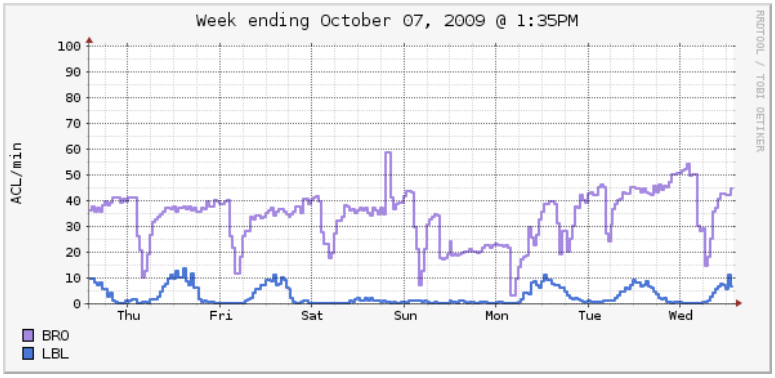
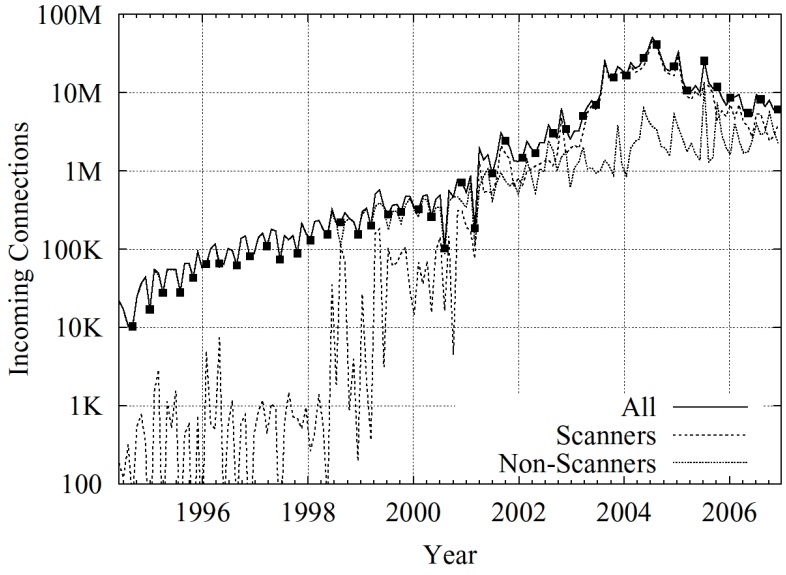
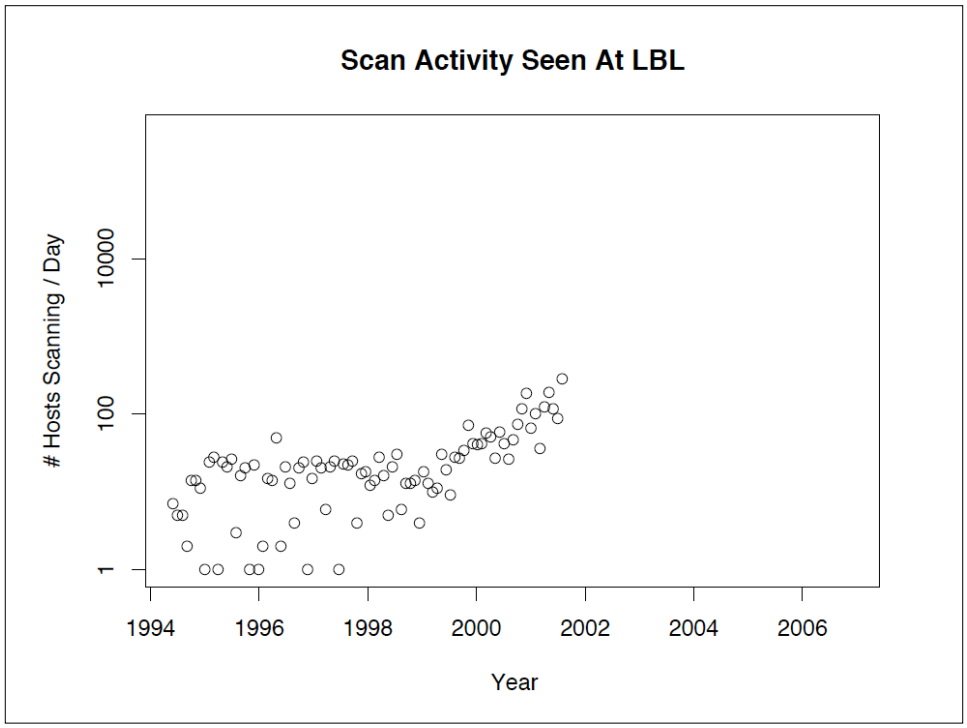
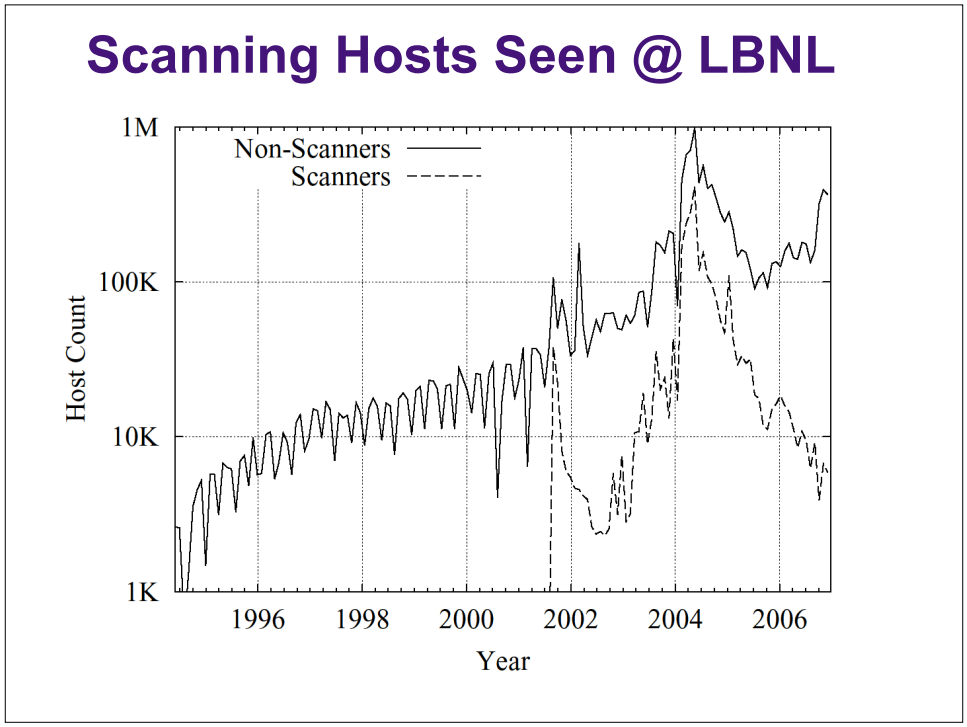


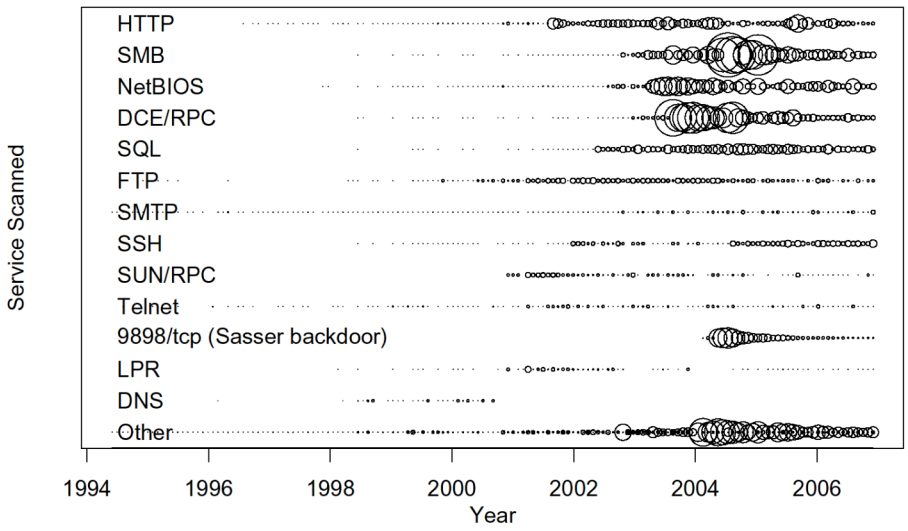
Scanning Activity Seen @ LBNL



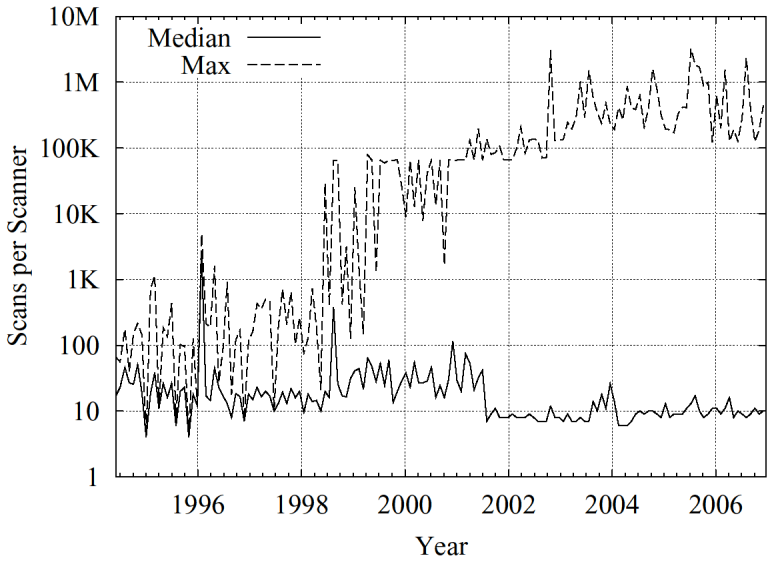

Scan Activity Seen At LBL
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year


Scanning Hosts Seen @ LBNL
Non-Scanners
Scanners
Host Count
1M
100K
10K
1K
1996
1998
2000
2002
2004
2006
Year

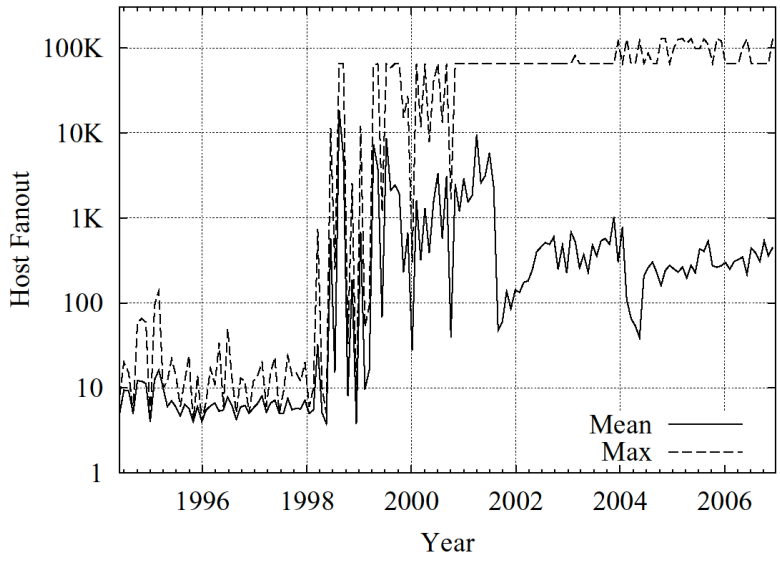
Services Scanned Over Time



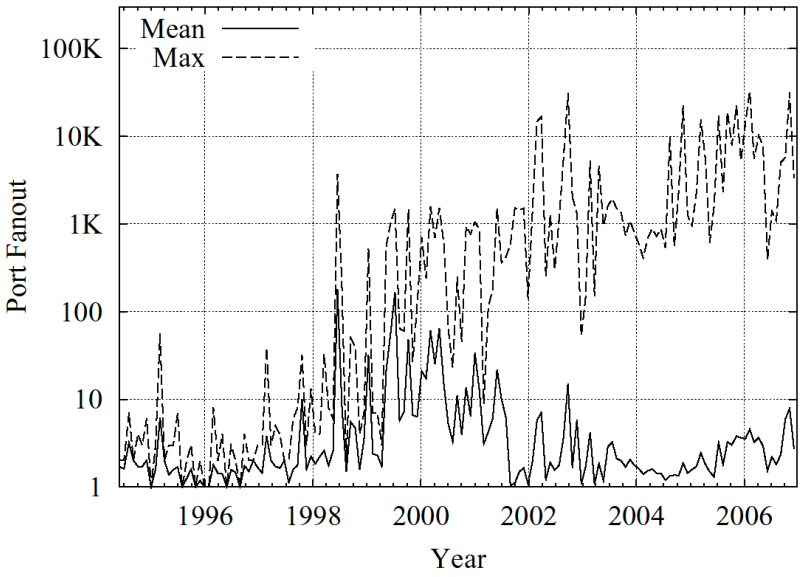
Scans Per Scanner



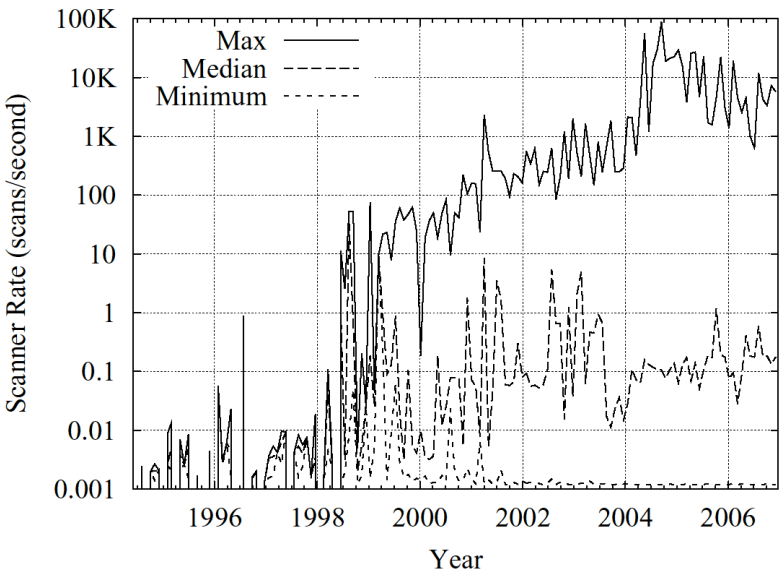
Hosts Scanned Per Scanner

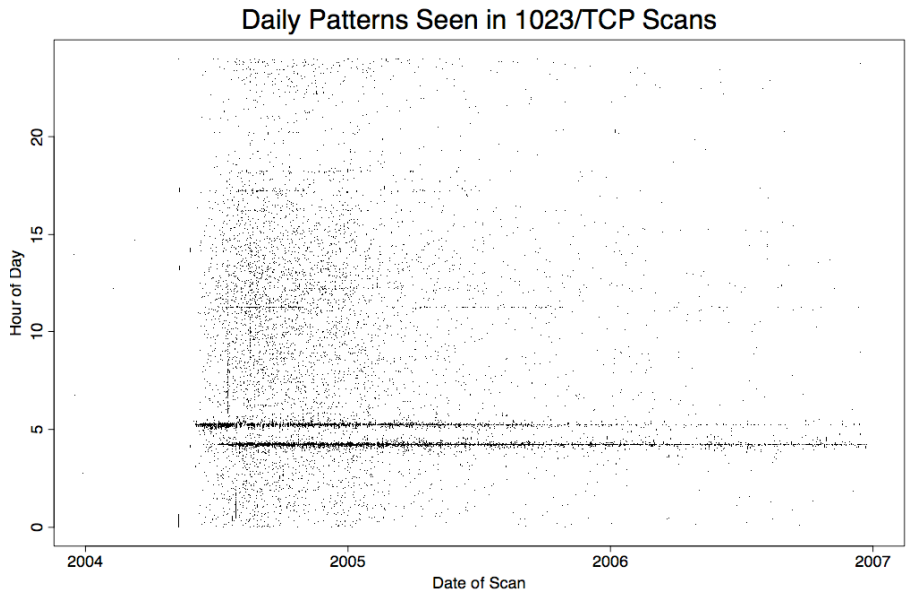


Ports Scanned Per Scanner

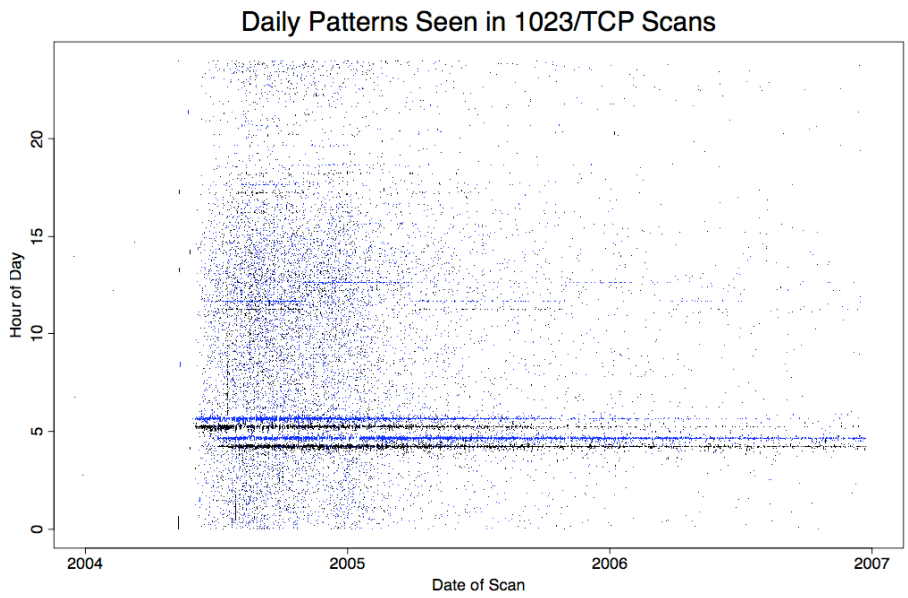


Scanning Speed

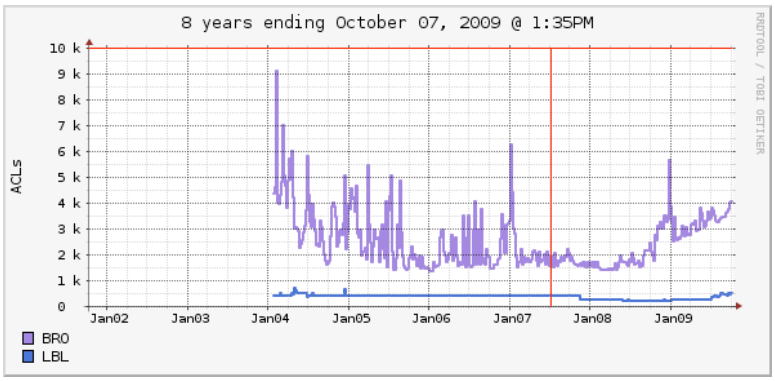


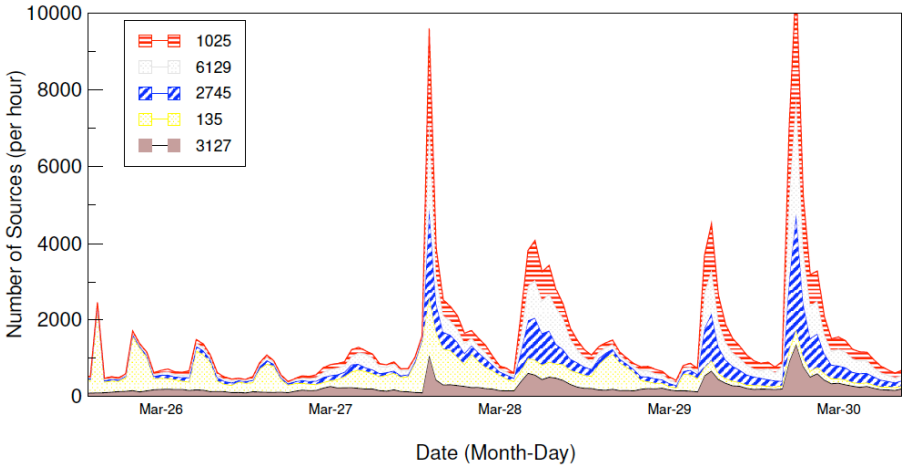


/16 at LBL, sampled 1-in-1K

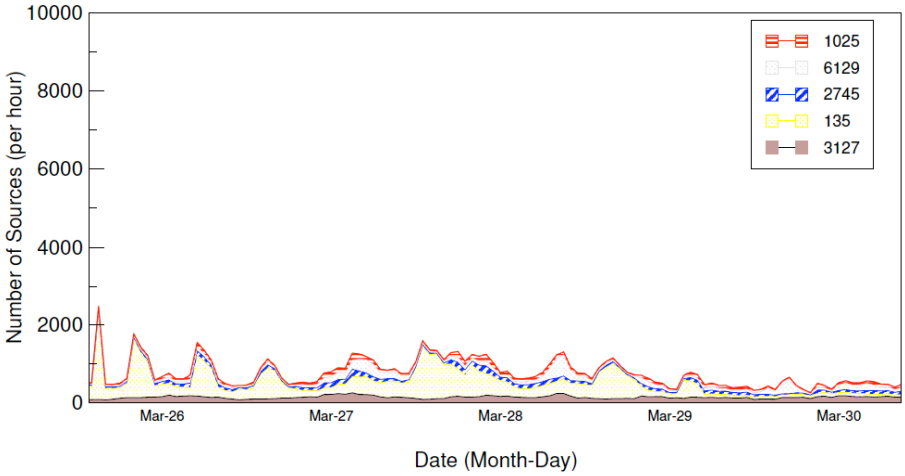


/16 at LBL, sampled 1-in-1K
2nd /16, sampled 1-in-1K



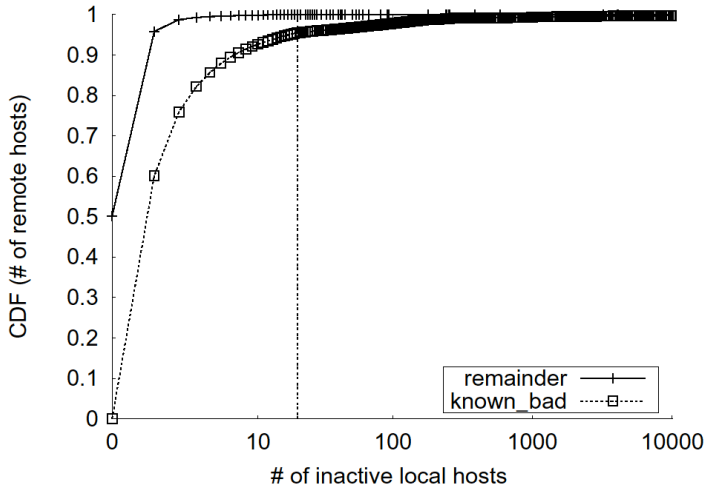


(a) Agobot Sources: UW I



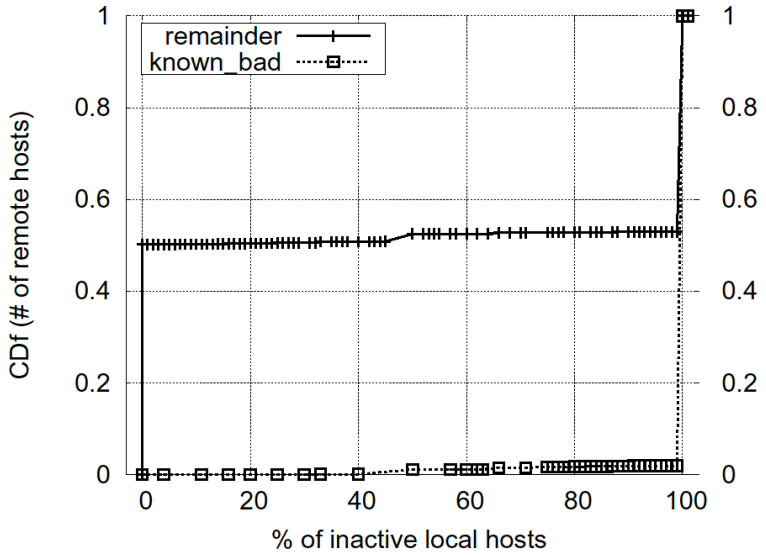
(b) Agobot Sources: UW II

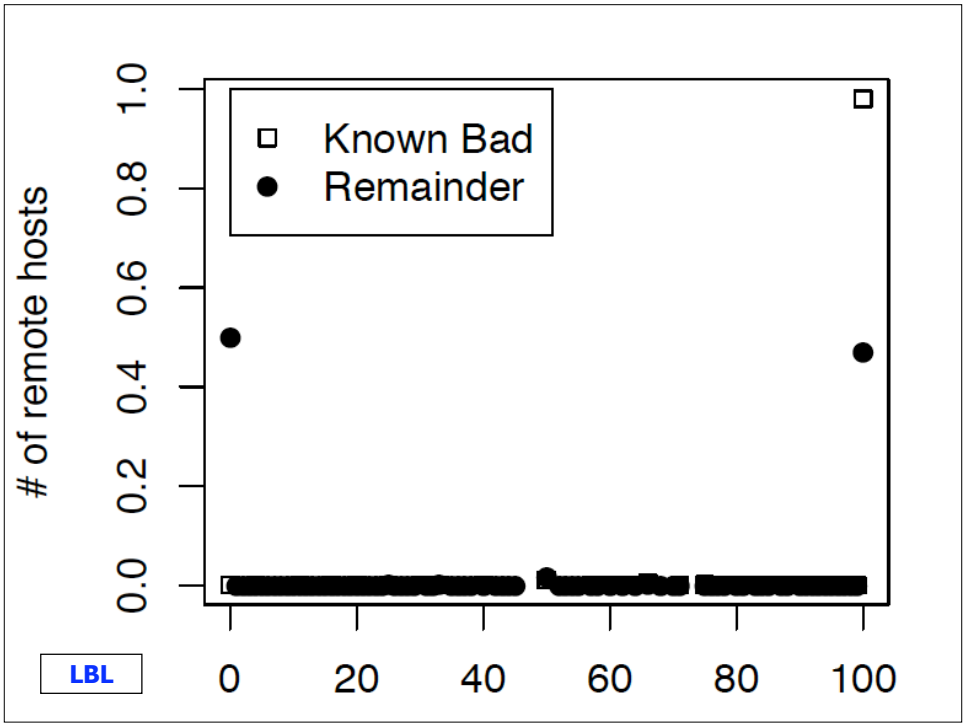
Failed Conn's Not Enough Info



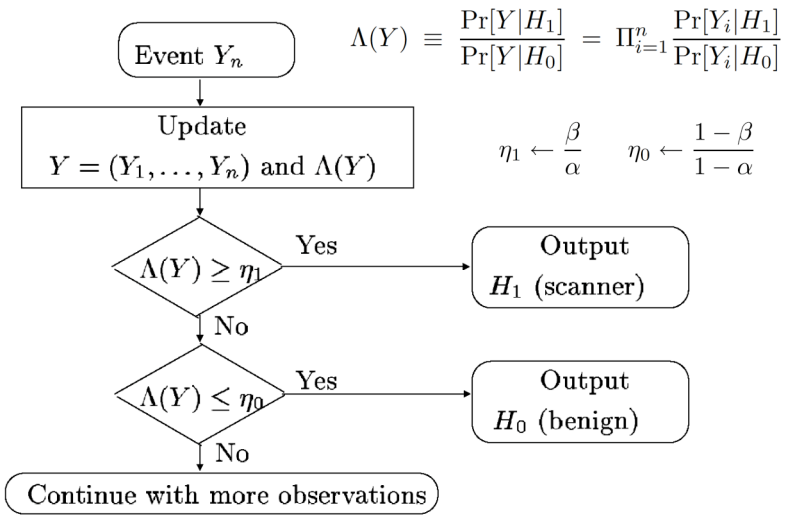
(a) LBL

Failure *Ratio* Much More Distinctive





Real-Time Detection



$$\Lambda(Y) \equiv \frac{\Pr[Y|H_1]}{\Pr[Y|H_0]} = \Pi_{i=1}^{n} \frac{\Pr[Y_i|H_1]}{\Pr[Y_i|H_0]}$$

$$\eta_1 \leftarrow \frac{\beta}{\alpha} \qquad \eta_0 \leftarrow \frac{1-\beta}{1-\alpha}$$

Expected Time Until Decision

$$E[N|H_0] = \frac{\alpha \ln \frac{\beta}{\alpha} + (1-\alpha) \ln \frac{1-\beta}{1-\alpha}}{\theta_0 \ln \frac{\theta_1}{\theta_0} + (1-\theta_0) \ln \frac{1-\theta_1}{1-\theta_0}},$$

$$E[N|H_1] = \frac{\beta \ln \frac{\beta}{\alpha} + (1-\beta) \ln \frac{1-\beta}{1-\alpha}}{\theta_1 \ln \frac{\theta_1}{\theta_0} + (1-\theta_1) \ln \frac{1-\theta_1}{1-\theta_0}}.$$