
Attribution and Privacy
John E. Savage
Brown University
Outline

• Review of types of cyber attacks
• Attribution problem
• Methods to avoid attribution
• Detecting attribution
• Alternatives to attribution
• Deterrence on the Internet
• Privacy in the modern world – two relevant papers
  – Untangling Attribution*, Clark and Landau.
  – A Survey of Challenges in Attribution*, Boebert

* Procs. Workshop on Deterring Cyberattacks, National Research Council, 2010
Types of Attribution

• Technical attribution
  – Where are the machines located?
  – Who owns the attacking machines?

• Human attribution
  – Who launched the attack?
  – On behalf of whom is the adversary acting?
Attribution on Internet is Difficult

“On the Internet nobody knows that you’re a dog.”
Recap of Internet-Based Attacks

• Distributed denial of service (DDoS) – botnet based
  – Goal: Overwhelm machines/networks with data.

• Penetration attacks – uses malicious functionality
  – Goal: Control the machine that is attacked.

• Exploitation attacks – a penetration attack
  – Goal: Penetrate to extract valuable information

• Destructive attacks – a penetration attack
  – Goal: Destroy/disrupt valuable system component or attached resource, either temporarily or permanently.
Staging Attacks

• Before an attack on a critical network, an adversary will most likely do reconnaissance
  – The goal of reconnaissance is to map out the network in order to maximize subsequent damage

• An adversary is most vulnerable to technical attribution during the reconnaissance phase

• Later the adversary can hide behind proxies
Effect of Assigning Attribution

• Reliable attribution can deter attacks
  – If attackers know they will be identified and punished, they are less likely to attack
• Attribution may be used to halt attacks
  – If attacker IDs known, a response may be possible.
  – E.g. Knowledge of botnet owner my permit authorities to halt/reduce botnet traffic
  – A “hack back” might also be possible
  – DDoS attacks might be stopped if attack IPs known
Proxies

• A proxy is a computer to intercept and possibly alter communication traffic
  – Lots of public proxies, e.g. Burp Suite and mitmproxy
  – They provide services, e.g. filtering, authentication, etc
  – Known as “hop points” when used for malicious activity

• Proxies have positive uses
  – They can help debug a website

• They have negative uses
  – They can hide traffic, as in The Onion Router (TOR)
Barriers to Technical Attribution

• Anonymous proxy
  – Hides source
  – E.g. Network Address Translators (NATs)

• Onion routing (see following slides)
  – Defend against network surveillance.
  – E.g. Tor and Freegate

• Covert communications
  – E.g. Steganography: message hidden insider another
Tor Onion Routing

• Goal is to hide Internet communications.

  ![](image1.png)

• Here Alice picks proxy nodes $P_1$, $P_2$, $P_3$. Encrypts message and destinations (see next slide). No machine can know all the machines that Alice uses.

• Tor developed by US Naval Research Labs for USG.
Onion Routing

- Alice forms message $M_3$ containing message $M$ and destination Bob using $P_3$’s public key.
- Alice forms message $M_2$ containing message $M_3$ and destination $P_3$ using $P_2$’s public key.
- Alice forms message $M_1$ containing message $M_2$ and destination $P_2$ using $P_1$’s public key.
- The outer onion ring is sent to $P_1$, who sends it to $P_2$, then to $P_3$, and then to Bob.
Onion Routing

- Proxy $P_1$ decrypts $M_1$ with its private key, sends result to $P_2$ who decrypts $M_2$ with its private key and sends it to $P_3$. Finally, $P_3$ decrypts $M_3$ (to reveal $M$ and Bob’s IP address) and sends result to Bob.
- Generalizes to more proxies. Public-key infrastructure (PKI) used.

![Diagram of Onion Routing with layers of encryption and decryption]

- Encrypted with public key of $P_1$  
  - Message $M$  
  - Dest. Bob  

- Encrypted with public key of $P_2$  
  - Encrypted with public key of $P_3$  
  - $M_1$  

- Dest. $P_3$  

- Dest. $P_2$
Botnets

• A botnet consists of thousands to millions of computers under centralized control
• Malicious botnets are controlled by a bot herder.
  – Botnets controlled by command-and-control (C&C) server or, more recently, via a peer-to-peer (P2P) network.
• Control communication often hidden via
  – Covert channels, such memory or timing
  – Fast flux – IP addresses for delivery sites changed rapidly often via DNS round robin with short time to live
# Notable Botnets

<table>
<thead>
<tr>
<th>Name</th>
<th>Created</th>
<th>Dismantled</th>
<th>Size (# bots)</th>
<th>Spam (bn/day)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BredoLab</td>
<td>2009</td>
<td>2010 (partial)</td>
<td>$30 \times 10^6$</td>
<td>3.6</td>
</tr>
<tr>
<td>Mariposa</td>
<td>2008</td>
<td>2009-Dec</td>
<td>$12 \times 10^6$</td>
<td></td>
</tr>
<tr>
<td>Conficker</td>
<td>2008</td>
<td></td>
<td>$10 \times 10^6$</td>
<td>10</td>
</tr>
<tr>
<td>Zeus</td>
<td></td>
<td></td>
<td>$3.6 \times 10^6$</td>
<td></td>
</tr>
</tbody>
</table>

- BredoLab propagated primarily via malicious email attachment. Armenian developer arrested but it remains in operation in Russia and Kazakhstan.

- Mariposa, run by Spaniards, was used to collect passwords, bank credentials and credit card information. Also used for DDoS, spam, and adware.

- Conficker is a stealthy worm for Windows OS. It infected many European military computer systems. French naval aircraft grounded when flight plans unavailable.

- Zeus is a trojan horse worm for Windows OS. Often used to steal information via a man-in-the-browser keystroke logging and form grabbing. It has been used to install CryptoLocker ransomware. Appears to be Eastern European in origin.
Identity Theft is a Problem

• **US DoJ says** 16.6 million Americans had identities stolen in 2012 at cost of $25 Billion.

• Identity Theft Resource Center says 675,000,000 US records lost in breaches since 2005, 1/12/15
  – Several types of identity theft

• Small fraction of breaches lead to identity theft.
  – Attacker must build profile
  – More profit available by using credit card info

• Many techniques are used to steal identities.
Identity on the Internet

• Secure real identities and pseudonyms are possible and needed on the Internet.
• Identity can be assured via public-key encryption
• Secure pseudonyms possible via trusted 3rd parties
  – They are trusted by parties engaged in a transaction
  – See National Strategy for Trusted Identities in Cyberspace (NSTIC) on the NIST website
• Anonymous credentials - a person proves they have authority for a transaction without giving up their identity – Jan Camenisch & Anna Lysyanskaya (2001)
Detecting Attribution

• IP addresses can be used for geo-location. See – Services can locate address to within city > 90% time
• Multistage attacks – many hop points between attacker & victim. Hard to peel back but doable.
• Knowledge of source IP address helpful to police – Identifies jurisdiction, can lead to search warrant.
• Following the money very useful for cybercrime
• Onion routers – Is traffic analysis possible?
Possible National Approaches

• In 2004 an ITU officer *proposed* that
  – IPv6 address blocks be allocated by states
  – It would “harden” the linkage between IP addresses and other information.

• What are advantages and disadvantages?
  – It would be easier for states to identify and punish citizens for activity that they declare illegal.
  – It would clearly identify states with malicious activity and provide other states with a lever to request action.

• What other implications might follow?
Nature of the Attribution Problem

• Clark and Landau:
  – A policy problem, not a technical one.
  – Attribution of forensic quality in US not possible.
  – Application level attribution via cryptographic means is possible.
  – Don’t believe that fine-grained attribution is either desirable from a privacy point of view or desirable
  – Multi-stage attacks a major unsolved problem.
  – Deterrence must be achieved by tools of the state
Deterrence Alternatives

• Hack back – **13 bugs found in exploit kits**
  – Law enforcement might use them
• Mount covert preemptive attack against sites suspected to be planning an attack.
• Human operators might be identified via biometrics, such as keystroke analysis, venue, time of day, holidays, language, etc.
Deterrence in General

• Individuals deterred from aggressive action by
  – Likelihood and severity of retribution
  – Risk of failure
• But hack backs may have unintended consequences
  – “blow-back” on friends and self
• Cyber attacks
  – Generally do not have kinetic effect
  – Level of certainty of effect is obstacle to attack
• Note: Response to attack need not be immediate.
Current Attitudes Toward Privacy

• Is privacy that important in today’s society?
• What are we doing to protect it?
• Today’s WSJ has an article saying that Facebook is offering a new product called Topic Data
  – Companies can learn what Facebook users are saying about brands, products, events and activities
  – http://www.wsj.com/articles/facebook-takes-on-new-role-marketing-consultant-1426036185
Can We Have Privacy in Digital Age?

• Not if we willingly give up personal info in return for a free service. Consider
  – Facebook
  – LinkedIn
  – Hotmail and Gmail

• We are a country of laws
  – We can ask for laws protecting private data
  – Will we?
We Can Learn from Pacific Islanders

• Dan McGarry, Canadian and Pacific islander
  – In village life collective gaze keeps everyone in line
  – Where peace is valued over liberty, privacy is rarity
  – However, excessive surveillance is not good for chief

“Chief Ieru from Tanna Island in Vanuatu. We’d never met before, but he knew where I lived.” by Dan McGarry, *Pacific Politics*, August ‘13
Is Privacy an Anomaly?

• Sean Kanuck, National Intelligence Officer for Cyber Affairs¹:
  – “It is arguable that the last 200 years of industrialized anonymity in urban centers was a privacy anomaly in human history.”

• National Intelligence Council is IC’s center for strategic analysis.

1. AFCEA Global Intelligence Forum, July 30, 31, 2013
Zuckerberg’s View of Privacy

• “You have one identity ... The days of you having a different image for your work friends or co-workers and for other people you know are probably coming to an end pretty quickly ... Having two identities for yourself is an example of a lack of integrity.”

  Mark Zuckerberg, Facebook

• Facebook’s business model relies on each user’s profile being genuine.
Some Issues to Consider

• How much privacy do you expect?
• Can you rely on business to provide it?
  – How do profit and competition affect privacy?
• Can we rely on government for security?
  – Do they have competing interests?
  – Can they play a role concerning cyber crime?
Review

• Review of types of cyber attacks
• Attribution problem
• Methods to avoid attribution
• Detecting attribution
• Alternatives to attribution
• Deterrence on the Internet
• Privacy in the modern world