

# A(nother) case for research on secure robot apps

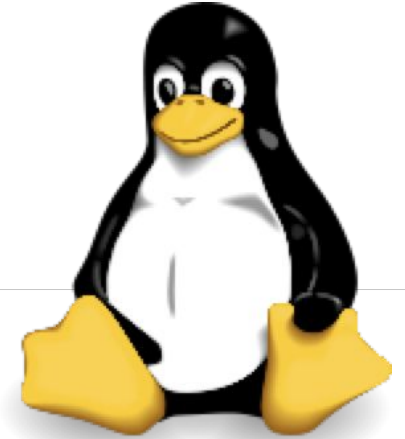
Sam King

Back in 2011, Murph Finnicum presented a case for secure robot applications, but not much research has happened since then!





# Robots are similar to traditional systems



# Robots are different

- They move!
  - Robots are inherently probabilistic
-

# Example: Labrador app

Act like a dog: fetch a tennis ball, bark enthusiastically








Woof!






```
def play_fetch():  
    while Ball.is_near(User):  
        wait(Ball)  
  
    ball_location = locate_object(Ball)  
    move_to(ball_location)  
    pick_up_object(Ball)  
    move_to(User.get_location)  
  
    drop_object(Ball)  
    play_sound("woof.mp3")
```



# Permissions for robot apps?

Permission	Use	Allow
Movement	Chase ball	
Manipulation	Pick up ball	
Camera	See the ball	
Speakers	Bark	
Internet		

# Permissions fail to capture the subtleties of robots

Permission	Use	Allow
Movement	Chase ball	
Manipulation	Pick up ball	
Camera	See the ball	
Speakers	Bark	
Internet		

# Recent developments make robots more practical

---

Self driving DARPA cars brought us SLAM, deal with uncertainty well



XBOX kinect brought us cheap range sensors



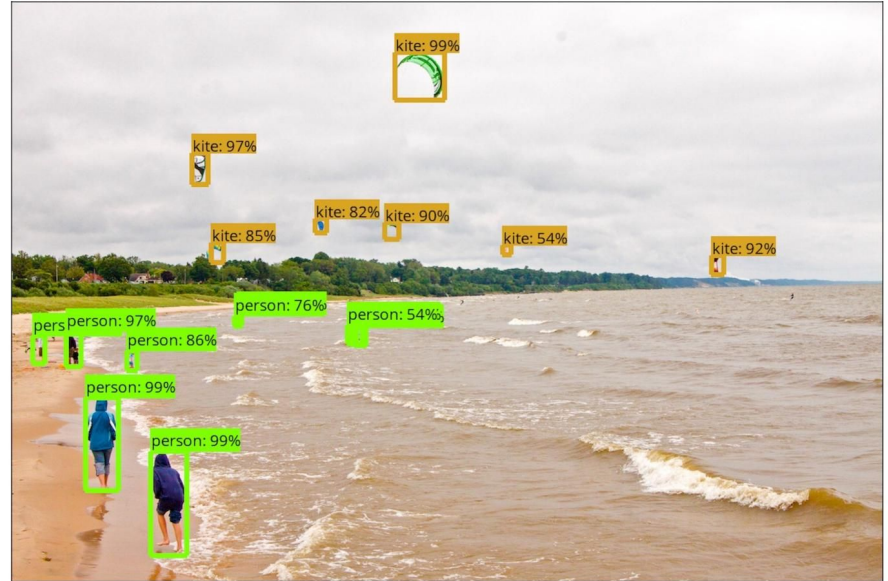
```
def play_fetch():  
    while Ball.is_near(User):  
        wait(Ball)  
  
    ball_location = locate_object(Ball)  
    move_to(ball_location)  
    pick_up_object(Ball)  
    move_to(User.get_location)  
  
    drop_object(Ball)  
    play_sound("woof.mp3")
```

```
def play_fetch():  
    while Ball.is_near(User):  
        wait(Ball)  
  
    ball_location = locate_object(Ball)  
    move_to(ball_location)  
    pick_up_object(Ball)  
    move_to(User.get_location)  
  
    drop_object(Ball)  
    play_sound("woof.mp3")
```

Still very difficult circa 2010

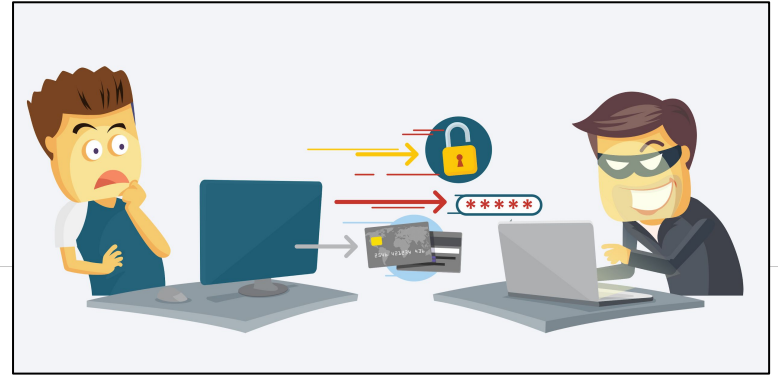
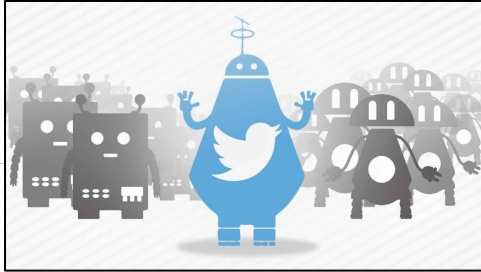


# GPU + object recognition CNN operate at higher level of abstraction





We're used to probabilistic authentication, see my next talk for more context ;)



[Home](#) / [Security](#)

**UPDATE**

## Lyft customers face potential hack from recycled phone numbers

The problem involves Lyft's use of cell phone numbers to verify customers' identities.

# Conclusion

Let's design notions of security from the start with robot apps

---

# Discussion

Are there other recent advances (self driving cars) that can help provide insight into robot app security?

---

What are the main abstractions that you'd operate on, from a security perspective?

How to evaluate security for robot apps?

# Graveyard

---



[Home](#) > [News](#) > [Animals in Research and Teaching at UC Davis](#)

## Animals in Research and Teaching at UC Davis

By Andy Fell on July 11, 2017 in Human & Animal Health



**T**he use of animal models in biomedical research benefits human health and is strictly regulated. Breakthroughs in treatments for illnesses such as Alzheimer's, heart disease, cancer, and HIV/AIDS would not have been possible without studies using animal models of disease.

Good scientific research requires strict adherence to the ethical and humane

### Quick Summary

- > **Animal research benefits human health and is strictly regulated**
- > **We provide the best possible care to animals in our charge**
- > **UC Davis' animal care program is internationally recognized and accredited**

### Related Stories



**Scientists Discover New Ebola virus in Bats in Sierra Leone**  
July 27, 2018



**How Experience Changes Basics of Memory Formation**  
July 23, 2018



**Rhesus Macaque Model Offers Route to Study Zika Brain Pathology**  
June 20, 2018

### Top Stories

**Chancellor Gary S. May Shapes Future in His First Year**  
August 3, 2018

**UC Davis Joins Network for International**













# Robot apps are coming

