Future Crimes Book Presentation

Steffen Cornwell, Claire Donovan, Harrison Silver, Nishita Jain, Rohan Menezes
Chapter 1.

Connected, Dependent, and Vulnerable
Matt Honan- Reporter for Wired

- Computer, Phone, and Ipad all Hacked
- Website for billing address, last four credit card digits from amazon
- All connected
Hacking: a better form of bank robbery

- Physical Location
- Evidence
- Cameras
- Limitation to amount of bills stolen

- Vladimir Levin (not pictured) stole $10.7 million from his apartment
- Transferred money to the US, Netherlands, Germany, and Israel
- Who has Jurisdiction?
In the beginning, they did it for ‘lulz’

Brain Virus developed by Amjad Farooq Alvi

Used it when to protect against people from pirating his software
Malware exposes websites for money, information and power

- 2010 there were 49 million stains of malware
- 2011 2 million new pieces of malware each week
- 2013 200,000 new malware samples each day
- Malware costs consumers $2.3 billion annually (only people who realized they have been attached)
- 2012 Antivirus programs only detect 5 percent of viruses because they look at known vulnerabilities
- Hackers are successful 75 percent of the time
- 85 percent of the time it only takes them a few hours
Chapter 2.

System Crash
2008 a train in Poland turned left when the conductor tried to steer it to the right

Went off the rails and crashed into another train

All caused by a 14 year old

"[It was] just for the lulz"
All of these things are connected to the internet

- Mostly run on Supervisory Control And Data Acquisition (SCADA) Systems that are getting connected to the internet
- Designed without security in mind
Hackers are becoming smarter and sharing

- Databases such as Shodan which have become the Google of crime
- Keep servers in many different countries
- Publishing is not a crime in most of the countries
Notable Hacking Groups

➢ Jobs and wozniak sold blue boxes that hacked cell phone companies to make free calls
➢ Organized Crime (Italian Mob, Triad, etc)
  ○ Easy money with more lenient sentencing minimums
➢ Cyber Crime organizations (ShadowCrew)
  ○ Buy and sell credit card information and identities
➢ WikiLeaks and Anonymous
➢ Terrorists using cyber crimes to recruit, finance, communicate and spread propaganda
US government that helped create internet still gets hacked

May 2013 US government accused China of hacking the $300 billion F-35 Program

Also accused them of hacking the missile defense system

Cyber attacks have become an international weapon between countries
Chapter 3.

Moore’s Outlaws
Moore people can be robbed in a shorter period of time
Lines of Code have increased and so have ways to be exploited

- 1969 - Apollo 11 took 145,000 lines of code
- 1980 - Space Shuttle took 400,000 lines of code
- 2013 - Microsoft Office took 45,000,000 lines of code
- Today - Healthcare.gov 500,000,000 lines of code

- More lines of code more errors
- 2003 Northeastern blackout caused partly by software bug
- Cyber exploits can be used again and again
Chapter 4.

You’re Not the Customer, You’re the Product
PatientsLikeMe

- An online forum for people suffering through illness to connect with others going through the same struggle and form a community
- Nielsen scraped the site to get medical data for pharmaceutical companies
- PatientsLikeMe disclosed this but also disclosed that they were selling customers’ medical data to companies!
- Both were legal under federal law and the privacy agreement of PatientsLikeMe
Our Growing Digital World – What They Never Told You

• The Internet is widely used across the world today
  • Americans spend more than 5 hours per day on their devices
  • 80% of people check their phones within 15 minutes of waking up in the morning
• The Internet is free because you are paying for it with your data
• Companies’ privacy agreements allow them to collect almost any data on you that they wish
• You and your data is the value that they are after!
• Google, in particular, has a huge amount of information about you across their multitude of different apps
You’re Leaking – How They Do It

• Cookies and other identifiers (like IP address) make it possible to track your activity across the Internet
• Other users can unintentionally give companies information about you
  • Tagging you in pictures
  • Putting your birthday in their calendar
  • Even just receiving an email from you!
• Long privacy policies can literally have anything in them – most people don’t read them
  • One policy gave a service the right to your immortal soul
Mobile Phones

• These are a huge source of loss of privacy – 600 billion unique data points per day

• They have a GPS that can track your location whenever and wherever
  • This is absolute “nirvana” for advertisers since it reveals so much information about you and can be used for targeting ad campaigns

• They know where you spent your money (Apple Pay, etc.)

• They know who you spend your time with (texting, etc.)

• Apps can also collect huge amounts of data since they receive permissions to access your camera at any time, your photos, your location, and potentially more
Chapter 5.

The Surveillance Economy
Data Brokers

• An industry that is rapidly becoming huge as the world moves online
• These companies collect your data and information from a variety of services across the Internet (ISPs, social networks, etc.) and resell it to marketers and advertisers
• This allows advertisers to sort you into categories (segmentation) and target their ads to your particular interests and tastes
• There are currently no restrictions on the type of information that these data brokers can collect (even if it is private or personal)
Analyzing You

- When all this data is aggregated together, it can be extremely informative
  - Can tell you are taking a trip to Miami to visit the beach via Internet searches
  - Can tell you are cheating on your spouse via GPS data from your phone
  - Can tell your sexual orientation from your social network profile
- Having “nothing to hide” is not good enough – each of us has private, special moments in our life (tax returns, using the bathroom, etc.)
- Real life examples
  - Target figured out a high schooler was pregnant before her father
  - Facebook outing a lesbian woman to her conservative father
  - OKCupid sells answers detailing personal information to data brokers
Opening Pandora’s Virtual Box

• The government and organizations are now using online data as evidence
  • Can be used in court
  • Can be used to reject your from a job

• The government and organizations are also demanding access to your social media
  • To protect reputation
  • To gather more evidence

• Ultimately, data is power and we’ve entrusted authority over this data to many private companies
Chapter 6.

Big Data, Big Risk
Data is generated constantly

- 92% of infants already have online presences
- Every 10 minutes we create more information than the first 10,000 generations of human beings

However, data should be protected adequately.

“The more data you produce and store, the more organized crime is happy to consume” - Goodman’s Law

- Eventually your personal details will in some form fall into the hands of criminals or malicious parties
Many, many accounts get compromised

- Facebook’s own security departments have disclosed that somewhere around 600,000 accounts are compromised on a daily basis.

Even one compromised account can give a hacker access to your whole online and potentially even offline life.

- 75% of people use the same password for multiple sites
- 30% of people use the same password for all sites
The data realities are shocking

- In 2013, Experian “mistakenly” sold the personal data of almost two-thirds of the population of the United States to an organized crime group in Vietnam because they did not do a due-diligence on the buyer.
- At least 40% of all social media users have been exposed to some form of malware; most Facebook users have seen “Koobface” (targeted by a Russian hacking group) that told them “OMG - I just saw a naked video of you!”
- Identity theft costs the US upwards of $20 billion each year and more than 13 million Americans have been victims (children are 51x more likely to be).
Children are severely affected

Nearly half of all teens are affected by cyber-bullying. The problem is so far-reaching and entrenched that almost 20% of middle-school students admitted to seriously thinking about attempting suicide because of online bullying.

- Stories such as ones of Amanda Todd serve as the cautionary tales that show us the really evil sides of cyber-crimes against children
Chapter 7.

I.T. Phones Home
Mobile phones are really insecure

- There are viruses and trojans designed specifically to target mobile OSs
- Most (almost 99%) of malware targets Android phones, because Android users are significantly less likely to update their phones with latest softwares

If Android users updated their OSs, 77% of security threats could be eliminated.

- Jailbroken iPhones are extremely susceptible to malware, especially if apps are downloaded from non-Apple sponsored app stores
We’re constantly being tracked

Most of our apps are recording insane amounts of data on us at any point.

- Even major players such as Snapchat have left millions of users vulnerable to attacks on their mobile phones.

In 2012, there were 3.4 US million victims of stalking who were tracked via GPS or spyware hacks.

- Retailers may use IPs and other public addresses to track you.
- Criminals have access to where you are and when you are there.
Chapter 8

In Screen We Trust
What you see is not what you get

- In 2005 the UN’s International Atomic Energy Agency found Iran in noncompliance with the Nuclear Non-proliferation treaty
- President Bush launched Operation Olympic Games
- The US and Israel produced Stuxnet: a computer “worm” that infected Iranian centrifuges used to create U-235

- Worm Phase 1: act dormant and observe
- Worm Phase 2: Slowly infect the whole system
- Worm Phase 3: Trick the security staff
How is what we see being manipulated?

“We no longer live life through our own innate primary human sensory abilities”

“Those who control the computer code also control our screens and thereby our experiences and perceptions”

- How would my Google search results compare to yours?
- How do you even know what you’re missing?
You never know who you’re talking to

- Facebook removing fake profiles led to Lady Gaga losing 32,000 Facebook fans and Rihanna and Shakira each losing 22,000 fans
- Spear Phishing: instead of sending a general fraudulent message to millions, target specific individuals/orgs
- Coca Cola was going to buy the Chinese drink brand Huiyan Juice Group until it discovered the Chinese government was monitoring them
- How? Deputy President of Coca Cola’s Pacific group, Paul, Etchells, was phished
Financial Markets Can be Swayed by Hackers

- In 2005, a college student from El Segundo, California created a fake press release for Emulex, which circulated quickly.
- Caused the stock to drop for $104 to $43 dollars, and the attacker shorted the stock.
Chapter 9

Mo’ Screens, Mo’ Problems
There are More Ways Than Ever to be Attacked/Hacked

- **Swatting:** bored hackers can telephone 911 with a spoofed phone identity to report nonexistent crimes
- **Heavily armed police SWAT units** are dispatched to these locations to the surprise of the homeowners
- **Celebrity victims** include Russell Brand, Tom Cruise, Rihanna, Charlie Sheen, and Miley Cyrus
GPS Attacks

- Students at Technion Israel Institute of Technology hacked the Waze app
- They registered a thousands of fake users
- Connected accounts to fake smart phones to report falsified GPS coordinates
- Intentionally submitted thousands of reports of traffic jams
- Waze then reourted the whole city away from a ficticious traffic jam
- This caused a gridlock!
- Done on a more massive scale, this can cause huge panic and chaos just like any other crime or terrorist attack
Smoke Screens and the Fog of War

- Screens are used to tell battle commanders locations of aircraft, ships, tanks
- Screens manage logistics and supplies
- Screens provide up-to-date intelligence on plans and intentions of the enemy
- In the battle between Syrian government and rebel forces, Reuters news site was hacked to disseminate false news of rebels suffering a large defeat
- U.S. government has fake Facebook provides intended for psychological operations (psycops) for “to counter ‘extremist ideology and propaganda’”
- June 2011 U.S. Central Command awarded $2.76 million to a CA company to make fake online personas to spread pro-American POV in social media
Given all of these hacks, the future is spooky

- Everything around us has screens, and we trust them all pretty easily
- The information grid is increasingly connected and we are increasingly dependent
- The development of new technologies also leads to new methods of attack and exploitation
- As robotics, AI, 3D manufacturing, and synthetic biology develop, we are at the forefront of a whole new future of crime and harm
Innovative Marketing

- Kiev, Ukraine
- Booming business from Malware Destructor, System Defender, Windows Antispyware
- Grew fast - occupied three stories of office space
- Global multilingual company
- High customer satisfaction - 95%
- Large social media presence
- Good place to work with good activities and vacations
Problems with Innovative Marketing

- Antivirus software fake
- Crimeware
- Average sales price of $35
- $180 million in revenue in 2009
- Prosecuted and founders fled
- Money went to bank accounts with no tracing
Crime, Inc.

- Organized cyber crime
- Prosecutions in less than 1/1000 of 1% of cases
- $2 trillion in revenue from organized crime
- 15-20% of world’s GDP
Organization Chart

- CEO
- CFO
- CIO
- CMO
- Middle Management
- Infantry
- R&D
- Engineers
- Quality Assurance
- Technical Support
- Money Mules
Lean Immoral Startup

- Criminals use technology better than legal world
- Lean startup methodology
- Apply similar techniques from Wharton and HBS as legal organizations
- Crime Sourcing
- Incentives
- Software as a service
- Malware-Industrial complex from learning from existing virus
Chapter 11

Inside the Digital Underworld
Silk Road

- Online amazon for drugs, child pornography, guns
- Dread Pirate Roberts - libertarian anarchist
- Accessible by TOR
- Dark Web:
  - Google indexes less than 1% of web
  - 50% of TOR sites involved in illegal activities
  - TOR bounces your IP so you can be covered
  - TOR Developed by U.S. Naval Research
  - al-Qeada and other groups
Dark Web Offerings

- Pirated Content
- Drugs
- Counterfeit Currency
- Stolen Goods
- Cards/Accounts
- Identity Theft
- Documents
- Weapons, Ammunition, and Explosives
- Hit Men
- Child Sexual Abuse Images
- Human Trafficking
- Human Organ Trafficking
- Live Child Rape
How you can support Crime, Inc.

- Download pirated content
  - Better to support Crime, Inc than content creators
  - The good is non-exclusive

- Purchase controlled substances
  - 100% of proceeds to Crime, Inc.
  - Help fund your local gang or cybercriminal
  - % of profits go back into Hitmen

- Visit pornography websites
  - Captcha you enter can help train Captcha alg
  - Ad revenues support all forms of pornography
  - Help support potential human trafficking