BRAINSTORMING
let websites keep themselves out of history
stop talking about encryption in primary UI
prevent weak passwords
Keep history around longer
reverse trust decisions
lock security contexts between devices
generate key pairs as part of login ritual on demand
delicious
migrate security prefs from browser to browser
XML schema of information for development of new UIs
SRP
always match warnings with safe alternatives
indicator of non-visible/user-initiated network traffic
maybe an N-space instead of a score
express "level of confidence" as scalar variable, not binary
only signal danger, never security
improve cookie management UI
better support for multi-factor auth
catch users at the locus of attention - at the time of task
identity dangerous snippets
leverage smarts of WWW userbase/ecosystem
only signal safety, never danger
wait before warn
represent geo-loc of the endpoint I'm talking to
never send proxy-auth in clear text
never send any auth in plaintext
pagerank
display security indicators without chrome
when a safe path exists, take it and verify user action
don't display https protocol on broken SSL
don't display protocol ever!
dkim
pacing
prevent whack-a-mole/popup floods
better handling of self-signed certs
no dialog boxes
history of trust transactions
decamp and stake out new ground for security indicators
modify form fill, etc.
# of users who've been here (FoaF, BBB, facebook)
nettrust
gather demographic data on browser users to inform decisions
bind password to SSL session
repudiation for transactions
treat links from webmail/external apps as suspicious
forget the URL bar
hash
leverage knowledge of user's history
learn from users reaction speed
modify page content
build awareness of where http handoffs are coming from
"nothing's changed since last time you were here"
existing formfill as an indicator
don't do anything unsafe automatically
migration of history data between browsers
add context with links, react differently