Browser based limits on logins

Browser based limits on logins

New feature idea. I'd be specially interested in opinions about using Trackers for storage.

Table of contents

Objective

This is about restricting access for people who would buy access to some paying restricted site and then share their login credentials with the rest of the world.

- When a registered user connects to website.tld, we set a cookie in his browser, and we register his browser as "authorised browser for 30 days"
- Every time he comes back to website.tld we read his cookie to check if he is an "authorised browser".
    - If he is already authorised we let him log in, and update the "authorised browser" expiration date to 30 days further
    - if he is not we check how many "authorised browsers" do we have listed from him.
        - If we have less than 3 authorised browsers: we register his new browser and let him log in.
        - If he already has 3 authorised machines: deny the login.

- In case a browser is not used in 30 days we drop it from the list of authorised browsers.
- I will also need a "control panel" so I can manually remove authorised machines from the list (I guess I will have to make some exceptions as users buy new computers, delete cookies, travel...), or change the number of authorised browsers to 4, 5, 2...

Data storage

I'm considering the storage of the cookies references could be in a tracker

- Plus: added flexibility and avoiding having yet another database table. A minimal "control panel" would be sufficient because anyone can create their own fancy management wiki page using LIST or LISTEXECUTE plugin.
- Minus: it might slow down login, which decreases user experience; it will break login when the index is not synchronized; we can't use the tiki methods because permissions to these records will be limited to admins

+ Mitigation strategies: skip the tiki methods and get the info using direct SQL queries during login process. Do we have ways of registering asynchronous deletion of tracker items and asynchronous updating of fields and flagging tracker items for being reindexed?

Clean up

How do we delete obsolete "authorised browsers" records? Keeping them forever makes no sense and will eventually slow things down.

- Doing it during the login process
  - Plus: Simple
  - Minus: Might slow down login, which decreases user experience.
- Setting up a scheduled process
  - Plus: If it works, there is no negative impact
  - Minus: This requires to set up the scheduler and is too cumbersome and people will just forget to do it, or do it wrong and never notice.
- A "delete all expired records" button in the "control panel".
  - Plus: Simple. Total control for the admin, in case they prefer to keep records for analysing suspicious activity
  - Minus: They might forget to do it after a while

Technical solution so far

Following the discussion in the dev mailing list, we can split this in two parts. The first one is a general-purpose new table which can be used for other features

Login history table

A new general purpose new table for login history with all required fields for all future use cases with the following fields (not necessarily already used), and use that for my use case which would be nicely separated:

- userId
- browser name
- operating system (usually part of browser name)
- last login time
- last logout time (for later use)
- geo-location (for later use)

I would not enable it per default and especially not on our community sites because they would actually collect personal data which users have *not* volunteered. So if we want this, we should first think about our "Terms & Conditions", as mentioned in this other thread on the topic of the new eu regulations. I'd also like that it's not an on/off thing, people should decide if they want to collect IP history, OS type, geolocalisation and not collect what they don't want to have in storage about their users.

Also, this sql table would have all the data which need quick access and updating during the login phase and which we would rather not have show up in searches, which is perfect.

I could just use some tracker for the use case specific data such as keeping track of each user's maximum browser limit.

Browser based limits

Additional requirement: It's only for some groups, not all.
This looks more and more like the user tracker features.