Engaging STEM Student Online – Lock Picking!

Debasis Bhattacharya (debasisb@hawaii.edu)
Leslie Ramos
http://maui.hawaii.edu/cybersecurity/
Supported by NSF Award # 1700562
October 22, 2020
Agenda

• Background
• Cybersecurity Education
  • Traditional
  • Across Disciplines
  • During Covid-19!
• Demo Activity
  • Lock Picking!
• Lessons Learned
• Q&A
Background - College

• University of Hawaii Maui College
  • Serves Maui County - islands of Maui, Molokai and Lanai
  • 150,000 or so resident population
  • 2 Million or so tourists per year (pre-Covid)
    • Dropped 95% after March 2020!
  • 2000+ full-time commuter students
  • 20 or so Associate Degrees
  • 3 Baccalaureate Degrees
  • 60% or so women students
  • Average of students ~25 years
  • Non-traditional students
  • Commuter island college
Cybersecurity Education - Traditional

- **Certificates in Cybersecurity**
  - Low Level - Intro, Network+, Security+
  - Higher Level - Ethical Hacking, Forensics
- **Internships**
  - Government, banks, utilities
- **Baccalaureate Degree**
  - Applied Business and Info Tech
  - Cybersecurity courses are embedded
- **Cyber competitions and Workshops**
  - NSA GenCyber, US AFA CyberPatriot
- **Supported by NSF Grants**
  - ATE Program Award# 1700562
Cybersecurity Education - Across Disciplines & Segments

- Cybersecurity educations cuts across various segments
  - Community College program disciplines
  - Gender
  - Minorities
  - Background - high schools, professionals, returning veterans etc
  - Various Industries
    - Accounting, Hospitality, Law Enforcement, Utility, Tourism etc.
- One size education does not fit all types of students!
Cybersecurity Education - Across Disciplines

- Focus on 5 disciplines at Associate Degree level
  - Accounting
  - Administration of Justice
  - Electronics
  - Hospitality, Travel and Culinary
  - Business

- Supported by NSF
  - ATE Grant, Award# 1700562
  - SFS Capacity Building Grant, Award# 1437514
Cybersecurity Education - Across Student Population

- Focus on students from a variety of backgrounds
  - Women
  - Minorities
  - Veterans
  - Working Professionals
  - High School Students
  - Remote students who rely totally on distance education
  - Economically disadvantaged
  - Low math/science proficiency
  - Non-technical
  - Non-traditional
  - Not interested in Cybersecurity as a career!
Diverse Cybersecurity Education - Overall Approach

• Obtain administration and other institutional support
• Identify key faculty leaders in key disciplines
• Engage faculty and students
  • Guest Lectures in classes
• Engage employers who will hire students with cyber skills
  • Hotels, banks, tourism industry, law enforcement
• Identify one or two existing courses in each discipline
  • Explore cybersecurity modules that can be embedded
• Hold workshop with faculty from various disciplines
  • Stipend helps!
• Create modules and help faculty member teach it!
Diverse Cybersecurity Education - Overall Approach

- Obtain administration and other institutional support
- Identify key faculty leaders in key disciplines
- Engage faculty and students
  - Guest Lectures in classes
- Engage employers who will hire students with cyber skills
  - Hotels, banks, tourism industry, law enforcement
- Identify one or two existing courses in each discipline
  - Explore cybersecurity modules that can be embedded
- Hold workshop with faculty from various disciplines
  - Stipend helps!
- Create modules and help faculty member teach it!
Cybersecurity Education – During Covid-19!

• Online education via Zoom!
  • Students were engaged as they felt safe
  • Higher attendance in classes
• Lab sessions
  • Difficult without a physical space and equipment
  • Students need to rely on their Internet connectivity
  • Cloud assignments required students to log in from their homes
• Hands-on activities
  • Lock Picking
  • Raspberry Pi
  • Pen Testing Tools from www.Hak5.org
    • USB Rubber Ducky – writing Ducky Scripts
    • Bash Bunny - Pen testing tool to emulate various devices
    • LAN Turtle – Provides stealth remote shell access
LOCKPICKING
But everything changed in 1770s with the arrival of an inventor named **Joseph Bramah** to the English locksmithing scene. Bramah was a polymath engineer who would come to be known as one of the fathers of pneumatic power. But he also applied his talents toward improving locks. He created a lock that was vastly superior to any the world ever seen. His so-called **Bramah safety lock** had layers of complexity in between the key and the deadbolt that Bramah believed made it 100 percent theftproof. Bramah was so confident in his design that he published a pamphlet detailing exactly how it worked.
A small Chubb detector lock fitted to a circa-1910 gun case.
Lockpick Village

Want to tinker with locks and tools the likes of which you've only seen in movies featuring cat burglars, spies, and secret agents? Then come on by the Lockpick Village, run by The Open Organisation Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.
Defcon: Hardware Security Starts with Lockpicking Village

By Sean Michael Kerner  |  July 29, 2012

From the ’Good Locks Make for Good Security?’ files:

LAS VEGAS. I write a lot about software security. Which is why it's always a great reminder for me to visit Lockpicking Village at Defcon.

At the Lockpick Village this year there were 6 or so main tables where attendees tried out different locks and tried to pick them. There was also a presentation area, where I have to admit I spent a tonne of time, learning about how locks really work and how to defeat them. Then there was also the vendor, selling the tools of the trades (pic left is a pic of the lockpicks for sale).

All this at the world's largest hacker convention - and the reason why is simple. Hardware hacking is just as important in many cases, as the software side. Physical security, the simple lock and key that have protected civilized persons for hundreds of years are still quite literally the lynchpin of the security industry.

Am I advocating that everyone should learn how to lockpick?
DISCLAIMER

GROUND RULES PER THE OPEN ORGANIZATION OF LOCKPICKERS (TOOOL)

1. Only pick, or attempt to pick, that which you own.
2. Do not pick any lock that you may rely on (ex: lock to your house or car)
3. The possession of lockpicking sets is generally legal throughout the United States but exceptions do exist. Local municipalities may differ so check with your local code office.

TOOOL provides a brief overview of the possession and ownership of lockpicks by state at their website, https://toool.us/laws.html
Next Steps

• Lock components
• Lock operation
• Reading lockpicking instructions
• Watching YouTube videos from experienced lockpickers
The cylinder, part of the lock, houses the rest of the components, aka shell, housing, or body of the lock. It is what slides into a door or padlock, creating the upper limit of shear line. Consider this as the "top paper."

The plug surrounds the keyway, rotates freely within the housing, creating a rotational shear line. Consider this as the "bottom paper."

The shear line is where the plug and hull casing meet. The goal of lockpicking is to manipulate the pins so that driver pins are above the shear line and key pins are still within the plug, allowing rotation and unlocking.
The opening of the lock that the key may be inserted into is called the keyway, where you are able to see key pins. The lower pins makes contact with the key upon insertion.

The top pins are called the driver pins because it is driven down by the springs, responsible for obstructing shear line and providing the locking action. Unlike the key pins, the driver pins are usually same length. Consider this as the "pencil."

The springs have two jobs: forcing everything down into the plug and push the key pins against the key, which helps read the cuts of the key. Without springs, the pins could get stuck anywhere in the pin chamber.
1. Begin by holding the lock in a comfortable manner in your left hand with the torque wrench inserted.

2. Wrap your left thumb around the bottom of the lock to provide support and your left index finger straight up to provide tension to the torque wrench.

3. Holding your pick as you would a dart, grasping it with your index finger and thumb, insert it into the lock all the way to the back.

4. As you get near the back of the lock, begin applying tension with your left index finger on the torque wrench.

5. When the pick is at the back begin to draw the pick out, pushing down gently against the key pins as you continue to provide even pressure on the torque wrench.

6. The process of pushing and pulling the pick against the pins is called raking. If the lock does not open within three to four rakes, release tension on the torque wrench and try again as it is possible that a pin has been pushed too far and is binding.
Cryptography

Symmetric

Asymmetric

Public Key

Private Key

Plaintext → Encryption → Ciphertext → Decryption → Plaintext
Online Cybersecurity Education – Lessons Learned!

• Online education via Zoom!
  • Students feel safe
  • Students learn the theory
  • Students have to provide their own Internet connectivity and laptops

• Lab sessions
  • Cloud labs work, assuming they are free and no credit cards needed
  • Lab modules need to be transferred to a cloud environment
  • Students have to know about the cloud environment

• Hands-on activities – key to engagement!
  • Lockpicking
  • Raspberry Pi
  • Pen Testing Tools from www.Hak5.org

• Students learn to adapt and survive...
Questions? Comments? Feedback?! 

Debasis Bhattacharya, JD, DBA  
debasisb@hawaii.edu  
Leslie Ramos  
maui.hawaii.edu/cybersecurity