Future Crimes:
Inside the Digital Underground and the Battle for Our Connected World
Chapter 1: Connected, Dependent and Vulnerable
Friday, August 3, 2012

- Summer Olympics
- Curiosity rover 3 days from Mars
- 2 days ago: Snoop Dogg converts to Rastafarianism and changes name to Snoop Lion
Friday, August 3, 2012: 5 PM

- Mat Honan
- Playing with his daughter
- iPhone shuts down
iPhone reboot

- A strange screen
- No problem, restore from iCloud
Restore from iCloud fails

- No worries: restore from laptop!
Restore from laptop

- “Honan knew he had never set a password.”
Fallout, part 1

- Baby pics
- Relative pics
- Google account
  - Gmail
  - Reminders
  - Calendar events
- Twitter
Getting in touch

- “I honestly didn’t have any heat towards you before this. I just liked your username like I said before”
How it worked

- Twitter @mat -> website -> Gmail
- Gmail account recovery
  - No 2FA
  - Alternate email: m••••n@me.com.
  - hmm...
- Whois: get billing address
- Amazon: get last 4 digits of credit card from customer service rep
How it worked

- 4:33 PM- request Apple reset account
  - Gmail address, credit card (Amazon), billing address (Whois)
- 4:50 PM- set new me.com password
- 4:52 PM- set new Gmail password
- 5:00 PM- iPhone wipe
- 5:01 PM- iPad wipe
- 5:02 PM- set new Twitter password
- 5:05 PM- Macbook wipe
- 5:12 PM- Phobia posts to Twitter with @mat
Interconnectedness

- No requirement for being physically there
- Vladimir Levin 1994 Internet bank robbery
  - Finland
  - US
  - Netherlands
  - Germany
  - Israel
- Jurisdiction?
Terminology

- Virus: insert copy into another program
- Worm: standalone program
- Trojan: trick users into loading and executing
Incentives

- 2010: AV-Test claims 49M strains of computer malware in the wild
- 2011: McAfee reports 2M new pieces of malware/ month
- 2013: Kaspersky says 200k per day
- Security software: $20B 2012
  - But detection rate?
  - 5%
The game has changed

- More zero days
- Stealth over noisy entry
- Emerging technology: just trusting it!
Chapter 2: System Crash
Dependence on systems

- Credit cards & ATMs
- Trains, police cars, ambulances, fire trucks
- Water, electricity, gas
- The list goes on...
The game has changed: revisited

- Organized crime
  - Electricity grid Rio de Janeiro
  - Shodan: hacker database
- Nation states, hacktivists, insiders, spies, script kiddies
- Internet teaching terrorists
- China (41% of all worldwide attacks according to Akamai!), Russia, US
- “5th domain”- US military (after land, sea, air, space)
Chapter 3: Moore’s Outlaws
Exponential growth
What it feels like
Computing

- Apollo 11 vs. smartphone
- 1M times cheaper
- 1k times faster
- Leverage for crime
Lines of code

- Apollo 11: ?
- Microsoft Office 2013: ?
Lines of code

- Apollo 11: 145k
- Microsoft Office 2013: 45M
Lines of code, visualized
Chapter 4: You’re Not The Customer You’re the Product
The truth will set you free, but first it will piss you off.

- Gloria Steinem
Case Study: PatientsLikeMe

- A website for people with illnesses to meet other people with the illness
- Customers were notified of a breach by people scraping the site
- Turns out it was the Nielsen Company
- According to the privacy policy, this was completely legal!
- It was easy to use information to reverse engineer who you were and identify medical information
What they never told you

- The internet seems like a pretty good deal - you browse social networks like Facebook and use Google... for free!
- Or so you think -- the reality is that Google and Facebook are siphoning off tons of data every second you use it
- The privacy policy lets them collect almost any data
- They are getting more value out of you than you are out of the product
Your leaking info - how does it happen?

- Cookies and tracking files -- websites will attach cookies to your session when you visit a site and gather data about your internet usage
  - Example -- dictionary.com used a total of 234 tracking files per person
- Friends and family leak data as well through pictures, tags, and birthday posts, etc.
- Long privacy policies that are not read
  - Gamestation inserted clause that granted the customer’s immortal soul to them
Smart Devices are Tracking Devices

- Your smart phone is on you all time and always running
- People use smart phones to search and social network at almost all times of the day giving more data
- Google provides your information to apps and listening in on phone calls for background noise filtering
- 65 billion app store downloads -- apps are addicting due to immediate gratification
  - Each app has a privacy policy that can collect information about you
- Angry Birds collects location information?
Location, Location, Location

- Locational data is being attached to online transactions - often times this is unnecessary
- Sometimes people see it as a benefit e.g. Tinder - however, this can be used in a predatory way
- Advertisers - they don’t only care about where you are now but where you will be tomorrow or yesterday
- These people know a lot about your location but you know mostly nothing about them
Chapter 5: The Surveillance Economy
In the digital era, privacy must be a priority. Is it just me, or is secret blanket surveillance obscenely outrageous?

- Al Gore
Data Brokers

- Acxiom, Epsilon, Datalogix, Rapleaf, Reed Elsevier, BlueKai, Spokeo, Flurry to name a few
- Rapidly emerging industry -- worth $156 billion/year
- Get data from a variety of sources (e.g. credit card companies, mobile providers, banks, online activity)
  - Imagine how much information you give out in the form of social media interactions and likes
- Goal is behavioral targeting/marketing i.e. sell ads
  - E.g. it would be a waste of money to target ads about pregnancy for male users on a particular website
Analyzing You (Examples)

- You look up hotel rooms on Miami beach and then buy a swimsuit from Amazon
  - A machine may predict that you are going to Miami soon
- You use a calendar to schedule appointments. Your phone also tracks location
  - Google GPS may tell you that you have to leave soon if you want to catch your app.
- MIT study could detect your sexuality with 78% acc
- Phone proximity implies infidelity
But I have nothing to hide!

- “If you have something to hide maybe you shouldn’t be doing it...” - Schmidt, CEO Google
- Dichotomy between total surveillance and assuming that you’re a criminal is the wrong way to go
- Data collectors know who has searched for what
- Your privacy today may be more important for the future rather than the present
- Maybe something that seems innocuous today may manifest itself as a **Future Crime**
Privacy Risks & Unpleasant Surprises

- Daughter received coupons for baby clothes and parents found out she was pregnant
- If a husband takes his wife to court for being a bad parent he can use her many logged hours of video games as proof
- Employers can see your friends on Facebook and pictures
- There are very little regulations today on what data companies can and can’t keep
Chapter 6: Big Data, Big Risk
Goodman’s Law

“The more data you produce and store, the more organized crime is happy to consume”
2008 Terrorist Siege in Mumbai

- LeT terrorist group had a command-center in Pakistan during the siege
  - Command center monitored live news such as BBC, Al Jazeera, and local stations as well as social media platforms in real-time
  - Relayed information to terrorists in Mumbai
- Tweet of helicopter landing on top of building prepared them for ambush
- News channel reporting their suspected location alerted them to reposition to avoid capture
- Almost any platform can be used in ways other than how it was intended
Data is the New Oil

- How would 10 million barrels of oil be protected? Versus how data aggregators protect the petabytes of data they collect

- Google, Facebook, Target, etc. are the biggest targets
  - Reward is high and risk is low
  - Ex: 600,000 Facebook accounts compromised EVERYDAY
Trusted Data Brokers

- In 2013 Experian mistakenly sold identity information on two-thirds of the population to a Vietnamese organized crime group
  - Hackers posed as a private investigation firm based in the U.S.
- Full information leak
  - Leaked information was sufficient enough to open credit cards and take out loans
- Experian had no clue who they were
  - No red flags were raised even after the data was sold
- Can third party data brokers be relied upon?
Burglary 2.0

- Burglars don’t need to stake out houses and look for telltale signs
- Online websites that automatically scrape location data from tweets and social media check-ins into searchable database
  - Many successful burglars reported to have used
- Study shows that 78% of burglars admitted to using social media platforms to pinpoint a specific house
- Your own actions can be easily used against you
Chapter 7: I.T. Phones Home
“Hackgate” Scandal

- British newspaper discovered in 2011 to have been hacking voicemails
  - Prominent and high profile individuals had their phones hacked, including the royal family
- Hacking had been going on since early 2000’s
- Scandal only uncovered due to a murder investigation
- Mobile phones are more complex and store more data now than in early 2000’s
Current State of Phone Hacking

- Major security vulnerability with Android smartphones
  - Easy to bypass Google Play Store’s algorithms
  - Even worse, possible to download apps from unofficial app stores
- “Innocent” apps that actually collect information about you
  - Also exist fake/imposter apps
- Essentially Goodman’s Law at play
Location Data

- Most smartphones have GPS capability
- Latitude/longitude coordinates invisibly embedded into photos you take
- Army soldiers in Iraq gave away coordinates of secret base by posting a photo to Facebook
  - Enemy combatants monitored those Facebook accounts and used location info to launch a precise mortar attack
- Another example of information you provide unintentionally being used against you
Mobile Phones & Corporate Espionage

- Corporations may invest in their network security
- A network is only as secure as its weakest link
  - Personal devices and cell phones brought in by employees
- Gain access to one device on the network, use it as a pivot to access almost anything else
- Hacked “femtocells”, a cell phone signal booster
  - Make nearby cell phones think it is a legitimate cell tower
- Cell phones have become the most common personal computer
Chapter 8: In Screen We Trust
In Screens We Trust

- We no longer walk through life using our five senses
- Our experience is mediated by screens whose information is at best an approximation of reality and is subject to manipulation
StuxNet

Context

- Iran developed successful nuclear refinement facility
- US & Israel grew concerned about nuclear weapons development

The StuxNet worm

- Phase 1: observe correct behavior of centrifuges
- Phase 2: alter centrifuge behavior but report correct behavior
- "human operators in control room had no idea their reality had been hijacked"
Yelp Reviews

Nielsen Study

- 90% of consumers say online reviewers influence their buying decisions
- 70% trust online reviews as much as recommendations from friends
- But, 25% of Yelp reviews are fake

Real people. Real reviews.
Electronic Medical Records

A Deadly Case

- Hospitals are rushing to digitize patient records; the rush to convert records leads to inaccuracies
- At a London hospital, after an inaccurately entered prescription order, staff gave Gary Foster, a 27 year old, a lethal dose of chemotherapy.
Wrongful Release & Imprisonment

Dangerous Glitches

- In California, a computer glitch directed prison guards to release 450 gang members, rapists, and armed robbers.
- In England, data errors led 20,000 innocent individuals to be branded as criminals.
In Screens We Trust

- We rely on digital information with no regard for its accuracy.
- There are few safeguards even in domains as critical as healthcare and government.
Chapter 9: Mo' Screens, Mo' Problems
Mo' Screens, Mo' Problems

- In a world where we accept virtual information blindly, new forms of crime are emerging.
Phishing

Coca Cola's Failed Merger

- To expand into Asia, Coke planned an acquisition of China's Huiyuan Juice Group. Negotiations were going well until the deal inexplicably fell apart.
- The Chinese government had spoofed an email to a Coke Vice President which installed a keylogger on his computer, giving them access to all of Coke's negotiation strategies.
Market Manipulation

Forging Press Releases

- A 23 year old community college student, Mark Jakob, forged a fake, extremely negative press release for Emulex Corporation, a company he had shorted, and forwarded it to Internet Wire, a distributor of corporate announcements.

- The press release was picked up by Bloomberg and CNBC prompting the stock to plummet by $61/share, earning Jakob $250,000.
"SWATing"

- Many services exist allowing one to spoof any caller ID or phone number.
- This enables callers to spoof numbers in other cities or even states, call 911, and falsely report a shooting at anyone's house prompting an armed SWAT team to barge into their house.
- This occurs frequently to celebrities including Ashton Kutcher, Justin Bieber, Tom Cruise, Rihanna, and Miley Cyrus.
GPS Jammers

Intentional and Unintentional Mayhem

- GPS jammers are so freely available that truck drivers regularly use them to prevent their employers from tracking them. This inadvertently affects neighboring vehicles, office buildings, and even air traffic control towers in the vicinity.

- An organized crime group also used this technology to steal forty large tractor trailers with cargo worth in excess of $10 million.
HIjacking TSA X-Ray Machines

The TSA's Antiquated Software

- The viewing software for the TSA's X-Ray machines runs on Windows 98 and Windows XP, operating systems with thousands of documented vulnerabilities.
- It's possible to commandeer the viewing software to allow luggage full of guns to appear as luggage full of suits and sunscreen.
Social Media Manipulation

Putin's Propaganda

- The Kremlin pays "Internet operators" $36 to write at least a hundred pro-Putin posts per day, amounting to over 40,000 comments a day on his behalf.

- Whenever the Russian press writes about gay rights or opposition candidates, his social media army instantly strikes back.
Chapter 10: Crime, Inc.
Crimeware

Innovative Marketing’s technique

- A software that commits crime (also known as scareware or ransomware).
- Malicious computer program that plays on a user’s fear of virus infection.
- Customers never actually had a virus, instead their browsers and operating systems were hijacked.
- Company would activate the crimeware and force users to pay to protect their computers from nonexistent viruses.
Modern times call for modern crimes

Technology makes crime more efficient and criminals are perpetual early adopters of all things tech.

- Cyber crime is borderless and offers great anonymity.
- Prosecutions are exceedingly rare, occurring less than one one-thousandth of 1% of all cases.
- 80% of hackers are now working with or as part of an organized crime group.
Lack of available mules is the key bottleneck facing Crime, Inc. today.

- Mules are the face of cyber crime and operate in true name, meaning they have a very short shelf life.
Hackers are the new Mafia.

- And are contributing daily to the ever-increasing industrialization and professionalization of crime.
Crime U

Hackers are not born, they are trained, supported and self-taught.

- Enormous amount of free educational material in the digital underground.
- Detailed links arranged by category, on how to hack every possible device, app, software, and operating system in existence.
In the world of “In screen we trust” the public is easy to deceive.

- Technology makes it easier to crowdsource its work to unwitting co-conspirators who have no idea they are taking part in an illicit plot.
Apple’s Touch ID took 1 day to crack.
Crime, Inc. is a business and a highly profitable one.

- Uses freemium pricing, gamification, crowdsourcing, crowdfunding, reputation engines, just-in-time manufacturing, online training, and swarms for distributed project management in pursuit of the long tail of crime victims around the world.
Chapter 11: Inside the Digital Underground
Silk Road

“eBay of drugs and vice”

- Offered every possible illicit product imaginable, neatly organized by category such as drugs or weapons, each with accompanying pics and descriptions.

- Products included: stolen bank accounts/cards, counterfeit currency, computer viruses, compromised FB accounts, tutorials on hacking ATMs, child pornography, hit men for hire...

- All parties buying and selling (on Silk Road) remain anonymous.

- Only form of payment was Bitcoin.

- Officials had no idea to stop it, because it was not a standard website → (next slide)
The Onion Router (TOR)

Closest thing to actual anonymity on the Internet

- Works by routing your Web connections through a worldwide array of five thousand computer servers in order to hide the source and destination of your connection.

- Routing the traffic through multiple cities all around the world → Nearly IMPOSSIBLE to trace.
Dread Pirate Roberts

- Founder of Silk Road.
- Through rookie mistakes (such as getting always checking into the same lib in SF) he gets caught as he is in the lib.
- Real name: Ross William Ulbricht
- Net worth was $28.5 million at his time of seizure
Google search misses 99% of the World Wide Web’s Data.

- The Deep Web is a massive five hundred times larger than the surface Web you use and search everyday.
- Deep Web has 7500 TB of info, Google has 19TB.
The Dark Net holds some of the greatest secrets the Internet has to offer and it is where the criminals connect to conduct their illegal activities.
The Dark Net

Elite realm of criminal digerati

- Need approval to get in, but once you are accepted the world is your oyster.
- Among some of the things the dark net has to offer: pirated content, drugs, counterfeit currency, stolen luxury goods/electronics, cards/accounts, identity theft, documents, weapons/ammunition/explosives, hit men, child sexual abuse images, human trafficking, human organ trafficking, live child rape
With an untraceable illicit monetary system in place, crime is no longer something you just commit, it is something you can buy.
Computer Scientists lost their innocence in 2009 when they first started using malware as an offensive attack weapon.
Ever wonder why your computer runs so slowly?

- You may be unwittingly participating in an ongoing cyber attack against others, and you have no idea it’s happening.
With these systems in place, the depth and global reach of Crime, Inc.’s power mean that crime now scales, and it scales exponentially.

It is about to become much worse, as we hand Crime, Inc. billions of more targets for them to attack as we enter the age of “anytime and everywhere” computing and the Internet of Things.