Untangling Attribution

David Clark, MIT

Susan Landau, WPI

The Washington Post

Mike McConnell on how to win the cyber-war we're losing

Sunday, February 28, 2010

The United States is fighting a cyber-war today and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking …

We need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable.

Untangling Attribution

- What does attribution mean?

Untangling Attribution

- What does attribution mean?
- Does it mean owner of machine?

  location of machine?

  individual responsible for actions?

Untangling Attribution

- What does attribution mean?
- Does it mean owner of machine?

  location of machine?

  individual responsible for actions?
- Is it app level or packet level attribution that is being sought?

“Attacks” Means Many Different Things

- Attacks vary by type;
  by impact;
  by type of perpertrator;
  by level of threat.

What types of exploitations?

- Spam.
- DDoS.
- Criminal activity.
- Cyberexploits.

What types of exploitations?

- Spam: easily handled.
- DDoS.
- Criminal activity
- Cyberexploits.

What types of exploitations?

- Spam: easily handled.

- DDoS: before the attack, take steps to reduce its potency;

What types of exploitations?

- Spam: easily handled.

- DDoS: before the attack, take steps to
  reduce its potency;
  after the attack, find botmaster and
  bring to justice.

What types of exploitations?

- Spam: easily handled.
- DDoS: getting better (though a challenge).
- Criminal activity.
- Cyberexploits.

Criminal activity

- Can you track the criminal?
- Can you make the charges “stick”?
- Proving charges “beyond a reasonable doubt.”

What are the threats?

- Spam: easily handled.
- DDoS: getting better (though a challenge).
- Criminal activity: follow the money.
- Cyberexploits.

Cyberexploitations

- Often economic espionage.
- Criminal activity — or national-security issue?

Cyberexploitations

- Often for economic espionage.

- Criminal activity — or national-security issue?

"Although the threat to intellectual property is less dramatic than the threat to critical infrastructure, it may the most significant cyberthreat that the United States will face over the long term." William Lynn, 2010.

Classifying Attacks

- Multi-step
- Multi-stage

Multi-stage attacks

- Real threat.
- When they occur, the target machine has been penetrated.

Multi-stage attacks

- Real threat.

- When they occur, the target machine has been penetrated.

Consequence: personal-level credentials will not be useful for tracing for attribution or assigning blame.

Classifying Attacks

- Multi-step
- Multi-stage

- Aspects of attribution:
  - timing
  - type of identity
  - type of investigator
  - jurisdiction

Timing

Timing

- Before
- During
- After

Timing

- Before: securing prior to attack.
- During
- After

Timing

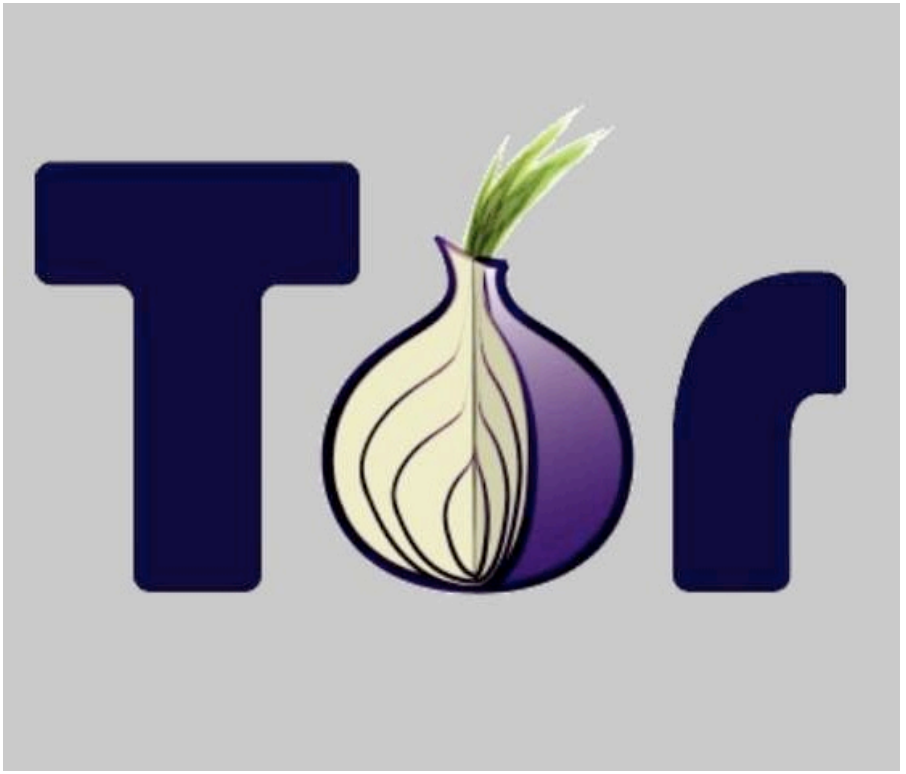
- Before: securing prior to attack.
- During: mitigation.
- After

Timing

- Before: securing prior to attack.
- During: mitigation.
- After: deterrence.

Aspects of attribution: types of identity

Aspects of attribution: types of identity



Aspects of attribution: identity

- IP address suffices for most practical purposes.

- In application-level attribution, the end-points may want to know who each other are.

Aspects of attribution: identity

- IP address suffices for most practical purposes.
- IPv6 and tying addresses to jurisdiction?

Aspects of attribution: identity

- IP address suffices for most practical purposes.
- IPv6 and tying addresses to jurisdiction?
- Virtualized networks, and ties between machine and user.

Aspects of Attribution: Type of Investigator

IP-packet level attribution

- Attribution at the level of a person is useful in very limited circumstances.

Aspects of attribution: type of investigator

Aspects of attribution: jurisdiction

Aspects of attribution: jurisdiction

Multi-stage attacks

- So how do you solve the attribution question for multi-stage, multi-jurisdictional attacks?

That's the real question.

Multi-stage attacks

- So how do you solve the attribution question for multi-stage, multi-jurisdictional attacks?

That's the real question.

- Are there tools that can improve the situation?

What are we trying to do with attribution?

- Spam: halt the onslaught.
- DDoS: stop the attack.
- Criminal activity: prosecute.
- Follow the money, arrest the criminals, convict them.
- Cyberexploitation: stop it, trace it, attribute it.

What are we trying to do with attribution?

- Spam: halt the onslaught.
- DDoS: stop the attack.
- Criminal activity: prosecute.
- Follow the money, arrest the criminals, convict them.
- Cyberexploitation: stop it, trace it, attribute it.

- **But often we don't want attribution.**

Aspects of attribution: identity

- IP address suffices for most practical purposes.
- In application-level attribution, the end-points may want to know who each other are.
- Other forms of attribution are at the basis of the machine, **not the person.**

Focus on Single Jurisdiction Multi-Stage

- Install home routers to monitor outgoing packets.

- Aggregate logs from multiple users (clean infested machines).

The Real Points

- Packet-level attribution is not the answer.

The Real Points

- Packet-level attribution is not the answer.
- Attribution at the level of a person is useful in very limited circumstances.

The Real Points

- Packet-level attribution is not the answer.
- Attribution at the level of a person is useful in very limited circumstances.
- IP address suffices for most purposes.

The Real Points

- Packet-level attribution is not the answer.
- Attribution at the level of a person is useful in very limited circumstances.
- IP address suffices for most purposes.
- Multi-stage, multi-jurisdictional attribution requires law and policy solutions, not technical ones.

Deterrence must be achieved through rules of state, not rules of engineering

What Attribution Can Deliver

- Machine level: forged IP address useful for DDoS, but not where data is exfiltrated.
- Application level: can determine the right tradeoff between anonymity and identification.

What Attribution Can Deliver

- Machine level: forged IP address useful for DDoS, but not where data is exfiltrated.
- Application level: can determine the right tradeoff between anonymity and identification.
- Tradeoffs: deterrence stops exfiltration, but nations can also use it for other purposes, e.g., to stifle dissent.

Shifting the Playing Field

- Would shifting addresses to align with jurisdictions help?
- Should owners of intermediate machines be held responsible?

Bottom Line

- Separate the social and political problems from the technical ones;
- Solve the social and political problems through policy and law;
- Solve the technical problems through technology.