Untangling attribution

David D. Clark
Susan Landau
October, 2010
Background

- Deterrence implies the ability to impose a penalty on an actor that carries out an inappropriate action.
- Which might imply the need to identify the actor.
  - May be other ways to impose a cost...
- Which has led to calls in Washington for an “accountable” Internet.
- Which could be both ineffective and harmful.
Our work

• Sort out various dimensions of attribution.
  – Person, machine, aggregate entity.
  – Private vs. visible.
• Identify key non-technical issues
  – Jurisdiction
  – Variation in laws and norms
• Relate to design of attacks
  – Multi-stage attacks.
• Draw a few conclusions.
Attribution today—packets

• At the packet level, IP addresses.
  – Directly identify a machine.
  – Only indirectly linked to person.
    • Example: RIAA using DMCA.
    • Rules depend on jurisdiction.
  – Can be mapped (imprecisely) to larger aggregates such as countries and institutions (e.g. Enron).
    • Commercial practice today for web queries.
  – Can be forged, but too much is made of that.
  – Can be observed in the network by third parties.
Attribution today--applications

- Many applications include methods by which each end can verify the identity of the others.
  - Banking.
- Sometimes a third party is involved.
  - E-commerce, certificates.
- Sometimes the identity is private to the parties.
  - Self-signed certificates.
- Sometimes the goal is “no identity”.
  - Sites providing sensitive health information.
- Identity information can be hidden in transit.
A seeming dichotomy

• Two kinds of attribution.
  – Machine-level visible to third parties.
  – Personal identity selectively deployed and private to the end-points.

• Is this structure an accident?
  – Not really.
  – Consistent with a general approach to do “no more than necessary” as a requirement.

• Do we need a third sort?
  – Packet level personally identifying information
Some use cases

• Criminal prosecution.
  – Might seem to require “person-level” identity of forensic quality. But this may not be right.
    • Prosecutors like physical evidence.
    • Use of network-based attribution may be more important in guiding the investigation.

• Espionage
  – Often want to assign responsibility to an institution or a state.

• Cyber-warfare
  – Again, need state/actor-level attribution.
Anti-attribution

• Critical for many purposes.
• Current approaches:
  – TOR
  – Freegate
  – VPNs.
• Note: they serve to mask IP-level information.
  – PLPll would be a disaster here.
Designing attacks

• Many attacks are “multi-stage”.
  – Person at computer A penetrates machine B to use it as a platform to attack machine C.
  – DDoS is obvious example, but not only one.
• Intended to make attribution harder.
  – Attackers are clever.
  – A form of identity theft.
• Tracing an attack “back to A” implies:
  – Support at intermediate points: issue of jurisdiction.
  – Use of machine addresses.
  – PLP-II does not seem to help.
Issues of jurisdiction

• Many sorts of variation.
  – Rules for binding identity to IP addresses.
  – Rules for when this can be disclosed.
    • And to whom.
  – Support for timely traceback of multi-stage attacks.
• Attackers “venue-shop”.
• Might imply a two-level response.
  – Both at the actor and the jurisdiction level.
Some conclusions

• IP addresses are more useful than sometimes thought.

• Any proposals/policies for better attribution should take into account:
  – Multi-stage attacks.
  – The need for “anti-attribution.

• Cross-jurisdiction issues are central.
  – Within one jurisdiction, with a single stage activity, RIAA has demonstrated deterrence.

• PLPII is not a good objective.