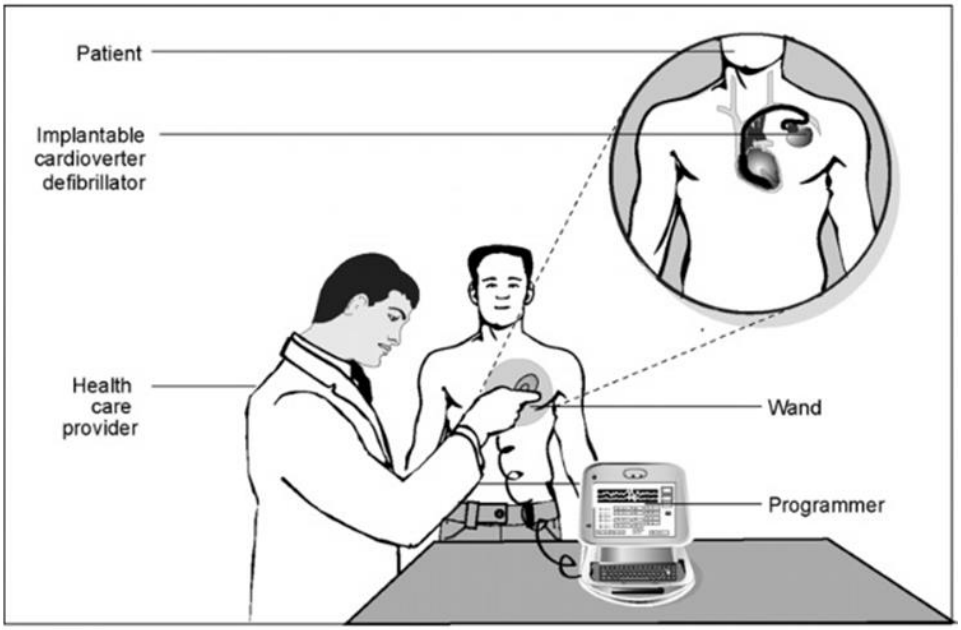
Scenario

Middle school girls become Cyber Super-Investigators (CSI) for a day to solve a cyber-crime.

During this interactive crime solving event, girls learn from women in diverse companies and agencies about what it takes to navigate the professional pipeline in the vast fields of Cybersecurity and Information Assurance, as well as other science, technology, engineering, and mathematics (STEM) fields.

The middle school girls complete hands-on activities with guidance from cybersecurity and STEM professionals in order to gather clues to help solve the crime. This year's cybercrime scenario focuses on vulnerabilities in networked medical equipment.



Source: GAO.

On an episode of the *Showtime* series *Homeland,* Vice President Walden's pacemaker was hacked becoming the weapon for his assassination. In a *60 Minutes* interview with former Vice President Dick Cheney, he confirmed that the possibility of his pacemaker being hacked had been discussed and the device's wireless access had been disabled to prevent such an attack on his life.

Although it may sound like science fiction several studies have proven that flaws in cyber security of medical devices could be exploited to induce death.

- Computer scientist Kevin Fu has demonstrated in a research lab that he could hack into a combination heart defibrillator and pacemaker to induce potentially fatal electric jolts.

- Researchers at computer security firm McAfee share they have found a way to hack into an insulin pump to make it release multiple days worth of insulin.
- Security analysts Terry McCorkle and Billy Rios discovered a simple password vulnerability affecting over 300 devices including ventilators, drug infusion pumps, external defibrillators, patient monitors, and laboratory and analysis equipment. Devices could be exploited to change critical settings or modify the device.

In the case of our scenario, the 2014 Cool Careers Cyber Crime: *Networked Medical Equipment Vulnerabilities*, the all girls' middle school Cyber Super-Investigators (CSI) have been hired to examine in greater detail how medical devices could be breached and make recommendations to the U.S. Food and Drug Administration.

The girls will collect and explore a variety of digital and physical evidence to learn more about medical device vulnerabilities. Clues provided by the lead investigators, the cyber professionals speaking at the Cool Careers in Cybersecurity for Girls Workshop, will help the middle school girls in their investigation!

Related Content

Some of the reports indicate some rudimentary causes; some from known software flaws, and others from end-user related vulnerabilities including:

- Lack of authentication to access or manipulate the equipment
    - Table activity: Physical security and lock picking
    - Table activity: Find the USB drives
- Weak passwords set by users as well as weak or default hard-coded passwords set by the vendor – passwords like "1234" and "admin"
    - Table activity: Cryptography
    - Table activity: Password strength
- Using very old versions of Windows that are susceptible to viruses from years ago. Hospitals have to use the older systems because some manufacturers will not allow their equipment to be modified with the newer versions, partially due to regulatory restrictions.
    - Table activity: Computer anatomy
- Embedded web servers and administrative interfaces that make devices obvious and vulnerable to a breach within the network
    - Wi-Fi network attacks