CSCI 1800 Cybersecurity and International Relations

Attribution and Privacy

John E. Savage

Brown University

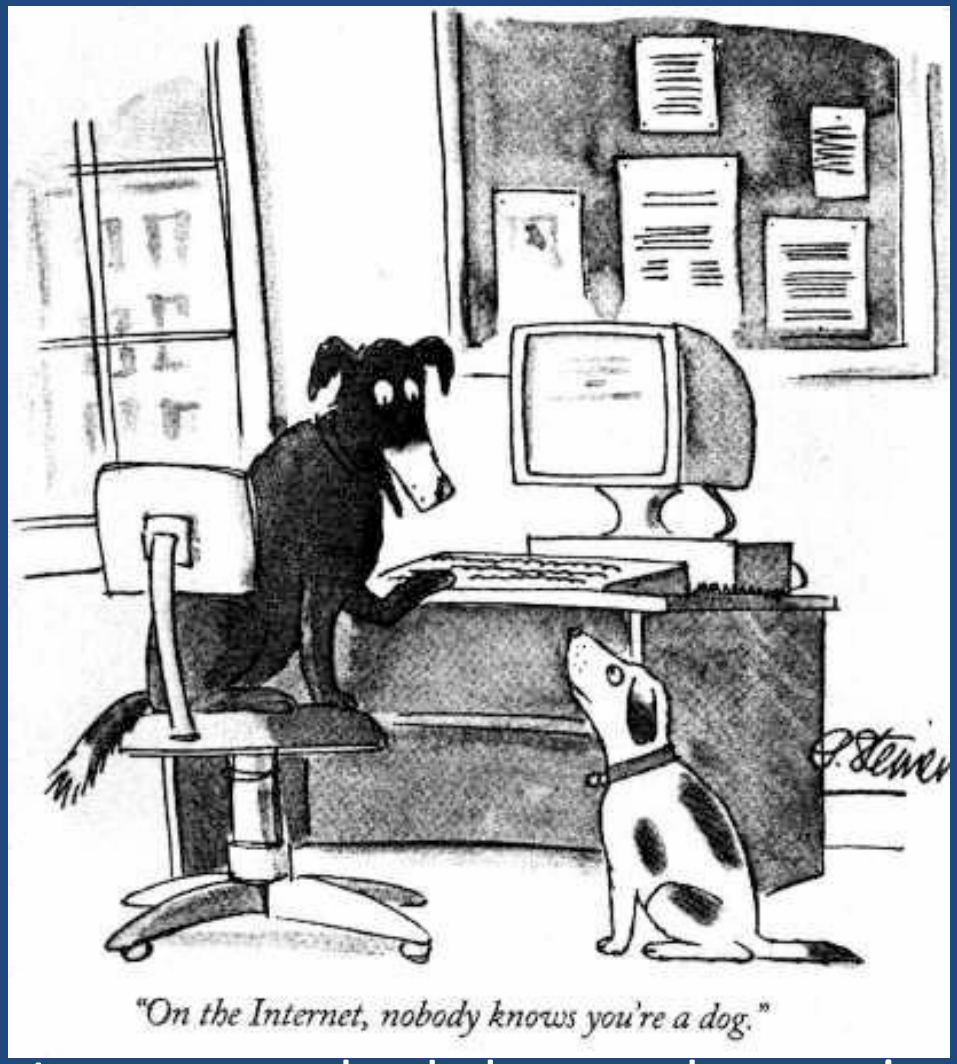
Outline

- Review of types of cyber attacks
- Attribution problem
- Methods to avoid attribution
- Detecting attribution
- Alternatives to attribution
- Intro to deterrence on the Internet
- The impersonation problem
- Based on
  - Untangling Attribution, Clark and Landau, Procs. Workshop on Deterring Cyberattacks, National Research Council, 2010.
  - A Survey of Challenges in Attribution, Boebert, Procs. Workshop on Deterring Cyberattacks, National Research Council, 2010.

Types of Internet-Based Attacks

- Distributed denial of service (DDoS) – botnet based
  - Goal: Overwhelm with data, possibly using amplification
- 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



"On the Internet, nobody knows that you're a dog."

The Attribution Problem

- Attribution important in deterring attacks.
  - If attribution of attacker were 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?
    - Is the attacker hiding behind a proxy?
  - Human attribution
    - Who launched the attack?
    - For whom was that person acting?

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.
  - Best bet: hire orgs with "big pipes" that can filter data
- Attacks on critical infrastructures require significant reconnaissance effort.
  - A diligent defender might catch the attacker in the act and, possibly, stop the attack.

Barriers to Technical Attribution

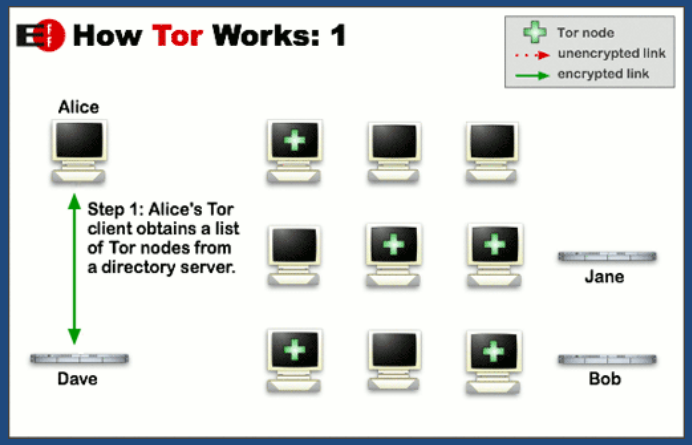
- Botnets – thousands to millions of nodes.
  - Used for DDoS, spam, phishing, password attacks
- Proxy
  - Host provides services, e.g. filtering, authentication, etc.
- Anonymous proxy
  - Hides source, e.g. Network Address Translators (NATs)
- Fast Flux – quick change in IP addresses
- Anonymous routing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

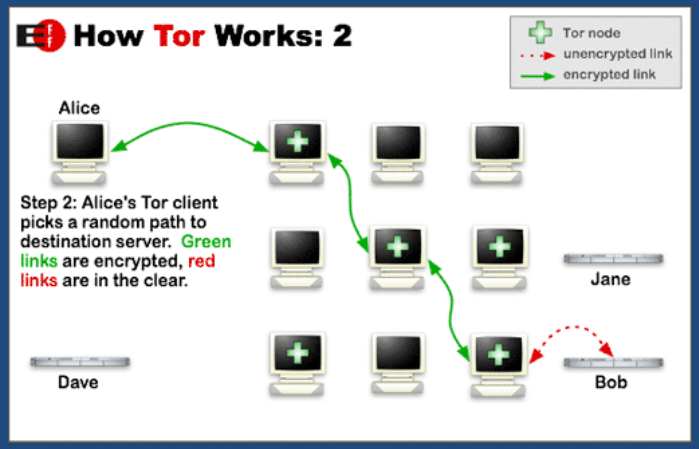
* For Tor see https://www.torproject.org/

** For Freegate see https://en.wikipedia.org/wiki/Freegate

The Onion Router (TOR)

- Goal is to hide Internet communications.

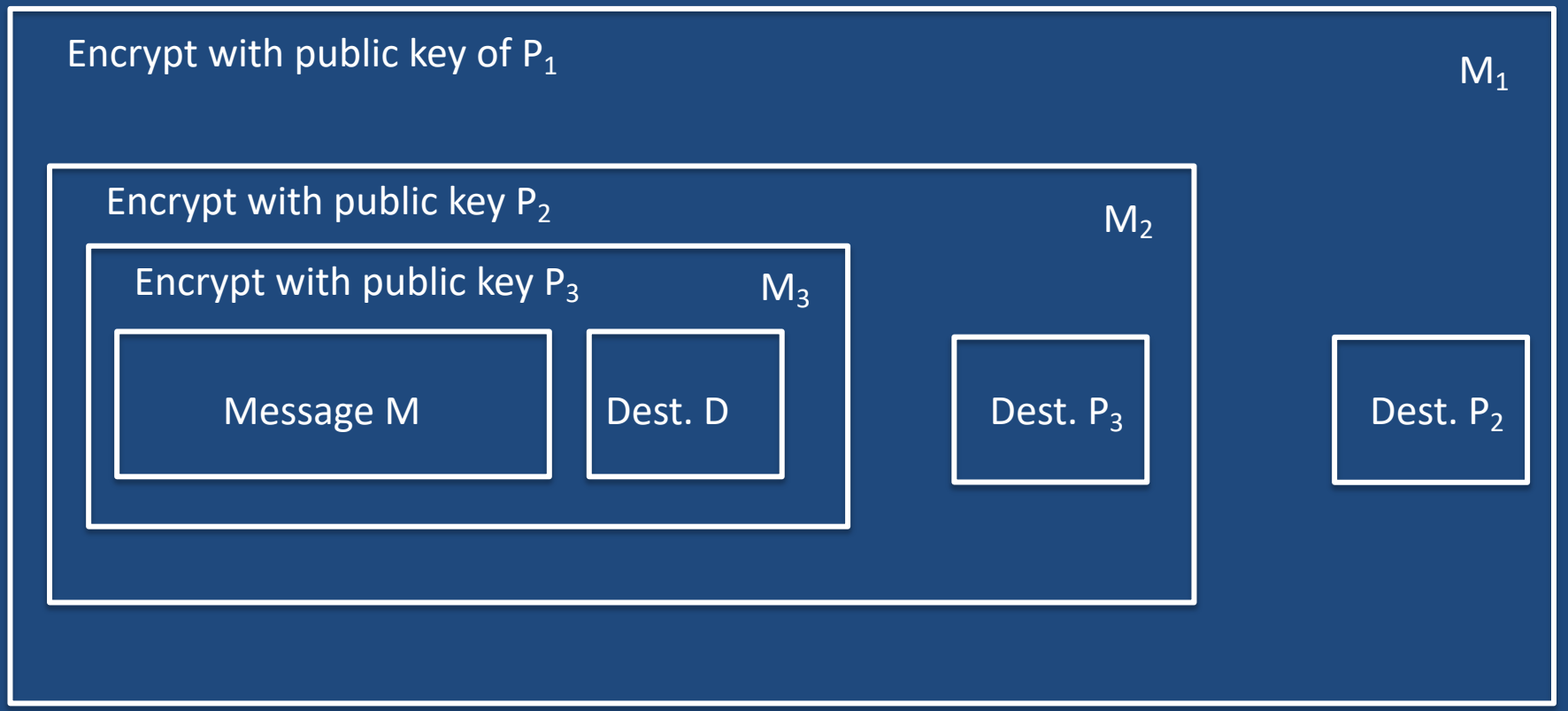




- Alice picks 3 proxy nodes. Messages & destinations encrypted. The proxies used are hidden from Yves.
- PKI used. Public/secret keys P_i and S_i used by M_i.
- Tor developed by US Naval Research Labs for USG.

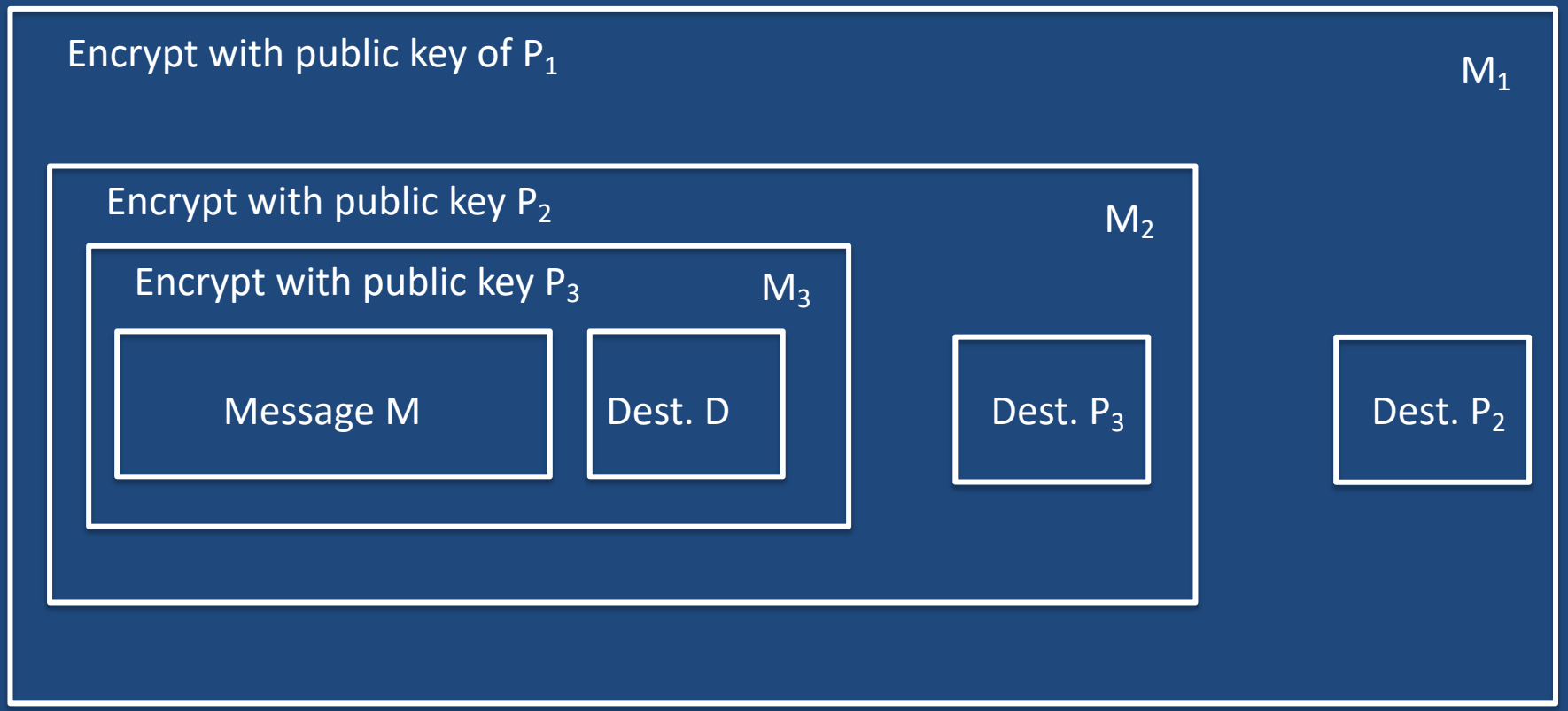
Onion Routing

- Alice's message goes from P_1, to P_2, to P_3, to D.
- Message and destinations encrypted inside out.



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 D.
- Generalizes to more than three proxies.



Identity on the Internet

- Secure real identities and pseudonyms are possible and needed on the Internet.
- Identity can be assured via public-key encryption
  - Sender sends identifying message encrypted with private key
  - Receiver uses sender's public key to verify sender identity
- Identity defined by social media accounts is not secure
- Secure pseudonyms acquired via trusted third parties.
  - Person needing pseudonym acquires one from a third party.
  - If pseudonym providers are federated, the trust boundary extends to all who acquire identities from the federation.

Identity Theft

- Insurance Information Institute says 14.4 million Americans had identities stolen in 2018.
- Many techniques are used to steal identities.
- In 2017 Equifax lost personal records, including SSNs, drivers licenses, addresses, etc., on 147 million Americans, that is, most adults.
  - In February 2020 US charged four members of the PLA military for the theft

* See https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Starting Points for Technical Attribution

- Indicators of compromise (IOCs)
  - Anomalous behavior, unusual activity records
  - Known IP addresses, type of malware
  - Hash of large pieces of data (see reputation services)
- Tools
  - Attackers don't change their tools very often
- Behavior
  - Humans are creatures of habit, same working hours
- Language
  - Comments in software reflect national language

Detecting Attribution

- Source IP addresses help police identify attacker
  - Identifies jurisdiction, can lead to search warrant.
- Geo-locate within postal code from IP address*
  - Use traceroute to find path to destination
- Multistage attacks – many hop points between attacker & victim. Hard to peel back but doable.
- Onion routers can obscure hopping, as we saw
  - But traffic analysis may reveal routes

* See http://www.maxmind.com/

The Willie Sutton Principle

- Willie Sutton was a notorious bank robber
  - When asked why he robbed banks, he is (falsely) reported to have said "That's where the money is!"
- Sutton's Law is taught in medical schools
  - Treat the obvious illness first!
- To find cyber criminals, follow the money!
  - Clients of criminal services must pay for them!
    - E.g., fake drugs firms must process credit cards
  - Criminals must deliver goods or be discovered!

Attribution Is Also a Political Problem

- In 2004 an ITU official 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

- Untangling Attribution by Clark and Landau*
  - It is primarily a policy problem, not a technical one.
  - Attribution of forensic quality in US not possible.
  - Application level attribution via cryptographic means may be possible – break the cypher
  - Fine-grained attribution can be threat to privacy
  - Multi-stage (multi-hop) attacks are hardest to solve
  - Deterrence best achieved through diplomatic action, such as norms and treaties.

* https://www.nap.edu/read/12997/chapter/4

Deterrence Alternatives

- Hack-back* – attack the attacker (via his toolkit?)
  - 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 is possible
- Cyber attacks generally do not have kinetic effect
  - An obstacle to attack is lack of certainty of effect
- Note: Response to attack need not be immediate
- US Government has used sanctions effectively against Russian oligarchs and Chinese military

The Impersonation Problem

- NYT has reported that “followers” are being sold on Twitter, Facebook and LinkedIn*
  - Devumi (US based) sells them to those seeking fame!
- A follower is an impersonation, a nearly identical replica of a real person
  - Millions of impersonations are circulating on web
  - They used to amplify real & fake news

* https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html

The Impersonation Problem

- Impersonations are causing grief to real people†
  - Dozens of complaints have failed to eliminate them
- A person is easily confused with impersonation
  - Reputations are being damaged
- Social media companies have policies against this
  - But they don't always enforce them.
  - They do require proof of identity to shut them down
- Governments may intervene
  - Companies have become ID validators!

† https://www.nytimes.com/2018/02/20/technology/social-media-impostor-accounts.html

Review

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