

# ECE750: Usable Security and Privacy

## Introduction

Dr. Kami Vania,  
Electrical and Computer Engineering  
[kami.vania@uwaterloo.ca](mailto:kami.vania@uwaterloo.ca)




# First, something random...

- First 5 minutes we talk about something interesting, often from recent events
- You will not be tested on the 5 minutes part of lecture
- This part of lecture will sometimes not be recorded
- Why do this?
  1. Some students show up late
  2. Reward students who show up on time
  3. Important to see real world examples

Security

## Who cracked El Chapo's encrypted chats and brought down the Mexican drug kingpin? Er, his IT manager

Feds flipped techie and recorded hundreds of calls

By Kieren McCarthy in San Francisco 9 Jan 2019 at 21:33 71  SHARE ▼



In an extraordinary twist, it was revealed on Tuesday that the man most likely responsible for bringing drug kingpin "El Chapo" Joaquin Guzman to justice was none other than his sysadmin.

But the drug trafficker isn't happy, complaining about having to get the computer himself, and about the long password needed to get into a different machine: A situation that every sysadmin on the globe will recognize. Except with one big difference - your boss is unlikely to track you down and kill you if you upset him.

"You didn't send me the engineer to install my machine. So, then, it's all your fault," Jorge Cifuentes complained. "No!" responded to Rodriguez.

"It's all your fault."

"No, Don Jorge, don't stress me out more, man, because..."

"Don't complain that I... what can I do? I haven't been able to do it."

"Hadn't we agreed that you were going to buy a mini computer and you were going to call us to configure it?"

"I'm so busy. I didn't even have time to breathe... I have a computer but, you know that I haven't been able to open it? A Vaio... Do you remember the small Vaio?"

"Yes, sir."

"Good, but that has a very long password."

"Yes, sir."

"The long one, that password that you place...is this the password?"

"Yes, sir."

"What a drag! It has symbols and things."

**INSTRUCTOR: KAMI VANIEA**

# Instructor

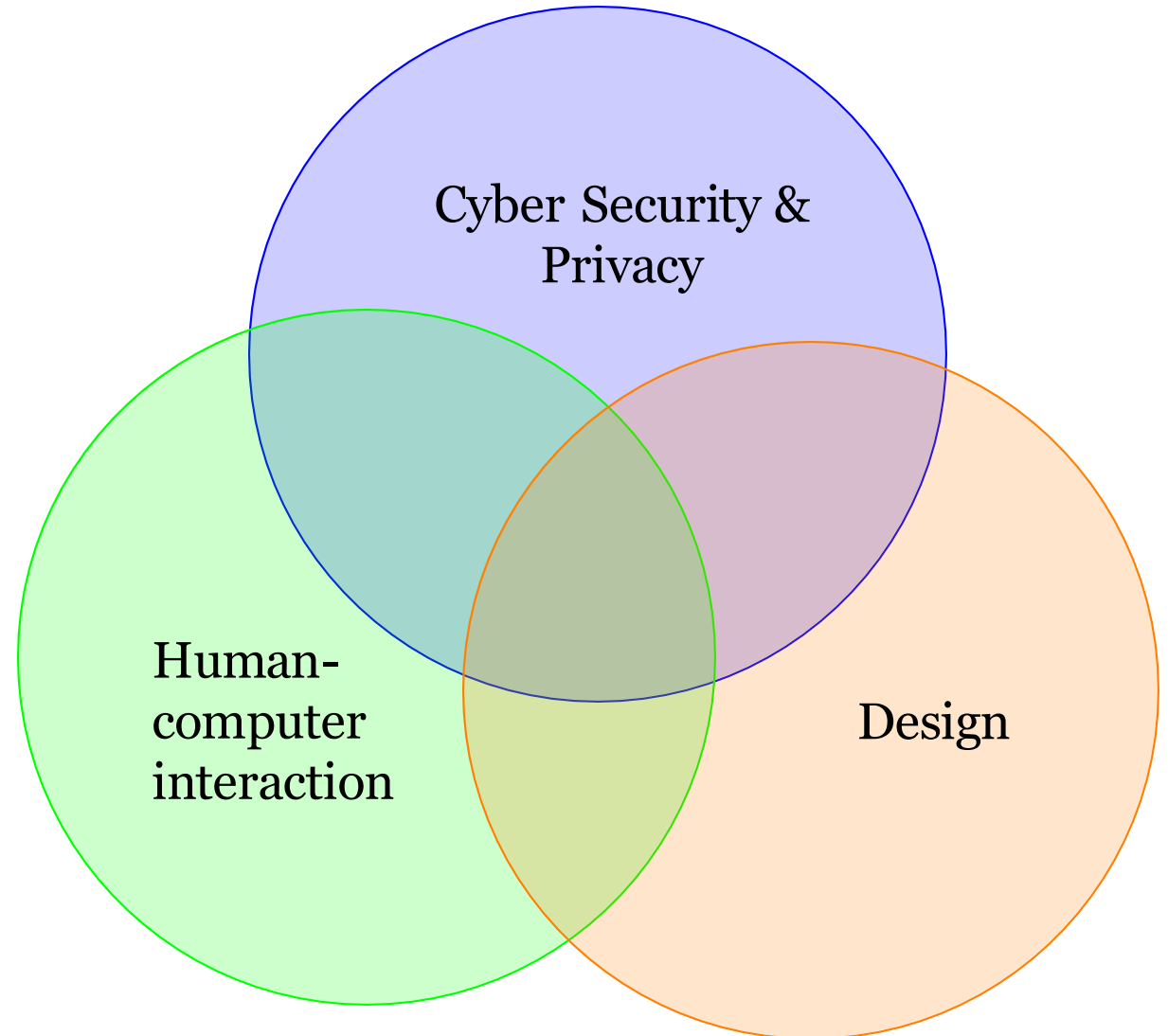


**Dr Kami Vaniea**

University of Waterloo

vaniea.com

kami.vaniea@uwaterloo.ca



# **Pronouncing my last name:**

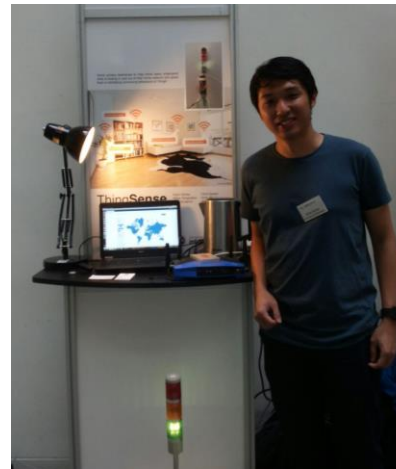
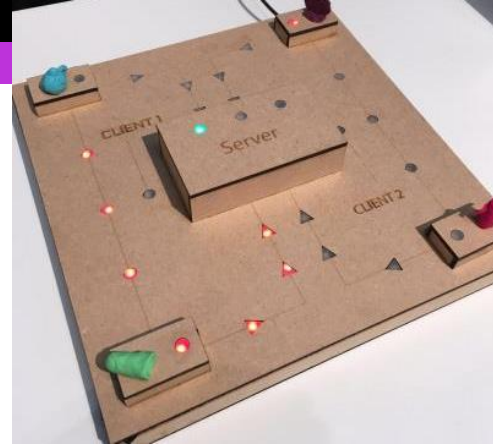
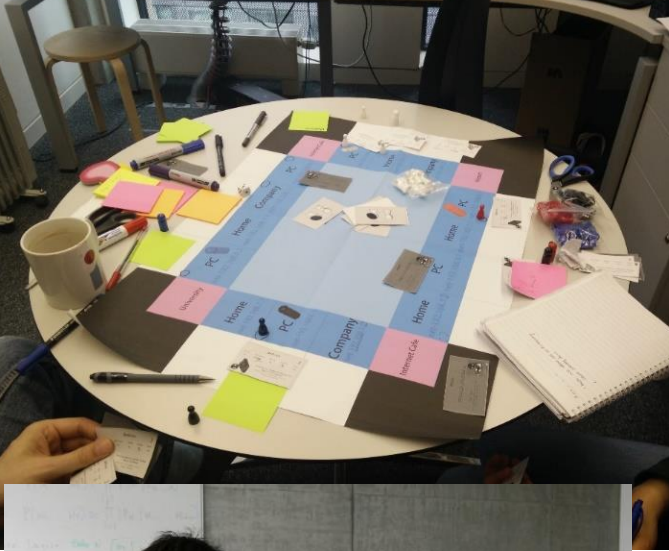
Actual: **Vaniea**

English: **Van-yay**

French: **Vanier**

Americans cannot spell French names ... especially in the colonial time period.





# tulipslab.org

- Phishing
- System administration patch management
- Developer-centered privacy
- Experimentation in VR
- Bystander privacy for smart speakers
- Serious games
- IoT
- Behavior tracking on websites

# COURSE STRUCTURE



# Advanced research course for HCI and Computer Security

## Human Computer Interaction

- Creating and testing theories
- Study design
- Interpreting and applying results
- Anticipating and avoiding human error

## Computer Security

- Human-factors issues in security
- Applied aspects – theory meets practice
- Adversarial thinking
- Authentication
- Phishing
- Threats

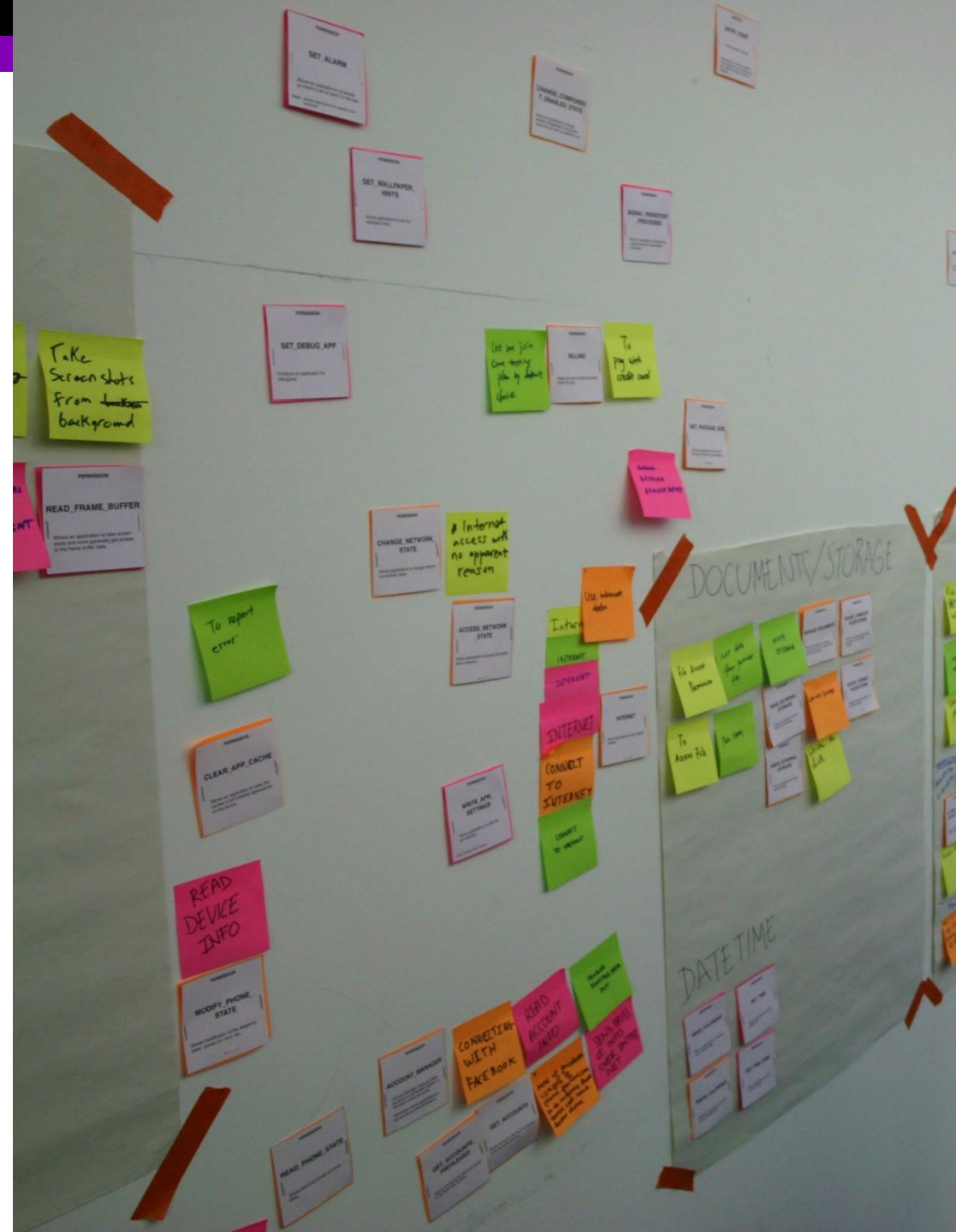
# Course structure

- Each lecture:
  - 5 minutes on a current trending topic
  - Lecture on the topic
  - Mix of lecture and discussion
- Readings:
  - Required readings need to be read before class
  - Additional resources are there for further learning



# In-class activities

- Some HCI concepts are hard to understand unless you do them
- We will be doing a small number of activities to learn about how this type of research is done



# Schedule

- **Lecture:** Monday, Tuesdays
- **Final:** Not yet scheduled

## Schedule exceptions

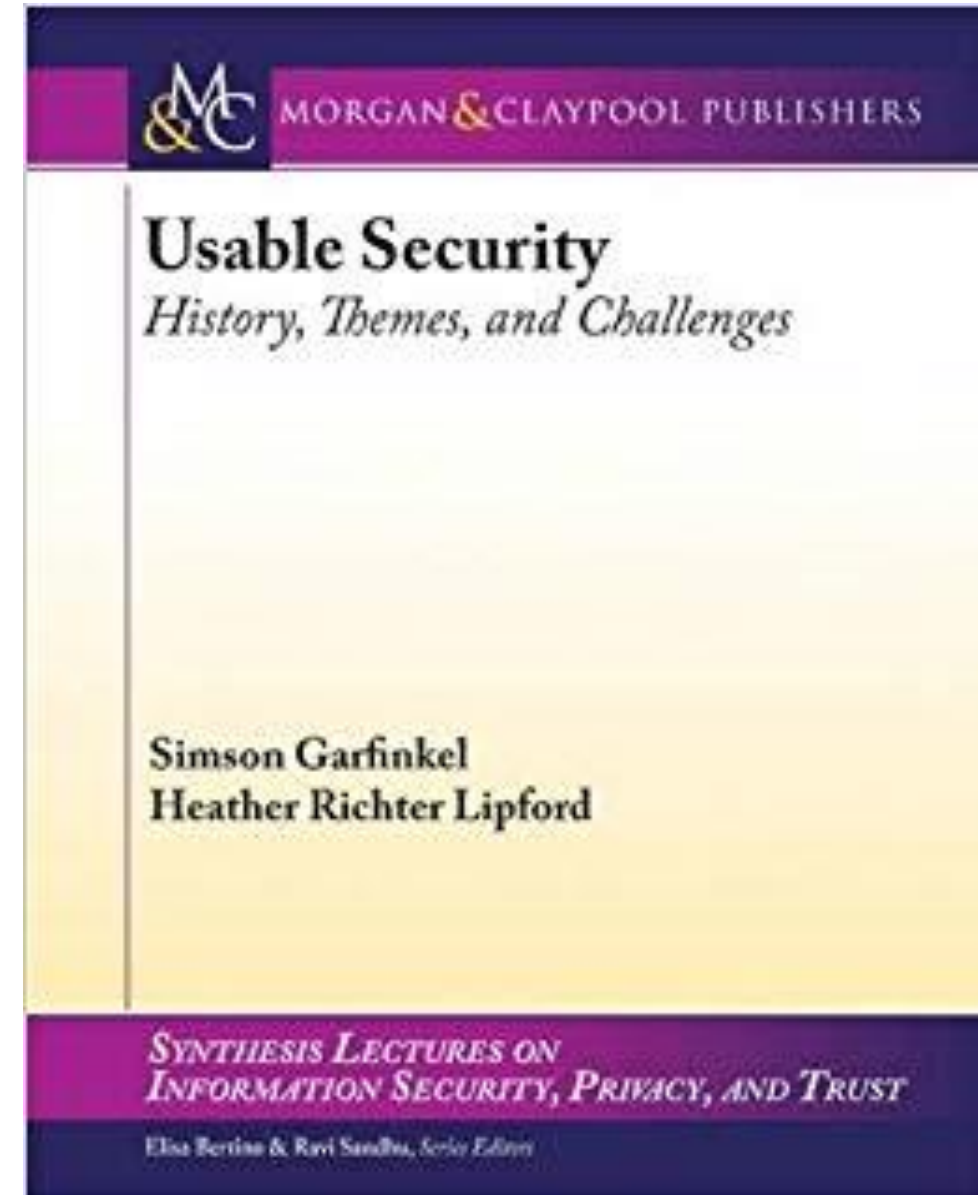
- 20 May – no class, holiday
- 9/10 June – lecturer out of town, trying to arrange guest speaker
- 2 July – Wednesday makeup course

# Assessment

- 20% - 2 homework assignments
- 10 % - Reading reflection
- 20% - Project
- 50% - Final exam, closed book
- 0% - Activities

# Good/Interesting news sources

- **Brian Krebs** – Investigative journalist who focuses on security. His blog is sometimes cited in legal proceedings.
  - <https://krebsonsecurity.com/>
- **Kashmir Hill** – Journalist that focuses on security and privacy issues often with a privacy and public policy focus.
  - <https://www.forbes.com/sites/kashmirhill/#42fbf157b415>
- **Bruce Schneier** – Blog on security running since 1998. Harvard Fellow, consultant, and board member at EFF. Very interested in social factors of security.
  - <https://www.schneier.com/>
- **Troy Hunt** – Author of HaveIBeenPwned.com, interesting views on data breaches and how to handle failure well.
  - <https://twitter.com/troyhunt>





# Late policy

- 10% lost per day up till 10 days late, weekend days count.
  - For example: An assignment due on Monday that is submitted on Wednesday has the mark of:  
 $\text{marks} * 0.8$

# Academic dishonestly

- See the official policy of the University and on Outline
- Please don't cheat, copy other students, or turn in work that is not your own
- Assignments will have clearly marked areas where you can collaborate
  - Some HCI methods require more than one person

# Standard security course advisory

- Nothing here is intended as an incitement to hack, crack, or otherwise break into computer systems!
- Breaking into systems to “demonstrate” security problems at best causes a headache to overworked sysadmins, and at worst compromises systems for many users and could lead to **prosecution**.
- If you spot a security hole in a running system, **don't exploit it**, instead consider contacting the relevant administrators confidentially.

# Responsible security experiments

- **If you want to experiment** with security holes, play with your own machine, or better, your own private network of machines.
- **Use VMs:** use virtualization: e.g., VMWare, VirtualBox, KVT/Xen/UML. The SEEDLab VMs are good for safe experimentation.
- **If you accidentally break into something:** tell me, ECE computing services, or University computing services right away. Universities are places of learning, and we respond very differently if you tell us than if we catch you.

**Any questions about the course setup?**