RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: STR-R06

Session Title: Defending Security is Probabilistic, Not Deterministic: Get Over It

Winn Schwartau

Security Theoretician
@WinnSchwartau

Dr. Mark Carney

Quantum Researcher
@LargeCardinal

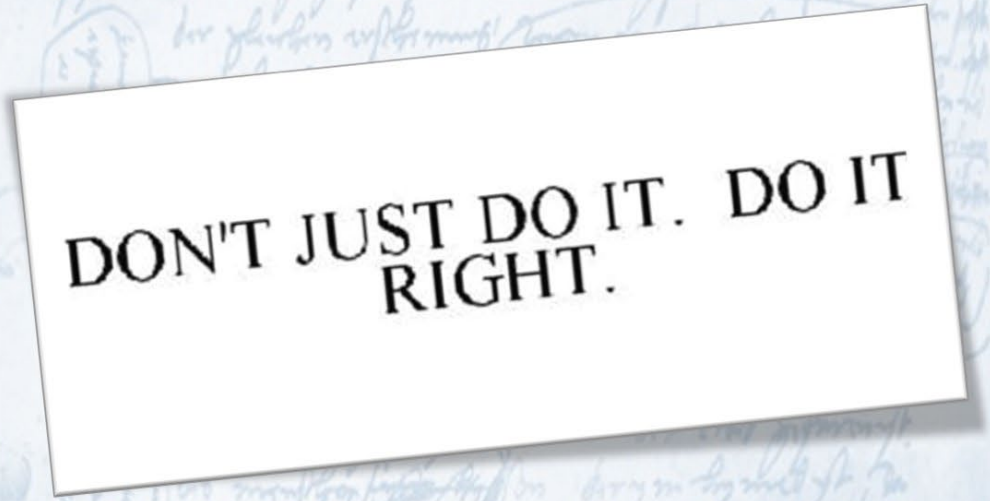
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

What Are You Going To Learn?

- How to view security as a Non-Binary endeavor
- Probability Basics
- Non-Intuitive Answers
- Apply Trust Questions
- Why time is the Fundamental Component of Security



Winn's Axioms (based upon, "Digital is not Binary")

- Trust is not Binary or Permanent.
- There is no security without Trust.
- Time is the common metric between security, privacy, and trust.
- Trust & security must have upper and lower boundaries: >0 and < 1

Does Security Exist? Is It Real or Imaginary? Define Security.

ENVIRONMENTAL SECURITY
PEACEKEEPING
DECISION-MAKING
ECONOMIC OPPORTUNITIES
POLITICAL REPRESENTATION
EDUCATION
PEACE NEGOTIATIONS
HEALTHCARE
HOW DO YOU DEFINE SECURITY?
FOOD SECURITY
LIVELIHOODS
CLEAN WATER
WOMEN, PEACE & SECURITY
VOTING RIGHTS
GENDER EQUALITY
FREEDOM OF SPEECH
PARTICIPATION

Security Only Can Exist if There is Trust

Trust is Relational. Networks Are Relational. People Are Relational.
If there is no Trust… there is no Security.

Are you 100% Positive…?

- You won't be involved in an Accident? (Relational)
- 'Hopefully' not
- 0 < Accident < 1

AUD: How can you be SURE?

Are you 100% Positive…?

- You will safely make the leap?
- Statistically based Trust on rider behavior.
- 0 < Loop Safely < 1

AUD: How can you be SURE?

Relational: Trust is the Inverse of Risk
The Limits of Trust

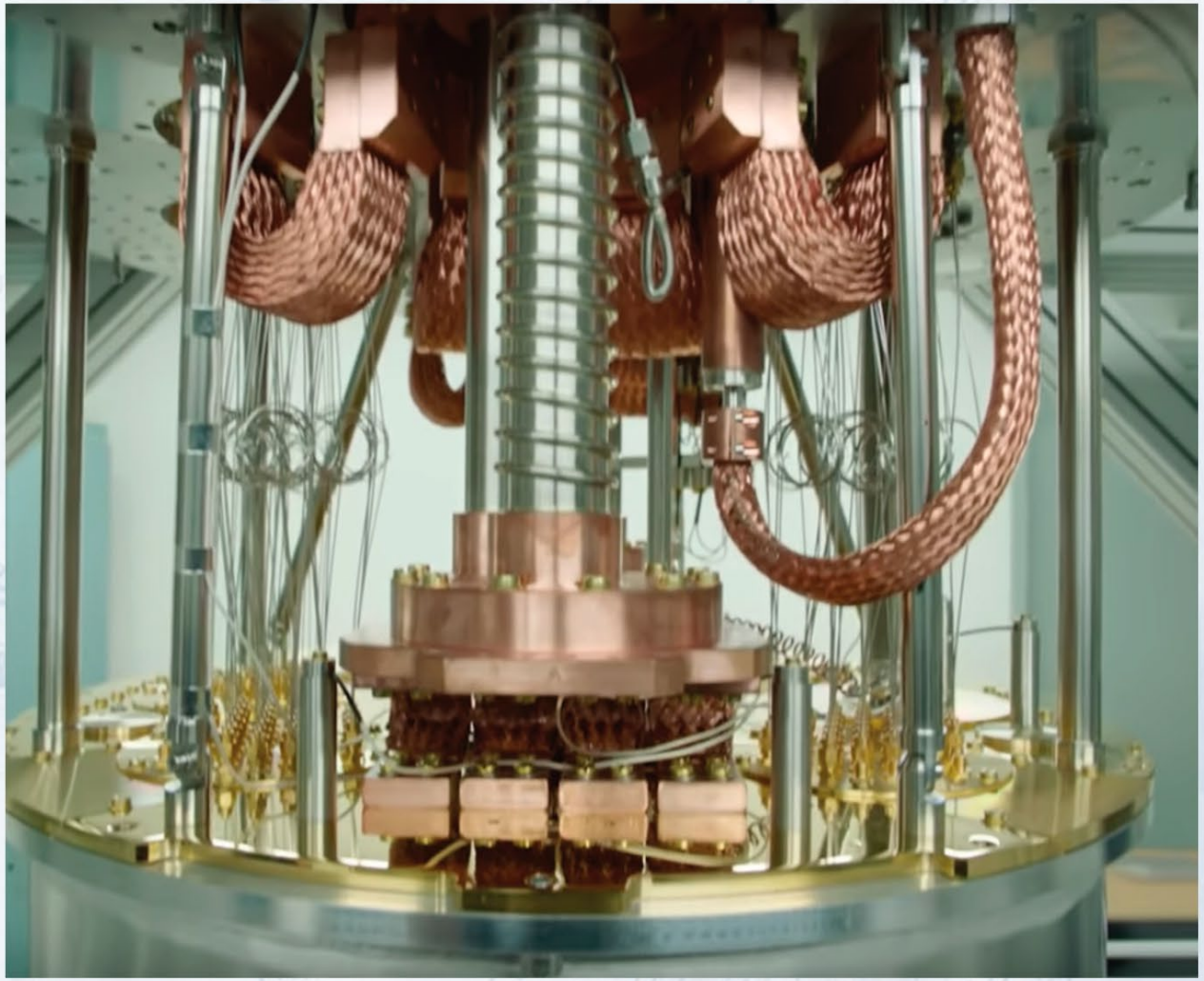
- If a relationship exists:
  - Risk Increases
  - Trust Decreases
  - Trust = 1/Risk
  - Risk = 1/Trust
- Your Belief Systems are meaningless.
- It's about the Maths!

0 < Trust < 1

0 < Risk < 1

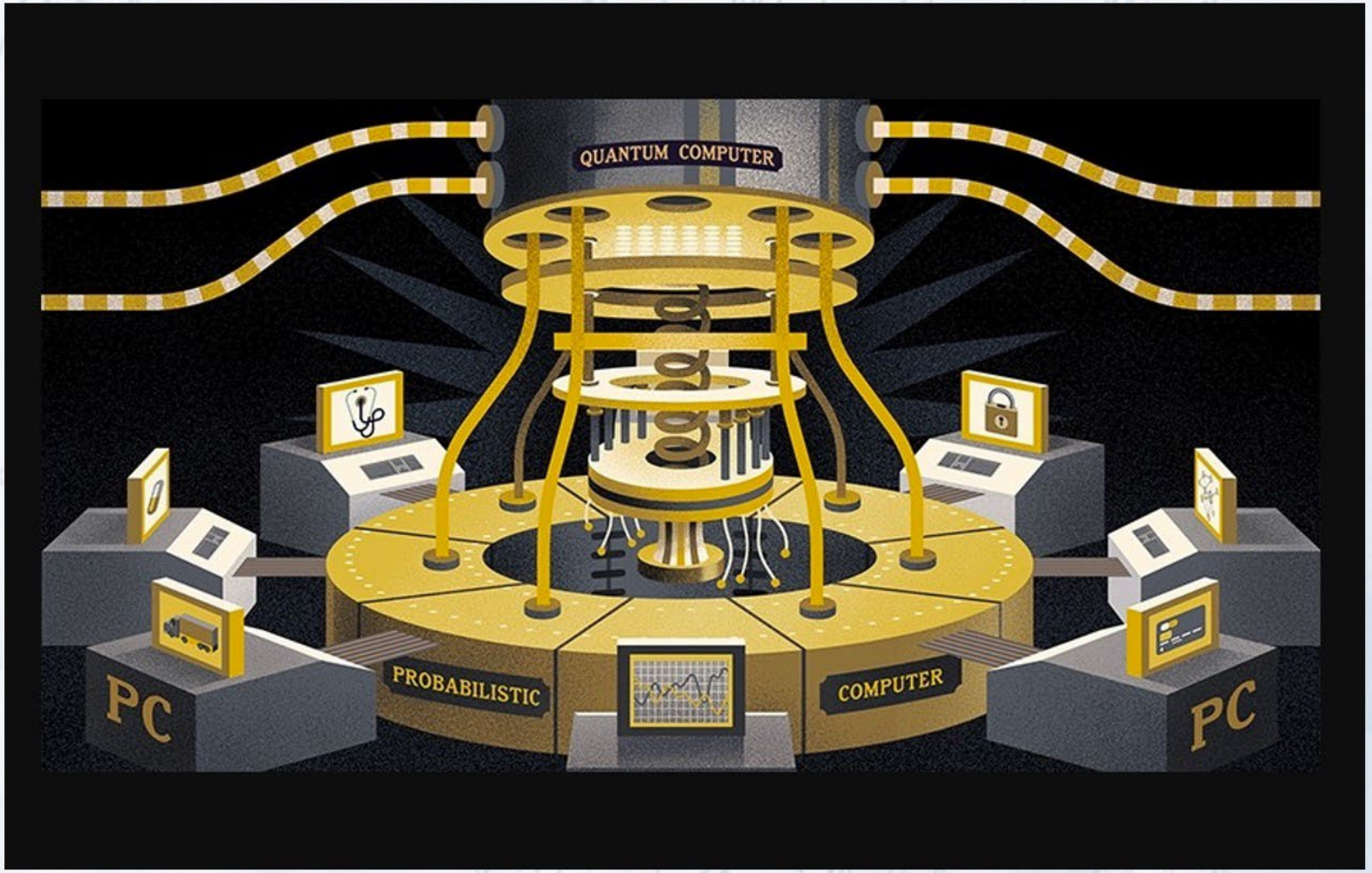
Quantum Computing is Probabilistic

- Superpositioning
  - Probabilistic limbo
  - → 0 K Required
- High Error Rates as Temp Increases
- Calculates Probability amplitudes of paths, then $0 < p < 1$
- Answers are NEVER certain, or 100%.



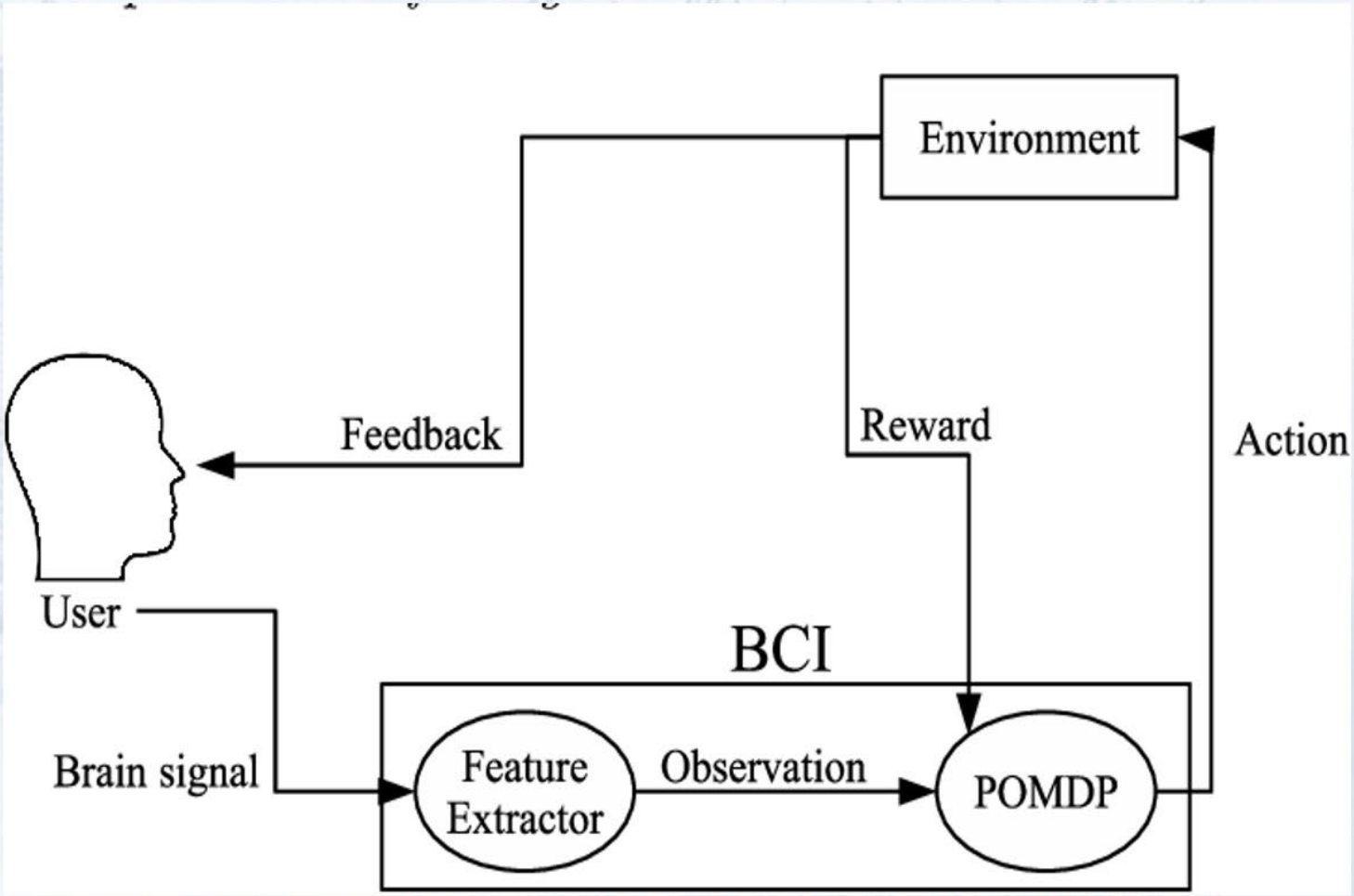
Meanwhile, at Purdue

- Probabilistic Computer
- Works at Room Temp
- Optimization Problems
- Step between Binary and Quantum
- Uses p-bits
- Adjustable randomness
- Note: The “Loop”



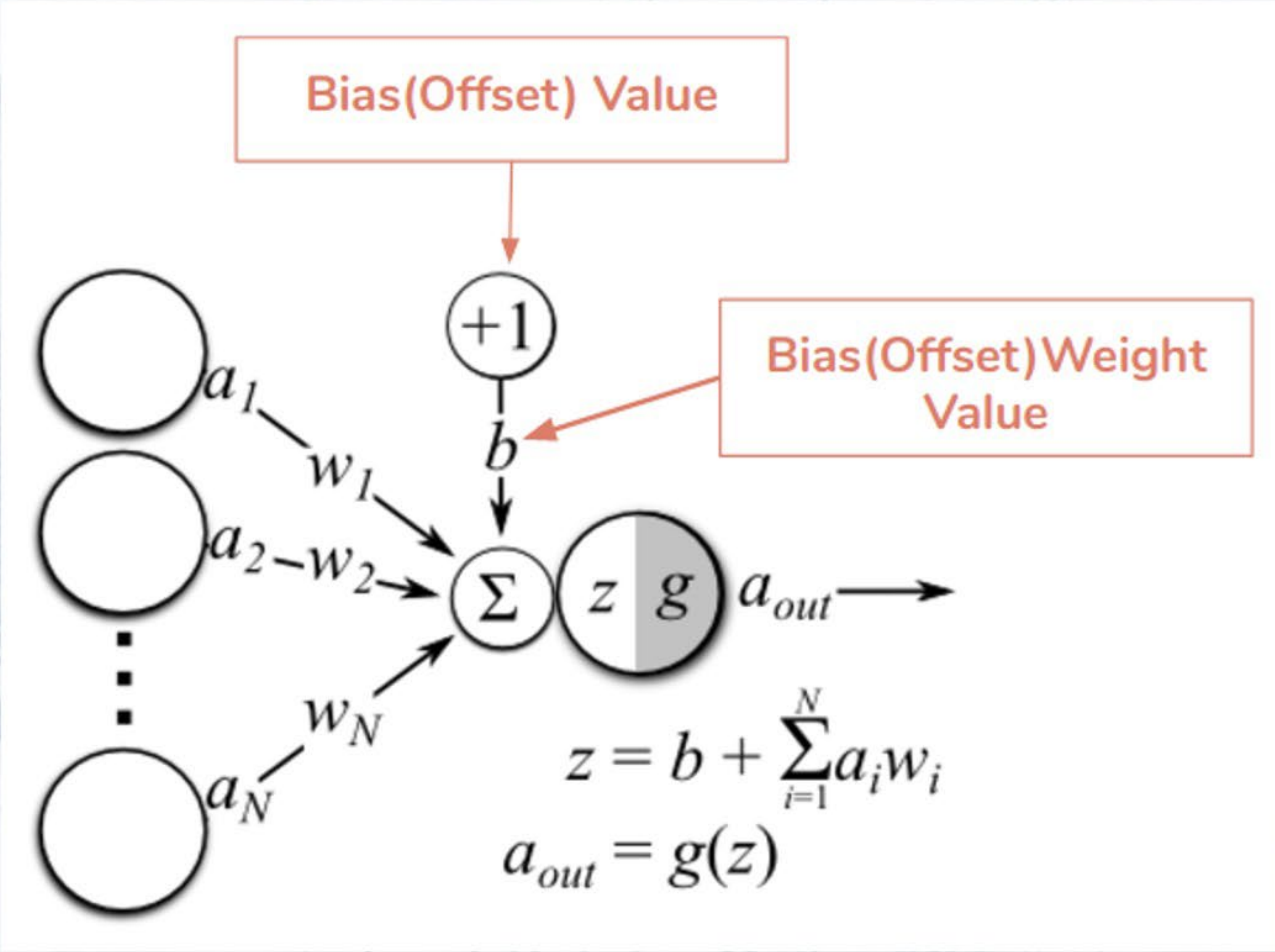
Human Brains are Probabilistic Averaging Machines

- Sensory
  - Sight
  - Hearing
  - Touch
  - Taste
  - Touch
- Neural
  - Averaging
  - Weighting
  - Polling/Voting
  - Stochastic Processing
  - Notably, Poor Memory



Neural Networks Are Probabilistic

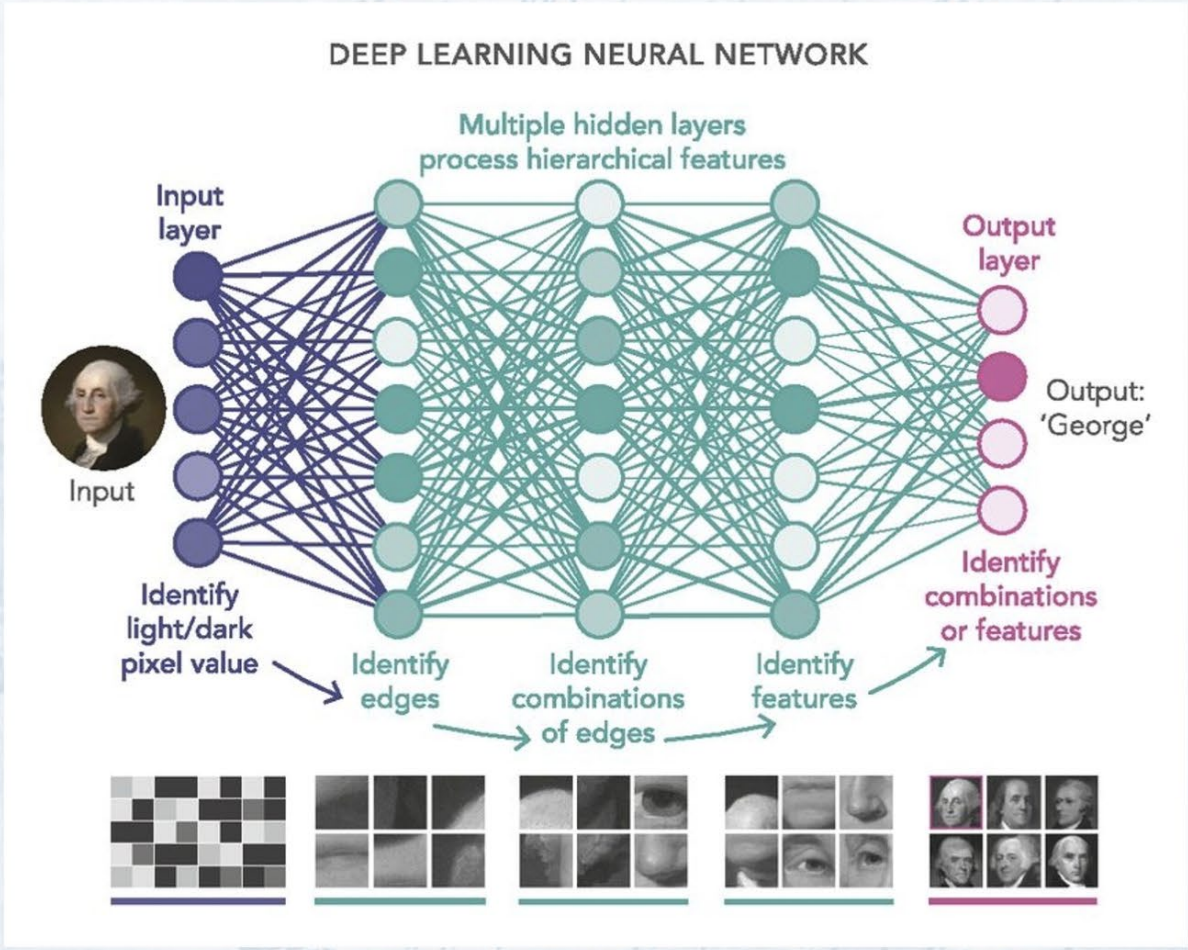
- Modeling the Brain (we think)
- Weighted outputs
  - Assumptive Bayesian
- Experience modifies output
  - Feedback/OODA



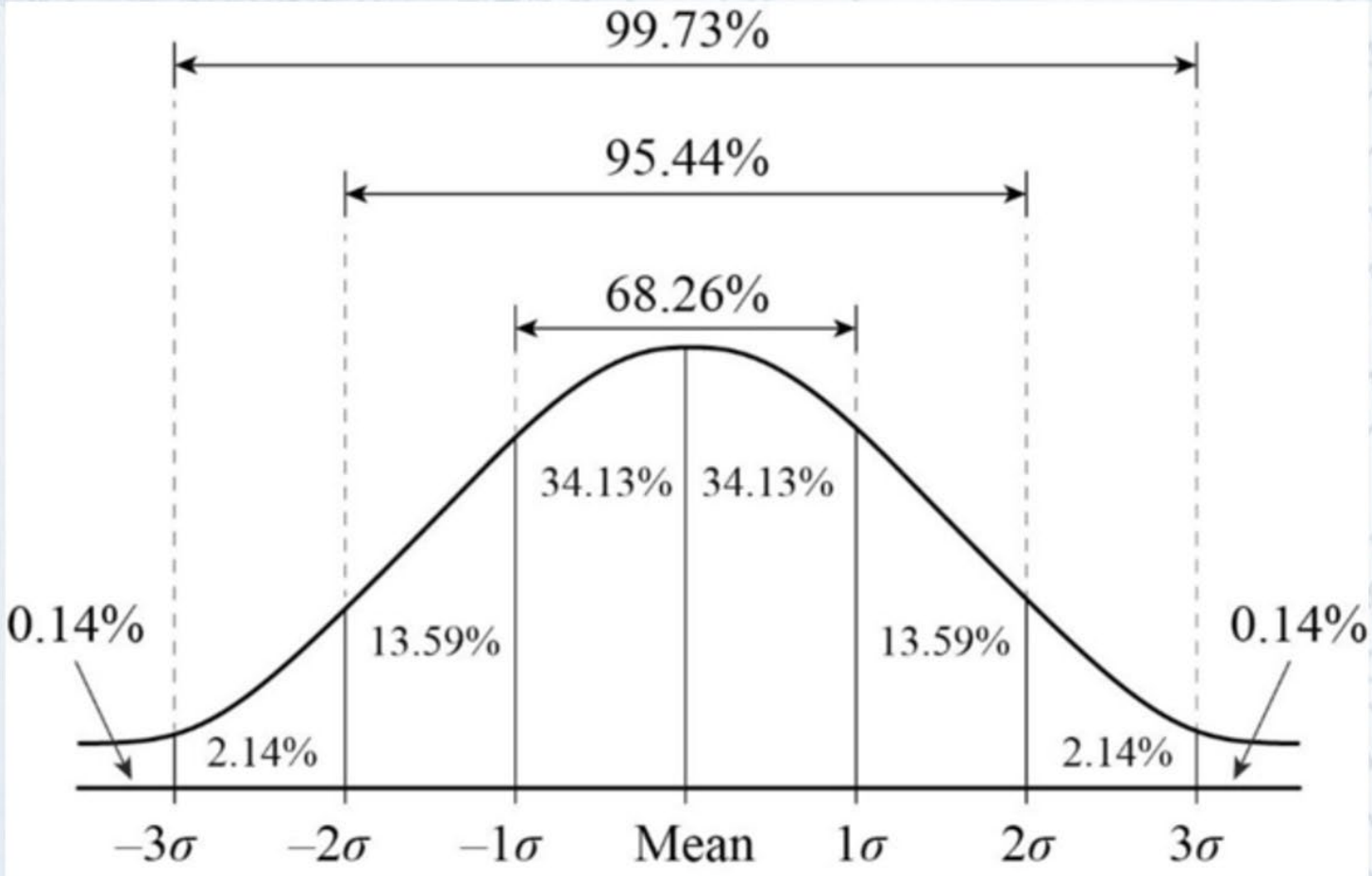
ML & DL & CNNs Are Probabilistic

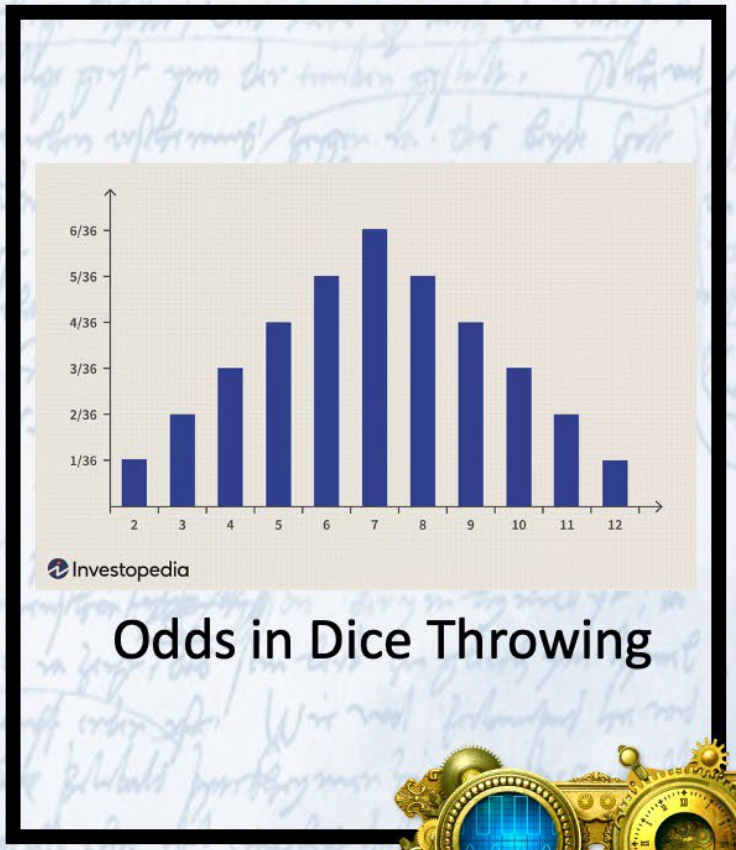
- Analogues
  - Weighting
  - Biases
  - Relative Values
- 1M+ Inputs
- 1B+ Layers (hidden+)
- Tomorrow's answers will be different than today's.

Probably is Close Enough – Depending Upon Application (Translation, Pattern recog, OCR, Predictions, etc.)



Probabilistic Curves

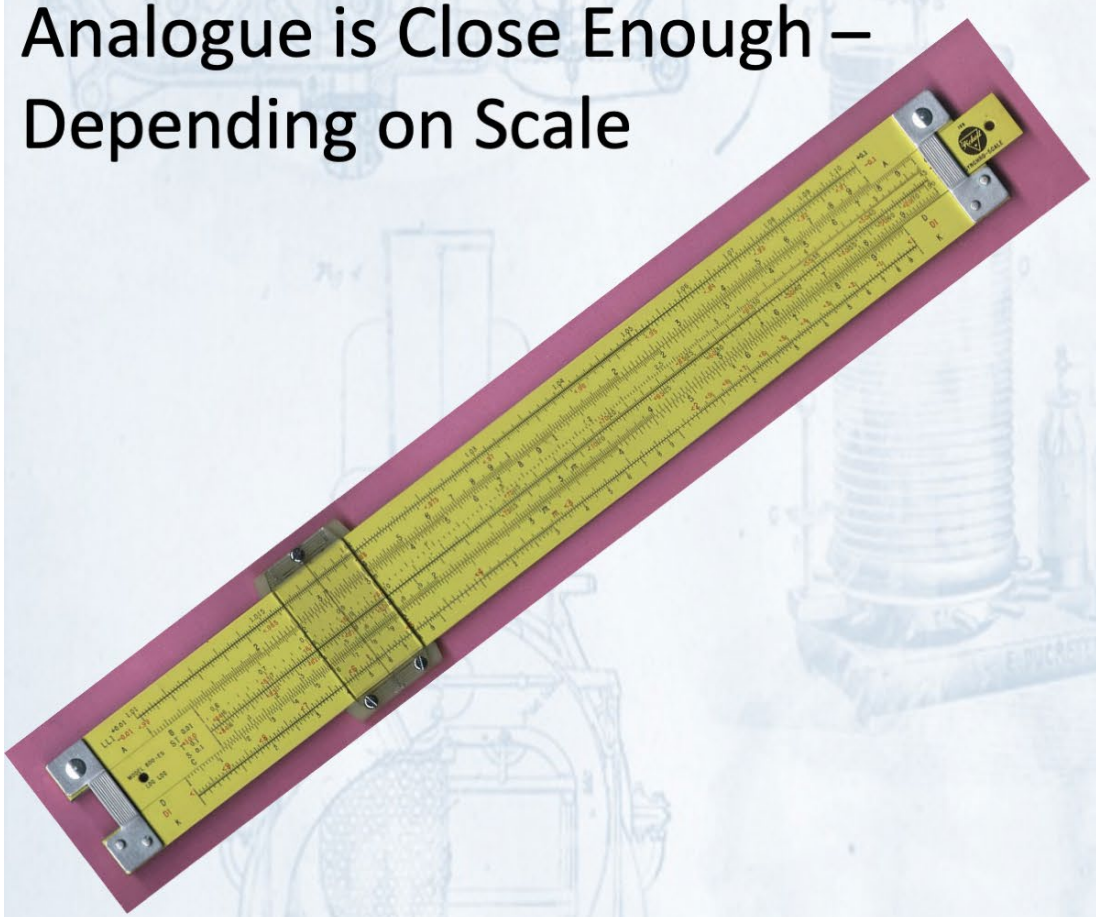


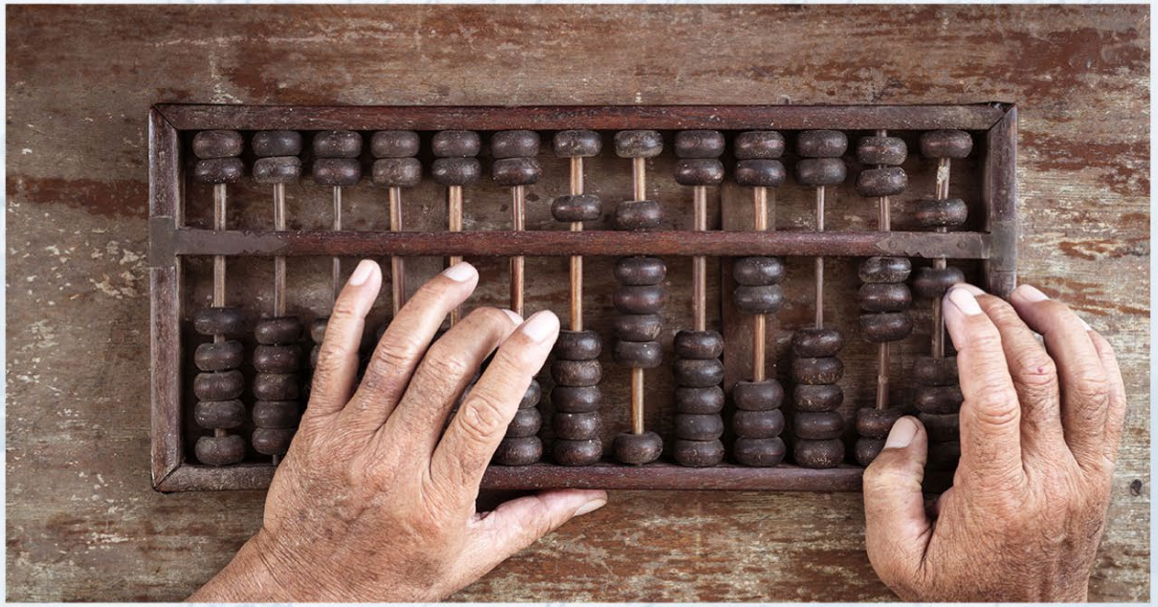


Analogue

Digital

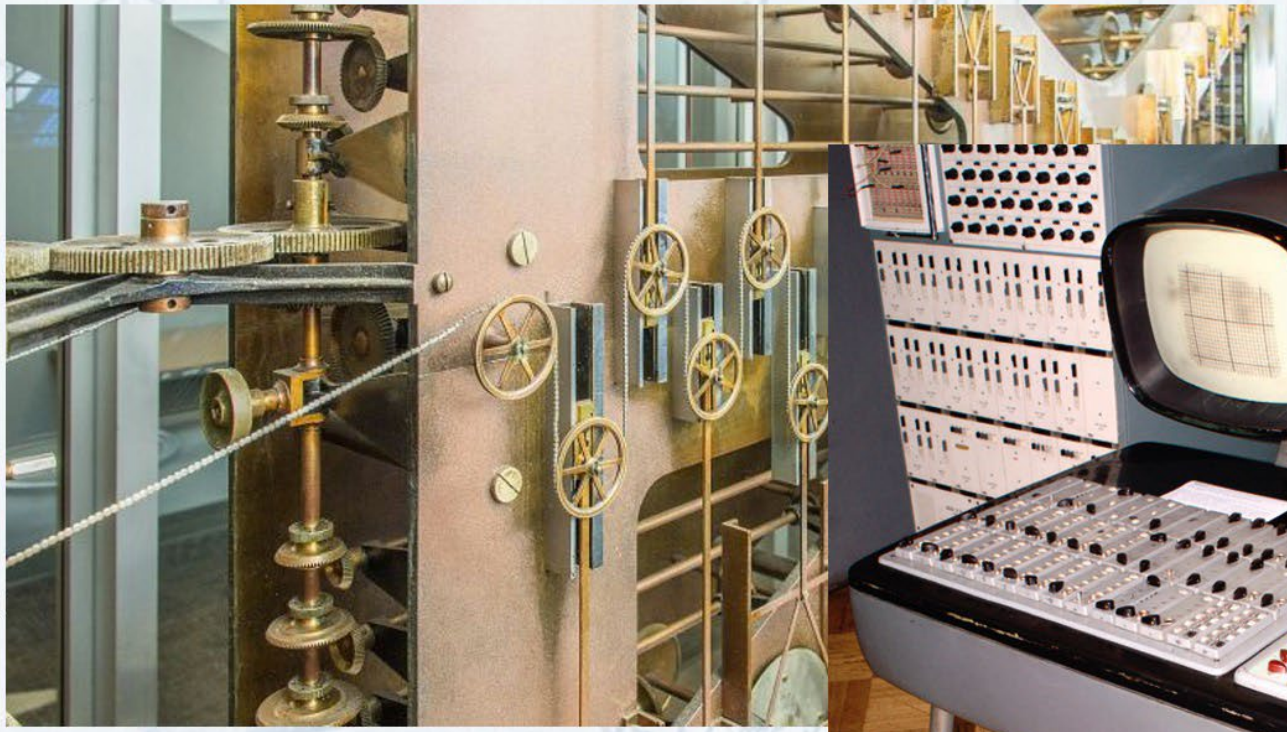
Analogue is Close Enough – Depending on Scale





Analogue Computing

- Can be Much Faster, Cheaper, Lower BW,
- Easy Prototyping & PoC
- More Eco-Friendly
- Precision Scalable
  - Lower accuracy
- EZPZ Physical Integration (Sensors, etc.)
- No ADACs or quantization errors. Low noise.
- Min < X < Max



The Basis of Time-Based Security

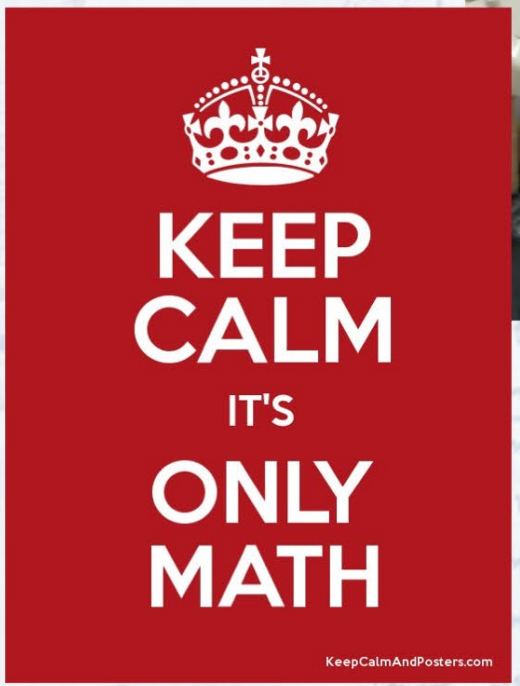
$$P_{(t)} > D_{(t)} + R_{(t)}$$

You can only be ‘secure’ if the amount of time it takes to both Detect and React to a particular event is LESS than the amount of Guaranteed time your Protection devices and processes can provide.

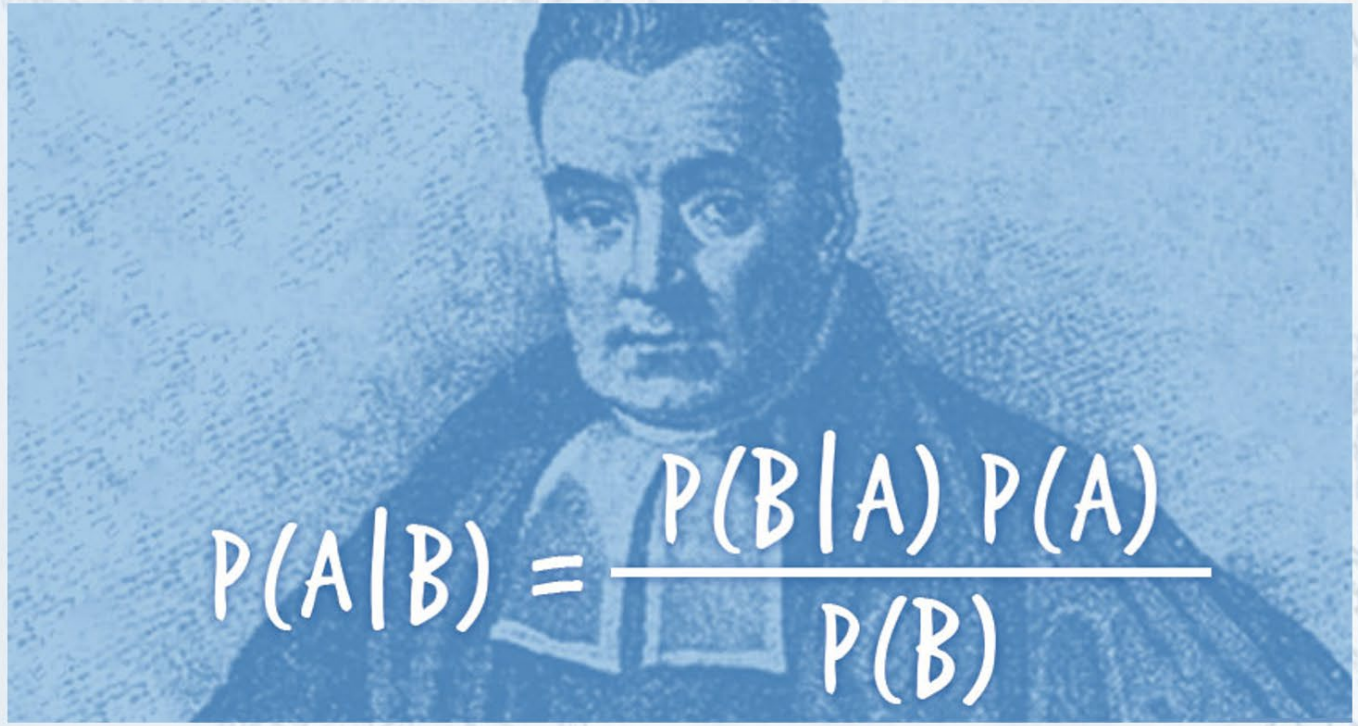
Is Your Network Secure Mathematically? (Nah…)

Dr. Mark Carney, FRSA

- Hardware Hacker and Cryptography guy
- Researcher
  - post-quantum and quantum cryptography
  - IoT device security
  - quantum algorithms for hacking/mining data in networks
- Musician first - former Chetham's School of Music
- Pseudo-Sound Engineer - good for winding up Winn...



Real math of ANS



"A Bayesian is one who, vaguely expecting a horse, and catching a glimpse of a donkey, strongly believes he has seen a mule."

"A frequentist is a person whose long-run ambition is to be wrong 5% of the time."

Real math of ANS

"One accurate measurement is worth a thousand expert opinions."

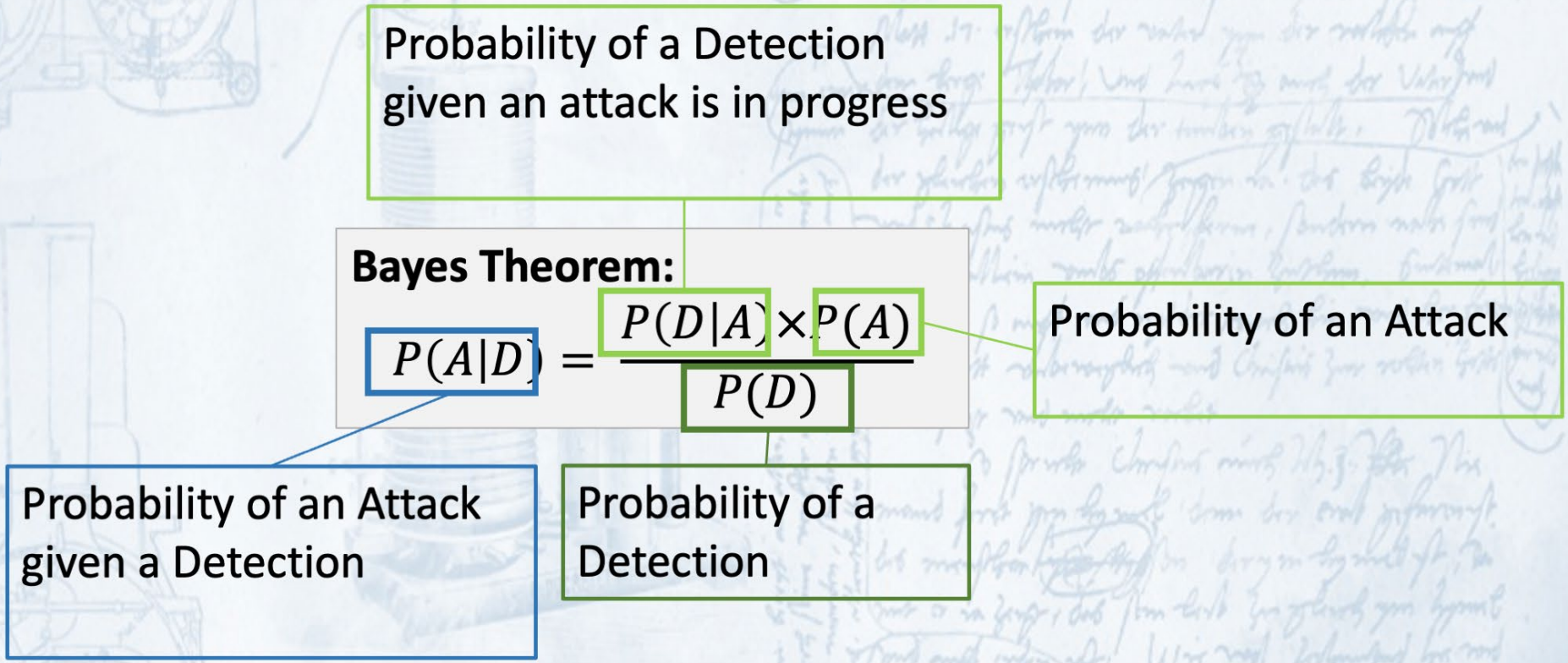
-- Adm. Grace M. Hopper

Real math of ANS

The Desired Inequality:

$$P(t) > [D(t) + R(t)]$$

A Short Anatomy of Bayes Theorem



A Worked Example – Substitute Numbers

Bayes Theorem:

$$P(A|D) = \frac{0.99 \times 0.001}{(0.99 \times 0.001) + (0.01 \times 0.999)}$$

A Worked Example – Substitute Numbers

Bayes Theorem:

$$P(A|D) = \frac{0.00099}{0.01098}$$

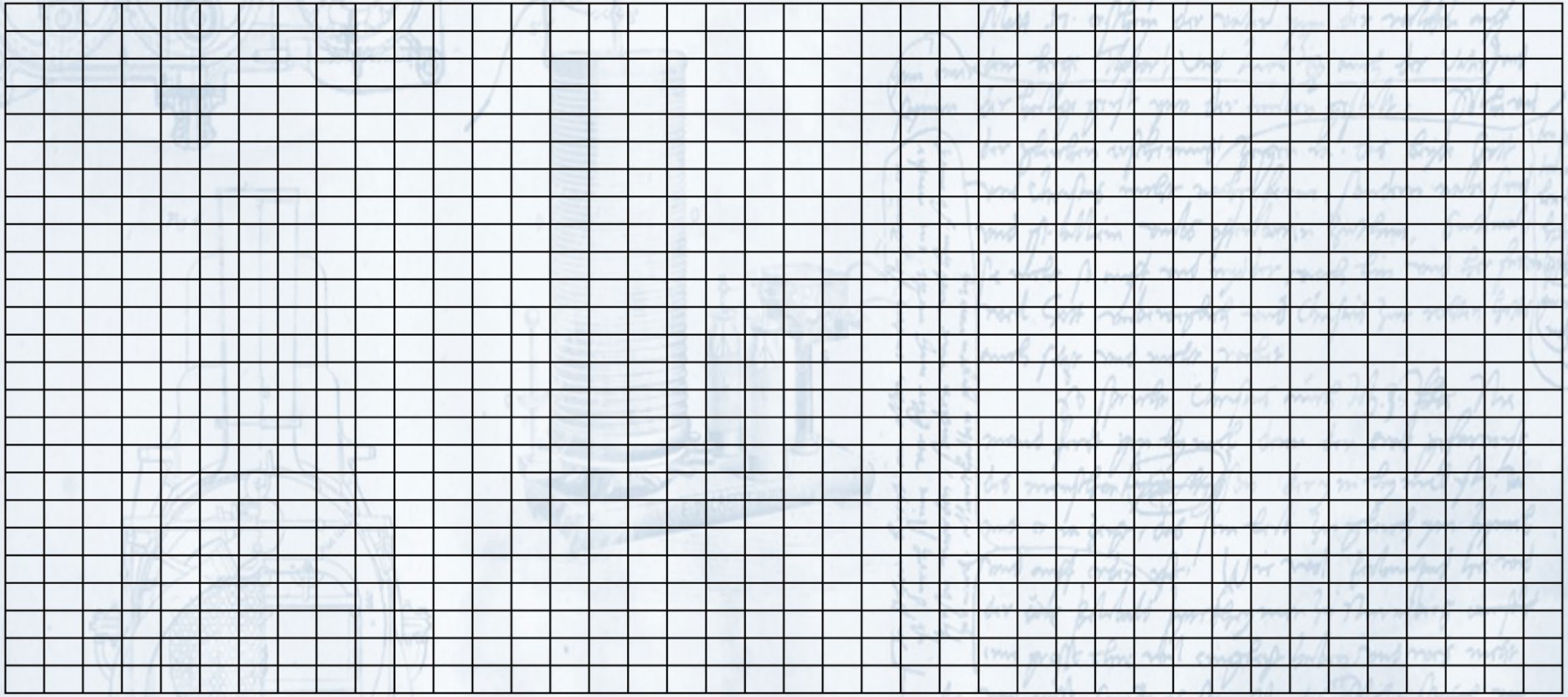
A Worked Example – An unusual result!

Bayes Theorem:

$$P(A|D) = 0.09016 \approx 9\%$$

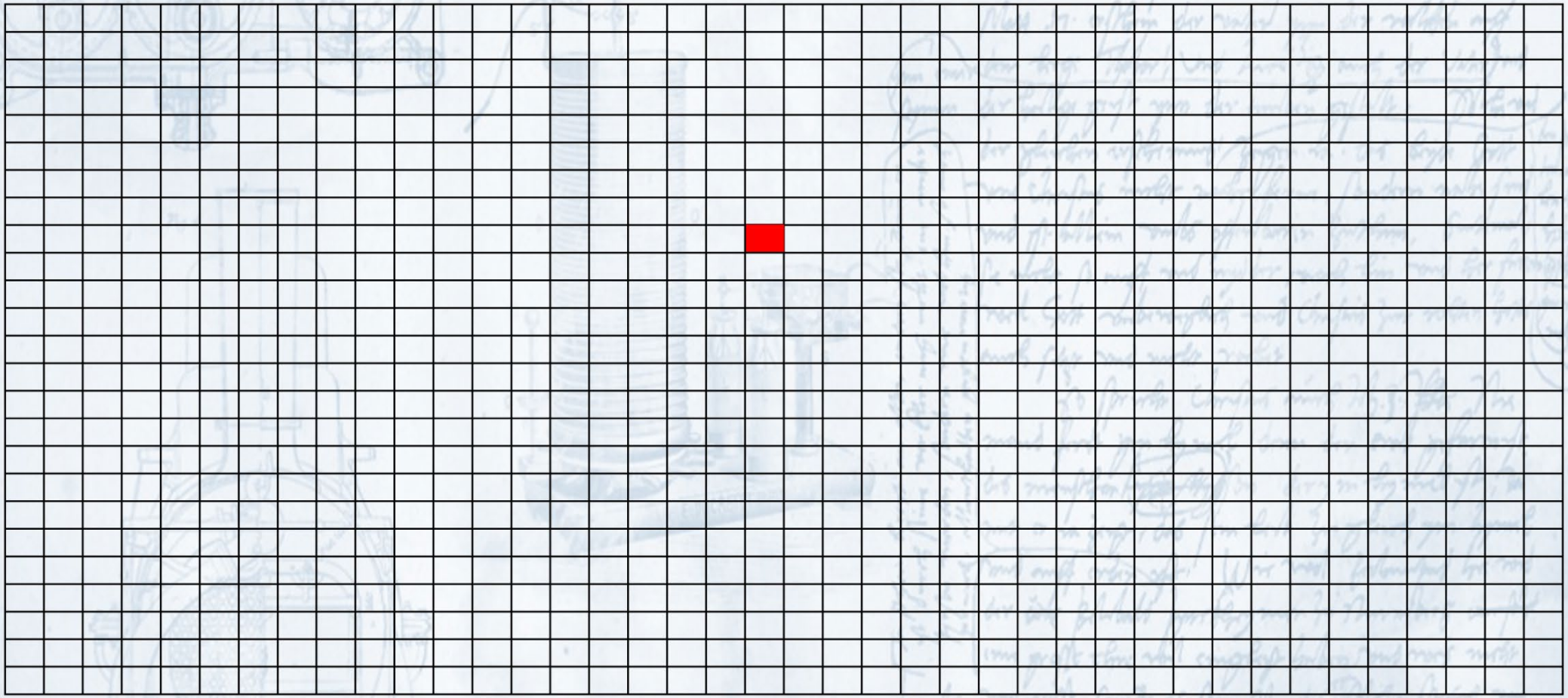
But **HOW** does this make sense?

A Worked Example – 1000 emails

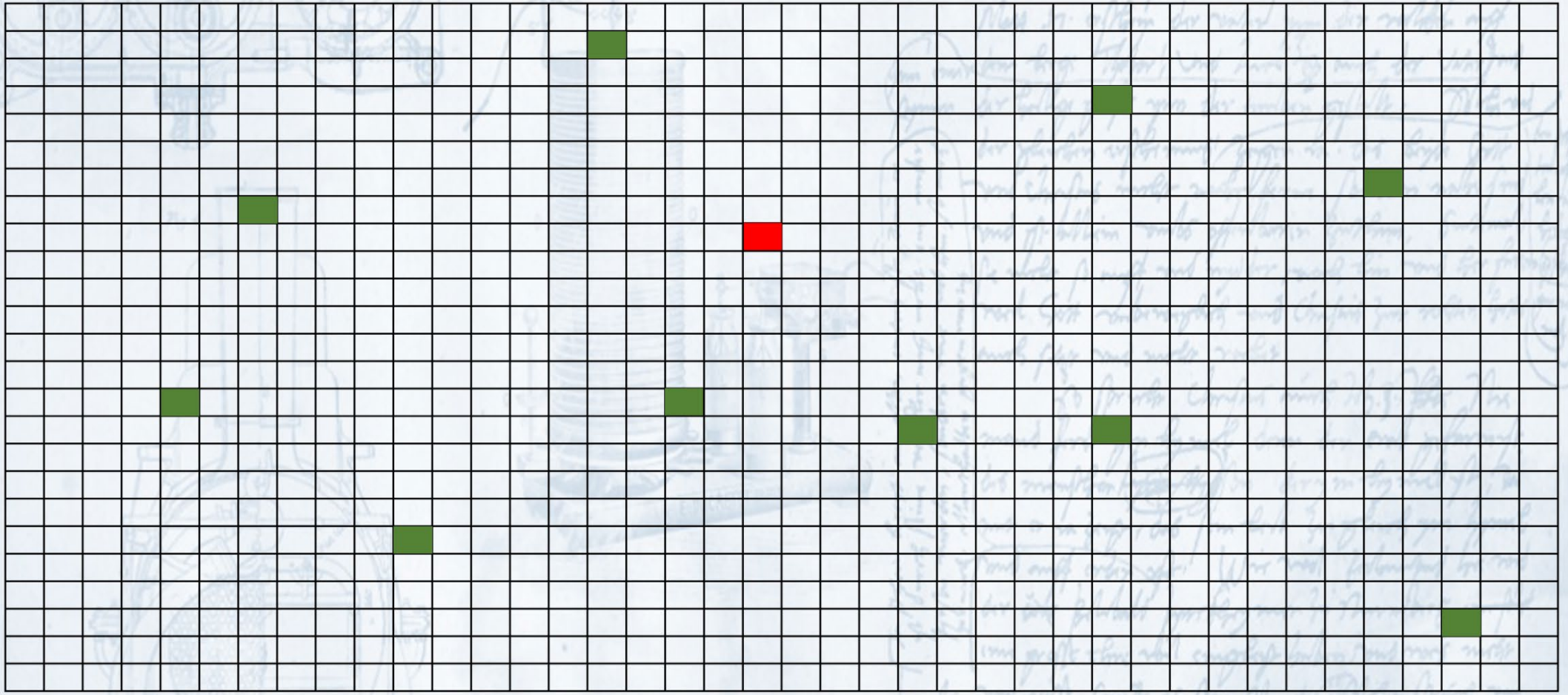


35

A Worked Example – The malicious email

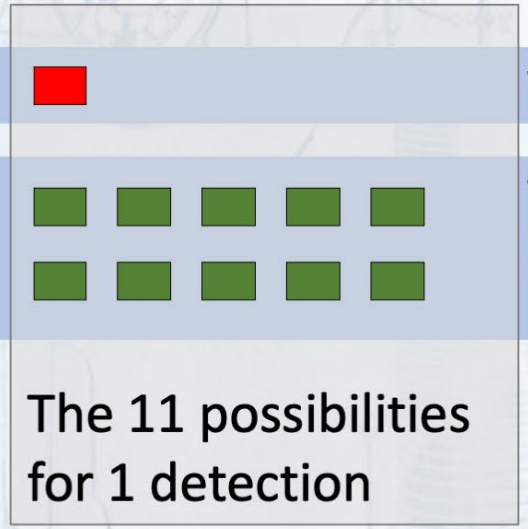


A Worked Example – The false positives



37

A Worked Example – An explanation of 9%



The 11 possibilities for 1 detection

The Malicious Email we need to detect

The 10 (1% of 1000) False Positives we need to consider this detection could be

Thus, we can see that the actual malicious email is 1 of 11 possibilities, or 1 in 11, or ≈ 9%

NB – Bayes is not fully using this logic, but it is handy for understanding

38

Is Your Network Secure? Probably Not!

- *P(D)* be the probability that we detected a real attack of some kind.
- *P(A)* be the probability that an attack of this kind is in progress.
- it's our value of *P(D|A)* that is, the probability that our detection was triggered given a real attack occurred.

$$P(D) = (P(D|A) \times P(A)) + (P(D|\overline{A}) \times P(\overline{A}))$$

$$P(A|D) = (P(D|A) \times P(A))/P(D)$$

Is Your Detection Vendor Telling You the Truth? How do They Come up With Numbers?

- Vendor says: P(D) = 99% accuracy
- Likelihood of attack, *P(A)*, is 0.1% - that is, say, e.g., 1 in 1000 emails or sites users on the network receive/visit are malicious.

$$P(D) = (0.99 \times 0.001) + (0.01 + 0.999)$$

- P(D) = ~1.1% ... but

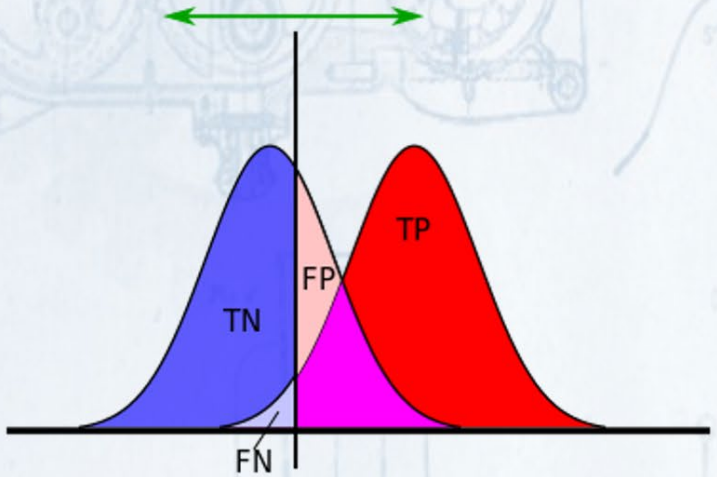
$$P(A|D) = (0.99 \times 0.001)/0.011$$

- P(A|D) = ~9.02% an actual attack occurred (single detection)
- With 2nd Detection event, probability increases.

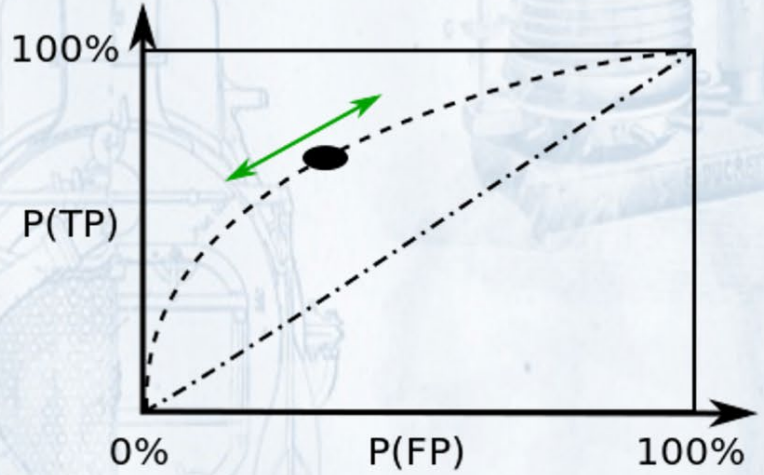
$$P(A|D) = (0.0902 \times 0.99)/0.0983 = 90.75\%$$

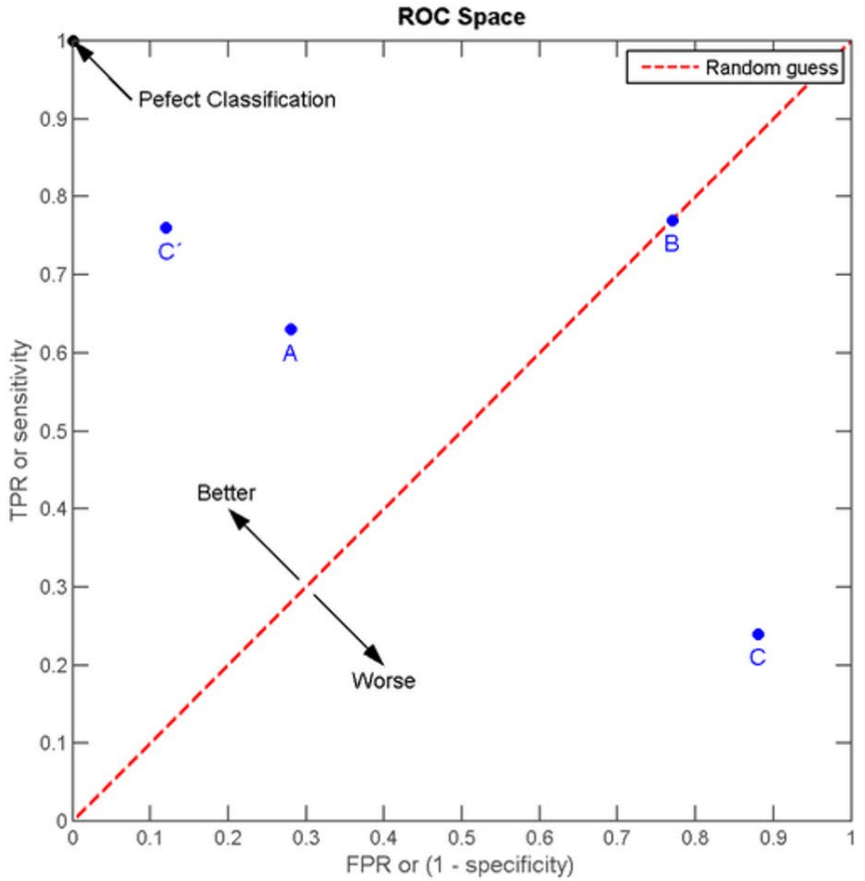
ROC Space (Receiver Operator Characteristic)

Sensitivity = TPR Specificity = TNR



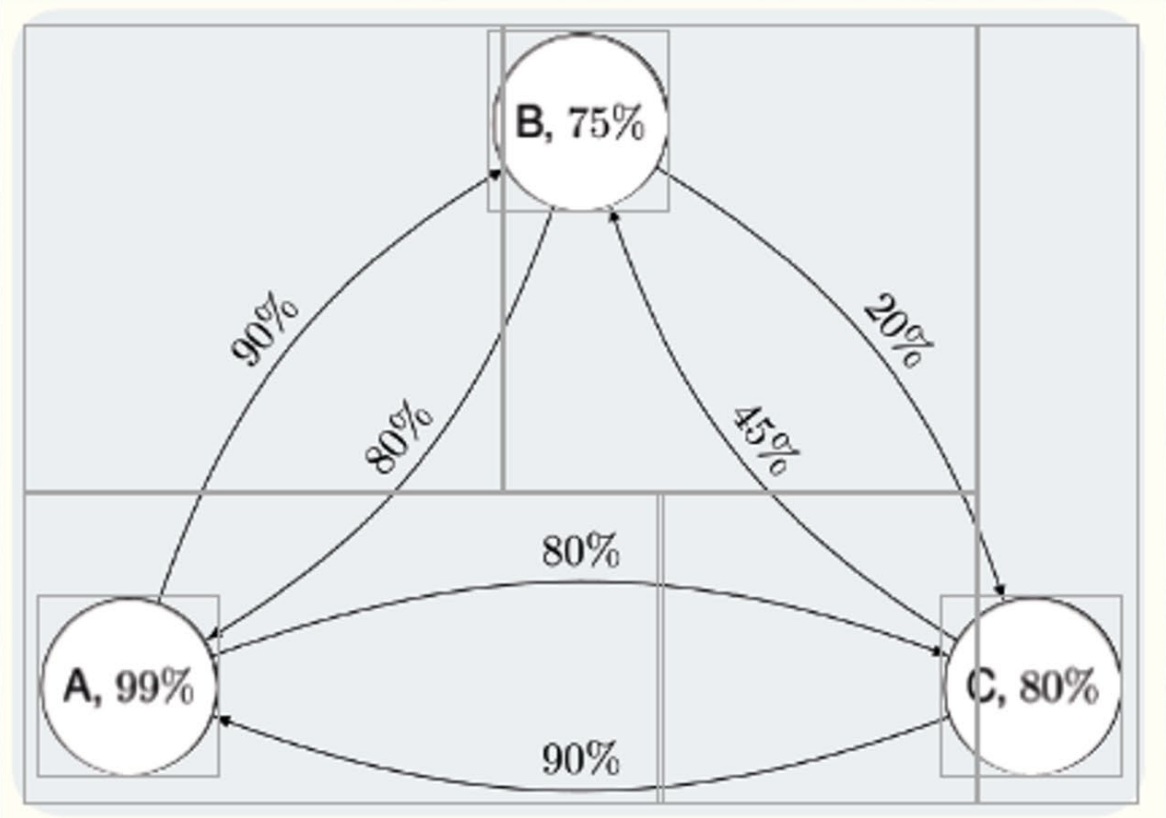
TP	FP
FN	TN





Trust Across Networks is Bi-Directional

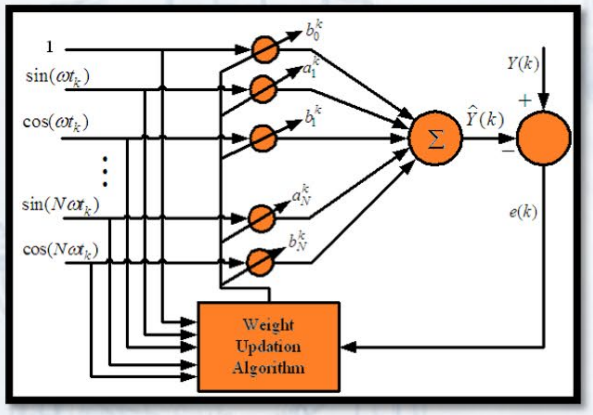
- A, B, C Nodal Trust Factors
- AB, AC, BC Relational Trust Factors
- This overall 3-node NW Trust Factor is only 52.6%



$$P_{ANS}(A \cup B \cup C) = (0.85 \times 0.99) + (0.4 \times 0.75) + (0.64 \times 0.8) - (0.85 \times 0.99 \times 0.75) - (0.85 \times 0.99 \times 0.8) - (0.3 \times 0.75 \times 0.8) + (0.6 \times 0.99 \times .75 \times 0.8) \approx 0.526 \approx 52.6\%$$

I Have Trust Issues

- Trust is NOT Binary!
  - Weighted
  - Changes over time!
  - Not 100% accurate
- Dynamic Trust Degradation
- Periodic Trust Re-Evaluation
- 0 < Trust Factor (TF) < 1
- TF = 1/Risk

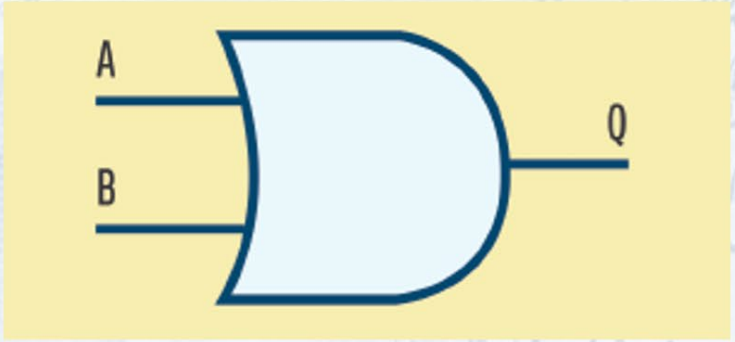


Measuring Trust		Case #1	Case #1	Case #2	Case #2
	Value	Weighting	Weighted	Weighting	Weighted
Criteria	0.0 to 1.0	Factor	Value	Factor	Value
Technical Competence	0.95	75.00%	0.713	6.00%	0.057
Past Job History	0.85	10.00%	0.085	5.00%	0.043
Recommendations	0.9	6.00%	0.054	2.00%	0.018
Vetting Level 1: Tech	0.97	1.00%	0.010	5.00%	0.049
Vetting Level 2: Background Check	0.86	0.00%	0.000	5.00%	0.043
Socia Media Behavior	0.65	0.00%	0.000	5.00%	0.033
Years on Current Job	0.5	1.00%	0.005	15.00%	0.075
Miscreant Illegal Behavior	1	1.00%	0.010	19.00%	0.190
Psychological Profile	0.67	1.00%	0.007	8.00%	0.054
Belief Systems	0.77	1.00%	0.008	3.00%	0.023
Weaknesses/Frailties	0.6	1.00%	0.006	9.00%	0.054
Commitment	0.78	1.00%	0.008	11.00%	0.086
Life Goals	0.7	1.00%	0.007	3.00%	0.021
Career Goals	0.7	1.00%	0.007	4.00%	0.028
Total Trust Factor	0.779	100.00%	0.918	100.00%	0.772

$$\text{for } x \in (0, 1) : \lim_{x \to c} f(x) = L$$

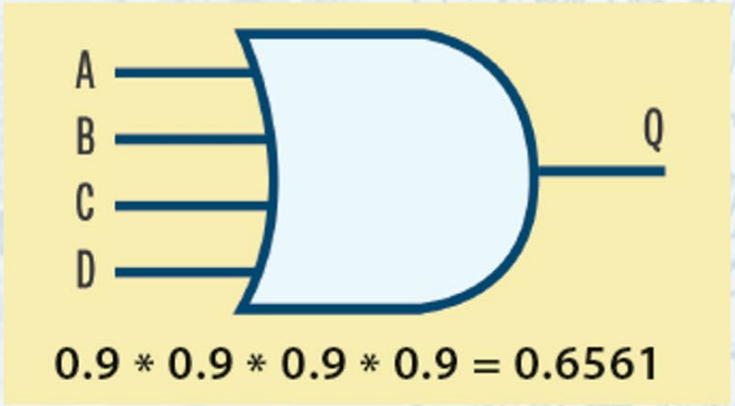
Bayes and the 2-Man Rule: More OR

- Both Alice and Bob have a Trust Factor of 0.9.
- If **TF(A) = 0.9** and **TF(B) = 0.9**, then, independently, they each represent a 10% risk, or probability of error (oops!), or miscreance (gotcha!).
- Multiple admin entities increase Risk and decrease Trust.



TF(A) * TF(B) = TF (A * B) = 0.81 *or inversely,*

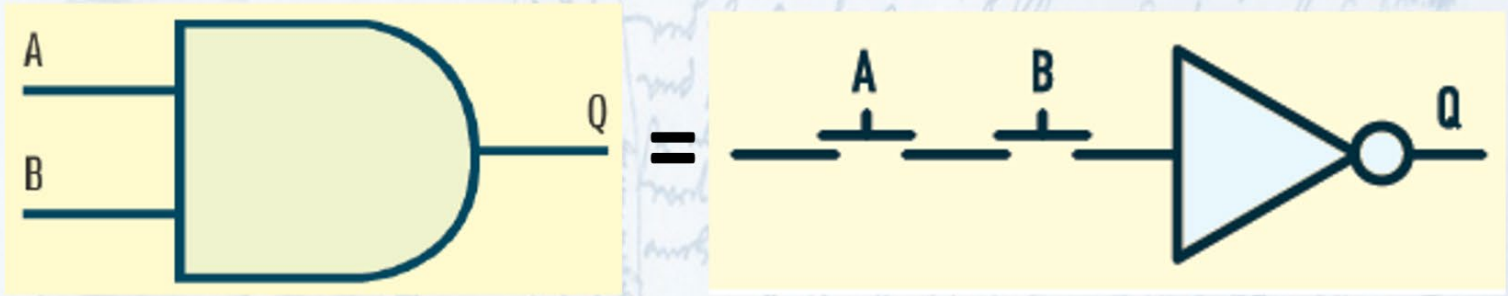
Risk has increased from 10% to 19%



$$P(A \cup B \cup C \cup D) = P(A)+P(B)+P(C)+P(D)-P(A \cap B)-P(A \cap C)-P(A \cap D)-P(B \cap C)-P(B \cap D)-P(C \cap D)+P(A \cap B \cap C)+P(B \cap C \cap D)+P(A \cap C \cap D)+P(A \cap B \cap D)-P(A \cap B \cap C \cap D)$$

Bayes and the 2-Man Rule: AND

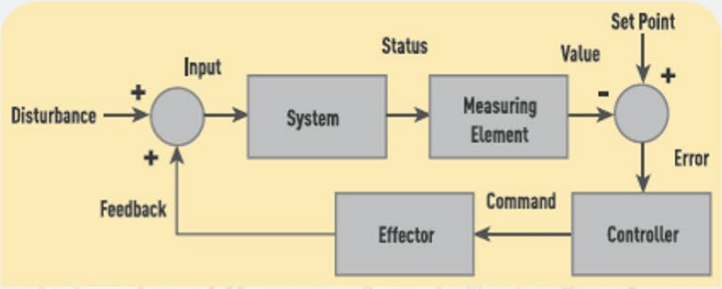
- Again, Both Alice and Bob have a Trust Factor of 0.9
- But… how long does it take Bob to agree with Alice to get to a TF of 0.99?
- A minute? A lunch hour? A weekend or holiday?



$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$
$$P(0.9 \text{ and } 0.9) = P(0.9) + P(0.9) - P(0.9 * 0.9)$$
$$= 1.8 - 0.81$$
$$= 0.99$$

Bayes and the Time-Based Flip-Flop

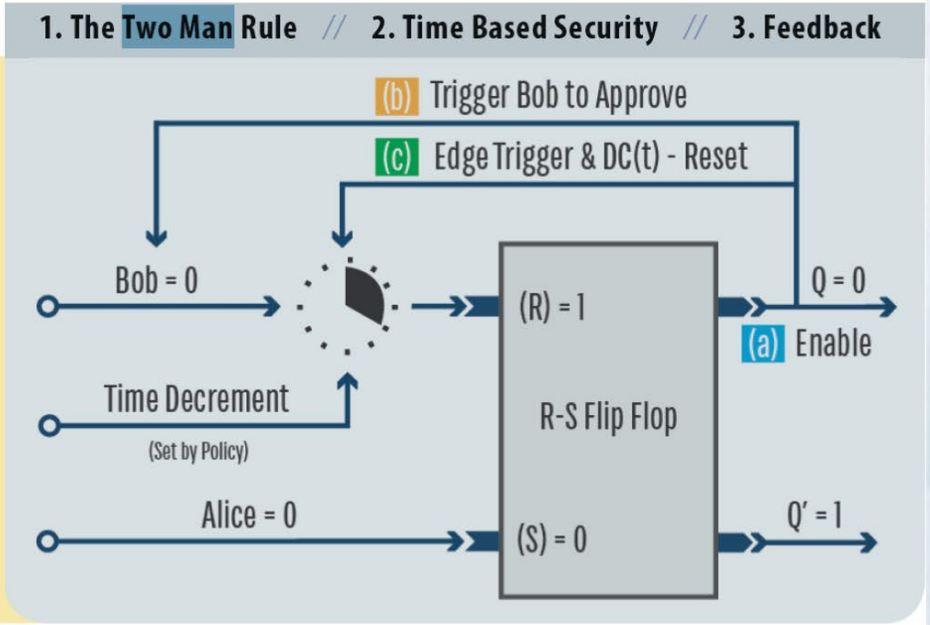
- Continuously Variable
- Min-Max
- Adjustable time-based weighting



Truth Table: TB-Flip-Flop

Alice (Set)	Bob (Approve)	Decrement(t)	Q = Enable
0	0	OFF	0
0	0	t > 0	0
0	0	t = 0	0
1	0	OFF	1
1	0	t > 0	1
1	0	t = 0	0
1	1	OFF	1
1	1	t > 0	1
1	1	t = 0	1
0	1	N/A	0
0	1	N/A	0
0	1	N/A	0

1. Alice = S = 0 = low.
2. Bob's input is Lo, or 0, and the R-input of the flip-flop = 1 = high. (Initial stability)
3. Q = 0 (Q' =1, and is useful in many applications.)
4. Decrementing Clock Time = DC(t) = X.
5. From a memory standpoint, the initial state represents a bit 0.



Adjusting Probability with Time

- 2 Man Rule Example
  - Scalable
- Feedback time for the decrementing clock clearly influences the probabilities of Trust and Risk.

As DC(t) → MA(t), Risk Reduction → 0%
and
As DC(t) → 0, Risk Reduction → 100%

Fig. 5F

In these charts, we see the effects of feedback time on TF(ab) when TF(a) ≥ TF(b). MA(t) is arbitrarily set to 10^3 seconds.

Any entity required to approve a primary decision must have an equal or greater level of trust than the original decision maker. This becomes especially obvious when:

TF(b) ≥ TF(a) *and*
TF(a) → 1.0 *and*
TF(b) → 1.0 *and*
DC(t) → 0 *then*
Risk Reduction → 100%

2MR – AND – with Feedback: Case #1

	Alice	Bob	Alice & Bob		MA(t)
					1000
TF	0.90	0.90	0.99		
Risk	0.10	0.10	0.01		
DC (seconds)	1.00		999.00		1,000.00
Trust Units	0.90		989.01	MA - TF >	0.9899
Risk Units	0.10		9.99	MA - Risk >	1.01%
Risk Reduction					89.9%

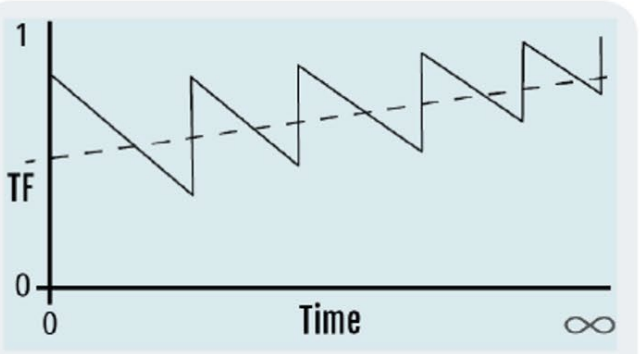
2MR – AND – with Feedback: Case #2

	Alice	Bob	Alice & Bob		MA(t)
					1000
TF	0.90	0.90	0.99		
Risk	0.10	0.10	0.01		
DC (seconds)	100.00		900.00		1,000.00
Trust Units	90.00		891.00	MA - TF >	0.9810
Risk Units	10.00		9.00	MA - Risk >	1.90%
Risk Reduction					81.0%

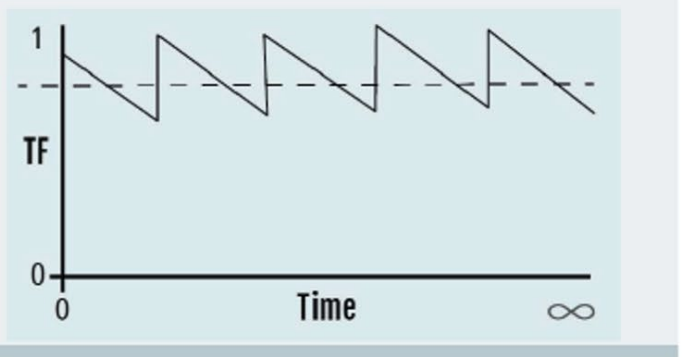
2MR – AND – with Feedback: Case #3

	Alice	Bob	Alice & Bob		MA(t)
					1000
TF	0.90	0.90	0.99		
Risk	0.10	0.10	0.01		
DC (seconds)	700.00		300.00		1,000.00
Trust Units	630.00		297.00	MA - TF >	0.9270
Risk Units	70.00		3.00	MA - Risk >	7.30%
Risk Reduction					27.0%

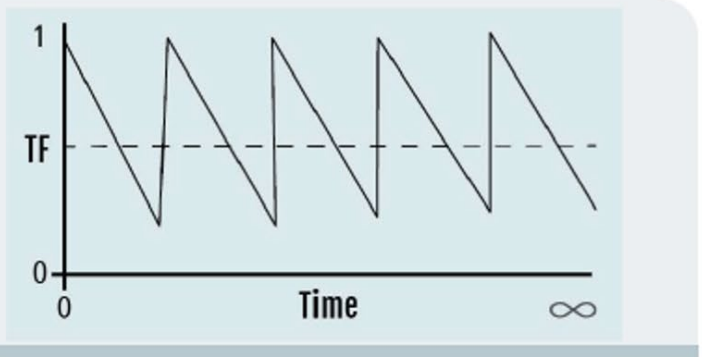
What Does Probabilistic Security Look Like?



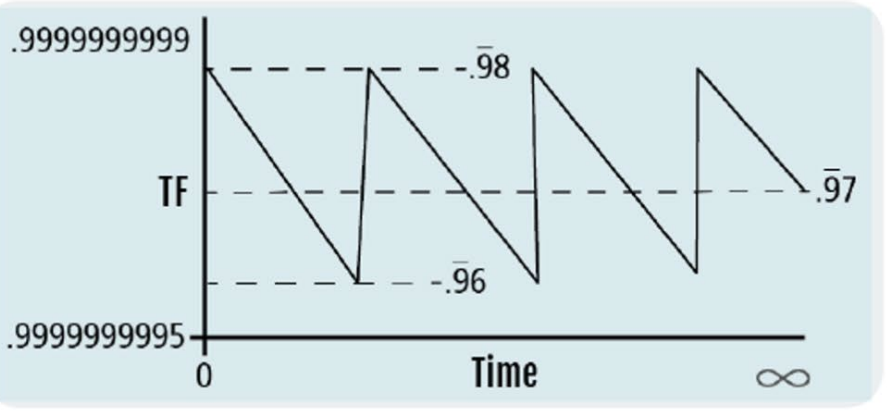
Trust must be earned over time.



Security = .8 ± . 1/ms (TF Min-Max Range = .9 ↔ .7)



Security = .5 ± .4/ms (TF Min-Max Range = .9 ↔ .1)

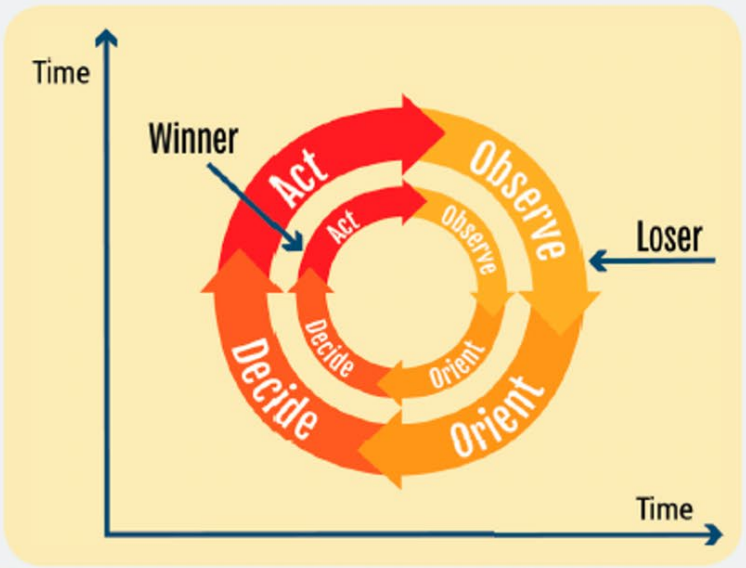


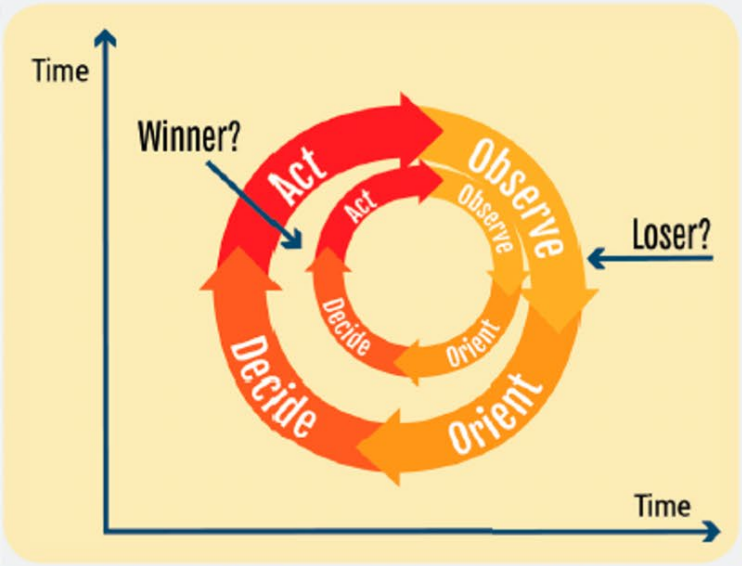
$.9999999999 = .\overline{9}_{10} = (1 - 10^{-11})$

$.999999999 = .\overline{9}_{9} = (1 - 10^{-10})$

.9999999995 ± .0000000002/ms = (.995 ± 2)/ms
= .9995 ± .0002/ms = (.935 ± 2)/ms

Winning…Probably…





If **A/L(t) > D(t) + R(t),**
Defense wins by **A/L(t) - [D(t) + R(t)],**
thus **L(t) < [D(t) + R(t)] < A/L(t)**

If **A/L(t) < D(t) + R(t),**
Offense wins by **[D(t) + R(t)] - A/L(t),**
thus **L(t) > [D(t) + R(t)] > A/L(t)**

L-Win(t) = O1(t) + O2(t) + DE(t) + Act(t) < L-Lose(t) = O1(t) + O2(t) + DE(t) + Act(t)

Winning at cybersecurity requires that your OODA-loop is faster than your adversary's.

Probabilistic Nature of Security laid bare

Much of security is managing known unknowns

The 'when' not 'if' of an attack, the probabilistic accuracy of a vendor's product or human's reaction time, or the likelihood that your OODA loop has high enough resolution for the threats you are managing.

The Future work of ANS

Evolutionary Game Theory – playing the 'security game' across the whole field of attackers, at the same time, and winning!

You Don't Need The Maths Yourself

But you SHOULD understand the basics of non-certainty.

Someone on your team MUST be able to apply probability to ANY network security evaluation, measurement and TRUST.

Network Security Is A Bear

This is the basis of Analogue Network Security.

V(Hunter 1) < V(Bear) < V(Hunter 2)

What Can You Do Now?

- View Enterprise with an Analogue Slant
- Apply Probability to Security
- Think of Security as a Time Function
- Add Trust to Risk Equations
- Use the Maths
  - Measure Your Detection/Reaction Process. Compare Products in Test Bed
  - Demand Hard Data From Your Vendor!

Thank You!

Comments? Questions?

Winn Schwartau
winnschwartau@gmail.com
Ph. +1.727.393.6600
www.WinnSchwartau.com
@WinnSchwartau

Dr. Mark Carney
iDelta0@gmail.com