Secure Design

1:30 – 4:30pm / CDM 228

Dr. Filipo Sharevski fsharevs@cdm.depaul.edu
Prof. Adam Trowbridge atrowbr1@cdm.depaul.edu

Course Description

Secure Design is a course that educates students in cybersecurity, information systems, interaction design, and graphic design in parallel, with a focus on Internet-of-Things architecture. The course extends usable security, while better integrating cybersecurity and design. Secure Design curriculum develops knowledge of cybersecurity principles, visual and user interaction design principles, as well as knowledge of cyber threats and vulnerabilities. The course includes hands-on, interactive activities that will allow students to practice the knowledge learned in cybersecurity and design courses; The course allows for the measurement of the knowledge gained by the students through the demonstration of acquired skills and abilities. **There are no pre-requisites**.

The main deliverables are a secure design prototype of an Internet-of-Things product, usability testing scenarios for the prototype, prototype presentation, and a peer critique of the usability and security of their peers' prototypes (students need to demonstrate they understand the principles of visual design, user interaction, and security). Each student is expected to participate actively in class.

Learning Outcomes

Upon completion of the course, students will be able to:

- Understand the cybersecurity principles of confidentiality, integrity, availability
- Understand the general system security mechanisms of identification & authentication, access control, and accountability
- Understand the design concepts of alignment, balance, order, contrast, proximity & similarity, rhythm, and whitespace
- Understand user-centered design principles: discoverability, affordance, signifiers, feedback, constraint

- Translate the cybersecurity, visual design, and user-centered design principles in the IoT environment
- Recognize the vulnerabilities in the structure, user interaction, and visual design that make Internet of Things (IoT)-related exploits possible
- Identify usability issues in IoT devices and systems using Jakob Nielsen's 10 Usability Heuristics for User Interface Design
- Analyze the security flaws of a given IoT workflow (application logic), including those introduced by the technology and those that could be introduced by an end user
- Use usability testing to validate secure design decisions and reveal flaws in IoT interface designs
- Design a secure IoT workflow (application logic) that eliminates security design flaws

Materials

No textbook is required. All tools, IoT devices, and readings will be provided by us.

Grading

Assessment Mechanism	**Points**
Test	25%
Student reflection writing	15%
Heuristic evaluation worksheet	5%
Lab report	35%
Peer critique	15%
Presentation	5%
Total:	**100%**

Course Schedule

W	Module Name	Description
1	Users: the weakest link in cybersecurity	This module focuses on the cybersecurity chain, the users as one of the most discussed links, and how the basic idea of secure design helps strengthen the user link.
2	Visual Design & Principles of User Interface Layout	Module A: This is a basic introduction to visual design, concepts of alignment, balance, order, contrast, proximity & similarity, rhythm, and whitespace.
		Module B: This is a basic introduction to the visual design, concepts of alignment, proximity, similarity, alignment and consistency, and extends their use to the basics of user interface layout.
3	Introduction to User Experience Design	This is an introduction to interface design, including interface design principles and usability heuristics.
4	Cybersecurity Basics	This module focuses on the main principles in cybersecurity: confidentiality, integrity, and availability.
5	Cybersecurity and Internet-of-Things (IoT)	This module focuses on the Internet-of-Things and the aspects of IoT cybersecurity, privacy and safety.
6	Experimenting with A Smart IOT Home	This module is focused on experimenting with a smart IoT home. Students (or groups of students) are given elements of a basic smart home package including: wireless router (TP Link), smart phone (Moto G5 Plus), voice assistant (Google Home), and smart lights (Philips Hue).
7	Outsmarting the Smart Home	This module is focused on experimenting with the cybersecurity of a smart IoT home. Students follow the Lockheed-Martin Cybersecurity Kill Chain steps to try to exploit the smart IoT home they have built in the previous module.
8	Prototyping	A prototype is an early sample, model, or release of a product built to test a concept or process or to act as a thing to be replicated or learned from.

9	Prototypes - Usability Testing	Usability testing is a technique to evaluate a product by testing it with representative users. In this module, students will learn basic approaches to usability testing by testing their prototype for a new Hue Bridge.
10	Secure Design Analysis	This module consists entirely of the Secure Design Analysis Lab. Students conduct a peer assessment of the presentations in class. This lab serves as an active review of the material from the previous modules.