

Week 12 - Friday

**COMP 4290**

# Last time

---

- What did we talk about last time?
- Privacy

# Questions?

# Project 3

# Assignment 4

**Abiral Pokharel Presents**

# Exam 2 Post Mortem

# Privacy in Emerging Technologies

# RFID tags

- **Radio frequency identification (RFID) tags** are usually small, inexpensive transmitters
  - They can be attached to almost anything
  - They can be as small as a grain of sand
- Some are passive and need an external signal to power their response
- Others have their own power supplies (and greater ranges)
- Their transmission range varies from a few centimeters to several meters
- They are currently used for:
  - Toll plaza payments
  - Some subway passes
  - Stock and inventory labels in warehouses
  - Passports and identity cards
  - Some credit cards with wave-style payment

# RFID issues

- RFID tags are being put in everything
  - A tag in your shirt could identify where you bought it and maybe even some unique identifier that could be tied to you in a database
  - This tag could be scanned as you walk down the street
- Some people with rare medical conditions have an RFID implanted in their bodies
- When I first taught this class, the infrastructure did not currently exist to track everyone's movements and activities
- As the price goes down for RFID tags and their readers, widespread tracking becomes a greater likelihood

# Apple AirTags

- Apple AirTags were first released in 2021
- You put them on and in things you worry about losing
- They use a combination of short-range radio wave technologies like Bluetooth Low Energy, allowing Apple devices to track nearby ones
- They are, essentially, RFIDs tracked by a global, crowd-sourced network
- But toss one into someone's backpack or car and you suddenly have a way to stalk them
- eBay and Etsy buyers have found AirTags with the warning speaker removed in items they have purchased
- Security blogger [Bruce Schneier](#) had a [post](#) about how they're being used to track secret government offices



Image from:  
[https://commons.wikimedia.org/wiki/File:Airtag\\_-\\_3.jpg](https://commons.wikimedia.org/wiki/File:Airtag_-_3.jpg)  
By user KKPCW  
Creative Commons Attribution-Share Alike 4.0  
International license

# Electronic voting

- Many polling places throughout the US (and many other countries) use computers to tally votes
- Voting systems should:
  - Keep a voter's choices secret
  - Allow a voter to vote only once
  - Be tamperproof
  - Report votes accurately
  - Be available through the election period
  - Keep an audit trail to detect irregularities but still not say how an individual voted

# Voting is a mess

- It's hard to engineer a system that you can guarantee only lets someone vote once and yet not keep track of how they voted
- The software and hardware design for these systems are generally not publicized
- Nine companies are currently registered with the U.S. government to make voting systems
- Internet voting will probably increase
  - Some US and UK elections have used it
  - Estonia has the largest Internet voting system, which relies on a national ID card that can be verified from home using an inexpensive card reader

# VoIP

- **Voice over IP (VoIP)** is a way to make phone calls over the Internet
  - Many phone companies actually use VoIP transparent to their users
- The pandemic saw an increase in VoIP and other forms of Internet video communication
- VoIP is attractive because long distance costs are essentially zero if you already have high speed Internet
- Issues:
  - ISPs and others can track who you're having phone calls with, even if the audio is encrypted
  - Skype uses 256-bit AES (but it's hard to verify whether Microsoft can eavesdrop or not)
  - Zoom, Google Hangouts, Microsoft Teams, and Cisco Webex don't use end-to-end encryption, allowing the companies to eavesdrop
  - WhatsApp claims to use end-to-end encryption

# Upcoming

# Next time...

---

- Security planning
- Disasters
- Lockpicking
- Jennifer Perez presents

# Reminders

---

- Work on Project 3
  - Phase 1 due next Friday
- Keep reading Chapter 10