

THE ROLE OF GEOSPATIAL DATA IN THE LARGER CYBER THREATSPACE

Max Kilger, University of Texas at San Antonio



Educational Objectives

- The costs of a data breach
- Ransomware – how much is your data worth to you?
- Learn about the six individual motivations of malicious online acts
- Uncover the dynamics of the threat relationships between Nation States and Non-Nation State Actors
- Understand the value of geospatial data from a national security perspective

What can a data breach cost you?

Consequences of a Data Breach

Direct Breach Costs

- Global average cost per breach: 3.92 million USD and 3.9% customer turnover
- < 1% customer turnover : 2.8 million USD
- 4%+ customer turnover: 5.7 million USD



Breach Timeline

- Average time to discovery: 206 days
- Average time to contain a breach: 73 days
- Total breach lifecycle: 279 days



2019 Cost of a Data Breach Report, Poneman Institute and IBM Security

Cost by Cause of Breach

- Average cost due to malicious cyberattack: 4.45 million USD
- Average cost due to human error: 3.5 million USD
- Average cost due to system “glitch”: 3.24 million USD



Ransomware

How much is your data worth to you?



What is Ransomware?

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

-TrendMicro



Current Statistics

A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. (Source: Cyber Security Ventures)

1.5 million new phishing sites are created every month. (Source: webroot.com)

Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)

A total of 850.97 million ransomware infections were detected by the institute in 2018.

34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky)

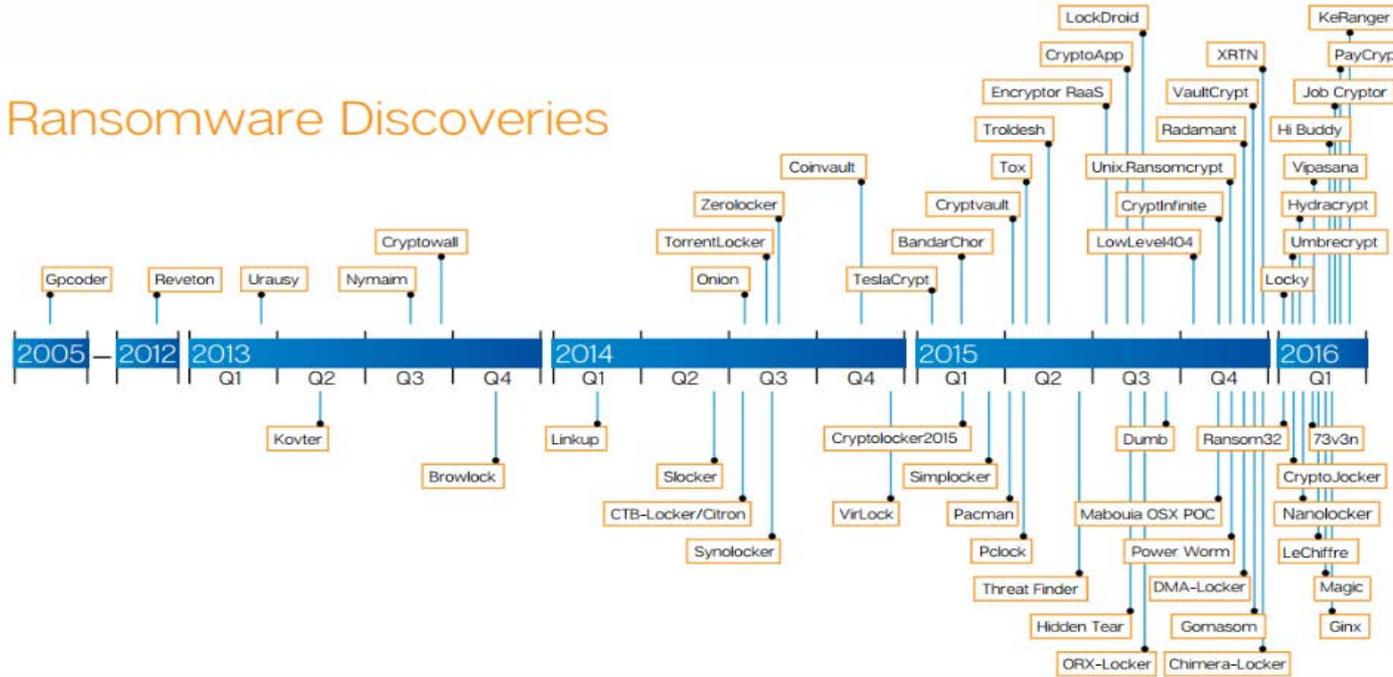
In 2019 ransomware from phishing emails increased 109 percent over 2017. (Source: PhishMe)



Source: <https://phoenixnap.com/blog/ransomware-statistics-facts>

Ransomware Evolutionary Timeline

Ransomware Discoveries



<https://heimdalsecurity.com/blog/anti-ransomware-protection-plan/>

Some Popular Ransomware Examples

- Cryptolocker
- DMALocker
- Jigsaw
- Mamba
- Petya
- Wannacry
- Bad Rabbit



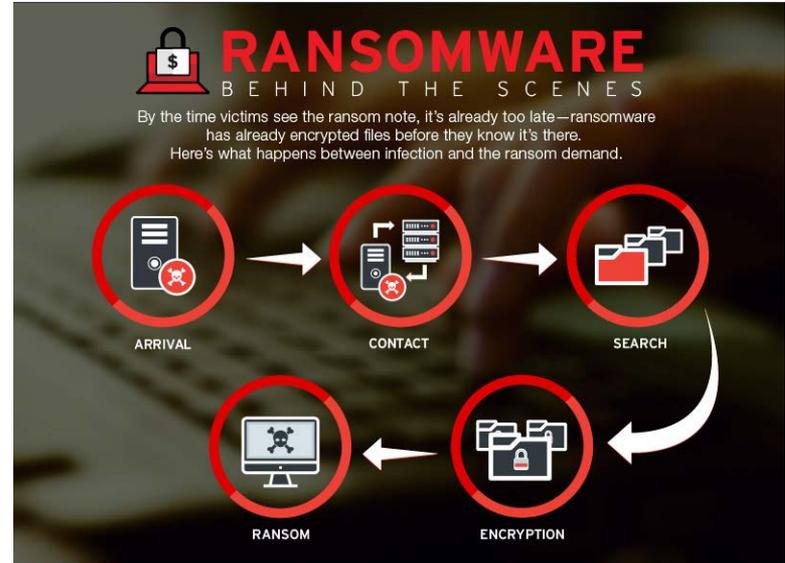
The Three Basic Types

- Scareware
- ScreenLockers
- File Encryption



Ransomware Infiltration Methods

- Infected email attachments that are opened
- Visits to infected websites
- Exposure to malvertisements
- Malware infected by ransomware
- Attacks on unpatched servers
- External devices like thumb drives
- Remote desktop protocols
- IoT devices
- Mobile malware and ransomware
- USB sticks



Protecting Yourself

- Backup, backup, backup (3-2-1 rule)
- Patch your OS and software
- Patch servers
- Endpoint protection
- Keep firewalls tight
- Deploy endpoint protection
- Have emails scanned for threats
- Remove browser plugins like Flash
- Disable Powershell for Windows users
- Turn off macros and ActiveX for MS Office
- Turn off Autoplay
- Use security products with advanced features such as sandboxing



It's too late – now what?

- The Federal Bureau of Investigation recommends never paying the ransom
- Check to see if there is a free decryptor tool. You can find tools to ID the ransomware infection and locate free decryptor tools here

<https://heimdalsecurity.com/blog/ransomware-decryption-tools/>

- Disconnect all infected machines from network
- Identify the ransomware family and particular variation
- Acquire a security product specific for removing that threat and use it
- If you do not have a strong IT department in terms of security you may want to enlist outside security help to complete remove the threat from your network



Why Do People Do Bad Things on the Net?

Motivations of Malicious Online Actors

Motivations in the Community – MEECES*

- A play off the old FBI counter-intelligence term MICE
- MEECES
 - Money
 - Ego
 - Entertainment
 - Cause
 - Entry to social group
 - Status



* Kilger, M. (2010). Social dynamics and the future of technology-driven crime. *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*. Hershey, PA: IGI-Global.

Motivations: Money



- No news to anyone – a very common motivator in the cybercrime world and perhaps at some point in the near future, the cyberterror community
- Individuals motivated by money still often are found mostly within groups that share this motivation
- Emergence of “currencies” in use
 - Stolen credit cards
 - Stolen bank accounts
 - Root ownership of compromised machines
 - Exploits
 - Virtual assets (QQ coins)
 - “Secret” data
 - Bitcoin and other digital currencies

Motivations: Money



- Money has a powerful effect on social structure and social relations (see B Maurer, 2006, The Anthropology of Money)
- Money acts as a force to attract individuals who are outside the community
- Money as a social object gives these outsiders opportunities for power and prestige inside the hacking community that were formerly not available to them

Motivations: Ego



- Derived from the satisfaction that comes from overcoming technical obstacles and creating code that is elegant and innovative
- Idea of mastery over the machine – getting it to do what you want, often in spite of numerous security obstacles
- The enticing idea of besting a nation-state

Motivations: Entertainment



- Originally an uncommon motivation, it has gained momentum over the past years due in part to:
 - Infusion of less technical individuals into the digital space
 - Expanded social environment in the digital space
 - Emergence of archetypes such as “griefers”
 - Example - objective of malicious online actors to generate lulz – a variation of ‘LOL’ or ‘laugh out loud,’ where individuals find joy in disrupting another’s emotional equilibrium*

Motivations: Cause



- Could be the most serious threat from a national security perspective
- Most common instance of this motivation – hacktivism:
 - the use of the Internet to promote a particular political, scientific or social cause
- Many levels of magnitude from website defacement to the theft of sensitive documents to attacks on critical infrastructure
- This is the most traditional cause for terrorism and cyberterrorism

Motivations: Entrance to a Social Group

- Hacking groups tend to be status homogeneous in nature and this may be the case for cyberterror groups
- This implies there is a certain level of expertise necessary for induction into the group
- Elegant code/exploits are one method for gaining acceptance into the group



Motivations: Status



- Community as meritocracy
 - Skills and expertise in networks, operating systems, hardware, security, etc. used as status characteristics
 - Your position in the status hierarchy – locally and globally – depends in great part on these characteristics
- A powerful traditional motivation within the hacking community and very likely within an emerging cyberterror community
- Cyberterror acts as instances of proving one's status within the cyberterror community

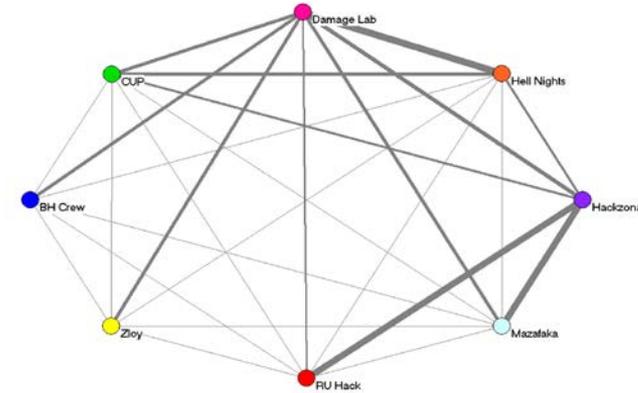
Group Dynamics, Non-Nation State Actors and Nation State Sponsors

Social Dynamics in Cybercrime Networks

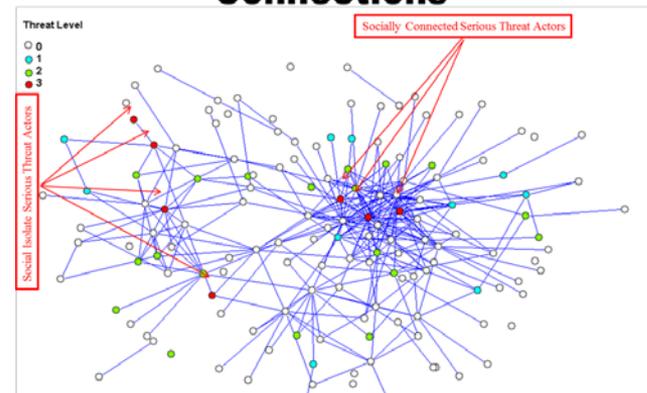
Holt, Strumsky, Smirnova and Kilger (2012) examine networks of online malicious actors from Russian hacking gangs

Identify actors that have multiple memberships and serve as “bridge” between groups

Examine threat level of actor and their location within the network and strength of group ties



Threat Level by Social Connections



Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, 6(1).

Four Stages of Non-Nation State Actor – Nation State Relationships*

Stage 1 - Nation state and non-nation state actors becoming salient to each other through the following mechanisms:

- Attribution of recent attacks
- Identified through ongoing investigations
- Informal contact through hacking cons
- Networked relationships with insiders



* Kilger, M. (2016). The Evolving Nature of Nation State – Malicious Online Actor Relationships. In Holt, T. ed., Cybercrime Through An Interdisciplinary Lens. Routledge: London.

Four Stages of Non-Nation State Actor – Nation State Relationship

Stage 2 – Motivations for actors to collaborate with nation state

- Nationalism and patriotism
- Enhanced status/legitimacy from covert association with state security services
- False flag
- Traditional and non-traditional coercion



Four Stages of Non-Nation State Actor – Nation State Relationship

Stage 3 – Maintenance of the relationship

- Immunity from prosecution for assistance
- Ignoring unrelated quasi-legal or illegal activities
- Resource assistance in the form of hardware or software
- Ongoing grooming of high status individuals within the groups
- Continued coercion



Four Stages of Non-Nation State Actor – Nation State Relationship

Stage 4 – Dissolution of the Non-Nation State Actor – Nation State Relationship

Collapse of the covert nature of the relationship

Replacement by other more skilled actors/groups

Scapegoating and prosecution

Non-Nation state actors/groups terminate the relationship (an unusual but interesting outcome)



Post-dissolution – One unusual but interesting outcome...

Kilger (forthcoming) suggests that these non-nation state actors/groups may evolve in the following ways:

- Increased technical skill with potential to threaten nation state sponsor
- Proceeds from financial crimes finance more hardware, software, payments to members
- Association with nation state security service lends legitimacy to hacking/cyberterror group



- Non-nation state actors may initiate termination of the relationship and evolve into domestic terrorist groups that utilize cyberspace to attack their own homeland

Geospatial Data, Cyber Security and Threats to National Security

Geospatial Data Applications in Cyber Security

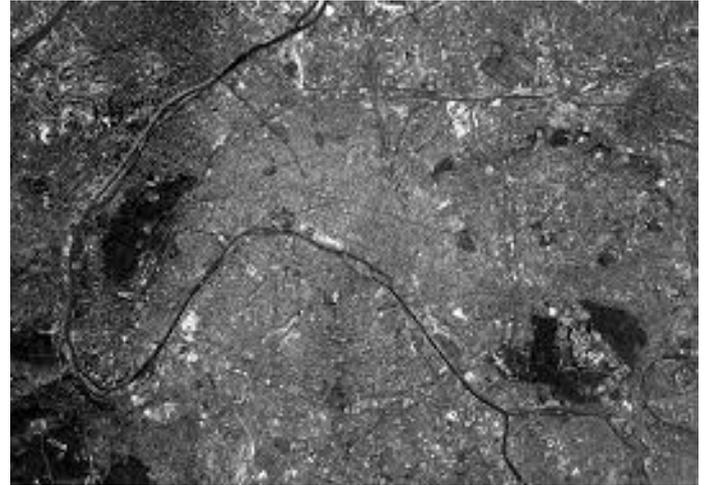
- Identification of Cyber Attacks Using Geo-Temporal Patterns
 - Classification clustering
 - Geo-Temporal time series analysis
 - Geo-spatial data in Support Vector Models and Hidden Markov Models



Gokaraju, B., Durbha, S. S., King, R. L., & Younan, N. H. (2011). A machine learning based spatio-temporal data mining approach for detection of harmful algal blooms in the Gulf of Mexico. *IEEE Journal of selected topics in applied earth observations and remote sensing*, 4(3), 710-720.

Geospatial Data Sources and National Security Concerns

- RAND canvassed a large number of publically available Federal geo-spatial databases
 - 6% of databases classified as potentially useful to terrorists
 - 1% of databases classified as critical in terms of use by terrorist
- Clean up of these databases followed



Baker, J. C., Lachman, B. E., Frelinger, D. R., Tseng, M. S., O'Connell, K. M., & Hou, A. C. (2004). Mapping the risks: Assessing homeland security implications of publicly available geospatial information (No. 142). Rand Corporation.

Geospatial Data and the Mumbai, India Attack

- 10 terrorists with automatic weapons and grenades
- Attack began November 26, 2008 2000 hours and lasted four days
- 174 dead and over 300 wounded
- Terrorists were given specific geo-spatial intelligence of the area as well as blueprints of all the four targets – The Taj Mahal Palace Hotel, Oberoi Trident, Nariman House and Chhatrapati Shivaji Terminus



Special Materials

Synergies between terrorist, cybercriminals and transnational crime Organizations (TCOs)



Cybercriminals

- Establishing physical location of special materials
- Recce of sites holding special materials
- Stealing/producing credentials allowing physical access to special materials



TCO

- Established routes and actors for smuggling traditional illicit materials
- Hold relationships with corrupt border and law enforcement officials

Kilger, M. (2016). Evaluating Technologies as Criminal Tools. In M. McGuire and T. Holt (Eds.), *The Handbook of Technology, Crime and Justice*. New York, New York: Routledge.

Constructing Materials, Mechanisms and Packaging

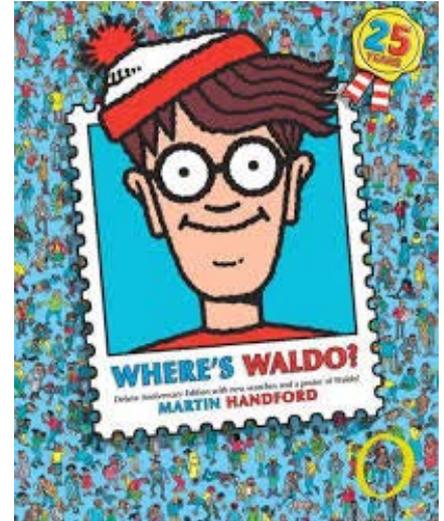
Synergies between terrorist, cybercriminals and transnational crime organizations (TCOs)



- Cybercriminals
 - Stolen secret information on material processing and weapon assembly
 - Identify skilled individuals that can be coerced to cooperate with processing and assembly
- TCO
 - Provide established secure locations normally used for traditional criminal activities as assembly points
 - Transport of the assembled weapon across borders

Where's Waldo?

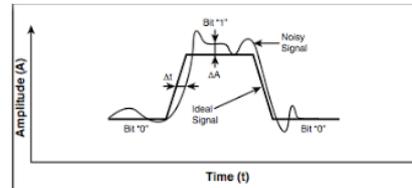
How much do you trust your GPS data?



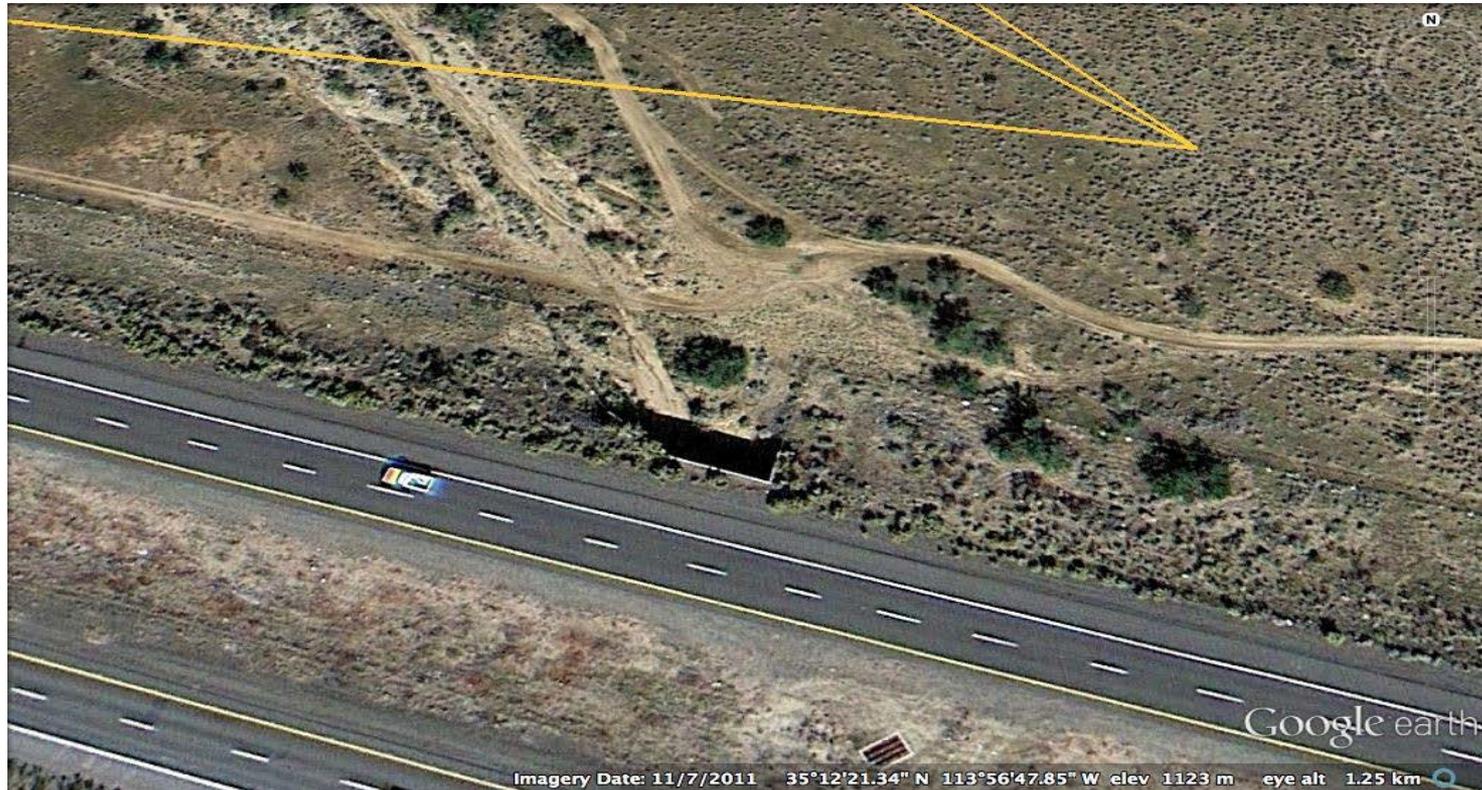
Bonus Round

Sources of GPS Error

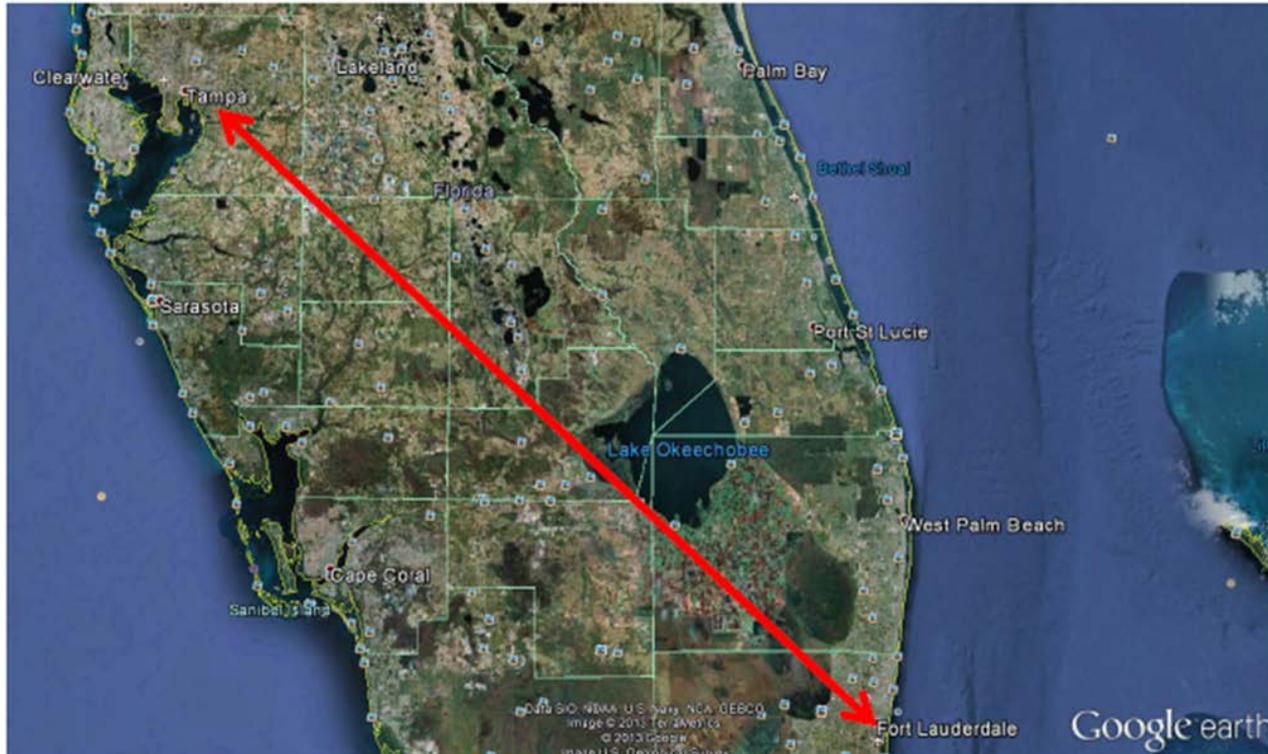
- Clock drift in a chip
- Multipath errors from buildings
- Faraday cage effects
- Signal jitter
- Cell tower signal strength
- Wifi database errors



Breaking Bad Example



Star Trek “Transporter Effect”



Every Consumer Grade GPS Chip has a Defect...



Can you guess what it is? A signed copy of my book to the first person who can tell me what that is...

Contact: max.kilger@utsa.edu