



Toolkit: Security-by-Design 101

What is cyber security?

“Cyber” comes from “cybernetics”: systems built from interconnected systems, with feedback loops where outputs from actions taken are used as input for next steps.

Cyber security is where different kinds of expertise intersect, with the aim of creating online, offline and hybrid spaces that are safe and secure: an opportunity to learn from each other.

Security-by-design

Security = risk reduction! The idea is that we think about security as early as possible, to avoid cost later on (e.g., time, money, development effort and loss of reputation).

The whole point of security... is that security is not the point. Security is meant to let good work happen (making the sandbox a safe place to be) and offers a level of trust in what you have built.

Highlight potential risks

Take time to think about security in terms of:

People, Process, Technology

Who are your users/community; where does your hack fit; do you know of any existing weaknesses (e.g., SQL injections)?

A sociotechnical approach

Consider social, mental, situational, behavioral and physical factors.

Responsible innovation

Your hack's impact (ethical issues, consequences, disruption...)

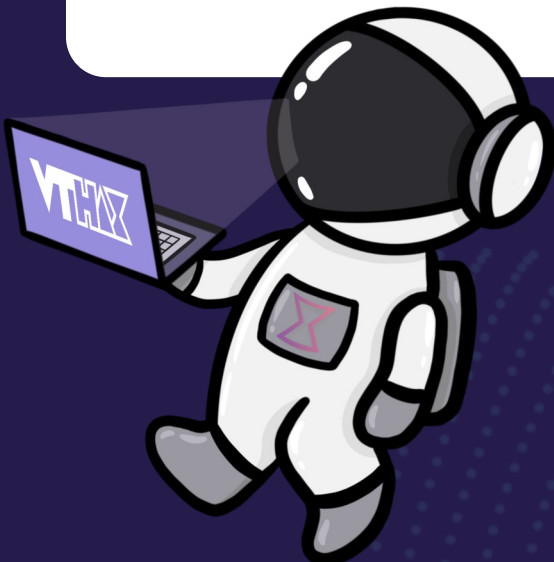
User testing

Invite other hackers over, to try out your hack.

This can be useful in seeing how people will interact with it.

Try to let them have a go before telling them how things work...

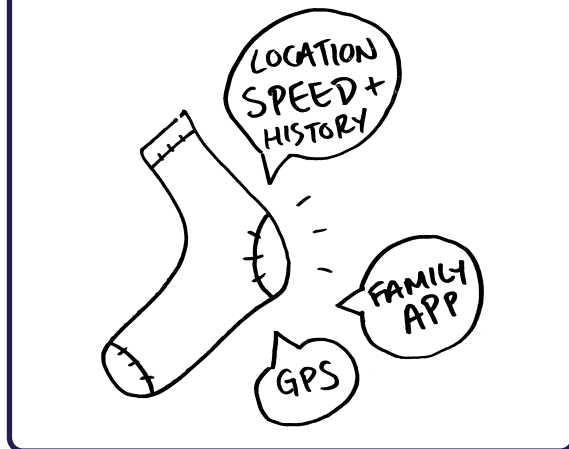
(unless they are about to do some damage!)



Contact: arianna@vt.edu | [@HackSecStudy](https://twitter.com/HackSecStudy)

Examples

Smart socks for Grandma



Security considerations

Grandma may forget to remove the sensors before washing the socks.

Grandma may not want to be tracked through her socks.

In the pitch...

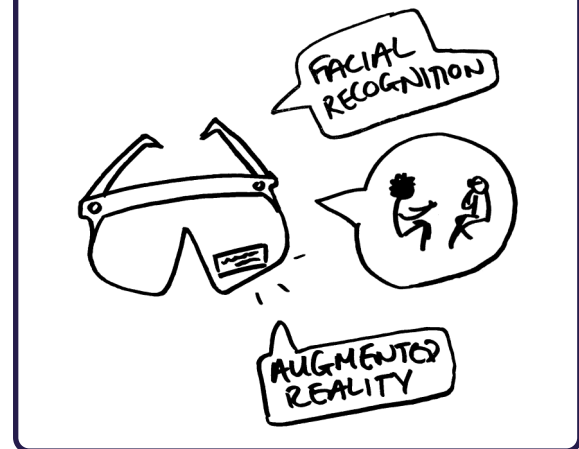
My Silver Surfer Grandma is an early technology adopter. She forgets where she is sometimes and calls us to come and get her, but she can be disoriented.

We present: 'smart socks' for Grandma.

We do not have access to Grandmas currently. Our next steps would be to consult with advocacy groups for elderly people, to understand whether Grandmas would want smart socks.

You can see that they definitely work!

Lip-reading in real-time



Security considerations

This is an augmented reality (AR) environment, which may cause users to experience motion sickness.

User privacy is at risk because AR tech sees what they are doing, who they are speaking to. We need to secure this.

In the pitch...

We need for solutions that transcribe conversations into words for those who are hard of hearing.

We present: 'lip-reading in real time'. It is a hardware/software hack. Our next step would be to build a robust AR platform.

We could offer training for people who want to learn to lipread...