Tails - Bug #10803
Network Connections persistence feature stores MAC address of network interface
12/29/2015 11:21 AM - goupille

| Status:     | Confirmed                      | Start date: | 12/29/2015 |
| Priority:   | Normal                         | Due date:   |             |
| Assignee:   | spriver                        | % Done:     | 0%          |
| Category:   | Persistence                    | Estimated time: | 0.00 hour |
| Target version: |                   | Spent time: | 0.00 hour |
| Feature Branch: |                      | Starter:    |             |
| Type of work: | Code                          |             |             |

Description
If the network persistence is activated, the real MAC address of the NIC used at that time are stored in the
/live/persistence/TailsData_unlocked/nm-connections/ files.
those files belong to root, but there no point to keep that kind of informations.

Related issues:
- Related to Tails - Bug #10985: Make it clear that Network Connections persist...
  Confirmed 01/23/2016
- Related to Tails - Feature #11681: Decide if/how we want plausible deniabilit...
  Rejected 08/20/2016

History
#1 - 12/29/2015 02:26 PM - spriver
- Assignee set to spriver

#2 - 12/29/2015 02:34 PM - spriver
I'll research if this could be solved via modifying or creating a dispatcher.d script after establishing a connection. Or should this be done in another way?

#3 - 01/02/2016 12:18 PM - sajolida
- Category set to Persistence
- Status changed from New to Confirmed
- Type of work changed from Research to Code

You can check the list of grep `':/etc/NetworkManager/system-connections/' | sed 's/\./\=\///' | uniq -c.`

spriver: a dispatcher sounds good but don't hesitate to check this with anonym who's the Network Manager spaghetti master!

#4 - 01/02/2016 10:06 PM - intrigeri
I'm very happy if someone works on this. It would be good to reality check how serious the potential consequences are, at some point.

I'll start playing. Off the top of my head: my persistence will keep track of all the computers I've been booting my Tails (with NM connections persistence enabled) on. So... what? At least, an attacker who gains root access on my Tails while my persistent volume is enabled can learn that info (but really, at this point they've also learnt so much other things Tails tries to protect that it's game over, and trying to optimize for this specific situation does not feel like a very good use of our time).

Anything else?

By the way, maybe nmcli con show $ID can give this info to the amnesia user, instead of root only. If this is indeed the case, then the problem may be more severe than what was initially described.

05/18/2020
I was wondering about the impact of this as well.

I agree that it doesn't seem like a big deal in the user scenarios that first come to my mind but on the other hand we're putting lots of warning around the persistence that say:

- "Take into consideration that you can be forced or tricked to give out its passphrase" which contemplates an attacker having access to your persistence.
- "Only the files and folders that you specify are saved" which contradicts what's happening here as we're not advertizing saving the identifiers of computers we use.

So I still think that this info should be cleaned for better consistency with what's we're telling people about the persistent volume.

---

sajolida wrote:

I was wondering about the impact of this as well.

I agree that it doesn't seem like a big deal in the user scenarios that first come to my mind but on the other hand we're putting lots of warning around the persistence that say:

- "Take into consideration that you can be forced or tricked to give out its passphrase" which contemplates an attacker having access to your persistence.
- "Only the files and folders that you specify are saved" which contradicts what's happening here as we're not advertizing saving the identifiers of computers we use.

So I still think that this info should be cleaned for better consistency with what's we're telling people about the persistent volume.

I'd like to follow up on the case if an attacker/adversary has access to the passphrase of the persistent volume. MAC-adresses are usually unique associated so in such case it would be possible to reproduce not only the network names but also the "real" physical addresses of the wi-fi networks and this could reveal information regarding to locations and so on. (of course in such case the main problem would be the fact that an the whole partition is available to an adversary)

---

MAC-adresses are usually unique associated so in such case it would be possible to reproduce not only the network names but also the "real" physical addresses of the wi-fi networks and this could reveal information regarding to locations and so on.
I agree it would be ideal not to save 802-11-wireless.seen-bssids in persistence. And if we can avoid saving it in just the same way as 802-11-wireless.mac-address, great.

Still, I don't think this would fully solve the problem you're highlighting: when one opts in, for the sake of convenience, to store the list of Wi-Fi networks they are visiting on their persistent volume, then almost by definition they're opting in to store a growing set of somewhat identifying geo-location information... and it'll be true even without BSSID:s. So, if our current configuration interface + documentation does not make this clear, we have a different problem here (that deserves its own ticket).

---

**#8 - 01/06/2016 03:50 PM - sajolida**

- Subject changed from Network Manager's persistence record real MAC addresses to Network Connections persistence feature stores MAC address of network interface

I think there's some technical misunderstanding here from what spriver said. We're talking here about the MAC address of the network interface (of the computer) and not about the MAC address of the Wi-Fi access point. So this is not about geolocation but about which computer the user has been using. Renaming the ticket accordingly.

For example, this could lead to associating a Tails USB stick with some computer it has been used on, either revealing the owner of the USB stick, the owner of a computer, or temporary relationships between the owner of the USB stick and the owner of the computer in case it was borrowed on some occasion. Such information goes quite beyond "which network I connected to" or geolocation.

---

**#9 - 01/06/2016 10:34 PM - intrigeri**

I think there's some technical misunderstanding here from what spriver said. We're talking here about the MAC address of the network interface (of the computer) and not about the MAC address of the Wi-Fi access point.

It may be that I misunderstood what spriver wrote, indeed. I'm sorry I went off-topic by mentioning BSSID:s, I hadn't re-read the ticket's description, and its title was general enough to make it look like BSSID:s could be sensibly included in the problem being discussed.

Such information goes quite beyond "which network I connected to" or geolocation.

Indeed they are different problems. It's not obvious to me which one goes "beyond" the other: depending on the threat model, one or the other may be worst. Anyway, I'm fine with refocussing this ticket as you did, I think it makes sense. Thanks! This doesn't make the other problem that I mentioned go away, though => I'll file a dedicated ticket about it, then, so we can address it differently if needed.
#10 - 01/23/2016 01:10 PM - intrigeri
- Related to Bug #10985: Make it clear that Network Connections persistence feature stores geo-location information added

#11 - 08/18/2018 09:53 AM - Anonymous
Is this still relevant? If yes, what are the next steps here?

#12 - 08/18/2018 09:53 AM - Anonymous
- Related to Feature #11681: Decide if/how we want plausible deniability for the persistent volume added

#13 - 08/21/2018 03:39 PM - sajolida
I think that when a network configuration (basically the password) was saved from a network interface with a given MAC address, then it won’t be reused for the same network but with a different MAC address.

So, let's say you try to connect to the say network from the same Tails USB stick but two different laptops, then you won't be able to reuse the password.