Resources
Applying Fuzzy
Phishing
The Fuzzy Process
History of Fuzzy
Intro

Fuzzy Logic Inferencing in Security Applications

Raymond Garcia, Ph.D.

Resources

Applying Fuzzy

Phishing

The Fuzzy Process

Intro to Problem & Solution

Intro

Describe

Problem and solution (Phishing & Fuzzy Logic)

Demonstrate

Apply Fuzzy to the web Web Phishing problem

Conclude

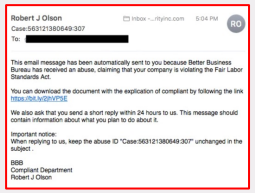
Discuss results, tools, and datasets

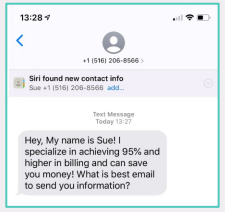
Smishing/Vishing

Smishing: Text or SMS,
Vishing: Voice->RDP

Angler Phishing

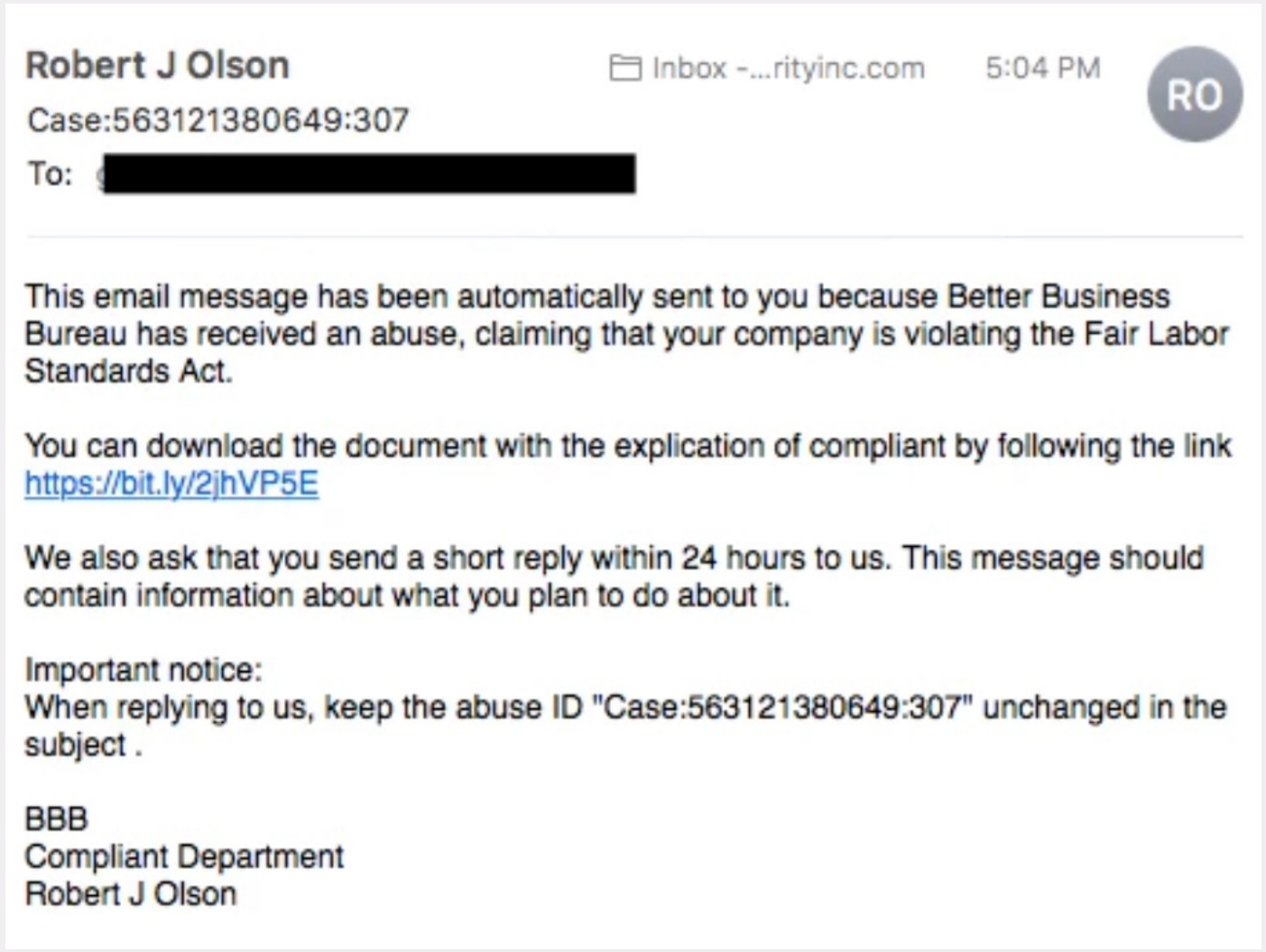
Hijacking responses inside social media





1. **Spear/Whaling**
   Targets a specific group (Spear: admins, etc., Whaling: C-Level)
2. *(Smishing/Vishing)*
3. **Email phishing**
   Email at-large and sextortion
4. *(Angler Phishing)*
5. **Search Engine**
   SEO Poisoning

*https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack



Robert J Olson Inbox -...rityinc.com 5:04 PM RO

Case:563121380649:307

To: [redacted]

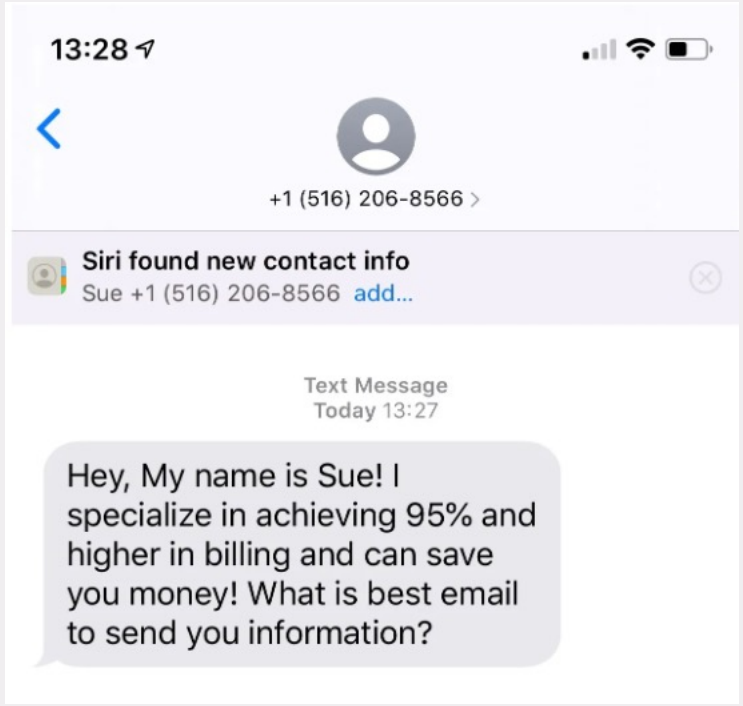
This email message has been automatically sent to you because Better Business Bureau has received an abuse, claiming that your company is violating the Fair Labor Standards Act.

You can download the document with the explication of compliant by following the link https://bit.ly/2jhVP5E

We also ask that you send a short reply within 24 hours to us. This message should contain information about what you plan to do about it.

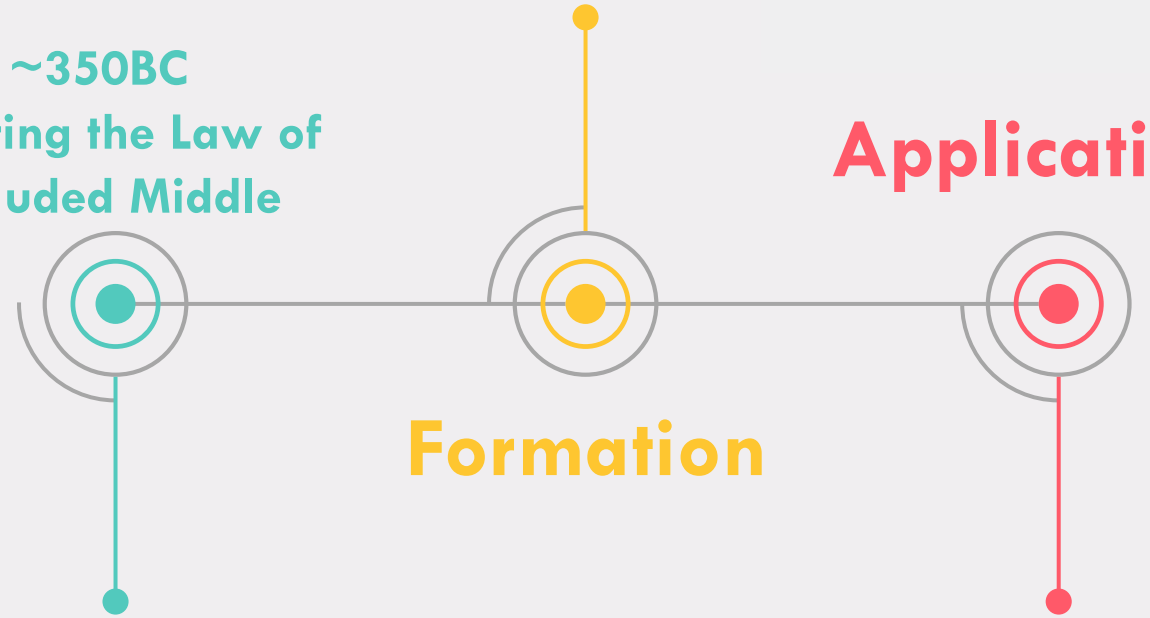
Important notice:
When replying to us, keep the abuse ID "Case:563121380649:307" unchanged in the subject .

BBB
Compliant Department
Robert J Olson


13:28
+1 (516) 206-8566
Siri found new contact info
Sue +1 (516) 206-8566 add...
Text Message
Today 13:27
Hey, My name is Sue! I specialize in achieving 95% and higher in billing and can save you money! What is best email to send you information?

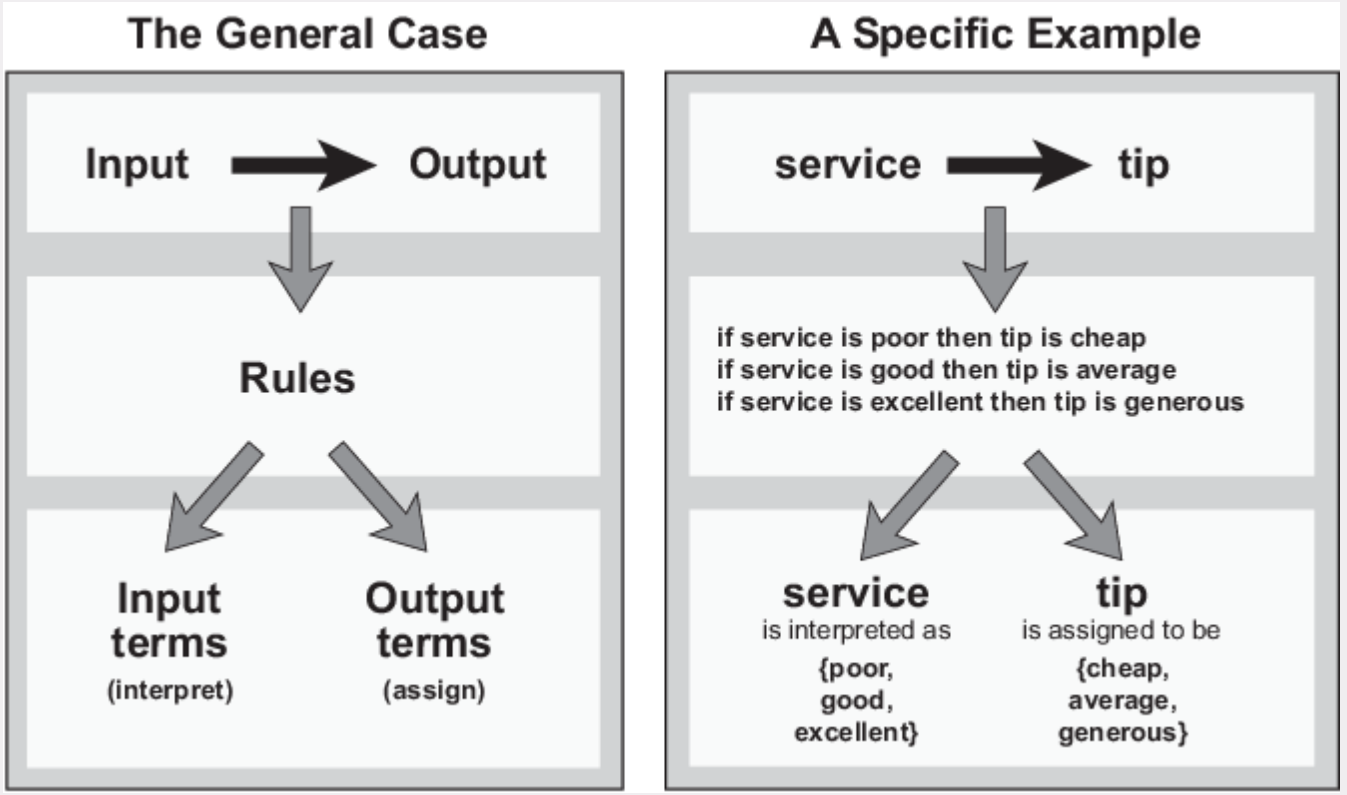

Stephanie @sreese25 22h
Finally here, cold as ice. Might as well have not brought it at all. Never ordering from @dominos again.
Domino's Pizza @dominos
@sreese25 Sounds like we dropped the ball and I'd like to help make this right! Can you pls follow/DM store info, your name, phone & email?
Hide conversation
4:38 PM - 28 Apr 12 via Radian6 · Details
Reply Retweet Favorite Buffer

1854- Boolean Algebra (George Boole)
1965- Fuzzy Logic (Lotfi Zadeh)

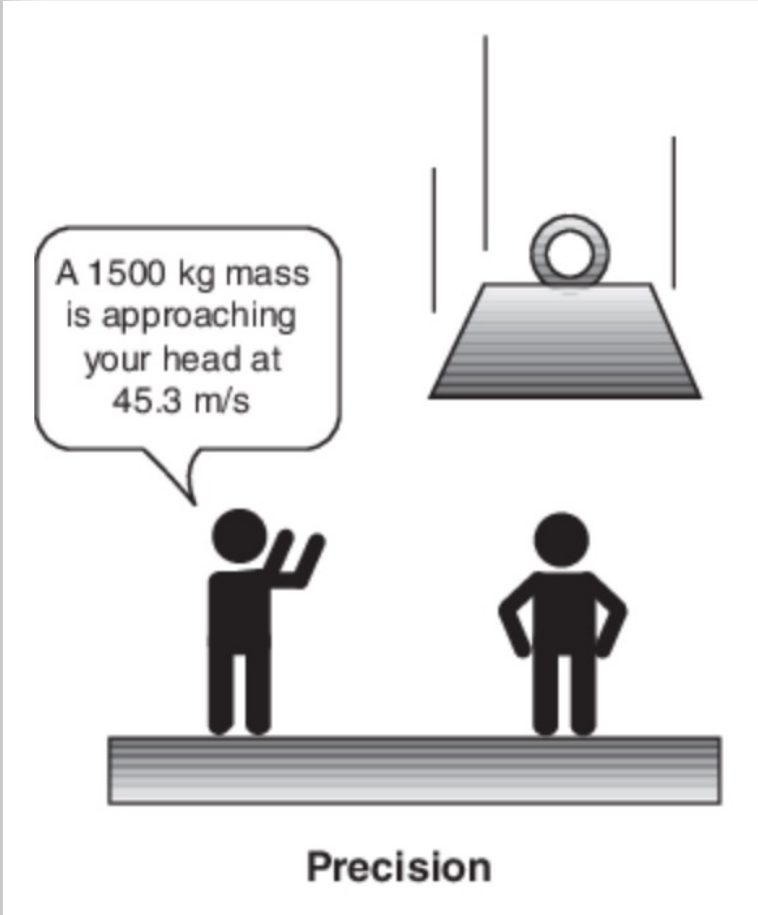


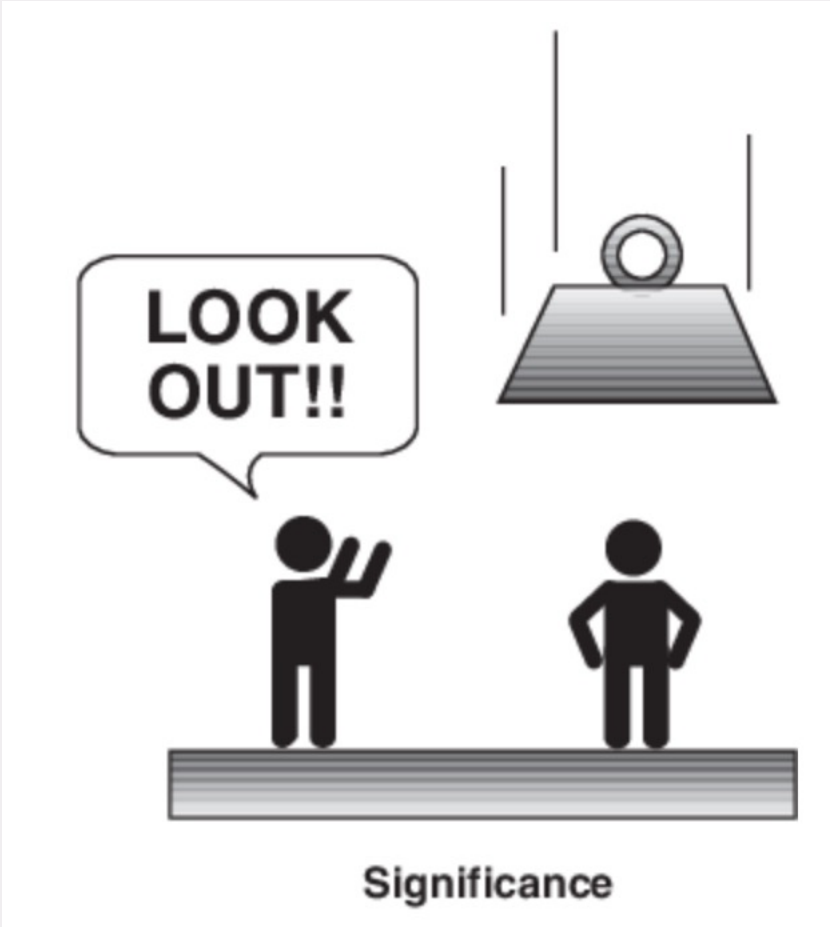
Either a proposition or its negation is true (Aristotle, 340BC),
Plato Rejected his pupil's notion

1990's – Risk, local monitoring, but mostly control,
2000's – Network Anomaly and Intrusion
2010's – Reputation, reliability, and trust,
2020's – Vehicular, iot, and resilience

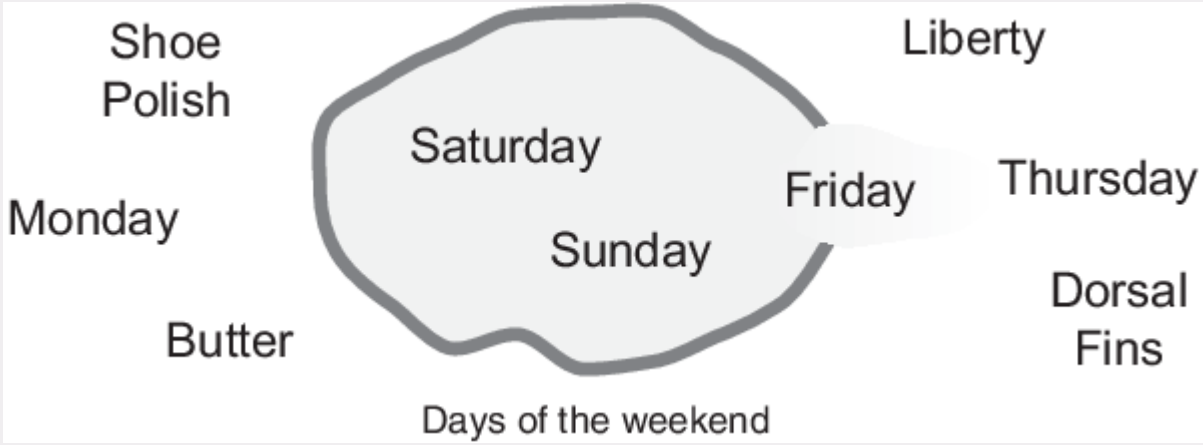

The General Case
Input
Output
Rules
Input terms
(interpret)
Output terms
(assign)
A Specific Example
service
tip
if service is poor then tip is cheap
if service is good then tip is average
if service is excellent then tip is generous
service
is interpreted as
{poor, good, excellent}
tip
is assigned to be
{cheap, average, generous}

Fuzzy logic is all about the relative importance of precision:
How important is it to be exactly right when a rough answer will do?

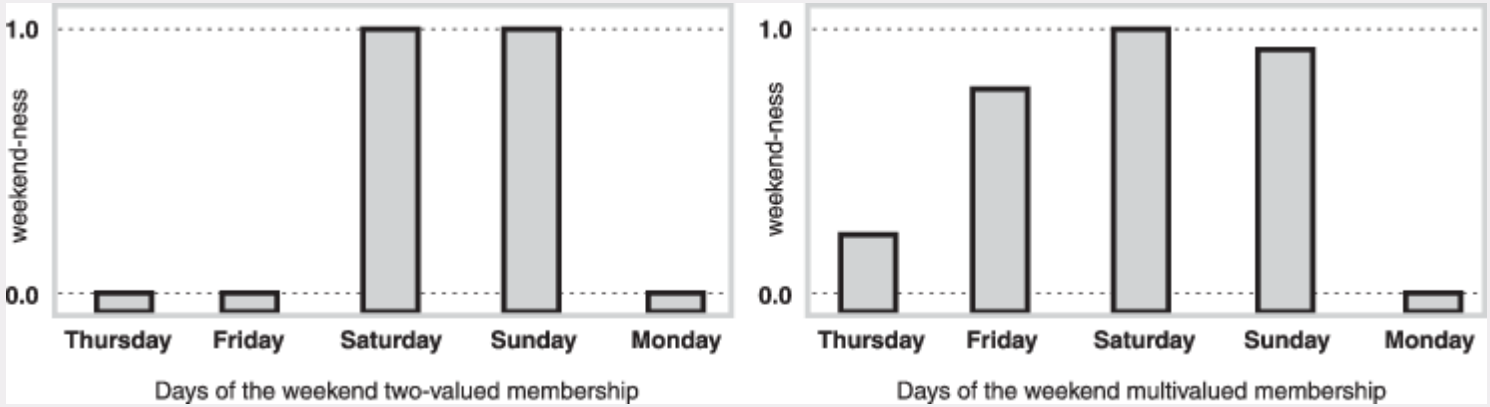


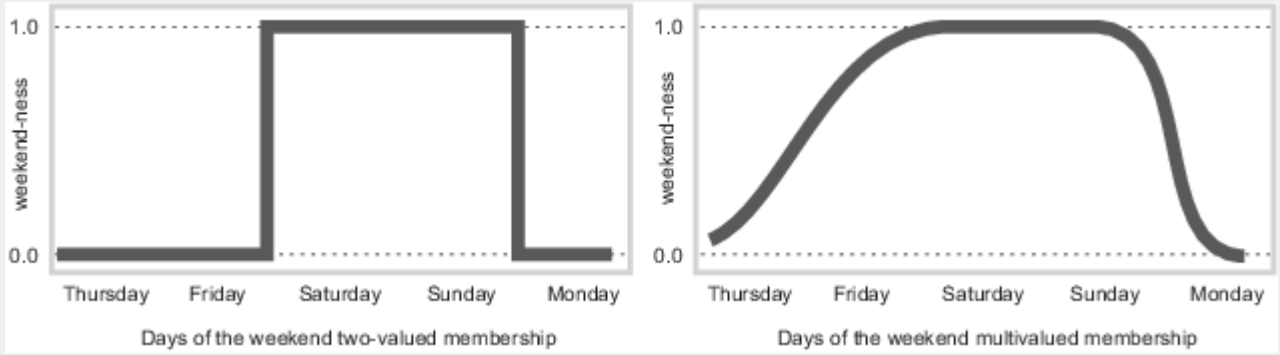


Fuzzy Sets

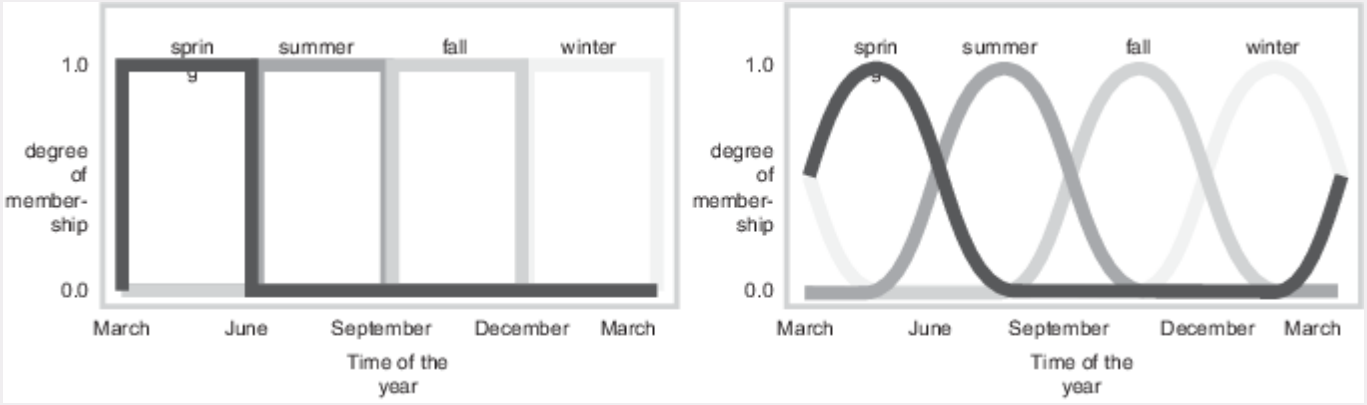

Shoe Polish
Liberty
Saturday
Friday
Thursday
Monday
Sunday
Dorsal Fins
Butter
Days of the weekend

Weekend-ness Example

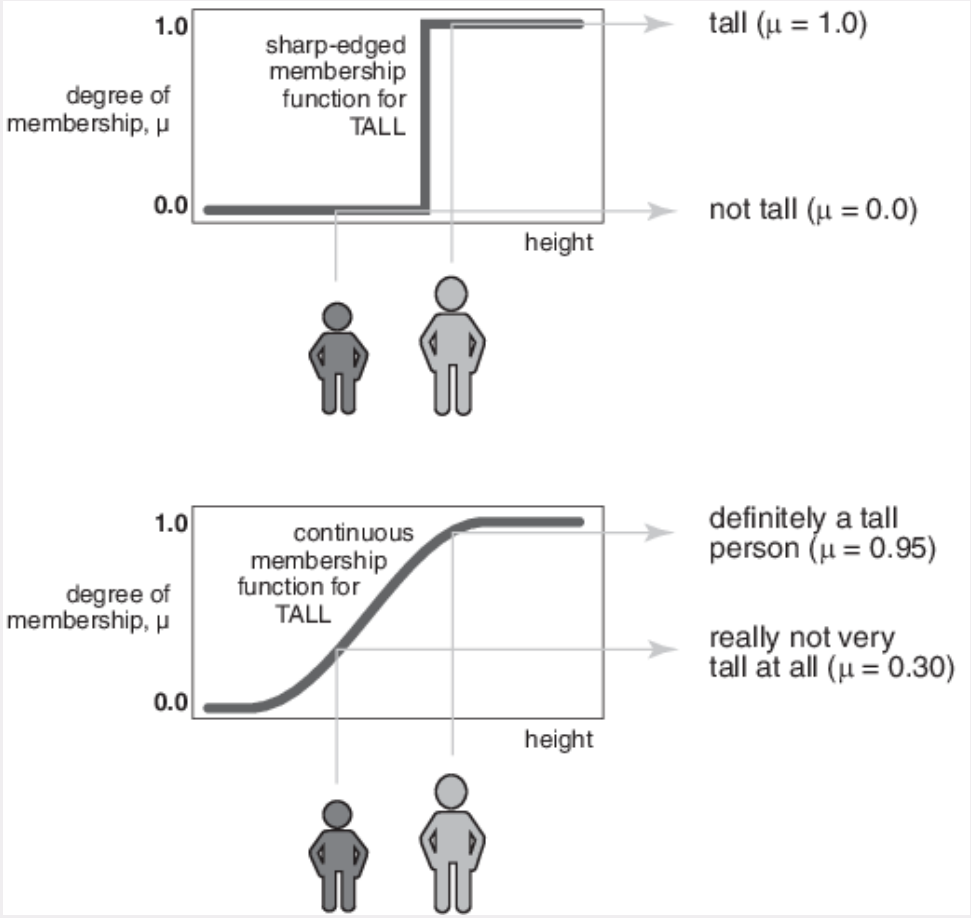




Fuzzy Membership Functions



Crisp vs Fuzzy Membership Functions



Fuzzy Inferencing: Fuzzy Set Multiplication

T-norm (Triangular norm) :

$$\mu_{A\cap B}(x)=T(\mu A(x),\mu B(x))$$

- Boundary — $T(0,0)=0$, $T(a,1)=T(1,a)=a$
  - *Crisp – product with identity or with zero*
- Monotonicity — $T(a,b)\leq T(c,d)$ if $a\leq c$ and $b\leq d$
  - a decrease in the membership values in *A* or *B* cannot produce an increase in the membership value in *A* intersection *B*
- Commutativity — $T(a,b)=T(b,a)$
  - the operator is indifferent to the order of the fuzzy sets to be combined
- Associativity — $T(a,T(b,c))=T(T(a,b),c)$
  - take the intersection of any number of sets in any order of pair-wise groupings

Fuzzy Inferencing: Fuzzy Set Addition

T-conorm (or *S*-norm): $\mu_{AUB}(x)=S(\mu_A(x),\mu_B(x))$

- Boundary — $S(1,1)=1$, $S(a,0)=S(0,a)=a$
  - *Crisp: identity or with zero*
- Monotonicity — $S(a,b)\leq S(c,d)$ if $a\leq c$ and $b\leq d$
  - a decrease in the membership values in *A* or *B* cannot produce an increase in the membership value in *A* intersection *B*
- Commutativity — $S(a,b)=S(b,a)$
  - the operator is indifferent to the order of the fuzzy sets to be combined
- Associativity — $S(a,S(b,c))=S(S(a,b),c)$
  - take the intersection of any number of sets in any order of pair-wise groupings

FIS: Crisp and Fuzzy Logic Tables

A	B	A and B
0	0	0
0	1	0
1	0	0
1	1	1

AND

A	B	A or B
0	0	0
0	1	1
1	0	1
1	1	1

OR

A	not A
0	1
1	0

NOT

A	B	min(A,B)
0	0	0
0	1	0
1	0	0
1	1	1

AND

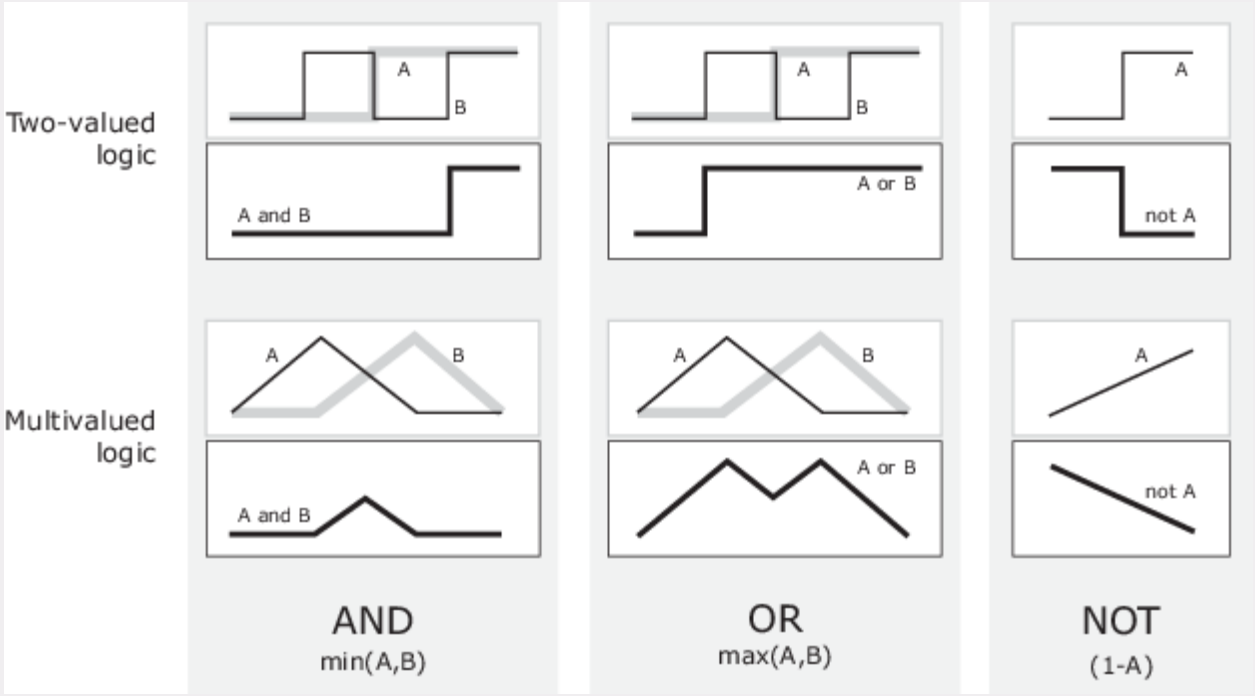
A	B	max(A,B)
0	0	0
0	1	1
1	0	1
1	1	1

OR

A	1 - A
0	1
1	0

NOT

Two-Valued & Multivalued Logic

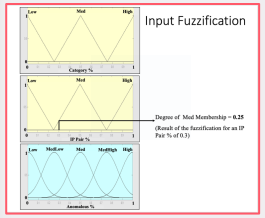


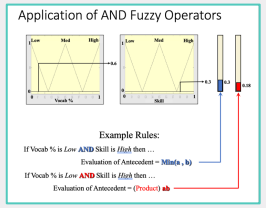
Application

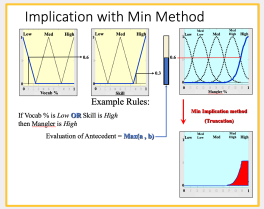
Application of the fuzzy operators for OR and AND

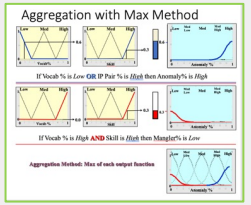
Aggregation

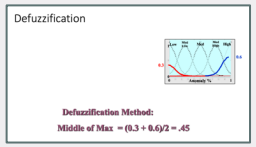
Aggregation Max used











1

Fuzzification

Fuzzification of the input values to membership functions

2

3

Implication

Write some brief here about the heading

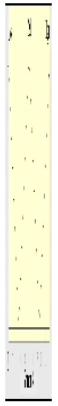
4

5

Defuzzification

Middle of Max used

Input Fuzzification



Phishing %

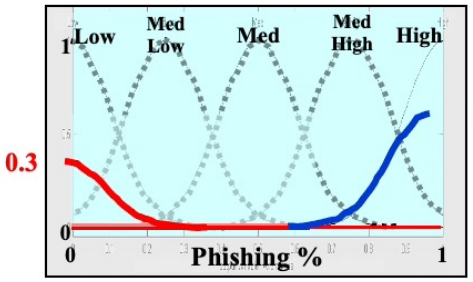
Application of OR Fuzzy Operators

Application of AND Fuzzy Operators

Implication with Min Method

Aggregation with Max Method

Defuzzification



Defuzzification Method:

Middle of Max = (0.3 + 0.6)/2 = .45

Spear/Whaling
Targets a specific group (Spear: admins, etc., Whaling: C-Level)

Smishing/Vishing
Smishing: Text or SMS,
Vishing: Voice->RDP

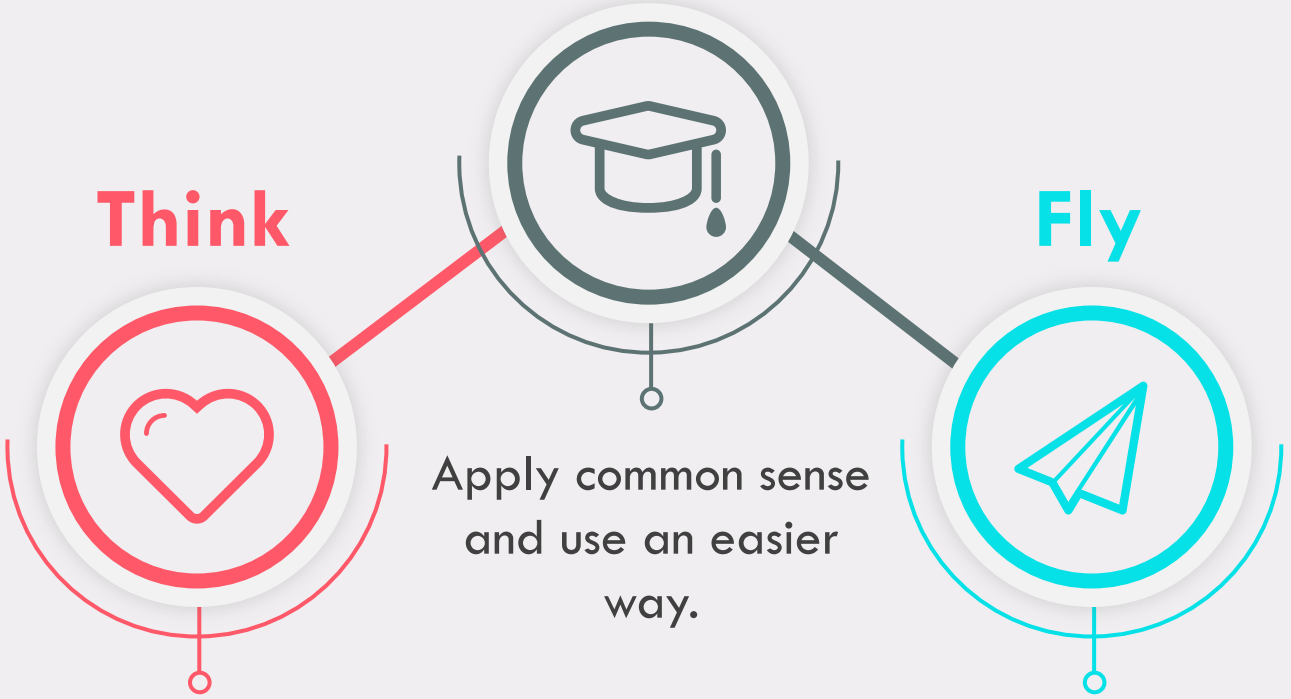
Email phishing
Email at-large and sextortion

Angler Phishing
Hijacking responses

Search Engine
SEO Poisoning

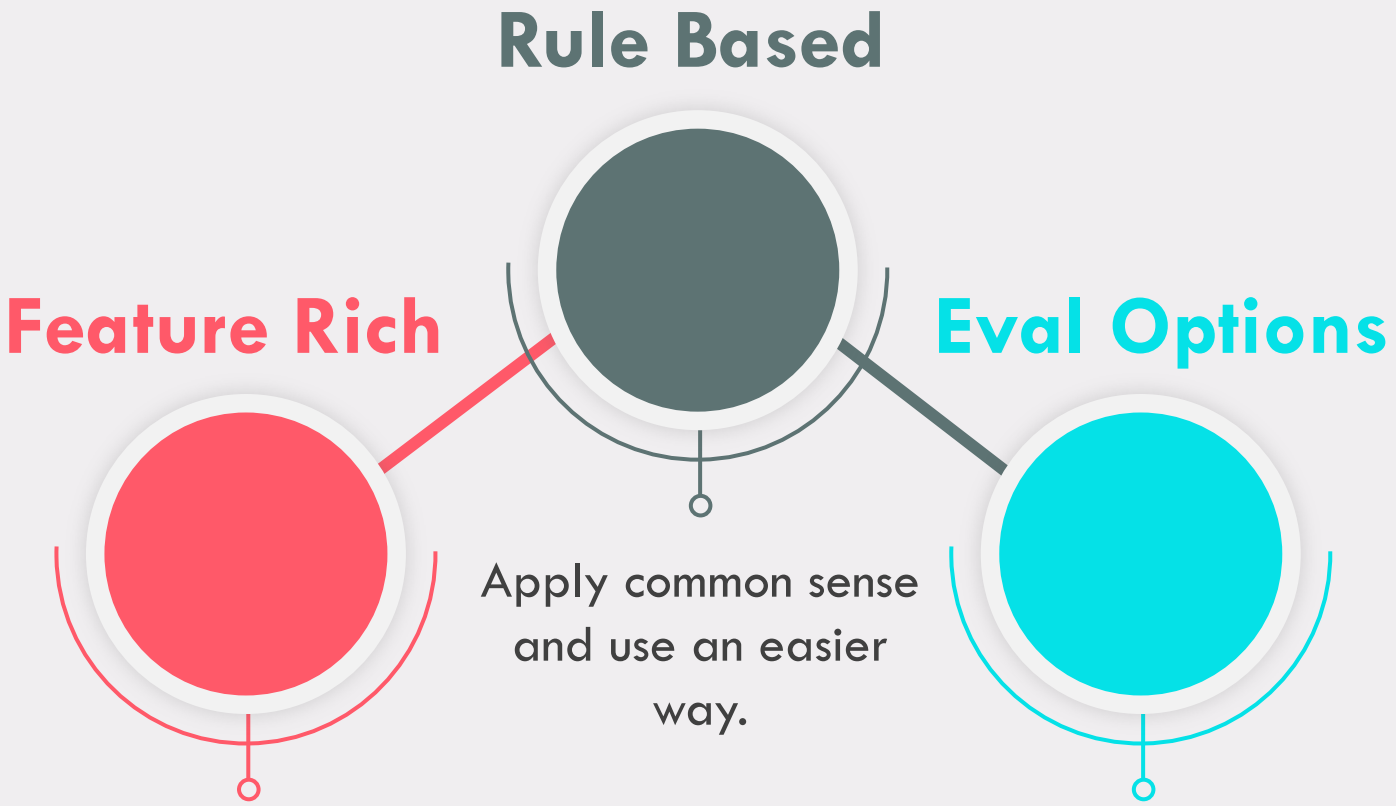
*https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

Burdensome Test



Think about the process, flow, heuristic, rule set, etc.

When it makes sense, you may also see insights into other similar problems


Rule Based
Feature Rich
Eval Options
Apply common sense and use an easier way.
Think about the process, flow, heuristic, rule set, etc.
When it makes sense, you may also see insights into other similar problems

Problem Set up: Input

dataset_phishing.csv (3.66 MB)

Detail | Compact | Column

10 of 89 columns

url	length_url	length_ho...	ip	nb_dots	nb_hyphens	nb_at
http://www.crestonwood.com/router.php	37	19	0	3	0	0
http://shadetreetechnology.com/V4/validation/a111aedc8ae390eabcfa130e041a10a4	77	23	1	1	0	0
https://support-appleld.com.secureupdate.duilawyeryork.com/ap/89e6a3b4b063b8d/?cmd=_update&dispatch=...	126	50	1	4	1	0
http://rgipt.ac.in	18	11	0	2	0	0

*DEMONSTRATING DIFFERENT PHISHING ATTACKS USING FUZZY LOGIC
Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)
IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

Problem Set up: Rules

a. Length of URL
Rule:IF
{URL length<54--->feature=Legitimate else if URL length>=54 and<=75--->feature=Suspicious Otherwise ---->feature=phished}
b.Using URL Shortening Services
Rule:IF
{TinyURL--->phished Otherwise---->Legitimate}
c. URL's having "@" Symbol
Rule: IF
{URL having @ symbol---->Phished Otherwise ---->Legitimate}
2. Domain based Features
a.Domain Age
Rule: IF
{Age of domain >=6 months---->Legitimate Otherwise ---->phishing
b. DNS Record
Rule:IF
{no DNS record for the domain---->Phishing Otherwise----> Legitimate}
c. Website Traffic
Rule:IF
{Website Rank<=100,000---->Legitimate Website Rank>100,000---->Suspicious Otherwise ----

d. PageRank
Rule:IF
{Pagerank<0.2---->Phishing Otherwise ---->Legitimate}
e. Google Index
Rule:IF
{Webpage indexed by google---->Legitimate Otherwise ---->Phishing}
3. HTML and JavaScript based Features
a.Status Bar Customization
Rule:IF
{onMouseOver changes Status Bar---->Phishing It doesn't change Status Bar---->Legitimate}
b.Disabling Right Click
Rule:IF
{Right click disabled---->Phishing Otherwise ---->Legitimate}
c.IFrame Redirection

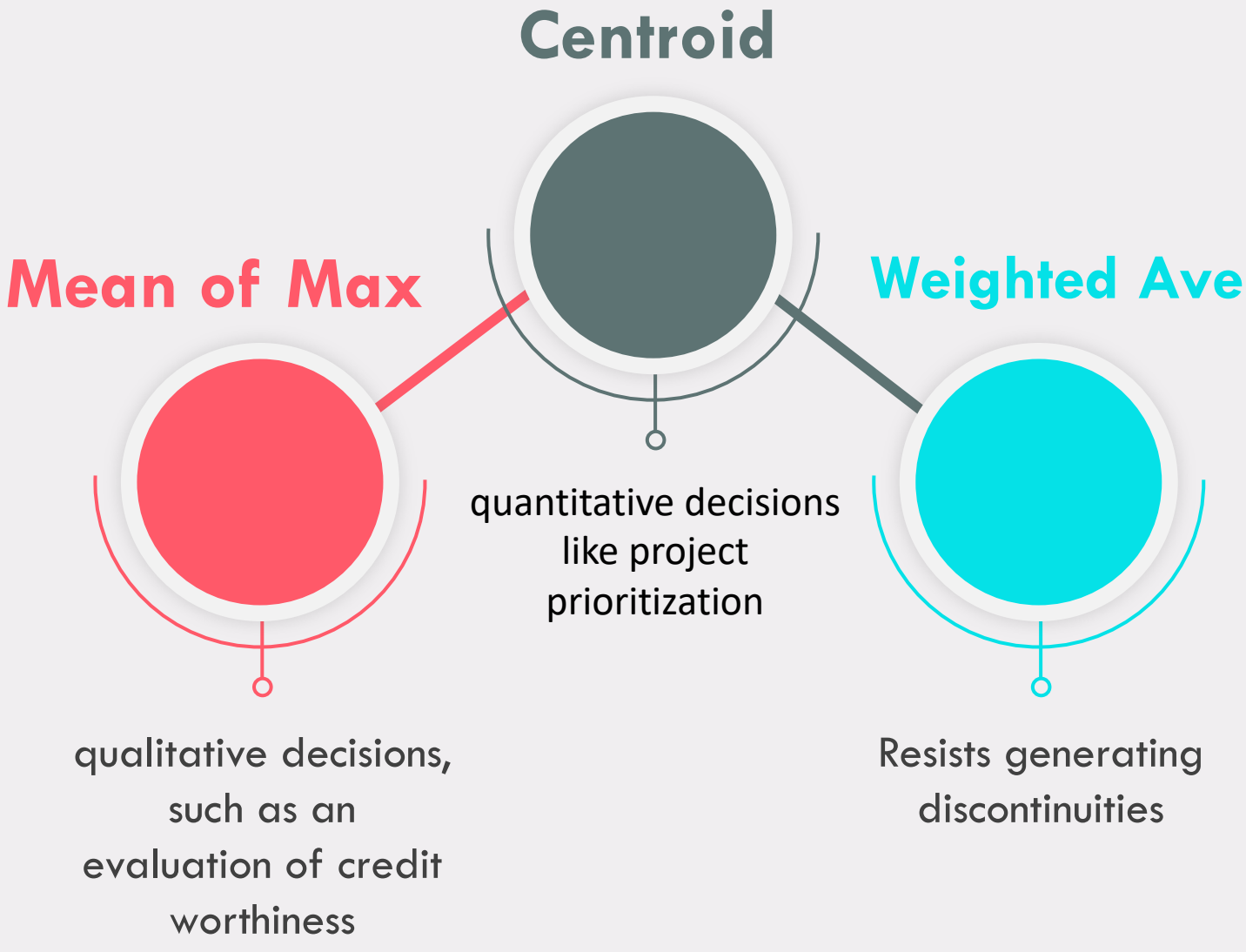
*DEMONSTRATING DIFFERENT PHISHING ATTACKS USING FUZZY LOGIC
Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)
IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

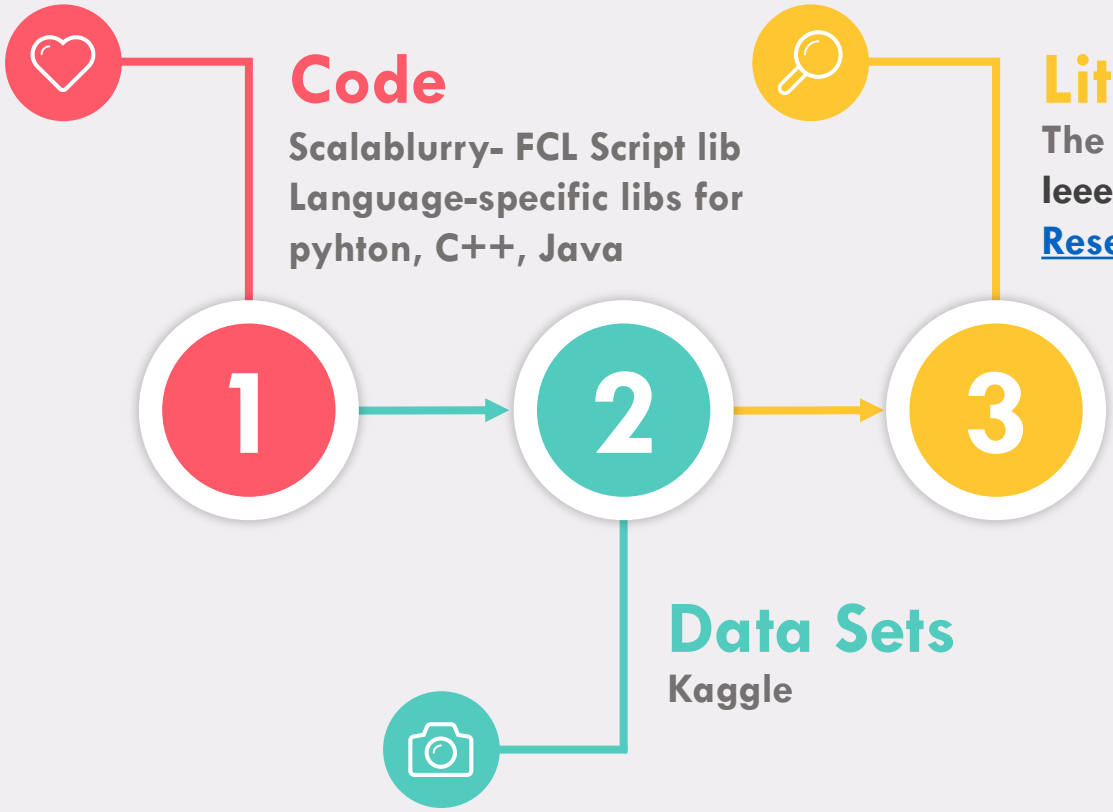
Conclusions

URLs	Defuzzification methods		
	Mean of maximum principle	Weighted average method	Centroid method
http://facelook.shop.co/login.php	Phished	Highly phished	Highly phished
http://www.esmartstart.com	Highly phished	Phished	Phished
http://facebooook.axfree.com/	Suspicious	Legitimate	Suspicious
https://paytm.com/	Highly Legitimate	Legitimate	Highly Legitimate
https://www.amazon.in/	Legitimate	Highly Legitimate	Legitimate

An important aspect of a defuzzification method is the continuity of the output.

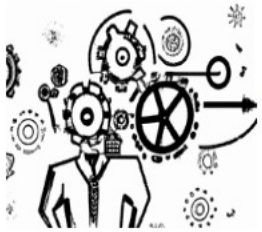
*DEMONSTRATING DIFFERENT PHISHING ATTACKS USING FUZZY LOGIC
Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018)
IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2


Centroid
Mean of Max
Weighted Ave
quantitative decisions like project prioritization
qualitative decisions, such as an evaluation of credit worthiness
Resists generating discontinuities


Code
Scalablurry- FCL Script lib
Language-specific libs for
pyhton, C++, Java
Literature
The Mathworks,
Ieeexplore, ACM,
Research Gate
1
2
3
Data Sets
Kaggle


Resources
Applying Fuzzy
Phishing
The Fuzzy Process
History of Fuzzy
Intro

Thank You!



Raymond Garcia, Ph.D.

ray@fathomdynamics.com

678-488-9522

LinkedIn

YouTube
rgvidworld

raygarcia