

Forum:[Hack Forums](#)

Thread: [AirHopper: Hacking Into an Isolated Computer Using FM Radio Signals](#)

The2G - November 4, 2014, 1:21 pm

Hi mates,

I just read a new that surprised me, Security researchers at the Cyber Security Labs at Ben Gurion University in Israel have found a way to snoop on a personal computer even with no network connection.

STEALING DATA USING RADIO SIGNALS

Researchers have developed a proof-of-concept malware that can infiltrate a closed network to lift data from a machine that has been kept completely isolated from the internet or any Wi-Fi connection by using little more than a mobile phone's FM radio signals.

Here's the proof:

[Video: <https://www.youtube.com/watch?v=2OzTWiGl1rM>]

So will the computers be always unsafe, even when they aren't connected to a LAN or other kind of net? Maybe no one is safe... However, would be cool if the researchers release the code (??)... After that I really get interested in research about that method, and I want to know other people opinions about it.

The original post: <http://thehackernews.com/2014/10/airhopper-hacking-into-isolated.html>

pomwtin - November 4, 2014, 2:15 pm

Hmm.. so those frequencies coming from MB (cpu??) can be decoded?

I noticed that each keystroke have its own frequency, but did not thought of that (afcourse if this is the same thing).... interesting, thank you for sharing :)

Mad76e - November 4, 2014, 2:16 pm

Are still not convinced .. Do you have more info from more sites

Links please :D

The2G - November 4, 2014, 11:33 pm

(Nov 4, 2014 03:15 PM)pomwtin Wrote: [\[CITE\]](#) Hmm.. so those frequencies coming from MB (cpu??) can be decoded?

I noticed that each keystroke have its own frequency, but did not thought of that (afcourse if this is the same thing).... interesting, thank you for sharing :)

No matter bro. I guess that the signal is send to somewhere (inf) with no objective, only because our PC "creates" automatically that kind of signal in each keystroke. I don't know very well how it works but, will read more about it.

(Nov 4, 2014 03:16 PM)mad76e™ Wrote: [\[CITE\]](#) Are still not convinced .. Do you have more info from more sites

Links please :D

Yes I do. I'll link a PDF of the creators.

Here it is (Is the datasheet and more info about the process and how it works):

<http://www.slideshare.net/mordechaiguri/air-hoppermalwarefinale>

mattybeds - November 5, 2014, 8:34 am

I've been experimenting via my RTLSDR and found a signal, not sure how to convert it to text. It only happens when I point aerial at GF's laptop while she's using it.

King of Clubs - November 5, 2014, 8:39 am

If this is true/works then it's pretty darn cool.

yacked2 - November 5, 2014, 9:39 am

If that actually works, even in a crowd, we fucked up... It's time to use Vigenere cipher again :)

The2G - November 8, 2014, 5:38 am

Yes I guess is true... But shall we develop the hack before the protection programs? I mean, if anyone who has that software which decodes radio signals into characters (working as keylogger) it may decode other stuff.

I'll continue reading about, possibly try to code an android app who reads that signals..

ciocan - November 8, 2014, 1:09 pm

This concept is very old. I know about experiments successfully conducted in '90 to intercept the signal from a computer monitor (wired) from miles away. Also the keyboard can be intercepted from large distances. Also it was a software to decode key strokes with audio (each key has a specific sound they claim).

Here is another example based on my experience when dealing with bad sound cards and shitty speakers, you can hear in speakers when the CPU is starting to work. It is a specific sound.

Now I also know that if you fine tune in the CPU frequency you can send it instructions like read hdd... All you need is the adequate equipment and funds to do that.

To intercept the signal from CPU is easy, the complicated part is to send instructions.

Mad76e - November 8, 2014, 2:33 pm

(Nov 8, 2014 02:09 PM)ciocan Wrote: [\[CITE\]](#) This concept is very old. I know about experiments successfully conducted in '90 to intercept the signal from a computer monitor (wired) from miles away. Also the keyboard can be intercepted from large distances. Also it was a software to decode key strokes with audio (each key has a specific sound they claim).

Here is another example based on my experience when dealing with bad sound cards and shitty speakers, you can hear in speakers when the CPU is starting to work. It is a specific sound.

Now I also know that if you fine tune in the CPU frequency you can send it instructions like read hdd... All you need is the adequate equipment and funds to do that.

To intercept the signal from CPU is easy, the complicated part is to send instructions.

Hmm.. So you need some kind of software that can translate the superweak electromagnetic pulse that the chipset inside the keyboard sends to the computer..

But different keyboards have different chipsets and may work on different frequencies?? or?

Anyhow, I know about tapping a copper cable and how you do that without harming the cable... But how about a keyboard from a distance? Let's say a 300 meters? Would it not be hard with a lot of interference?

I have to go over the text again :)

ciocan - November 8, 2014, 3:37 pm

All keyboard use the same signal. I dont think they target the CI from keyboard but the signal that travels trough cable and that signal is identical on all keyboards (different connectors, probably different signals and there are 3 types of connectors until now). If the signals are not the same then keyboard will not be recognized. Correct?

Now lets talk about with interference. If you have a bean very narrow you can tune it like a laser in the target spot. I believe that you see in movies equipment (antennas) for spying people what they are talking let say in a park. Something like that can be used also to intercept rf signals from keyboard, cpu or something else.

Oh and please change your pictures from your avatar because i was trying to kill the bug from my screen ?

Mad76e - November 8, 2014, 4:12 pm

(Nov 8, 2014 04:37 PM)ciocan Wrote: [\[CITE\]](#) Oh and please change your pictures from your avatar because i was trying to kill the bug from my screen ?

Damn... I hope you didn't slap the monitor to hard.. Monitors are expensive.. Remind me tomorrow ? almost time to sleep here

ciocan - November 8, 2014, 6:35 pm

Check this out!

<http://lasec.epfl.ch/keyboard/>

If is possible from 20m then can be possible from a bigger distance with an adequate antenna/equipment.

Now all we have to do is to deauth a client and force it to input again the pass. Here is a new idea how to get wpa/wpa2 keys ?

By the way, from where i can get this AirHopper apk? I try to search but i found something else with similar name...

Here is something else interesting

<http://books.google.ro/books?id=OOe5C79fQQsC&pg=PA185&lpg=PA185&dq=intercept+keyboard+signal&source=bl&ots=ABCT3OtBPR&sig=k0osbr6ilxmfV6dGTvQYRuYviO0&hl=ro&sa=X&ei=z9ReVLimB4rCPO2kgZgB&ved=0CDAQ6AEwAzgU#v=onepage&q=intercept%20keyboard%20signal&f=false>

So the concept is very old and can be used even today...

The2G - November 9, 2014, 3:19 am

Ciocan: I guess you can't get the apk instead of is coded by you. I don't think they're going to release to all the public. But can try to code something similar..

However I thinks is a bit hard to code that, because you should gather all the frequencies before and add it to a lib or something to be able to read and after to convert it to a character.

ciocan - November 9, 2014, 4:16 am

I try to search on FM and i find some frequency where you can hear when a key is stroked. Probably i need a spectrum analyzer to see what is the correct frequency.

I dont think it will require a database if the signal is decoded. Is just a code that correspond to a specific key. The code can be found on internet or in the old books about computers.

This is my opinion, maybe is right or wrong, i cant be sure...

The2G - November 9, 2014, 4:52 am

Yes probably can do it with the spectrum analyzer. I don't know the exact functionality but can be both of them depends on the coder I guess. I'm still looking for that apk or code... If I finally can find the code I'll share here.

PD: I found a website with lot of radio signal analyzers for android

<http://www.radioworld.com/article/apps-for-engineers-android-phones-and-tablets/211452> only one is free :S

brandon4511 - November 9, 2014, 5:33 pm

i send this the day it came out fking crazy

Anonymous_35H - June 9, 2018, 8:13 am

I suggest creating a group of people interested in this tool
To complete the search and reprogramming it :)

Basically: I do not think anyone will give me the tool easily and without charge

So I doubt it is for

During my search, someone gave me this link to download the tool:

Link: docs.google.com/document/d/1ewclA5b4dGtvApoXHodKqPDx-Mg-APDQw3YCp_INkoE/edit

But I repeat .. I strongly doubt that it is a trap

Edit::

I detected the file and confirmed it was a virus ?

But whatever it is, I suggest that we Create a Team devoted his time to looking behind this idea and re-establishing it better than it is ?

Note: I am a new member on the site .. but not new in the science of piracy ?

Check this out!

#####github.com/maq/tfc/wiki/Security-design

gotta go - June 11, 2018, 9:57 pm

can i do the same thing on computer?

pasnger57 - June 12, 2018, 9:59 am

I fell this is interesting but only apply\ to computer/s that are using a Wireless keyboard or mouse and thus not a Fully ISOLATED ... what access is in use then to say FM/RF so i'am guessing wireless keyboard and mouse is the hole in this case
...stick to wired keyboard+mouse and this provably wont work

gotta go - June 15, 2018, 8:31 pm

is anyway to defend the attack?

Anonymous_35H - June 18, 2018, 2:39 pm

I do not think so : pasnger57

Because I have been able to access some books that talk about this subject
even I came to the book that the author who invented this tool

Authors are:

4 authors .. including :

#Gabi Kedma

#Yuval Elovici

I have been able to steal some paid books that talk about it ?

Wow it's very interesting ?

Thread real .. but it is very complicated and sensitive

I hope to be a team of people interested in this tool and develop it ?

tron - June 18, 2018, 9:11 pm

Back in the 90's there was something similar called Van Eck Phreaking, sniffing signals off of CRT and LCD monitors.

Way to dig up a 4 year old thread BTW.