Protect against fingerprinting via active Wi-Fi networks probing

Even once feature/spoof-mac is merged, Tails does not protect against AdvGoalTracking and AdvGoalProfiling due to "active probing" performed by NetworkManager for Wi-Fi connections. This puts AvoidTracking at risk, especially when using the NetworkManager persistent connections feature.

Subtasks:
- Feature # 6454: Evaluate how hard it would be to disable active probing in NetworkManager

Related issues:
- Related to Tails - Feature #7380: Randomise MAC address when scanning for Wi-Fi networks even when MAC spoofing is disabled
- Related to Tails - Feature #11293: Check if/how we should use NetworkManager'

Associated revisions
- Revision c6097c52 - 01/30/2017 05:32 PM - intrigeri
  MAC spoofing design doc: clarify that at most five SSIDs from stored connections are used for directed Probe Requests.
  refs: #6453

History
#1 - 02/21/2014 11:05 AM - intrigeri
  - Description updated

#2 - 06/09/2014 10:18 AM - BitingBird
  - Related to deleted (Feature #5421: Spoof MAC address)

#3 - 06/09/2014 10:18 AM - BitingBird
  - Related to Feature #7380: Randomise MAC address when scanning for Wi-Fi networks even when MAC spoofing is disabled

#4 - 01/02/2015 06:36 PM - BitingBird
  - Related to Feature #6549: Prevent MAC address leak for non-root users

#5 - 01/03/2015 11:26 AM - intrigeri
  - Related to deleted (Feature #6549: Prevent MAC address leak for non-root users)

#6 - 04/10/2015 03:04 PM - BitingBird
  One of the upstream tickets linked on the blueprint is fixed, the other is "fixed-upstream", the third is wontfix.
#7 - 03/31/2016 09:39 AM - intrigeri
- Related to Feature #11293: Check if/how we should use NetworkManager's new MAC address spoofing capabilities added

#8 - 06/26/2016 11:01 AM - BitingBird
- Status changed from Confirmed to In Progress

#9 - 08/28/2016 03:47 AM - intrigeri
- Subject changed from Protect against fingerprinting via active Wi-Fi networks probing to Protect against fingerprinting via active Wi-Fi networks probing

#10 - 01/30/2017 05:41 PM - intrigeri

BitingBird wrote:

One of the upstream tickets linked on the blueprint is fixed, the other is "fixed-upstream", the third is wontfix.

I see nothing about this topic on the blueprint, so I guess the current state of the art is documented on https://tails.boum.org/contribute/design/MAC_address/, in the "Active probe fingerprinting" section (which doesn't point to any upstream ticket actually).

#11 - 06/29/2017 10:17 AM - Anonymous
- Status changed from In Progress to Confirmed
- Assignee set to intrigeri

It's unclear to me what the next steps on this ticket are. Can somebody from the foundations team please clarify this. Unassign yourself afterwards if you're not going to work on this. Maybe this should simply be documented or added to the design documentation?

#12 - 06/29/2017 03:25 PM - intrigeri
- Blueprint changed from https://tails.boum.org/blueprint/macchanger/ to https://tails.boum.org/contribute/design/MAC_address/#active-probe-fingerprinting

#13 - 06/29/2017 03:26 PM - intrigeri
- Description updated

#14 - 06/29/2017 03:28 PM - intrigeri
- Assignee deleted (intrigeri)

u wrote:

It's unclear to me what the next steps on this ticket are. Can somebody from the foundations team please clarify this. Unassign yourself afterwards if you're not going to work on this. Maybe this should simply be documented or added to the design documentation?
https://tails.boum.org/contribute/design/MAC_address/#active-probe-fingerprinting says “active scanning should be disabled in NetworkManager when MAC spoofing is enabled”. I guess next step is to implement an option in NM to allow this.