CSCI 245: Life, Computers, and Everything
Cybersecurity and Ethics
Malware

Get together in your breakout groups and brainstorm on what is malware and work to develop a list of all the different kinds of malware that you can identify.
Malware ≠ Cybersecurity

There’s a lot more to keeping systems secure than simply making it impervious to external threats.

What about internal threats? What can users do that will create vulnerabilities to a system?

Qui custodiet ipsos custodes? (“Who watches the watchmen?”)
Can The Remedy Be Worse Than The Disease?

In order to provide security, your system will keep secrets: passwords, activity logs, etc. Can these secrets come back to create exposures to the system itself and to its users?
What Are the Cybersecurity Professionals’ Obligations to the Public?
Case Study 4

Source: An Introduction to Cybersecurity Ethics
Prof. Shannon Vallor, University of Oxford
In 2015, just in time for the holiday season, Mattel released its WiFi-enabled Hello Barbie doll, which allowed the doll’s microphone to record conversations with a child and send it via Wi-Fi to third parties for audio language processing, allowing the doll to then offer the child an appropriate natural language response. Because the conversations were stored in the cloud, parents were also able to monitor the child’s conversations with the doll; parents can even share the audio clips of their children’s conversations online on the website of ToyTalk, the maker of the third-party software.

The toy raised a broad range of ethical issues, including the appropriateness of allowing parents to spy on their children during imaginative play. Also, as one legal scholar noted, “In Mattel’s demo, Barbie asks many questions that would elicit a great deal of information about a child, her interests, and her family. This information could be of great value to advertisers and be used to market unfairly to children.”\(^{10}\) However, security flaws were also prominent ethical concerns.

Security researchers quickly recognized significant security weaknesses in the doll that could be exploited by hackers for malicious purposes. One independent security researcher claimed that he was able to hack the device in such a way that he could access the user account information, stored audio files, and microphone for the doll, and potentially spoof ToyTalk’s third party website server to assume control of the doll’s speech. Somerset Recon, an organization devoted to security analysis and reverse engineering, eventually found 14 vulnerabilities in the system, including allowance for weak passwords, no protections against brute force password attacks (allowed unlimited password guesses), and exposure to URL redirect and phishing efforts. There was also the potential for malicious Javascript to be stored on ToyTalk’s third party website, allowing “persistent backdoor access to a ToyTalk user account.”\(^{11}\) Somerset Recon acknowledged that some efforts to provide adequate security had been made by ToyTalk, but also noted that there appeared to have been “little to no pre-production security analysis” and that the company appeared to be “using their bug bounty program as a low-cost alternative” to an independent security audit that could have identified the vulnerabilities before the product was released, and before real-world users were exposed to a post-market “race between security researchers and malicious hackers” to find the system’s flaws.\(^{12}\)