Clarify the privacy implication of setting a locale

First, most, if not all, exploited applications have access to locale configuration.

Wrt. network fingerprinting:

- We have to assume that some applications may expose the system's locale configuration as part of their network activity.
- For Tor Browser and Thunderbird, our configuration tries to avoid this (best effort) but it's impossible to prove we did not miss anything.

Wrt. local storage:

- If an adversary can read the content of the persistent storage, I'm pretty sure that the locale configuration can be easily inferred from that.
- If/once we allow persisting the locale in cleartext on the system partition, this information will be available to an adversary who seizes the Tails device.

History

#1 - 03/18/2020 07:04 PM - sajolida
I have no idea regarding how important this would be to document and it's not trivial so I'm not making it part of core work for now.

#2 - 04/15/2020 06:02 AM - intrigeri
- Affected tool changed from Greeter to Welcome Screen