Title: Safe and Sound: The Physics of Hacking

Length of Course: Full Year (2 semesters; 3 trimesters; 4 quarters)

Subject Area – Discipline: Laboratory Science (“d”) – Physics

CTE Sector: Information and Communication Technologies

CTE Pathways: Networking & Software and Systems Development

Grade Level(s): 11-12

Course Overview:

The “**Safe and Sound: The Physics of Hacking”** course is designed as a 11th-12th grade advanced Science, Technology, Engineering, Mathematics (STEM) class that integrates important physics concepts and principles with their use and necessity within the Information and Communications Technologies (ICT) sector and Next Generation Science Standards (NGSS). Because cybersecurity courses at this level should focus on the fundamentals of computer science and ICT, the beginning of the course weaves programming basics with practical physics to introduce foundational knowledge that that will lead to an exploration and understanding of cybersecurity in later units. In those later units, students will learn how an understanding of physics allows for a deeper theoretical understanding of and ability to solve problems related to cybersecurity and the protection of information systems. Students will be introduced to requisite high school physics topics such as: kinematics (motion), waves, energy, heat, and forces (mechanics), while learning to utilize key programming, computer science, and, ultimately, cybersecurity foundations and applications. The course is designed to specifically allow students to develop career awareness, skill acquisition, and preparation for postsecondary education and careers for the multiple professional pathways found within the ICT spectrum. Throughout the course, students will become familiar with information and communications technology, coding, data transmission and networks, cyber-hygiene, ethical hacking, and real world applications.

Course Content:

Unit 1 - Programming and Kinematics

This foundational unit sets the stage for the study of cybersecurity and physics in the later units. Computer and network technologies and the digital representation of information is the key difference between security and cybersecurity. The effective understanding of cybersecurity rests upon an understanding of computers, networks, and digital data, and computer programming is an essential skill for cybersecurity workers. The relationship between physics and computer hardware is readily recognized because the electronic devices that make-up the physical computer are governed by the laws of physics. Computer software, however is considerably more abstract and more difficult to relate to the laws of physics. This unit makes that connection by using programming knowledge and skills to solve physics problems, and therefore builds foundational knowledge in programming and physics that will be connected to cybersecurity in later units.

The first assignment guides students to make ethical decisions related to cybersecurity, an indispensable first step in cybersecurity education. Then, a foundation of kinematics and programming will be developed that culminates in a final assignment in which a student-created program will be used to predict the distance traveled by a projectile shot from a student-made catapult. Students will learn the basics of coding and programming with the introduction of binary code to understand data and its origin. This will then progress to manipulating data to deliver instructions to a computer in the form of a simple program to create movement. Online resources may be utilized to help students make the connection between the instructions they create and the subsequent character movement. Kinematics will help the students understand the physical laws that govern motion and help them program movement. Students will explore force and motion in both the horizontal and vertical directions, culminating with an understanding and application of projectile motion. Students can then test real world data against computer generated predictions.

Unit 1- Assignments

1. White Hat / Black Hat Hacking Research Opinion Paper

In the world of cybersecurity, a hacker is someone who searches for weaknesses in computer systems or networks in order to exploit them. Hackers may be motivated by a plethora of reasons such as protest, profit, enjoyment, or to assist in removing weaknesses from a system. In this lesson, students will research the origins of hacking and write both pro and con arguments for the problems and benefits of hacking. Students will explore the usefulness and utility of White Hat hacking to improve systems or networks and how it can be extremely useful to mitigate malicious attacks and protect critical infrastructure. Students will then review properties and activities of Black Hat hacking and how it is used to break into servers and systems with malicious intent. In some cases, whether the hacking is black hat or white hat can be simply a difference of perspective. Finally, students will examine the overall ethics involved in both types of hacking and debate their opinions. Students will sign a white hat contract.

2. Coding Vectors: Introduction to Binary Coding

In this lesson, the students learn about the binary number system and its importance to coding. Groups of binary digits (bits) are used in digital systems to represent more abstract information such as letters, words, sounds, and pictures. An activity such as "Binary Baubles" will be utilized to introduce these concepts (http://code.org/files/CSEDbinary.pdf). Given a reference chart for the American Standard Code for Information Interchange (ASCII) symbol set, students will complete a worksheet converting characters from alpha to ASCII and back again. After the brief introductory coding activity, the students will draw and code a vector game map using simple programming softwares such as Scratch, code.org/learn, and Khan Academy. Students will receive a maze in which they must create ordered vectors to move a character from a start point to a finish point. Once they have created the vectors to achieve the goal, they will then turn those vectors into code and create a simple program to animate a character across the maze(vector game map) to the finishing point.

3a. Programming

Building on the simple coding from assignment two, students will now be introduced to programming languages and software creation tools. This work also prepares students for the more complex programming required in assignment four. The students will create a simple program that converts units of measure using a high level language such as Python or VB.net. Students will then be able to use this program for the rest of the year as they complete their other activities and assignments. Students will research the wide application of computer software in modern devices and write a paper discussing their findings.

3b. Projectile Motion Lab

Students will explore projectile motion and learn to calculate both the vertical and horizontal components of projectile motion using kinematic equations. Using a marble and a ramp, the students will measure the horizontal distance of the projectile rolling off a table. The students will then calculate the horizontal distance the projectile traveled using kinematic equations relating time, distance, and velocity. They will then compare the actual numbers recorded with the theoretical calculated numbers to obtain a percent error. A write up will explore the numbers calculated and discuss any differences that led to an abnormal percent error. The calculations and equations used in this lab introduce students to the kinematic and projectile motion equations they will need for their final assignment in this unit.

4. Catapult Coding - Unit One Capstone

In this lesson the students will build a functional catapult to investigate key physics concepts and strengthen computational abilities. The catapult will launch a small, marble-sized projectile to hit a target at a fixed distance. Theoretical calculations will first be made to measure angle of launch and distance to be traveled. The catapult will then be set according to these calculations and the actual distance will be measured and recorded by the students. Students will also write a program to predict the distance a marble will travel if catapulted from a fixed position. They will then compare the hypothetical results from the program to the actual results produced by the catapult. Source code and findings will be communicated in a lab report.

Professional Community

In this activity, the students will have an opportunity to communicate and learn from professionals from related disciplines from local professionals and online community. An ideal guest speaker would be a working physicist, programmer or ballistic expert who can further educate the students in the related career explorations and advising. Through these speakers, the students will get a glimpse of the teamwork necessary to work in a professional setting to develop a useful product. Students should complete a writing assignment at the end of each presentation that identifies the key physics and cyber security concepts discussed as well as making connections to their real lives.

Unit 2 - Information and Communications Technology

Information and communications technology (ICT) involves an interplay of computational hardware and logical processes that are built upon a foundation of physical laws. In this unit students will continue to build foundational knowledge by exploring answers to the question, “how does the application of electrical principles from physics underlie the development of communications and information systems?” Cybersecurity ultimately involves protecting these information systems and the data they contain.The goal of this unit is for students to both master key physics principles involving circuits and thermodynamics and then apply this knowledge to understand the foundations for the origin and development of today’s modern operating systems. In the unit students continue to refine programming skills begun in unit one by learning to utilize application program interfaces.

Unit 2 - Assignments

1. **Analyzing Circuits**
   In this activity students will build various series, parallel, and compound circuits using wire, batteries, switches, and resistors. Students will use a digital multimeter to measure current, voltage, and resistance at different points in each circuit. By adding in additional resistors students will experimentally determine the behavior of electricity in circuits. The students will record their measurements, draw circuit diagrams for each circuit, and make calculations using Ohm’s Law (V=IR) and the electrical power equation (P=IV) to compare their experimental measurements to calculated values for each circuit. Further investigation of circuits can be made using online simulations (https://phet.colorado.edu/en/simulation/circuit-construction-kit-dc) or by developing a simple computer program able to make electrical calculations. Once the students have an understanding of circuits, they will research and write a report the application of circuits into the components and connectivity of motherboards. This work prepares students for assignment three in this unit.

2. **Transistors and Computer Chips**

Transistors are the building blocks of computer chips. In this activity students will expand upon their understanding of circuits by investigating the role of a transistor in moving from electric circuits to electronic systems capable of logical computations. Students will use a phototransistor and a breadboard to build a simple device capable of turning on a light-emitting diode (LED) in response to an input light (see http://learn.parallax.com/node/255 for an example). After completing this investigation students will research Moore's Law. This will lead to a project where students investigate the design of various integrated circuits at different points in time. As part of this project students will focus on the critical role of heat generation as a design constraint in chip development. This heat is a form of entropy as energy is lost to the system. For each chip students will calculate the efficiency of the chip based upon its heat generation. As a final reflection students will make the connection between transistors and the development of the computer chip in shaping modern society.

3. Preparing a Single-board Computer

Students will build upon their knowledge of understanding of circuits, transistors, computer chips, and programming by preparing a single-board computer (SBC) and creating a program. This is a laboratory activity that should be completed by small groups of students. Students will search the Internet to find online resources for the SBC that they will be using. Using this information each team should:

1. Download the selected Operating System to the SBC boot medium
2. Assemble the hardware including connection to the breadboard that will support various student electronic circuit projects. Students will observe basic power-on sequencing and interpret LED indicators.
3. Connect to the local area network (LAN).
4. Verify Internet connectivity
5. Install software development system
6. Verify setup by writing, compiling, and executing a simple program, such as "blinky" that will activate the student created electronic circuit on the breadboard.

Students will provide a source code listing of the program that they wrote. Students write a reflection or report that summarizes and explains the physics principles which allow the computer to work and informed their building of the computer.

4. System Hardening

Computer Systems are designed to work with a broad range of applications. This flexibility means that there are many configuration options and inevitably many possibilities for configurations and operational modes that increase the vulnerability of a computer to attack (attack surface). In addition, hackers actively attempt to discover and exploit weaknesses within the operating systems and application programs. Systems must be hardened to protect them from these types of attacks. Using the computer they built in assignment three, students will work in groups, using open source software to identify vulnerabilities in SBCs and take mitigation steps to harden these systems against the identified vulnerabilities.

Students harden their systems while other students find vulnerabilities. Students should produce a table listing the vulnerabilities identified, the penetration testing tool that identified the vulnerability, the mitigation applied, and any additional observations. Though this assignment does not incorporate physics, it builds in essential knowledge used in the final unit project.

5. **PIO Programing**

   In this assignment, the students will strengthen their understanding of current electricity by creating and coding an application program interface. The students will apply their knowledge of electric potential difference, electric current, electric resistance, circuit connections, and other related physics concepts to build and control an external breadboard circuit using the single-board computer (SBC) with programmed input/output (PIO) capabilities.

   The students will build and code automated circuit connections using either series or parallel circuits and their knowledge of Ohm's Law. The students will use circuit symbols including battery, connecting wire, resistor, and switch to construct a schematics diagram of their circuit. In addition to the diagram, the students will turn in a schematic diagram detailing their choice of circuit and its effects upon the electrical quantities such as electric potential, resistance, and current. Sample activities could be:

   https://www.arduino.cc/en/Tutorial/Blink?from=Tutorial.BlinkingLED (for the Arduino)

   http://www.instructables.com/id/Raspberry-Pi-Python-scripting-the-GPIO/step6/Blink-an-LED-in-Python/ (for the Raspberry Pi).

6. **Professional Community**

   In this activity, students will have an opportunity to communicate with professionals in the area or online community forums/discussions so they can learn from professionals in the related disciplines. An ideal professional community would be system administrator specialists who can further the students knowledge of the process of hardware, softwares, and network installations in the related career explorations and advising. Through these speakers, the students will get a glimpse of the teamwork necessary to work in a professional setting to develop a useful product. Students should complete a writing assignment at the end of each presentation to identify the key physics and cybersecurity concepts discussed as well as making connections to their real lives.

Unit 3 - Network Security and Information Transmission

Given the worldwide connectivity of the Internet, the computer network is an obvious hacker target. In this unit students understand how computer networks are attacked by hackers and how the physics of information transmission influences the hacking approach. A common approach to penetrating a computer network is to gain physical access via the network media and exploiting weaknesses in the communications protocols. There are three major types of network media: copper wire, air, and fiber optics. Physics concepts such as magnetic induction, the properties of waves, and Snell's Law help students to understand both the physical data transmission and the hacker's exploitation techniques. Once hackers have access to the data stream, they can either simply interfere with the signal (jamming), listen to the information (eavesdropping), or replace the original data with malicious data (man-in-the-middle). Through various labs students investigate various physics principles (i.e. Snell's law and the relationship between wavelength and frequency) that make it worldwide connectivity possible at the same they make it a security target. Students engage in a WiFi sniffing activity to broaden and extend their understanding of electromagnetic waves, set up a computer network to investigate firewalls and data transmission via electromagnetic waves, and finally using their programming knowledge to write a program that transmit morse code signal using a laser.

Unit 3 - Assignments

1. Wavelength / Frequency Lab

WiFi uses radio waves to transmit information. Different WiFi standards and channels operate within different radio frequency bands and at different radio frequencies. Students will examine the relationship between wavelength and frequency using a slinky to create both longitudinal and transverse waves. Changing the wavelength of the slinky will consequently change the frequency and the students will create graphs to measure these changes to plotting the relationships using the formula for wave speed. An oscilloscope will also be utilized to create a visual relationship between pitch and wavelength. Information from this assignment will be recorded in a laboratory report.

2. Refraction Lab

Snell's Law will be examined as students measure the refraction of light as it transfers from air to a glass lens. The angle of refraction will be measured as light transfers from one media to another and numbers will be plugged into Snell's Law to solve for the index of refraction for glass. These computed numbers will be compared to the known index of refraction for glass. The application of these principles explains fiber optic cable construction and operation. Building upon this understanding, students will investigate the techniques for encoding information within a light stream and how this is used in contemporary Information and Communication Technology (ICT) systems. Information from this assignment will be recorded in a laboratory report.

3. Magnetic Induction Lab

To understand the susceptibility of copper wire circuits to eavesdropping, students will understand how induction works through a simple lab in which a spinning magnet will be used to spin a can acting as a coil. The moving magnetic field will induce an electrical current in the can which creates its own magnetic field opposing the field of the spinning magnet. The students will research and develop a schematic drawing for a conceptual device that uses magnetic induction to eavesdrop on an ICT data stream across a twisted-pair cable. Working in a lab, students will use a network tap and network packet capture program to observe the actual data travelling across the network. Students will then prepare a position paper on the value of encrypting data in motion even when travelling across a “secure medium.”

4. WiFi Sniffing Activity

Electromagnetic waves exist all around us and can be used to transmit information; radio, cell phone, television, hotspots, and WiFi. All traffic on a network is naturally received by all computers capable of accepting signals on that network -- WiFi or waves are inherently a security risk because of their accessibility by those within range. In this lesson students learn to configure a single board computer(SBC) for network monitoring purposes. Students will setup the raspberry Pi to perform WiFi sniffing between two network devices. The SBC is placed in the middle and any data traveling between each device is captured by it. A second USB to Ethernet adapter is used to provide the second interface. Students will write a report detailing their work. In this lab report students should calculate the frequencies, wavelengths, transmission times, and energy of these signals. Potential alternate / additional report/activity: Students will configure the Wireless Access Point to utilize a standard WiFI encryption. They should once again observe network traffic and see how encryption protects the confidentiality of the information transmitted by the WiFi.

5. Network FIrewalls

Students will build upon their knowledge of data transmission via electromagnetic signals and understand that once a device is part of a network it has access to the resources of that network. This connectivity increases the value of a network but also exposes all devices on a network to traffic from all other devices on that network. This creates an inherent security vulnerability that we cannot solve with physics. Cybersecurity professionals solve this problem with firewalls that use the networking protocols to black or allow network connections. Working in teams, students will build a small computer network using an ethernet switch and several single board computers (SBCs). This small network will be used as a model for the Internet based on TCP/IP concepts. Using ICMP protocol (ping), students will verify that every system can communicate with every other system on the network. One SBC will then be set-up as a firewall to isolate one group of SBCs from another. By repeating the ping testing, students will see how the firewall effectively isolates systems on networks. Students will turn in a lab report detailing the firewall configuration along with a logical network diagram.

6. LASER Data Transmission

Now that students understand packets and firewalls they are ready for the unit capstone. A **laser** is a device that emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation. Lasers are used for many applications from optical disk drives to laser surgery. In this assignment the lasers role in fiber-optic and free-space optical communication is under investigation. As an introduction to the laser, students should complete an online simulation to understand the optics and phyiscs behind the laser (https://phet.colorado.edu/en/simulation/lasers). In this culminating activity for Unit 3, students will use the SBCi to encode sound as an electrical impulse to a modulated laser. This laser can be purchased from scientific supply catalogs or can be modified using a laser pen. Instructions for this activity are available online (http://www.laserfest.org/about/store/). The output from the laser shines on a photocell connected to a small amplifier and speaker. In this investigation students will create a program with the SBC to output a morse coded message. This message will input to the modulated laser, be sent across the classroom to the photocell, and output as a sound from the speaker. Students in the class will then decode the message created by each group and submit the source code in their lab report.

After completion of the above activity, students, in project teams, complete the following project that allows them to apply their learning:

1) Select from a teacher supplied list of problems that can be solved using a single board computer to control an attached laser that will emit a series of coded pulses of laser light.
2) Hypothesize a solution.
3) Conduct research.
4) Document/design experiment.
5) Conduct experiment when/if possible.
6) Write a technical report that explains the design and, when possible, the experimental results.

7. Professional Community

In this activity, student will have an opportunity to communicate and learn from professionals from a related discipline. The professional network administrator community can further the students knowledge of the process of hardware, software, and network installations in the related career explorations. Through the professional community, the students will further understand the importance of teamwork in a professional setting. Students should complete a writing assignment to identify key physics and cyber security concepts discussed as well as making connections to their real lives.

Unit 4 - Mitigating Security Risks

Cybersecurity involves protecting the confidentiality, integrity, and availability (CIA) of information stored within or transmitted by Information and Communications Technology (ICT). In this unit, students will synthesize and apply the knowledge and skills developed in the earlier units to answer the question “what are the physical, virtual, and societal risks to electronically stored and transmitted information and how do security professionals mitigate these risks?" By understanding physics principles of electricity, magnetism, and wave propogation, students will have a much deeper and more sophisticated "tool kit" to respond to these challenges. Physical vulnerabilities students will consider include controlling access to assets, preventing physical damage, and the importance of including redundancy in security systems. The importance of social risks becomes clear when we consider the vulnerabilities of human behavior and cultural norms in creating threats to our information systems and the virtual environment. The need to protect against virtual attacks is essential in mitigating and reducing security risks and is a key theme and skill set developed in this unit and course.

Unit 4 - Assignments

1. **Burglar Alarm**
   Cyber security professionals are also tasked with controlling access to physical assets (servers, routers, computers, etc.). In this project groups of students extend their knowledge of the principles of circuits from unit 2 to design and build a simple burglar alarm that attaches to a door. This burglar alarm should have a switch that activates when the door is opened. The alarm itself should be operated by a control box capable of producing either an audible alarm (sound), a visible alarm (light), or both when the burglar enters the room. Accompanying the physical alarm prototype should be a circuit diagram and an isometric scale drawing of the alarm with a description of the alarm's operation and physics principles involved. Through this activity, students not only show their ability to apply electrical principles to solve a problem but also get valuable experience in engineering practices and the engineering design cycle.

2. **Phone Drop (kinematics)**
   In this activity, students will design a structure to protect a device from impact from various given heights. Teachers should create parameters for the dimensions of the protective structure to be consistent with a portable device. Schematics should be created and include multiple views of the protective structure and it should be drawn to scale. Students will calculate the speed of the device at two points in time; halfway through the fall and right before impact. Pre-programmed sensors will be placed at these two points to measure the speed of the device as it passes each sensor and these measurements will be compared to the theoretical speeds previously calculated by the students. Students will also calculate the force acting upon the device at impact. The final product is a successful device which adheres to the given parameters and protects the phone from damage, and a set of calculations showing the speeds achieved by the device and the forces acting upon it.

3. **Securing Networks/Systems (Hack your Buddy)**
   This laboratory activity will build upon all of the cybersecurity and physics principals in prior units as students simulate actual cyber attacks and mitigations of those attacks. Students will be required to defeat physical security measures to

gain access to the single board computers (SBCs) which are inside a maglock box. Inside the box is a photoelectric alarm that will sound in a specified amount of time unless a mirror is placed at an appropriate angle to disarm the alarm. Once physical security is breached, student groups will construct two SBCs configured with preprogrammed scripts developed by students. The SBCs will serve as both network attacker and network defender systems. The attacker SBC will use open source network security tools to penetrate the defender SBC which is running open source intentionally vulnerable systems. Students should identify vulnerabilities, apply appropriate mitigation measures, verify the efficacy of the mitigation, and analyze and write an incident report. Instructor generated hacks designed to be associated with a physical principle such as wave-based or circuit-based weaknesses will be added to the two-computer system. Students will follow a standard troubleshooting model to identify the cause of the vulnerability. Students will document the troubleshooting process and analyze the vulnerability and should include an understanding of specific physics principles related to vulnerability observed.

4. Professional Community

In this activity, student will have an opportunity to interact and learn from a community of professionals. These professionals should focus on the physical aspects of information security. Students reflection at the end of each activity should identify the key physics and cybersecurity concepts discussed as well as making connections to their real lives.

Texts

Primary Text - District approved Physics text

Online Cybersecurity Resources-

The Internet provides a growing number of well organized and curated student cybersecurity experiences. Many of these activities are available to high school students.

Cyberpatriot (https://www.uscyberpatriot.org/)

MITRE corporation's annual capture the flag competition: (http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/annual-capture-the-flag-cyber-challenge)

High School Forensics competition: (https://csaw.engineering.nyu.edu/hsf) Global CyberLympics: (http://cyberlympics.org)

PBS Cybersecurity Lab http://www.pbs.org/wgbh/nova/labs/lab/cyber/#

Khan Academy https://www.**khanacademy**.org/

Scratch https://**scratch**.mit.edu/

Snap! **snap**.berkeley.edu/

Code.org