Enabling a New Generation of Experts by Finding and Fixing Students' Persistent Misconceptions

NSF Award #1821788 SATC RUI EDU

Dr. Peter A. H. Peterson <pahp@d.umn.edu>

Asst. Professor, University of Minnesota Duluth

Online at: **https://lars.d.umn.edu/misconceptions**

UNIVERSITY OF MINNESOTA
Driven to Discover®

Significant exploits – affecting millions – fill the news, even though many result from issues well-known to security professionals. **Students have deeply ingrained misconceptions about how computer security ought to work, and students rely on this false intuition when reasoning about security.** The goal of this project is to:

1. **identify those misconceptions** through a survey of experts,

2. create and validate a **concept inventory** to evaluate students' understanding of these concepts,

3. produce **engaging videos** describing each misconception and correct concept, and

4. develop and test a series **of active learning exercises** to teach the correct concepts

---

Current Status:

- Survey of 87 security experts complete
- Asked about commonly observed misconceptions in 8 areas of security
- Coded 469 individual responses
- Found 17 most common misconceptions
- Developing multiple-choice concept inventory (to be validated)
- Creating easy to adopt, self-contained exercises and videos
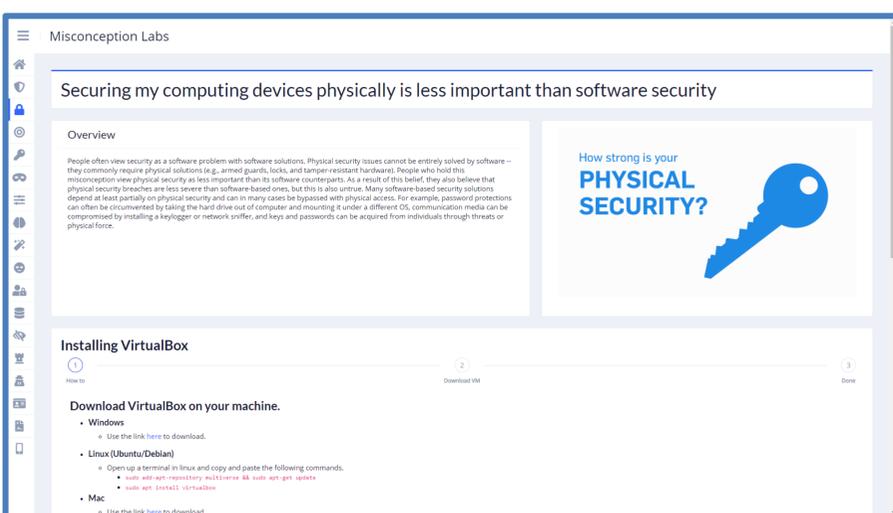
Screenshot of exercise delivery framework. All exercises will be open-source and available online, delivered via the web, including live access to virtual machines and other exercise materials.

Security Misconceptions

- Physical security isn't critical.
- Encryption is a "silver bullet".
- Developers designed with security in mind.
- I'm not a target.
- Security product X makes me secure.
- This works, so it's probably secure.
- "Security by obscurity" is good.
- Anonymized data can't leak information.
- Good password practices aren't important.
- Humans are rational and can't be tricked.
- "Least privilege" is unnecessary.
- Input is trustworthy.
- I have nothing to hide.
- You can be totally anonymous on the Internet.
- Two Factor Authentication isn't worth it.
- Defense in depth is unnecessary.
- Crypto = free authenticity and integrity.

Who will benefit?

- Citizens and nations benefit through improved security education
- Instructors benefit through easy-to-adopt materials
- Students benefit from improved understanding

Key Benefits

- List of misconceptions
- Concept inventory
- Engaging videos
- Hands-on exercises
- Project tools
- Improved security

Screenshot of video concept. Videos will be animated or otherwise engaging and freely available on YouTube.