CSCI 1800 Cybersecurity and International Relations

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
• Intro to deterrence on the Internet
• Based on
Types 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.
The Attribution Problem

• Attribution important in deterring attacks.
  – If attribution of attacker is known to be easy, attackers may be deterred by threat of retribution.

• Attribution is known to be hard. Why is it?
  – Technical attribution
    • Who owns the attacking machine?
    • Where is the machine located?
  – Human attribution
    • Who actually launched the attack?
"On the Internet, nobody knows you're a dog."
Coping with Attacks

• Distributed Denial of Service (DDoS) attacks
  – Difficult to stop. Attribution not very helpful given that it must be stopped ASAP.
  – Retribution after the fact not a good deterrent. Attacker is hard to find.

• However, attacks on critical infrastructures do require significant reconnaissance effort.
  – A diligent defender might catch the attacker in the act and, possibly, stop the attack.
Barriers to Technical Attribution

• Botnets – thousands to millions of nodes.
  – Used for DDoS, spam, phishing, password attacks
• Proxy
  – Host provides services, e.g. filtering, authentication, etc.
• Anonymous proxy
  – Hides source, e.g. Network Address Translators (NATs)
• Fast Flux – quick change in IP addresses
• Anonymous routing – The Onion Router (Tor*) & Freegate**
  – Defend against network surveillance.
• Covert communications
  – E.g. Steganography: message hidden inside another message

* For Tor see https://www.torproject.org/
** For Freegate see https://en.wikipedia.org/wiki/Freegate
Tor Onion Routing

- Goal is to hide Internet communications.

- Here Alice picks 3 proxy nodes. 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 sends message $M_1$ to proxy $P_1$.
- Proxy $P_1$ decrypts $M_1$, sends result to $P_2$ who decrypts $M_2$, and sends it to $P_3$. Finally, $P_3$ decrypts $M_3$ (to reveal $M$ and $D$) and sends result to Bob.
- Generalizes to more than three proxies. Public-key infrastructure (PKI) used.
Identity on the Internet

• Secure real identities and pseudonyms are possible and needed on the Internet.

• Identity can be assured via public-key encryption
  – User has public and private keys
  – Messages can be encrypted with one, decrypted with other
  – Only user can decrypt with private key, which assures identity

• Secure pseudonyms possible via trusted third parties.
  – Third parties are trusted by persons who acquire pseudonyms from them as well as entities who engage in transactions with third parties.
Identity Theft

• US Bureau of Justice Statistics says 17.6 million Americans had identities stolen in 2014.
• Many techniques are used to steal identities.
• $45 million stolen* from thousands of ATMs!
  – Processors of Visa and MasterCard prepaid debit cards hacked. Limits on accounts raised.
  – Cashing crews in > 24 countries withdrew funds.
  – In 12/2012 raised $5 M. 2/2013 raised $40 M more.

Detecting Attribution

- IP addresses can be used for geo-location*
- Services can locate address to within city > 90% time
- Onion routers – Can traffic in/out be correlated?
- 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.

* See http://www.maxmind.com/
A National Approach to Attribution?

• 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 desirable from a privacy point of view.
  – Multi-stage attacks a major unsolved problem.
  – Deterrence must be achieved by tools of the state.
Deterrence Alternatives

• Hack-back* – attack the attacker.
  – Appears to be illegal under US law.
• Mount covert preemptive attack against sites suspected to be planning an attack.
• To identify humans, it may be useful to record and replay intruder actions to identify him/her via keystroke analysis, venue, time of day, observance of holidays, language, etc.

* See http://www.theregister.co.uk/2010/06/17/exploiting_online_attackers/
Deterrence in General

• Individuals deterred from aggressive action by
  – Likelihood and severity of retribution
  – Frustration

• But actions 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.
Review

- Review of types of cyber attacks
- Attribution problem
- Methods to avoid attribution
- Detecting attribution
- Alternatives to attribution
- Intro to deterrence on the Internet