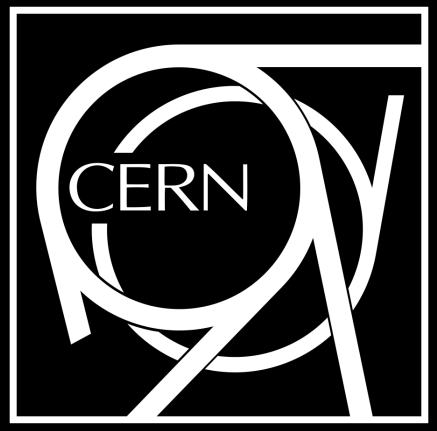
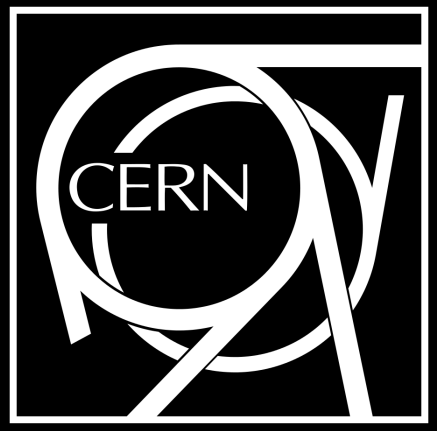
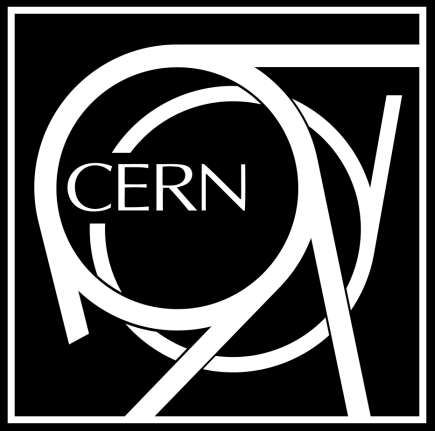


Are you hiding all you intended? Probably not.



WHO AM I?

BRANDON NIEMCZYK – HP DVLABS

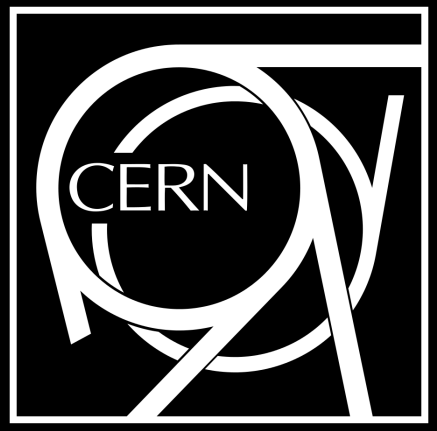


What I want you to think about.

How much do you depend on encryption?

How wide/narrow is the scope of protection provided?

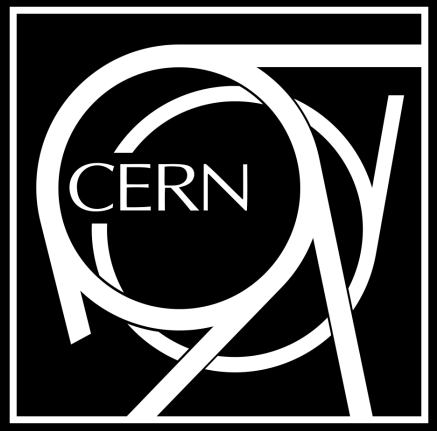
Do you account for this?



An example that may defy your expectations.

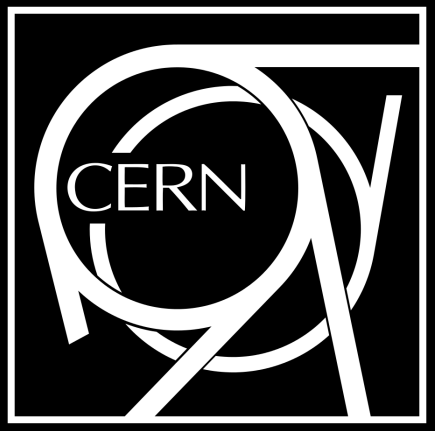
PACUMEN

“packet acumen”

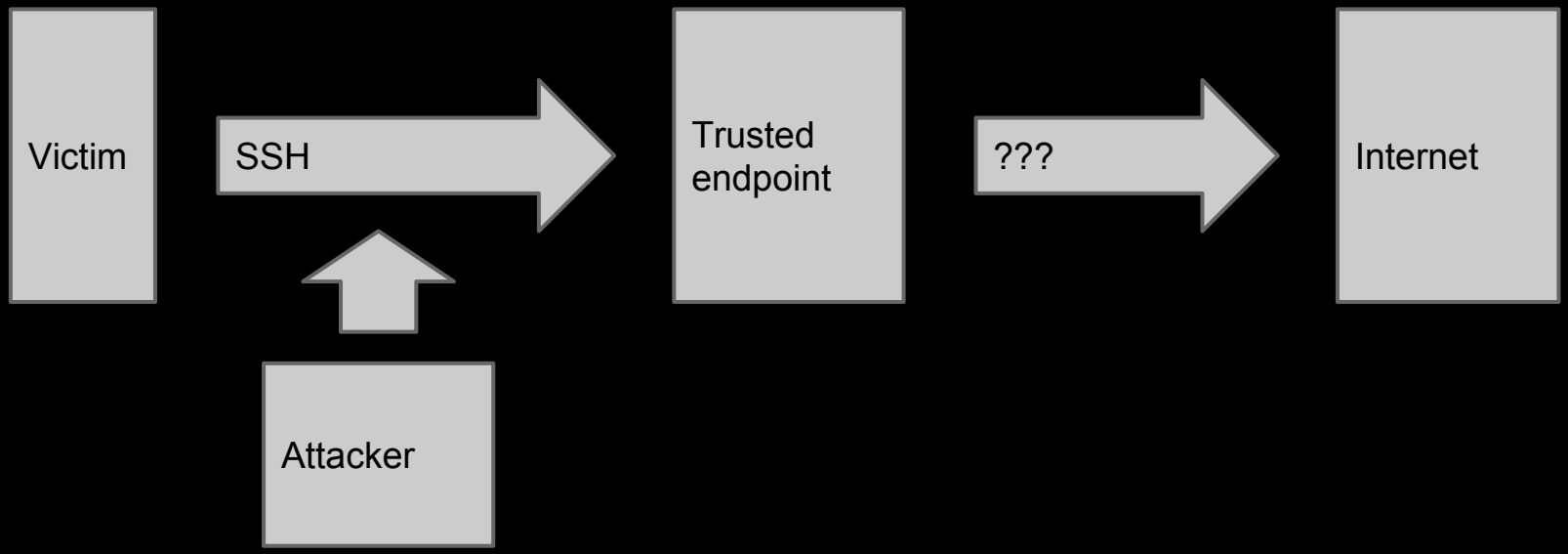


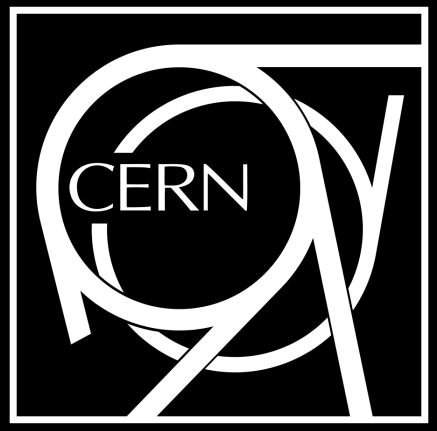
We all know encrypting our data is good right?

Of course, that only hides what we are saying, not who we talk to.

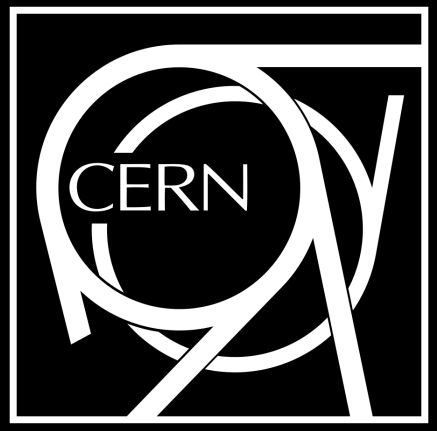


So just tunnel everything through an encyrypted connection, like an SSH session.



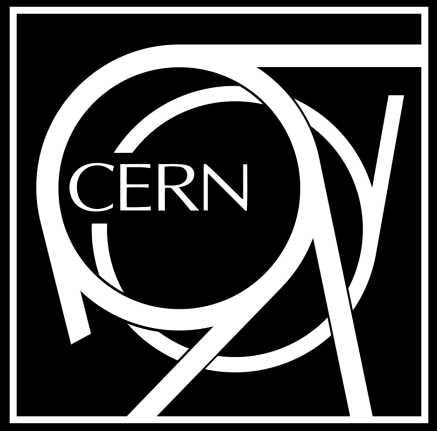


Can the attacker infer anything using data mining techniques?



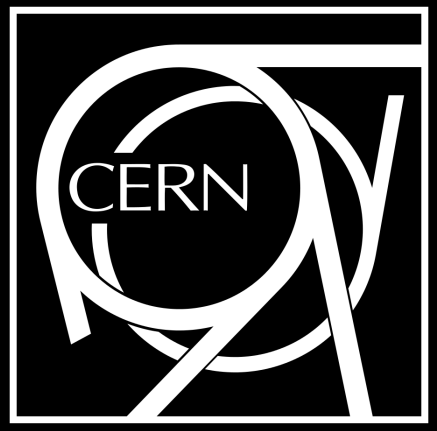
WHAT IS PACUMEN ?

A tool to identify what applications are being used over an encrypted tunnel.



ACADEMIA HAS PRODUCED PAPERS…

Where’s the code?

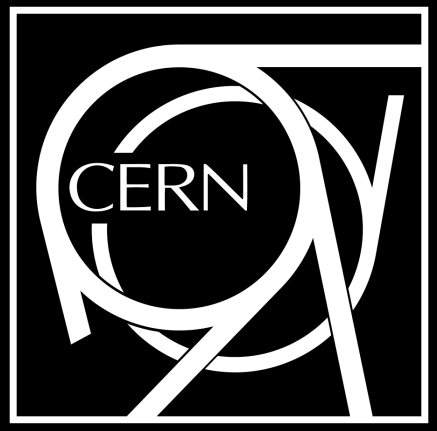


PREVIOUS WORK

Focus on one application at a time.

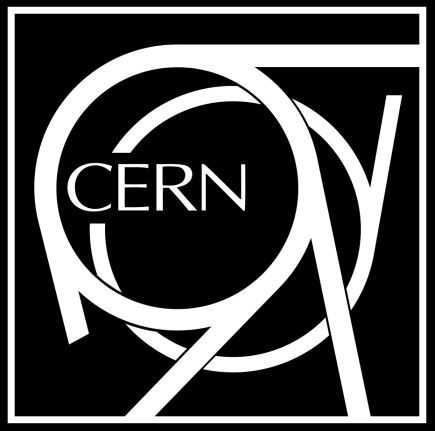
Results only.

Results are difficult to interpret.



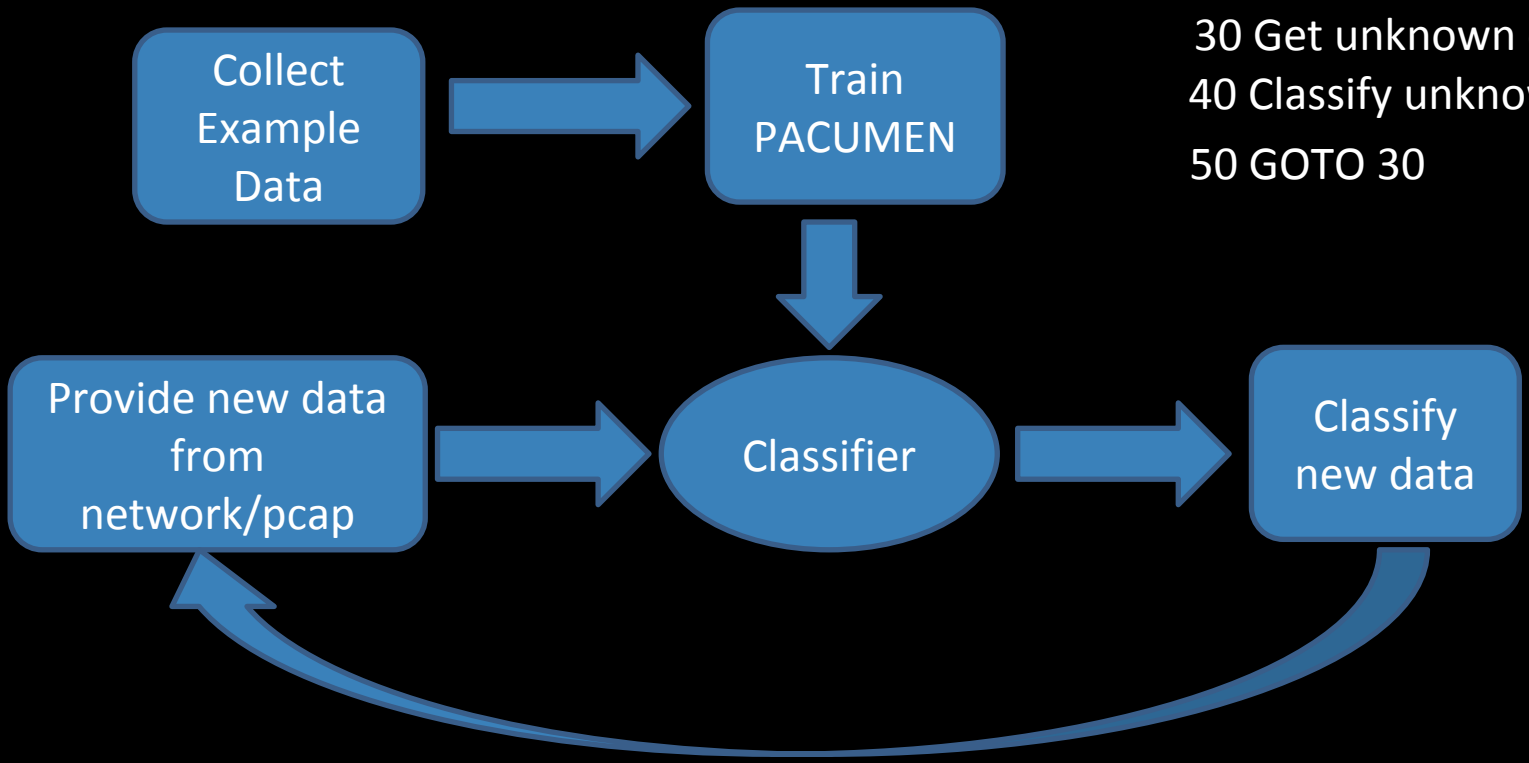
HOW DOES PACUMEN WORK?

PACUMEN learns by example.

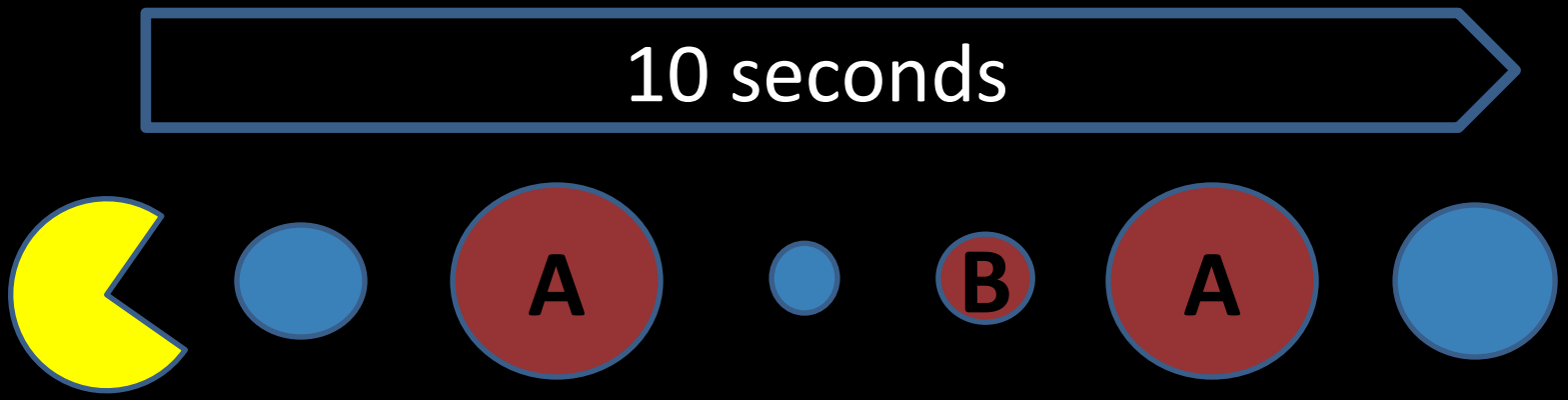


HOW DOES PACUMEN WORK?

10 Collect Training Data
20 Build Classifier
30 Get unknown data
40 Classify unknown data
50 GOTO 30



HOW DOES PACUMEN WORK?



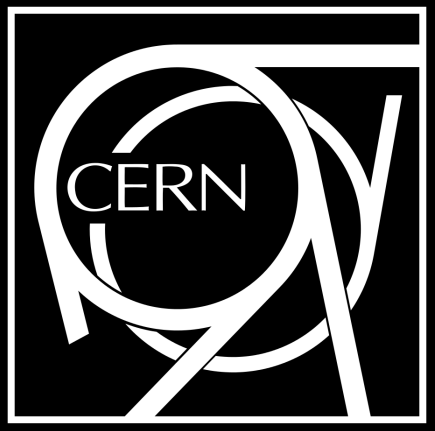
SIZE A 1 2

SIZE B 1

CLASSIFY

UPDATE CONFIDENCE

IRRELEVANT SIZE 1 2 3

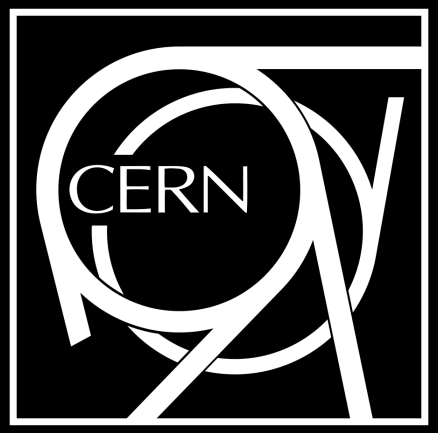


HOW DOES PACUMEN WORK?

Multiple types of classifiers can be created.

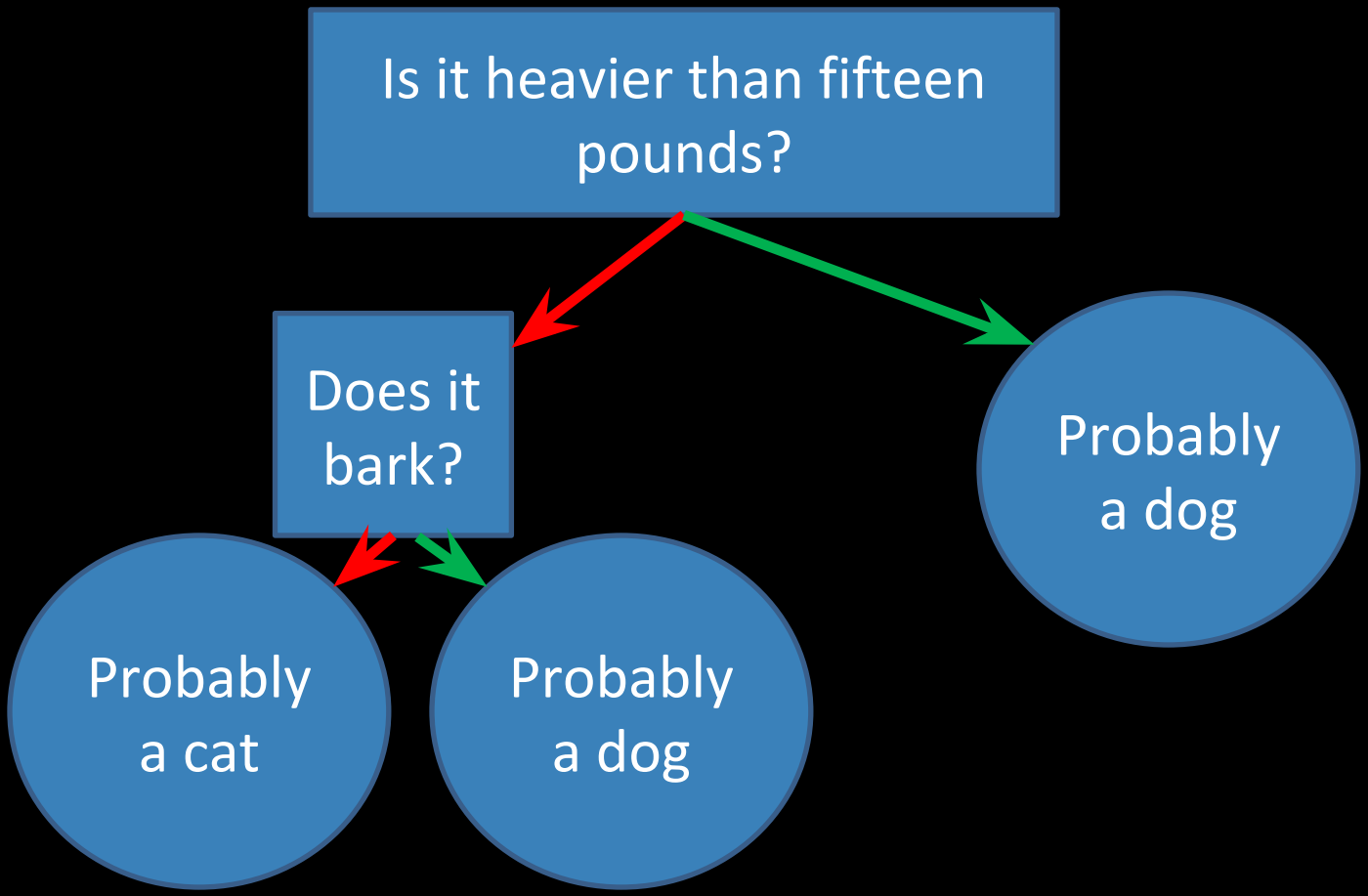
- Decision Trees

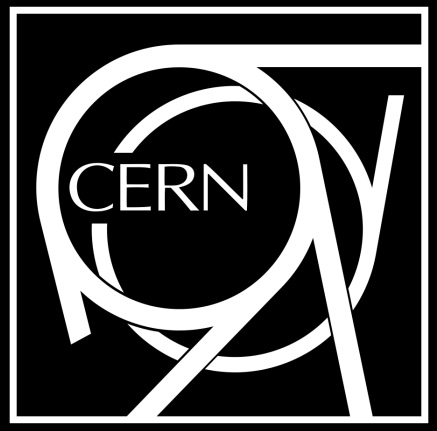
- Mixed Gaussian Likelihood functions



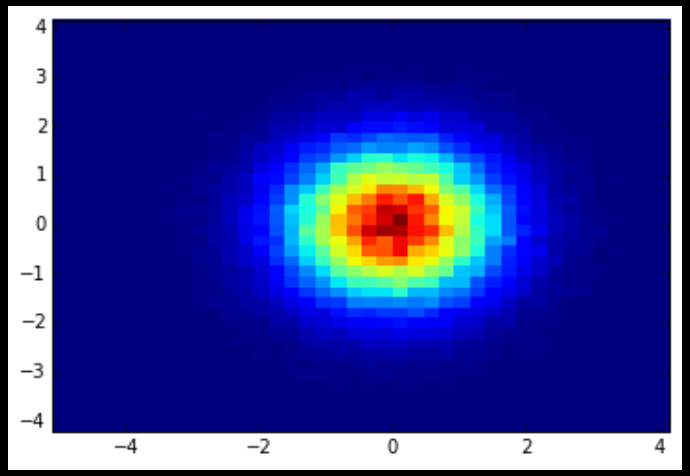
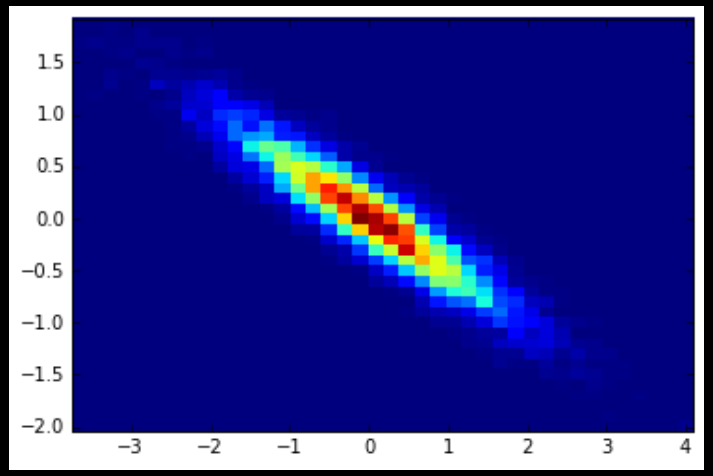
DECISION TREES

Is it a dog or a house cat?

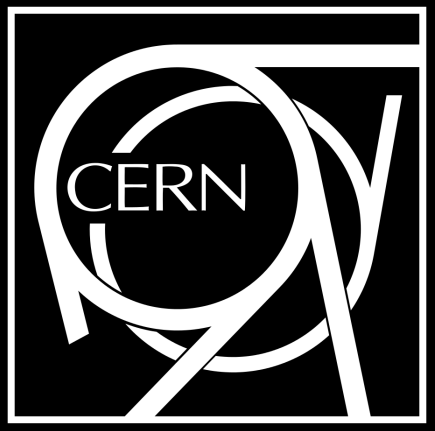




MIXED GAUSSIANS

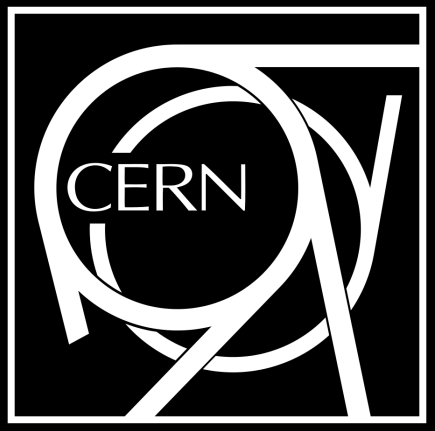
M  = 

$$L = e^{-\frac{1}{2}\ln(|\Sigma|)-\frac{1}{2}(\mathbf{x}-\mu)^T\Sigma^{-1}(\mathbf{x}-\mu)-\frac{k}{2}\ln(2\pi)}$$



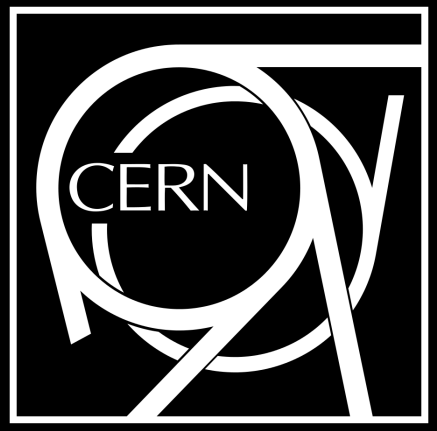
What is the impact on privacy?

- Not only social media data can be mined
- Data that seems far more obfuscated can be just as revealing.



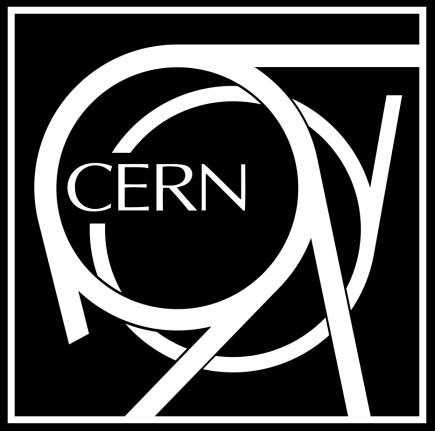
Does it get even worse?

- Implementation bugs can give away the keys to the kingdom - AKA HeartBleed
- Bad entropy pools in devices lead to factorable keys! - Lenstra et al.



I still trust encryption more than anything else

What about you?



THANK YOU
Any Questions?

PACUMEN - https://github.com/bniemczyk/pacumen.git

Brandon Niemczyk – insecurity@hp.com

Prasad Rao – prasad.rao@hp.com

Vib Chhabra – vaibhav.chhabra@hp.com