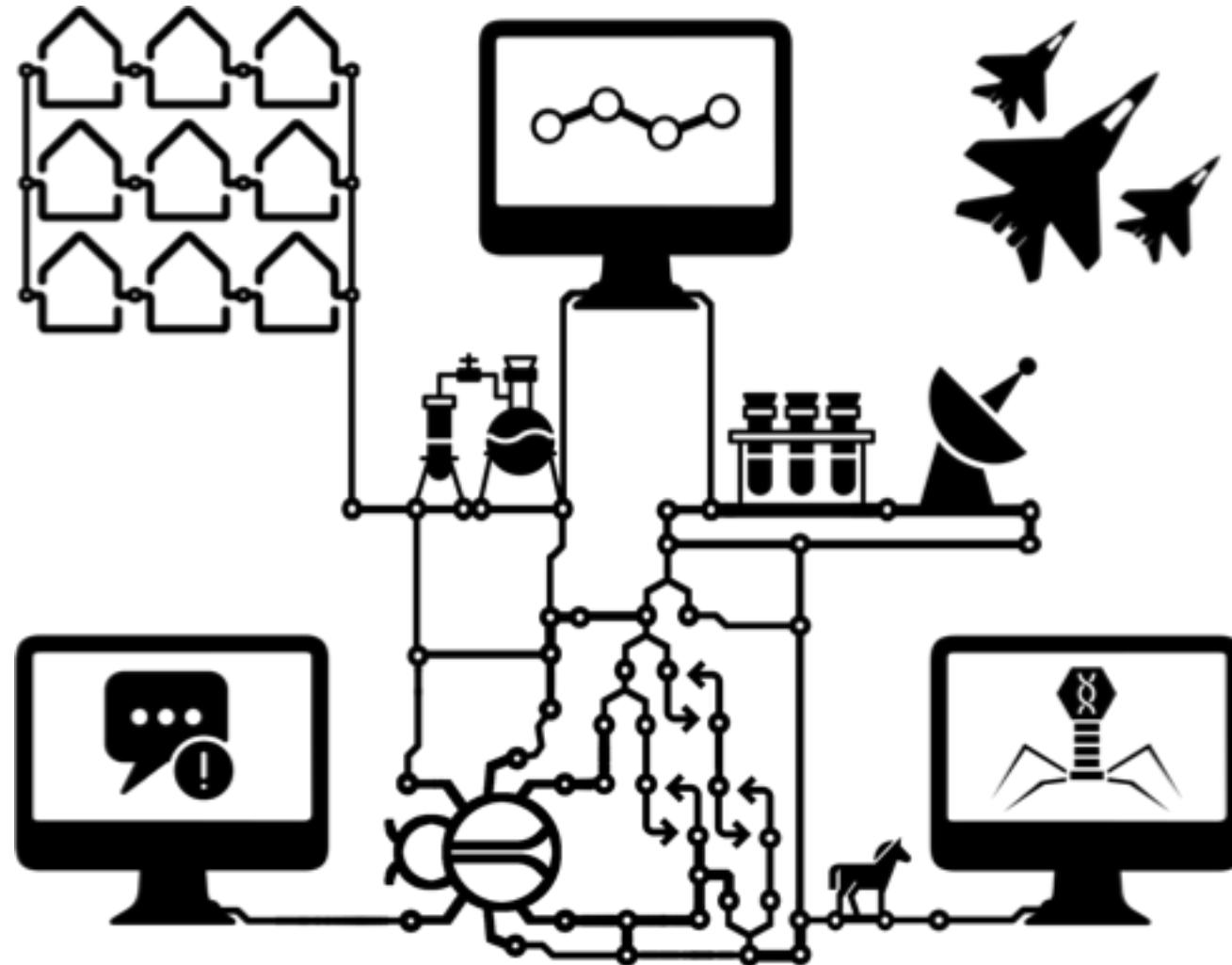


# Program Analysis for Cybersecurity



[ben-holland.com](http://ben-holland.com)

# \$ whoami

- Ben Holland
- B.S. in Computer Engineering (2005-2010)
  - Internships: Wabtec Railway Electronics, Ames Lab, Rockwell Collins
- B.S. in Computer Science (2010 – 2011)
- M.S. in Computer Engineering and Information Assurance (2010 – 2012)
  - Internships: MITRE
- Iowa State University Research (2012 – 2015)
  - DARPA Automated Program Analysis for Cybersecurity (APAC) Program
- Ph.D. in Computer Engineering (2015-2018)
  - DARPA Space/Time Analysis for Cybersecurity (STAC) Program
- Apogee Research (2019+)

Let's break the ice...



# What's a Hacker?

## Part 2 of 3: Thinking Like a Hacker



**3 Learn to recognize and fight authority.** The enemy of the hacker is boredom, drudgery, and authoritarian figures who use censorship and secrecy to strangle the freedom of information. Monotonous work keeps the hacker from hacking.

- Embracing hacking as a way of life is to reject so-called "normal" concepts of work and property, choosing instead to fight for equality and common knowledge.

A little melodramatic...  
Who draws all these anyway?

[Web](#) [News](#) [Images](#) [Videos](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 2,200,000 results (0.30 seconds)

## hack·er

/'haker/

*noun*

1. a person who uses computers to gain unauthorized access to data.  
*synonyms:* cybercriminal, pirate, computer criminal, keylogger, keystroke logger;  
[More](#)
2. a person or thing that hacks or cuts roughly.



Translations, word origin, and more definitions

### [Hacker - Definition and More from the Free Merriam ...](#)

[www.merriam-webster.com/dictionary/hacker](#) ▾ Merriam-Webster ▾

3 : an expert at programming and solving problems with a computer. 4 : a person who illegally gains access to and sometimes tampers with information in a computer system. See [hacker](#) defined for English-language learners.

### [Urban Dictionary: hacker](#)

[www.urbandictionary.com/define.php?term=hacker](#) ▾ Urban Dictionary ▾

A person skilled with the use of computers that uses his talents to gain knowledge. There are three classifications of [hackers](#): White-hat ([hacking](#) f...

### [What is hacker? - Definition from WhatIs.com - SearchSecurity](#)

[searchsecurity.techtarget.com/definition/hacker](#) ▾

Hacker is a term used by some to mean "a clever programmer" and by others, especially those in popular media, to mean "someone who tries to break into computer systems."

### [Hacker | Define Hacker at Dictionary.com](#)

[dictionary.reference.com/browse/hacker](#) ▾ Dictionary.com ▾

Slang. a person who engages in an activity without talent or skill: weekend [hackers](#) on the golf course. 3. Computer Slang. a person who has a high level of skill ...

Ok the media definition of hacker wins...  
Hackers are criminals by popular definition.

# Let's define hacking (in non-media terms)

- Problem solving
- Critical thinking
- Tinkering
- Exploring how things work

# Learning Objectives

By the end of this course you should be able to:

- Think like a hacker
- Demonstrate basic bug hunting, exploitation, evasion, and post-exploitation skills
- Describe commonalities between vulnerability analysis and malware detection
- Describe fundamental limits in program analysis
- Challenge conventional viewpoints of security
- Confidently approach large third party software
- Critically evaluate software security products
- Locate additional relevant resources
- ASK “HOW DOES THIS WORK”?
- THINK CRITICALLY!

# Digression

- Let's get our minds thinking like a hacker...
- 3 quick examples

# Hacking: Tamper Evident Devices

- Detect unauthorized access
- Not a “lock”
- Also known as “seals”
- How is the seal inspected?

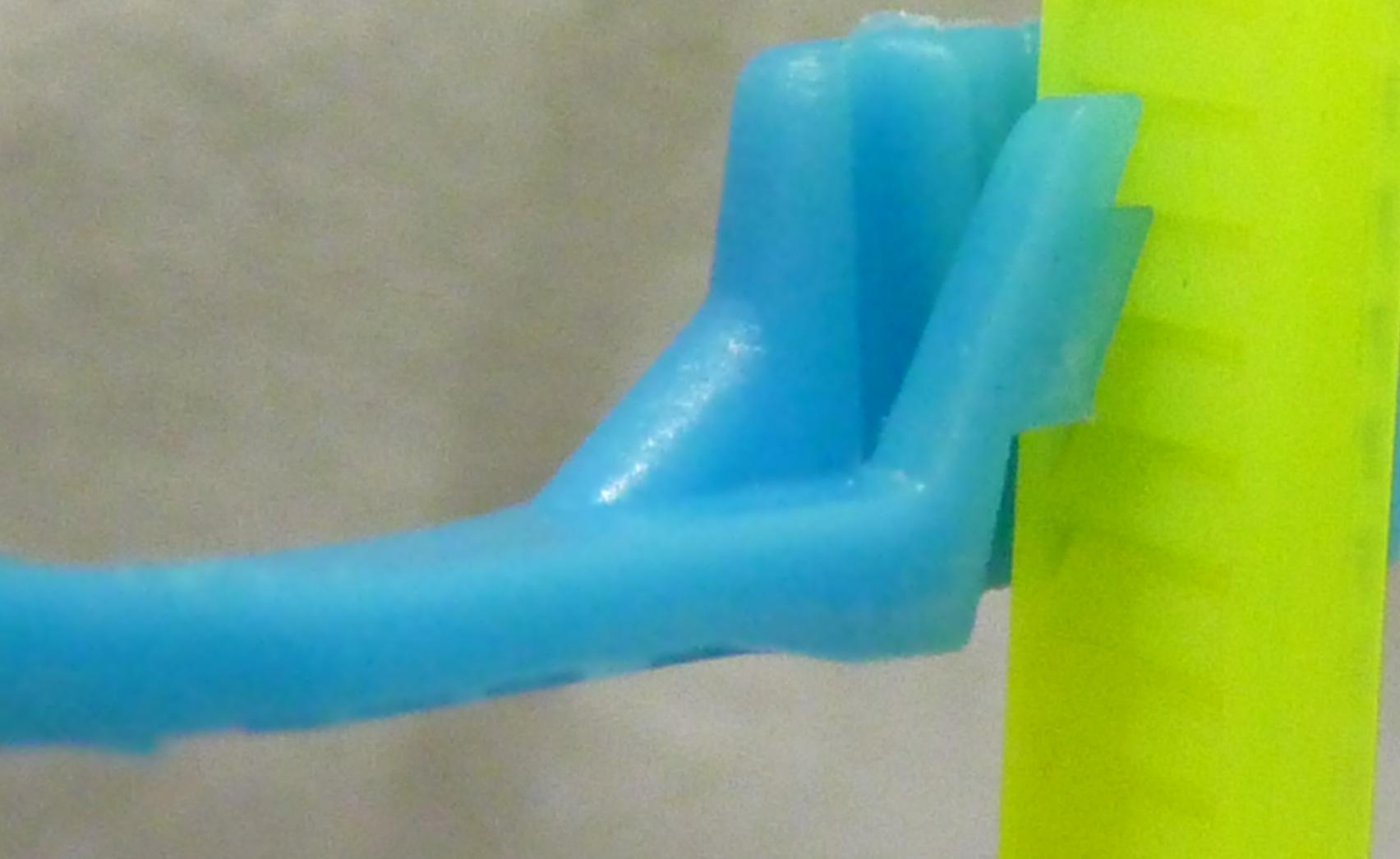




# Defeating Tamper Evident Seals

- Important Question: How does it work?
- Works similar to a zip tie

# Cutaway of a Zip Tie



# Defeating a Zip Tie

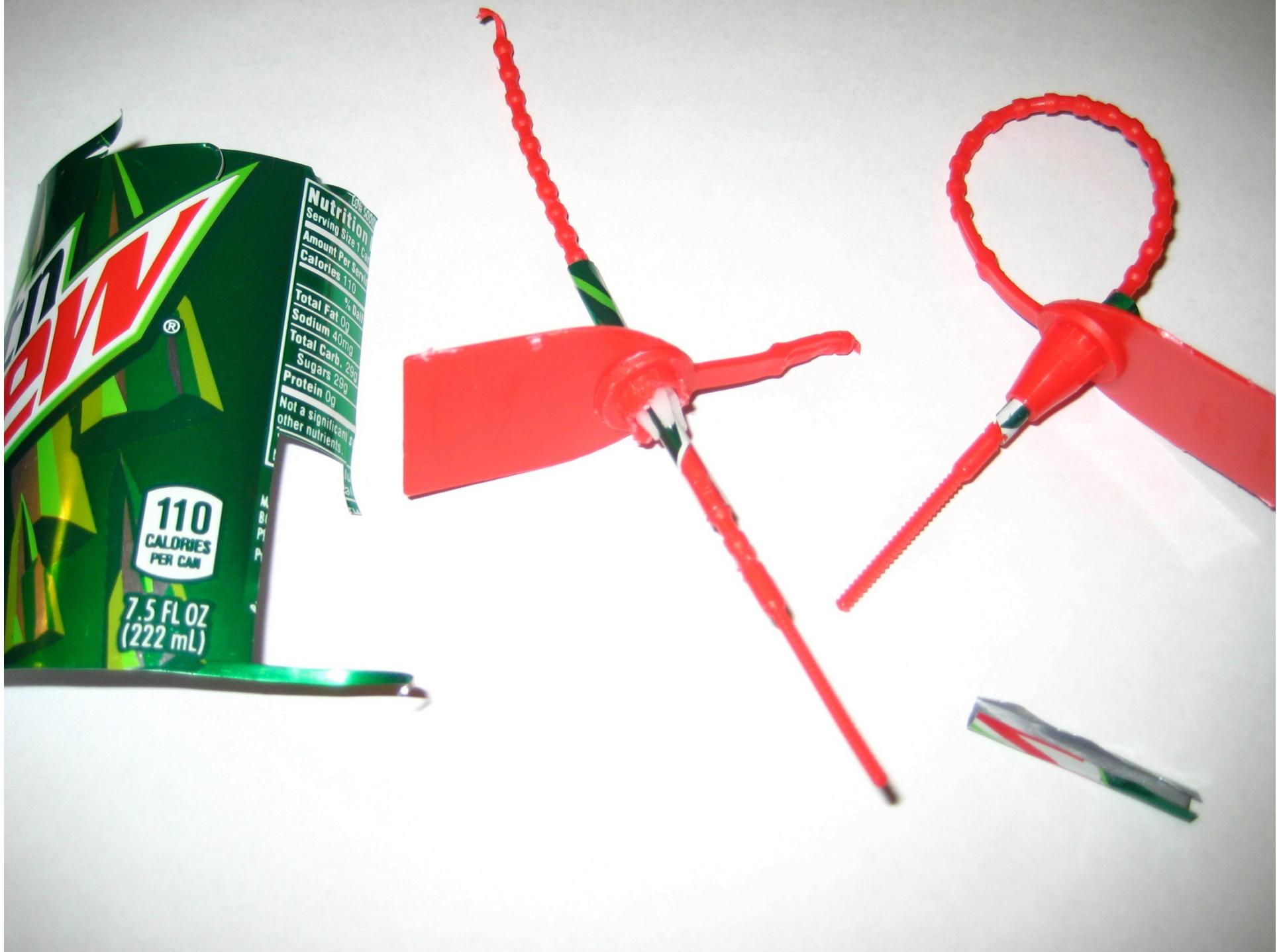


A close-up photograph of a red plastic seal, likely made of a flexible polymer like polyvinyl chloride (PVC). The seal has a central circular opening with a translucent or clear center. A red zip tie is wrapped twice around the handle of the seal. The seal is set against a plain white background.

**How do we  
defeat this seal?**

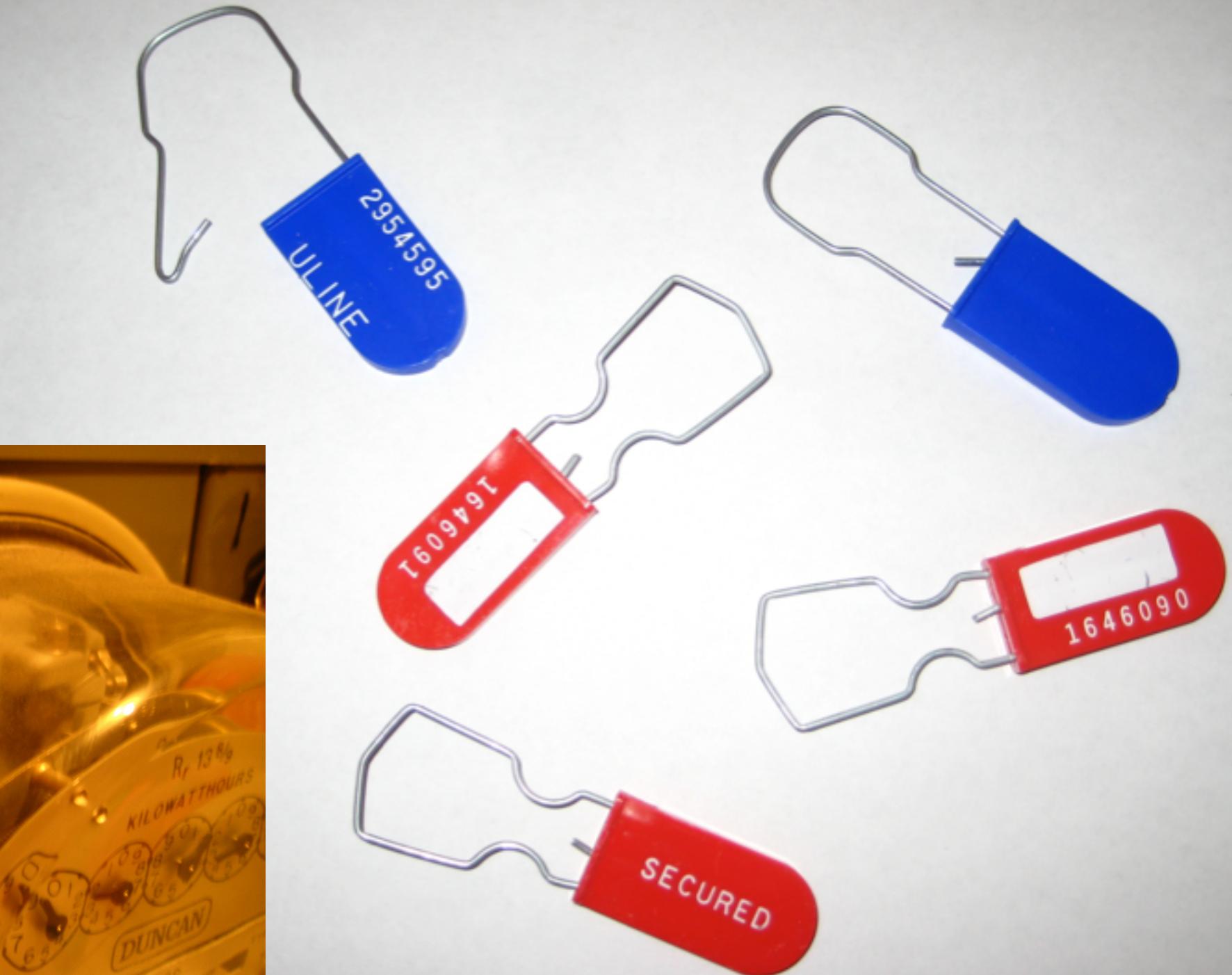
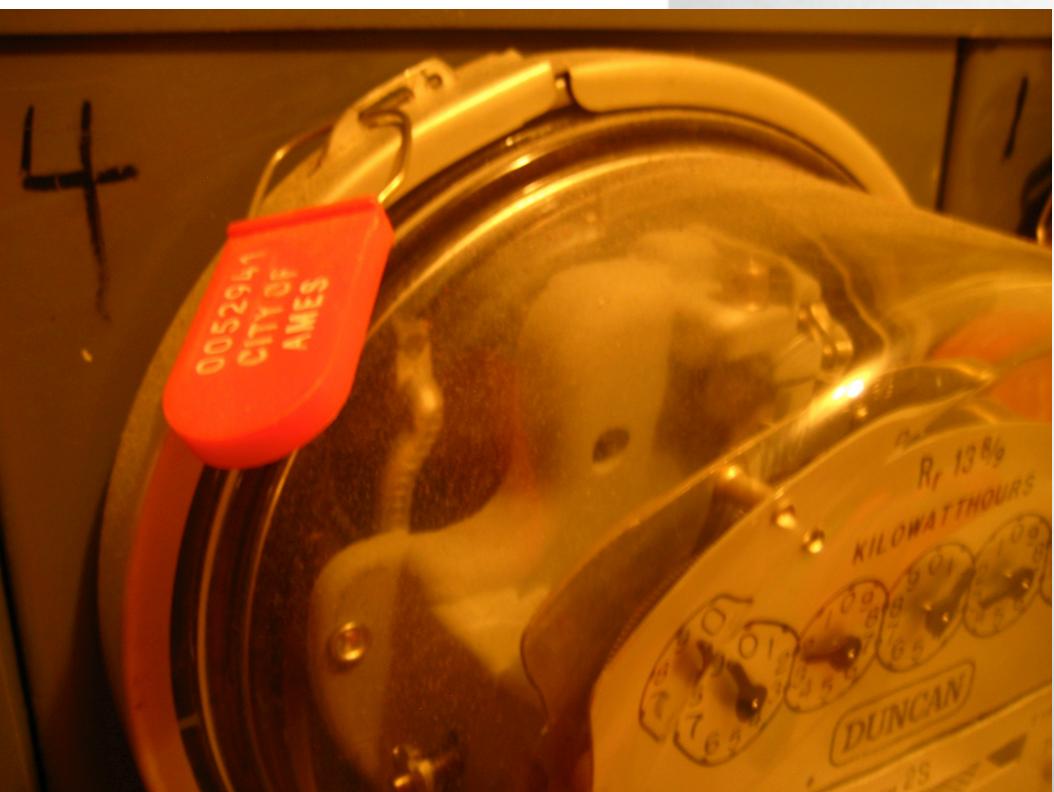
**Shimming with  
a pop can...**





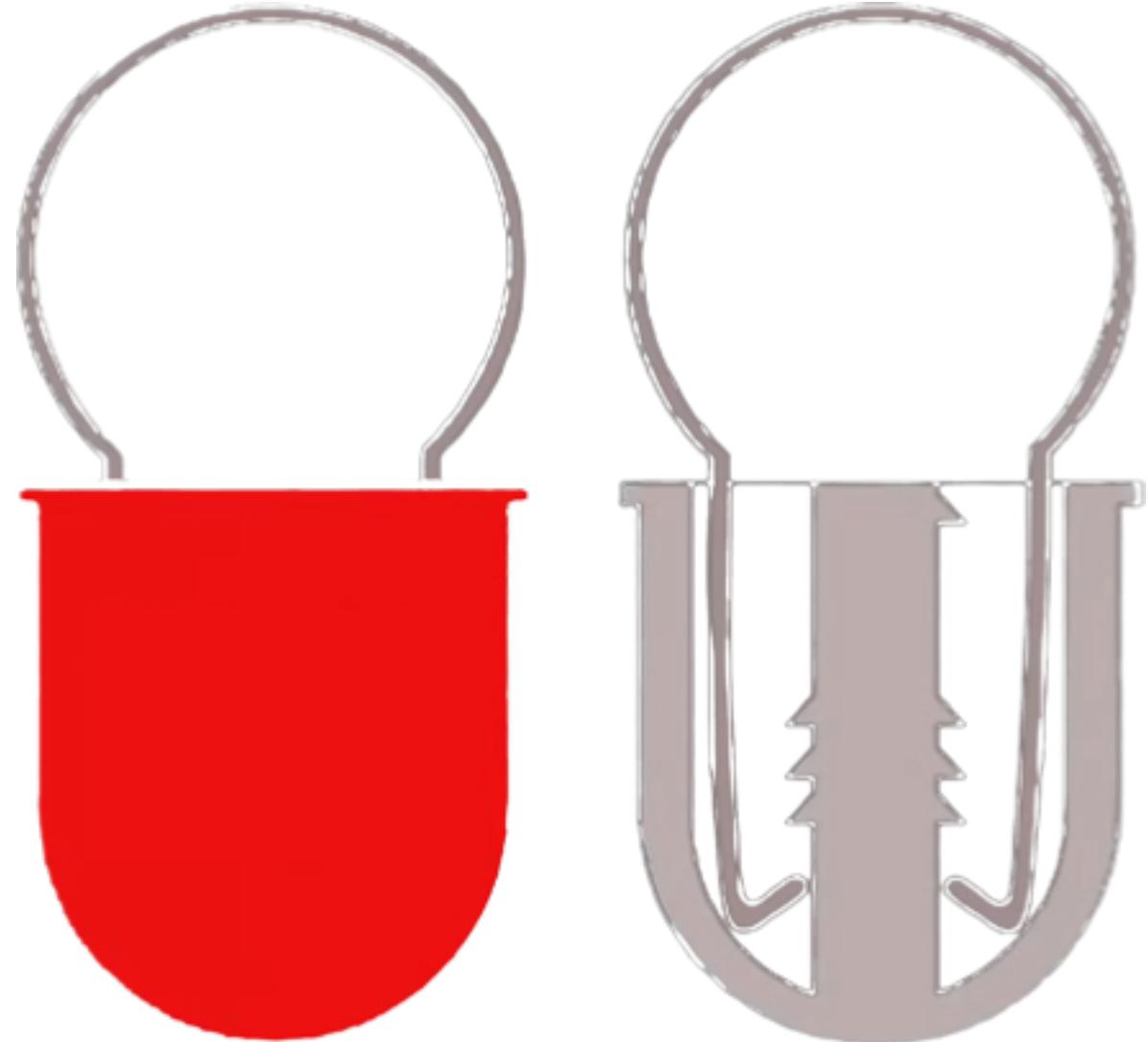
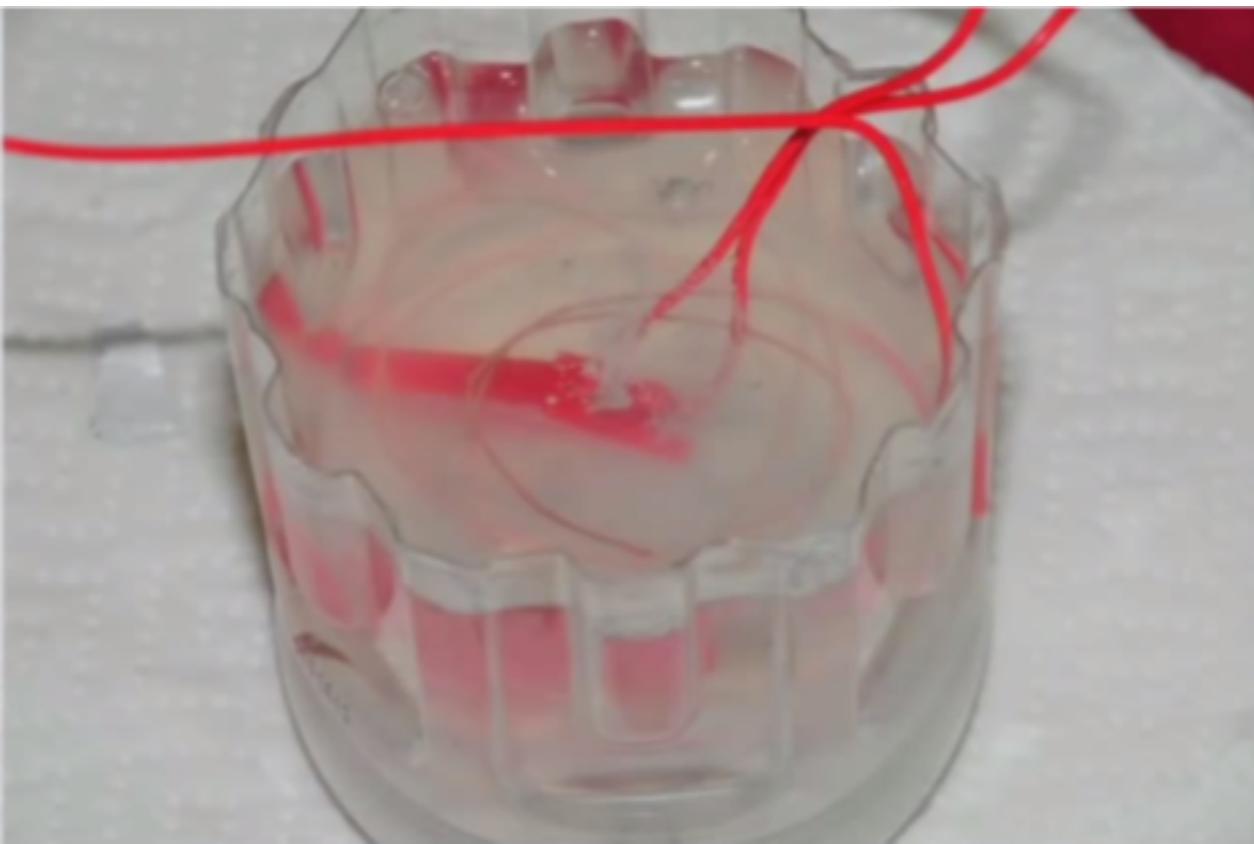
Nutrition  
Serving Size 1 Can  
Amount Per Serving  
Calories 110  
Total Fat 0g  
% Daily  
Sodium 40mg  
Total Carb. 29g  
Sugars 29g  
Protein 0g  
Not a significant source of  
other nutrients.

# How do we defeat this seal?

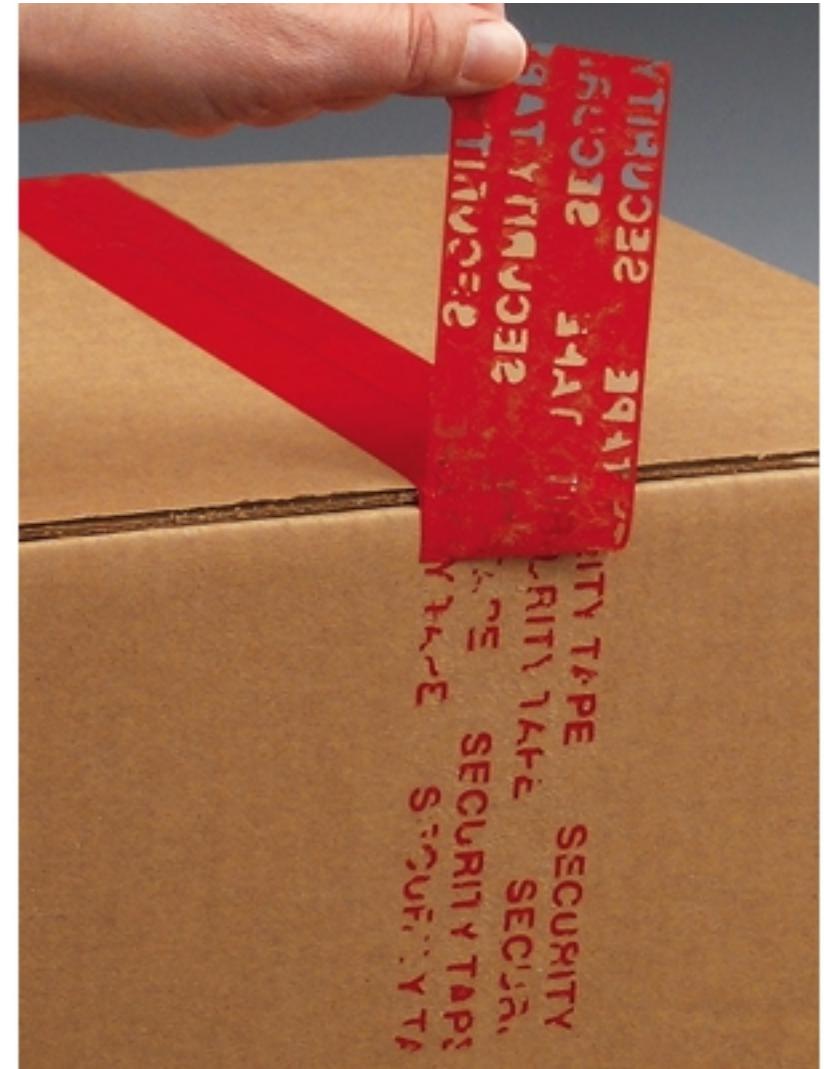


# Defeating Tamper Evident Seals

- How does it work?



# Tamper Evident Adhesives







# Defeating Adhesive Seals

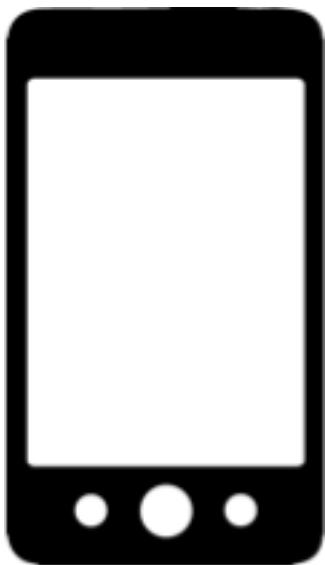
- Dry Peeling/Breaking/Lifting
- Water/Steaming
- Heating/Cooling
- Counterfeiting (replace)
- Solvents
  - Acetone (nail polish remover)
  - Isopropyl Alcohol
  - Mineral Spirits
  - “Stamp lift” Fluid

# Hacking: Voicemail

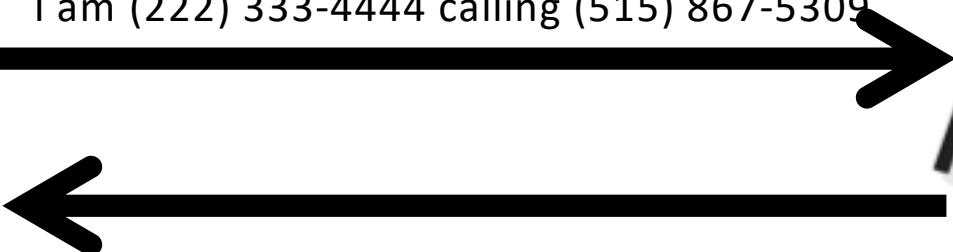
- What question(s) should we ask?

# How does voicemail work?

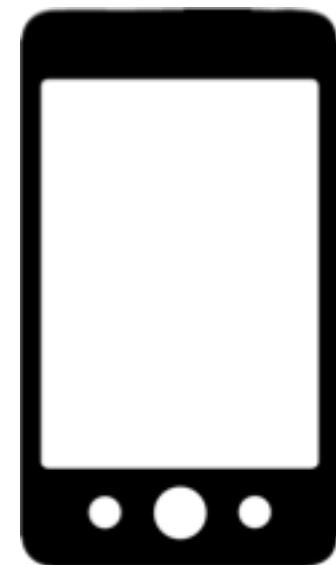
(222) 333-4444



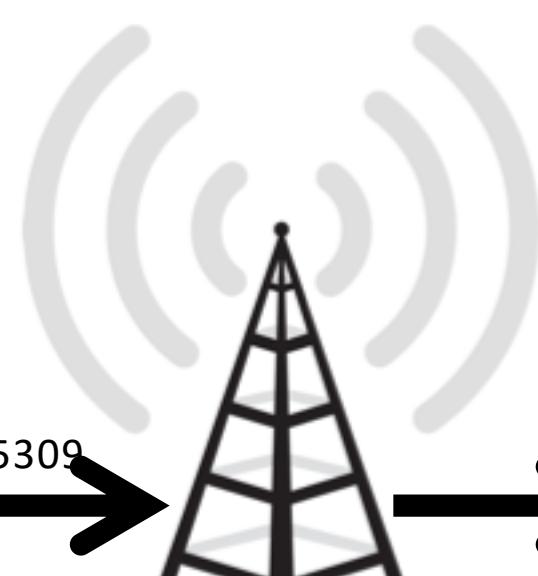
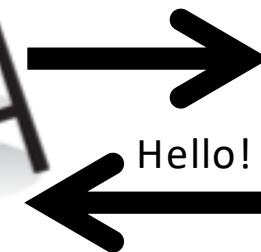
I am (222) 333-4444 calling (515) 867-5309



(515) 867-5309

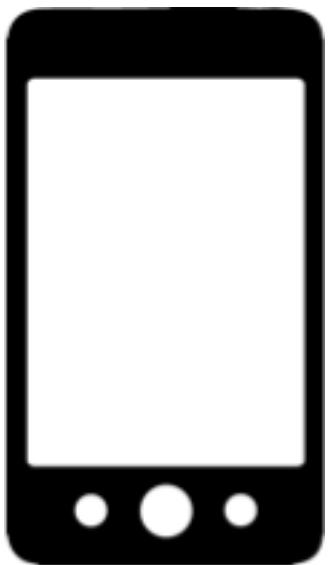


Hello!

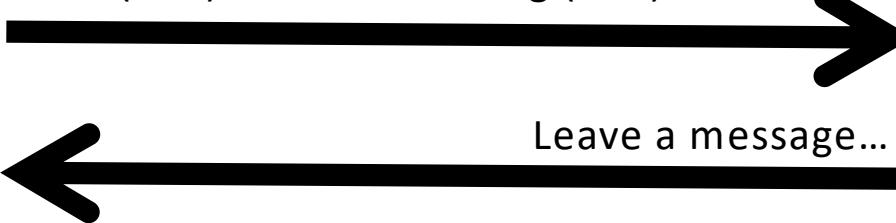


# How does voicemail work?

(222) 333-4444



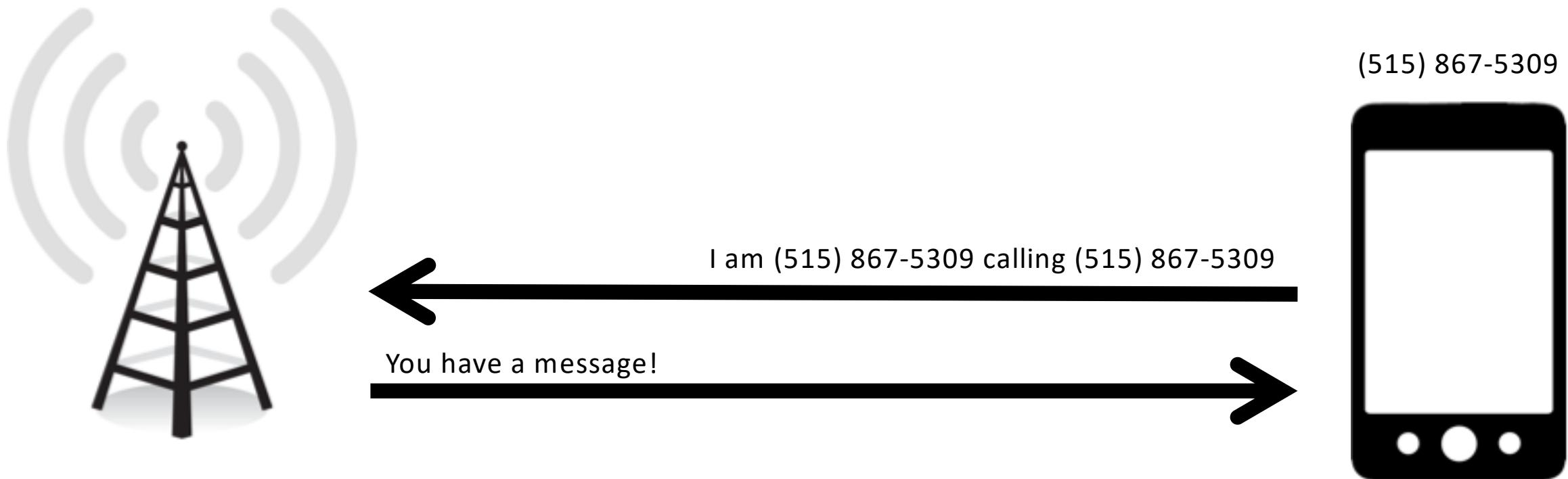
I am (222) 333-4444 calling (515) 867-5309



(515) 867-5309

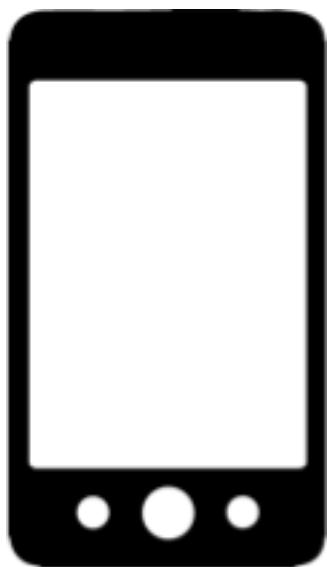


# How does voicemail work?

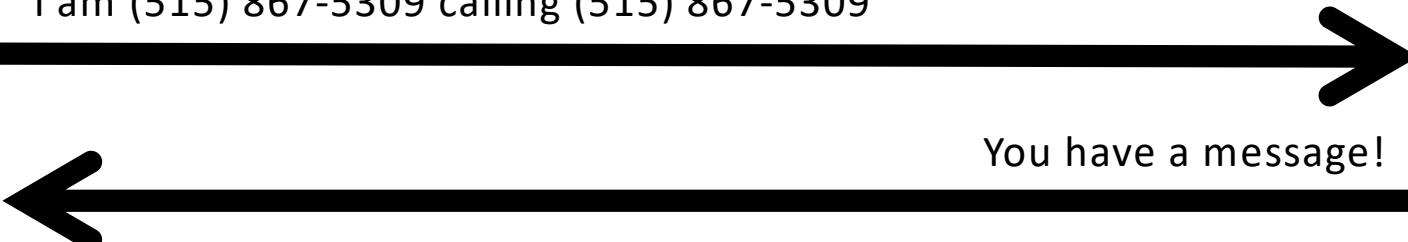


# How does voicemail work?

(222) 333-4444



I am (515) 867-5309 calling (515) 867-5309



You have a message!



# Voicemail Hacking Demo

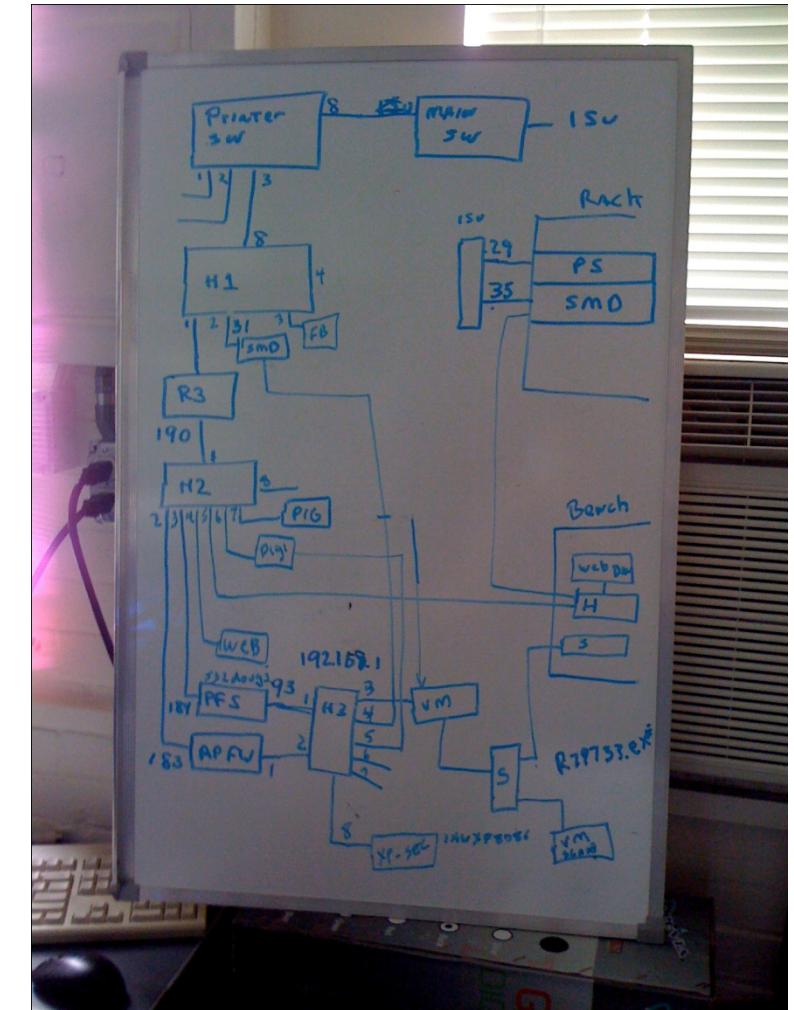
- Fake Victim: (515) 200-1301 ([github.com/benjholla/VoicemailVictim](https://github.com/benjholla/VoicemailVictim))
- SpoofCard Service: (305) 501-2777
  - Press 1 (login with your phone number)
  - SpoofCard User: (319) 435-0116
  - SpoofCard PIN: 1234
  - Press 1 (place a call)
  - Press 1 (use your normal voice)
  - Press 2 (don't record call)
- Caller ID spoofing is legal in the United States if it is not done with “the intent to defraud, cause harm, or wrongfully obtain anything of value”.

# Information Warfare Course (ISU CprE 532)

- Professor gave me the IP addresses of his computers to hack for the course project
- Computer have “flags”
  - Text files whose contents that prove you gained access
- What did I do?
  - Remember that hackers try to be lazy.

# Information Warfare Course (ISU CprE 532)

- Physical Break-in Story



# Ethical Concerns

- Disclaimer: The content in this course was created for educational purposes only.
- Consider the consequences of your actions. *Remember that every action may have unforeseeable consequences.*



A graphic featuring a stylized spider web background. Overlaid on the web are the words of the Spider-Man quote in a bold, sans-serif font. The text reads:  
**WITH  
GREAT POWER  
COMES GREAT  
RESPONSIBILITY**  
- SPIDER-MAN

# Daily Overview

- Day 1: Binary Exploitation
- Day 2: Web Application Security
- Day 3: Fundamentals of Program Analysis
  - Bug Hunting and Malware Analysis
- Day 4: Threat Modeling and Real Time Awareness
  - Bugs Vs. Malware, A/V Evasion, Log Analysis, Future Directions
- Day 5: Team Competition!
  - Attack and Defend Vulnerable Video Service (like YouTube)

# General Plan

- Focus on getting hands on experience!
- If labs are completed early we can explore more advanced topics
- I will adapt materials to you
- Form teams on Tuesday
  - Balance teams based on experience
  - Study buddies before competition
  - Teammates during competition
  - May develop specialized roles
  - Start preparing as a team for competition

# Competition Environment

- Every team gets one AWS web server instance
- Every team attacks and defends at the same time!
- Every teammate gets a local copy of the code
  - Analysis and attack tools already installed
- Open ended competition
  - Mix of easy, difficult, and unsolved problems
  - Write reports to earn points
  - Teams can start to work on competition early
  - Have fun! Share some memes ☺

# Ice Breaker Exercise: EIL5 “Programming”

- Explain It Like I'm Five (EIL5): How do computer programs work?
- Can your explanation intuitively address:
  - Complexity of software
  - Programming bugs
  - Security issues

