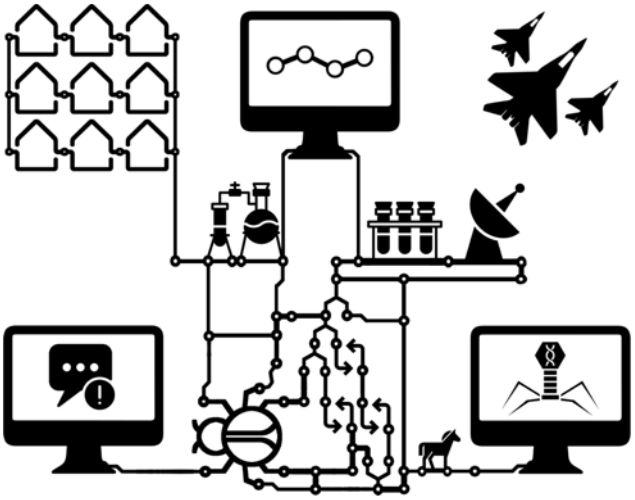
Program Analysis for Cybersecurity



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?

wikiHow Search

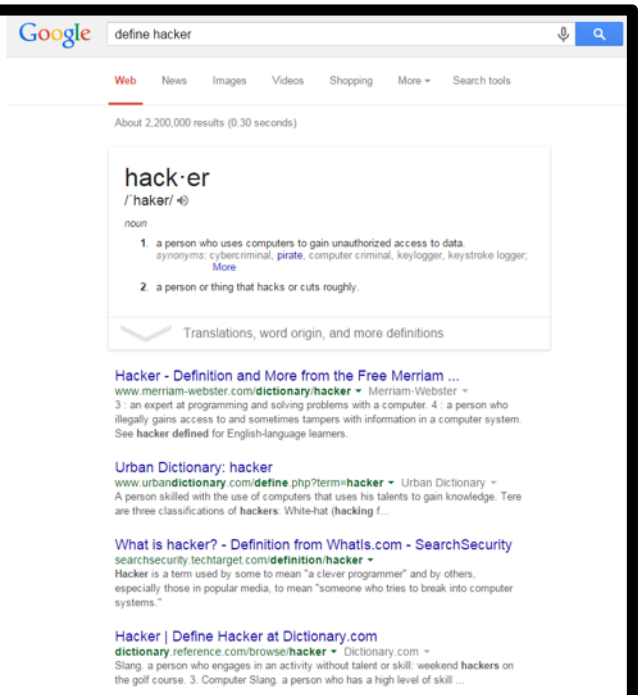
Part 2 of 3: Thinking Like a Hacker

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?

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!

This course sets ambitious learning goals that span both defensive and offensive techniques. Each topic is connected by a common theme of program analysis, which we use to cover topics in vulnerability analysis, malware detection, exploit development, antivirus evasion, and post-exploitation topics. Of course, there is no way that you can become an expert in all of these areas in one day (or even a week). Instead what this course aims to do is give you the tools to confidently approach intractable problems in security. It is my hope that by the end of the course, you feel prepared to seek out additional knowledge on your own that brings you closer to success in your own personal interests and goals.

Digression

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

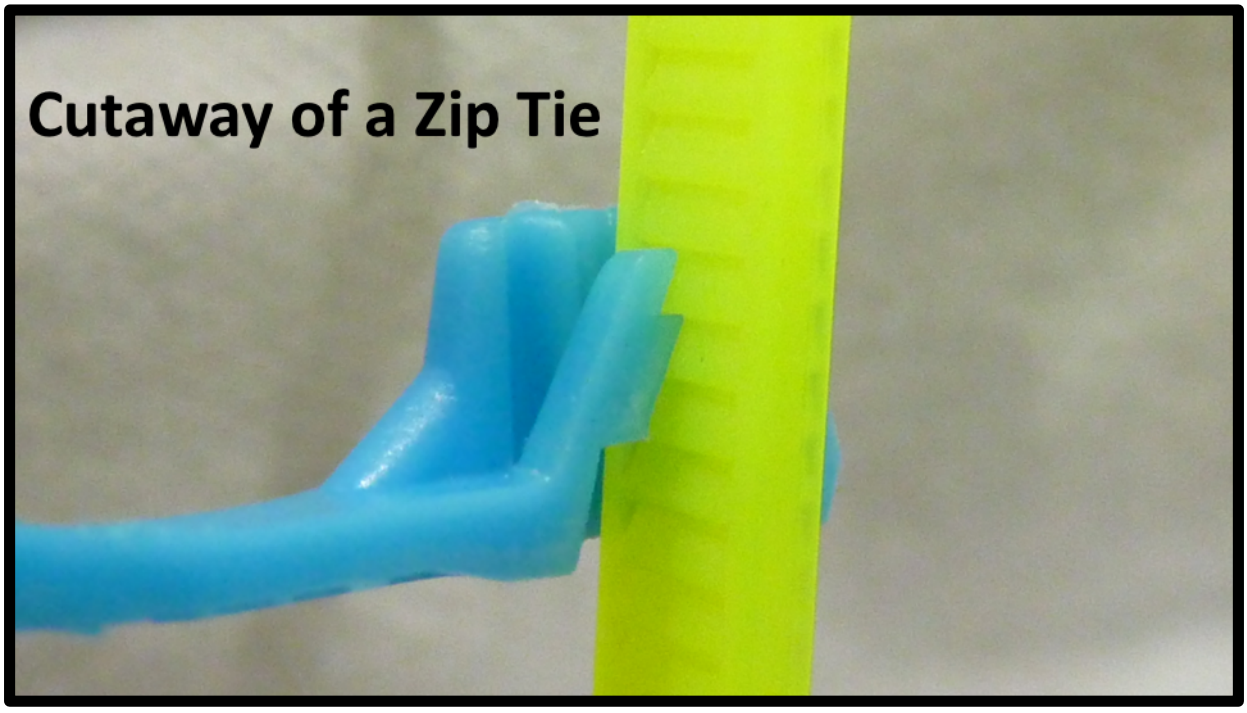
Hacking: Tamper Evident Devices

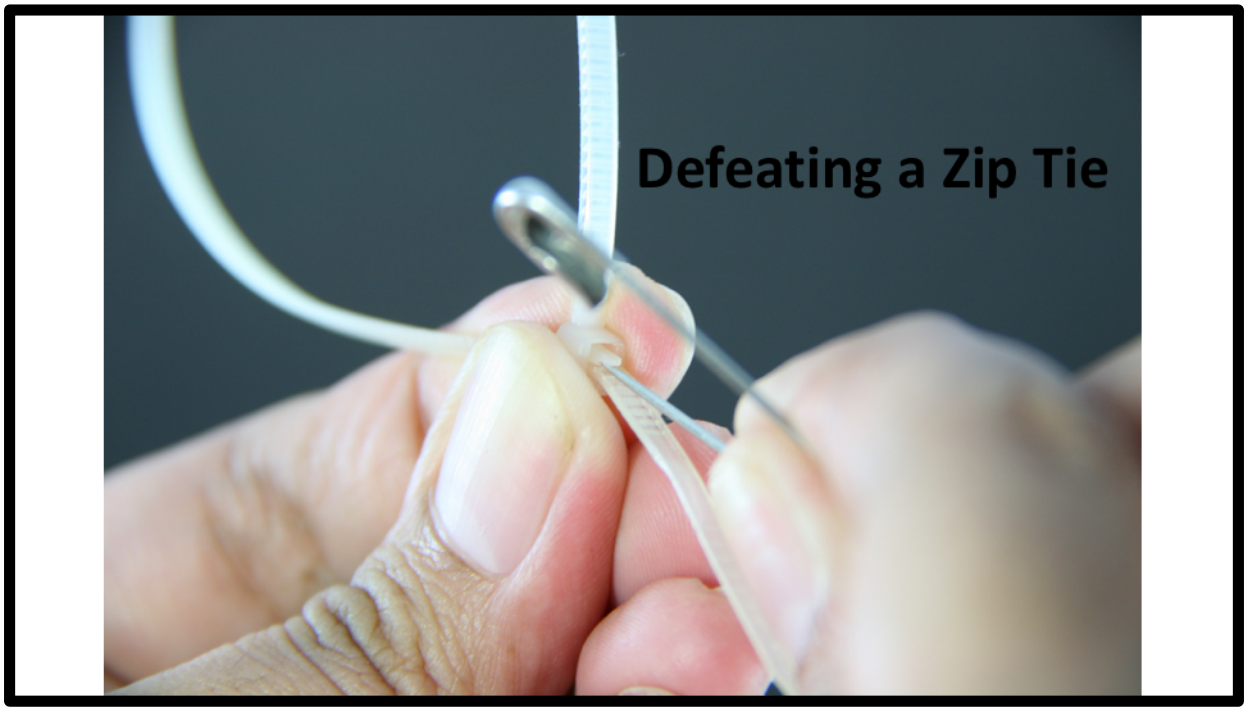
- Detect unauthorized access
- Not a “lock”
- Also known as “seals”
- How is the seal inspected?

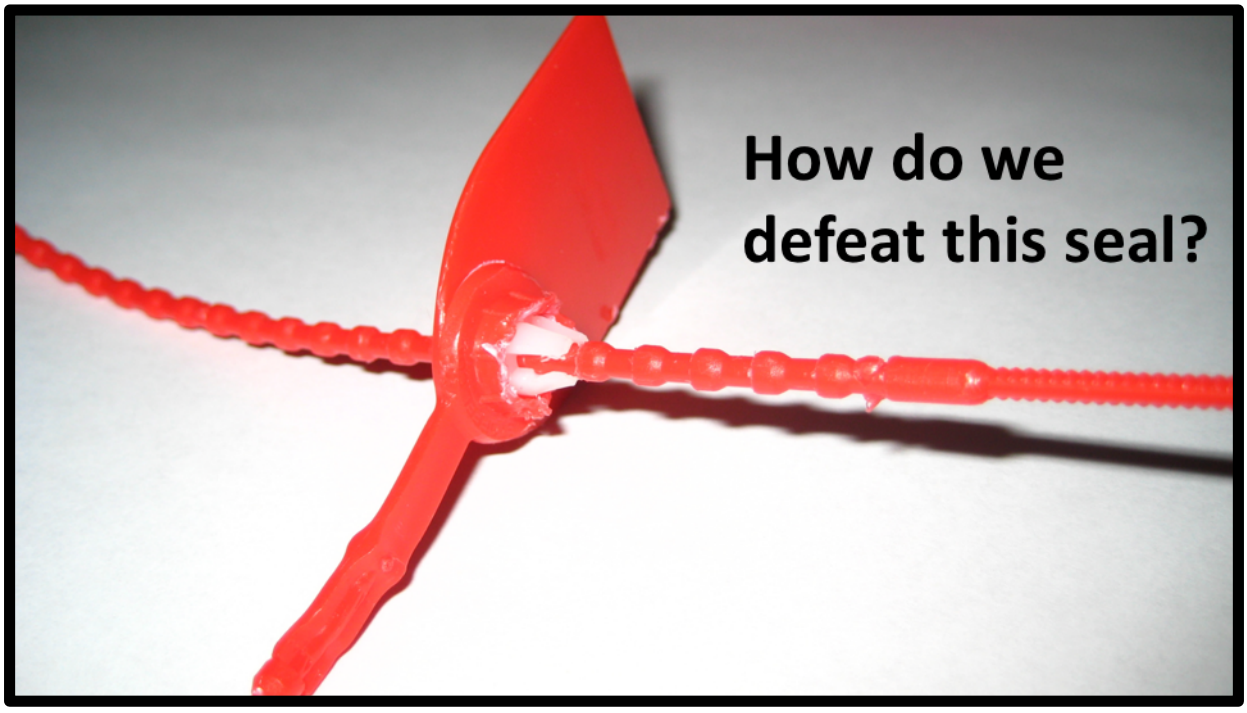

SEALED
0023518
022850

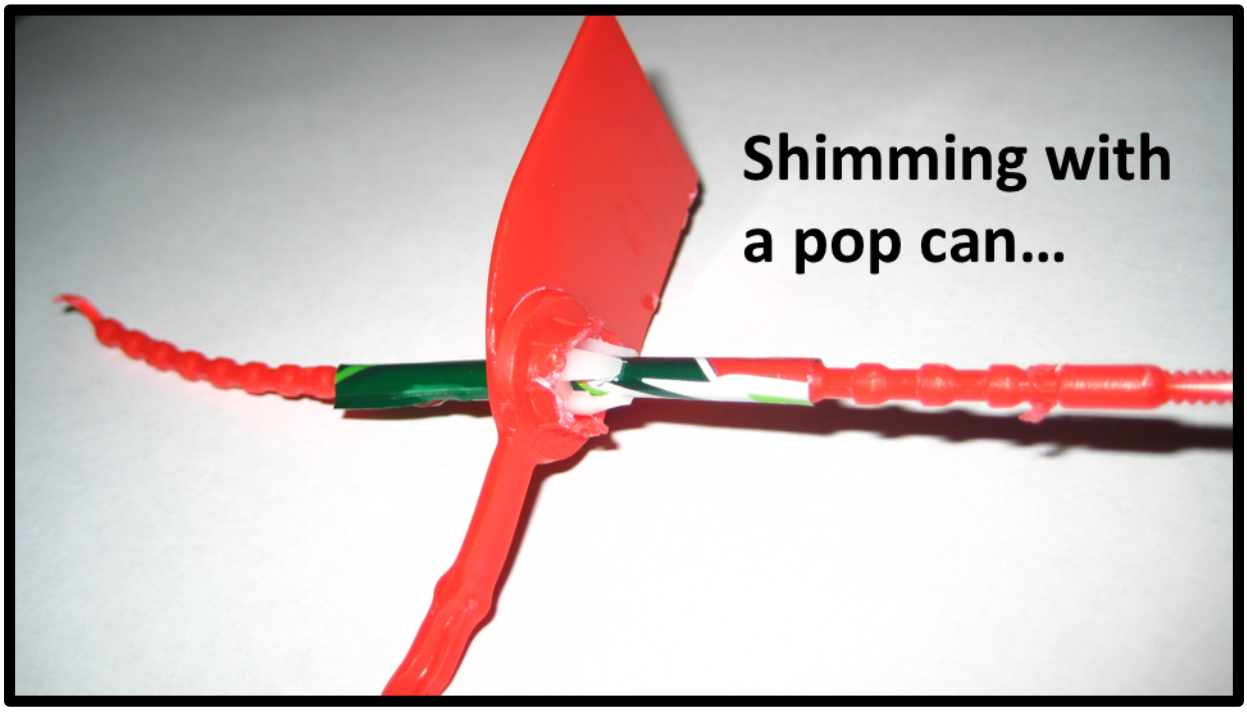
Defeating Tamper Evident Seals

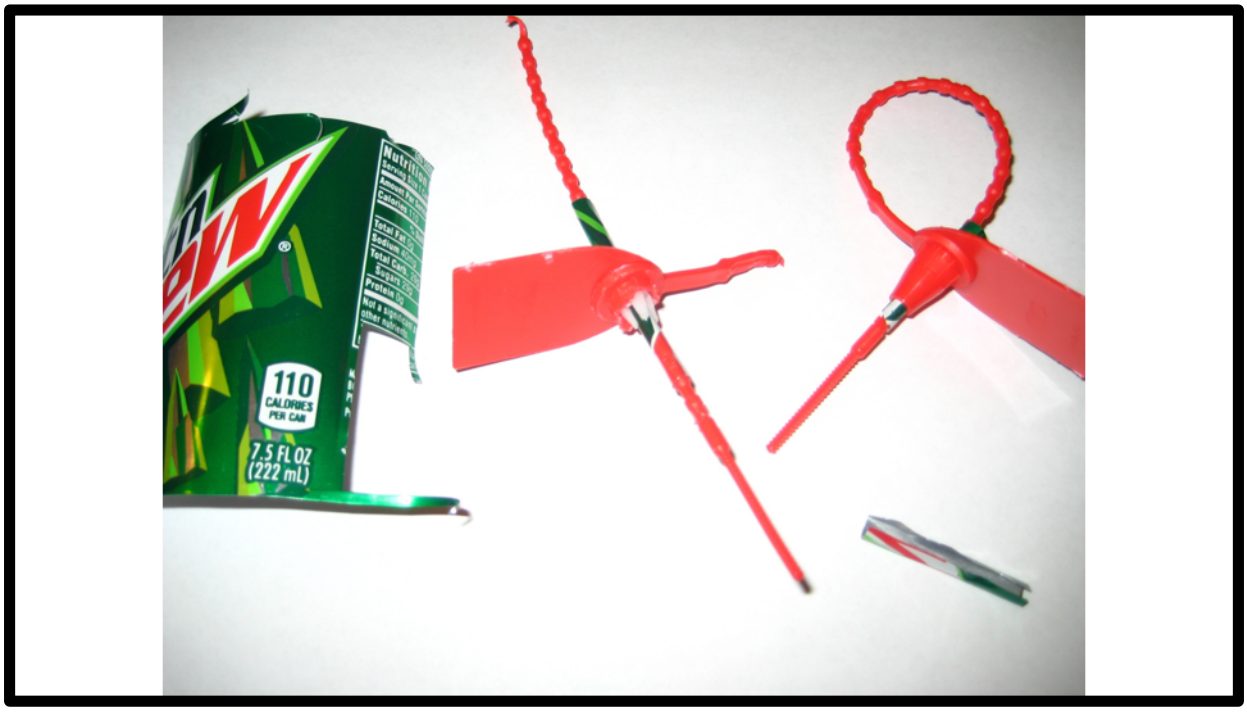
- Important Question: How does it work?
- Works similar to a zip tie


Cutaway of a Zip Tie

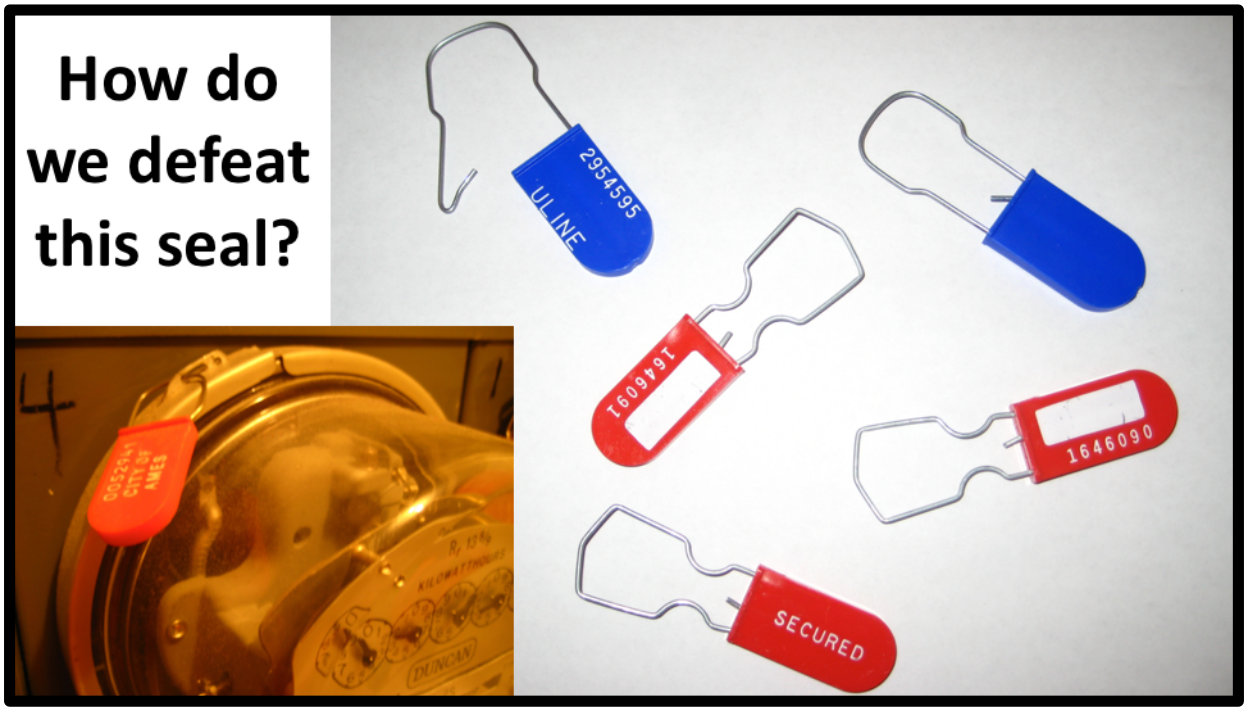

Defeating a Zip Tie


How do we
defeat this seal?


Shimming with
a pop can…

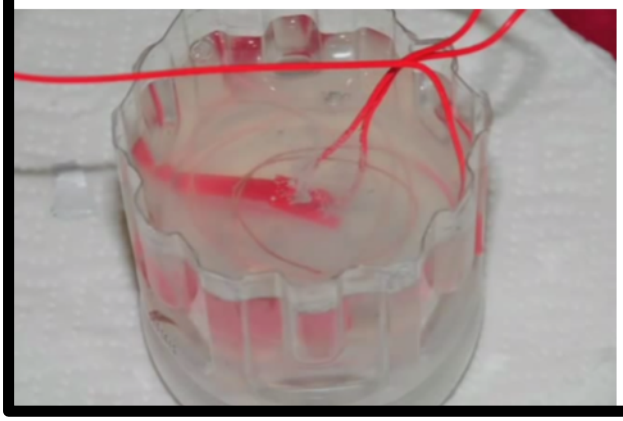

110
CALORIES
PER CAN
7.5 FL OZ
(222 mL)

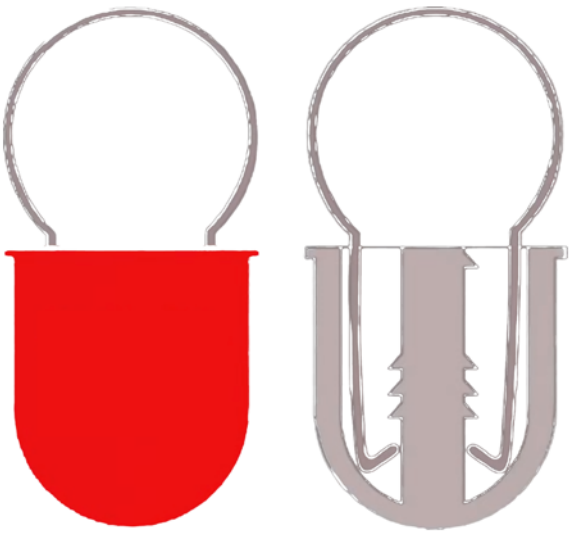
How do we defeat this seal?



Defeating Tamper Evident Seals

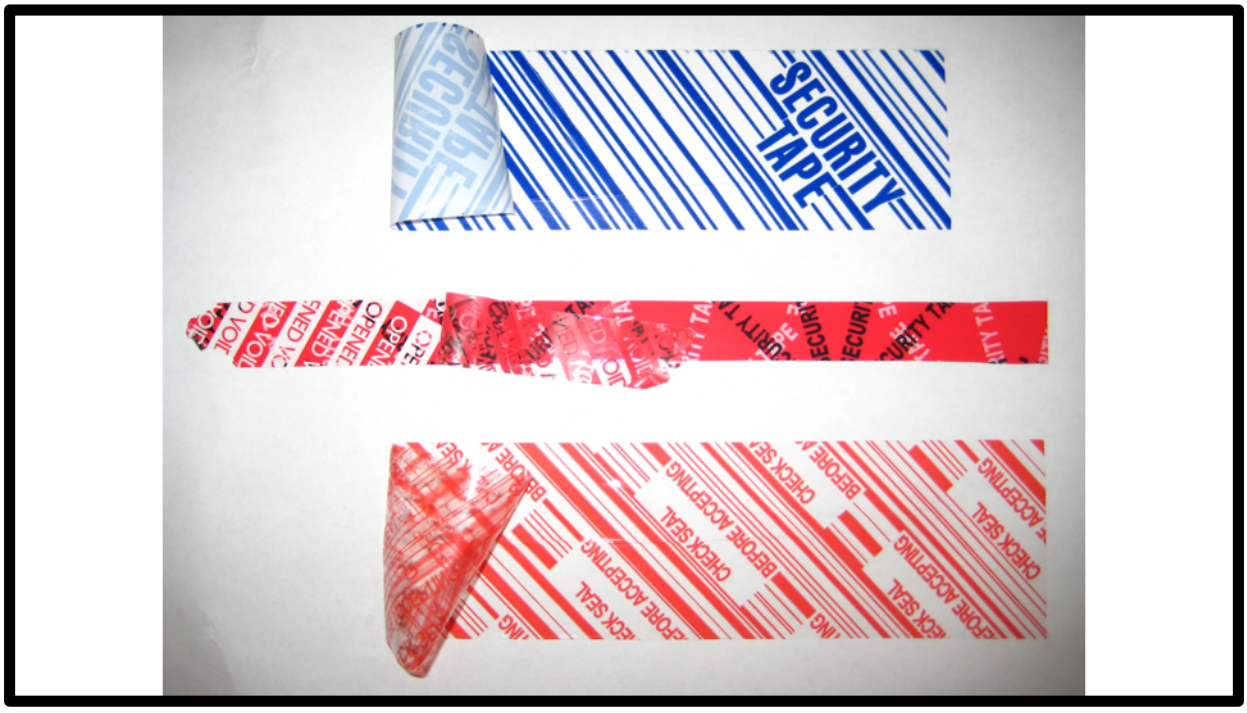
- How does it work?





Tamper Evident Adhesives


SECURITY TAPE
SECURITY TAPE
BEFORE ACCEPTING
CHECK SEAL


SECURITY
TAPE

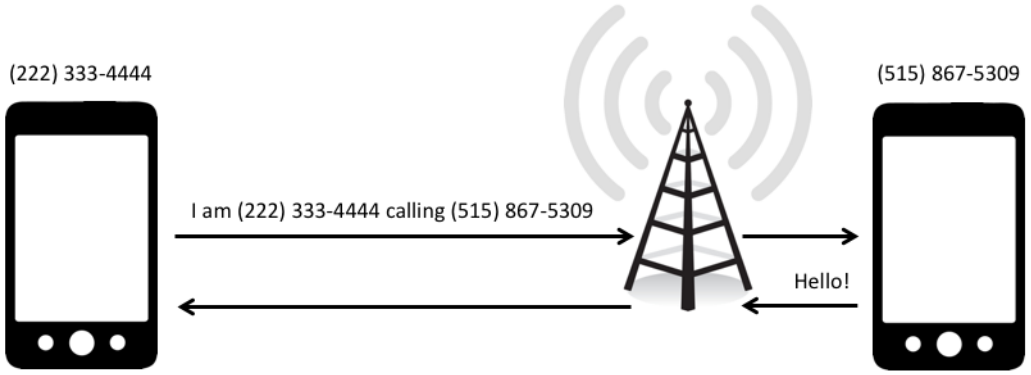
Defeating Adhesive Seals

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

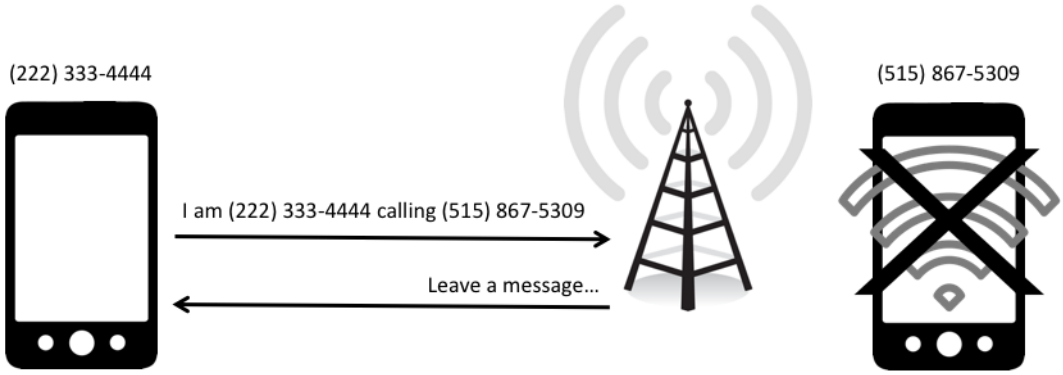
Hacking: Voicemail

- What question(s) should we ask?

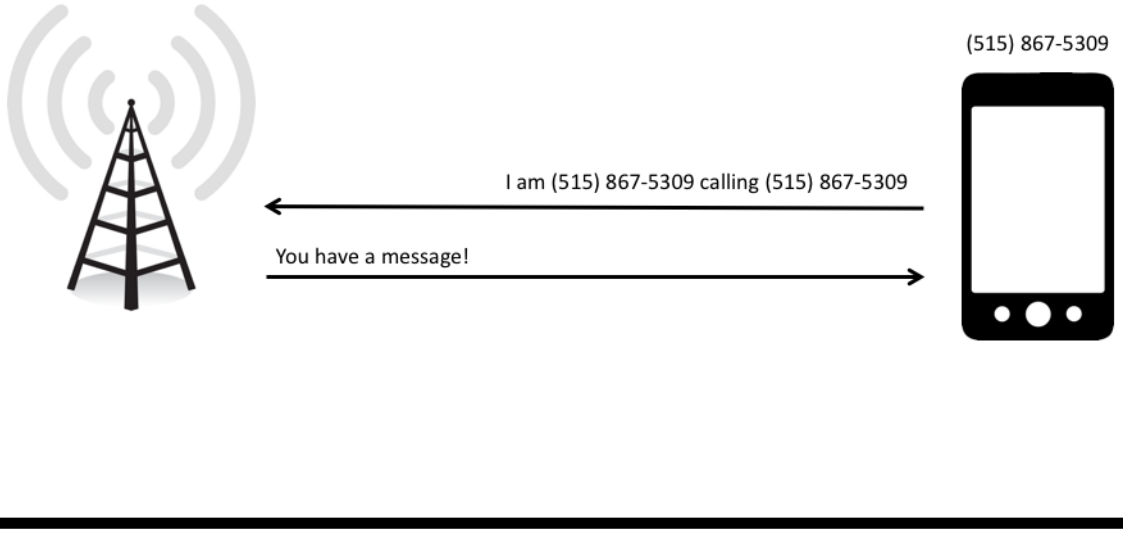
How does voicemail work?



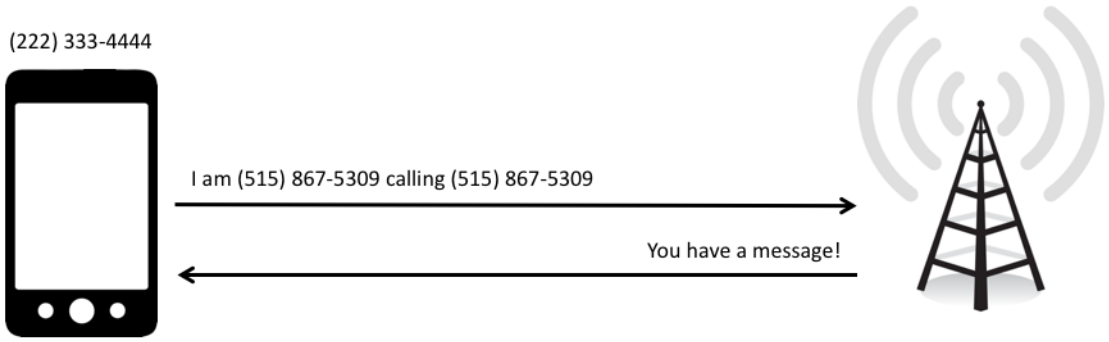
How does voicemail work?



How does voicemail work?



How does voicemail work?



Voicemail Hacking Demo

- Fake Victim: (515) 200-1301 (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".

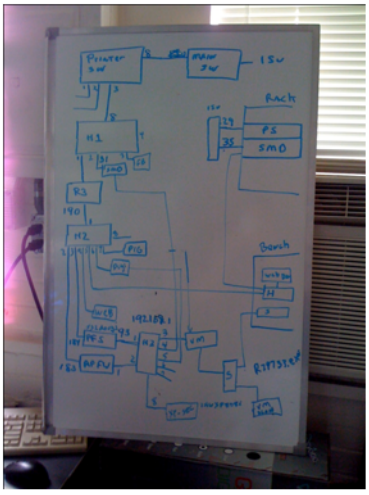
github.com/benjholla/VoicemailVictim

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.*

It is up to each of us to decide what we believe is morally right and wrong. With live in a society with legal precedents and consequences and we must all be responsible for our actions. Remember that every action may have unforeseeable consequences, so you must consider if you are willing to live with those consequences, whatever they may be, even when you think nobody is watching. As Spiderman's Uncle Ben said, "With great power comes great responsibility".

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)

Note: The labs in this course are designed to push everyone in this course. Likely there will be some subject that you feel ill equipped to try, but don't let that be a barrier. Attempt the lab to the best of your ability and try your best to learn the core ideas behind each activity. Then attempt the lab again when you have more time. Please send questions, thoughts, and comments to pac-india@ben-holland.com and I will be happy to help you find your way to success for any of the labs. There are multiple solutions to each lab, and in some cases there are no right answers!

General Plan

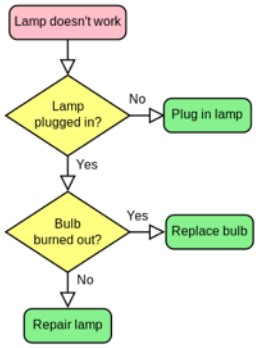
- Focus on getting hands on experience!
- If labs are completed early we can explore more advanced topics
- I will adapt materials to you
- Form teams on Tuesday
  - Balance teams based on experience
  - Study buddies before competition
  - Teammates during competition
  - May develop specialized roles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



Computers understand and follow very simple instructions. They do not know right from wrong, they only follow instructions exactly as they see them. Programs are made of these simple instructions and cab be thought of like flowcharts. Flowcharts take some *data* (YES/NO) to make decisions. If/Then relationships (Did you eat breakfast today? -> YES/NO) let us *control* decisions based on the answers. We can even loop (Did you eat breakfast today -> No? -> Go back to the start.). We can make lots of flowcharts and combine them to make really complicated programs. Even though the idea of flowcharts is very simple, a big flow chart can be very confusing to understand right? What if you make a mistake in the flowchart? How do you find the mistake? Could someone think of bad answers that cause your flowchart to give a wrong answer? What if I gave some inputs that cause you to go in a loop forever in your flowchart and never give an answer (example: I say I never eat breakfast)?