Waterhouse: secure e-mail for human beings

Alex Lambert
Steve Bezek
COGNITIVE WALKTHROUGH
Task: E-mail a friend

Hey, after I installed Waterhouse, I started seeing my Facebook friends’ pictures here. Cool! This lock is new, too…must have something to do with security.
Extra protection: Your message will be sent securely. Evil hackers won’t be able to intercept and read it.

After I chose Steve’s name, it added a lock icon. This must mean something is secure.

Now I feel a lot better about sending my credit card number to Steve. I always hear stories about hackers stealing credit cards online.

Ahh...this is what the lock icon must mean. I hate evil hackers.

I guess this is an improvement over usual e-mail.
I guess this message doesn’t have the extra protection. If I were sending something important, I might want the extra protection. When that happens, I’ll click “Learn more”.

For extra protection, ask Jordan to use Waterhouse and add him as a Facebook friend. Learn more
You can be confident that Steve Bezek really sent this message.

Hey, it’s Steve’s picture. Cool! Hey, I guess he really sent this. Good to know, after that Chancellor thing. I hate hackers.
You can be confident that Steve Bezek really sent this message, and that evil hackers can’t read it. I feel better about using e-mail now.
HEURISTIC EVALUATION
Validity of system status

• We provide feedback through the familiar lock icon
• We update the “extra protection” message as the user chooses recipients
• There’s always a “learn more” link next to our UI text.
Match between system and the real world

• We *never* use terms like “encrypt”, “sign”, “private key”, “public key”, “RSA”, “1024-bit”, etc.

• We *intentionally* use colloquial terms like “evil hackers” and “extra protection” because they resonate with average users’ understanding of security

• Simple shorthand: when I see the sender’s picture, I know I can trust it

• Picture provides an important incentive *outside* of security benefits (which are likely boring to the average user)
User control and freedom

• No worse than conventional e-mail interface
• User can temporarily disable “extra protection” using the small “X” in the composition screen
• Easy to uninstall
  – Can gracefully degrade even if removed improperly: “if the recipient’s Waterhouse client hasn’t updated in x days, assume the user uninstalled it and ignore his public key (send without encryption)”
Consistency and standards

• Unobtrusive extension to e-mail interface
• Doesn’t disturb any existing workflows – just makes things *better*
Help users recognize, diagnose, and recover from errors

• Can gracefully degrade even if removed improperly: “if the recipient’s Waterhouse client hasn’t updated in $x$ days, assume the user uninstalled it and ignore his public key (send without encryption)”

• If something fails (can’t reach Facebook), replace “extra protection” guarantee with a short message with a reasonable explanation

• If signature is missing or bogus, just don’t display the extra sender ID panel (in lieu of scary red error message, since experience shows the user won’t understand it and they can’t take corrective action anyway)

• (Possibility for error reporting to detect bugs in our client)
Error prevention

• Hard to make errors: can’t make (m)any choices
• Signing is *automatic* everywhere
• Address book and key list constantly refreshed
• Uses long-term credentials to access Facebook
• Graceful failure if recipient reads an encrypted message on non-Waterhouse client (“This secure message was sent using Waterhouse; please install...”)
Recognition above recall

• Only three things you can really do: send secure e-mail, uninstall, or change your Facebook account
• No menus
• No choices for security level: automatically sends with best security possible
• Minimal configuration options integrated with “Settings” UI for e-mail client
• Face recognition ⇔ security
  – (And it’s much quicker to recognize a face than to read a security statement and remember what it means)
Flexibility and efficiency of use

• It just works: automatically determines the best security options for your recipients
  – ALL outgoing messages are signed
  – No friendship: sign only
  – Encrypt iff the recipient has Waterhouse (public key in directory) and is a Facebook friend

• No accelerators needed; rides on existing composition UI
Aesthetic and minimalist design

• Incredibly simple design
  – “Why Johnny Can’t Encrypt” missed a key point: users shouldn’t *have* to use a dedicated security UI
  – Integrates into existing workflow
  – Looks just like existing e-mail client (e.g. Gmail)

• Secure by default
Help and documentation

• “Learn more” links for every Waterhouse message
• Help content will be written assuming that user doesn’t care about details
• Advanced technical details allow independent evaluation (important for tech-savvy early adopters)
Another benefit

“The societal benefit of building an infrastructure that protects well against passive attacks is that it makes it much harder to do undetected bulk monitoring of the population. It's a defense against police-states, not against policemen.”

John Gilmore, on the motivation for FreeS/WAN, his open-source IPsec implementation