SAND2011-0070C

Roles and Challenges for Sufficient Cyber-Attack Attribution in PCS

Dr. Jeffrey Hunker
Bob Hutchinson
Jonathan Margulies

The Purpose of This Paper

- Describe the importance of attribution in protecting PCS
- Provide an overview of attribution challenges
- A proposal for a first step toward more complete attribution for the PCS community

What is Attribution

- Determining the location or identity of an attacker or an attacker's intermediary
- Attribution includes the identification of intermediaries, though an intermediary may or may not be a willing participant in an attack.
- Determining motivation, particularly by technical means, is challenging at best; this problem is even more challenging when applied to intermediaries.

Why is Attribution Important for PCS?

- Infrastructure systems have adopted the vulnerabilities and threats of modern IT
- CI principals have outsourced significant aspects of their operations
- Manufacturers, vendors, consultants, and support providers are all effectively trusted insiders
- Fortification will not keep them out
- Attribution can enable new protection strategies
  - Enable treaties, policy, law, and new technology
  - Lower the malicious noise floor

Ideal Attribution

- Ideal attribution is not possible, but can provide a sense of direction
- Global in context with overt support from all nations, but should be possible even without universal cooperation
- Attribution should only be provided for malicious activity
- Possible to attribute all cyber attacks with sufficient precision to support response strategies
- Generate threat data to inform defensive strategies

The Difficulty of Attribution

- No provisions for strong authentication of IP communication
- IP packets are easily laundered through intermediaries such as zombie hosts
- No central authority for packet tracing
- Forensics are counter to PCS business models where up-time is critical
- Many technical impediments
  - Tunneling, anonymizers, spoofing, cyber cafes, storage of logs, privileged insiders

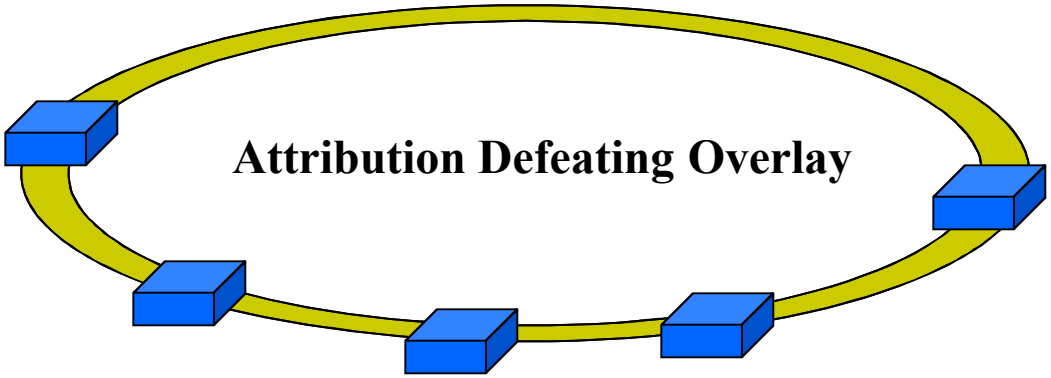
Attribution Policy Issues

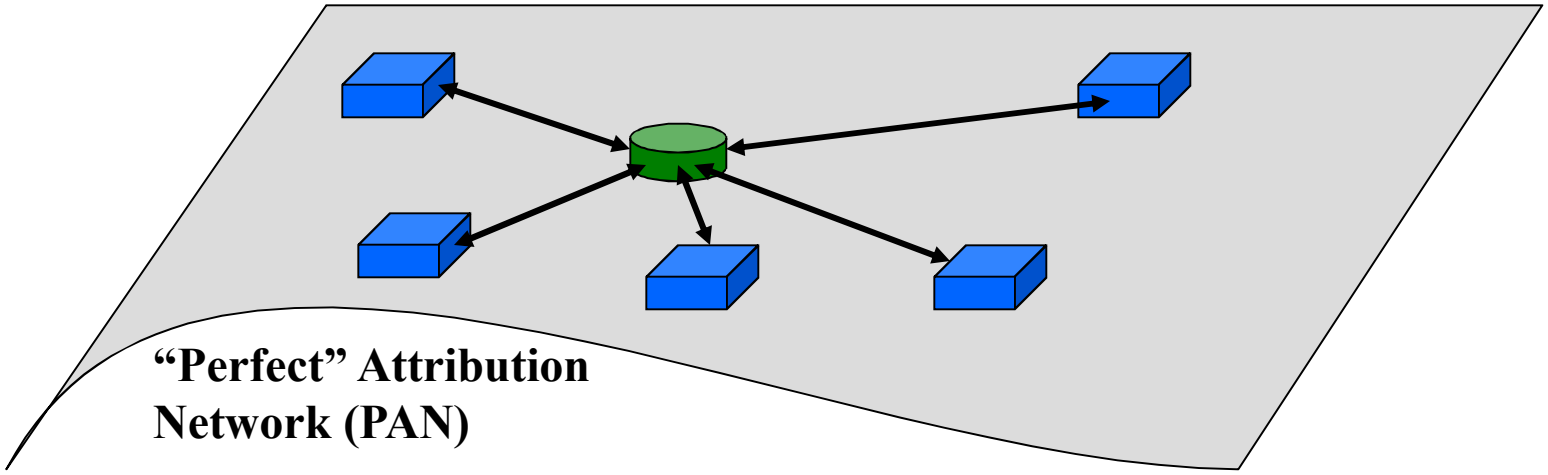
- Policy challenges to attribution
  - Cross-jurisdictional boundaries
  - Balancing privacy and attribution
- Domestic legal authorities
  - Complex legal environment
- International Cooperation
  - Internet-wide cooperation is required

Attribution Technology Issues

- Technical challenges to attribution
  - Anonymous access, distributed ownership and administration, evolving anonymizing technology
- Select current technical attribution approaches
  - Hash-based IP trace-back
  - Network ingress filtering
  - ICMP return to sender
  - Overlay for IP trace-back
  - Probabilistic packet marking
  - Generating trace packets
  - Hack-back
  - Watermarking

A Purely Technical Attribution Solution is Impossible





Steps Toward Achieving Attribution

- There are a number of possible approaches
  - Out-of-band signaling to log each connection
    - Similar to switched telephony
  - Implement multiple systems, some designed for attribution, others not
  - Adopt a clean slate approach with attribution as a fundamental design requirement
- Need a solution that does not require a wholesale upgrade of the Internet

A Technical Approach for Limited Attribution

- Construct a logical overlay on the Internet that makes attribution possible for a subset of PCS users
- PCS operators cannot expect anonymity, relaxing one very difficult constraint
- Only messages from participants in the attribution overlay are processed
- Each message is fully attributable to its source
- If a member is compromised, investigation can be focused to reveal and remove the compromise

Questions?