Packet Tracker:
Finding the Source of
Network Traffic

Tom Daniels, Benjamin Kuperman, Florian Buchholz
PI: Clay Shields
The Problems

Anonymity in the network

– Address Spoofing
  • Attackers are able to falsify the source address of their traffic

– Redirection
  • Attackers may send their traffic through multiple (possibly compromised) hosts to hide their location

– Sophisticated anonymity systems
  • Crowds, Onion Routing, etc.
Address Spoofing

is addressed as from David

Redirection

Bob sees a stream Appearing to come from David, not Alice
The Goals of Packet Tracker

• Better understanding of:
  – Mechanisms behind network anonymity
  – Previously suggested solution
  – The issues both social and technical
  – How to design the next round of solutions

• Encourage other work in this area
Approach

• Literature review
  • found few known solutions
• Reproduce prior work
  • confirms findings
  • increases our understanding
• Enhance prior work
  • fix problems/adding features
• Propose new solutions
• Academic outreach
  • Workshop planned
Caller ID System in the Internet (CISIE)*

- Host-based, active system for tracing extended login connections
- Only useful in limited, well controlled networks

*Jung, et.al. Caller Identification in the Internet Environment. UNIX Security Symposium IV. 1993
Network Traffic Thumbprinting

- Technique for correlating login streams captured at different points in the net.
- Uses a statistical thumbprint of each minute of a stream

Modeling Network Anonymity and Identity

• Based on OSI model
• Relates the entity at each level with the entities below it.
• The model should
  – concisely present the general problem of net. anonymity
  – identify what information should be kept and from where
Results So Far

• CISIE appears to never have been built
  – paper lacks key information
  – may require kernel info.

• Thumbprinting is not well understood
  – many arbitrarily chosen parameters
  – technique is unproven

• The Model
  – still under development
Future Work

• CISIE
  – complete an implementation of the system
  – add authentication

• Thumbprinting
  – evaluate in a “real world” environment
  – evaluate changes to parameters

• Modeling of Identity…
  – continue to develop the model