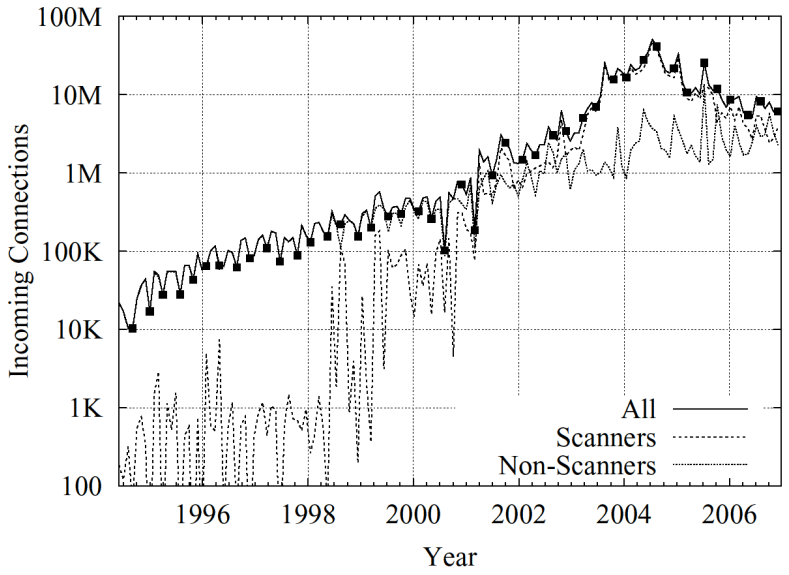
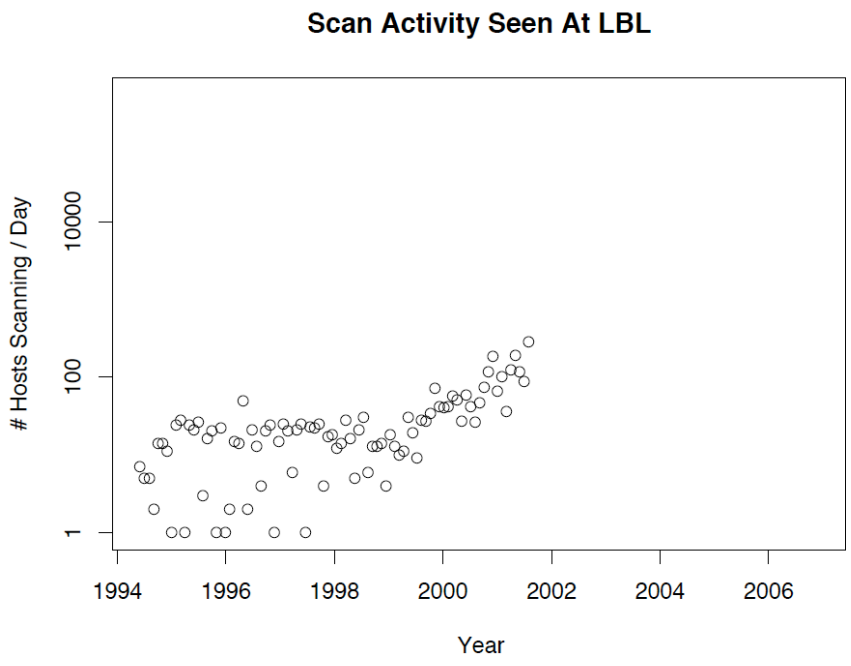
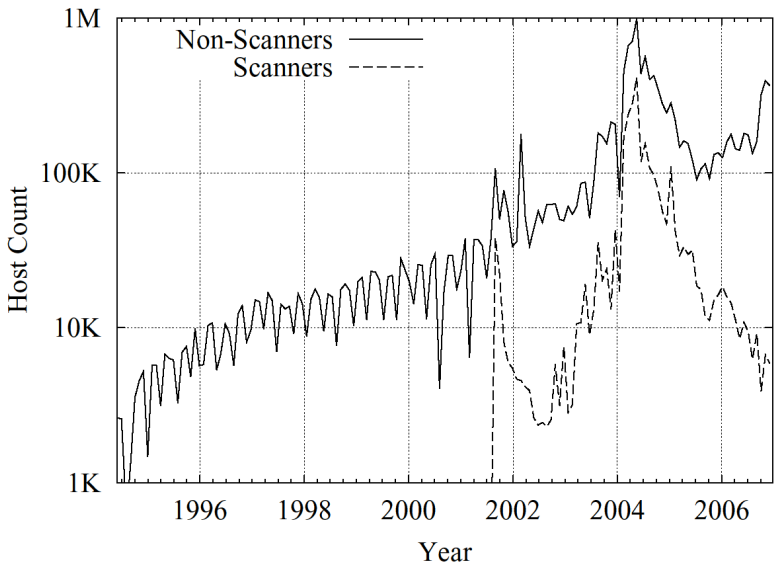
Scanning Activity Seen @ LBNL

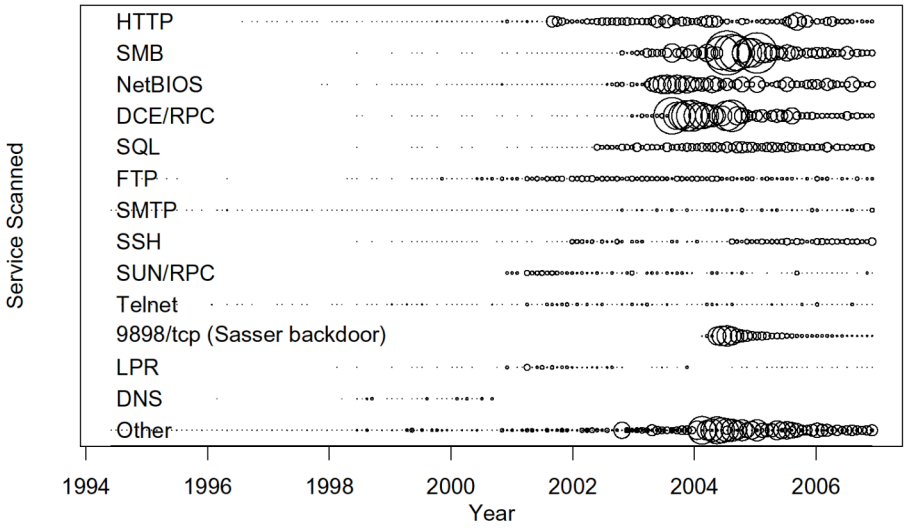




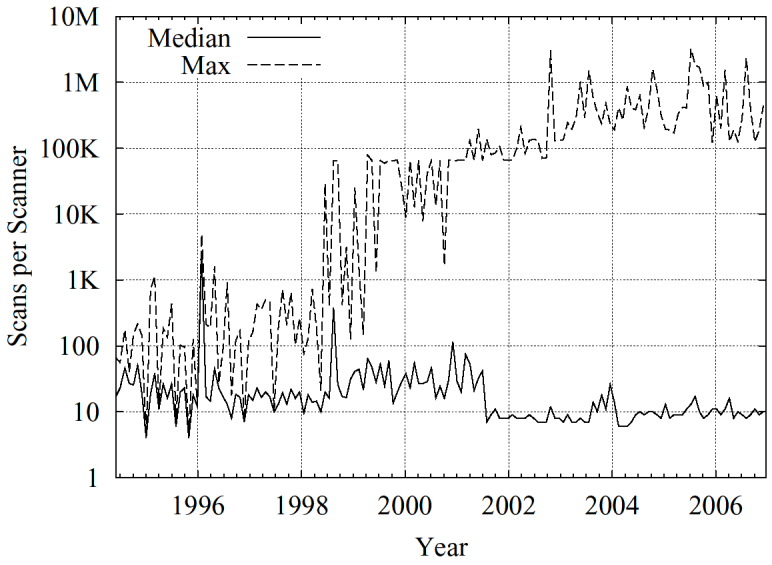
Scanning Hosts Seen @ LBNL



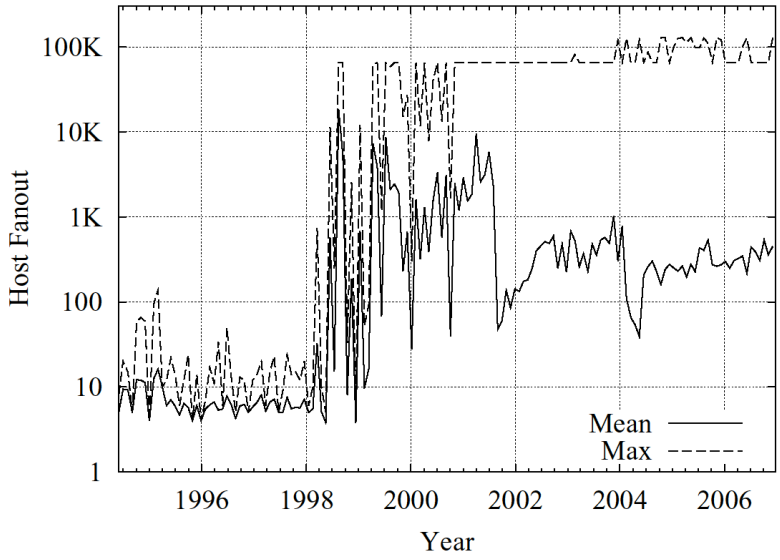
Services Scanned Over Time



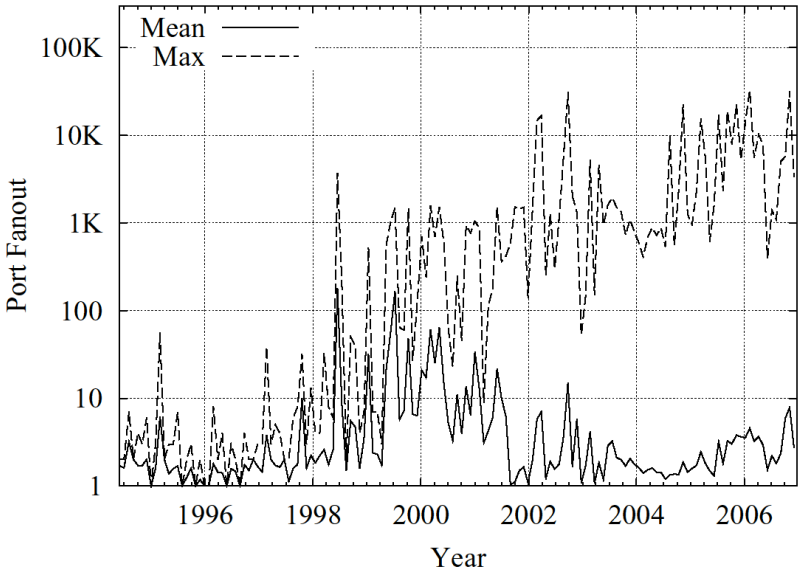
Scans Per Scanner



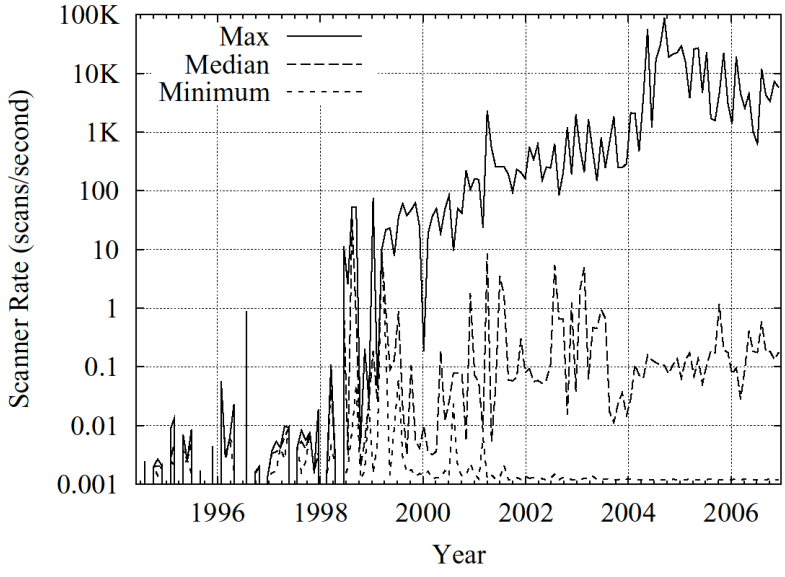
Hosts Scanned Per Scanner

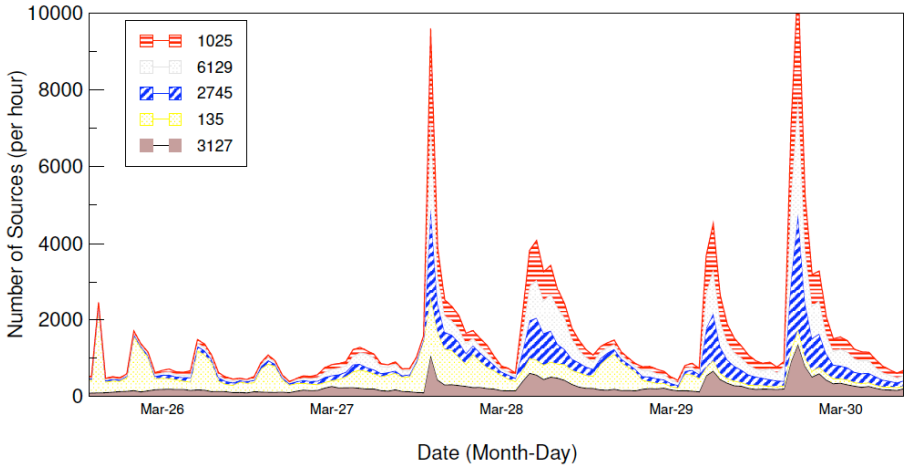


Ports Scanned Per Scanner

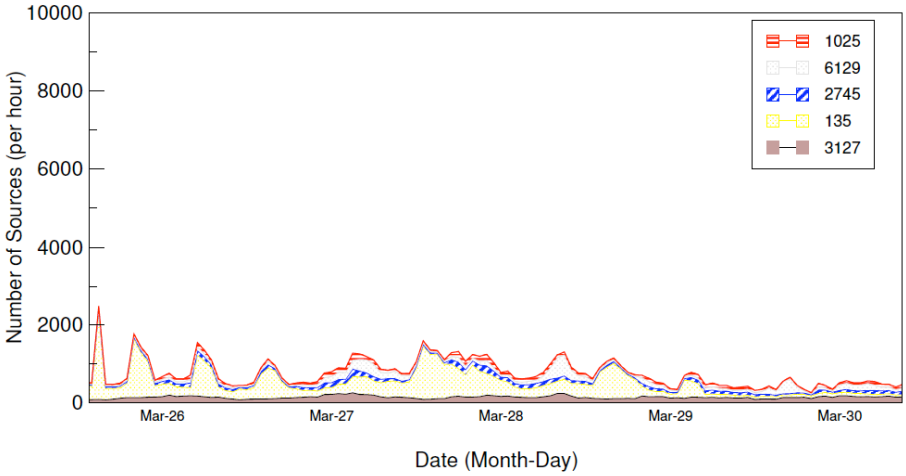


Scanning Speed



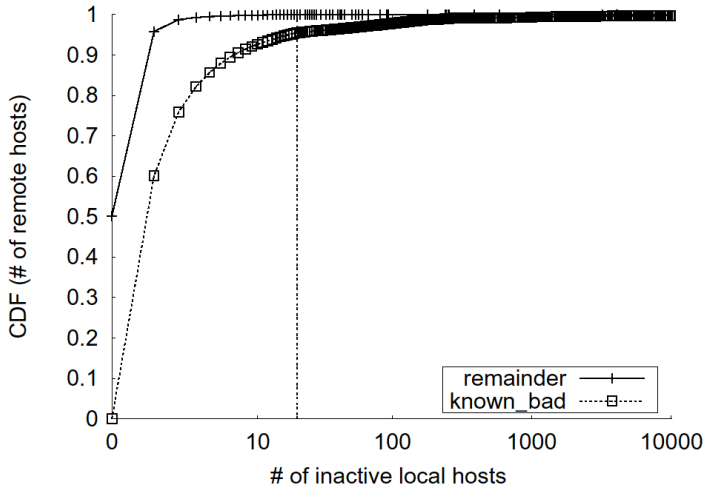


(a) Agobot Sources: UW I



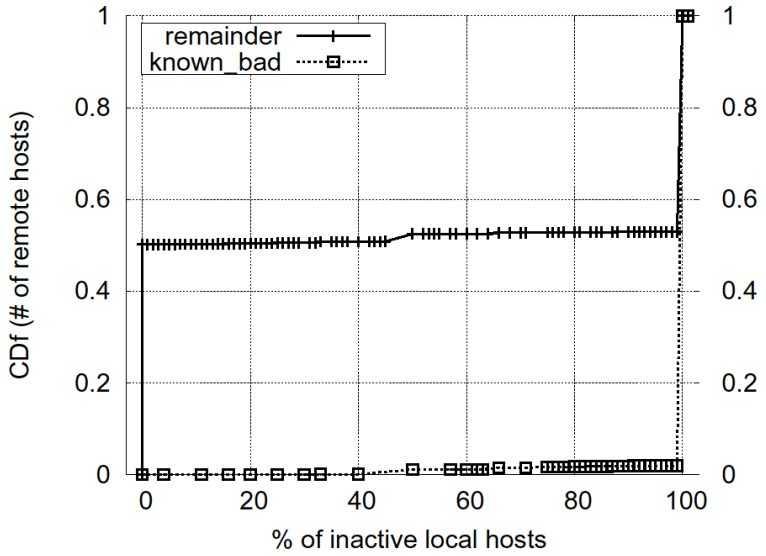
(b) Agobot Sources: UW II

Failed Conn's Not Enough Info

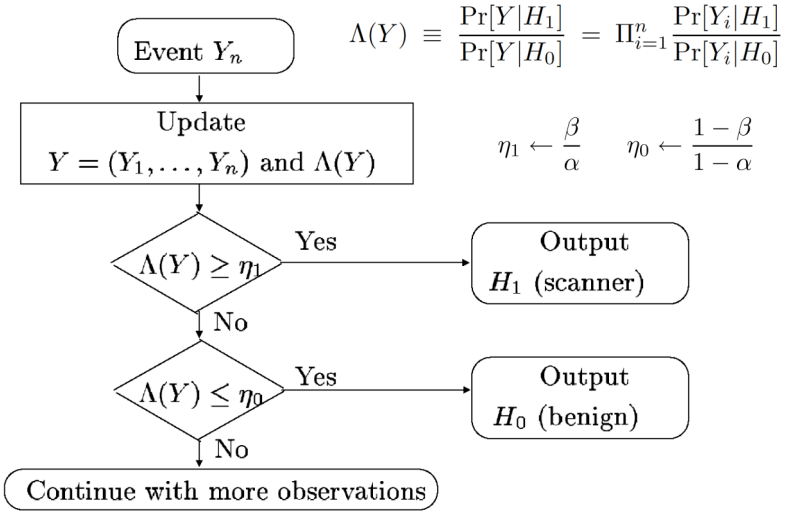


(a) LBL

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

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

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

RB-SHT: Rate-Based Detection

- FCC's interarrival times follow exponential dist. with mean $\frac{1}{\lambda_1}$ (scanner) or $\frac{1}{\lambda_0}$ (benign host). $\frac{1}{\lambda_1} < \frac{1}{\lambda_0}$
- T_n : elapsed time until n FCC arrivals follows n-Erlang distribution

$$\Lambda(n, T_n) \equiv \frac{f_n(T_n \mid H_{\text{scanning}})}{f_n(T_n \mid H_{\text{benign}})} = \left(\frac{\lambda_1}{\lambda_0}\right)^n \exp^{-(\lambda_1 - \lambda_0)T_n}$$