Report

1 Path Bias Attacks in TOR

Path Bias Attack occurs when an adversary controlling an entry node may be able to force a client's traffic to use an exit node controlled by the attacker and hence compromise the essential Anonymity and Privacy properties of the TOR network and discover their activity.

1.1 Active Adversary/Path Bias Adversary :-

For a path-bias attack
A Defender wishes to ensure that the number of circuits through any pair of guard-exit pairs should not exceed $E_{gx}-$the expected no of paths through g and x given size n whereas
An Active Adversary intends to achieve $n_{\hat{g}\hat{x}} > E_{\hat{g}\hat{x}} + (\phi E_{\hat{g}\hat{x}} + \lambda)$ where $n_{\hat{g}\hat{x}}$ is total no of circuits through g and x ,$\phi E_{\hat{g}\hat{x}}$ is a constant fraction increase over $E_{\hat{g}\hat{x}}$ that the adversary may gain by increasing traffic through $\hat{g}\hat{x}$, λ is a constant
Defender ensures that $E[n_{gx}] \leq E_{\hat{g}\hat{x}} + (\phi E_{\hat{g}\hat{x}} + \lambda)$ for every guard-exit pair and marks a node as malicious if the above equation fails

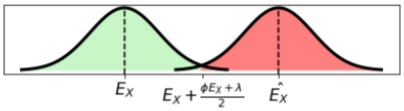

Fig. 4. Observed frequency distributions for exit x with no attack (centered around E_x) and with an attack defined by parameters ϕ and λ (centered around $\hat{E}_x$).

Based on the above statistical analysis it is clear that if n_x crosses the mid point it is considered as attack or else no attack
If $n_x \leq (E_x + \hat{E}_x)/2 \Rightarrow$ **No Attack**
If $n_x > (E_x + \hat{E}_x)/2 \Rightarrow$ **Attack**

$$(E_x + \hat{E}_x)/2 = \frac{E_x + E_x + (\phi E_x + \lambda)}{2} = E_x + \frac{(\phi E_x + \lambda)}{2}$$

Theorem: A sample size of

$$n \geq 12 \log(\frac{1}{\beta}).\frac{1}{p}.\frac{1}{(min\{1, (\phi + \frac{\lambda}{E_x})\})^2}$$

suffices to ensure that $n_x \leq E_x + (\phi_x + \lambda)/2)$ with probability at least $(1-\beta)$,p is probability of any circuit passing through x

Proof:-
Using Chernoff bound (Proof given at last)

$$P_r(X \geq (1+\delta)\mu) \leq e^{-\delta^2/3}, 0 < \delta \leq 1$$

Assuming $0 \leq \phi + \frac{\lambda}{E_x} \leq 1$, $(min\{1, (\phi + \frac{\lambda}{E_x})\})^2 = (\phi + \frac{\lambda}{E_x})^2$

$$P[n_x > (1 + \phi/2 + \frac{\lambda}{2E_x})E_x] \leq e^{-\frac{E_x(\phi/2 + \frac{\lambda}{2E_x})^2}{3}}$$

Since this probability is bounded by β (i.e at least $1-\beta$ =atmost β prob),

$$e^{-\frac{E_x(\phi/2 + \frac{\lambda}{2E_x})^2}{3}} \geq \beta$$

Applying log on both sides, $\frac{E_x}{4}(\phi + \frac{\lambda}{E_x})^2 . \frac{1}{3} \geq \ln \frac{1}{\beta}$,$(E_x = np)$

$$\frac{np}{12}(\phi + \frac{\lambda}{E_x})^2 \geq \ln \frac{1}{\beta}$$

$$n \geq 12 \ln 1/\beta . \frac{1}{p} . \frac{1}{(\phi + \frac{\lambda}{E_x})^2}$$

Hence it it proved for $0 \leq \phi + \frac{\lambda}{E_x} \leq 1$

Assuming $\phi + \frac{\lambda}{E_x} \geq 1$,Using Chernoff bound

$$P_r(X \geq (1+\delta)\mu) < e^{\frac{-\delta\mu}{3}}, \delta \geq 1$$

$$P[n_x > (1 + \phi/2 + \frac{\lambda}{2E_x})E_x] \leq e^{-\frac{E_x(\phi/2 + \frac{\lambda}{2E_x})}{3}}$$

$$n \geq 6 \ln 1/\beta . \frac{1}{p} . \frac{1}{(\phi + \frac{\lambda}{E_x})} \geq 12 \ln 1/\beta . \frac{1}{p} . \frac{1}{(\phi + \frac{\lambda}{E_x})^2}$$

Hence it is Proved for $\phi + \frac{\lambda}{E_x} \geq 1$

The above result shows that PB attacks(Active Adversary) diverting significant amounts of traffic can be detected with privacy guarantees from small amounts of data.The usefulness of this lemma is by using the sample size(n) we try to limit the false positive rates.i.e A small number of samples which are in mid-way between the observed distributions will have false positive rate which is bounded by β.

2 Chernoff bound proofs

Definition of Chernoff bound(Proof given at last)

$$P_r(X \geq (1+\delta)\mu) < \Big(\frac{e^\delta}{(1+\delta)^{1+\delta}}\Big)^\mu, \delta > 0$$

$$P_r(X \geq (1+\delta)\mu) \leq e^{-\delta^2/3}, 0 < \delta \leq 1$$

$$P_r(X \geq (1+\delta)\mu) < e^{\frac{-\delta\mu}{3}}, \delta \geq 1$$

Proof:

$$P_r(X \geq (1+\delta)\mu) = P_r(e^{tX} \geq e^{t(1+\delta)\mu}), t > 0$$

Using Markov's Inequality ,$P_r(e^{tX} \geq e^{t(1+\delta)\mu} \leq \frac{E[e^{tX}]}{e^{t(1+\delta)\mu}}$

$$\leq \frac{E[e^{t\Sigma X_i}]}{e^{t(1+\delta)\mu}} = \frac{E[e^{tX_1}.e^{tX_2}...e^{tX_n}]}{e^{t(1+\delta)\mu}} = \frac{\prod_{i=1}^n E[e^{tX_i}]}{e^{t(1+\delta)\mu}}, X_i\text{'s are independent}$$

$$E[e^{tX_i}] = p_i e^t + (1-p_i) = 1 + p_i(e^t - 1) \leq e^{p_i(e^t-1)}$$

$$\frac{\prod_{i=1}^n E[e^{tX_i}]}{e^{t(1+\delta)\mu}} \leq \frac{\prod_{i=1}^n e^{p_i(e^t-1)}}{e^{t(1+\delta)\mu}} = \frac{e^{\sum_{i=1}^n p_i(e^t-1)}}{e^{t(1+\delta)\mu}} = \frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}}, (\mu = \sum_{i=1}^n p_i)$$

$$\frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}} = \Big(\frac{e^\delta}{(1+\delta)^{1+\delta}}\Big)^\mu \text{,As } t = ln(1+\delta) > 0 \text{ proving}$$

$$P_r(X \geq (1+\delta)\mu) \leq \Big(\frac{e^\delta}{(1+\delta)^{1+\delta}}\Big)^\mu, \delta > 0$$

To prove $\Big(\frac{e^\delta}{(1+\delta)^{1+\delta}}\Big)^\mu \leq e^{-\mu\delta^2/3}, 0 < \delta \leq 1$
Taking log on both sides,We obtain an equivalent condition

$$f(\delta) = \delta - (1+\delta)\ln(1+\delta) + \frac{(\delta)^2}{3} \leq 0$$

$$f'(\delta) = 1 - \frac{1+\delta}{1+\delta} - \ln(1+\delta) + \frac{2}{3}\delta = -\ln(1+\delta) + \frac{2}{3}\delta$$

$$f''(\delta) = -\frac{1}{1+\delta} + \frac{2}{3}$$

We see that $f''(\delta) < 0$ for $0 \leq \delta < 1/2$ and that $f''(\delta) > 0$ for $\delta > 1/2$. Hence $f'(\delta)$ first decreases and then increases over the interval [0,1]. Since $f'(0) = 0$ and $f'(1) < 0$, we can conclude that $f'(\delta) \leq 0$ in the interval [0, 1]. Since $f(0) = 0$. it follows that $f(\delta) \leq 0$ in that interval proving

$$P_r(X \geq (1+\delta)\mu) \leq e^{-\delta^2/3}, 0 < \delta \leq 1$$

For $\delta \geq 1$, $\ln\left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu = \mu(\delta - (1+\delta)\ln 1 + \delta)$

$\ln 1 + \delta > \frac{2\delta}{2+\delta}$ (Using derivative test for $\delta > 1$)

$\mu(\delta - (1+\delta)\ln 1 + \delta) \leq \mu\left(\frac{-\delta^2}{2+\delta}\right) \leq \mu\left(\frac{-\delta^2}{2\delta+\delta}\right) = \frac{-\delta\mu}{3}$

$$P_r(X \geq (1+\delta)\mu) < e^{\frac{-\delta\mu}{3}}$$

Markov's Inequality

If X is a Discrete Random Variable that takes only non-negative value,then

$$P(X \geq a) \leq \frac{E[X]}{a}$$

Proof:

$E[X] = \sum xf(x) = \sum_{x \geq a} xf(x) + \sum_{x<a} xf(x) \geq \sum_{x \geq a} xf(x) \geq \sum_{x \geq a} af(x) \Rightarrow \frac{E[X]}{a} \geq \sum_{x \geq a} f(x)$

Hence $P(X \geq a) \leq \frac{E[X]}{a}$