Computer and Network Security

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu

Traffic Analysis Prevention (TAP)

1 Traffic Analysis

1.1 Form of Message Confidentiality Violation

1.1.1 Types of Traffic Analysis

Source and Destination

- port
- host
- network interface
- network

Quantities

- load
- load changes
- window issues

1.1.2 Issues in TA

- Where to measure
- When to measure (windows)
- How to measure
- What to measure

1.2 Goals

- Get true Traffic Matrix
- Detect changes in TM
- Detect specific parts of TM
- Answer questions about TM

1.3 Motivation

- Diplomatic Contacts
- Business dealings
- Domino Pizza Channel
- Personal interactions

2 Traffic Analysis Prevention

2.1 TAP Goals

- Make packets look same
- Break linkages between packets
- Disguise true Traffic Matrix
- Disguise changes in TM
- Still allow efficient routing
- Minimize imposed delays

2.2 TAP Mechanisms

2.2.1 Encryption

- Make contents opaque
- Disguise true destinations

2.2.2 Rerouting

- Avoid insecure areas
- Disguise true flows

2.2.3 Padding

- Make all packets same size
- Pad link traffic
- Pad flows

2.2.4 Delay

- Traffic Shaping

2.3 Relationships

2.3.1 Covert Channels

- Signaling via TA
- Prevent TA $\Rightarrow$ prevent CC

2.3.2 Anonymity

Individual linkages vs. TM

- msg to msg
- msg to source
- msg to destination
- source to destination

2.3.3 Steganography

- Hide existence of communication
- Innocuous cover
- Existence of "path"