

Passive Internet Health Monitoring with BGP



Dennis McGrath
Institute for Security
Technology Studies
Dartmouth College



Measures, Metrics, and Indicators

- Biological
 - ◆ Blood Pressure
 - ◆ Body Temperature
 - ◆ Pulse
 - ◆ Respiration
- Meteorological
 - ◆ Air Temperature
 - ◆ Barometric Pressure
 - ◆ Wind Speed/Direction
 - ◆ Relative Humidity
- Seismic
 - ◆ Richter Scale
 - ◆ Seismic Moment
- Economic
 - ◆ DJIA, S&P500
 - ◆ Unemployment Rate
 - ◆ GNP, GDP
- Internet Health
 - ◆ ?

Internet Metrics

- How do we compare the effects of traumatic events on the Internet?
 - ♦ Scanning Worms
 - ♦ 9/11
 - ♦ Baltimore Tunnel Fire
 - ♦ Blackout
- How do we describe and monitor current Internet conditions?
- Packet Probes
 - ♦ Packet Loss
 - ♦ Packet Latency
- Service availability
 - ♦ Email
 - ♦ Web
 - ♦ E-commerce
- Interdomain Routing
 - ♦ Stability
 - ♦ Reachability

Toward Standard BGP Metrics

- Metrics should be reductive
 - ◆ Dampen transient phenomenon (reset spikes)
 - ◆ Dampen localized phenomenon
 - ◆ Strongly indicate widespread phenomenon
 - ◆ Should be normalized to a standard scale
- BGP metrics
 - ◆ Instability, based on route flapping or time density of route announcements and withdrawals
 - ◆ Reachability, based on table sizes (measured in IP blocks) or total number of IP addresses.

Global Instability Index (GII)

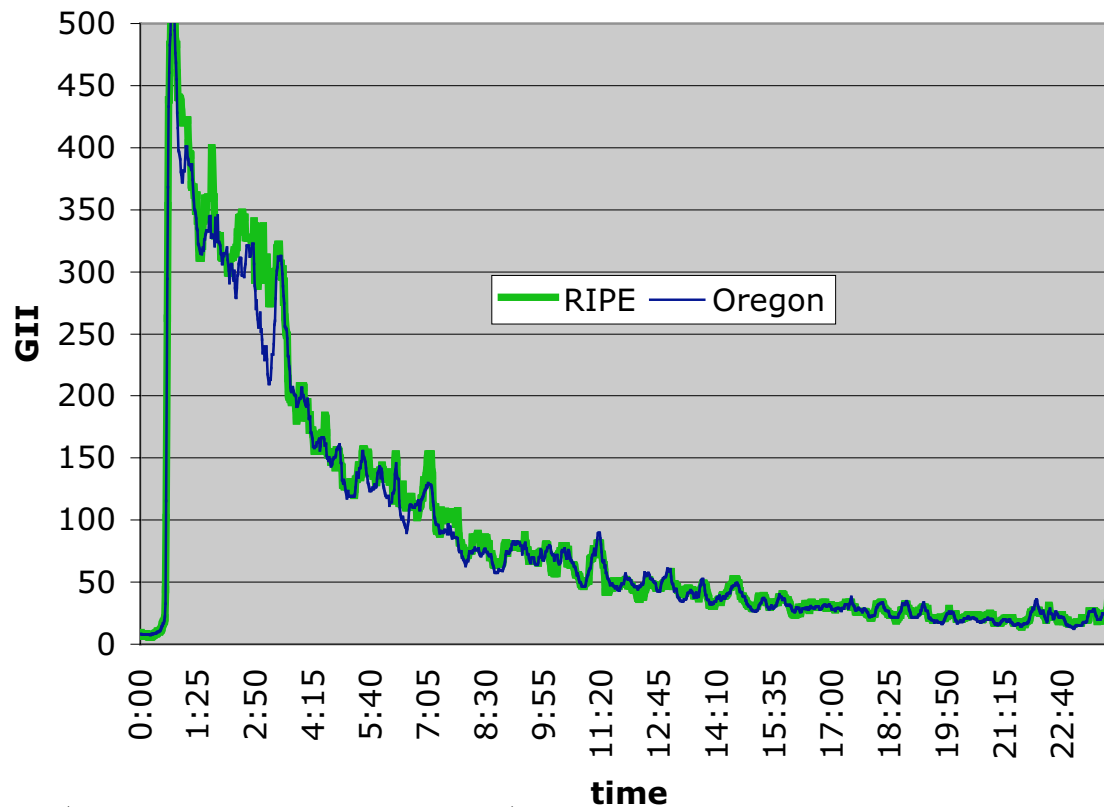
- Given n BGP peers
- For each peer, calculate local weighting factor (w_i) based on long term hourly activity
- For each peer, count announcements and withdrawals per minute (u) over 15 minute sliding window and determine median value (u_{median})
- Calculate Local Instability Index (LII) for each peer where $LII_i = u_{\text{median } i} \cdot w_i$
- $GII = LII_{\text{median}}$

GII Characteristics

- Values 0–50 normal
- Values 50–100 unstable
- Values > 100 very high instability
- Lags significant events by 8 minutes
- Values calculated with different data sets are very similar
- High water mark: 536 at 12:48 AM EST on January 25, 2003

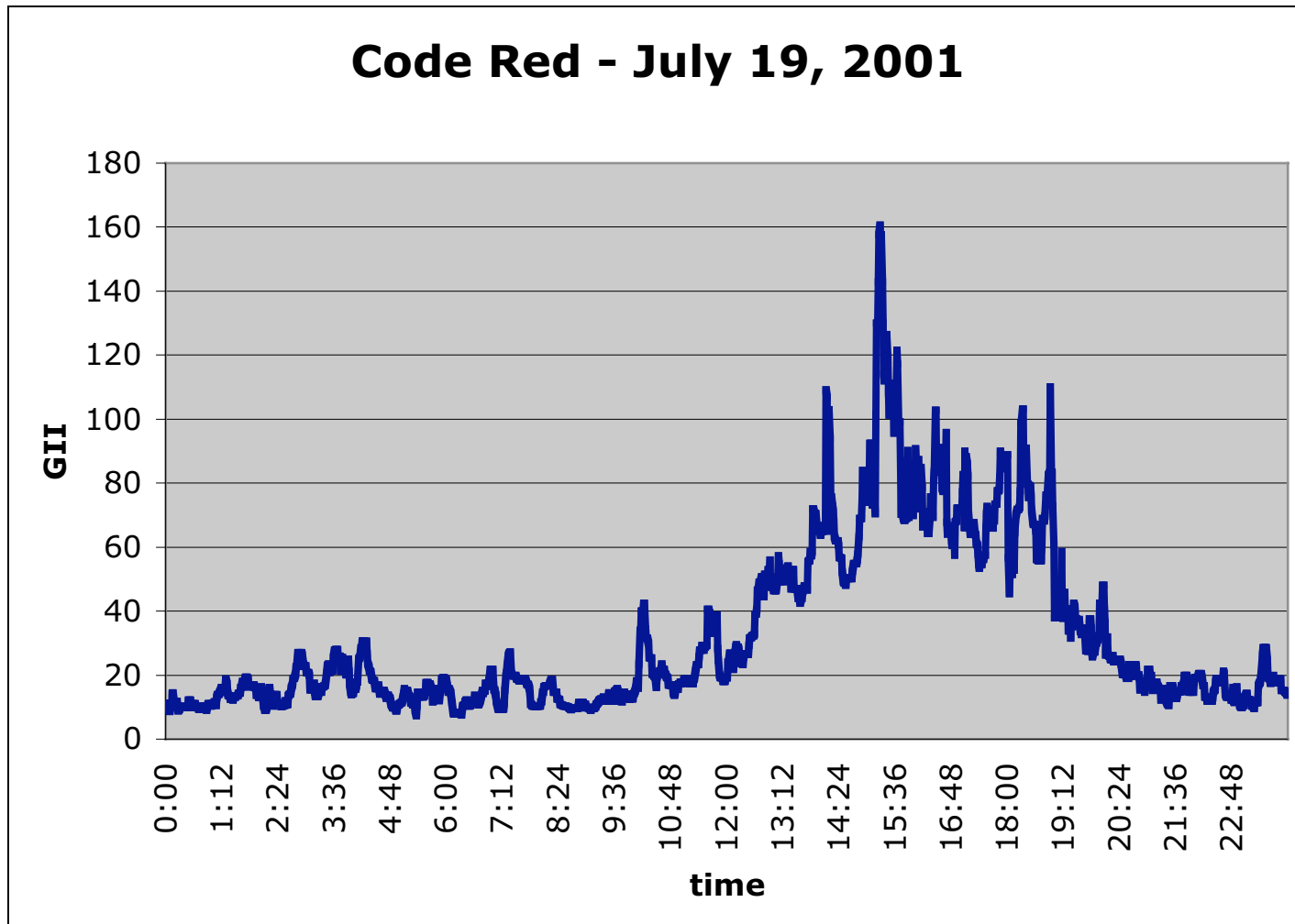
Slammer Worm Instability

Slammer - January 25, 2003



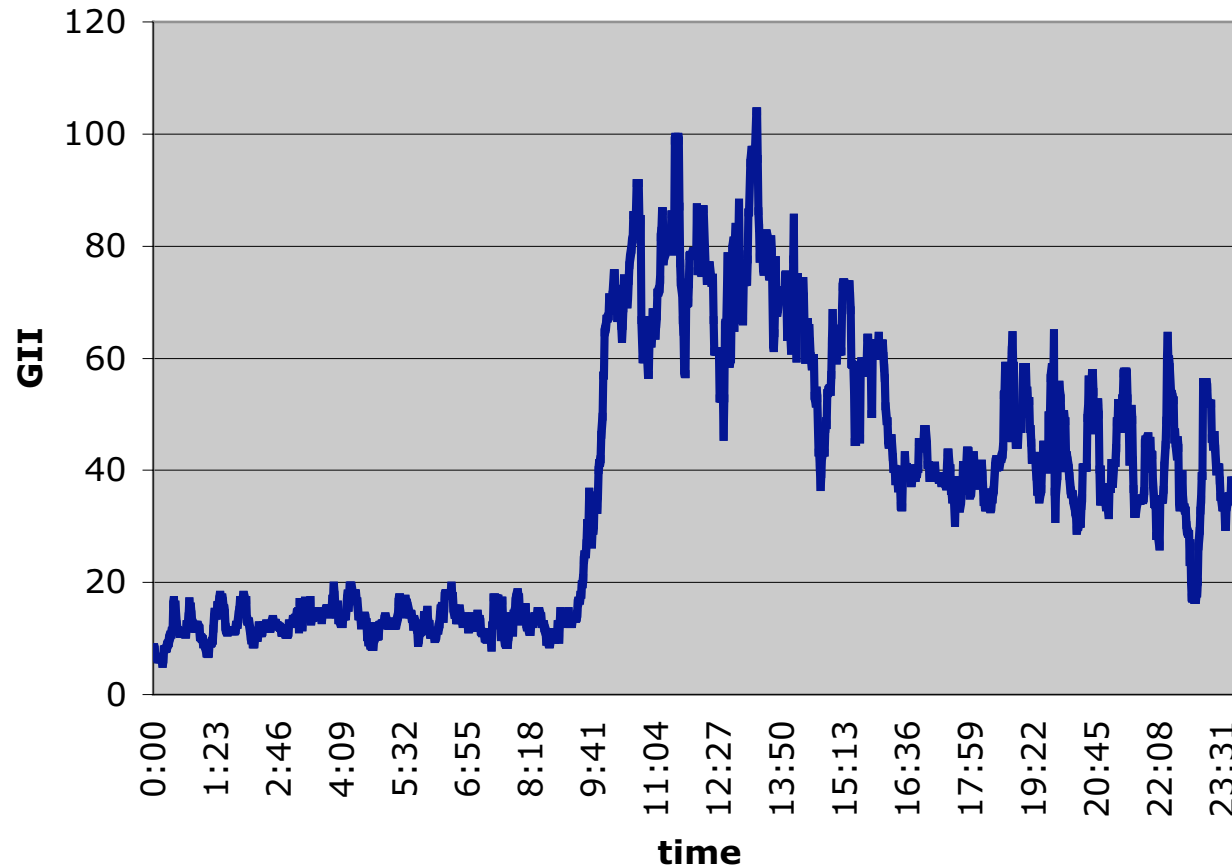
*(sim_{ripe,oregon} = 98.6%)

Code Red Instability



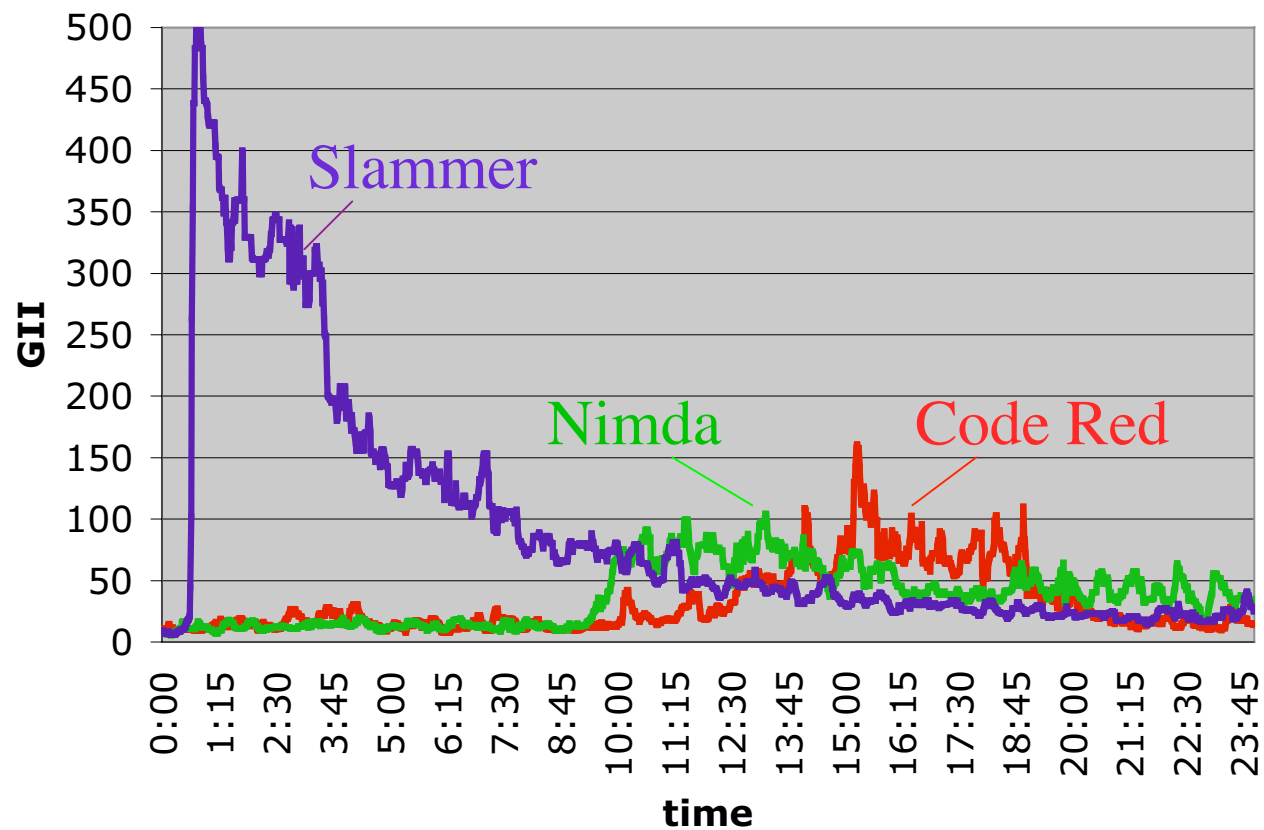
Nimda Instability

Nimda - September 18, 2001

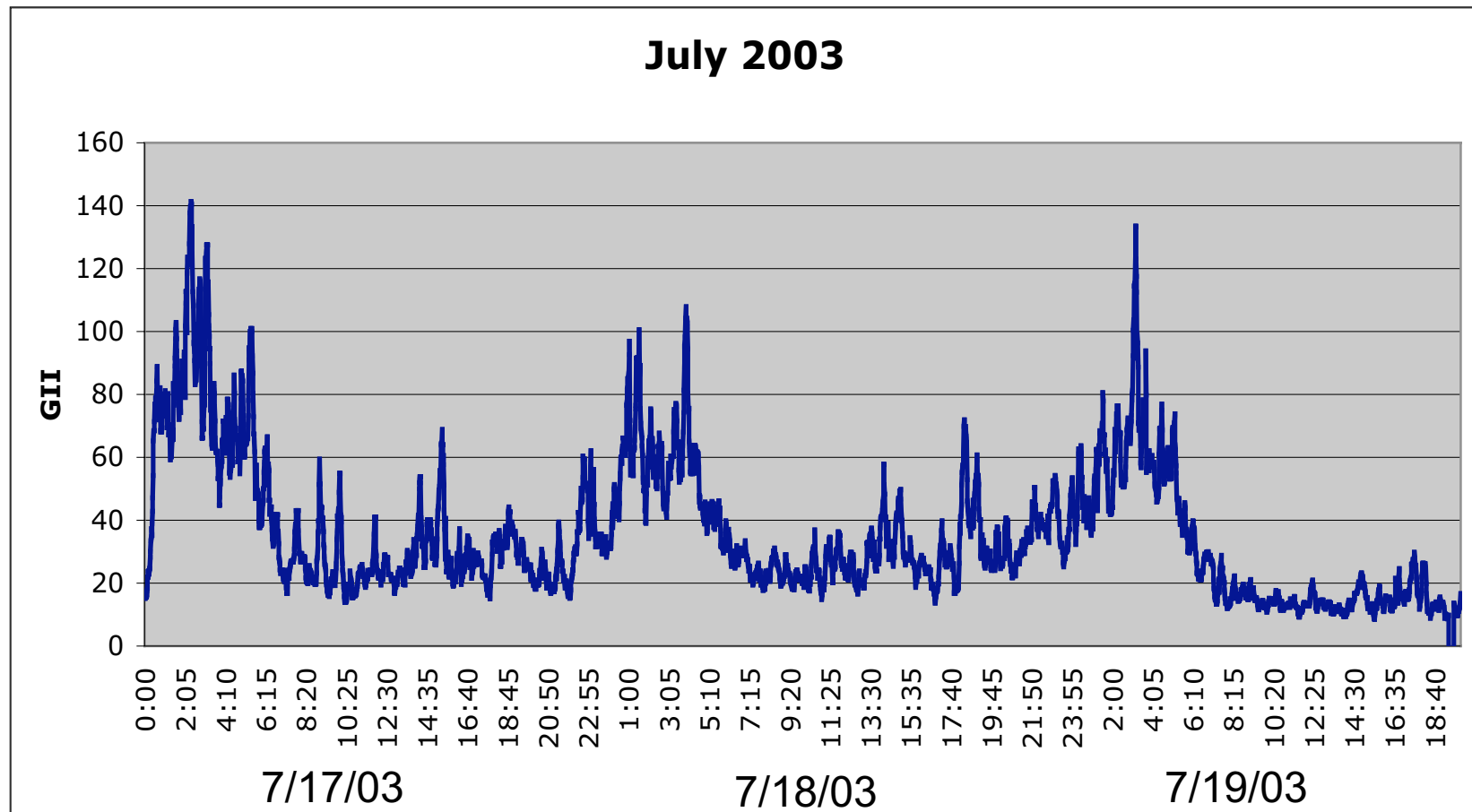


Three Bad Days

The Big Three

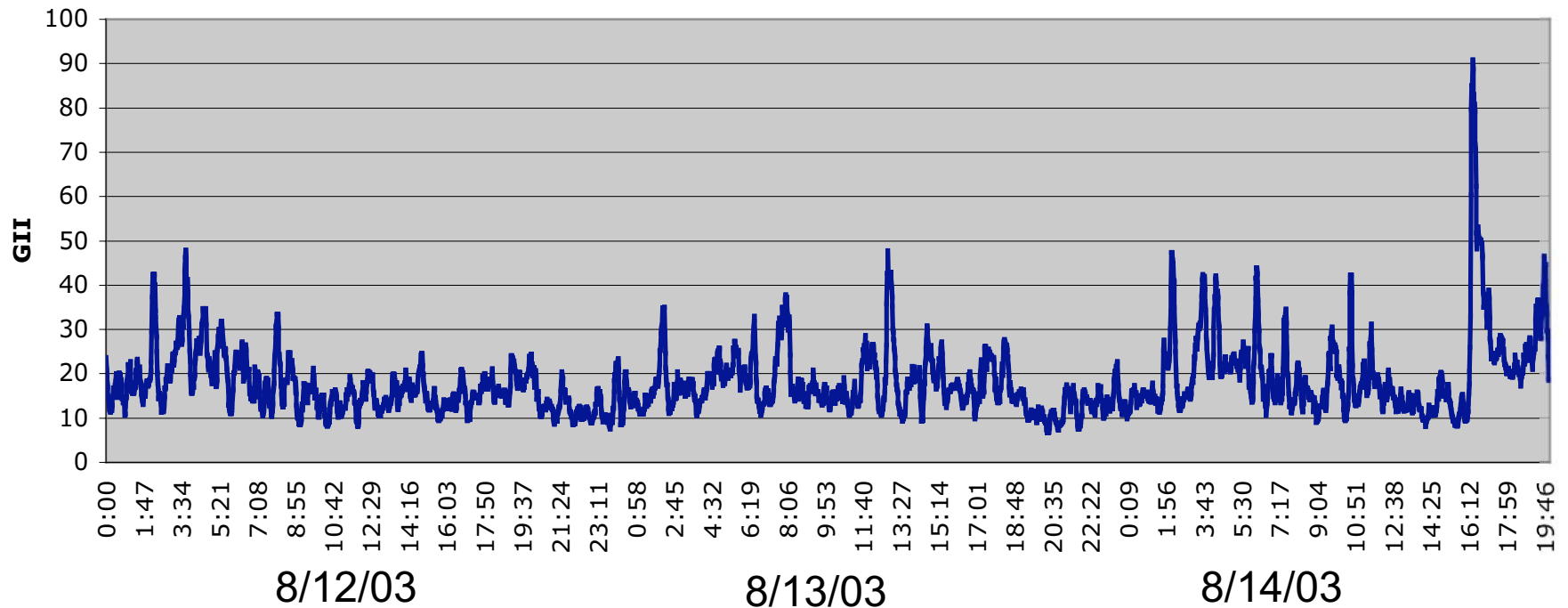


Three Days in July

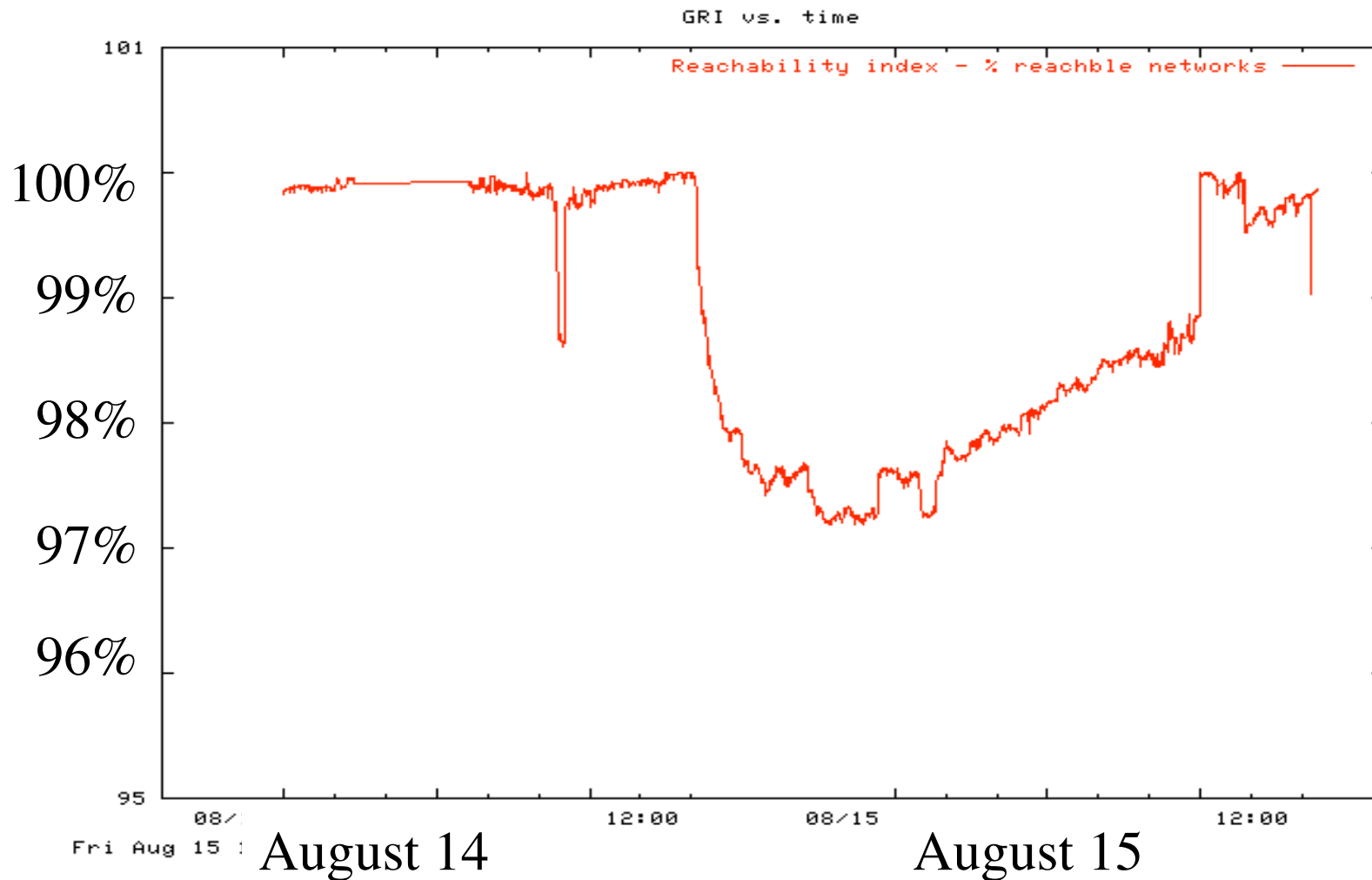


Three Days in August

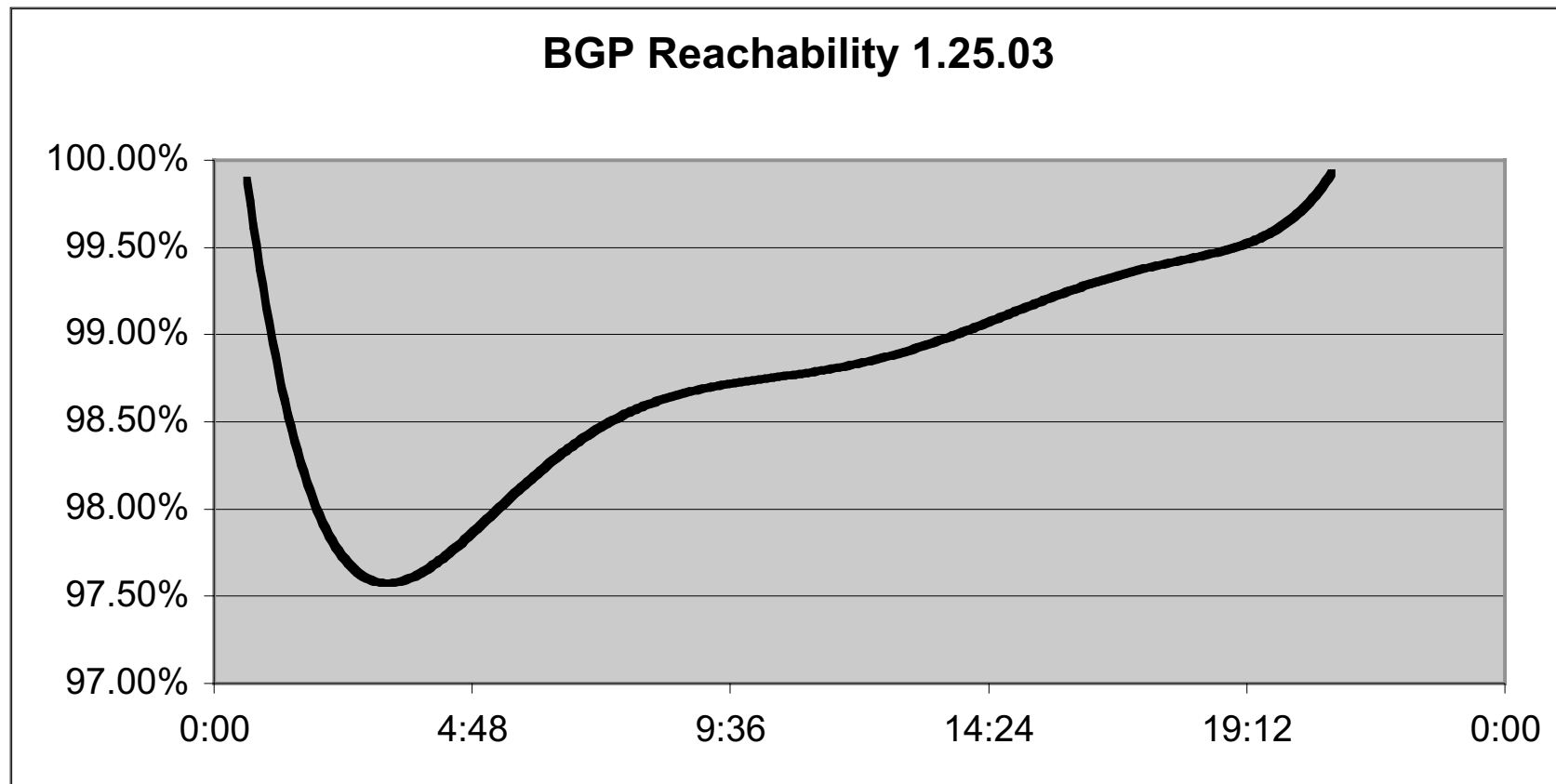
August 2003



Global Reachability Index- Blackout



Global Reachability Index – Slammer Worm



Errata

- Other BGP metrics ?
- Other network health metrics
 - ◆ Packet latency, loss
 - ◆ Service availability
- GII plot: netwatch.ists.dartmouth.edu
- Ideas and feedback are welcome
- We need data!