEET but, still not what im talking about or even about the scene in "Eagle Eye" where the self aware robotic running the country was able to capture sensitive data by watching vibrations in a cup of water, even tho it kinda ties into what im saying here.

Did you know this, cause I really didn't until I did some background research into it and have discovered that its legit and currently in use, some computers even laptops emit a high-pitched noise during operation, due to vibration in some of their electronic components. we don't hear these because simplify our ears are just not sensitive enough to hear the sounds.

three researchers have been testing this theory, and have actualy developed a phone app.. the 3 tested the theory on a laptop with a 4096-bit RSA encryption—which, in layman's terms, is an incredibly tough code to crack. When the key to decrypt the code is entered into the computer, the computer runs a series of protocols to unlock the encrypted data, and the CPU makes a noise. The researchers then placed a mobile phone 30 centimetres from the target laptop, and pointed the phone's internal microphone towards the laptop's fan vents.

from they data they recorded vs pre matched and confirmed data, they were able to write a Key to bypass the password, now for those of you who don't know 4096 bit encryption would take 100 super computers a millions years to crack it the key, these guys done it in 30 seconds only thing was they had to be near the machine or atleast have a directional microphone in the same room pointed at the vents.

this type of attack has now been named acoustic cryptanalysis.. the app itself is hidden and not yet available... but I feel soon someone smart will see the potential will see it and design and app to do it either for Gov use or for BlackHat use...

a example of a how this attack would go down was said by the lead researcher.

The whole attack could be packaged into a software "app" requiring no special hardware or knowledge. An attacker would install this software, reach physical proximity to the target computer under some pretext, and place the phone appropriately for the duration of the attack. For example, in a meeting, the attacker could innocuously place his phone on the desk next to the target laptop...and obtain the key by the meeting's end. Similar observations apply to other mobile devices with built-in microphones, such as tablets and laptops.

Ok now what you guys want to know THE APP ISNT AVAIBALE if you want it write yourself and read trough the 1000 page report the research published...

another way of look at this, like what I said before about "Eagle Eye", in theory this same method could be used to recorded ripples in a glass of water left on a table beside the machine, by having a list of possible words that create a type of vibration... OK our eyes couldn't see it but in a small sound proofed room there would be tiny vibrations in the water that a very High focused and high frame camera may be able to pick up

how would this attack be stopped.... emmm Block your vents yeah now I don't know how it would work, without destroying your system. maybe hardware hacker will make a frequency emitter to send out scrappy pitched noise to screw with the microphone, that wouldn't be such a hard thing to make really, just a buzzer on low frequency sending out randomised pulses at a low level of power just enough to cover the noise of the machine.

Ok I feel iv posted this in the wrong section.... Sorry, but it may become the right section if someone here actually knows about a tool that does this