CSCI 297: ~~Ethical~~ Hacking

Computer Security, Privacy, and Anonymity Tools

William J. Tolley

May 2, 2024

W&L

Topics Covered Today:

- Understanding hacking: creative problem-solving.
- Computer security fundamentals: privacy on public networks.
- Deep dive into Tor: architecture, operation, and use cases.
- Hands-on demo: Installing and using Tor.
- Legal and security implications of using anonymity tools.

What is Hacking?

0

- Hacking involves using something in a way other than its intended purpose.
- It includes creative problem-solving, reverse engineering, and finding unconventional solutions.

Historical Hacks: The 2600 Hz Tone

- The 2600 Hz tone was discovered to grant access to a privileged mode on ATT's long-distance switching systems.
- Hackers could use this frequency to manipulate the phone system and make free long-distance calls.
- This tone could be perfectly replicated using a toy whistle given away in Cap'n Crunch cereal boxes, earning John Draper the nickname "Captain Crunch."

Joybubbles: The Blind Hacker

0

- Born as Joe Engressia, Joybubbles was a blind hacker with perfect pitch, allowing him to recognize and reproduce the exact tones needed to control the phone system.
- He is known for his ability to whistle precisely the right tones to manipulate phone networks, essentially performing what we now consider as early network hacking.
- His contributions highlight the role of ingenuity and unconventional methods in the development of hacking techniques.

John Draper: Captain Crunch

- John Draper discovered that a whistle given away in cereal boxes emitted a precise 2600 Hz tone.
- Using this whistle, he was able to mimic the tones used by ATT's system to route calls, effectively "hacking" the network.
- His exploits made him a legendary figure in the hacker community and brought the concept of "phreaking" (phone hacking) into the public eye.

Cultural Impact of Early Hacks

0

- These early hacks not only showcased vulnerabilities in telecommunication systems but also fostered a culture of curiosity and exploration.
- The exploits of figures like Draper and Joybubbles have inspired generations of hackers to explore systems and push the boundaries of what is possible.
- They also led to significant changes in technology security and regulation.

W&L

Privacy on Public Networks

0

- The internet is designed as a public network where routing information is visible.
- Encryption can hide the payload but not the routing information.
- Importance of protecting both content and routing information for complete privacy.

Introduction to Tor

0

- Tor is a network designed for anonymous communication.
- It uses a volunteer overlay network to route internet traffic across multiple nodes.
- This routing obfuscates user's location and usage, enhancing privacy and security.

How Tor Works: Detailed Architecture

0

- **Entry Node** (Guard Node): The first relay where encrypted traffic enters the Tor network.
- **Middle Node** (Relay Node): The relay(s) that pass your encrypted traffic to the next point.
- **Exit Node**: The final relay where encrypted traffic leaves the Tor network and reaches the internet.

Encryption in Tor

- Tor uses multi-layer encryption (often visualized as an onion).
- Each node decrypts only enough to know the next destination, but not the final target.
- This layered encryption ensures that no single node knows both the source and the destination of the traffic.

Using Tor for Exploring the Dark Web

0

- The dark web is part of the internet not indexed by traditional search engines, accessible via Tor.
- It contains a mix of legal and illegal content, from anonymous forums to marketplaces.

Installing Tor

0

- Demonstrating installation on different systems: Windows, macOS, and Linux.
- Key security settings and practices when using Tor to maintain anonymity and safety.

Legal and Security Considerations

0

- Understanding the legal implications and potential risks of accessing the dark web.
- Best practices for using Tor safely, including avoiding illegal activities and securing personal data.

Conclusion
0

- Recap of Tor's role in enhancing online privacy and security.
- Encouragement to explore further and responsibly use knowledge and tools for privacy.

Questions and Resources

0

- Open for questions.
- Additional resources for further study and exploration.