Teaching cybersecurity across the disciplines: Using USB Rubber Ducky and BLE Beacons

Debasis Bhattacharyya
debasisb@hawaii.edu
maui.hawaii.edu/cybersecurity
HI-TEC Pittsburgh, 2016
AGENDA

● Background
● Cybersecurity Education – Traditional
● Cybersecurity Education – Across Disciplines
  ○ Overall Approach
● Case Study
  ○ USB Rubber Ducky
  ○ BLE Beacons
● Challenges/Benefits
● 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!
  - 3000+ full-time commuter students
  - 20 or so Associate Degrees
  - 3 Baccalaureate Degrees
  - 66% or so women students
  - Median age 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, NSA GenCyber
- Supported by NSF Grants
  - ATE Program Award# 1204904 (2012-15)
  - SFS Program Award# 1437514 (2015-17)
- Applied for NSA/DHS CAE CDE
Cybersecurity Education - Across Disciplines/Segments

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

- Focus on 6 disciplines at Associate Degree level
  - Accounting
  - Healthcare
  - Electronics
  - Hospitality
  - Business
  - Administration of Justice
- Supported by NSF 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
  - Highlight high tech industry examples that involves cybersecurity
- Engage employers who will hire students with cyber skills
  - Hotels, banks, tourism, hospitals, 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!
Case Study

- Target Disciplines
  - Accounting, Business, Electronics, Hospitality, Healthcare

- Fall 2015
  - Guest Lectures
  - Industry Examples - Hotel Digital Key, BLE Beacons, Kanisa Thermometer
  - Competitions - USB Rubber Ducky, USAF CyberPatriot, NSA GenCyber

- Spring 2016
  - Target two courses - introductory, intermediate/advanced

- Early June 2016
  - All Day Faculty Workshop (summer overload)
  - $250 stipend, supported by NSF SFS Award# 1437514
  - Finalize target courses for Fall 2016, discuss security modules/labs

- Fall 2016 and Spring 2017
  - Create cybersecurity modules and embed in existing courses
  - Modules are based on KUs from NSA/DHS CAE CDE program
USB Rubber Ducky

Keystroke Injection Tool
By www.Hak5.org

Buy from ($45 each)
http://hakshop.myshopify.com/

YouTube Demo - https://www.youtube.com/watch?v=sbKN8FhGnqg
Micro SD Storage
Replay Button
LED Indicator
Type A Plug

60 MHz 32-Bit CPU
Covert Case
Optional Decal

Source: http://usbrubberducks.com/
DUCKY SCRIPT

Ducky Script. Simply Simple.

The USB Rubber Ducky's scripting language is focused on ease-of-use. Writing payloads is as simple as writing a text file in notepad, textedit, vi or emacs.

- Type "Hello World" with STRING Hello World
- Add pauses between commands with DELAY.
Use DELAY 100 for short 100 milliseconds pauses or DELAY 1000 for longer 1 second pauses.

- Combine specials keys. ALT F4, CONTROL ESCAPE, WINDOWS R, SHIFT TAB. They all do exactly as expected.
- Use REM to comment your code before sharing it.
  - That's it! You just learned Ducky Script!
Sample Student Competition: Quack-A-Thon

- **Target Students**
  - New to cybersecurity, basic computer knowledge, high interest level
  - High schools, middle schools, college students, non-IT students

- **Competition Format**
  - Form teams of 3-5 students
  - Set aside 4 hours for training/coding, plus 20 minute presentations
  - Provide grading and scoring rubric to all teams

- **Provide basic training and one USB Rubber Ducky per team**

- **Students write, encode, load and deploy Ducky Script!**
- **Students present their payload and project to judges...**
Introduction to Rubber Ducky

The Rubber Ducky is a microcontroller USB that acts like a keyboard when plugged into a computer. It executes a set of instructions that you load into it; however, it is not possible to load other kinds of executables into the Ducky and have the victim computer run them. When creating a Rubber Ducky executable, you have to pretend you're at your victim's computer typing. You can do anything with the Rubber Ducky that you could do with a keyboard, such as opening a command line or powershell and running a few commands for example, so the possibilities are nearly endless.

Source: http://uhmc.github.io/Ducky_Demo/
Repository for hosting the Rubber Ducky demo resources. — Edit

- 5 commits
- 2 branches
- 1 release
- 2 contributors

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
<th>Latest Commit</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>README.md</td>
<td>Initial commit</td>
<td>63f6962</td>
<td>May 6</td>
</tr>
<tr>
<td>Rubber-Ducky_Declaration-of-Judging-Criteria.docx</td>
<td>Add resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rubber-Ducky_Declaration-of-Judging-Criteria.pdf</td>
<td>Add resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welcome to the 2016 Quack-a-thon.pdf</td>
<td>Add resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welcome to the 2016 Quack-a-thon.pptx</td>
<td>Add resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>security-quizzer-v1.0.apk</td>
<td>Update zip with latest app release</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: https://github.com/UHMC/Ducky_Demo
Welcome to the Duck Toolkit

This website allows you to choose from pre built payloads, create your own payloads and decode existing payloads for the Hak 5 USB Rubber Ducky.

The site contains 30 scripts you may select individually or combine to make whatever payload you require.
The Physical Web

- Everyday objects with ability to interact with the Internet, mobile devices
  - Smart TVs, Refrigerators, Microwaves etc.
  - Provides information, status etc.

- Bluetooth Low Energy (BLE)
  - New protocol to transmit information
  - Low power, short distance

- Beacons!
  - Many Vendors: Estimote, Radius Networks, BKON
The Physical Web is an open source approach to unleash the core superpower of the web: interaction on demand. People should be able to walk up to any smart device - a vending machine, a poster, a toy, a bus stop, a rental car - and not have to download an app first. Everything should be just a tap away.
So, what is a Beacon anyway?!

- Small transmitter device
  - Sold by many small/large companies
  - Uses Bluetooth Low Energy (BLE)
  - Uses batteries (cell, AAA etc.)
  - Long battery life (years)
  - Price ranges from $10-$30
  - Advertises itself on a regular basis
  - Recognized by mobile phone apps
  - Transmits when a receiver is close (proximity)
  - Small size data transfers
  - Unique Beacon ID, can be managed remotely
So, how does it work?

• Beacon Advertisement
  – Regular transmissions of UID etc.

• Receiver in Proximity (Range)
  – Typically a smartphone with app
  – Many vendors have beacon apps
  – Google Play: The Physical Web
  – iTunes: The Physical Web

• Beacon Transmits Data
  – Ex. Eddystone URL resolves URL on mobile app
How does it work?
Beacon Scan

Do you work with beacons with iBeacon Technology or Physical Web Beacons? Then download Beacon Scan, and see all the information you need about nearby beacons.

Feature Set:

- See nearby beacons!
- Supports both iBeacons and Physical Web Beacons!
- Copy hard to type UUID and other beacon identifiers!
- Works great with the best beacons on the market, Bleu Beacons from Twocanoes Labs...

...More
OK, so what?

- Beacons provide proximity info
  - Beacons are not connected to the Internet
  - They provide “nearby” information
  - Receiver does [will] not need any app
    - Google in integrating beacon info in Android
    - Somewhat similar to searching for Wi-Fi
  - Beacons can be associated with objects
  - Or, locations, people, animals etc. etc.
  - Beacons = Physical things + Web
Case Studies

**Retail**
Attract, engage and understand your customers. Deliver exact information, not mass messaging.

**Tours**
Provide visitors with customized guided tours, including food and entertainment ideas.

**Trade Shows**
Provide interactive maps, seamless check-in, attendance details and relevant schedule updates.

**Healthcare**
Improve efficiency and generate data as proof of compliance. Engage families and staff relative to proximity.

**Real Estate**
Enrich house hunting experiences. Provide far greater detail, serve up listing content, boost realtor efficiency.

**Events**
Improve experience and increase engagement by analyzing traffic and making real-time campaign changes.
BLE Beacons Demo

• Beacon Vendors
  ○ Estimote and BKON

• Beacons are ready to go!

• Web Management
  ○ https://cloud.estimote.com/
  ○ https://www.phy.net/beacons/
  ○ Setup Beacon information, URL, Geolocation, Transmission Strength etc.

• Track Analytics
  ○ New customers, recurring customers
  ○ Dwell time, stats by location, beacon tag

• Obtain telemetry (Eddystone-TLM) information on beacons
  ○ Battery level, frames transmitted, active life, temperature etc.
phyID
qFJLxL

Alias
HI-TEC Conference Beacon

Notes
Beacon for Conference

Custom Destination URL
http://www.highimpact-tec.org/

Default Proximity (Beta)
- Immediate
- Close
- Far
- Deactivate Range Control

Information below is a sample preview of how this content may be seen in a Physical Web Browser. Due to screen size, operating system and system settings, content may display differently on your device.
Sample Reports

Analytics

Last 4 weeks

Visits
21,763
up 1%

Unique Visitors
12,391
0%

Average Dwell Time
00:21:52
down -5%
Beacons - Challenges

- Remote Management
  - Locations need to be mapped
    - Somewhat similar to deployment of WAPs
  - Need to be managed
    - Weather, battery life, status
  - Transmittal URL information
    - Needs to be current and updated

- Costs
  - $10-$30 per beacon can get expensive
  - Time and cost for IT to manage beacons and content
Beacons - More Challenges

- Current State of Beacon Security
  - Nothing!

- Unauthorized Tracking
  - Any receiver can track a beacon UID and Location

- Forgery
  - Adversary can forge the advertisement UID

- Showrooming
  - Adversary can insert competing info in beacon data
Beacon Security - Eddystone Ephemeral ID (EID)

- Google’s new Eddystone Ephemeral ID
  - Every beacon has a private symmetric key
    - Known only to the owner of the beacon
  - Unique Beacon Ephemeral ID (EID)
    - Symmetric key + pseudo-random function of Beacon clock
  - Unique Beacon EID needs registration
    - Global online trusted resolver of Beacon IDs
    - Sharing permission policy allows other to connect
  - Receiver securely connects to a Beacon when...
    - Smartphone receives Beacon EID
    - Sends EID to the cloud/global resolver service
    - Cloud/global service matches EID with registered keys
Overall Challenges

- Faculty members need to be open and interested!
  - Cybersecurity does not appeal to all
- Faculty members need to see value
  - Inserting course modules within an existing syllabus and timeframe
- Students need to see value!
  - See cybersecurity as a means to enhance job/career opportunities
- Embedding new courses and projects takes time and work
  - Faculty member needs time off existing work to create new modules
- Ongoing training to ensure new faculty can learn InfoSec
  - Making this sustainable requires one-two years of effort
- Administration needs to be behind all this effort!
Benefits!

- Handson projects engage diverse students with fun work!
- Cyber savvy workforce can come from various disciplines
- Increase interest in cybersecurity from a diverse group
- Grow the overall awareness of cybersecurity defense
- Enhance ability of non IT faculty to teach cyber topics
- Requirement for NSA/DHS CAE application

6. Cyber Defense is a Multidisciplinary practice at the Institution
The institution must demonstrate that CD is not treated as a separate discipline, but integrated into additional degree programs within the institution.
Questions? Comments? Feedback?!

Debasis Bhattacharya
debasisb@hawaii.edu
maui.hawaii.edu/cybersecurity