**Thesis statement:** we aim to analyze cybersecurity. Specifically, how and where spying happens (software / hardware), how it is utilized, and what measures can be taken to prevent it.

1. **(Jake)** Introduction to Spyware
2. History of Cisco getting busted by agencies
3. Current row with Huawei 5G infrastructure being implemented in the West
4. Segway into what is in hardware that makes it spy-friendly

(Give a summary of the points to be covered)

(Hook: Facts, Story, Question, ect.)

III. **(Alia & Max)** What is spyware

1. Spyware is malware that tries to keep itself hidden while secretly recording and tracking your activity on a computer or mobile device. It can monitor and copy everything you enter, upload, download, and store. Some spyware have the capability to turn on microphones and cameras without the user even knowing.
   * 1. Articles
        1. Avast security systems is a cyber security company that offers user real-time intelligence from over 435 million Avast users and block more than 1.5 billion threats every month.
           1. <https://www.avast.com/c-spyware>
2. What is a backdoor
   1. In cybersecurity, a [backdoor](https://blog.malwarebytes.com/glossary/backdoor/) refers to any method by which a user is able to get around normal security measures and gain high level user access (aka [root access](https://en.wikipedia.org/wiki/Superuser)) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.
      1. Malwarebytes is a cybersecurity company that provides cybersecurity products for all businesses. Malwarebytes is at home, in the home, on-the-go, and in the corporate conference room. Made for individuals, public organizations, private entities, and everything in between.
         1. <https://www.malwarebytes.com/company>
3. A Spyware tool to get into cars.
   1. <https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/>
4. Encryption - if we encrypt our info (e-mails) does it matter if our info gets sent off to govt agencies
   1. Encryption does prevent gov. access and this is why research into backdoors has become so prevalent
      1. Articles
         1. ZDNet, a business technology news website owned and operated by Red Ventures.
            1. [Yes, the FBI and CIA can read your email. Here's how | ZDNet](https://www.zdnet.com/article/yes-the-fbi-and-cia-can-read-your-email-heres-how/)
         2. RSI Security offers a complete suite of IT security services that provide reliable, flexible, and scalable cybersecurity resources to mitigate threats, test for vulnerabilities, and monitor your networks
            1. [5 things you need to know about how email encryption works (rsisecurity.com)](https://blog.rsisecurity.com/5-things-you-need-to-know-about-how-email-encryption-works/#:~:text=In%20todays%20world%2C%20email%20encryption%20functions%20on%20the,Public%20Key%20to%20encrypt%20the%20message%20before%20sending.)
   2. Can files be filtered from general encryption to potentially dangerous encrypted information that the government should know about?
      1. Articles
         1. Thousands of businesses use **Expert insights** to research and compare enterprise business IT and cybersecurity solutions
            1. [What is Email Encryption, How Does It Work, and How Can It Protect Your Organization? | Expert Insights](https://expertinsights.com/insights/what-is-email-encryption-how-does-it-work-and-how-can-it-protect-your-organization/)
         2. CBS News
            1. [Encrypted messages: Does the government need a way in? - CBS News](https://www.cbsnews.com/news/paris-attacks-encrypted-messages-does-the-government-need-a-way-in/)
         3. HeinOnline is a premier online research platform that provides more than 199 million pages of multidisciplinary periodicals, essential government documents, international resources, case law, and much more
            1. [Cracks in the Armor: Legal Approaches to Encryption 2019 University of Illinois Journal of Law, Technology & Policy 2019 (heinonline.org)](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jltp2019&div=5&id=&page=)
   3. Packets - can we not see where our data packets are being sent (from observing wireshark) and if not is that why outside infrastructure is used
      1. Wireshark does allow the user to see a packet's source and destination.
      2. Knowing the destination of a packet doesn’t mean that it is the final destination, and that may be out of Wiresharks’ view.
         1. I.e., you can see the packet being sent to computer 1, however it might be sent to a different network that Wireshark doesn’t have access to.
      3. Packets may be filed as a sub-point for Encryption.
      4. Articles
         1. How-To Geek is an online technology magazine and one of the top 500 websites in the United States. How-To Geek has been recommended as an expert resource by industry groups like [the Wi-Fi Alliance](https://twitter.com/WiFiAlliance/status/1083162775688482816) and newspapers like [The New York Times](https://www.nytimes.com/2018/12/05/smarter-living/should-you-buy-someone-a-phone-for-the-holidays.html).
            1. [How to Use Wireshark to Capture, Filter and Inspect Packets (howtogeek.com)](https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/#:~:text=Wireshark%20captures%20each%20packet%20sent%20to%20or%20from,of%20only%20packets%20addressed%20to%20your%20network%20adapter.)
         2. **SpringerLink** is the world's most comprehensive online collection of scientific, technological and medical journals, books and reference works. The leading edge of information for people on the frontier of research
            1. [Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking | SpringerLink](https://link.springer.com/article/10.1007/s10586-019-02996-0)
5. Is software embedded on our routers to send it elsewhere with us not knowing
   1. How does spyware work from within routers?
   2. What can we look for to identify it?
   3. Where is the data sent
      1. Data is sent to spyware servers where advertising companies can use the users data to create reference ads specifically for that user.
      2. Articles
         1. We provide a full range of e-discovery and forensic data collection services for legal cases. For example: imaging computers and cell phones; collecting data from computers, servers, and databases; providing search technologies for computer and online data; providing expert witness services; and providing trial presentations and evidence presentations.
            1. [Using Router Analysis to Detect Surveillance & Bug Sweep Services (howelawfirm.com)](https://www.howelawfirm.com/counter-surveillance-and-bug-sweep-services/routers/#:~:text=Generally%2C%20transmission%20data%20is%20available%20through%20the%20routers%E2%80%99,someone%20spying%20on%20me%20through%20my%20WiFi%20router%3F)
6. Virtual implementations of spyware
   1. What vulnerabilities are manipulated
   2. How they stay hidden
   3. How they transfer information
      1. Articles

## Security Gladiators acts as an online protection and security information source, as well as a privacy and security protection agency for internet users. Security Gladiators is an encyclopedia of web security for every possible internet vulnerability for web users, from VPNs to anti-virus applications.

* + - * 1. [What Is Spyware? (securitygladiators.com)](https://securitygladiators.com/threat/spyware/#:~:text=Spyware%20will%20infiltrate%20via%20an%20install%20package%2C%20malicious,communicates%20your%20private%2C%20confidential%20information%20to%20an%20attacker.)
      1. VPNRanks.com is a website that presents unbiased reviews for the general benefit of VPN users. Our team conducts in-depth tests and evaluates each provider on multiple factors
         1. [Spyware – How To Detect and Protect Yourself Against It? (vpnranks.com)](https://www.vpnranks.com/blog/spyware-how-to-detect-and-protect-yourself-against-it/)
      2. Alexander Moshchuk, Tanya Bragin, Steven D. Gribble, and Henry M. Levy, leading experts within the Department of Computer Science & Engineering University of Washington
      3. Experts within their field and authors of over 20 articles regarding the study and implementation of spyware
         1. [spycrawler.pdf (washington.edu)](https://courses.cs.washington.edu/courses/cse454/15wi/papers/spycrawler.pdf)

IV. **(Max)** Utilization

1. How opponents use it
   1. Cyber criminals use spyware programs to capture/monitor a user’s computer activity and store the information for third parties to access.
   2. Associated cookies may be a form of Spyware because they identify a single user each time they connect to any member sites. These cookies track and store data gathered from the user's interaction with each member site. While this is happening the member sites allow advertising companies access to the users information to give reference ads to that specific user. These reference ads are produced from spyware data servers and allow spyware sites to look for recognizable cookies on the user’s system. If the spyware finds none they produce a globally unique identifier(GUID) to identify the user any time they are on a member site.
      1. Articles
         1. The articles in this journal are peer reviewed in accordance with the requirements set forth in the [IEEE PSPB Operations Manual](https://pspb.ieee.org/images/files/files/opsmanual.pdf) (sections 8.2.1.C & 8.2.2.A). Each published article was reviewed by a minimum of two independent reviewers using a single-blind peer review process, where the identities of the reviewers are not known to the authors, but the reviewers know the identities of the authors. Articles will be screened for plagiarism before acceptance.
            1. <https://ieeexplore.ieee.org/abstract/document/1362621>
         2. Eric Chien joined Symantec Corporation at the Symantec Security Response headquarters in Santa Monica, California in 1997. Eric graduated from the University of California, Los Angeles with a Bachelor of Science degree in Electrical Engineering and Molecular Genetics. Currently, Eric heads research in the Europe, Middle East, and Africa (EMEA) regions, analyzing current virus threats and researching new threats in the world of viruses and malicious software. He has been a key developer in projects such as the Digital Immune System (DIS), Symantec's automated system of virus analysis, and the Seeker project, which proactively finds viruses on the Internet. Eric has spoken at various conferences and published a variety of papers addressing threats to computer security via malicious software.
            1. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.174.3560&rep=rep1&type=pdf>
   3. Black hats - vigilante group of hackers
2. How we use it
   1. Cookies: A web server sends a small file of information, called a cookie, to be stored on a user’s system. This cookie identifies the user upon return.
      1. Same source as how opponents use it.
         1. <https://ieeexplore.ieee.org/abstract/document/1362621>
   2. White (Volunteer work)
   3. Script Kiddies (Creating tools and software to detect, prevent/protect against spyware)
   4. Green (Hired by companies to find security vulnerabilities)
   5. Gray (Similar to green, but are not hired and can post the vulnerability on the internet)
   6. Red (Seen as vigilanties, go against black. Not law enforcement)
   7. Blue (Using their skills for personal vengeance/revenge) [Dark script kiddie]
3. Articles
   1. [7 Types of Hackers You Should Know | Cybrary](https://www.cybrary.it/blog/0p3n/types-of-hackers/#:~:text=%207%20Types%20of%20Hackers%20You%20Should%20Know,who%20lacks%20programming%20knowledge%20and%20IT...%20More%20)
   2. [Authorities use hackers to find missing persons (hackread.com)](https://www.hackread.com/authorities-use-hackers-to-find-missing-persons/#:~:text=The%20Hackathon%20was%20an%20attempt%20to%20find%20new,Gold%20Coast%2C%20Melbourne%2C%20Perth%2C%20Sydney%2C%20and%20Sunshine%20Coast.)

V. **(Alia)** Preventative Measures

1. Encryption
   1. What is it
   2. How is it used
      1. Utilization depends on the technique that is used
      2. Different types of encryption (Be brief)
         1. [RSA (cryptosystem) - Wikipedia](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
         2. [Advanced Encryption Standard - Wikipedia](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)
         3. [Elliptic-curve cryptography - Wikipedia](https://en.wikipedia.org/wiki/Elliptic-curve_cryptography)
      3. Articles
         1. The American Health Information Management Association is a professional association for health professionals involved in the health information management needed to deliver quality health care to the public.
            1. [Encryption Basics (ahima.org)](https://library.ahima.org/doc?oid=104090#.Yik48YnMLMY)
2. Firewalls
   1. What are they
   2. Do they ever help us
      1. Articles
         1. Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world.
            1. [How Does a Firewall Work? | Fortinet](https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work#:~:text=Software%20Firewalls%201%20Packet%20Filtering.%20Data%20is%20organized,packet%20and%20compares%20it%20against%20a%20threat%20database.)
   3. How can they be bypassed
      1. Articles
         1. Trend Micro Inc. is an American-Japanese multinational cyber security software company that develops enterprise security software for servers, containers, & cloud computing environments, networks, and end points. Its cloud and virtualization security products provide automated security for customers of VMware, Amazon AWS, Microsoft Azure, and Google Cloud Platform.
            1. [Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes - Security News (trendmicro.com)](https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101)
         2. Guardicore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to protect critical applications from compromise through unmatched visibility, micro-segmentation and real-time threat detection and response
            1. [The dangers of firewall misconfigurations | Guardicore](https://www.guardicore.com/blog/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them/)
         3. FireMon is an enterprise security management company that allows its users to continuously analyze, visualize, and improve their existing network security infrastructure and firewall management. It helps organizations find, correct, and avoid gaps in their existing network security infrastructure.
            1. [5 Causes of Firewall Breaches | Network Security Automation (firemon.com)](https://www.firemon.com/uplevel-your-security-and-networking-capabilities-with-automation/#:~:text=%205%20Root%20Causes%20of%20Firewall%20Breaches%20,the%20network%20can%20provide%20unauthorized%20or...%20More%20)
   4. How to protect against spyware
      1. Manage your cookies (Daily spyware)
      2. Downloading/Implementing security software
      3. Doing scans of your workspace and investigating suspicious activity

VI. **(Jake)** Conclusion

1. What can we expect in the future
2. Will spyware become harder to detect or will encryption become more efficient

(Restate the introduction but better)  
(Leave the reader thinking or with a call to action)

VII. **(Jake - Citations)** Resources

1. Original Resources (Not currently in use, so list at the end)
   1. Security Engineering Third Edition: A Guide to Building Dependable Distributed Systems by Ross Anderson
   2. Professor Varghese
   3. UWRF Resource Database
   4. TBD Resources found while gathering data and information
2. Current resources (Will format later)
   1. [What is Spyware? | Spyware Definition | Avast](https://www.avast.com/c-spyware)
   2. <https://www.malwarebytes.com/company>
   3. [Yes, the FBI and CIA can read your email. Here's how | ZDNet](https://www.zdnet.com/article/yes-the-fbi-and-cia-can-read-your-email-heres-how/)
   4. [5 things you need to know about how email encryption works (rsisecurity.com)](https://blog.rsisecurity.com/5-things-you-need-to-know-about-how-email-encryption-works/#:~:text=In%20todays%20world%2C%20email%20encryption%20functions%20on%20the,Public%20Key%20to%20encrypt%20the%20message%20before%20sending.)
   5. [What is Email Encryption, How Does It Work, and How Can It Protect Your Organization? | Expert Insights](https://expertinsights.com/insights/what-is-email-encryption-how-does-it-work-and-how-can-it-protect-your-organization/)
   6. [Encrypted messages: Does the government need a way in? - CBS News](https://www.cbsnews.com/news/paris-attacks-encrypted-messages-does-the-government-need-a-way-in/)
   7. [Cracks in the Armor: Legal Approaches to Encryption 2019 University of Illinois Journal of Law, Technology & Policy 2019 (heinonline.org)](https://heinonline.org/HOL/LandingPage?handle=hein.journals/jltp2019&div=5&id=&page=)
   8. [How to Use Wireshark to Capture, Filter and Inspect Packets (howtogeek.com)](https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/#:~:text=Wireshark%20captures%20each%20packet%20sent%20to%20or%20from,of%20only%20packets%20addressed%20to%20your%20network%20adapter.)
   9. [Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking | SpringerLink](https://link.springer.com/article/10.1007/s10586-019-02996-0)
   10. [Using Router Analysis to Detect Surveillance & Bug Sweep Services (howelawfirm.com)](https://www.howelawfirm.com/counter-surveillance-and-bug-sweep-services/routers/#:~:text=Generally%2C%20transmission%20data%20is%20available%20through%20the%20routers%E2%80%99,someone%20spying%20on%20me%20through%20my%20WiFi%20router%3F)
   11. [What Is Spyware? (securitygladiators.com)](https://securitygladiators.com/threat/spyware/#:~:text=Spyware%20will%20infiltrate%20via%20an%20install%20package%2C%20malicious,communicates%20your%20private%2C%20confidential%20information%20to%20an%20attacker.)
   12. [Spyware – How To Detect and Protect Yourself Against It? (vpnranks.com)](https://www.vpnranks.com/blog/spyware-how-to-detect-and-protect-yourself-against-it/)
   13. [spycrawler.pdf (washington.edu)](https://courses.cs.washington.edu/courses/cse454/15wi/papers/spycrawler.pdf)
   14. <https://ieeexplore.ieee.org/abstract/document/1362621>
   15. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.174.3560&rep=rep1&type=pdf>
   16. <https://ieeexplore.ieee.org/abstract/document/1362621>
   17. [7 Types of Hackers You Should Know | Cybrary](https://www.cybrary.it/blog/0p3n/types-of-hackers/#:~:text=%207%20Types%20of%20Hackers%20You%20Should%20Know,who%20lacks%20programming%20knowledge%20and%20IT...%20More%20)
   18. [Authorities use hackers to find missing persons (hackread.com)](https://www.hackread.com/authorities-use-hackers-to-find-missing-persons/#:~:text=The%20Hackathon%20was%20an%20attempt%20to%20find%20new,Gold%20Coast%2C%20Melbourne%2C%20Perth%2C%20Sydney%2C%20and%20Sunshine%20Coast.)
   19. [RSA (cryptosystem) - Wikipedia](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
   20. [Advanced Encryption Standard - Wikipedia](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)
   21. [Elliptic-curve cryptography - Wikipedia](https://en.wikipedia.org/wiki/Elliptic-curve_cryptography)
   22. [Encryption Basics (ahima.org)](https://library.ahima.org/doc?oid=104090#.Yik48YnMLMY)
   23. [How Does a Firewall Work? | Fortinet](https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work#:~:text=Software%20Firewalls%201%20Packet%20Filtering.%20Data%20is%20organized,packet%20and%20compares%20it%20against%20a%20threat%20database.)
   24. [Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes - Security News (trendmicro.com)](https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101)
   25. [The dangers of firewall misconfigurations | Guardicore](https://www.guardicore.com/blog/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them/)
   26. [5 Causes of Firewall Breaches | Network Security Automation (firemon.com)](https://www.firemon.com/uplevel-your-security-and-networking-capabilities-with-automation/#:~:text=%205%20Root%20Causes%20of%20Firewall%20Breaches%20,the%20network%20can%20provide%20unauthorized%20or...%20More%20)