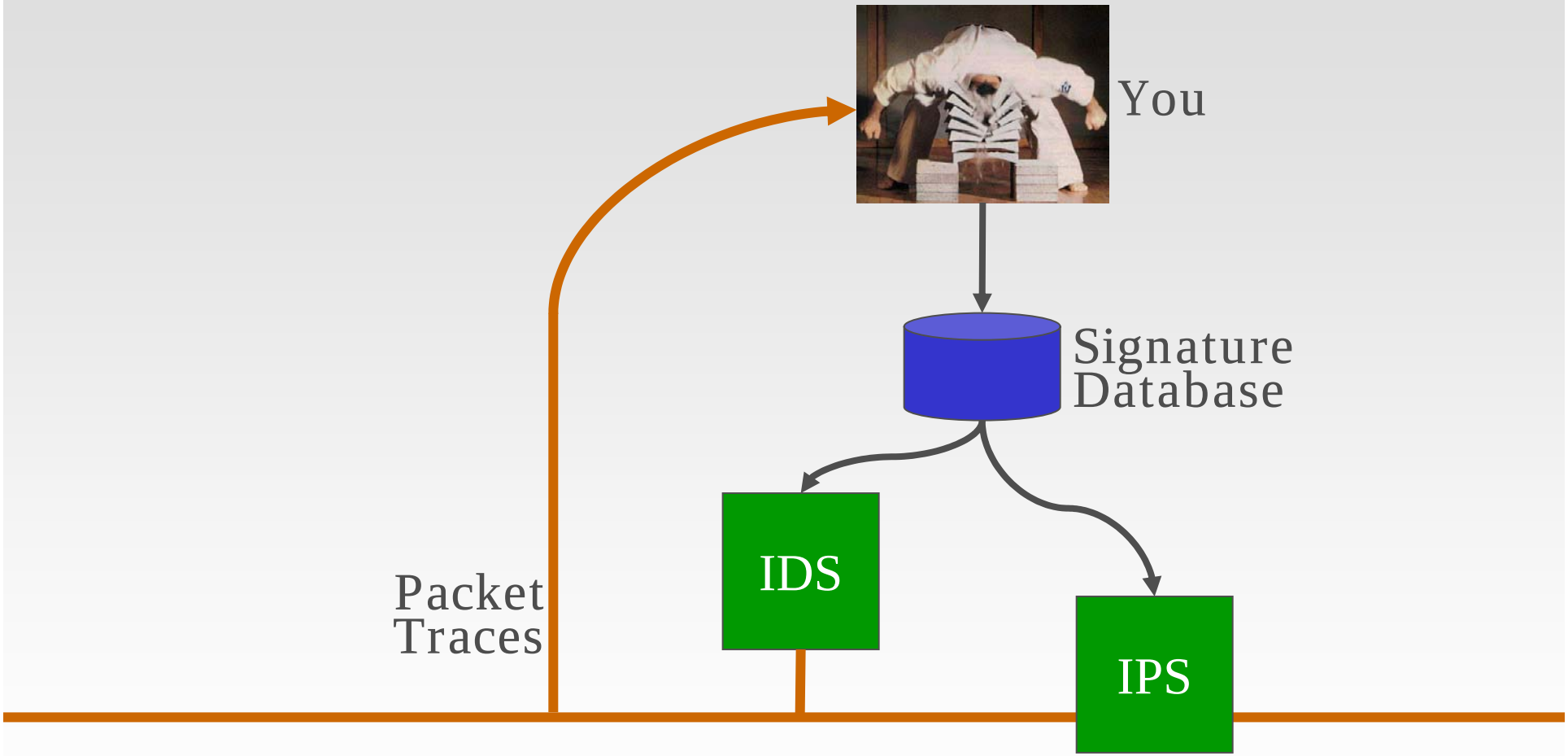
# An Architecture for Generating Semantics-Aware Signatures

*Vinod Yegneswaran, Jonathon T. Giffin,*
*Paul Barford, Somesh Jha*

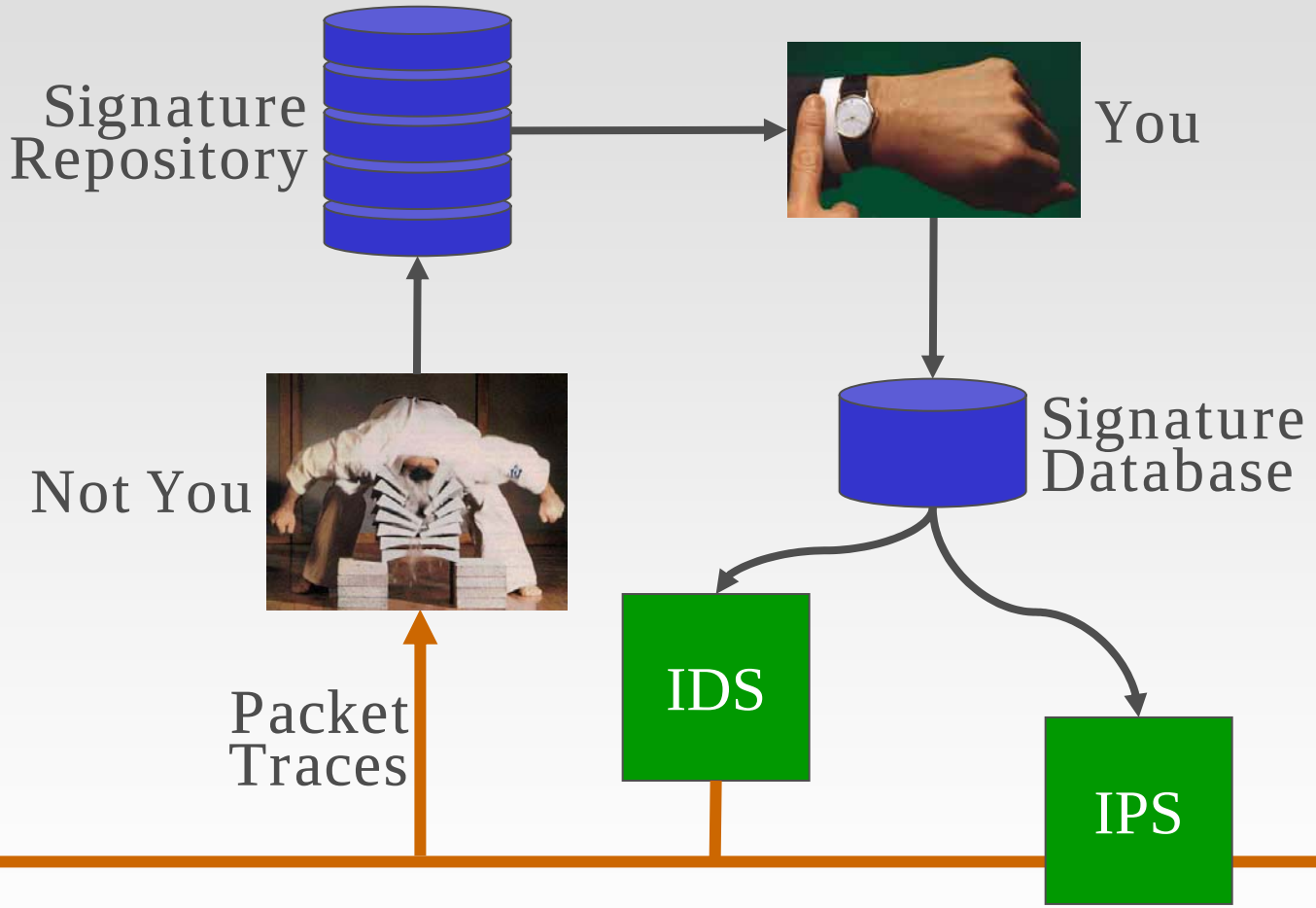
University of Wisconsin
**{vinod,giffin,pb,jha}@cs.wisc.edu**

2005 USENIX Security Symposium

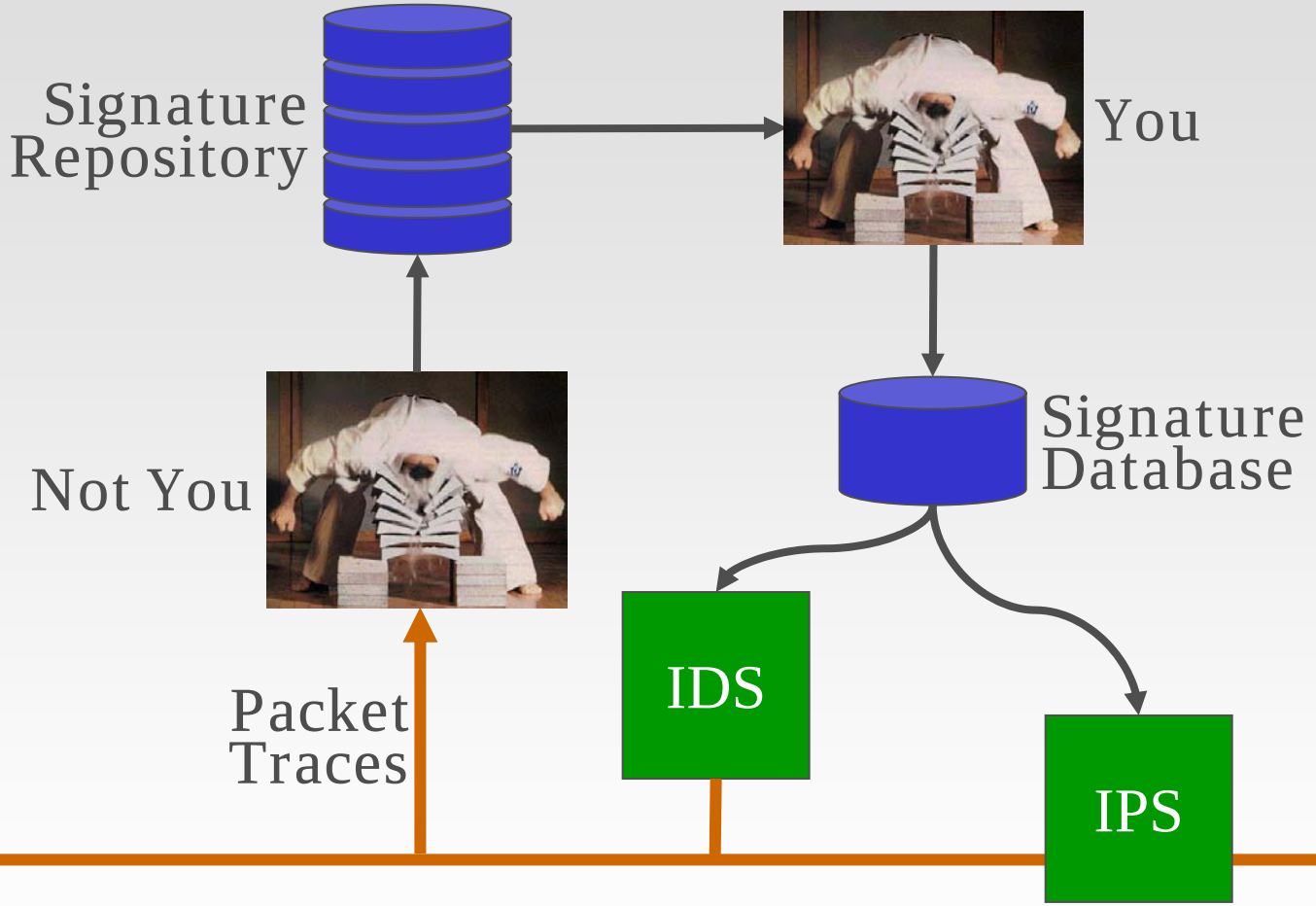
# Worldview



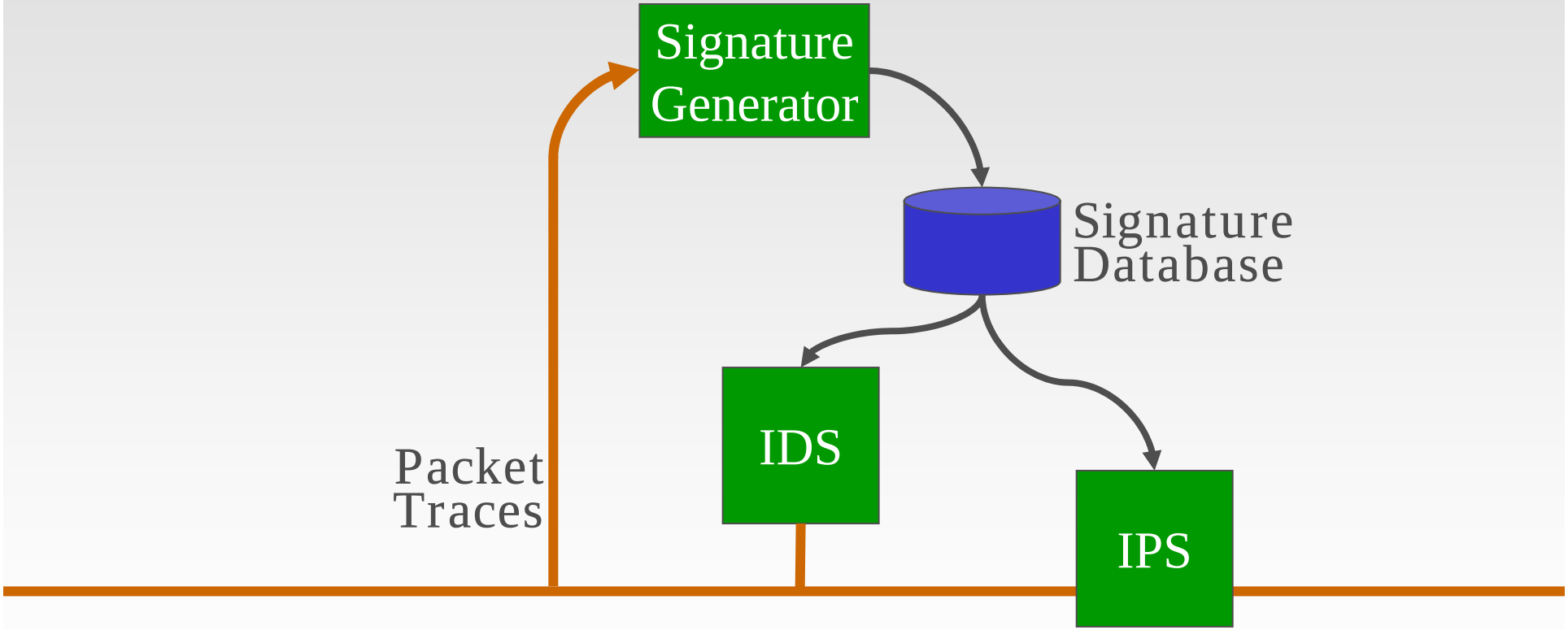
# Worldview


Signature Repository
You
Not You
Signature Database
Packet Traces
IDS
IPS

# Worldview


Signature Repository
You
Not You
Signature Database
Packet Traces
IDS
IPS

# Worldview


Signature Generator
Signature Database
IDS
IPS
Packet Traces

# Automatic Signature Generation

**Specific signatures**

Identify only characteristics of attack profiles

**General signatures**

Match variants of known attack profiles

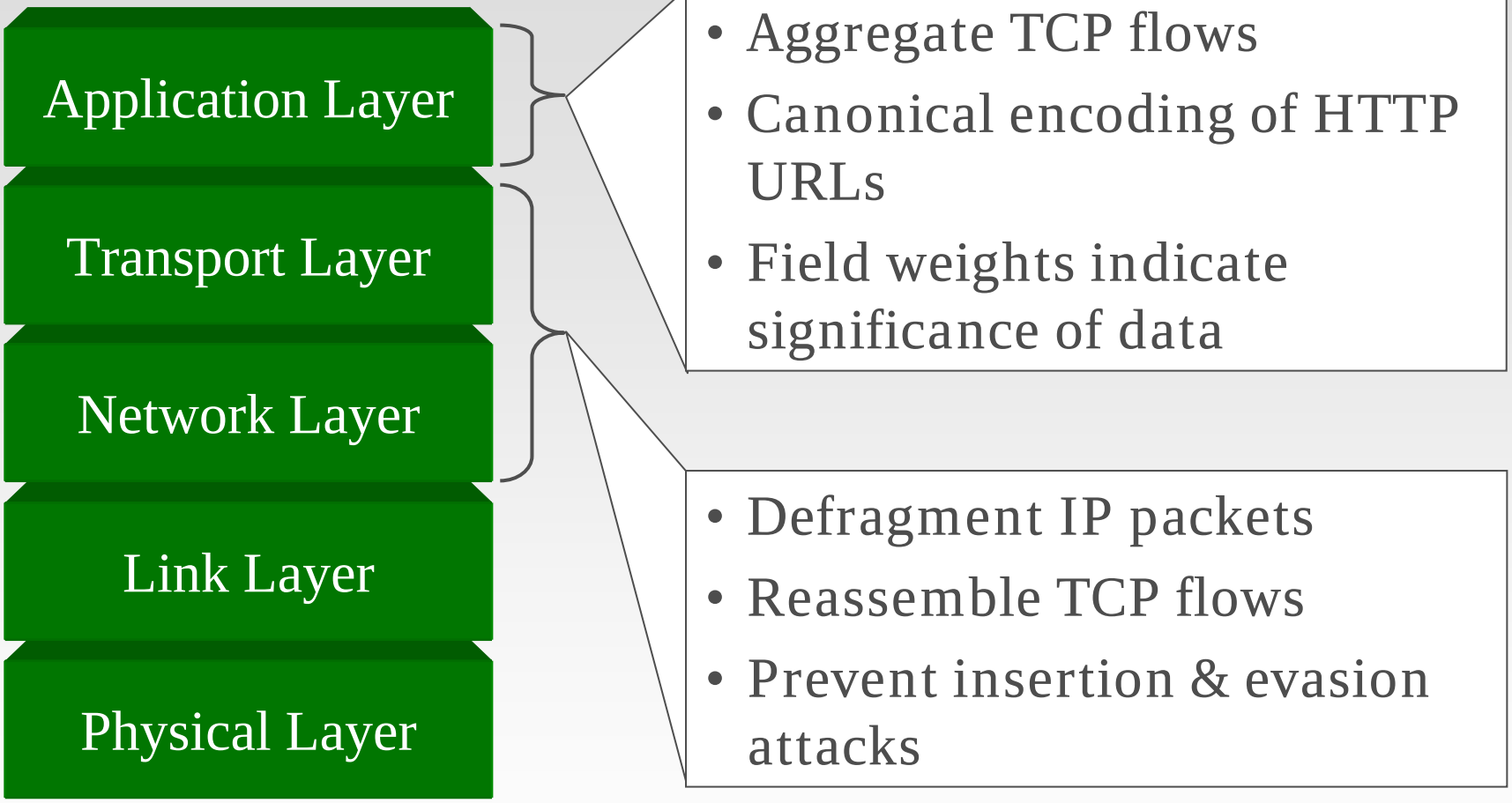
Balance specificity and generality

# Related Work

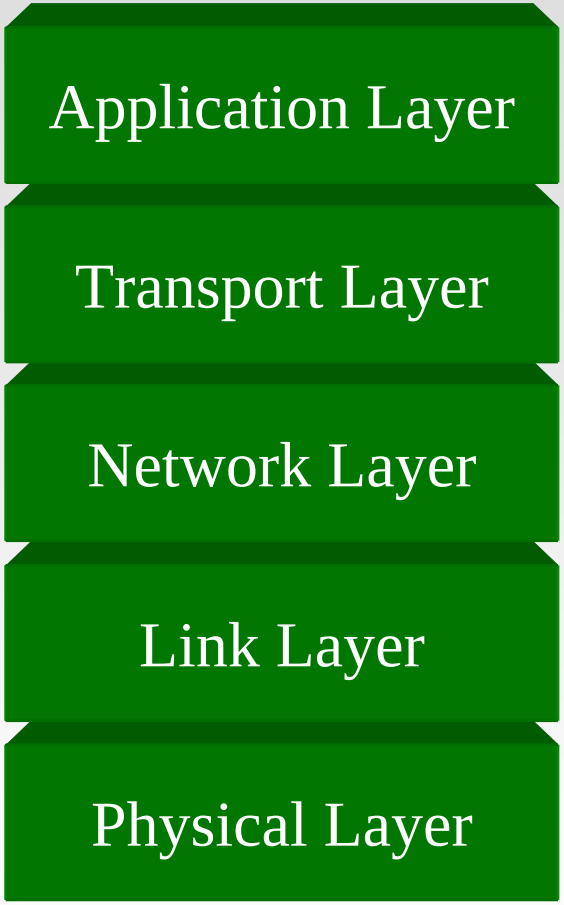
| | |
|---|---|
| Controlled virus infection | [Kephart & Arnold 1994] |
| Honeycomb | [Kreibich & Crowcroft 2003] |
| Autograph | [Kim & Karp 2004] |
| Earlybird | [Singh *et al.* 2004] |
| Polygraph | [Newsome *et al.* 2005] |

- Not aware of application-level protocol semantics
  - Distracted by irrelevant byte sequences
    `\r\nConnection: Keep-Alive\n\r\n`
- Worm-oriented
- Real-time use

# Semantics-Aware Signatures

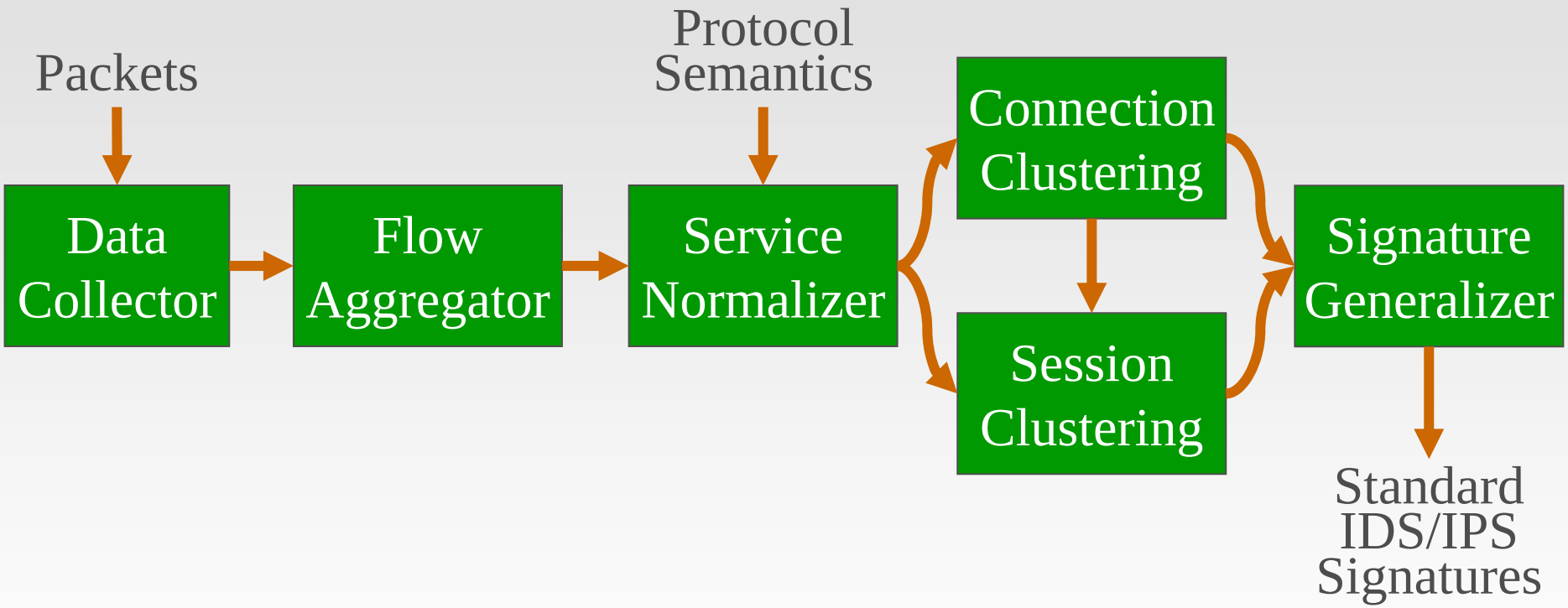


# Semantics-Aware Signatures




- Generate signatures for attacks where the exploit is a small part of entire payload
- Generate contextual connection- and session-level signatures for multi-step attacks
- Produce generalized signatures from small number of training samples
- Produce signatures that are easy to understand & validate

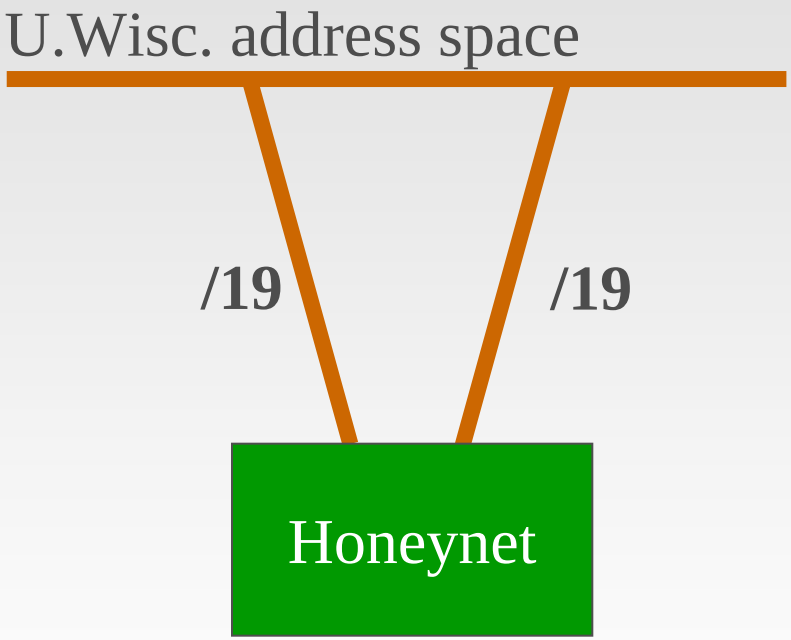
# Architecture



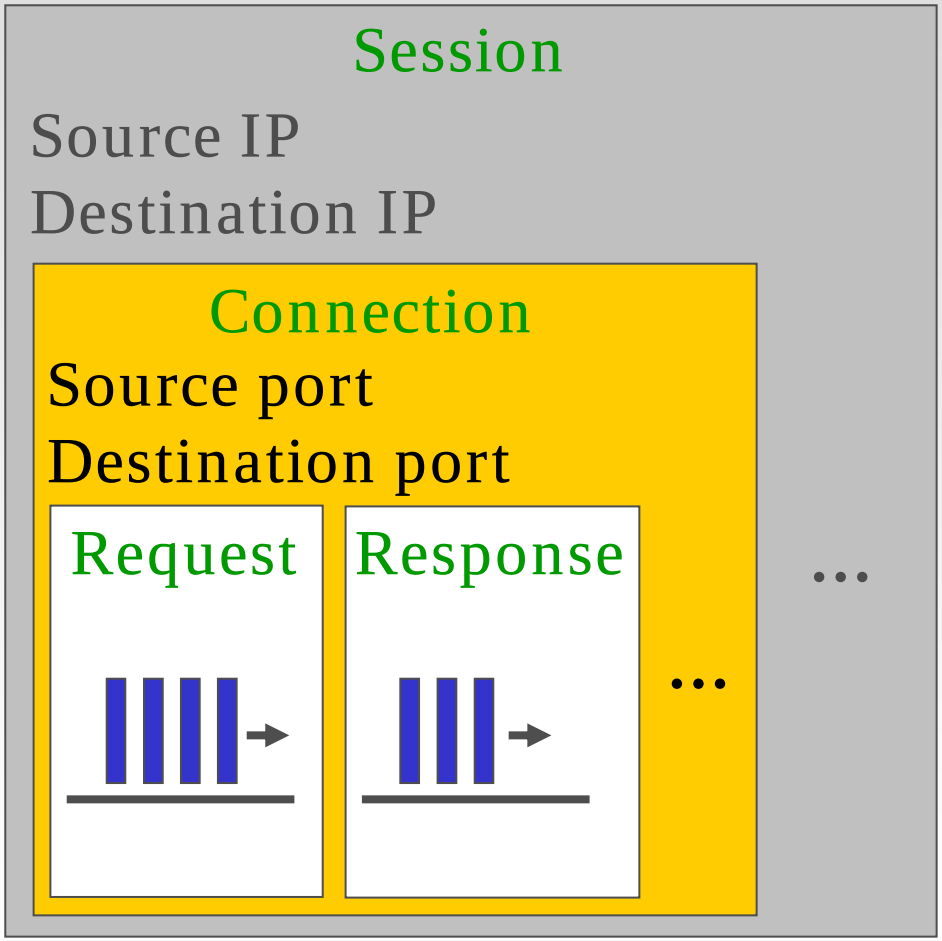
# Data Collection

- Problem: build signatures only for malicious traffic
- Solution: collect traffic sent to honeynet
  - Routed but unused IPs
  - Legitimate traffic never sent to honeynet
  - Actively respond to HTTP & NetBIOS traffic

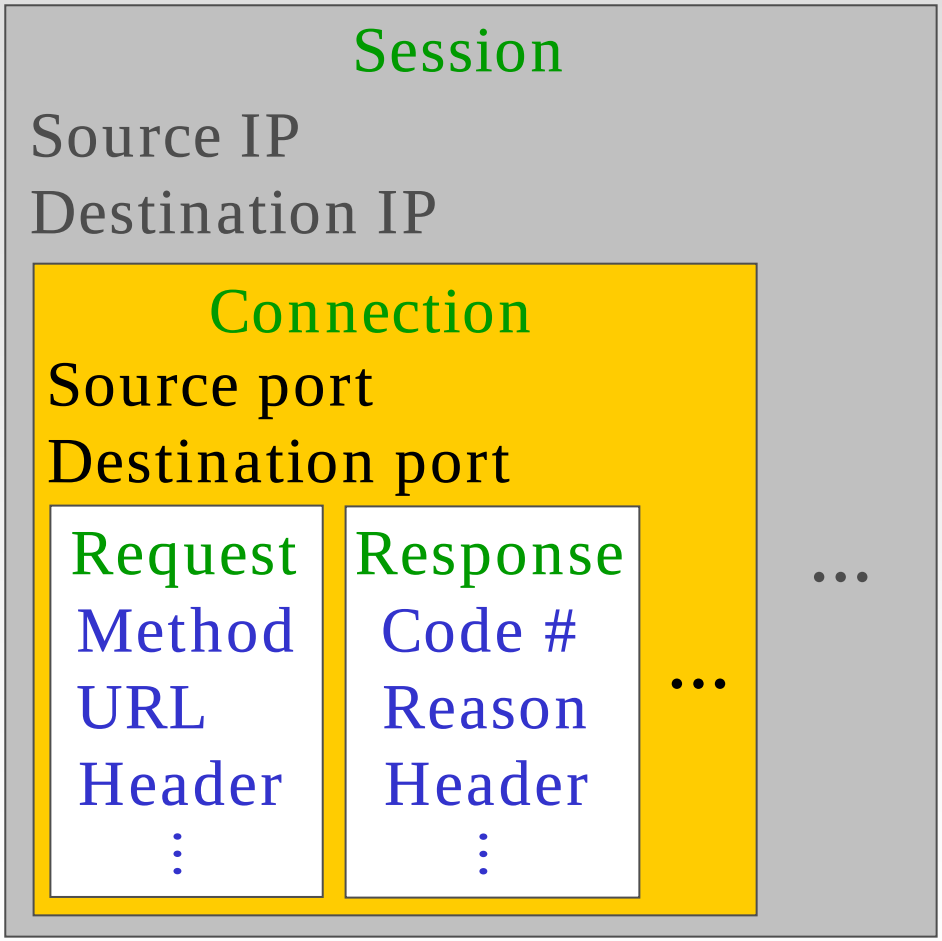
[Yegneswaran *et al.* 2004]



# Flow Aggregation



# Flow Aggregation & HTTP Semantics



# Flow Aggregation & HTTP Semantics

attacker:2492 → honeypot:80

GET /scripts/root.exe?/c+dir
Connection: Close

attacker:2492 ← honeypot:80

404 Object Not Found

Nimda exploiting Code Red backdoor

# Flow Aggregation & HTTP Semantics

## Session

Source IP = “attacker”

Destination IP = “honeynet”

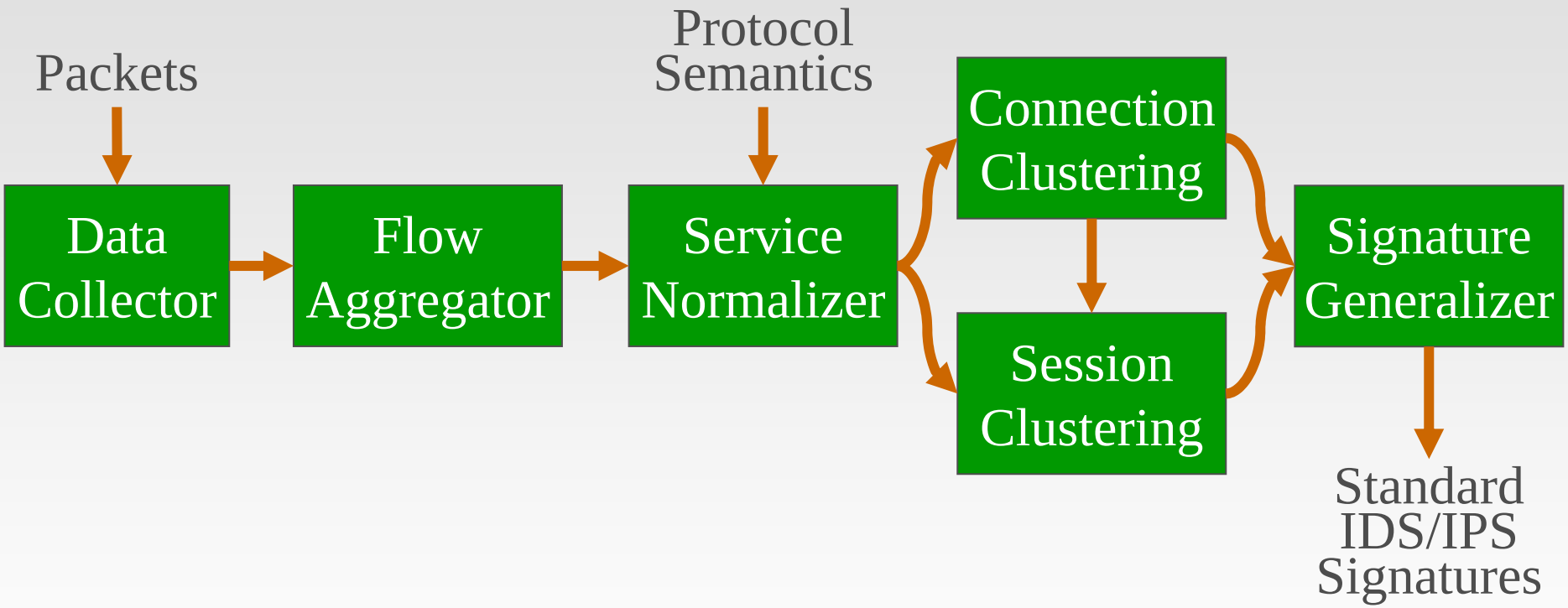
### Connection

Source port = 2492

Destination port = 80

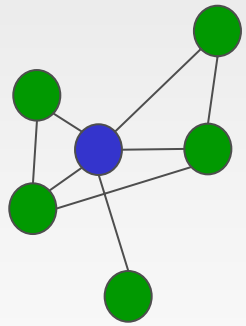
| Request | | Response | |
|---|---|---|---|
| weight | 1000: Method | weight | 1: Code # |
| weight | 1: URI | weight | 0: Reason |
| weight | 50: Header | | |
| weight | 1: /c+dir | | |
| weight | 0: Connection: close | | |

# Architecture



# Clustering

- Star clustering algorithm [Aslam *et al.* 1999]
  - Construct similarity graph
    - Connections become nodes
    - Edges between nodes weighted with connection similarity
  - Find a star cover comprised of star clusters
  - Robust to data ordering
  - Algorithm determines number of clusters
- Cosine similarity metric



# Connection Clustering

attacker:2492 → honeypot:80

GET /scripts/root.exe?/c+dir
Co[illegible]on: Close

attacker:2492 ← honeypot:80

404 Object Not Found

C1

attacker:2496 → honeypot:80

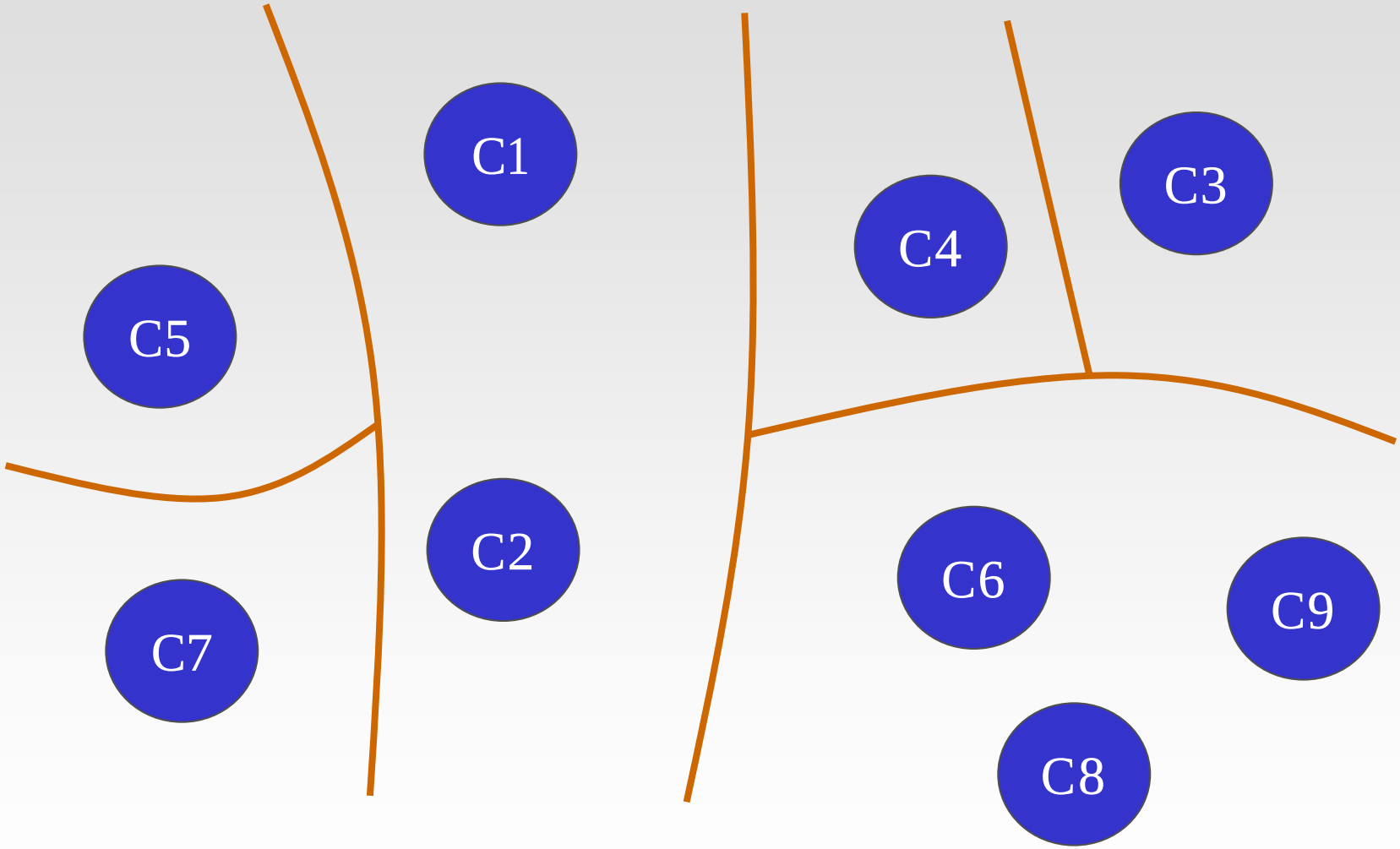
GET /MSADC/root.exe?/c+dir
Co[illegible]on:close

attacker:2496 ← honeypot:80

403 Access Forbidden

C2

# Connection Clustering



# Connection Clustering

attacker:2492 → honeypot:80

GET /scripts/root.exe?/c+dir
Co[illegible]on: Close

attacker:2492 ← honeypot:80

404 Object Not Found

C1

attacker:2496 → honeypot:80

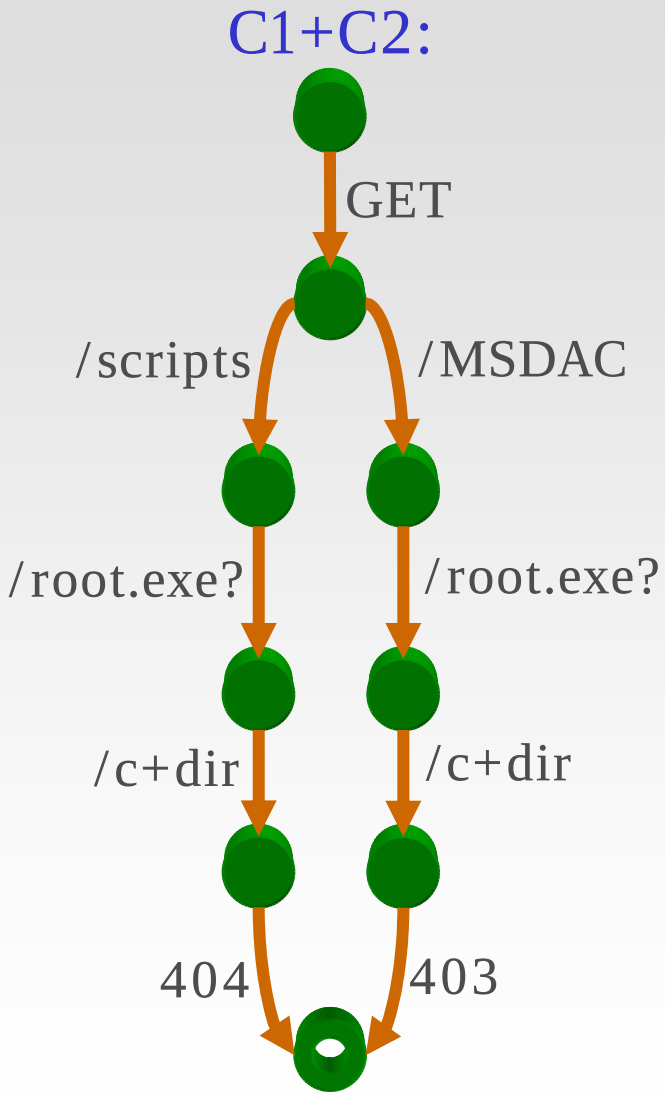
GET /MSADC/root.exe?/c+dir
Co[illegible]on:close

attacker:2496 ← honeypot:80

403 Access Forbidden

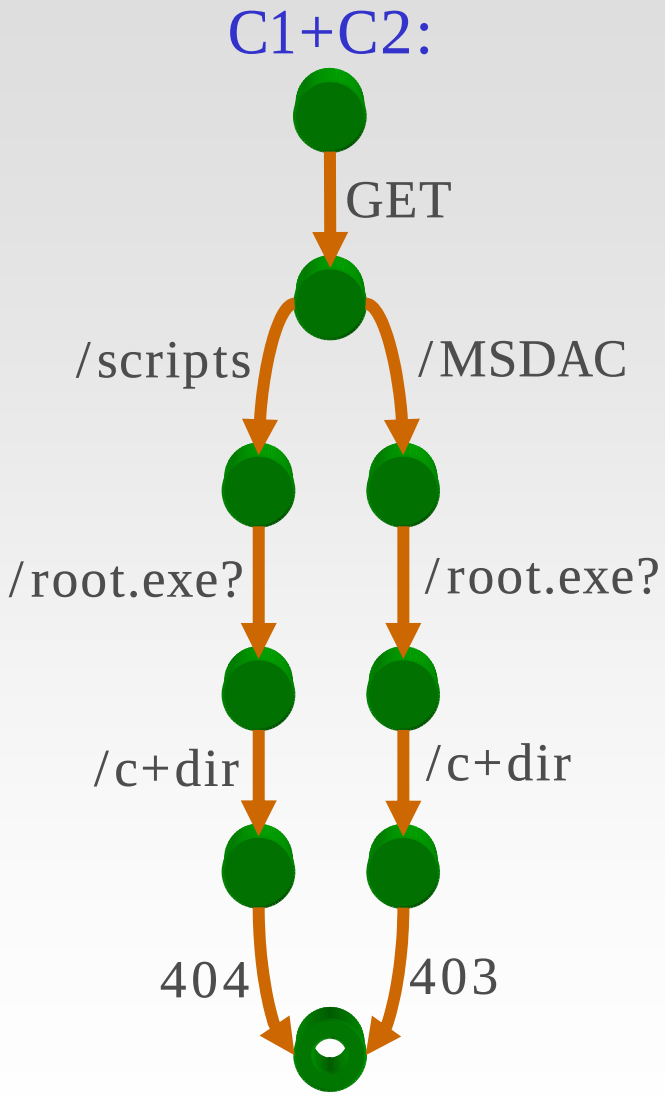
C2

# Connection Signature




- PFSA generalization
  - Compute probability that each edge is traversed
  - Merge states when probabilistically indistinguishable
  - Add transitions representing reordering & repetition

# Connection Signature



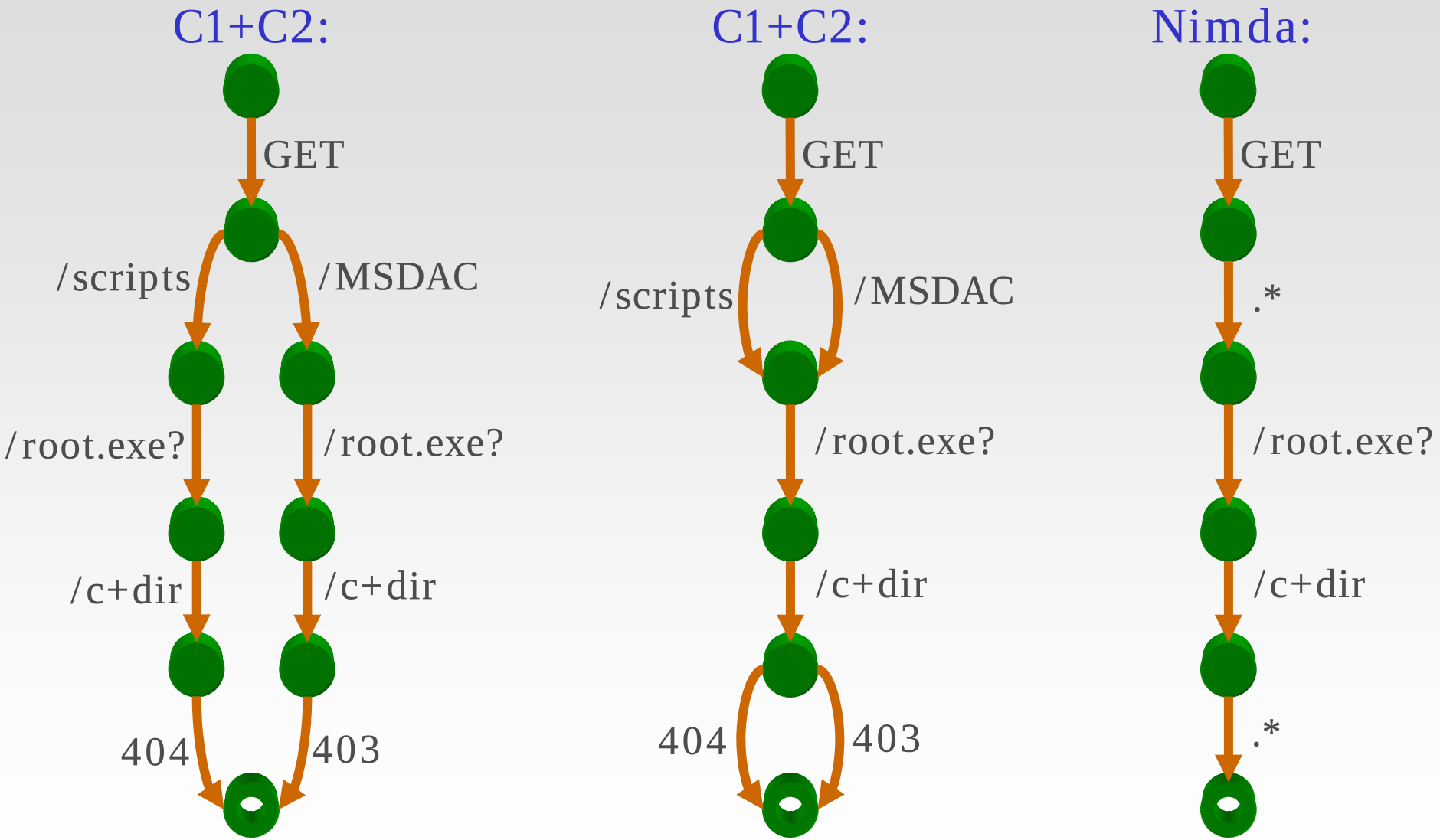

- Subsequence creation
  - Accept any data at points of high variability

Let $A, B \in \Sigma^*$

Let $w, x, y, z \in \Sigma$

Convert signature accepting $AwB, AxB, AyB, AzB$ to $A[.*]B$

# Connection Signature



# Experiments

- Trained on honeynet data (Two unused /19s)
  - HTTP: 2 days 25,587 connections
  - NetBIOS: 2 days 38,722 connections
- Detection effectiveness: 99.9%
  - Test period: 7 days 2,846,783 connections
- False alarms and misdiagnoses: 0
  - U.Wisc. CSL HTTP production data
    - 19,000 clients 4,400 servers
  - Test period: 8 hours 194,001 connections

# Effective Detection—HTTP

| *Signature* | *# Present* | *Nemean Detected* | | *Snort (ver 2.1.0) Detected* |
|---|---|---|---|---|
| | | *Connection* | *Session* | |
| Options | 1172 | 1172 | 1160 | 1171 |
| Nimda | 496 | 496 | n/a | 495 |
| Propfind | 229 | 229 | 205 | 229 |
| Welchia | 90 | 90 | 90 | 90 |
| Win Media Player | 89 | 89 | 89 | 89 |
| Code Red Retina | 4 | 4 | 4 | 0 |
| Kazaa | 2 | 2 | 2 | 2 |

# Effective Detection—NetBIOS

| *Signature* | *# Present* | *Nemean Detected* *Connection* |
|---|---|---|
| Srvsvc | 19934 | 19930 |
| Samr | 8743 | 8741 |
| Epmapper | 1263 | 1258 |
| NvcplDmn | 62 | 61 |
| Deloder | 30 | 30 |
| LovGate | 1 | 0 |

# Balancing Specificity & Generality

## Specificity

- Honeynet data collection
- Clustering
- Application-level protocol semantics-awareness

## Generality

- Normalization
- PFSA generalization
- Subsequence creation

# Questions?

## ... or send us email:


Vinod Yegneswaran vinod@cs.wisc.edu

Jonathon Giffin giffin@cs.wisc.edu

Paul Barford pb@cs.wisc.edu

Somesh Jha jha@cs.wisc.edu



## Thanks to:

U.Wisc. CSL

Christian Kreibich

Fabian Monrose

Vern Paxson