James Otis

IS428 Reading Notes

Future Crimes

Chapters: 1,4,10,11,14,15,16,17,18

Chapter 1.

* Connected, Dependent, and Vulnerable:
  + Hacker used: ICLOUD email to unlock AMAZON for Credit Card to recover his password.
  + All other data on matt such as his address could be found from a WHOIS or a Whitepages.
  + This ultimately allowed the hacker “PHOBIA” to unlock his gmail and thus take his twitter name.
  + Treaty of Westphalia: No other nation should meddle in domestic affairs of another nation
  + Attacks from multiple nations have to jurisdiction, and because of the nature of hopping from domain to domain, it is impossible to pinpoint an attacker.
  + Topic of thought: Medical devices, should they be made with security in mind, as to do so would require them actually be built that way, making the task very difficult. Your thoughts?

Chapter 4:

* Examples:
  + PatientsLikeMe.com: Ahmed’s intimate details were sold to a private company “Nielsen”, and this was perfectly valid as the privacy policy dictated that the data could be shared.
  + Social Media is the new public forum for data scraping.
  + The implications of Google Glass:
    - Advertisements
    - Video Streaming to be analyzed in real time
    - Who owns the video bank for google Glass?
  + Evaluations of companies like google and Instagram do not come from the employees or the content, but on the users and their data
    - Average Facebook user is worth about 80$
  + All data is mined and companies that link to facebook, Instagram, etc are all able to access your PII (personally Identifiable Information)
  + Furthermore: One weak link is this chain could cause for a spill of your information
  + 80 % of applications track location.

Chapter 10: The future of Crime:

* Mules, or individuals who unknowingly or knowingly launder money are the bottlenecks in criminal organizations. (Hacks are easy and data is easily retrievable)
* Prison education has allowed some individuals who are truly criminals and have been incarcerated, access to tools that are dangerous.
* Crowdsourcing is powerful tool to criminals, in addition well monetized rewards allow for simple bodies to be easily acquired.

Chapter 11: Dread Pirate Roberts

* DPR was taken from an alias in “*The Princess Bride”* . DPR was the man behind Silk Road and the subject of a global manhunt.
* DPR apprehended in a library after he unlocked his PC. The FBI faked assassination photos and utilized the information that DPR provided to “assasins” to take him down. 29 year old Ross Ulbricht made 80 million in one year.
* Tor, an anonymous software routes location information through multiple servers allowing for anonymity. This service allows silk road to run as well as to allow other people such as journalists, terrorists, and other clandestine groups to operate in total secrecy.
* Searching across the web is akin to fishing the first two feet of the whole worlds ocean.
* Russian Carder sight Maza has an 8 day waiting limit and you must gain access from being approved by an existing member
* Kim DotCom and the invent of MegaUpload (175million a year)
* Scopolomine (Zombie Drug)
* Sold PII costs the IRS 21Billion and Medical Fraud 5.6 Billion
  + HitMen
  + Weapons
  + Drugs
  + Child Porn / Abuse
  + Human trafficking
  + Human Organ Trafficking
* Bincoin:
  + Untraceable cryptocurreny
  + Mt. Gox hacked for 470million (New Bankrobbery)
* TakeAways:
  + There is a load of Malware that is used for making money through scams and exploits, all of which is made viable by untraceable currencies.
  + WERE ALL SO FUCKED

Chapter 14: Medicine and The IOT

* Consider IMDs (Implanted Medical Devices)
  + These devices can be subverted over Bluetooth or Wifi
  + Pacemakers / Insulin Pumps / and many others are targets for potential ransomware in the future
* Biometrics:
  + Cannot change them once they’ve been compromised
  + Israel had their whole data base of Biometrics Stolen
  + Adhaar in india is a database of the whole countries metadata
* VR / AR: becoming Homo Virtualis:
  + Dangerous because of the inability to enforce
  + Virtual Currency
  + Virtual Attacks on Online valuables.

Chapter 15: When Cyber Crime goes 3D

* Google’s Acquisition of robotics coming, a true motive or an untrue motive. (In a world that is connected does it make sense for a super-giant to have all of that control)
* Ethics behind drones and strikes.
* Does it make sense for us to have all these robots, when does laziness consume us.
* The Ethics of Robotics:
  + Who is to blame for the inevitable mistake of a robot?
  + Privacy Risks (Especially with drones being in the public airspace)
  + The ethical risks of open software: Is it safe that ROS is available to everyone? It allows people with malicious intent to see all of the code that allows for these Robots to run, making it much more easily exploitable.
* How do we combat 3D printing:
  + Wilson was able to produce blueprints to produce guns that could be 3D printed. Congress couldn’t do anything about this
  + Why is it necessary to ship things when they can be printed locally?
  + Accessibility of blueprints is the only limiting factor, which slowly is becoming less of a limiting factor
  + Plastic weapons cannot be detected on most scanners.

Chapter 18: Why cyber threats are only the beginning

* Algorithms and how they control our world:
  + The FICO score is based on an algorithm that is not transparent (Democracy?)
  + AI can be used as the accomplice to crimes (The Aguilar case with Siri)
  + Watson beating Ken Jennings: At what point does non-human intelligence surpass our own?
  + The dangers of AI vendors? Who is the person to blame if AI is the distributor of illegal goods. (AI run amazon.com)
* The creation of the human brain:
  + IBM created “TrueNorth”, an artificial brain with neurons and synapses that is capable of making wise-calculated decisions. A Immense step forward in AI
  + Currently only limited by the size of computers (PetaFlops for operations). With Moore’s law we will be there in only a manner of years
  + Moore’s Law: Since 1965 the amount of transistors on chip has doubled every year.
  + Already we are on the forefront of mind reading (IBM can deduce objects and people by measuring brain waves via an MRI)
* SynBio:
  + The process of creating biological molecules using processes (often using computeres)
  + 10 cents per base
  + Companies may be able to actually accept free DNA samples and give you Ancestry, Health and other DNA records. (Could sell your biological makeup however)
  + Just like code, different types of Viruses can be engineered to be more deadly.
* Quantum Computing:
  + 5 bits instead of 2, using Qubits
  + Able to break standard Crypto schemes like AES in realistic time
  + Already both the NSA and google are working on security for the quantum realm
* “75 percent of all computer systems can be penetrated in mere minutes, and only 15 percent require more than a few hours to hack.” Excerpt From: Marc Goodman. “Future Crimes.” iBooks.

Chapter 17: Surviving Progress

* Software is often shipped with the developers knowing that there are serious flaws, but the push based on speed has led to insecure products on the open market.
* How can we police software to make it more secure for the user? Punish the Engineer? The company?
* The EU has data protection acts that limits what information can be held on an individual and for how long.
* Education of the youth on good practices for CyberSecurity
* One weak link in a company, often a human error will be the difference between a major hack and one not occurring.
* Verizon says that 97% of attacks could be avoided with moderate security measures.

Chapter 18: Moving forward and the future

* SINET: Security Innovation Network works with the public and private sectors for education about CyberSecurity.
* Crowdsourced law enforcement, use what the hackers are using against them.
* Many people believe that we are not taking the cybersecurity threat as serious as we should.
  + This is due to a lack of understanding from the general public and a laid back approach to internet security