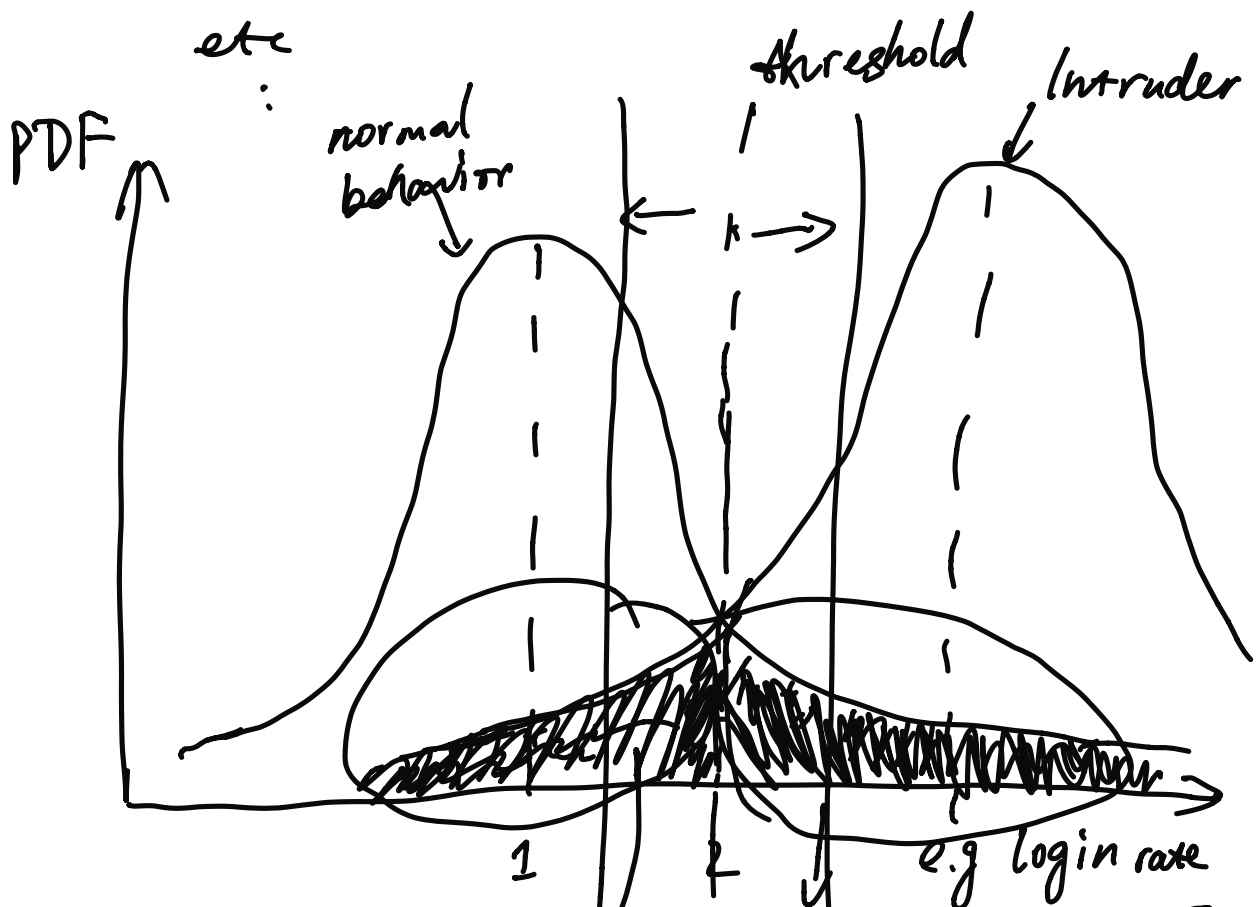


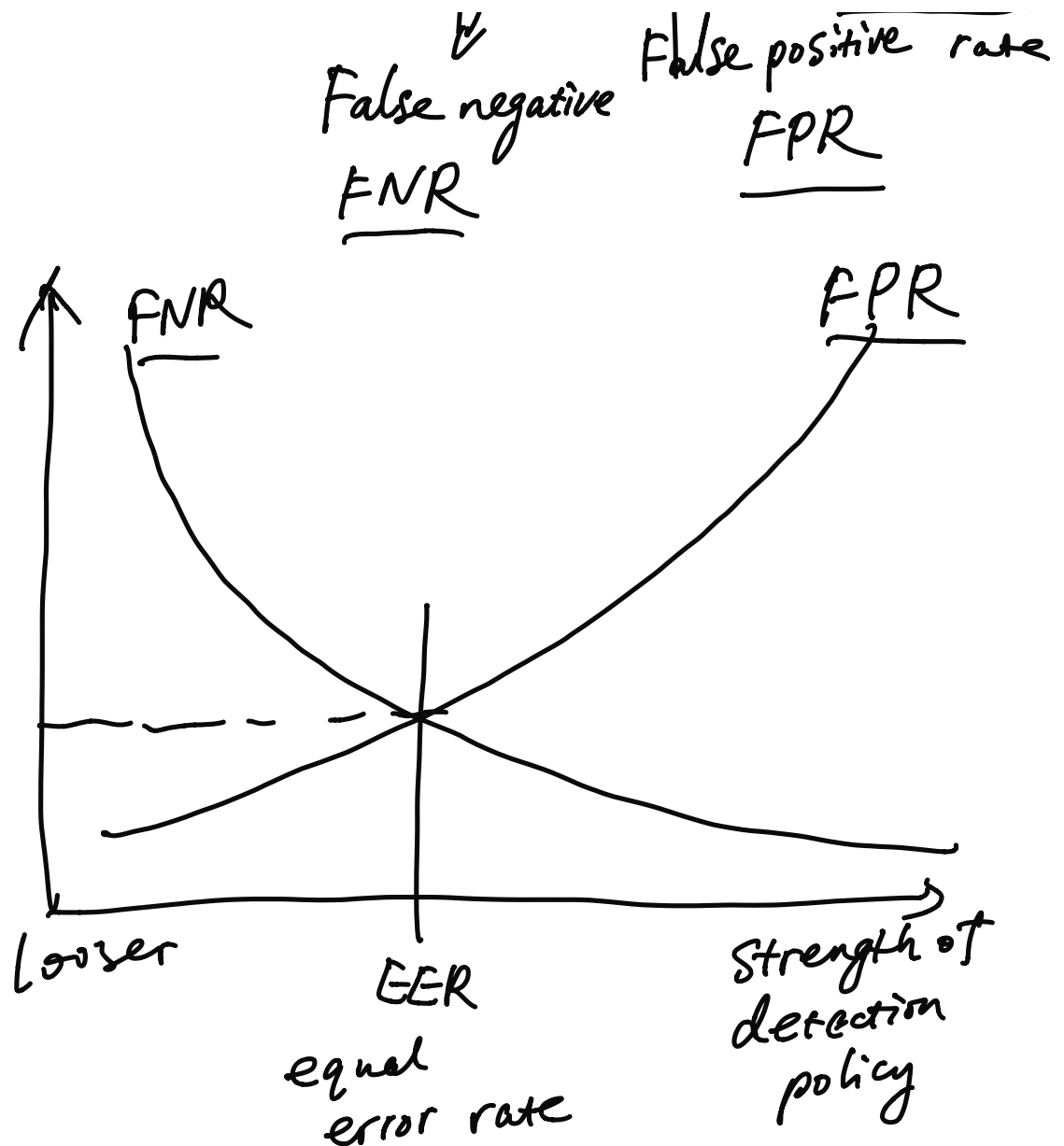
ECE 471/571

IDS

## Examples of Intrusion

- Compromise a server
- guessing or cracking pswd.
- Install a malware
- steal data (e.g. credit card.  
password)
- web server defacing.





D — disease

P — test is positive

ND — no disease

N — test is negative

$$\Pr[ND|P] = \frac{\Pr[P, ND]}{\Pr[P] \rightarrow \text{base}}$$

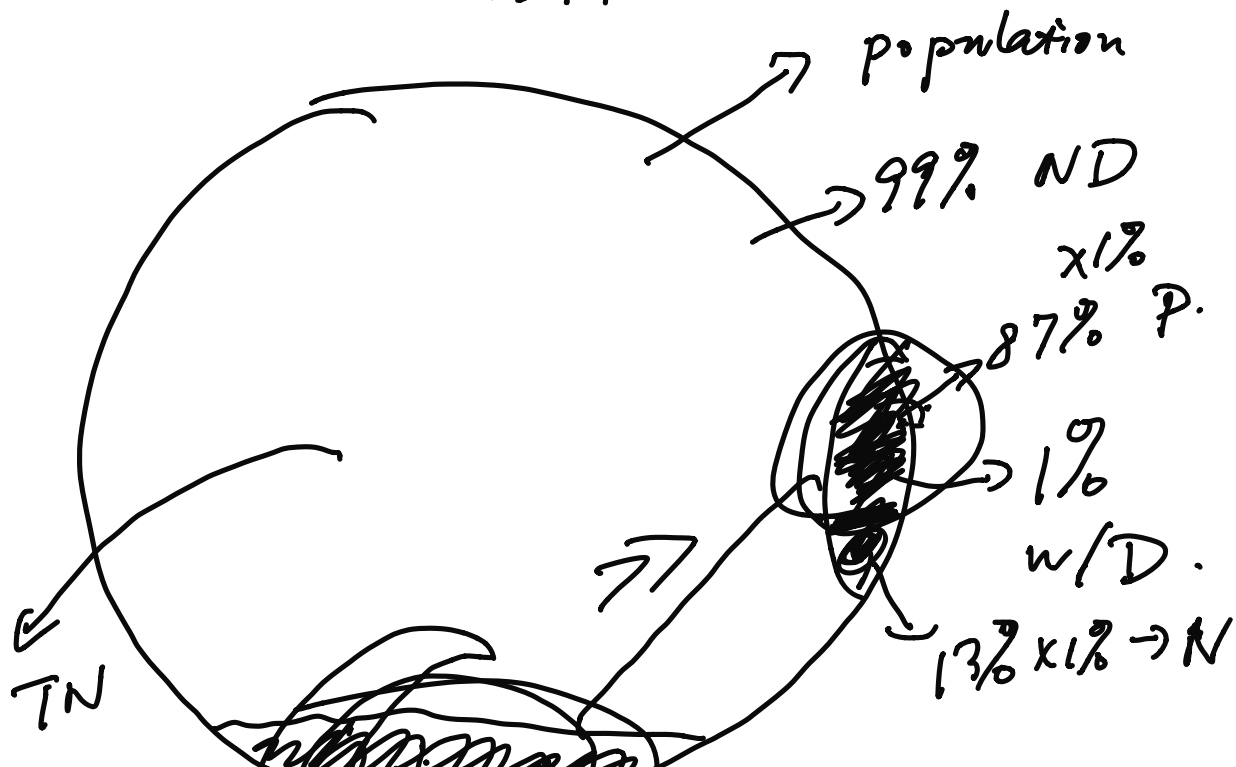
$$\Pr[P | ND] = \text{FPR} = 13\%$$

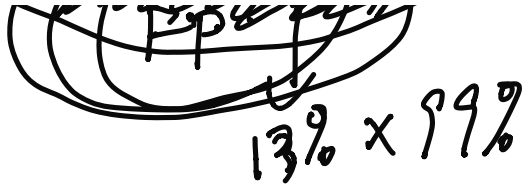
rate

$$= \frac{\Pr[P | ND] \cdot \Pr[ND]}{\Pr[D] \cdot \Pr[P | D] + \Pr[ND] \cdot \Pr[P | ND]}$$

$$= \frac{0.13 \times (1 - 0.01)}{0.01 \cdot 0.87 + 0.99 \cdot 0.13}$$

$$\approx \frac{0.13}{0.1374} = 93.7\%$$





$$13\% \times 99\%$$

Base rate fallacy.

if 0.1% FP for IDS

99.9% is accurate

if 1% traffic is malicious

$\Rightarrow$  9%

0.0001 traffic is malicious

91%