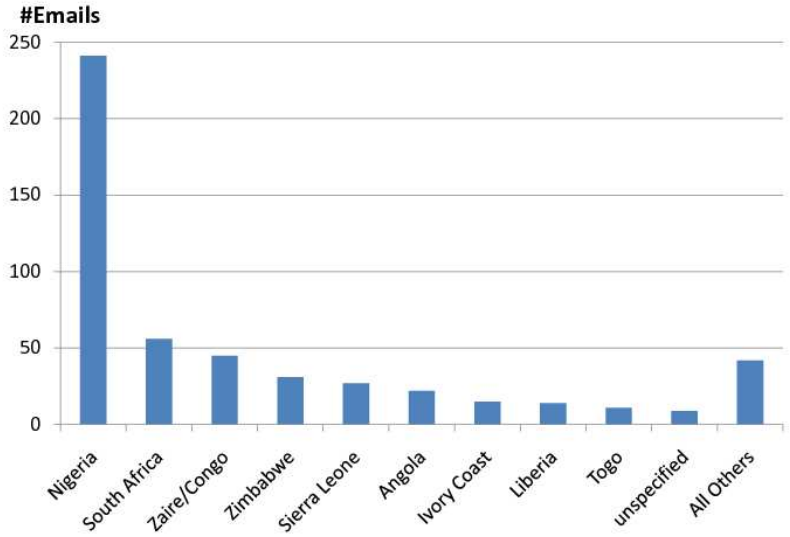
Why Do Nigerian Scammers Say They Are From Nigeria?

Cormac Herley

Microsoft Research, Redmond

Nigerian Emails:
Who falls for these things?

- What's with the spelling mistakes, BLOCK CAPS?
- Why not Sweden, or Bolivia or New Jersey?
- Who hasn't heard of Nigerian Scam?



How does esconomic opportunity change as a function of victim density?

- Population with density d viable victims

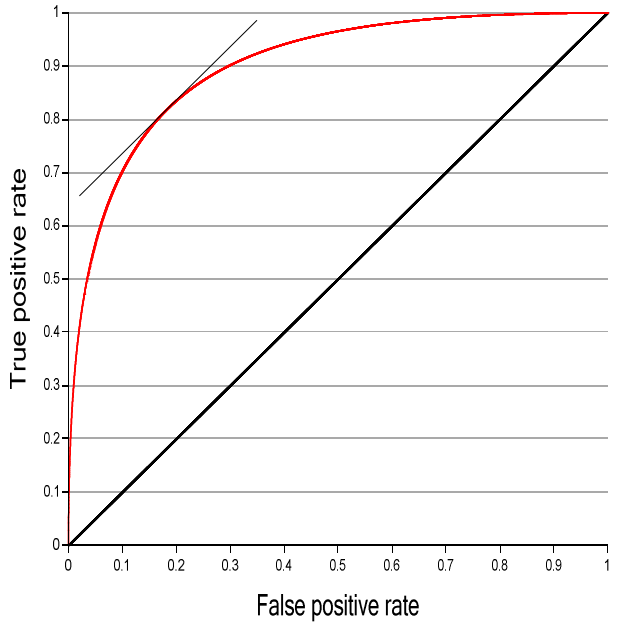
Opportunity = d G N

- What if we reduce density by 2x?
  - Does opportunity fall 2x, > 2x, < 2x?

- ***Opportunity drops much faster than density***

Attackers have False Positives too

	Attack	Don't Attack
Viable	TP	FN
Non-viable	FP	TN



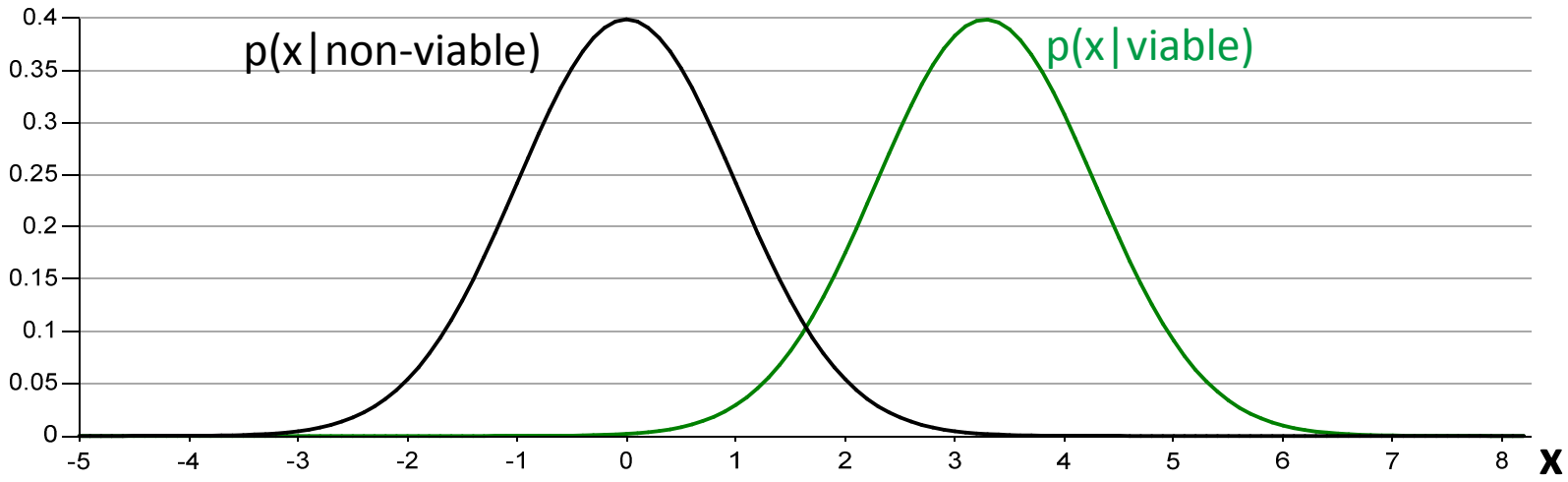
Expected Return:

$$E\{R\} = d\ t_p\ G\ N - (1-d)\ f_p\ C\ N$$

d = victim density
N = population
t_p = true pos. rate
f_p = false pos. rate
G = net gain (success)
C = Cost (fail)

Viability is not observable

- Encapsulate all *observable* info about viability in x



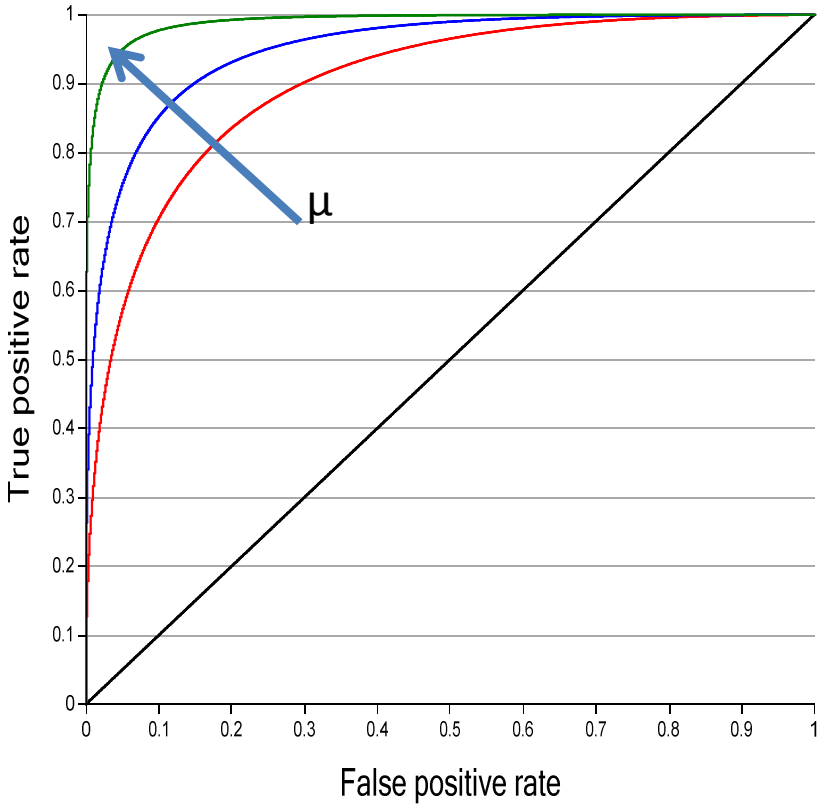
- Model:
  - p(x|non-viable) ~ N(0,1)
  - p(x|viable) ~ N(μ,1)

- ***Rich does not mean viable!***

ROC Curves:
true positives vs. false positives

- Increasing μ gives better detection

1. Curve is monotonic
2. Slope decreases monotonically
3. Area Under Curve (AUC) = Prob. viable ranked higher than non-viable



AUC = 0.99
AUC = 0.95
AUC = 0.9

Optimal Operating Point (OOP)

Expected Return:

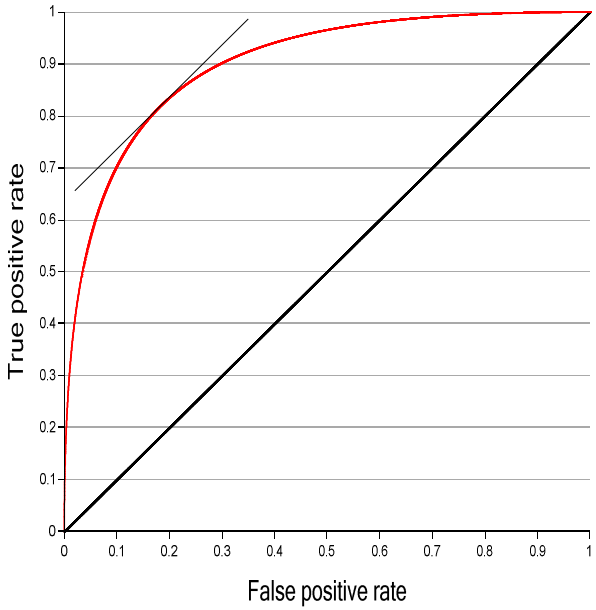
$$E\{R\} = d\, t_p\, G\, N - (1-d)\, f_p\, C\, N$$

Maximize E{R}:

$$\frac{dt_p}{df_p} = \frac{1-d}{d}\,\frac{C}{G}$$

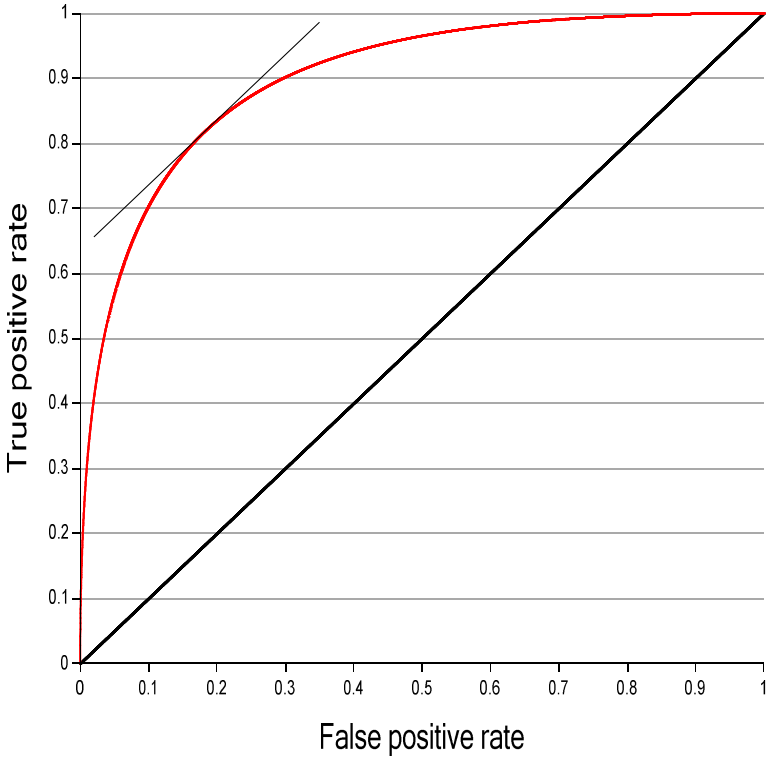
Slope at OOP:

- Inversely proportional to d
- Inversely proportional to G/C

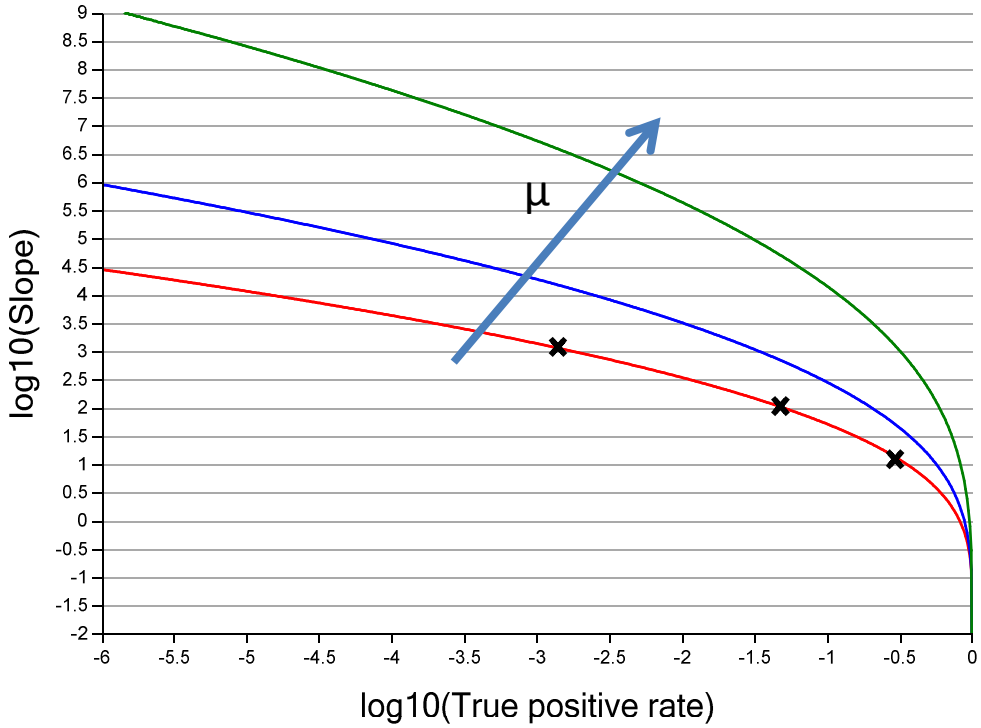


Consequences

- ***As d→0 slope at OOP increases***
  - Slope at OOP: $\frac{dt_p}{df_p} = \frac{1-d}{d}\frac{C}{G}$
- ***As slope increases fewer attacked***
  - Viable users attacked = d t_p N
  - Non-viable attacked = (1-d) f_p N
- ***Opportunities with lower densities harder to exploit***



Slope vs t_p



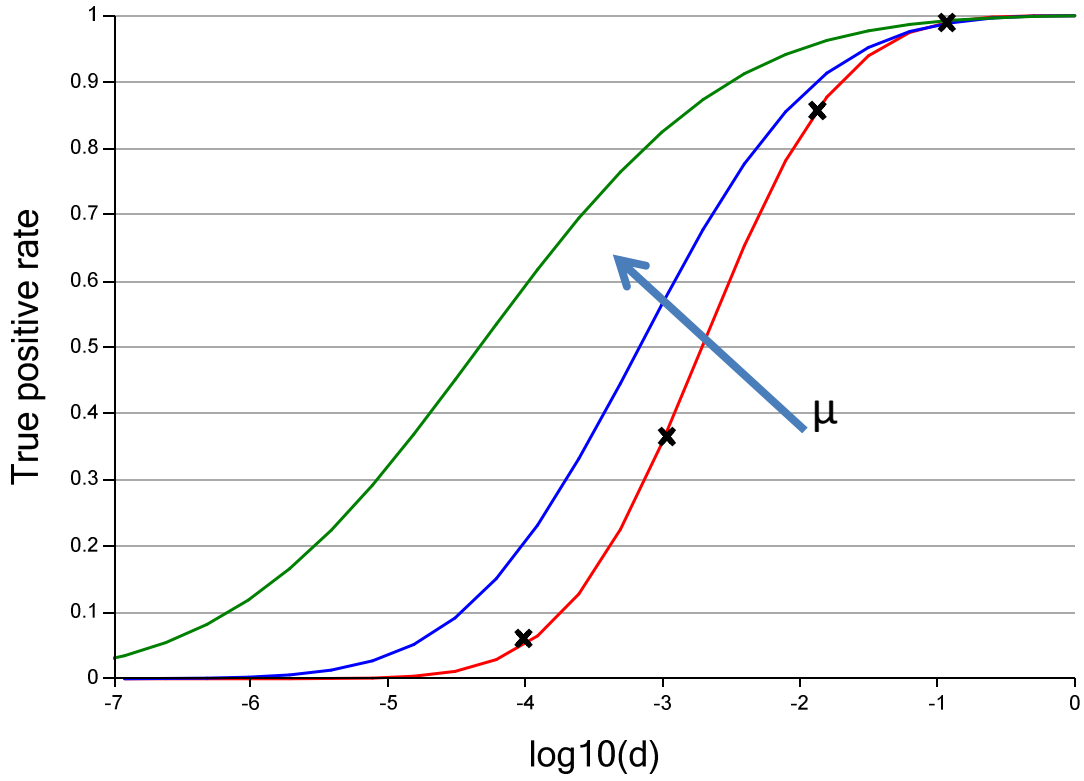
Example slope of:

- 10 => $t_p = 0.36$
- 100 => $t_p = 0.05$
- 1000 => $t_p = 0.0019$

True Positive rate vs victim density
t_p vs. d (at G/C = 100)

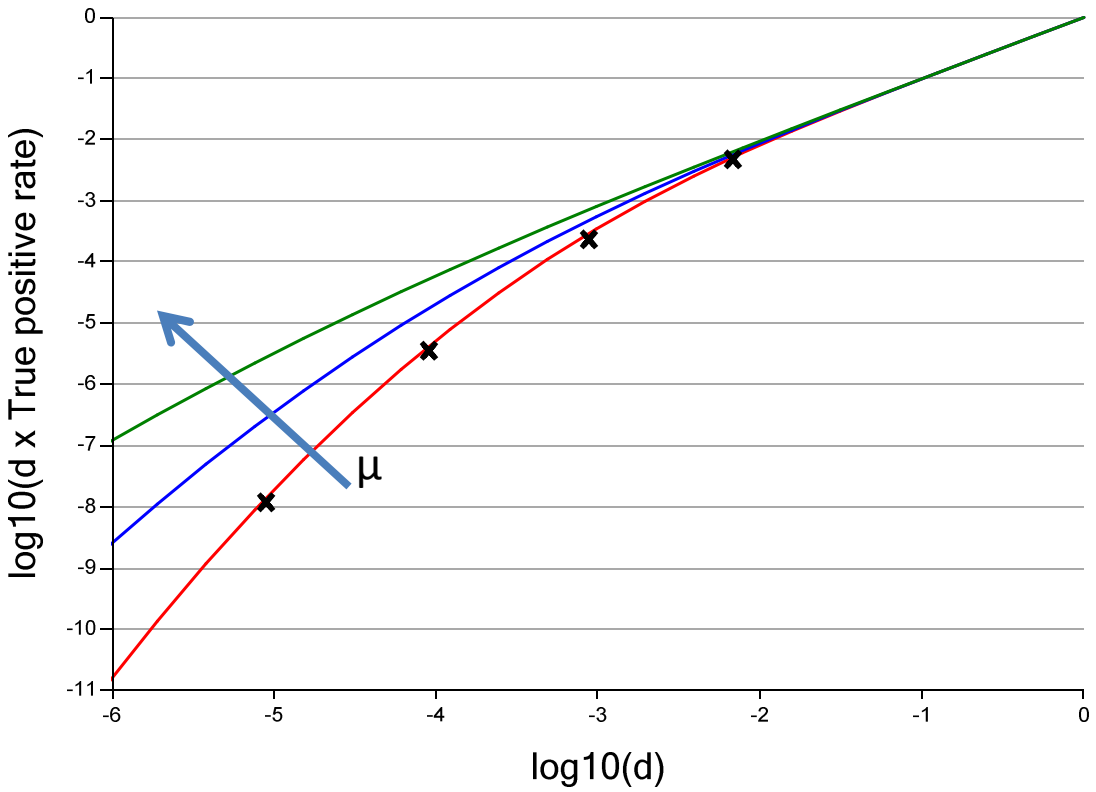
If fix G/C can plot t_p vs d

$$\frac{dt_p}{df_p} = \frac{1-d}{d}\,\frac{C}{G}$$



- ***True positive rate falls fast with density***

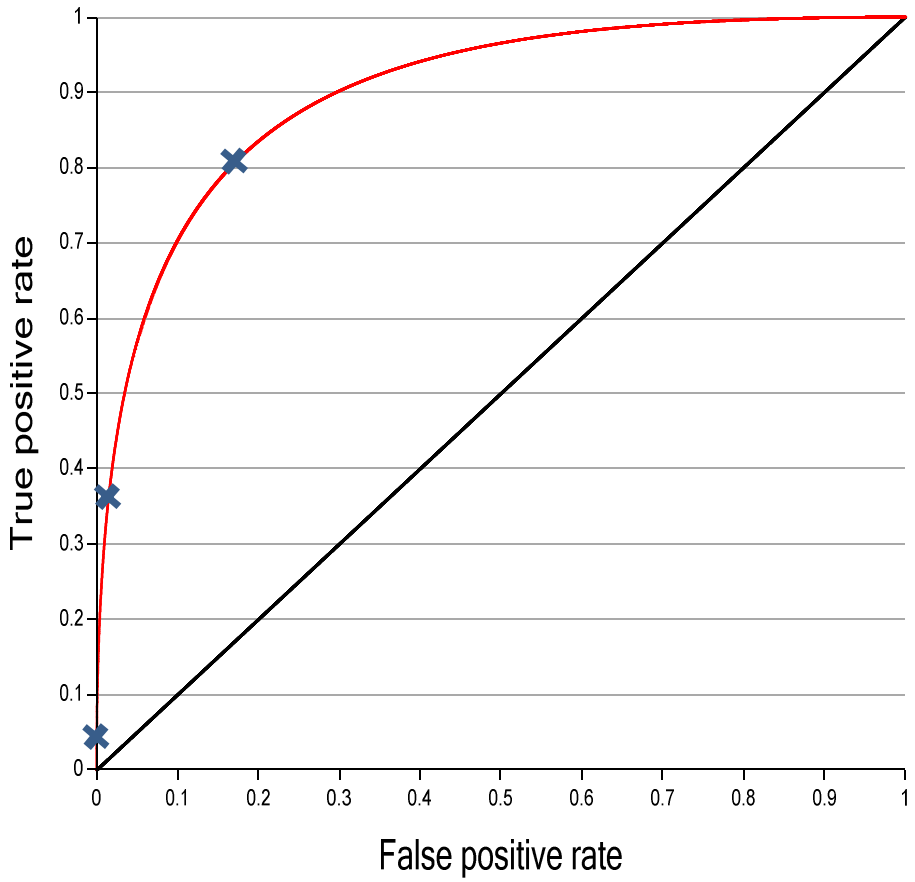
Victims found vs density (G/C=100)



- **Victims found falls *much* faster than density**
  - $d = 10^{-5}$ gives $d\ t_p = 10^{-8}$
  - E.g. Population 200 million, 2000 viable, 2 profitably victimized

Diversity is more important than strength

- Suppose d, G/C s.t. slope = 1
  - $t_p = 0.82$, $f_p = 0.18$
- Now divide into 10 attacks with density d/10
  - $t_p = 0.36$, $f_p = 0.015$
- Thus, no change in #viable targets, or G/C
  - Viable users attacked drops 2x

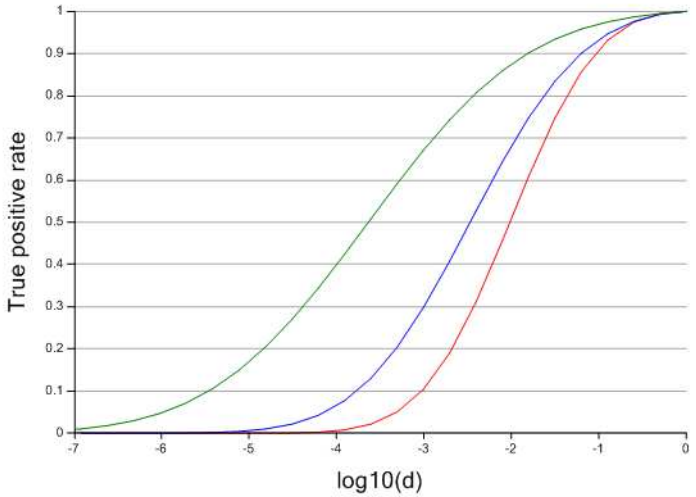


Everyone vulnerable, no-one attacked?

- Divide population into Q attacks each with d/Q
- Viable victims attacked:

$$\frac{d}{Q}\sum_{k=1}^{Q} t_p(^{d}/_{Q})\ \mathrm{N} = d\ t_p(^{d}/_{Q})\ \mathrm{N}$$

- $t_p(d/Q) \rightarrow 0$
- d=1 (everyone vulnerable)
- Q large (no-one attacked)

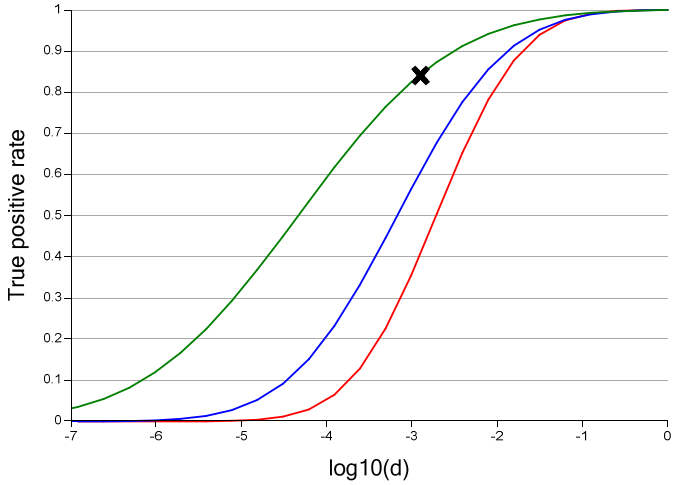


Optimism does not pay

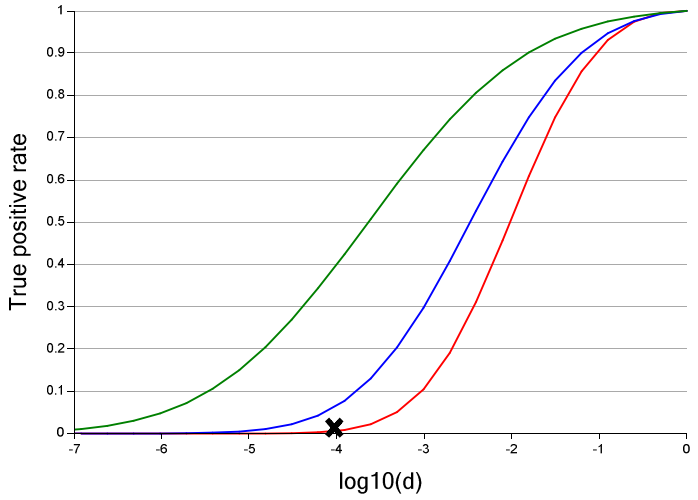
- Attacker thinks:
  - $d = 10^{-3}$
  - G/C = 100
  - AUC = 0.99

- But attacker gets:
  - $d = 10^{-4}$
  - G/C = 20
  - AUC = 0.9

G/C = 100



G/C = 20



Factor difference:

$$\frac{10^{-3} \times 0.826 \times 100}{10^{-4} \times 0.006 \times 20} = 6883$$

Three factors affect return

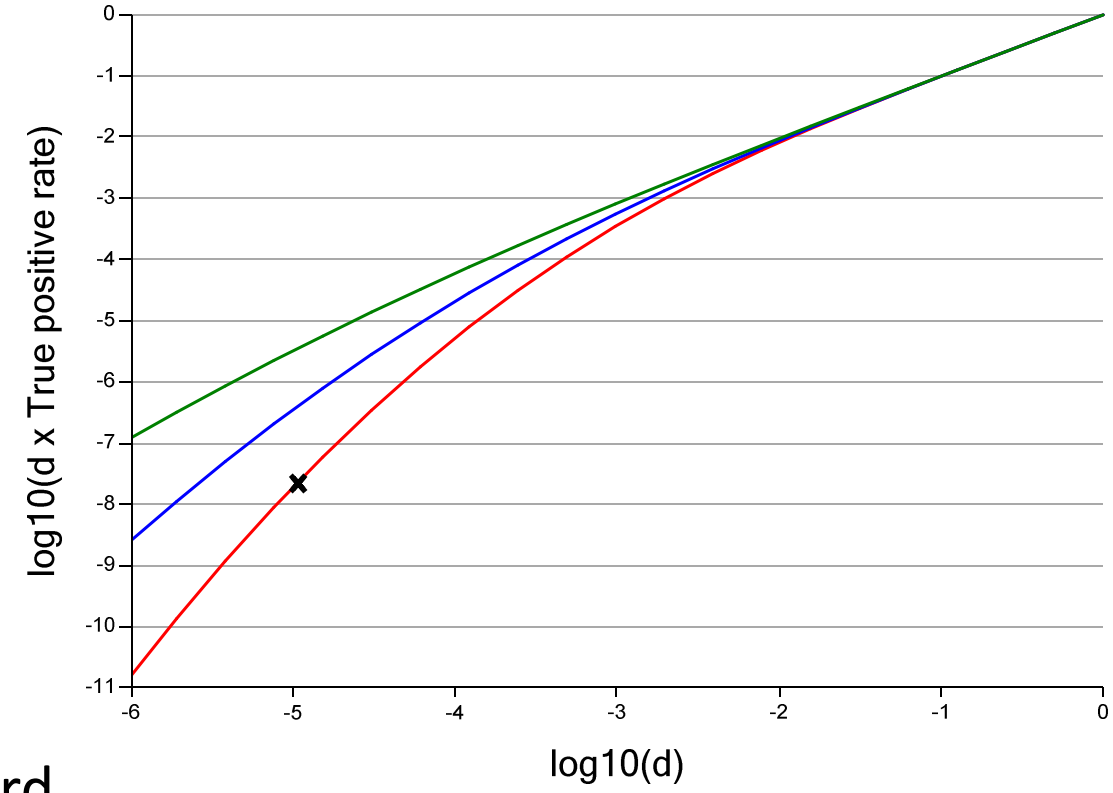
- ***Density d***
- ***Profitability G/C***
- ***Ability to detect (i.e. ROC curve)***

How about G/C = “A Gazillion”?

- At OOP return is like (G/C+1) sided coin
  - Gain G with prob C/G
  - Otherwise lose C
- Variance ≈ Mean
- Suppose G/C = 1000
  - binocdf(0,1000,0.001) = 36.8% chance no victim after 1000 attacks.
- Keynesian attacker is more conservative
  - Slope = $\frac{1-d}{d}\frac{1}{k_{max}}$
  - where k_{max} = max avg between hits

How about Classifier Accuracy = 99.999%

- How did you get to be so good?
- How learn to distinguish viable from non- when viable are so rare?
- Need many samples of each for training
- Iterative improvement hard

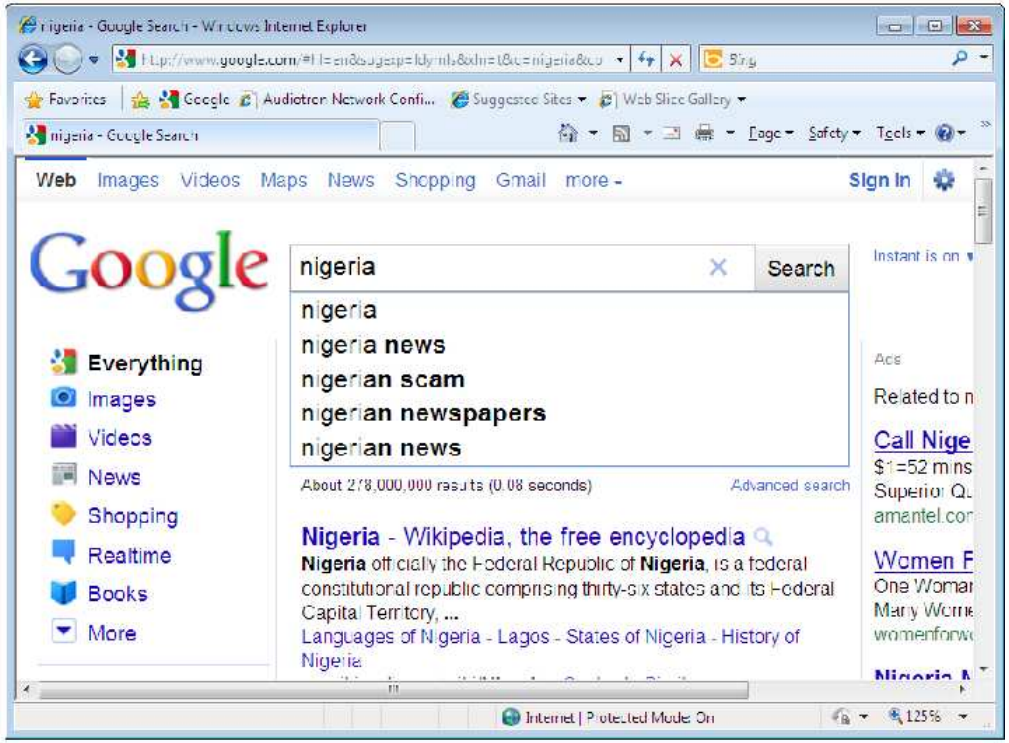


Catch-22 at low densities

- **Need to find them to learn how they can be found**
  - Must distinguish viable from non-viable with great accuracy
  - Need many viable samples to learn to distinguish.

Nigerian Emails:
Who falls for these things?

- Who hasn't heard of Nigerian Scam?



- ***Ideally: attack only those who haven't heard of it.***

Why do Nigerian Scammers say they are from Nigeria?

- ***Initial email has cost ≈ 0 per user***
- ***Follow-up has cost > 0***
  - ***Detector = wording of initial email***

- ***When d is low***
  - ***Only small fraction of vulnerable can be found***
  - ***Repelling FP's more important than finding TP's***

Conclusions

- ***Economic Opportunity falls far faster than victim density***

- ***Extreme difficulty for low density attacks***