CS 523: Social, Economic, and Legal Aspects of Security

IP Address (Mis)use
Search warrant applications

• Often contain statement that IP addresses are
  – “like physical street addresses” (wrong)
  – “like vehicle license plates” (also wrong)
• Such metaphors wrongly suggest that an IP address corresponds to 1 person or 1 location
  – DHCP (constant change), NAT (address sharing)
  – A whole frat house may have 1 IP address
  – Your mobile’s IP address changes as you cross tower boundaries, and is shared with other mobile users
Corroboration is needed

• Proper corroboration can make it possible to reliably associate an IP address with 1 person or 1 geographic location
  – By using records from ISPs and mobile carriers that give info about the users, over time, of a particular IP address

• Knowledgeable police use such corrobortations
  – Some use IP geo-location services (low accuracy)
Hazards of careless use of IP address

• Severe invasions of privacy
• Waste of time/resources for law enforcement
• Embarrassment for law enforcement
• Often avoidable with little burden on police
  – Do reverse DNS query (reveals info on registrant)
  – Is it a Tor exit relay, a VPN, or proxy server?
  – Could more than 1 person have used IP address?
  – Avoid misleading metaphors in warrants
The “Farm in Kansas” fiasco

• Accused of theft, spamming, fraud
• Visited by FBI, IRS, ambulances trying to prevent suicides, police looking for runaways
• Targeted by vigilantes, threatened
• Why to a farm in the middle of nowhere?
  – A major IP geo-location service’s answer to an IP query was the center of the region of uncertainty
  – For high uncertainty (“anywhere in the USA”) the answer was the center of the USA (= that farm)
Mis-targeted police raids

• Police raids on operators of Tor exit nodes
  – Extensive search of their homes, seizure of their equipment and lengthy forensic analysis thereof
  – A waste of police resources because no node in Tor knows where the traffic originated (but it certainly did not originate at the Tor exit node)

• Police raids on locations providing open wi-fi
  – Arrest, waste of police resources, only to discover that culprit is some unknown user of the wi-fi
Bit Torrent copyright infringement

• U.S. Magistrate G. Brown granted motions to squash subpoenas for ISP subscriber info linked to IP addresses identified in several lawsuits:
  – “The assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded [...] is tenuous, and has grown more so over time”
  – “It is no more likely that the subscriber to an IP address carried out a particular computer function [...] than to say an individual who pays the telephone bill made a specific telephone call”
Fourth Amendment issues

• The Fourth Amendment to the Constitution prohibits unreasonable searches and seizures
  – No search without warrant (need probable cause)

• Courts ruled against warrants based only on rumors or anonymous tips received by police
  – Police are required to do more to confirm the tips
  – Corroborating info or info on informant’s reliability

• EFF: Law should mandate for IP addresses the same skepticism as for anonymous informants