Network Metrology: Security

This class

- Role of Network Measurements in Security
- Traffic Anomaly detection
- Network intrusion detection systems
- Network telescope

ROLE OF INTERNET MEASUREMENT IN SECURITY

Network Security

- Security is an old problem
- Arms race between attackers and network operators/developers

Security Attacks

- Many examples of attacks:
  - Spoofing
  - BGP prefix hijacks
  - Worms and botnets
  - Denial of service
  - Spam

Common Craft - Worm, Virus, and Trojan Horse?

Security-related measurements

- Presence of a third party:
- Adversaries can complicate accuracy and usefulness of measurements
- Evasion techniques:
  - Vary volume of traffic
  - Vary frequency of packets being sent.
  - IP spoofing.
- Scrutiny is required in designing security measurement experiments.

TRAFFIC ANOMALY DETECTION

Traffic anomaly detection

- Data source: SNMP/netflow/packet capture
- Method
  - Outlier behavior with respect to some normal pattern
  - Most post-facto, so more for intrusion detection
- Suitable for volume attacks
  - E.g., denial of service
- Anomalies can be malicious or unintentional
  - Attacks, virus, worms, port scans, etc.
  - Operator errors (outages, overloads, etc.)
  - Customer traffic, flash crowd, etc.

Approaches

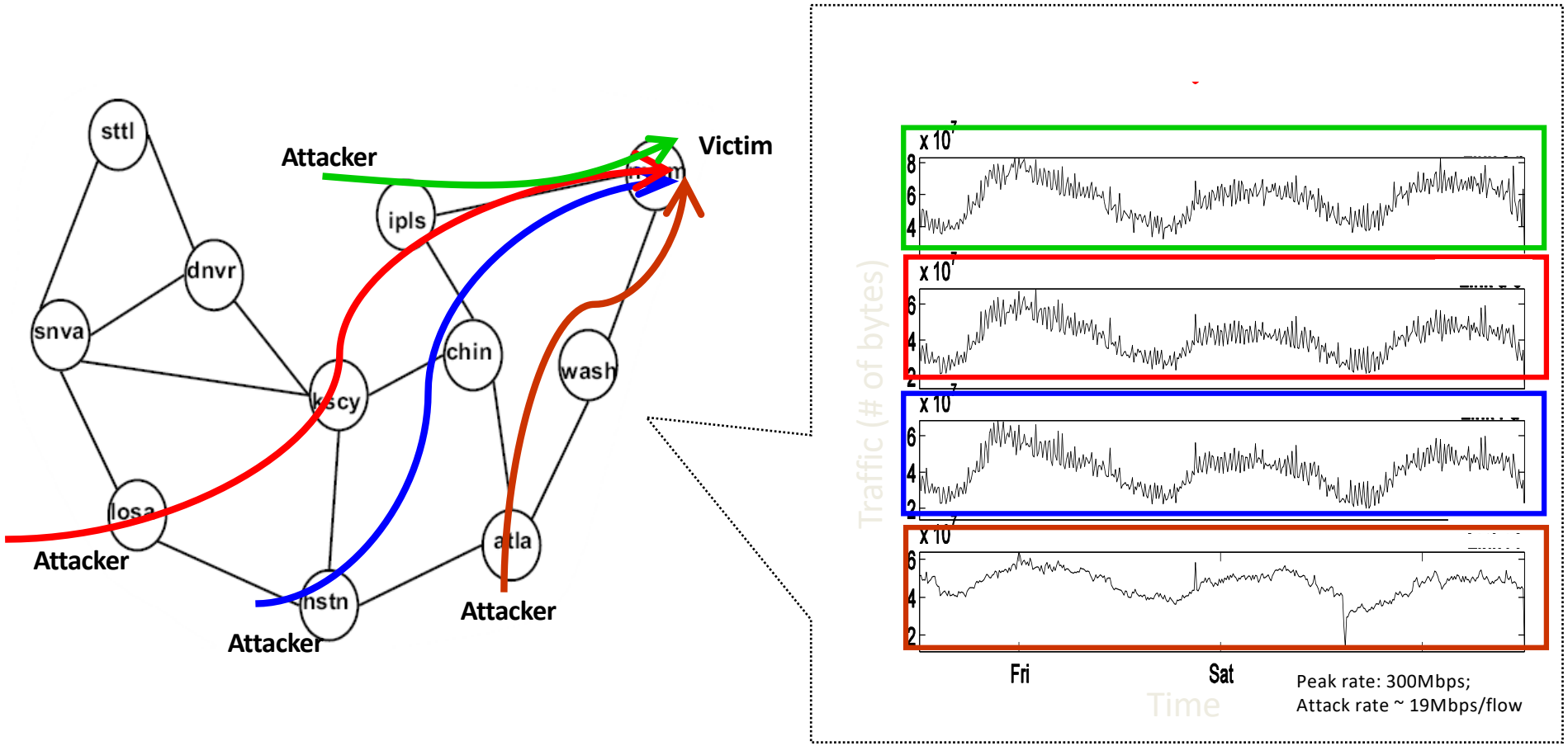
- Temporal
  - Identify normal traffic behavior by analyzing time series of each link
  - E.g.: ARIMA, Fourier Analysis, Wavelet Analysis, Temporal PCA, Kalman
- Spatial
  - Identify normal traffic behavior across multiple elements of the traffic matrix
  - E.g., Spatial PCA

Example method by Lakhina et al.

- Organize traffic statistics in time series
  - Byte, packets, flow counts, features, depending on what data is available
  - Represent as link or traffic matrices
- Detect anomalies: the subspace method (PCA)
  - Separate normal & anomalous traffic
  - Statistical thresholds to identify anomalies

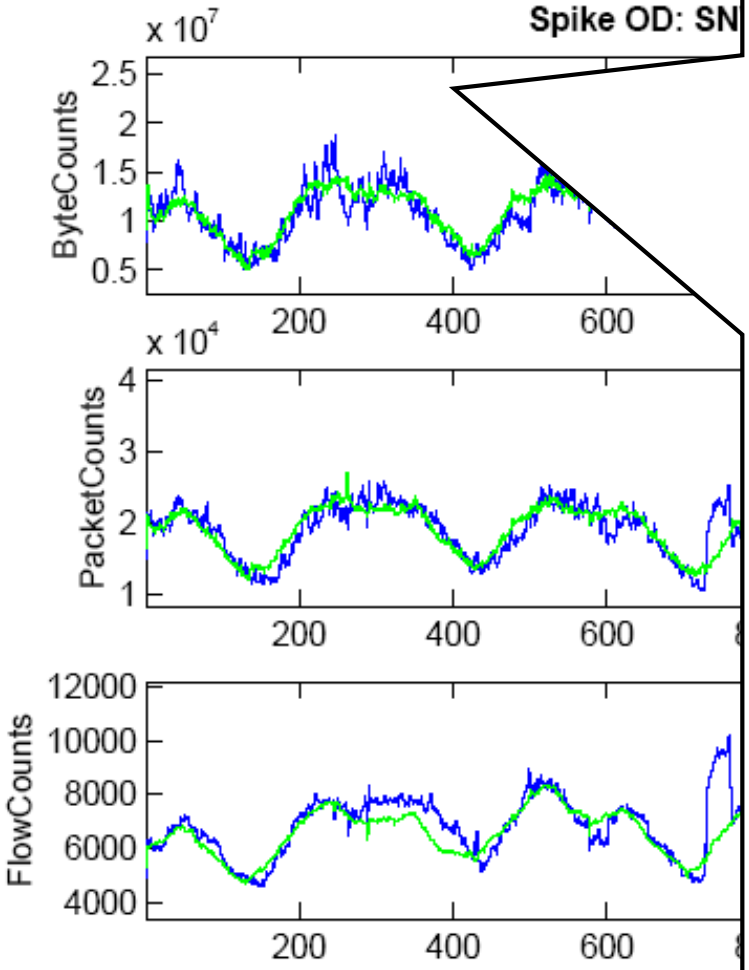
Lakhina, Anukool, Mark Crovella, and Christophe Diot. "Diagnosing network-wide traffic anomalies." *ACM SIGCOMM computer communication review* 34.4 (2004): 219-230.

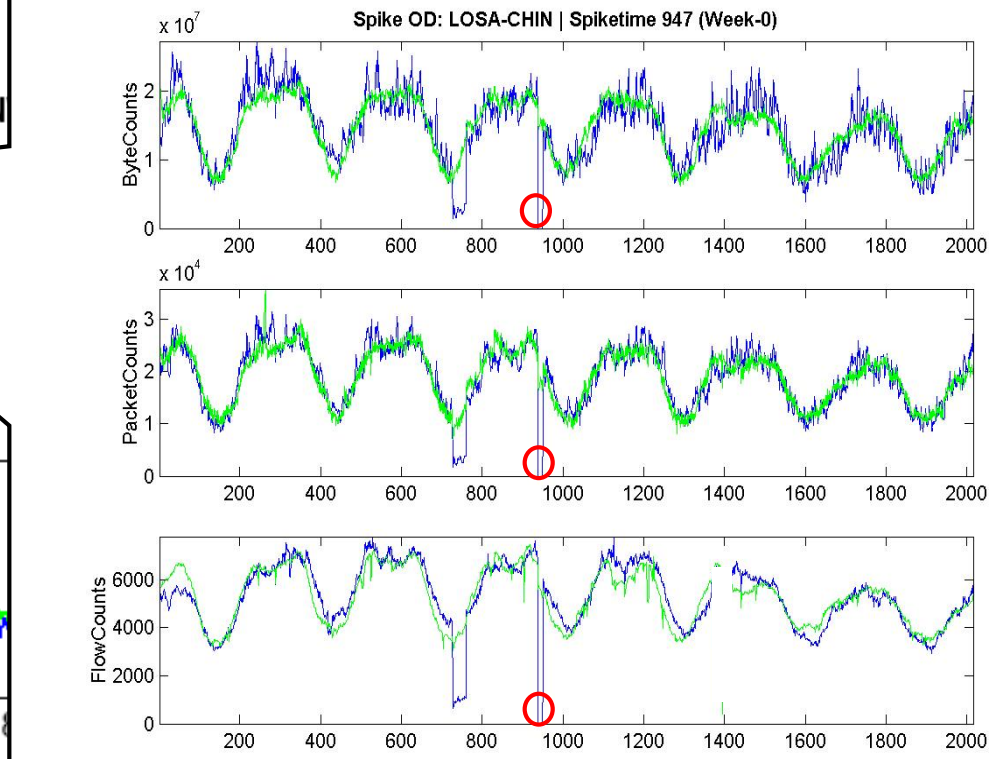
Example: Temporal versus spatial



From: Lakhina, Crovella, Diot

An example operational anomaly





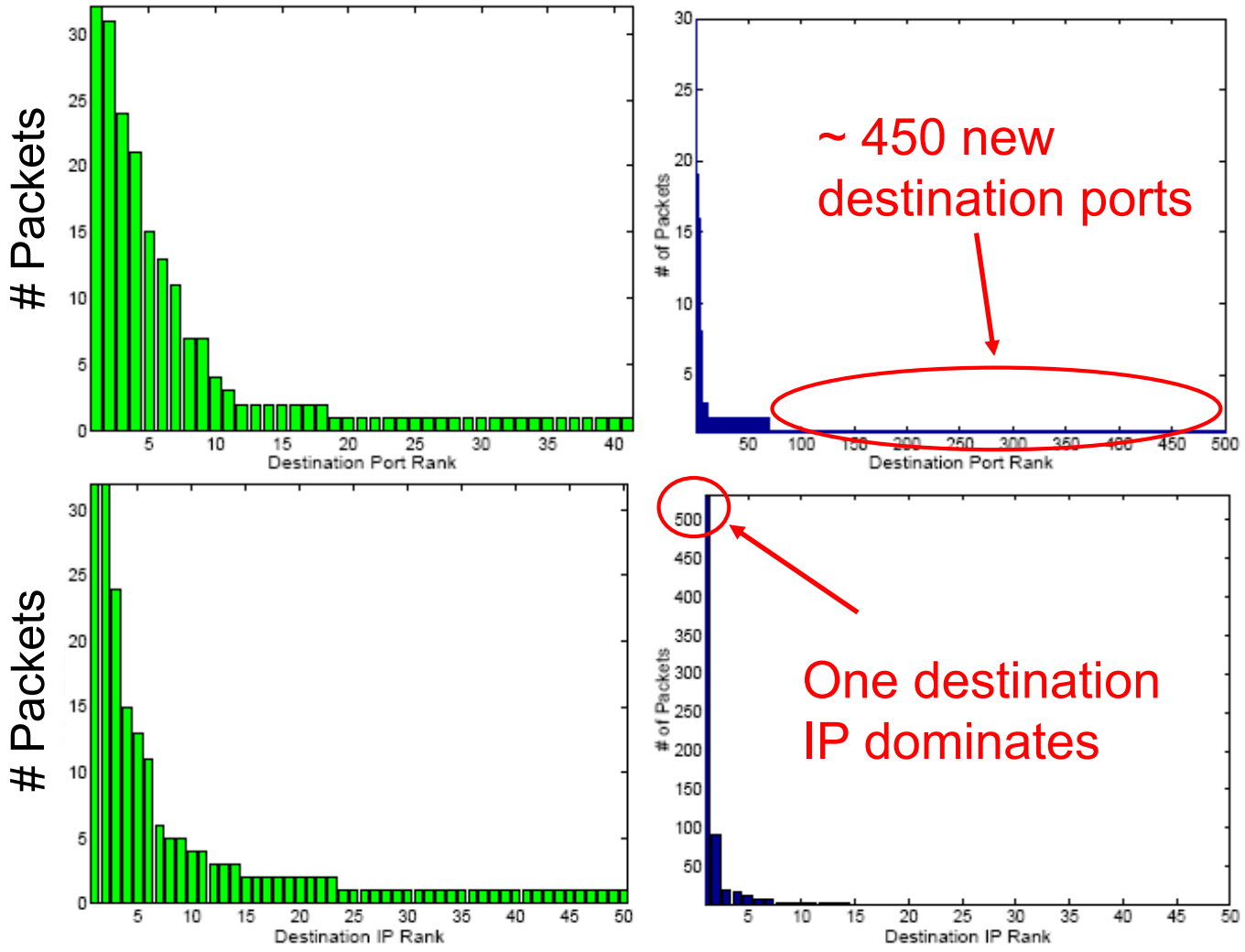
Cause:
Multihomed customer CALREN reroutes around outage at LOSA

From: Lakhina, Crovella, Diot

Traffic feature distributions

Dest. IPs

Dest. Ports



Typical Traffic

vertical port scan

From: Lakhina, Crovella, Diot

NETWORK INTRUSION DETECTION

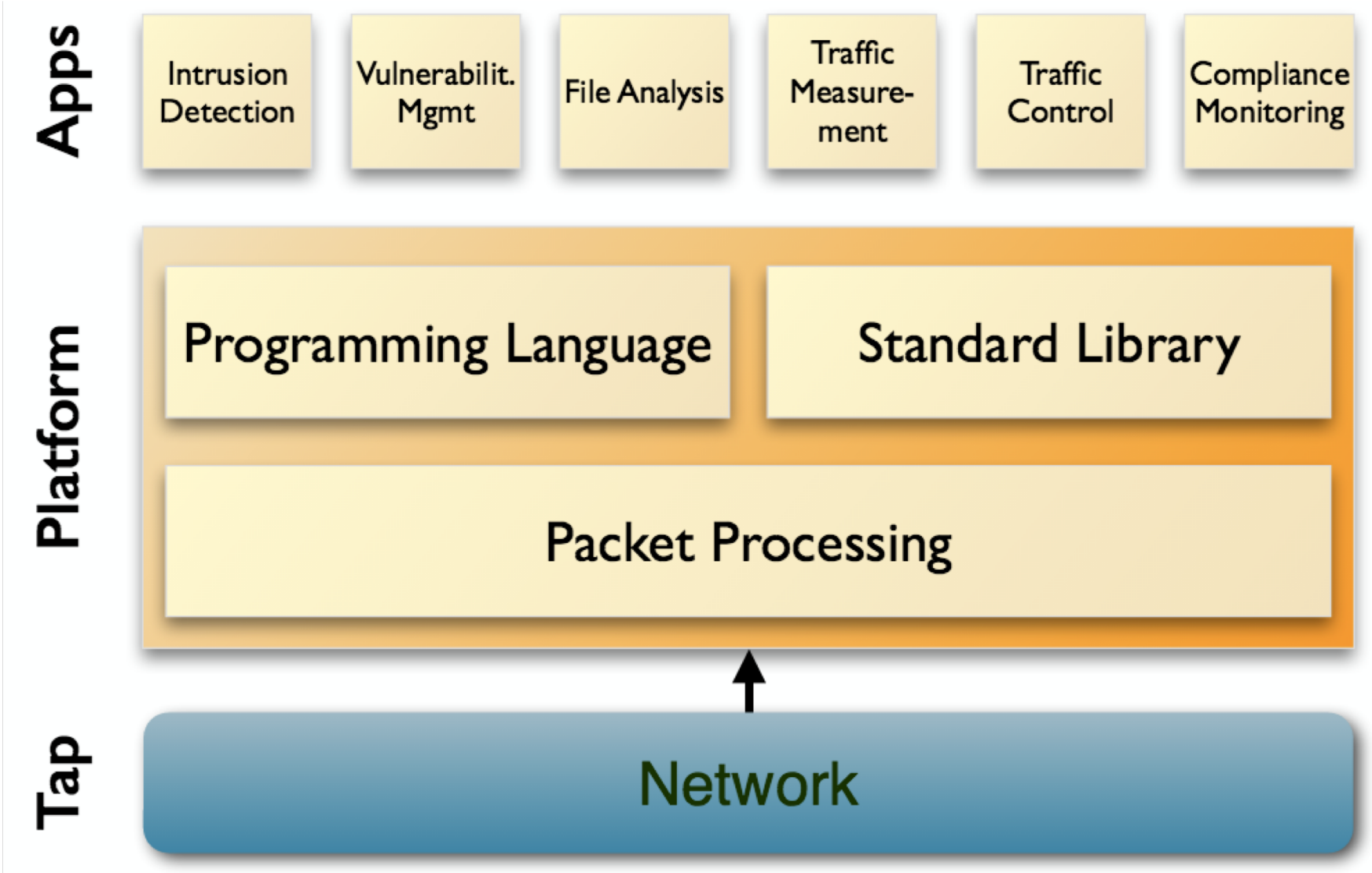
Network Intrusion Detection Systems (NIDS)

- Data source: online packet analysis
- Method
  - Configured with access control lists and signatures
  - Traffic that flagged as attack is logged to improve signatures in the future
- Examples
  - Watch for violations of protocols and usual connection patterns
  - Look for malicious command sequences

NIDS: Challenges

- Reactive, not proactive
- Monitor performance at high-speed links
  - E.g., matching signatures is slow
- Evasion
  - Encryption
  - Skilled opponent can confuse/manipulate monitor
- Tradeoff: false positives vs. false negatives
  - Too many false alarms overwhelm operators
  - Can’t miss attacks

Example NIDS: Zeek (Formally Bro)



Example Zeek script

Task: Report all Web requests for files called “passwd”.

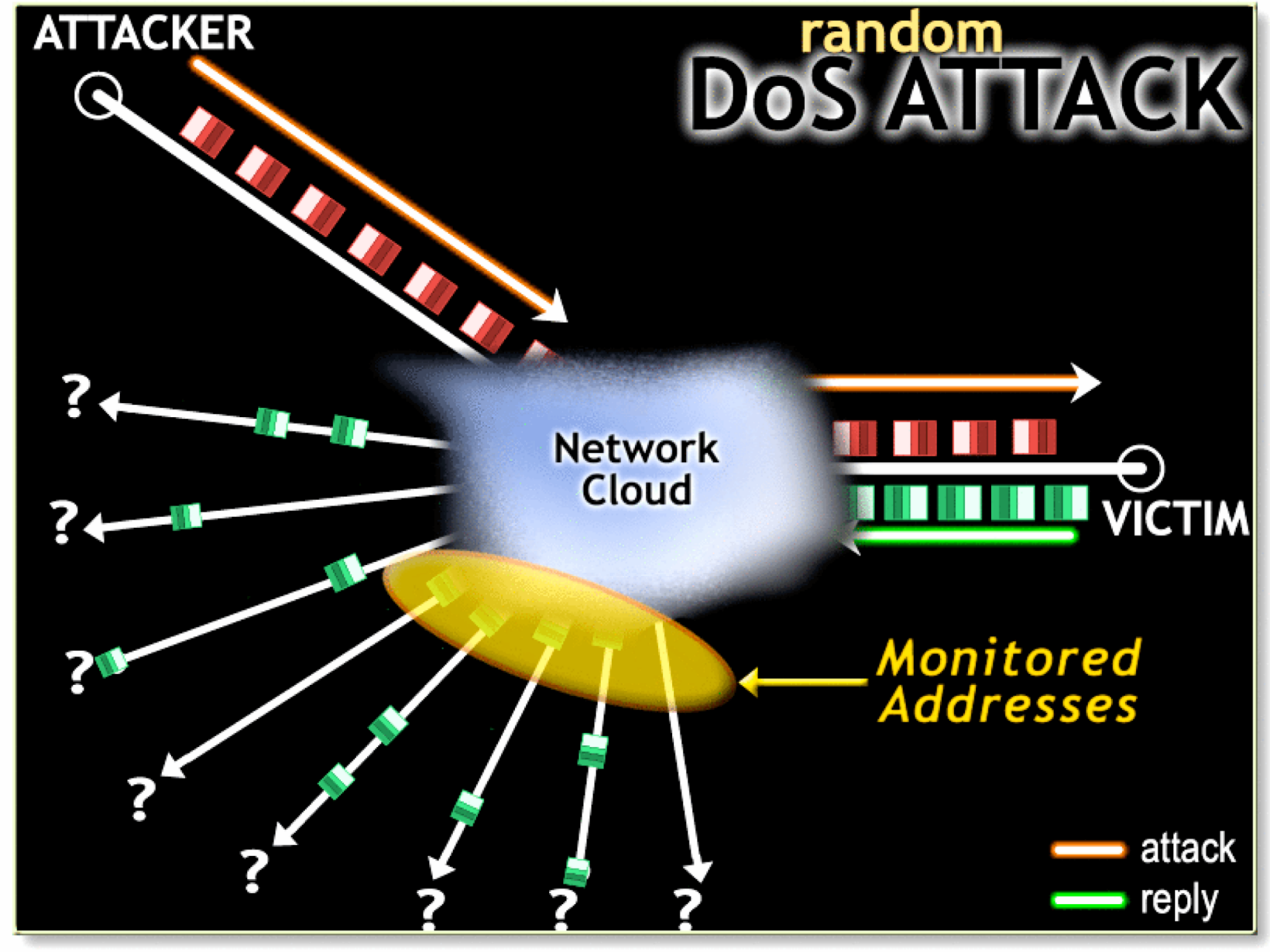
```
event http_request(c: connection,          # Connection.
                   method: string,         # HTTP method.
                   original_URI: string,   # Requested URL.
                   unescaped_URI: string, # Decoded URL.
                   version: string)        # HTTP version.
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
        NOTICE(...); # Alarm.
}
```

NETWORK TELESCOPE

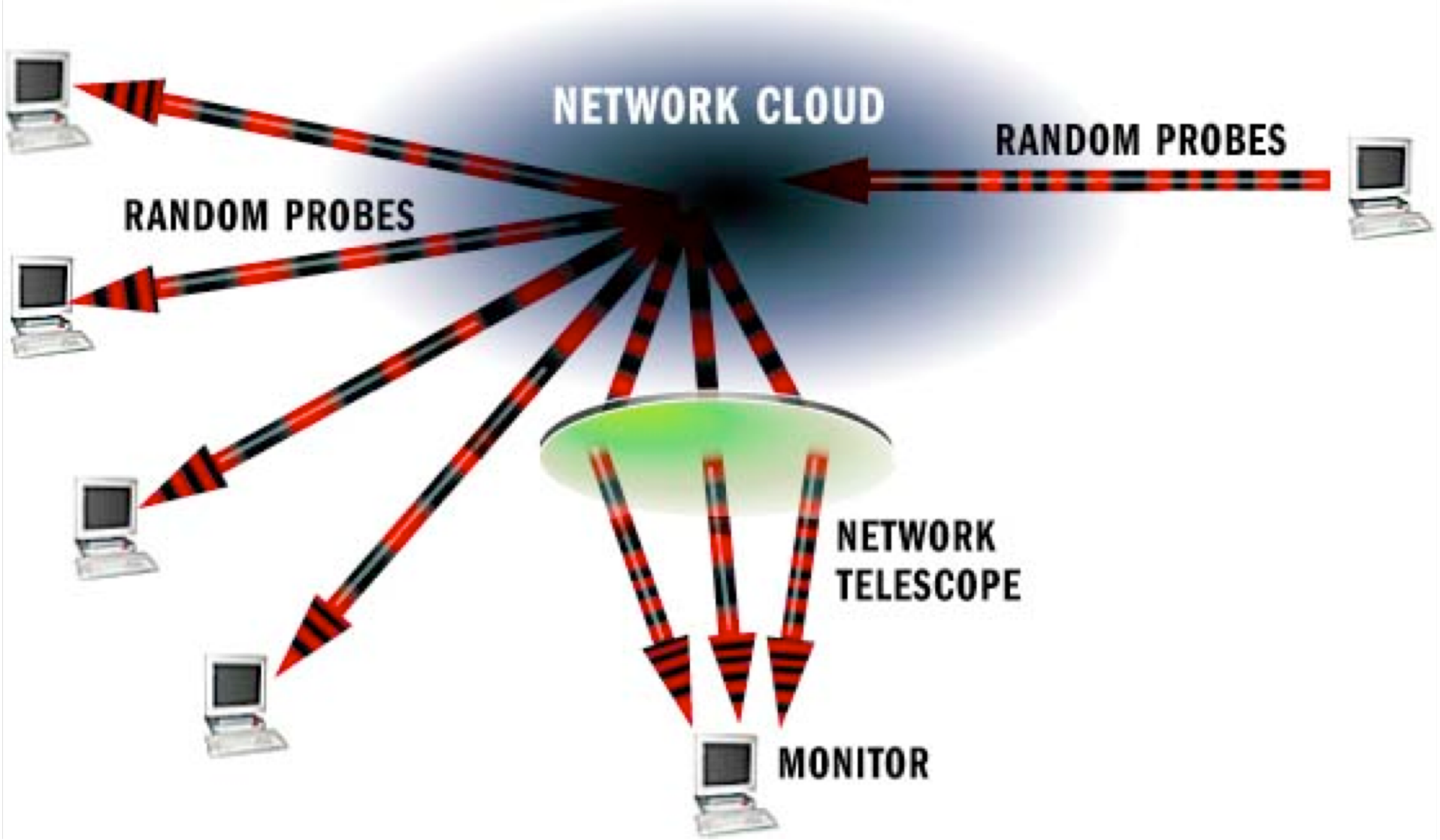
Network telescope (or darknet)

- Intuition
  - Monitor traffic targeting unused address space of the network (globally routed /8 network)
  - Incoming packets represent unwanted traffic
- Detects a number of attacks
  - Denial of service
  - Worms/viruses
  - Scanning for vulnerable hosts (maintain botnets)

Example: DoS attack



Example: Worm



Summary

- Anomaly detection
  - Detects wide-range of attacks (including novel)
  - Miss low volume attacks
- Network intrusion detection systems
  - Combine a number of techniques: signature matching, access control, analysis of protocol/application patterns
  - Must constantly update attack libraries
- Wide-area monitoring: Network telescope
  - Identify unwanted traffic from attacks

References

- CNIL data protection
  - http://www.cnil.fr/english/data-protection/
- “Internet measurement: Infrastructure, traffic & applications”, Chapters 8 and 9
- Class on k-anonymity and other cluster-based methods
  - https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwjEst2N8pnKAhUI_A4KHSzKAJQQFggrMAI&url=https%3A%2F%2Fwww.cs.utexas.edu%2F~shmat%2Fcourses%2Fcs380s_fall09%2F21kanon.ppt&usg=AFQjCNEwUcK9mXssQBgE2jS5gsvrsrXGmA&sig2=Fb4T1mhViTP5WJY9le4syg
- “Differentially-private network trace analysis”, SIGCOMM 2010
  - http://www.sigcomm.org/node/2880