Learning to Think Like a Hacker

Ben Holland

bholland@iastate.edu

ben-holland.com/publications

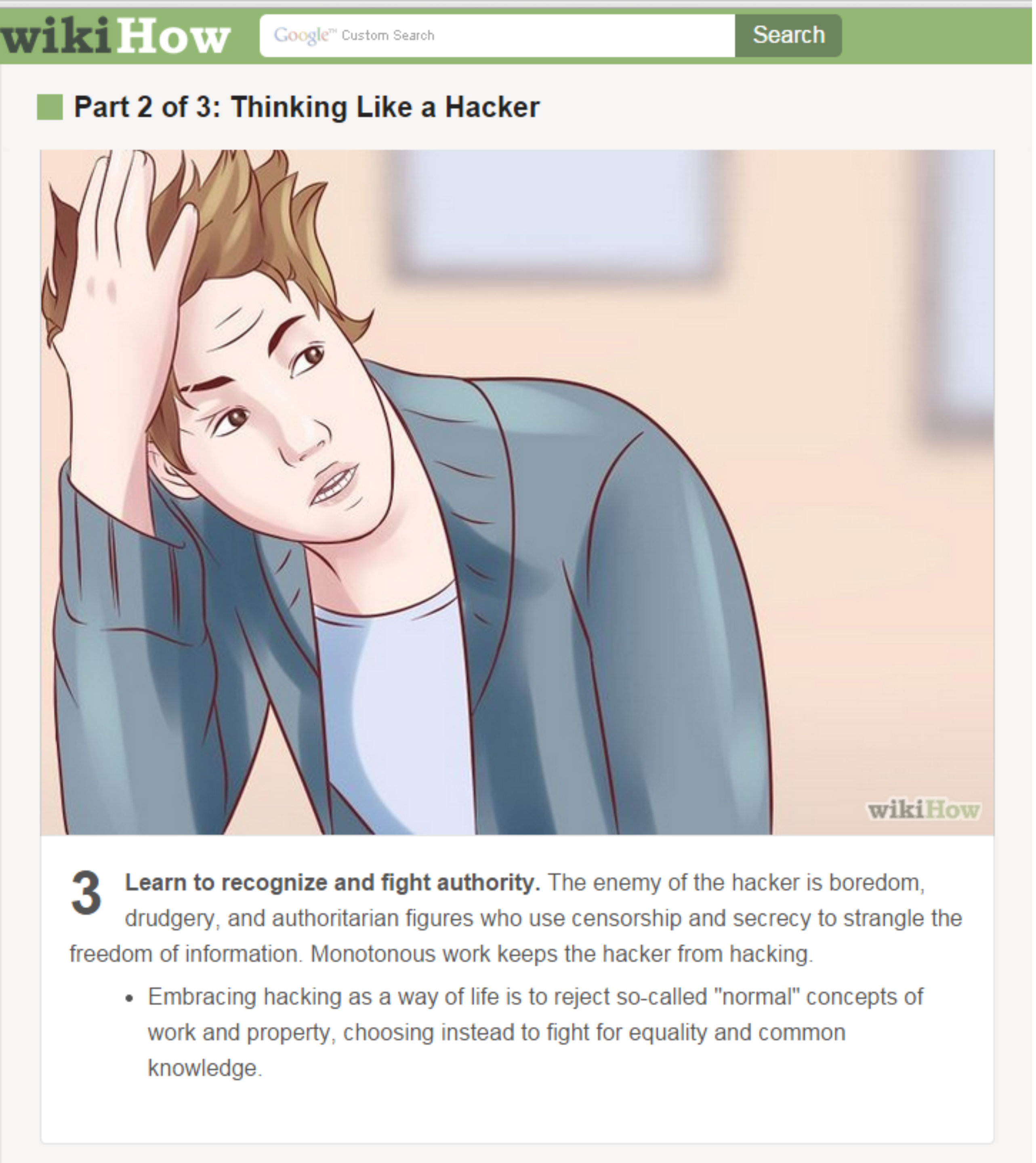
Who Am I?

- Ben Holland
  - B.S. in Computer Engineering (2005-2010)
  - B.S. in Computer Science (2011)
  - M.S. in Computer Engineering and Information Assurance (2012)
  - ISU Research Associate (present)
    - DARPA grant for Android malware detection research

I just never left. So super duper Senior?

Let’s break the ice…

What’s a Hacker?



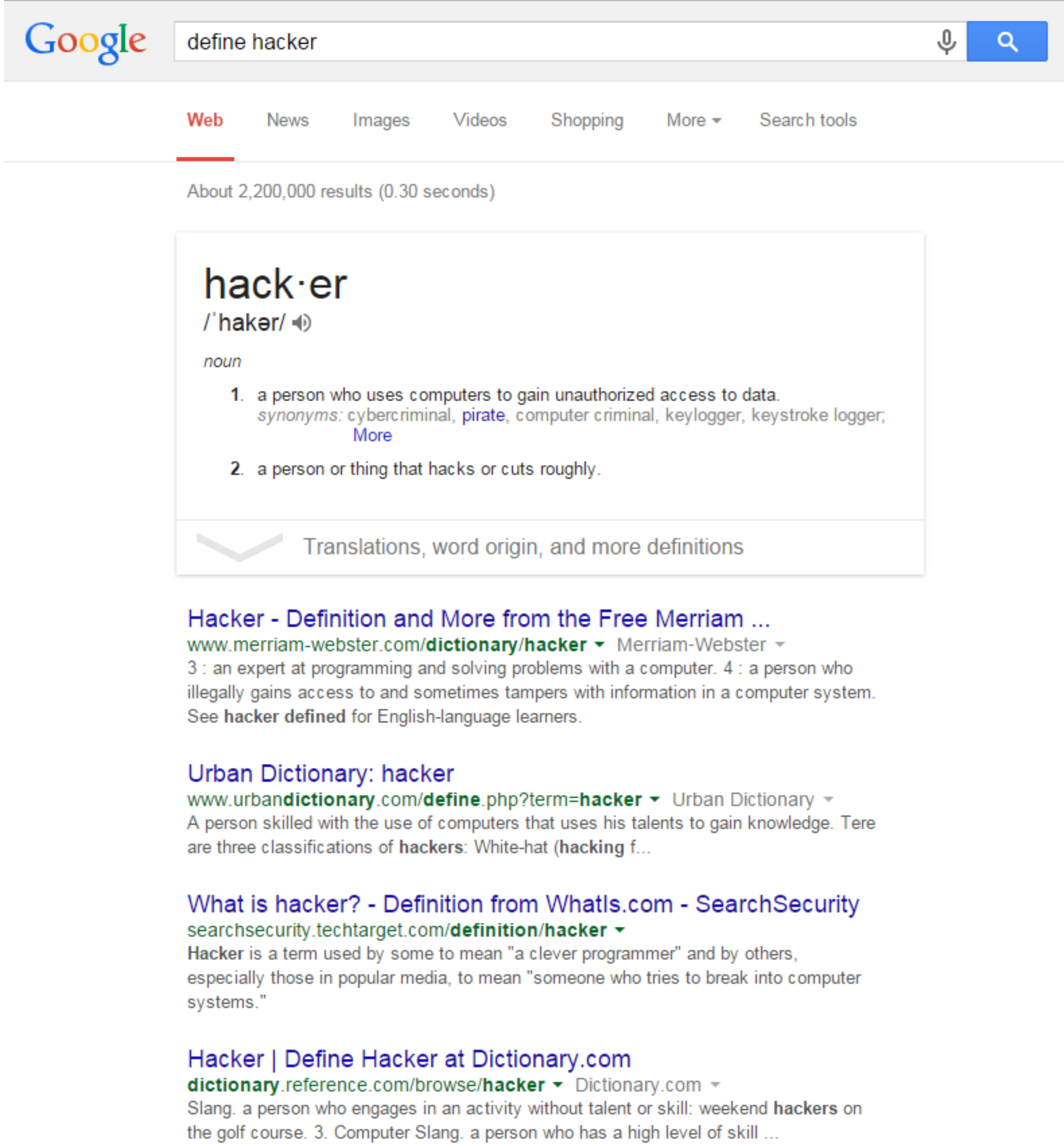
Part 2 of 3: Thinking Like a Hacker

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?

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



define hacker

About 2,200,000 results (0.30 seconds)

hack·er
/ˈhakər/

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.urban**dictionary**.com/**define**.php?term=**hacker** Urban Dictionary
A person skilled with the use of computers that uses his talents to gain knowledge. Tere 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 ...

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

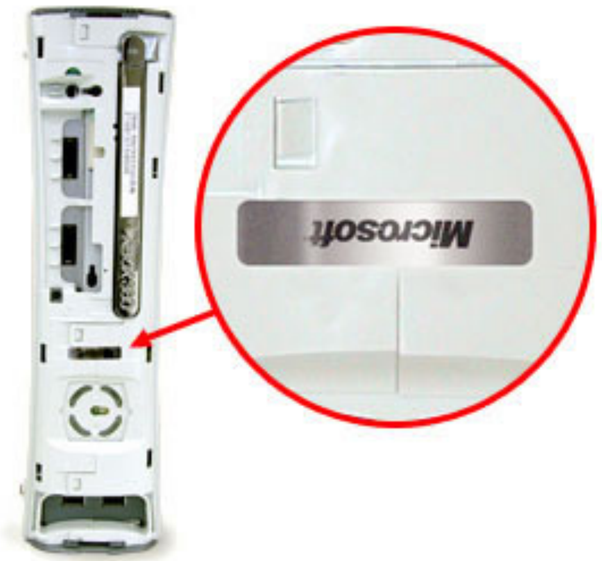
- Problem solving
- Critical thinking
- Tinkering
- Exploring how things work

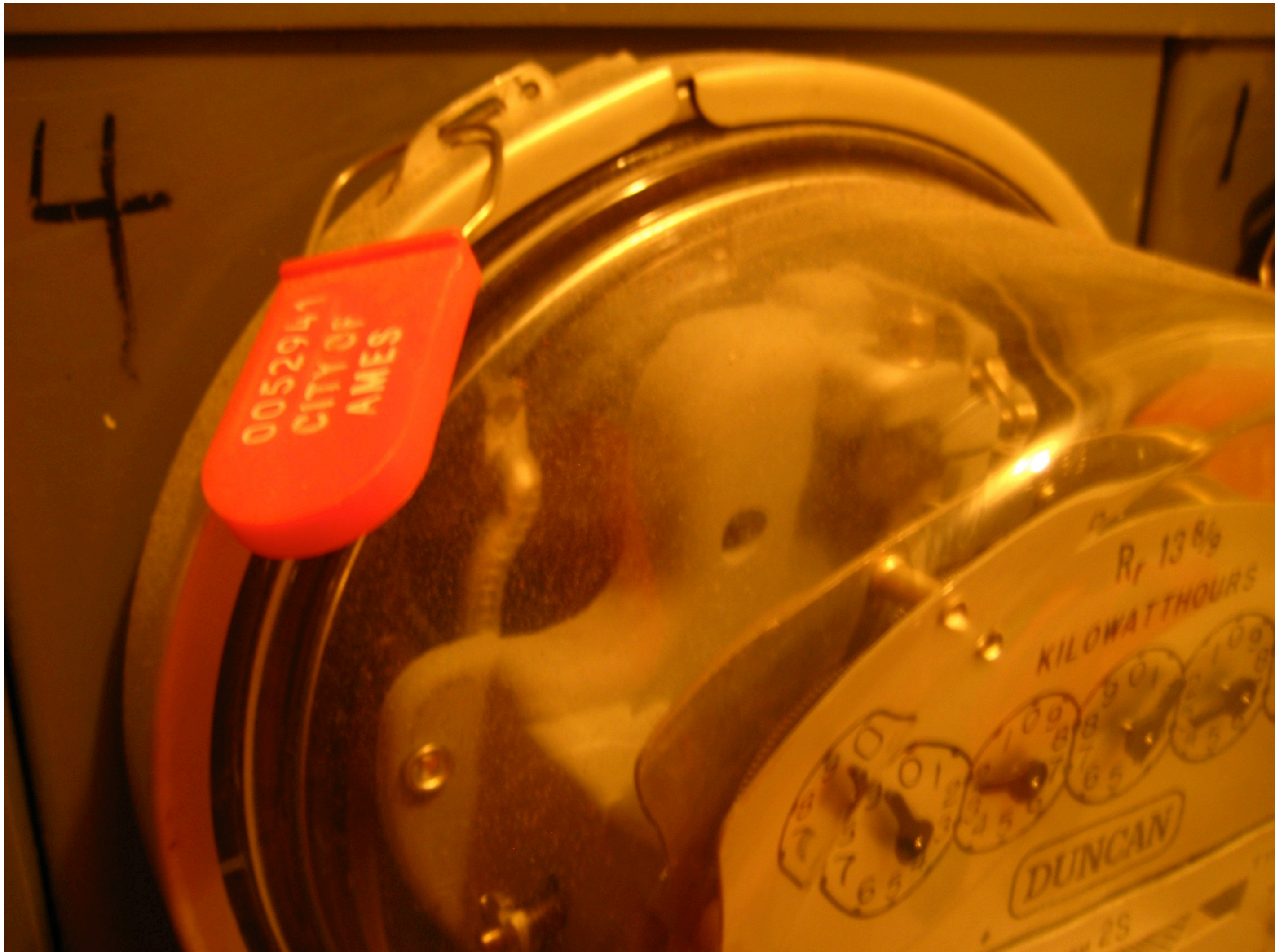
Outline

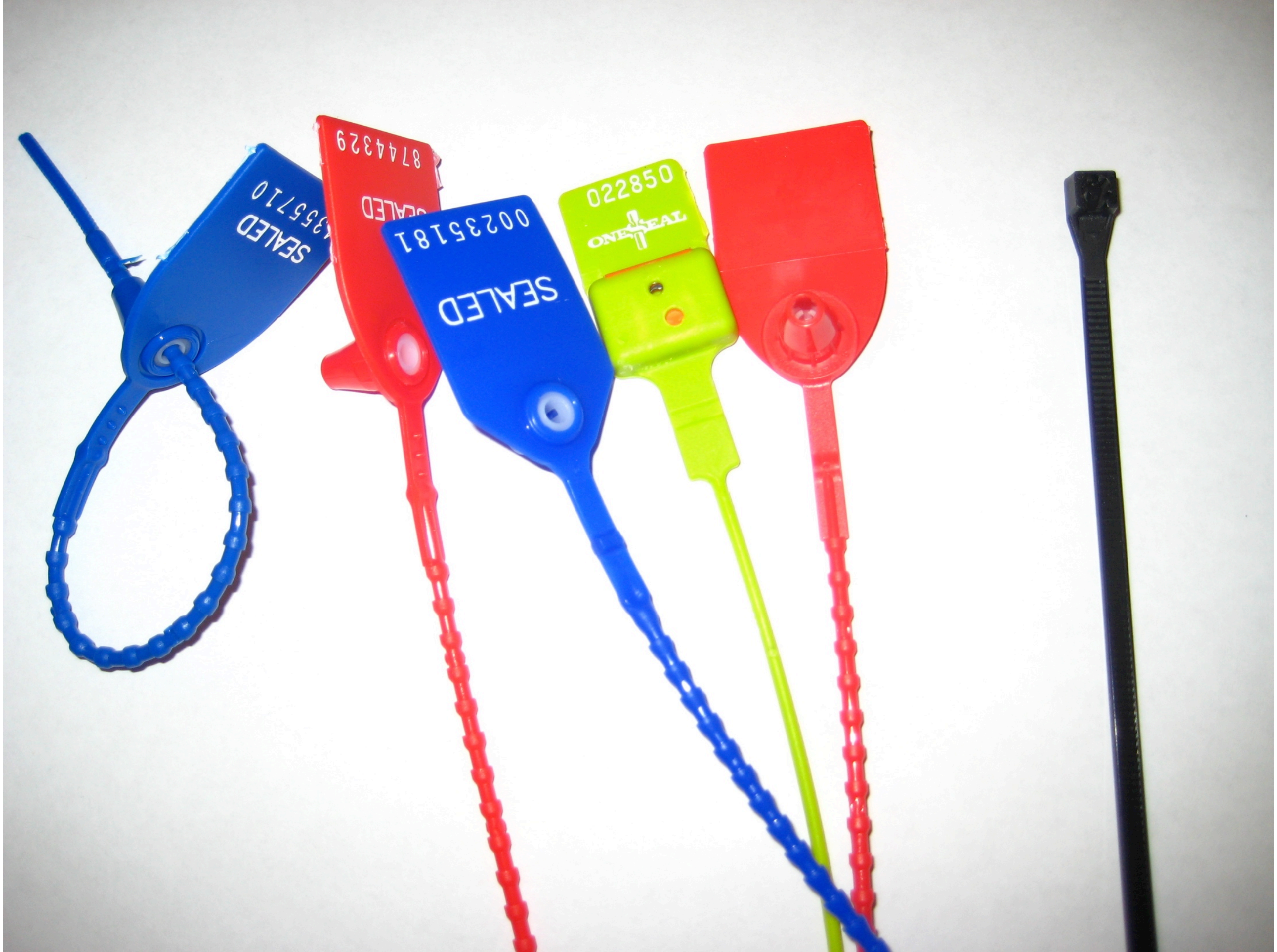
- Hacking Physical Systems (15 mins)
  - Activity 1 (10 mins)
- Hacking Digital Systems (10 mins)
  - Activity 2 (5 mins)
- Hacking Social Systems (5 mins)
  - Activity 3 (5 mins)
- Related ISU Programs (5 mins)
- Q/A (5 mins)

Hacking: Tamper Evident Devices

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



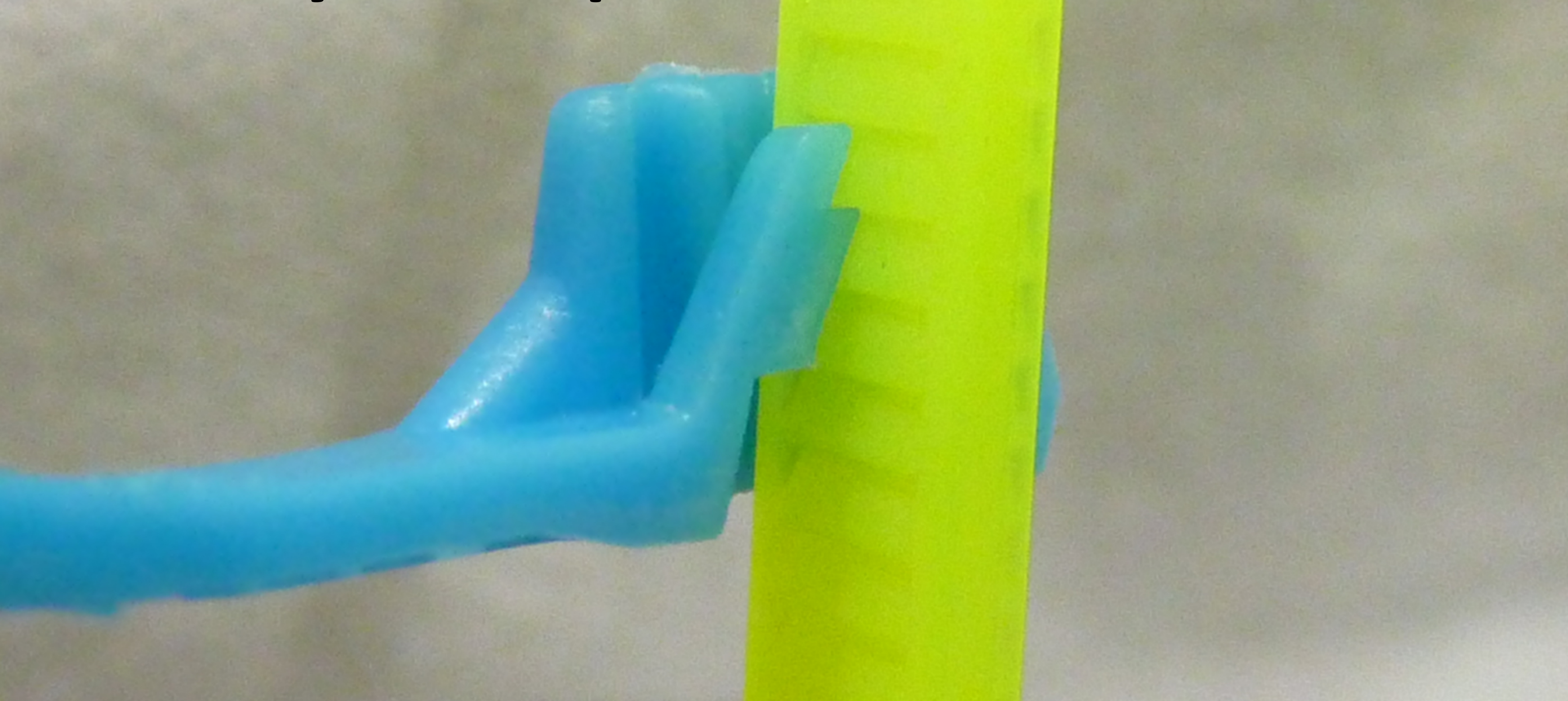



355710
SEALED
8744329
SEALED
00235181
SEALED
022850
ONE SEAL

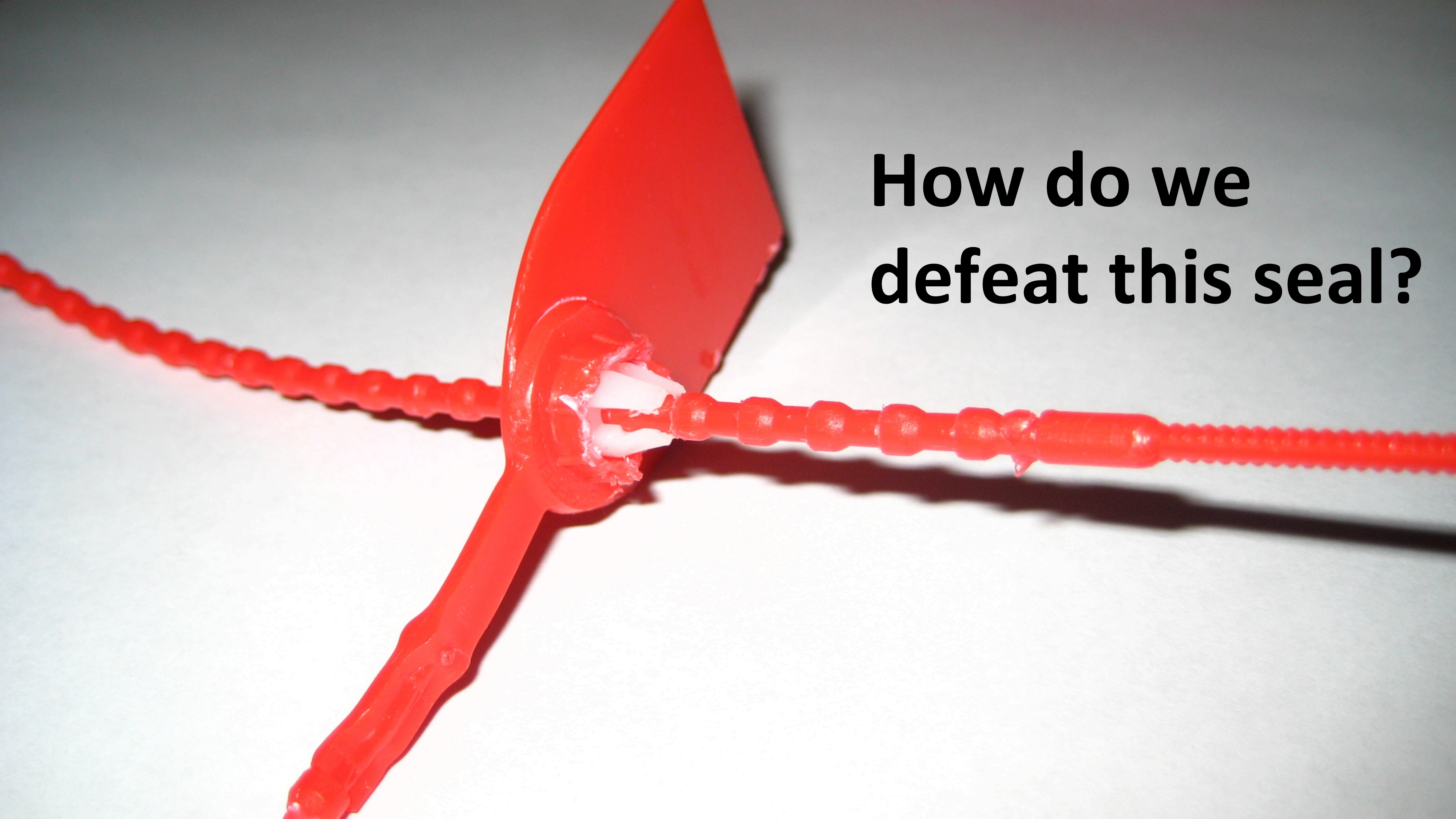
Defeating Tamper Evident Seals

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

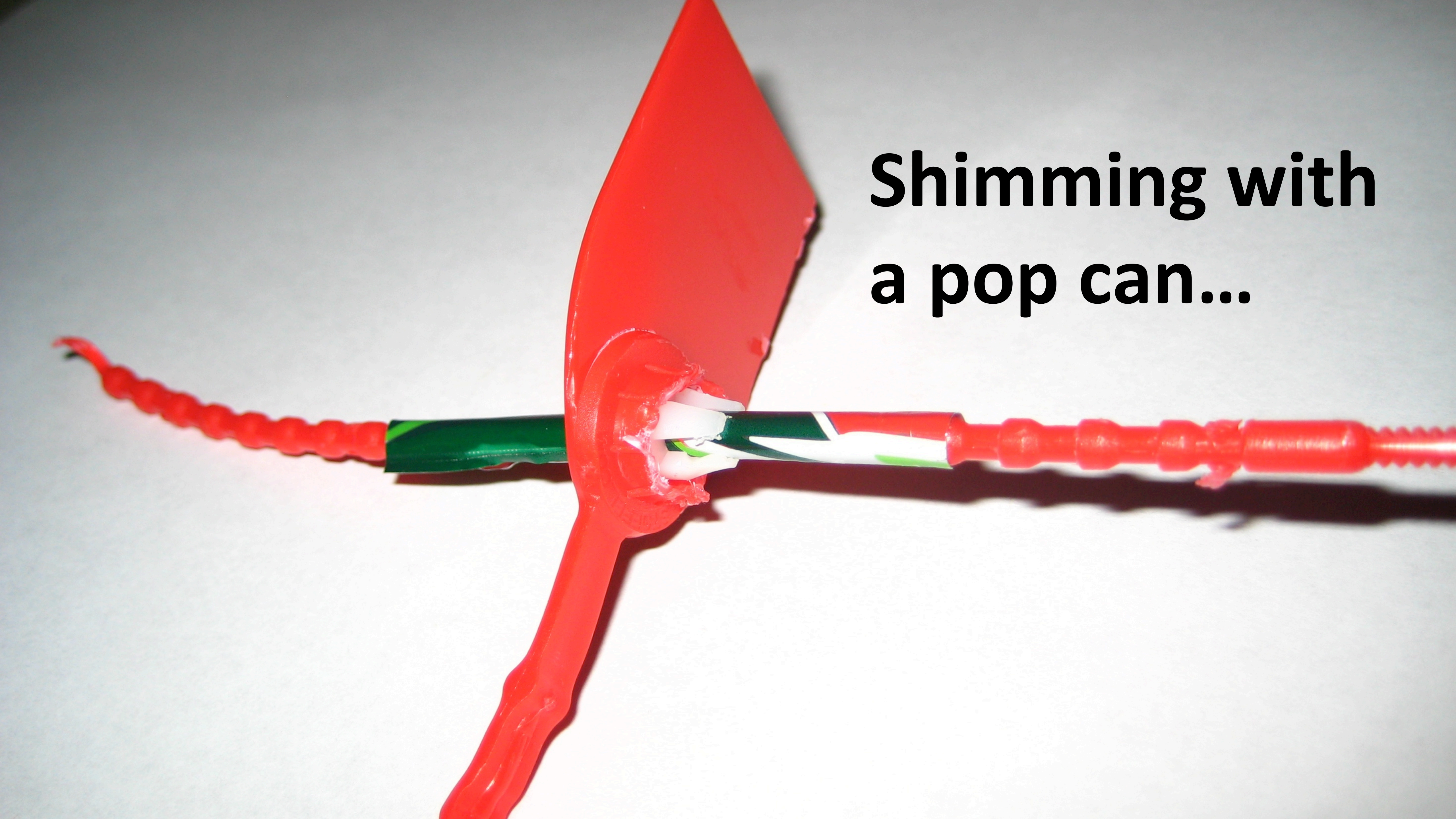
Cutaway of a Zip Tie



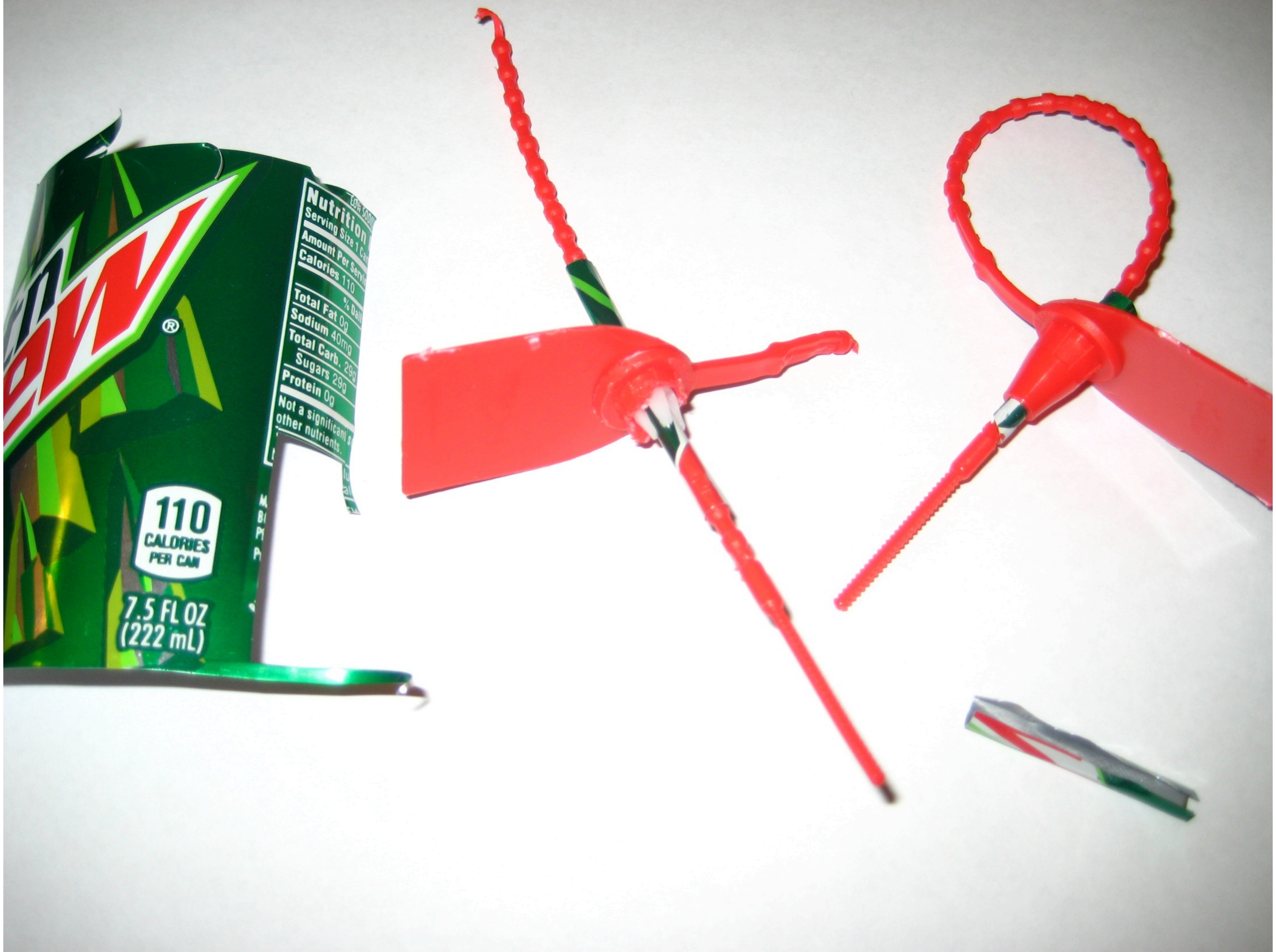
Defeating a Zip Tie



How do we defeat this seal?

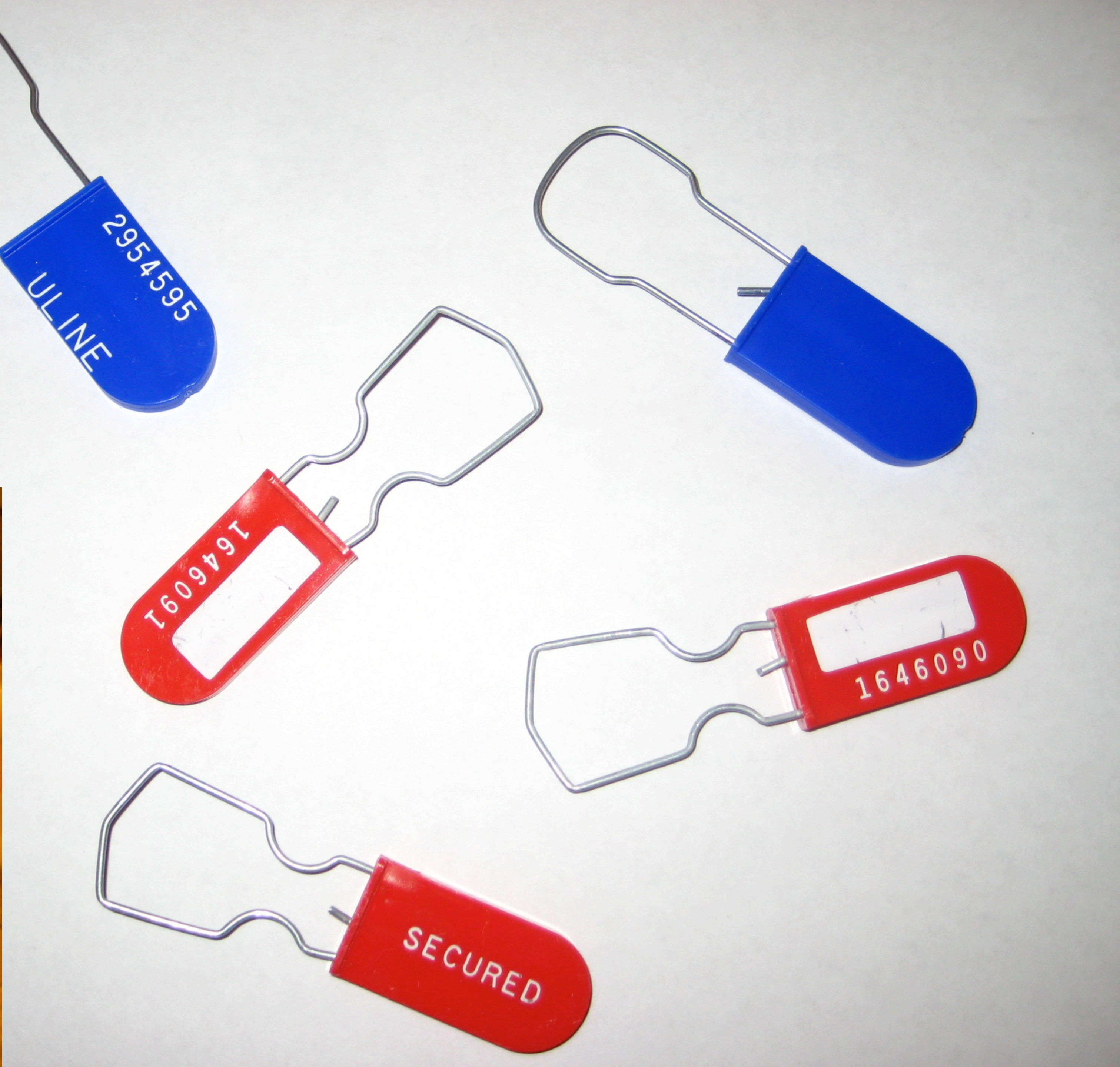


Shimming with
a pop can…



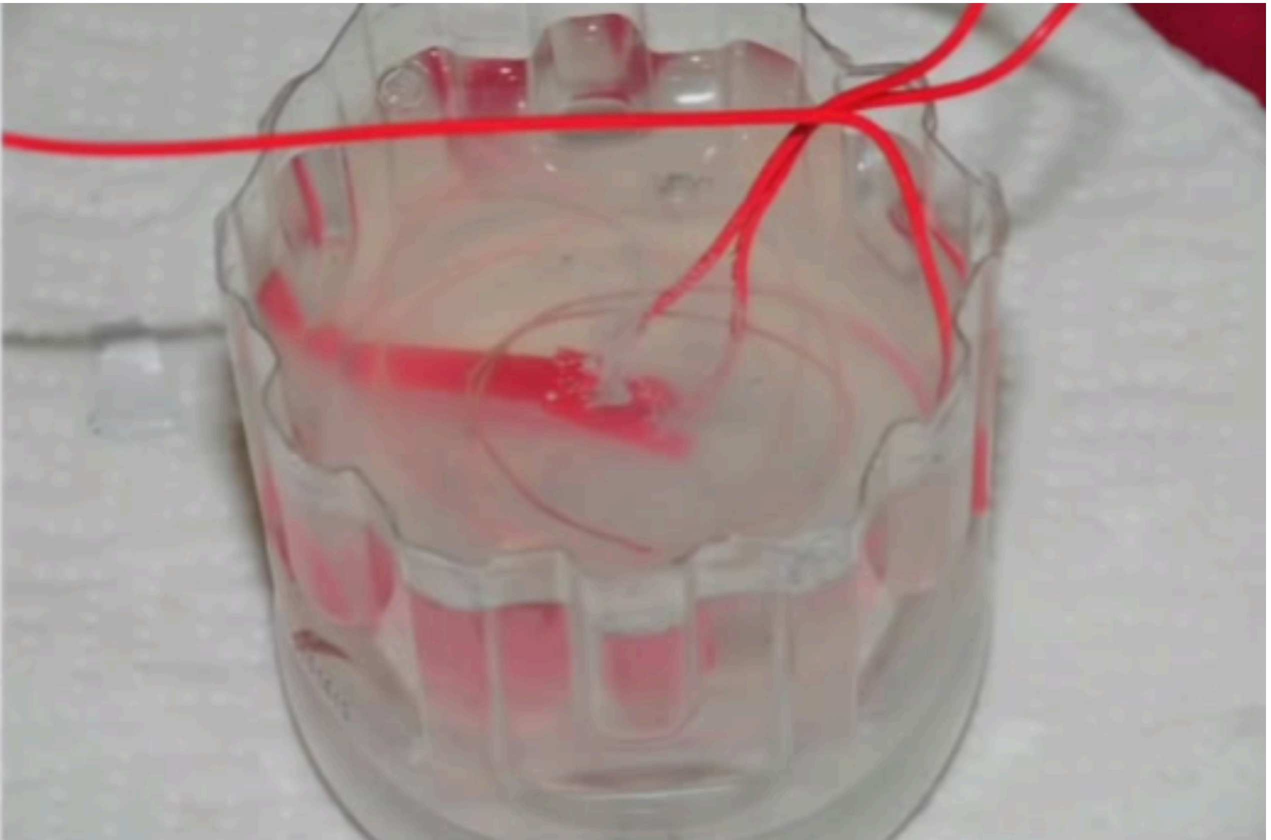
Nutrition
Serving Size 1 Can
Amount Per Serving
Calories 110
% Daily
Total Fat 0g
Sodium 40mg
Total Carb. 29g
Sugars 29g
Protein 0g
Not a significant source of other nutrients.
110
CALORIES PER CAN
7.5 FL OZ
(222 mL)

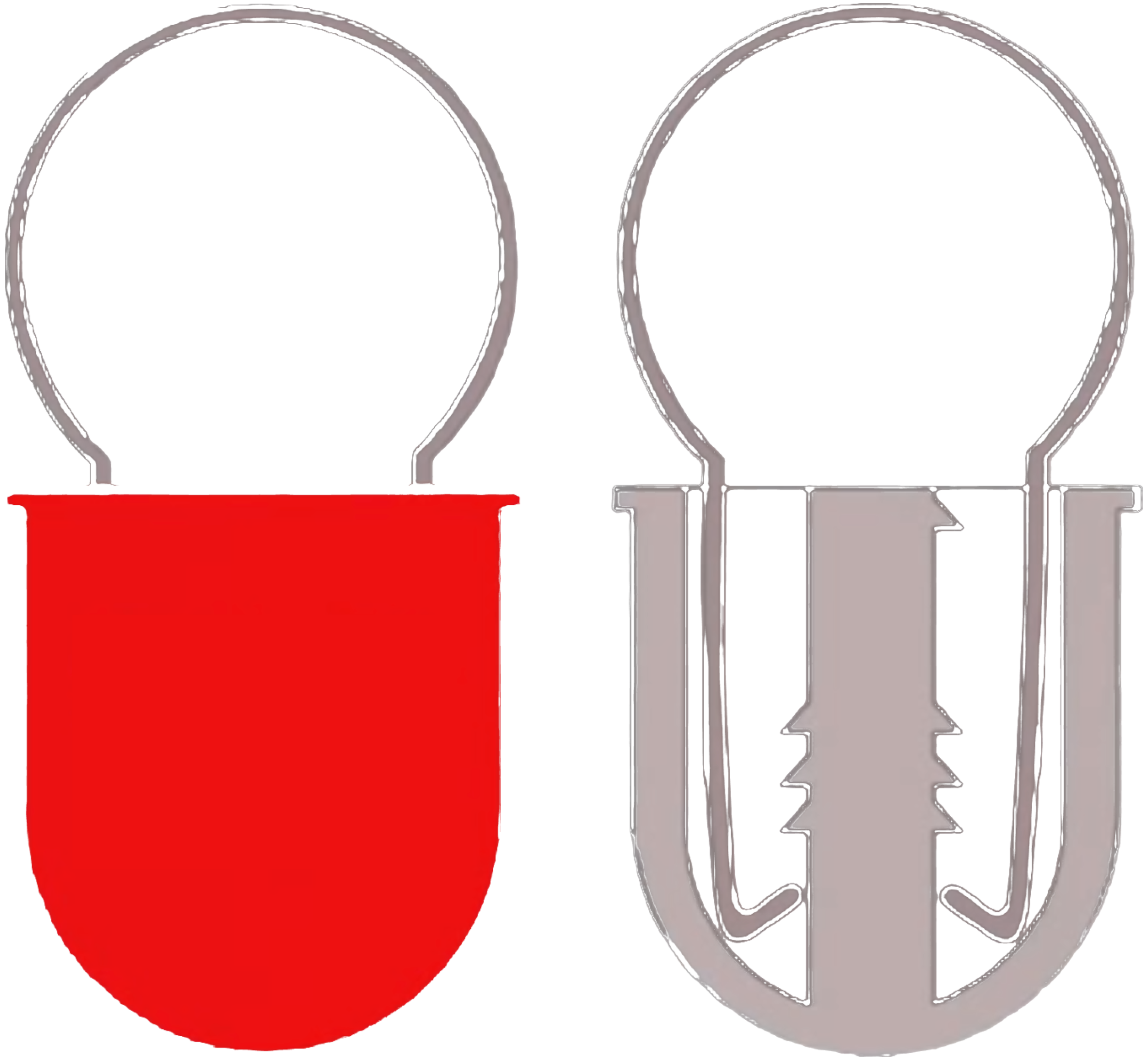
How do we defeat this seal?



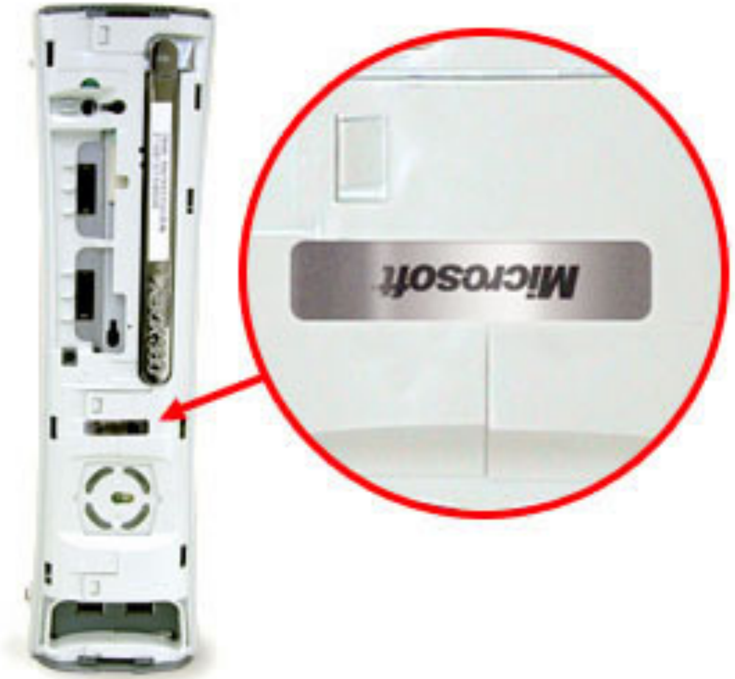
Defeating Tamper Evident Seals

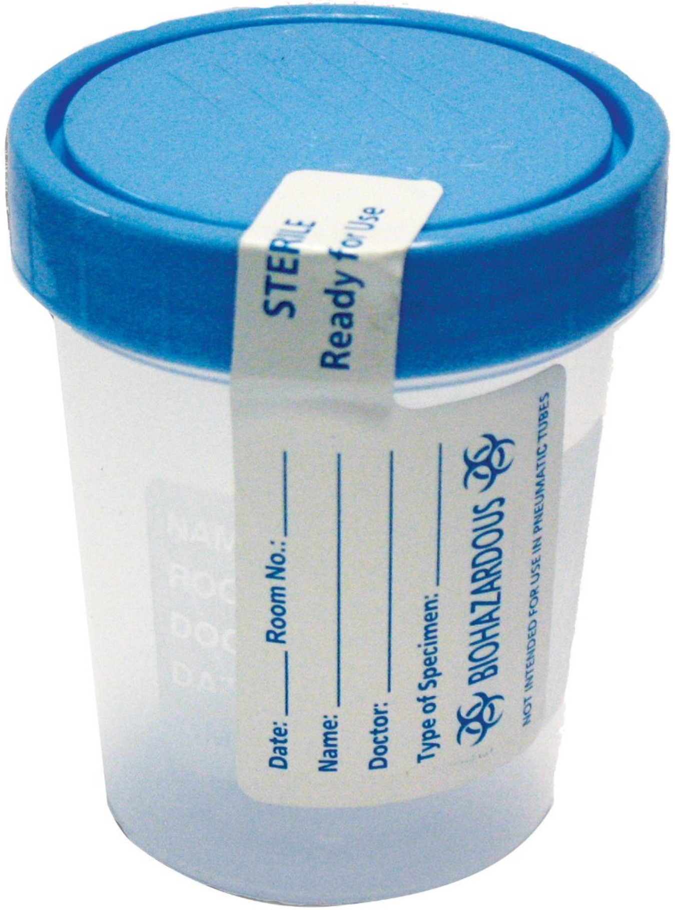
- How does it work?

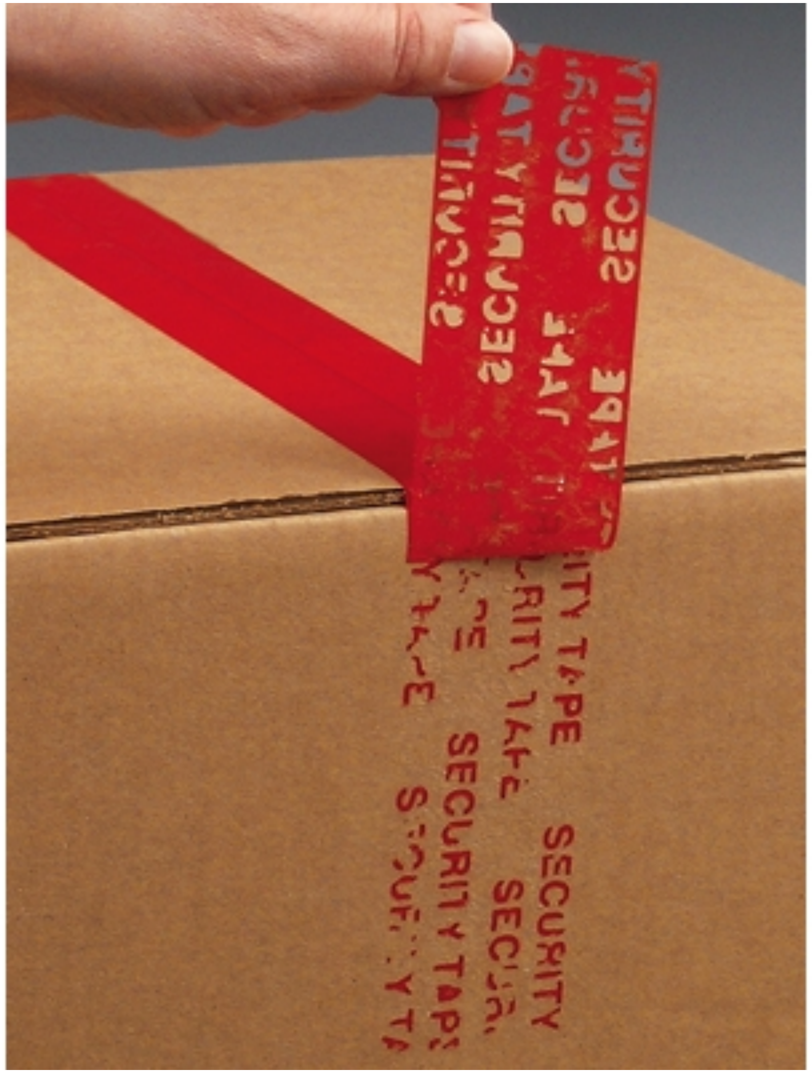


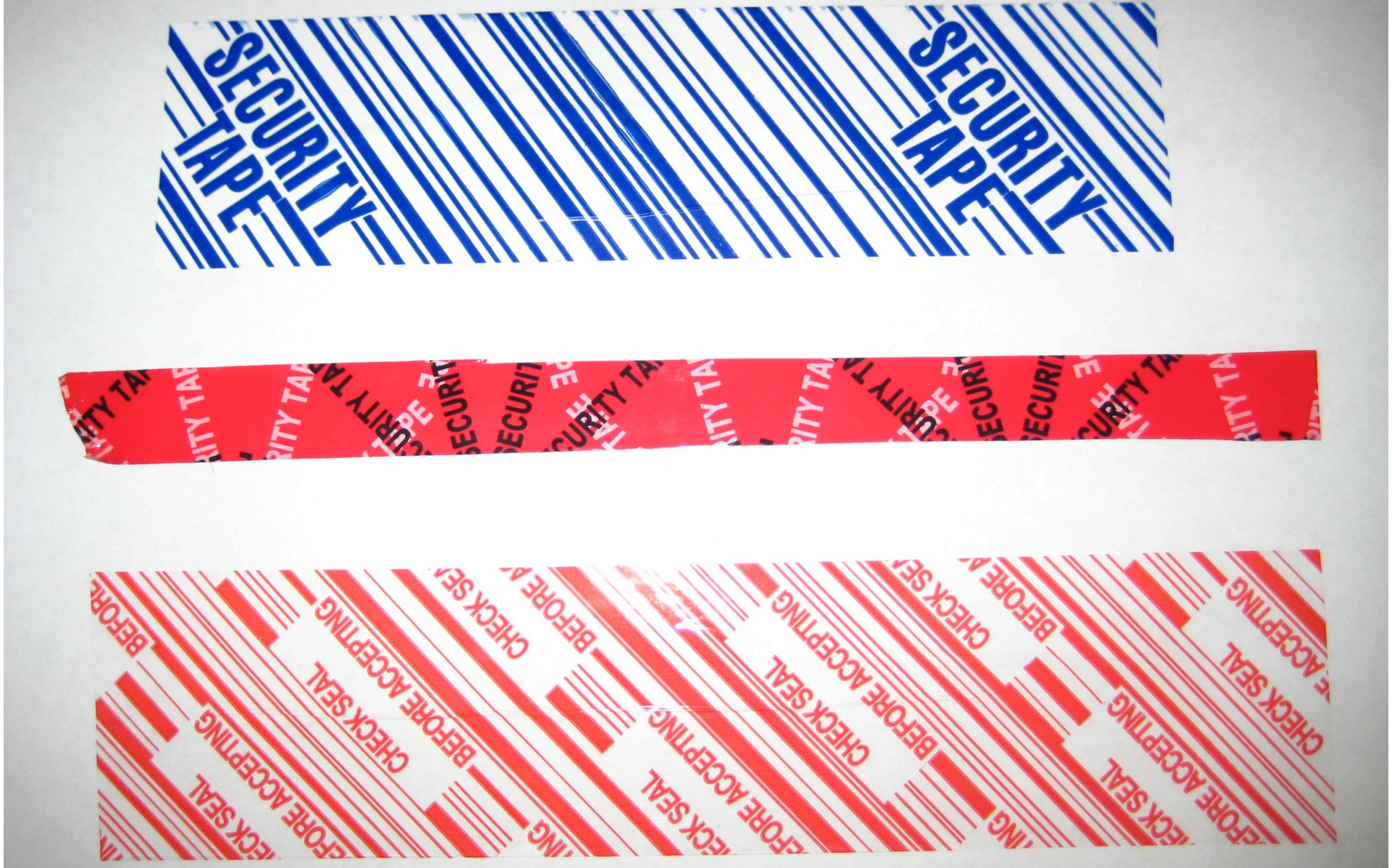


Tamper Evident Adhesives

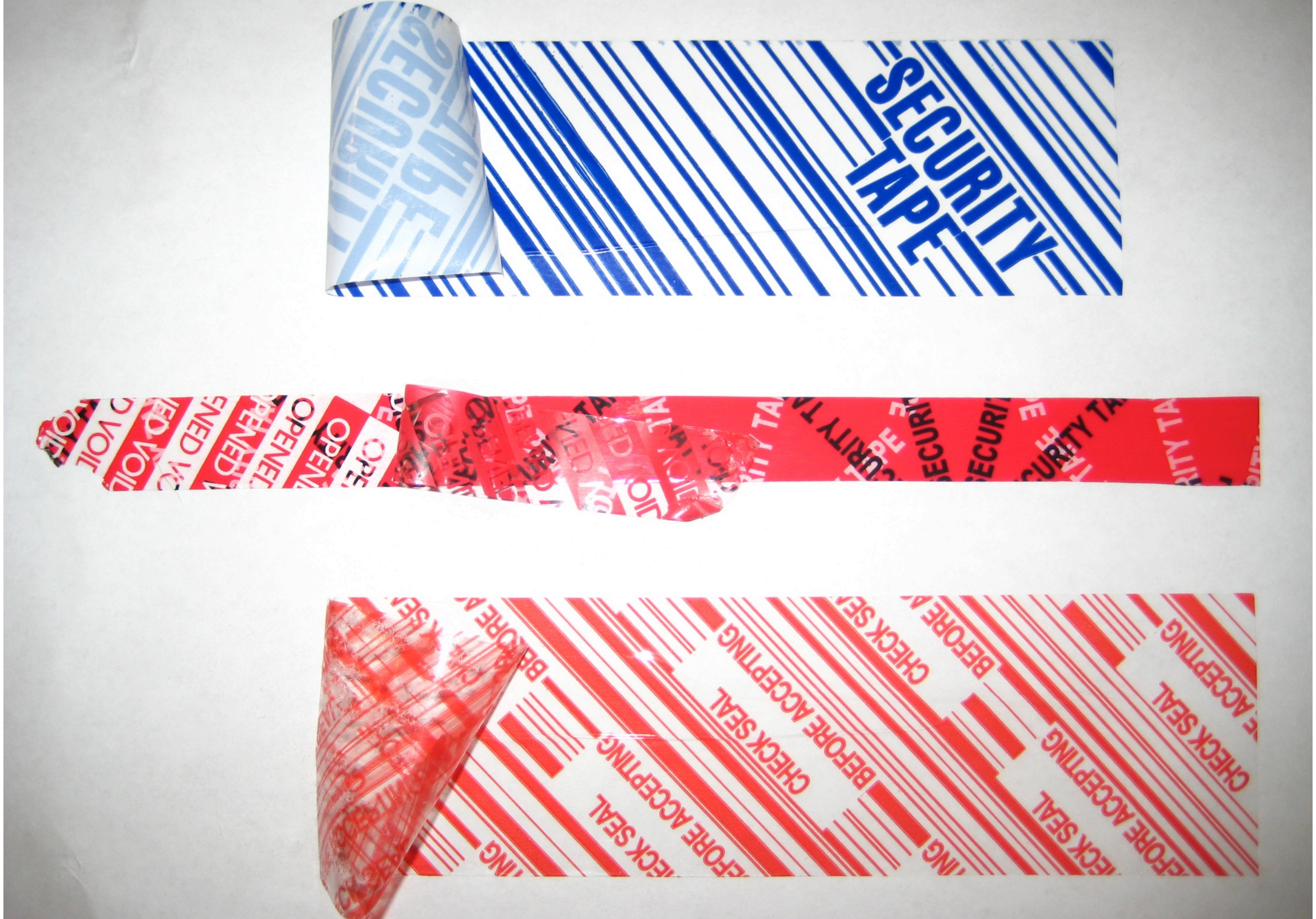








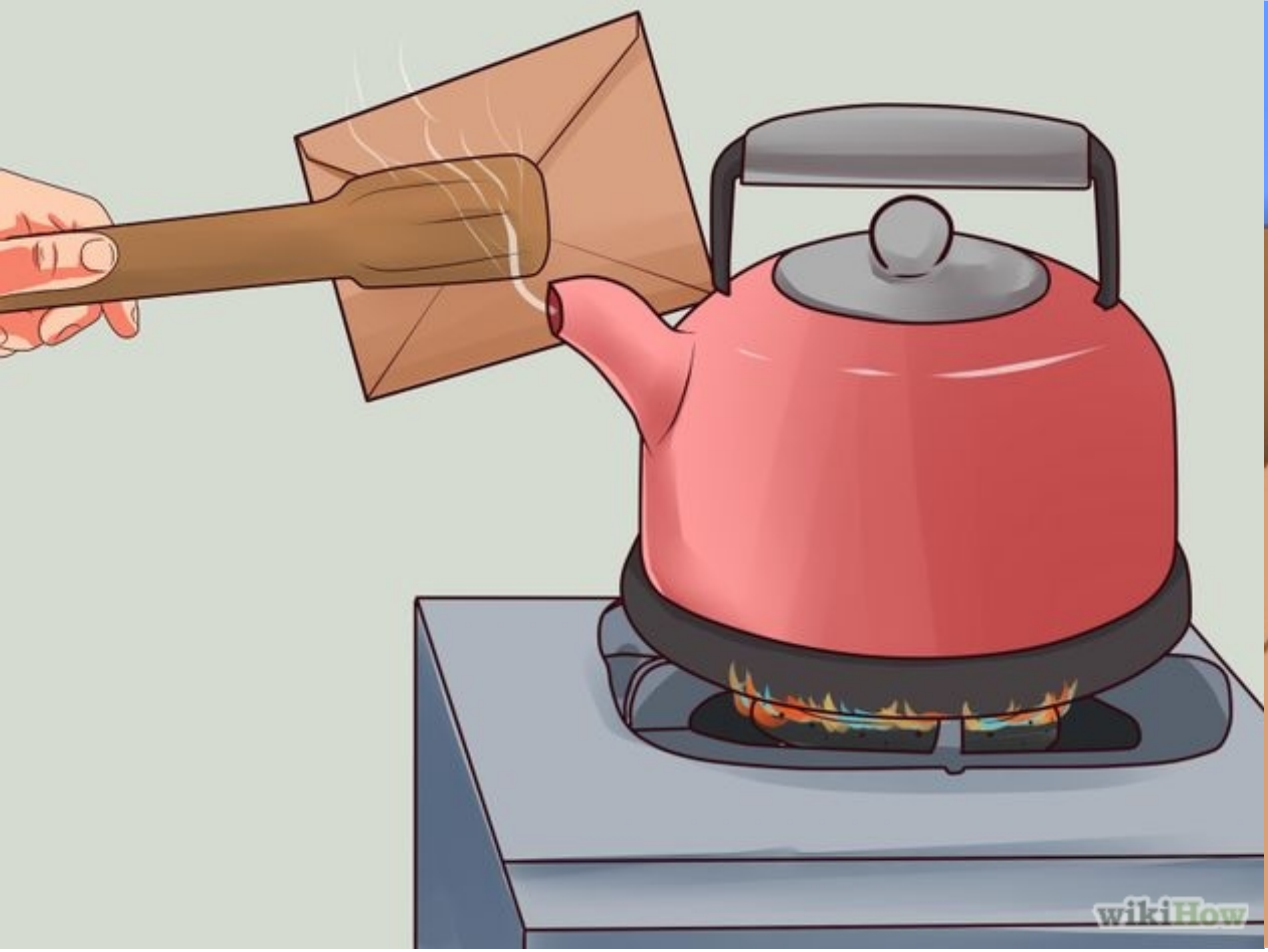
SECURITY TAPE
SECURITY TAPE
CHECK SEAL BEFORE ACCEPTING

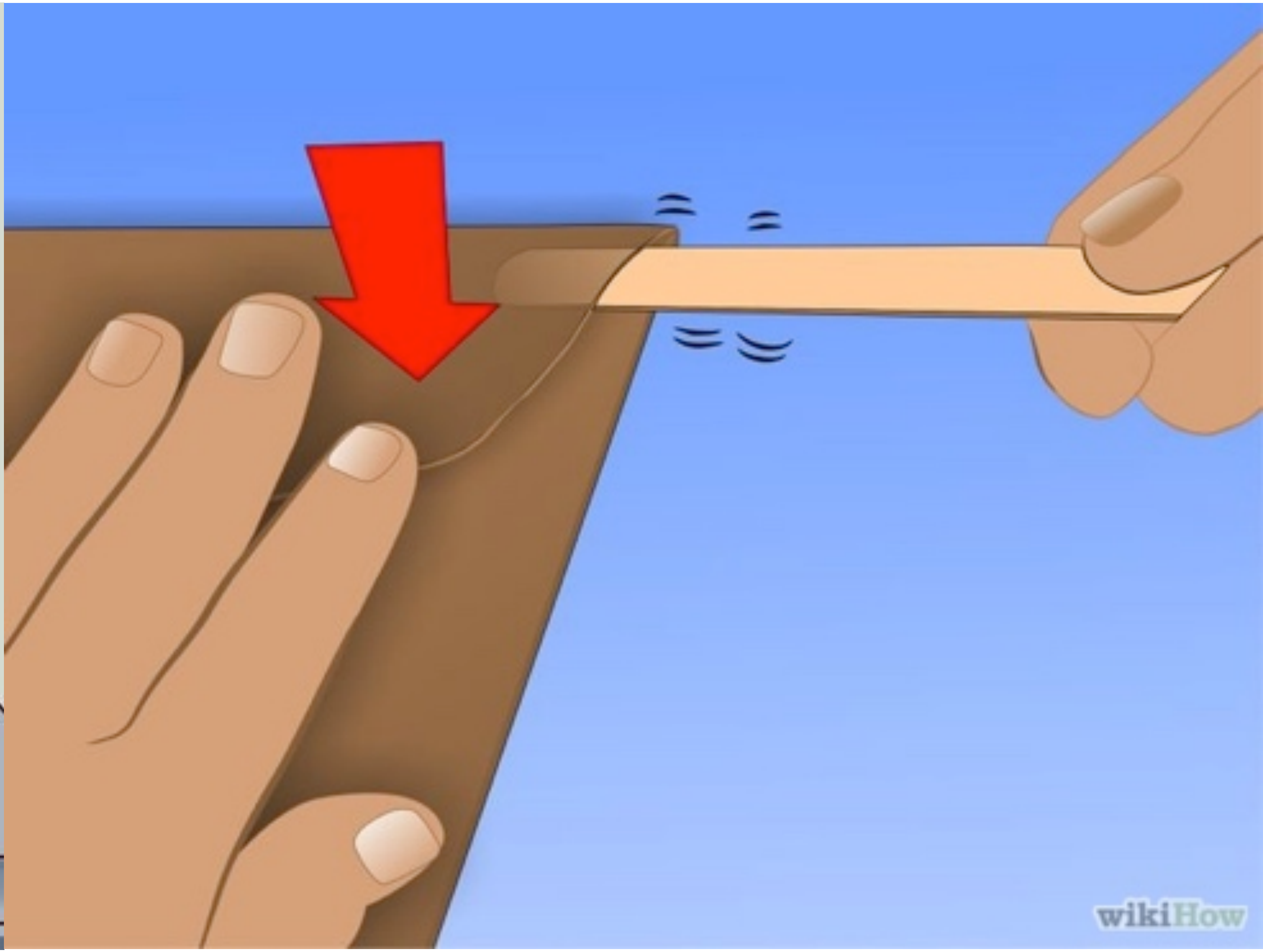

SECURITY TAPE
OPENED VOID
SECURITY TAPE
CHECK SEAL BEFORE ACCEPTING

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

Mail Tampering

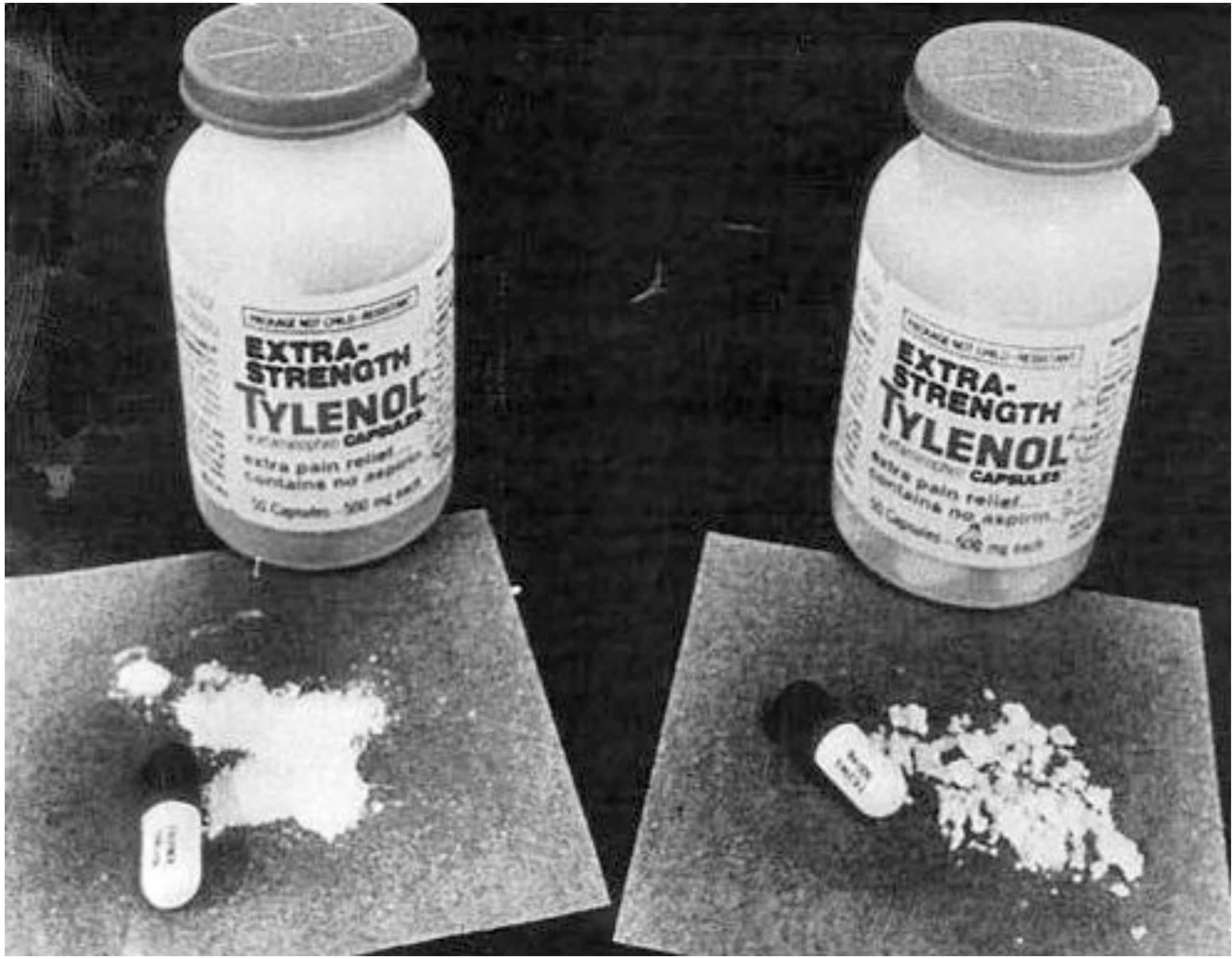


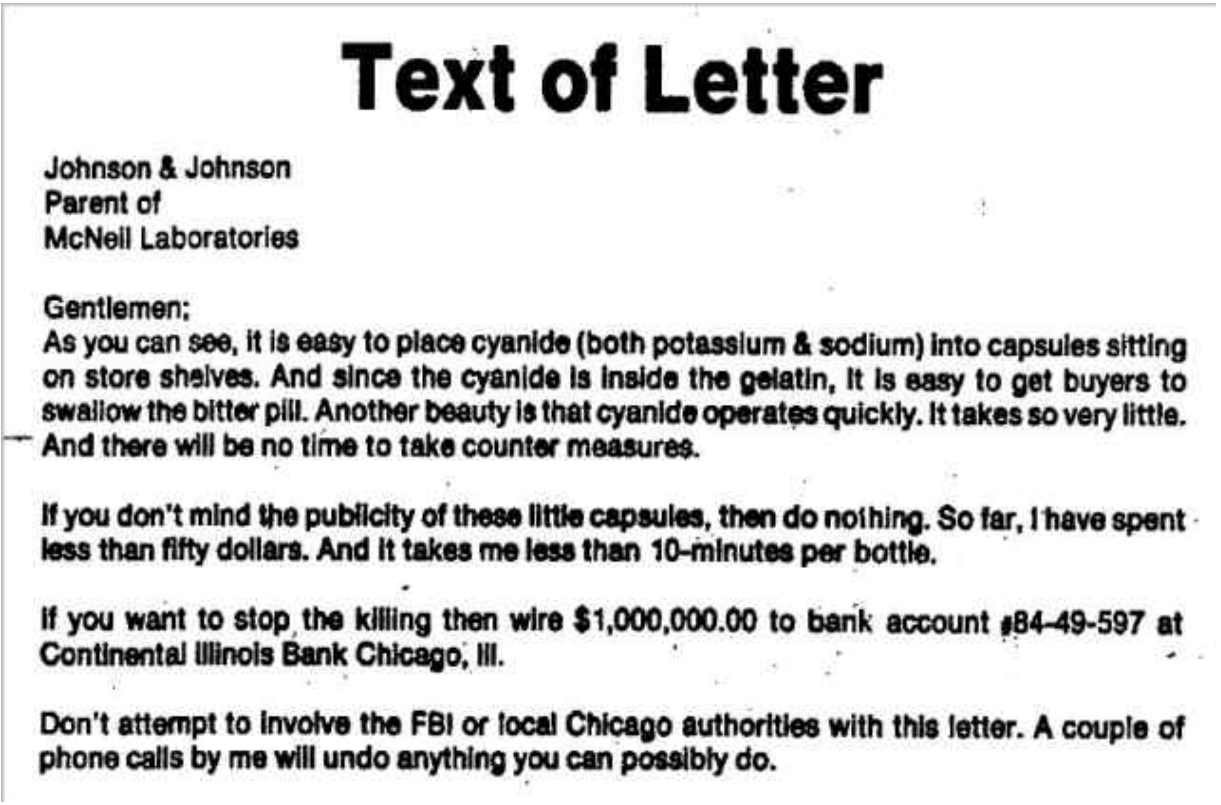


Breakout Session 1

- Get into groups (5-8 people)
- Try shimming/defeating the seal
- Try a dry break for envelope tampering
- Be creative, experiment, share what you learn with your team!
- 10 minutes!

Tamper Evident Devices





Text of Letter

Johnson & Johnson
Parent of
McNeil Laboratories

Gentlemen;
As you can see, it is easy to place cyanide (both potassium & sodium) into capsules sitting on store shelves. And since the cyanide is inside the gelatin, it is easy to get buyers to swallow the bitter pill. Another beauty is that cyanide operates quickly. It takes so very little. And there will be no time to take counter measures.

If you don't mind the publicity of these little capsules, then do nothing. So far, I have spent less than fifty dollars. And it takes me less than 10-minutes per bottle.

If you want to stop the killing then wire $1,000,000.00 to bank account #84-49-597 at Continental Illinois Bank Chicago, Ill.

Don't attempt to involve the FBI or local Chicago authorities with this letter. A couple of phone calls by me will undo anything you can possibly do.

- Cyanide-laced Tylenol Murders 1982-1986
  - Never solved, several copycat killers
  - Some bottles had broken seals
- Federal Anti-Tampering Act 1983

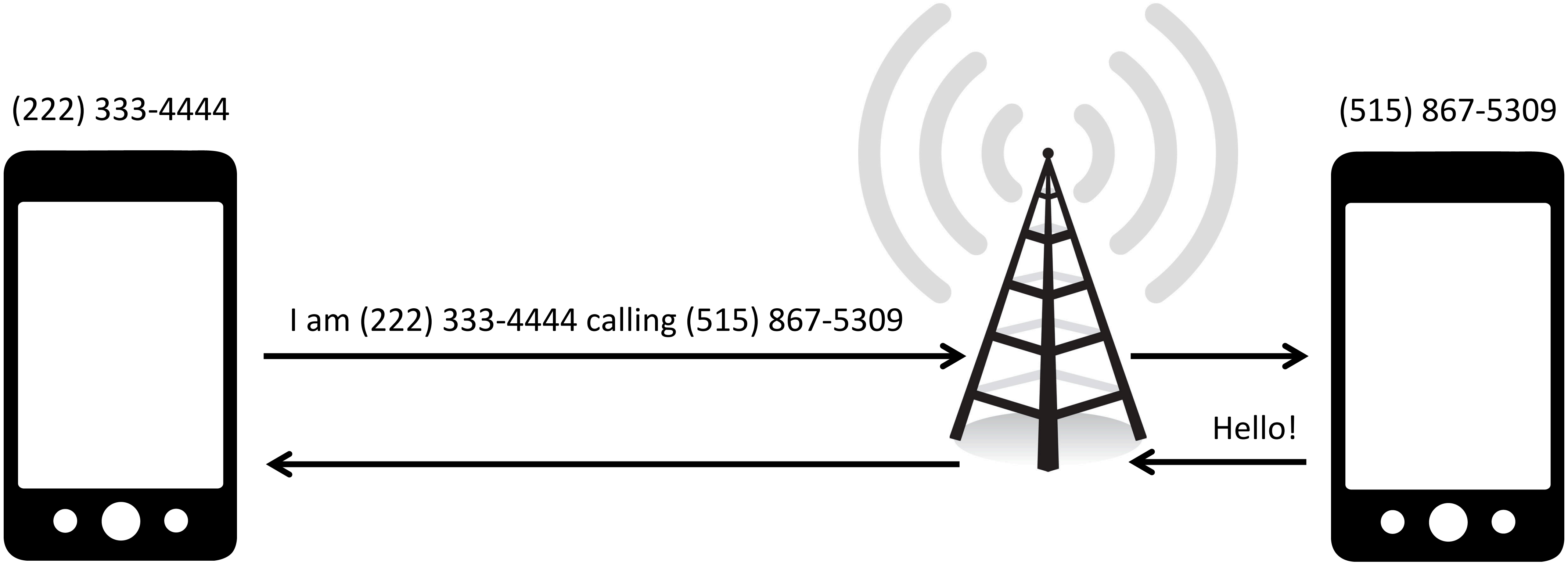
Hacking: Physical Systems

- Checkout DEFCON 19: Introduction to Tamper Evident Devices talk
  - https://www.youtube.com/watch?v=SIQml3MBJoE
- Des Moines Lock Pick Club
  - http://www.dsmlocksport.com

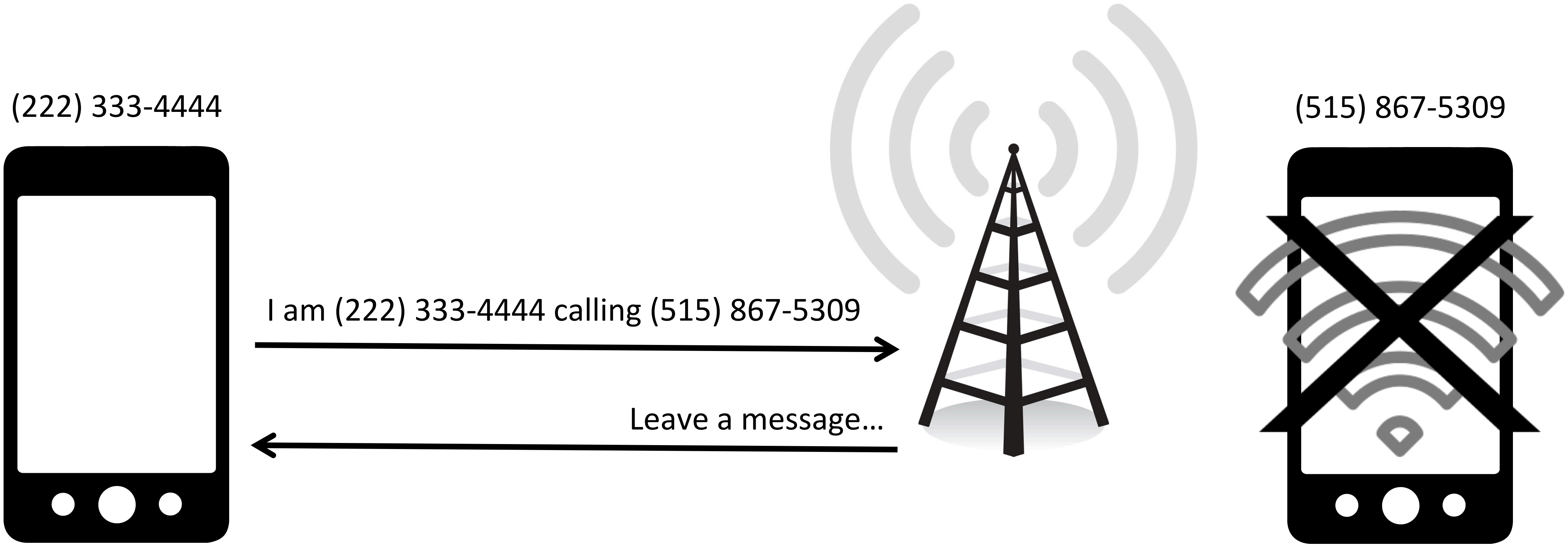
Hacking: Voicemail

- What question(s) should we ask?

How does voicemail work?



How does voicemail work?



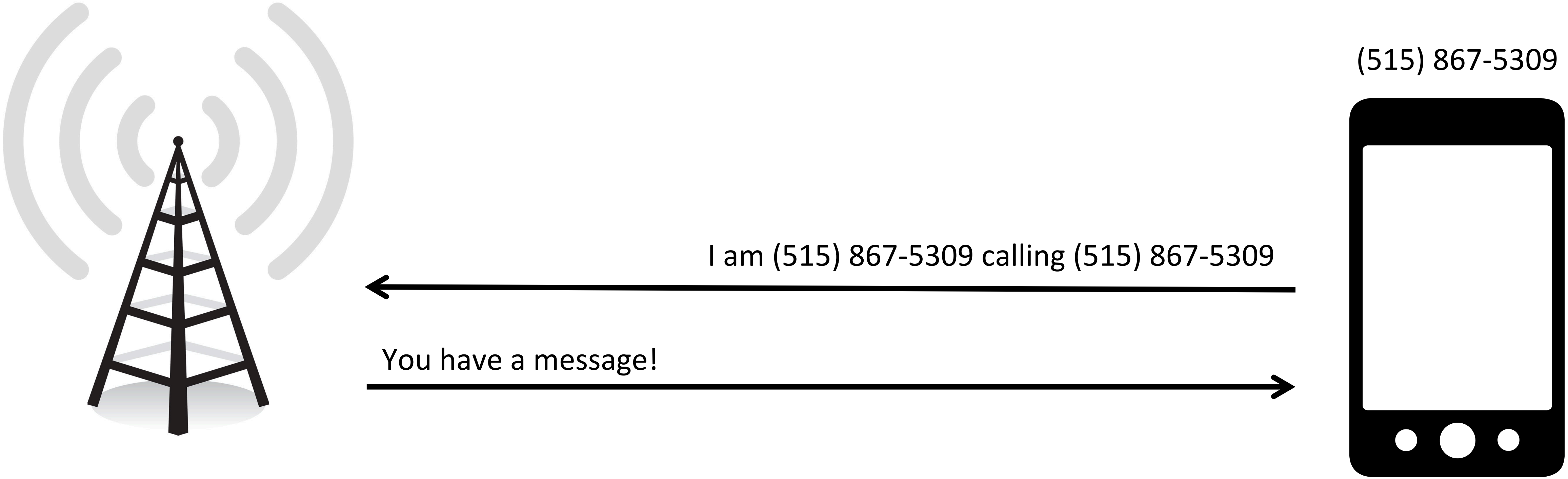
(222) 333-4444

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

Leave a message…

(515) 867-5309

How does voicemail work?

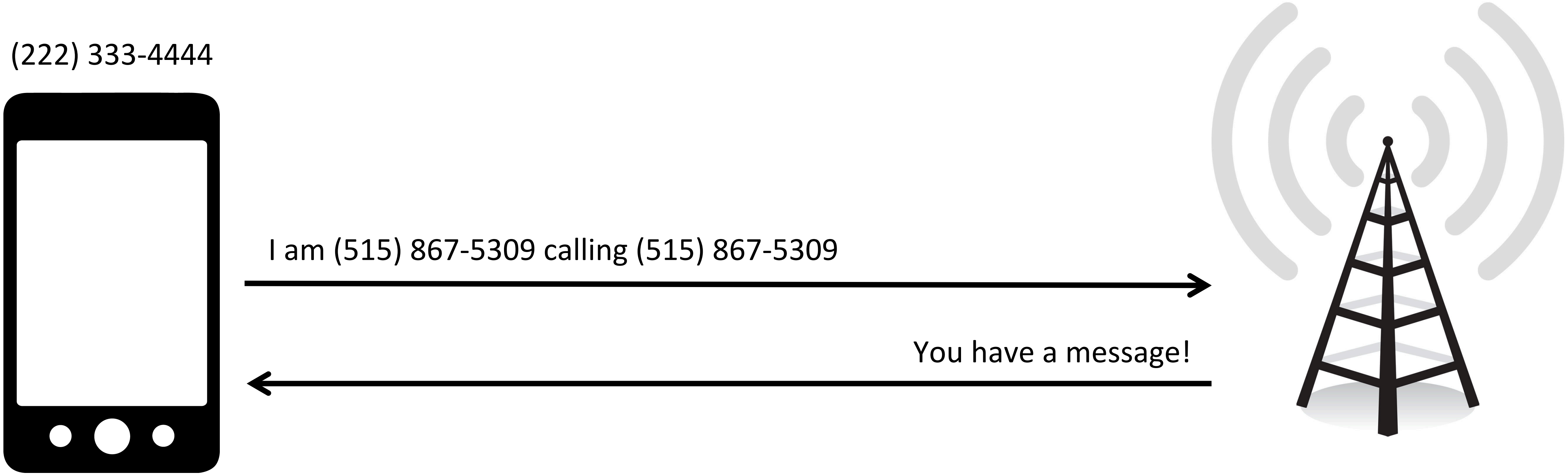


(515) 867-5309

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

You have a message!

How does voicemail work?



(222) 333-4444

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

You have a message!

Breakout Session 2

- Fake Victim: (515) 200-1301
  - https://github.com/benjholla/VoicemailVictim

- Please nominate one person per group to make spoofed calls!

- 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”.

Hacking: Social Systems

- Social Engineering
- Kevin Mitnick
  - Caught 1999 -> prison
  - Made an example of
  - No phone calls
  - Solitary confinement
  - Now does consulting

U.S. Department of Justice
United States Marshals Service

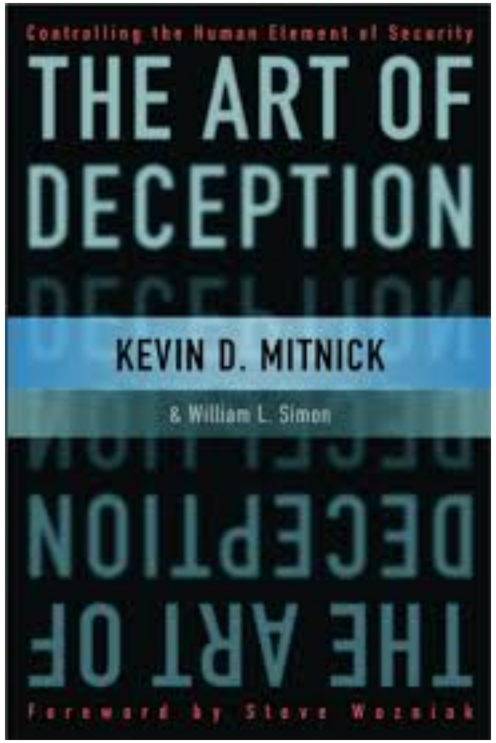
WANTED
BY U.S. MARSHALS

NAME: .... MITNICK, KEVIN DAVID

[illegible]

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

November 1992



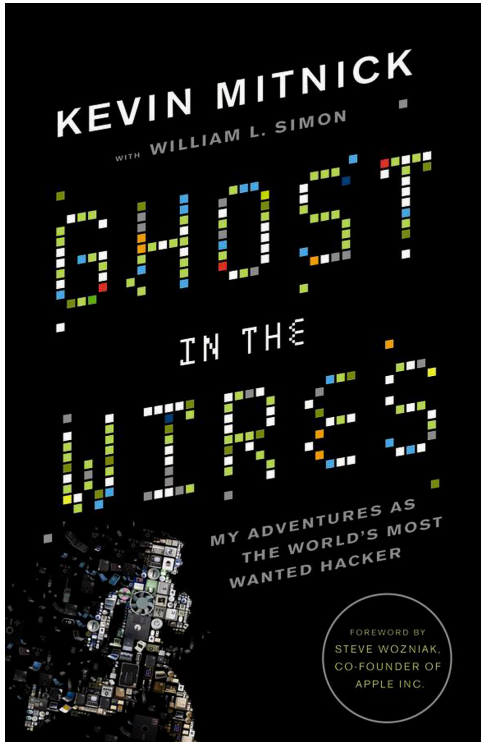
Controlling the Human Element of Security

THE ART OF DECEPTION

KEVIN D. MITNICK

& William L. Simon

Foreword by Steve Wozniak



KEVIN MITNICK

WITH WILLIAM L. SIMON

GHOST IN THE WIRES

MY ADVENTURES AS THE WORLD'S MOST WANTED HACKER

FOREWORD BY STEVE WOZNIAK, CO-FOUNDER OF APPLE INC.

Breakout Session 3

- Scenario: You work as a programmer for Facebook. Facebook pays the public for first reports of major security bugs reported (bug bounties). Facebook gets a report that a bug in Facebook allows anyone to view private Facebook accounts under rare conditions.

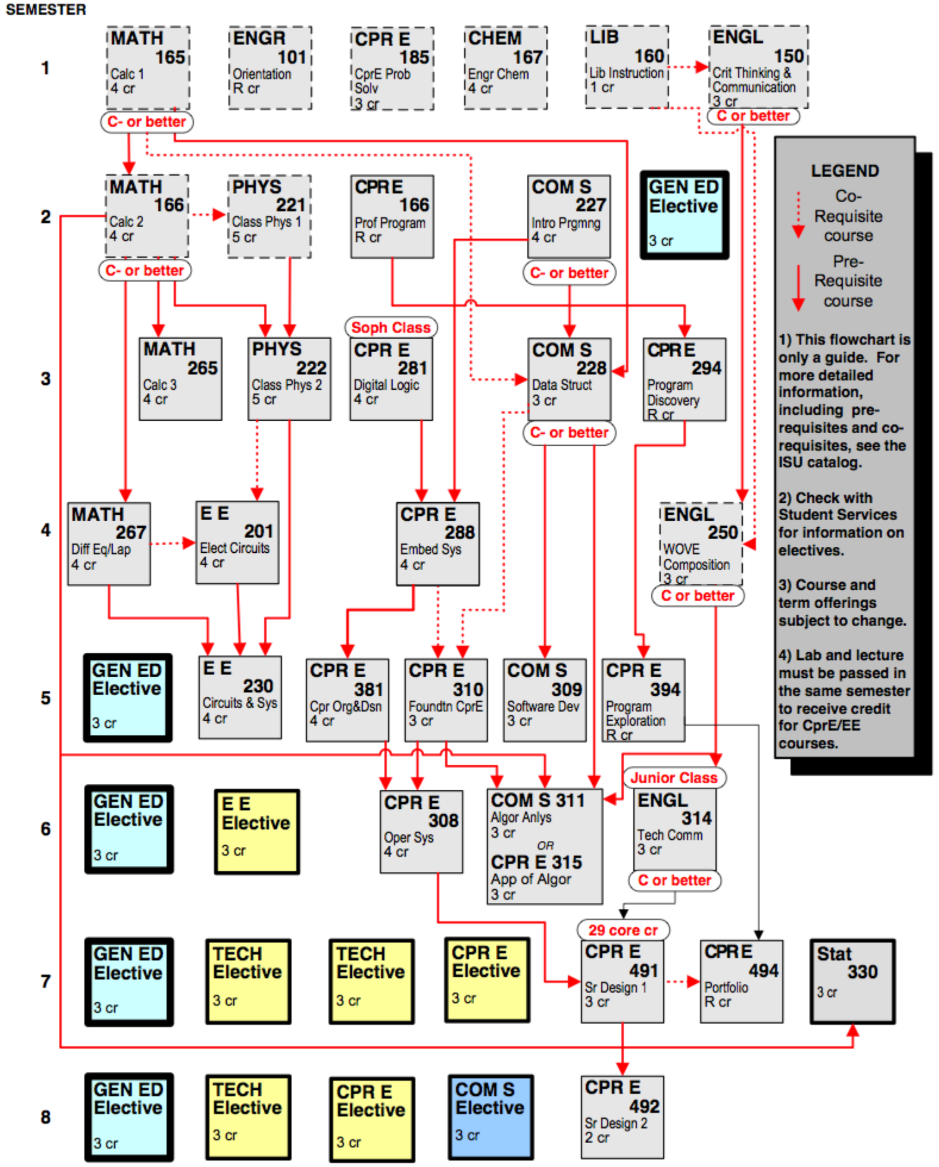
- Debate the following with your group:
  - You intentionally wrote this “bug” and sold it to your friend at Microsoft. Your friend claimed the reward money and split it with you. Is this unethical? Is this illegal?
  - You quit Facebook. After a few months you are thinking about code you wrote and realize the bug exists. Your employee contract said employees can not claim bug bounties. So just to be safe you register a fake Facebook account to report bug under and claim the reward money. Is this unethical? Is this illegal? What if you sold to the Government? Which Government?

Degree Curriculums

- Google “iastate <your major here> flowchart”
  - Computer Engineering (CprE)
  - Electrical Engineering (EE)
  - Software Engineering (SE)
  - Computer Science (CS)
  - Management Information Systems (MIS)

- Graduate Program
  - Information Assurance (INFAS)

COMPUTER ENGINEERING FLOWCHART, 2013-2014 CATALOG (127 credits)


SEMESTER
1
2
3
4
5
6
7
8
MATH 165 Calc 1 4 cr
C- or better
ENGR 101 Orientation R cr
CPR E 185 CprE Prob Solv 3 cr
CHEM 167 Engr Chem 4 cr
LIB 160 Lib Instruction 1 cr
ENGL 150 Crit Thinking & Communication 3 cr
C or better
MATH 166 Calc 2 4 cr
C- or better
PHYS 221 Class Phys 1 5 cr
CPRE 166 Prof Program R cr
COM S 227 Intro Prgmng 4 cr
C- or better
GEN ED Elective 3 cr
MATH 265 Calc 3 4 cr
PHYS 222 Class Phys 2 5 cr
Soph Class
CPR E 281 Digital Logic 4 cr
COM S 228 Data Struct 3 cr
C- or better
CPRE 294 Program Discovery R cr
MATH 267 Diff Eq/Lap 4 cr
E E 201 Elect Circuits 4 cr
CPR E 288 Embed Sys 4 cr
ENGL 250 WOVE Composition 3 cr
C or better
GEN ED Elective 3 cr
E E 230 Circuits & Sys 4 cr
CPR E 381 Cpr Org&Dsn 4 cr
CPR E 310 Foundtn CprE 3 cr
COM S 309 Software Dev 3 cr
CPR E 394 Program Exploration R cr
GEN ED Elective 3 cr
E E Elective 3 cr
CPR E 308 Oper Sys 4 cr
COM S 311 Algor Anlys 3 cr
OR
CPR E 315 App of Algor 3 cr
Junior Class
ENGL 314 Tech Comm 3 cr
C or better
GEN ED Elective 3 cr
TECH Elective 3 cr
TECH Elective 3 cr
CPR E Elective 3 cr
29 core cr
CPR E 491 Sr Design 1 3 cr
CPRE 494 Portfolio R cr
Stat 330 3 cr
GEN ED Elective 3 cr
TECH Elective 3 cr
CPR E Elective 3 cr
COM S Elective 3 cr
CPR E 492 Sr Design 2 2 cr
LEGEND
Co-Requisite course
Pre-Requisite course

1) This flowchart is only a guide. For more detailed information, including pre-requisites and co-requisites, see the ISU catalog.

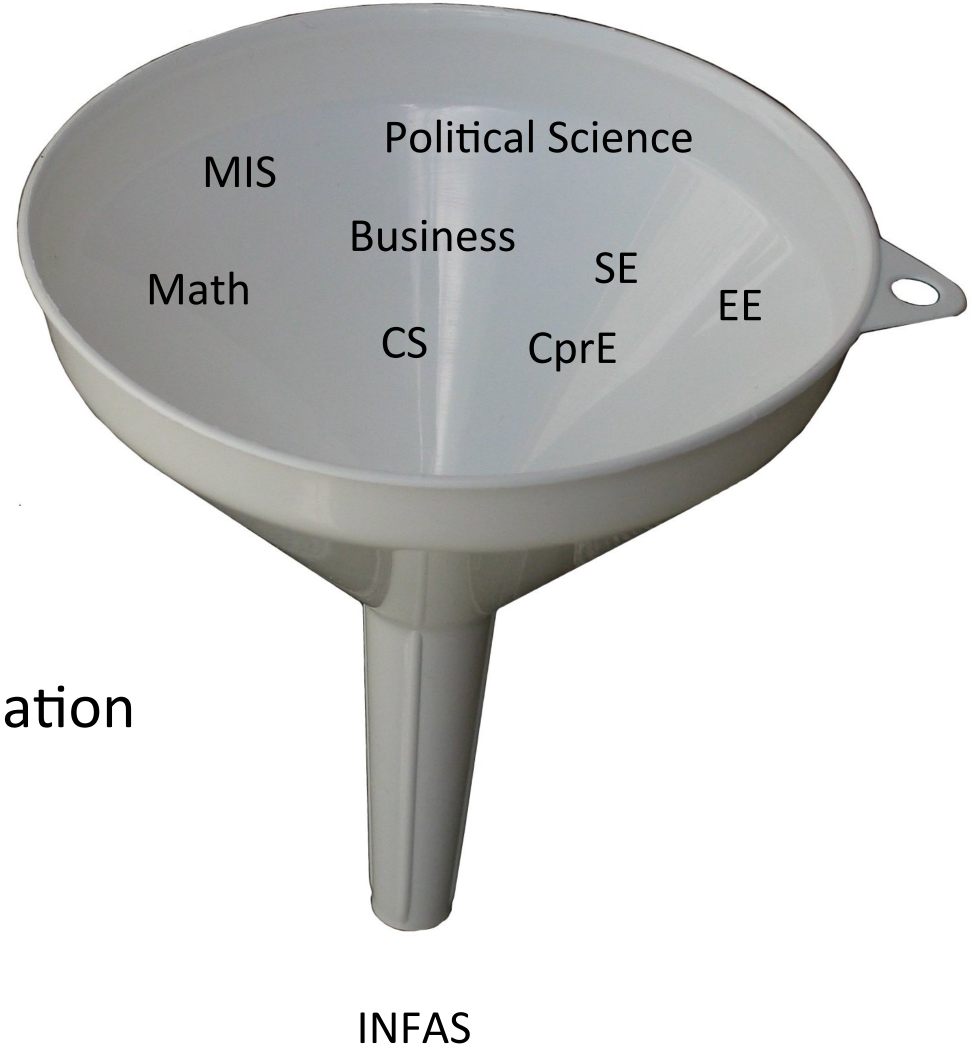
2) Check with Student Services for information on electives.

3) Course and term offerings subject to change.

4) Lab and lecture must be passed in the same semester to receive credit for CprE/EE courses.

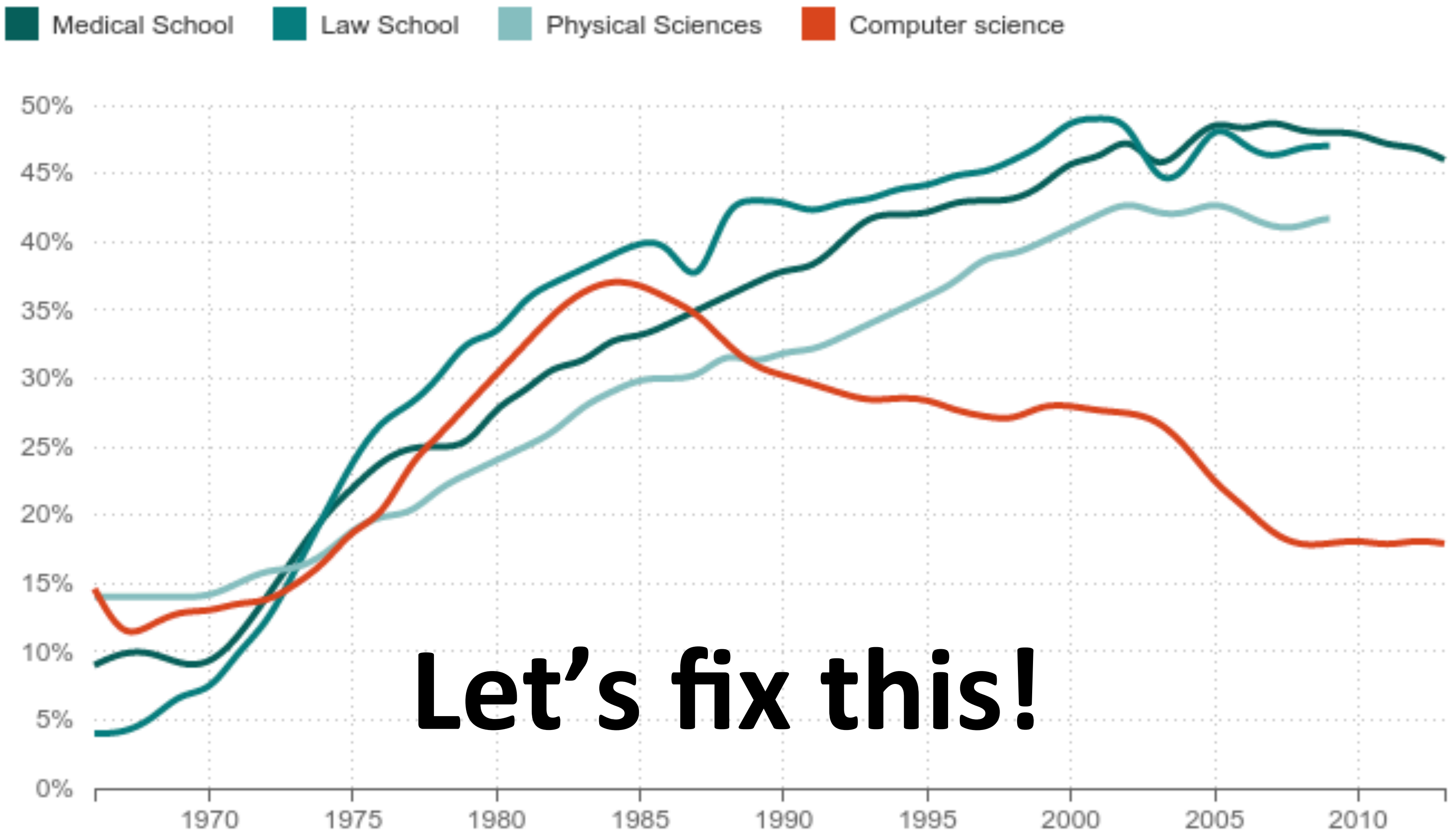
Cybersecurity @ ISU

- Masters in Information Assurance (INFAS)
  - Cryptology/Steganography
  - Reverse Engineering
  - SCADA Systems
  - Digital Forensics
  - Network/Wireless Security
  - Laws and Ethics
  - Information Warfare, Capstone
- NSA designated Center of Excellence in INFAS Education
  - Any 4 classes earns you two Gov. certifications
- Information Assurance Security Group (IASG)
  - Club open to everyone!
  - Cyber Defense Competitions
    - Class credit, hands on experience, professional Red team



What Happened To Women In Computer Science?

% Of Women Majors, By Field



Let’s fix this!

Source: National Science Foundation, American Bar Association, American Association of Medical Colleges

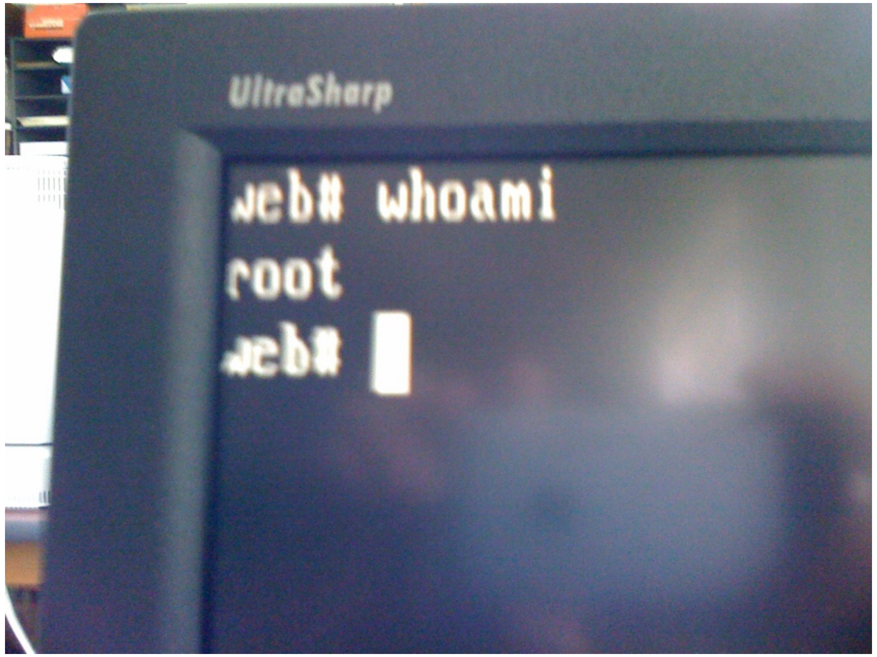
Credit: Quoctrung Bui/NPR

What do you want to talk about?

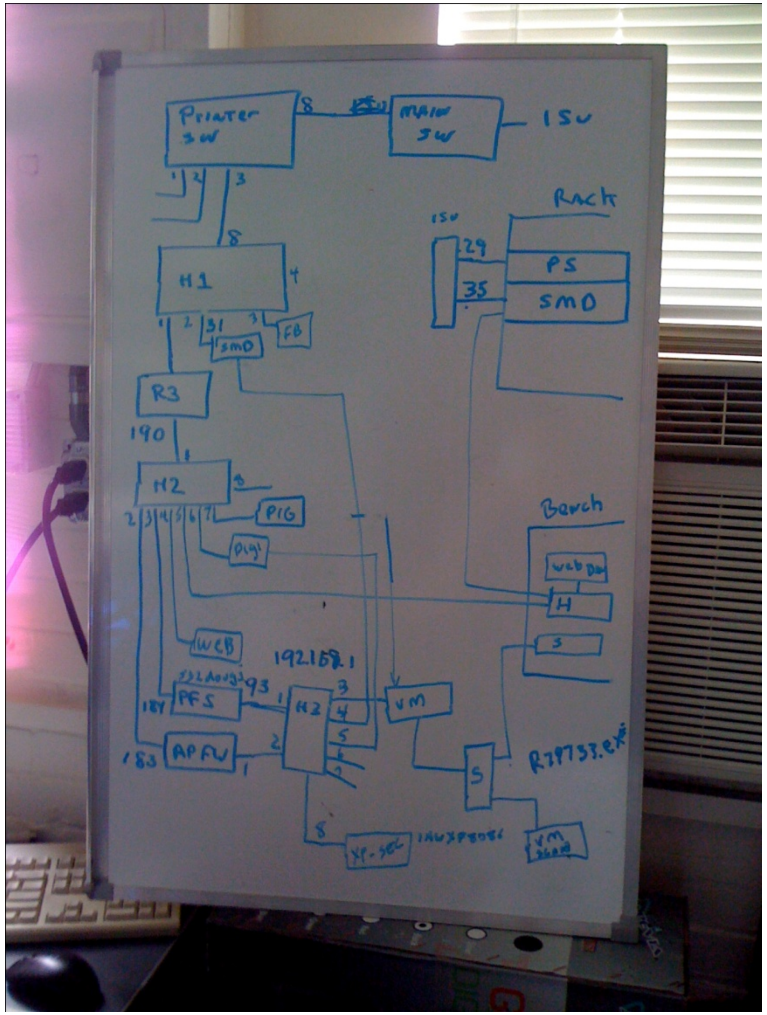
- Slides here (if you want them): www.ben-holland.com/publications
- Thanks for coming out today!
- Questions?

Information Warfare (CprE 532)

- Physical Break-in Story



```
web# whoami
root
web# █
```


Printer SW
8
MAIN SW
ISU
1
2
3
8
H1
4
1
2
31
3
SMD
FB
Rack
ISU
29
35
PS
SMD
R3
190
1
H2
8
2
3
4
5
6
7
PIG
Pig1
Bench
web Dev
H
S
WEB
192.168.1
532 Abug
93
187
PFS
183
APFW
1
2
1
H3
3
4
5
6
7
VM
S
R79733.exe
8
XP-SEC
IAWXP8086
VM Share