

Policy Makers & Provable Security



Winn Schwartau

Security Theoretician

Founder of The Security Awareness Company, InfowarCon, and Security Experts

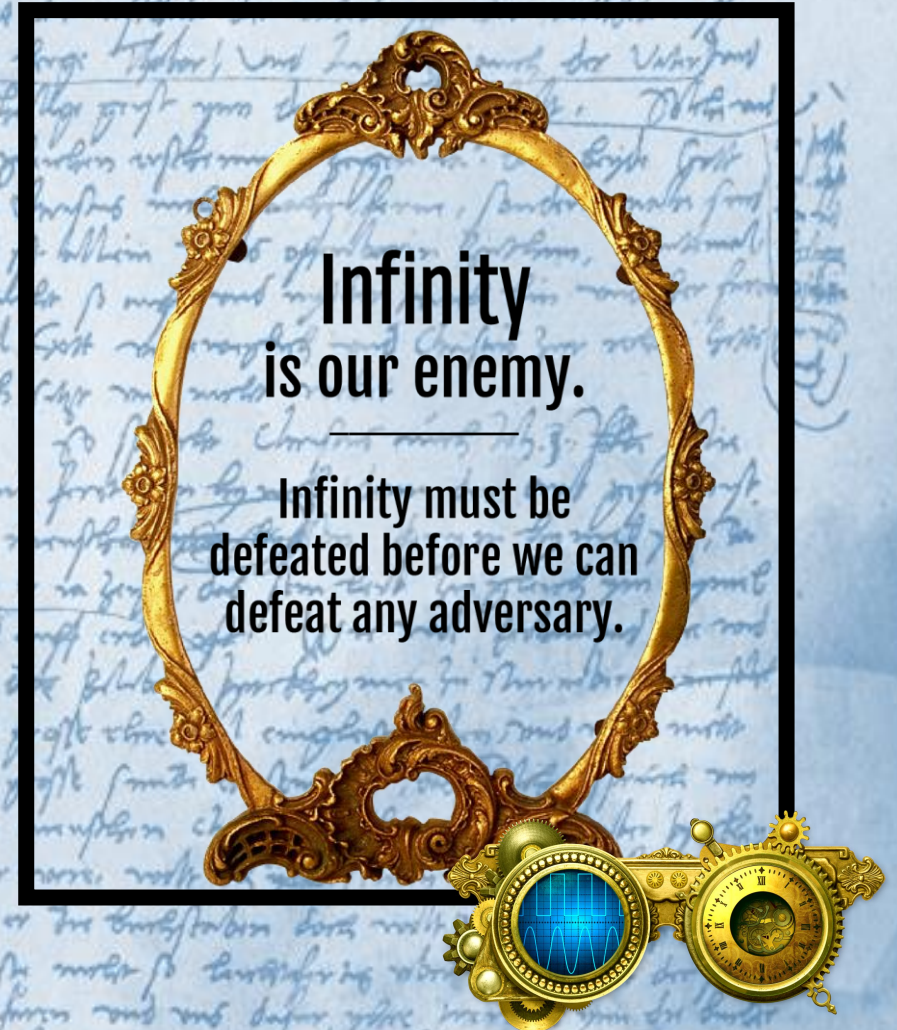
**19th Annual Privacy and Security
Conference**
**Security & Privacy: A Global
Evolution**
Feb. 7-9, 2018, Victoria, BC

PRIVACY &
SECURITY
CONFERENCE

 | reboot
COMMUNICATIONS LTD

Analogue Network Security for Policy Makers

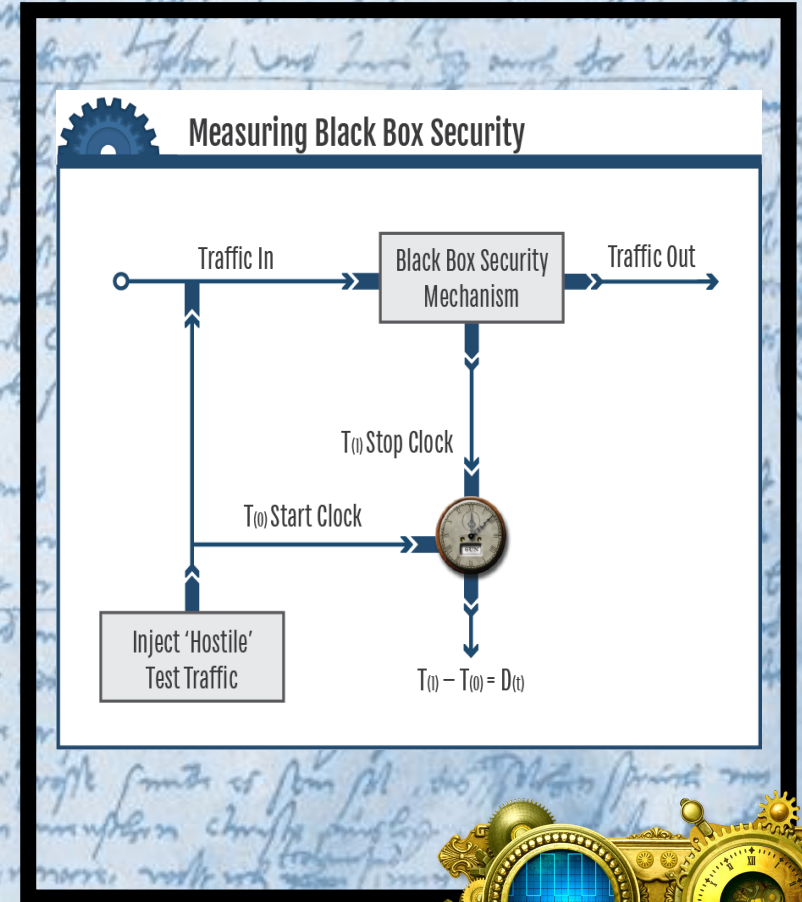
- Security is NOW measurable. Code, Networks, People and Process.
- We KNOW how to measure and compare security products... quantitatively.
- We CAN solve Phishing, SPAM, DDoS, Data Exfiltration +++ ... Mathematically.



What Do Policy Makers Do Now?

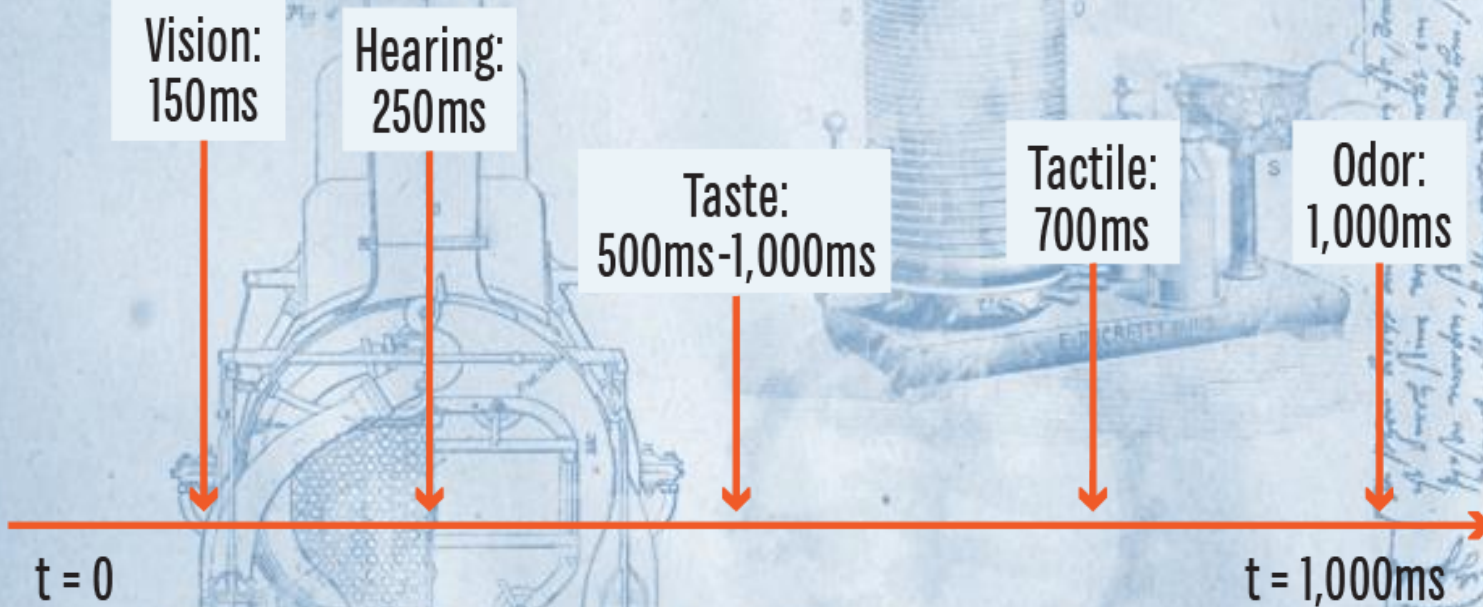
No More Guessing: Policy Makers Can Now ...

- Accurately Compare Products
- Hold Entities Responsible
- Develop Meaningful Standards
- Enact Effective Legislation
- Translate Risk, Security & Privacy into Metrics
- Use Provable Math
- Visualize Security



It's All About Time

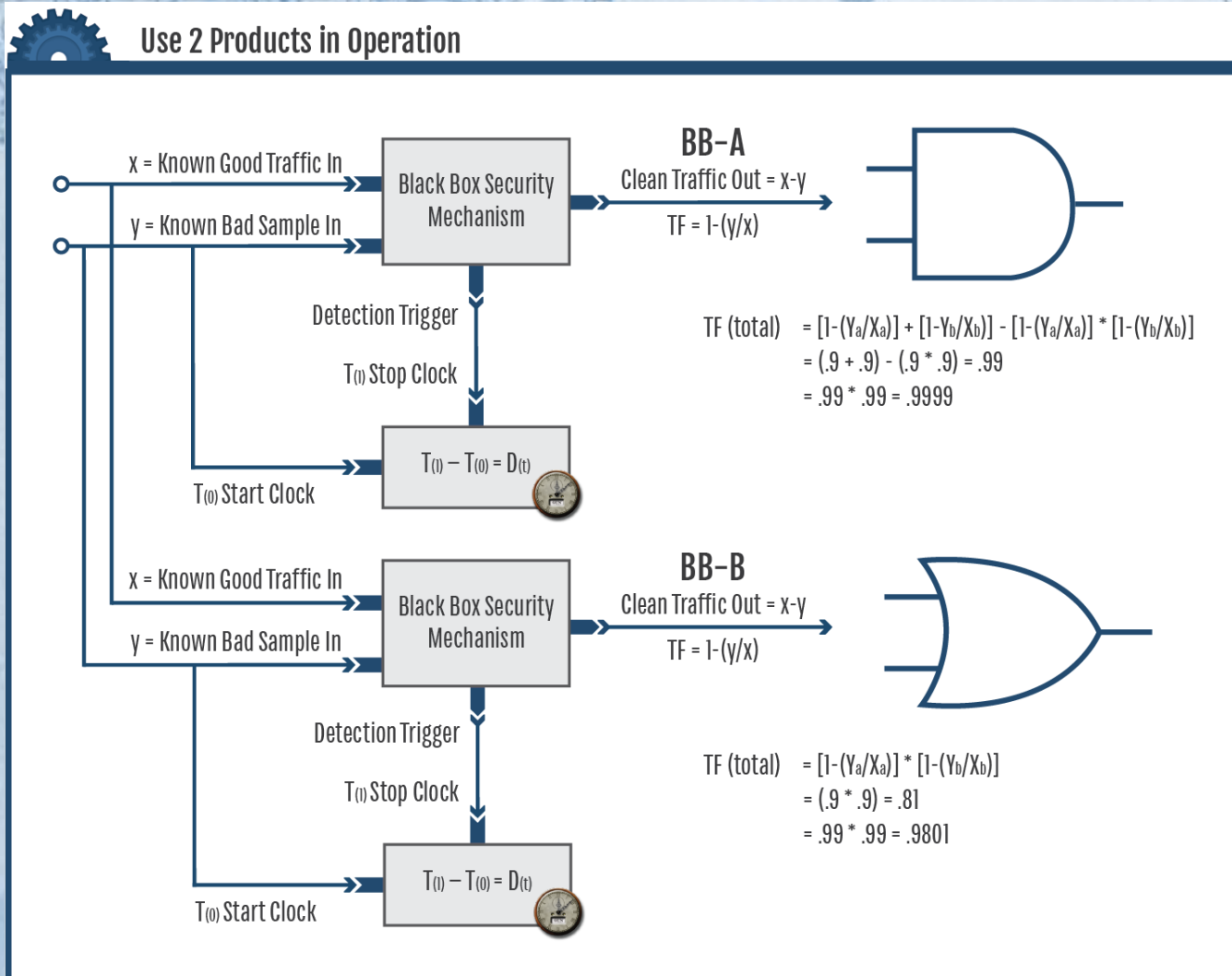
Range of Human Sense Detection Times



- Security & Privacy Are Continua
- Detection Should Approach 0-Time
- Reaction Should Approach 0-Time



Comparing 2-Products' Effectiveness

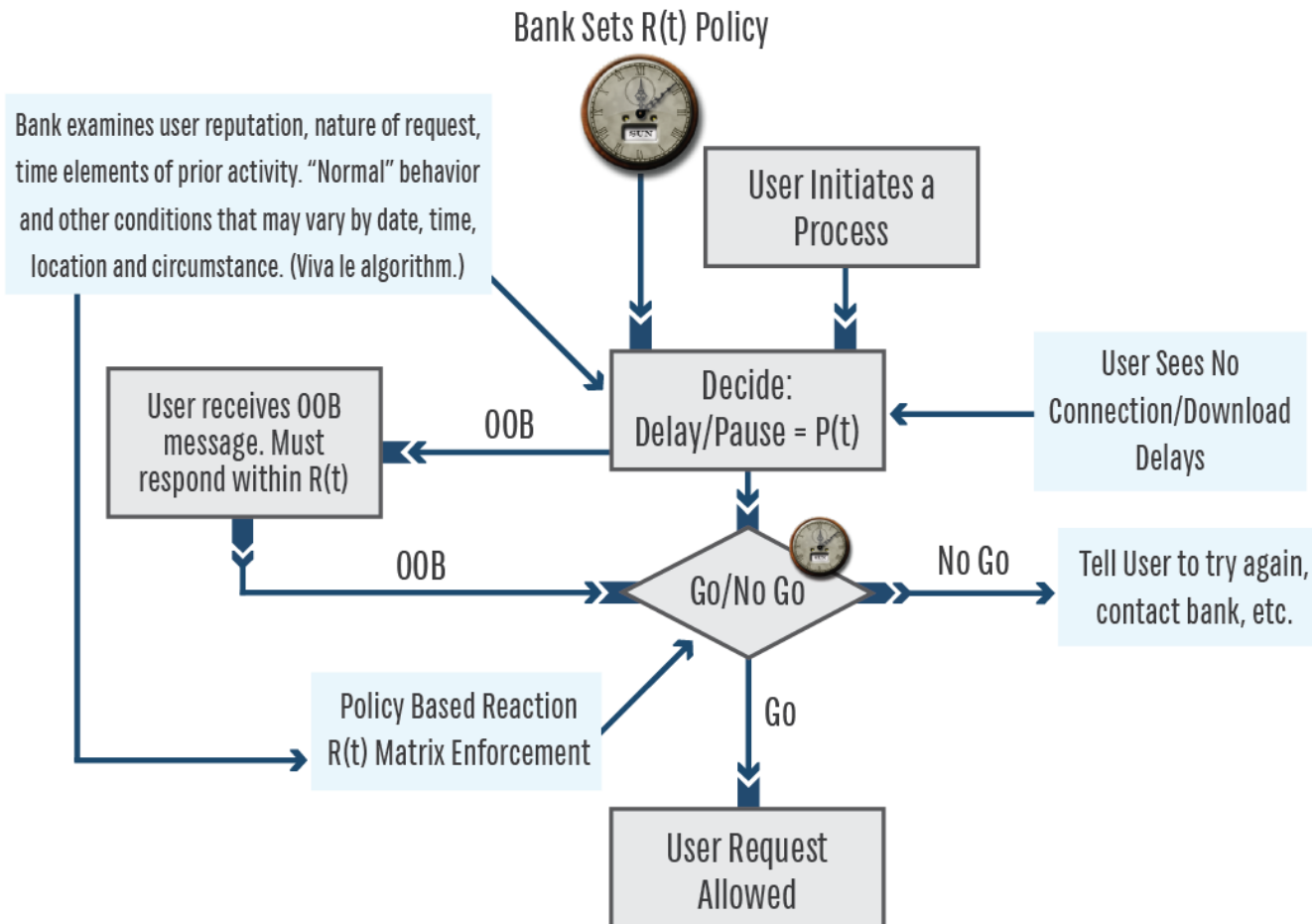


Using More Than One
Detection Product
Is NOT ALWAYS the
Right Approach.



2MR & Strong Authentication

Time Based Out of Band Re-Authentication

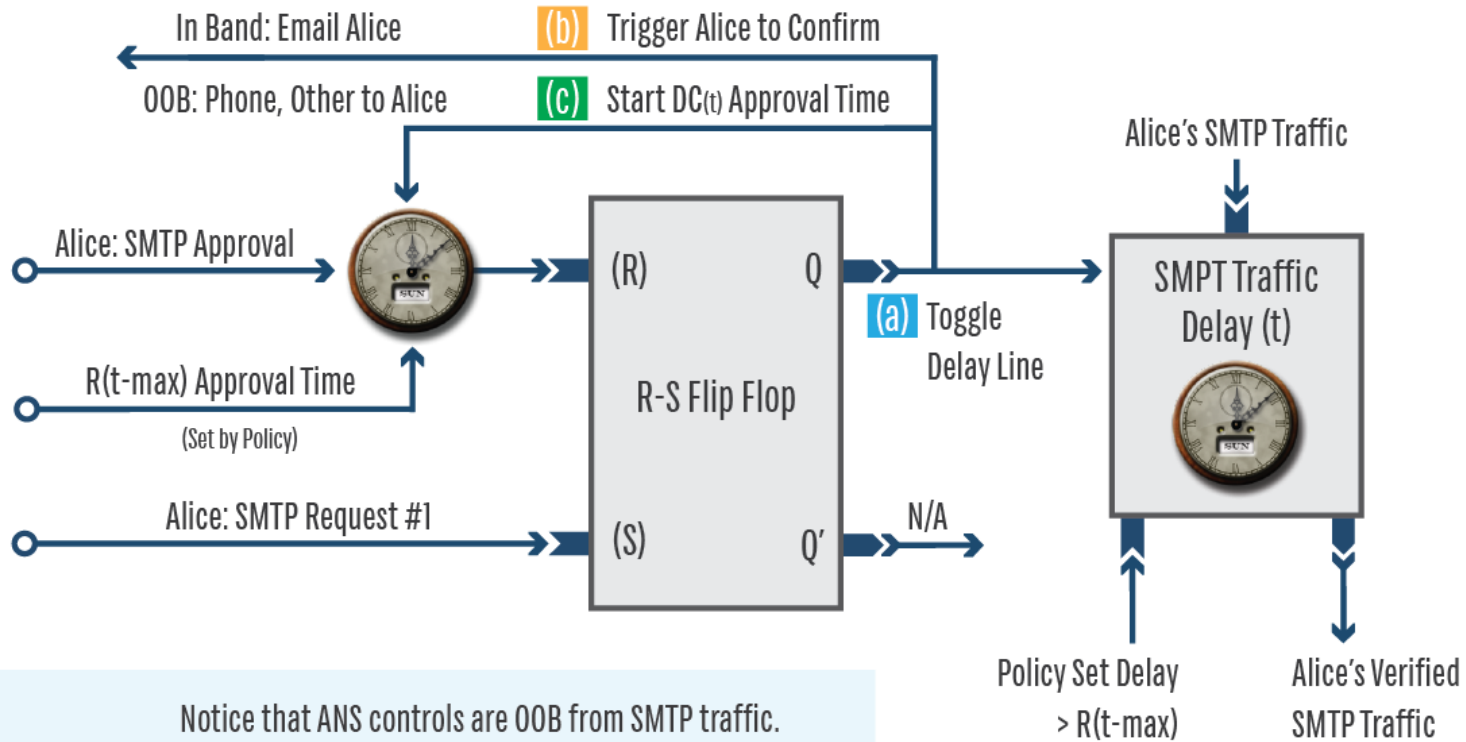


- Policy Driven Risk
- Measurable
- Provable
- Math First
- Build Second



Mitigate Data Exfiltration

SMTP Ass Saver: Alice to Alice



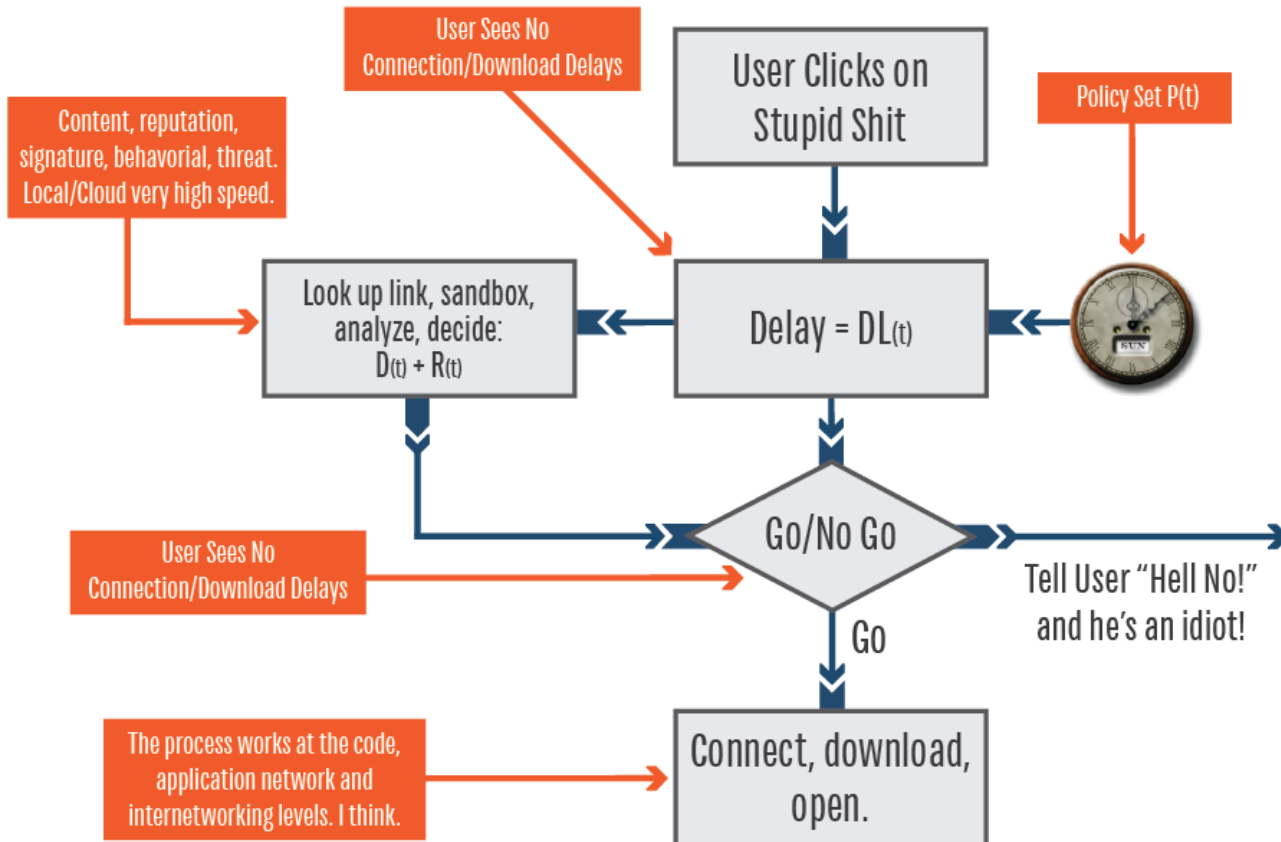
- BW Compression
- Data Padding
- Time-Based Feedback

1GB sec	Time	Data Extricated	
	1 sec	1 GB	
	1 min	60 GB	
	1 hr	3.6 TB	
100MB sec	Time	Data Extricated	90% reduction in data extraction
	1 sec	100 MB	
	1 min	6 GB	
	1 hr	360 GB	
10MB sec	Time	Data Extricated	99% reduction in data extraction
	1 sec	10 MB	
	1 min	600 MB	
	1 hr	36 GB	
1MB sec	Time	Data Extricated	99.9% reduction in data extraction
	1 sec	1 MB	
	1 min	60 MB	
	1 hr	3. GB	



Stop Phishing in (and with) Time

The Time Based Phishing Stopper



- Add Negative Time
- Security SKY ROCKETS!

Single Admin Examples of Trust Factor/Risk: Time = Infinity

	Alice	Alice	Alice	Alice	Alice
TF	0.90	0.95	0.70	0.60	0.10
Risk	0.10	0.95	0.30	0.40	0.90

2MR - AND - No Feedback: Time = Infinity

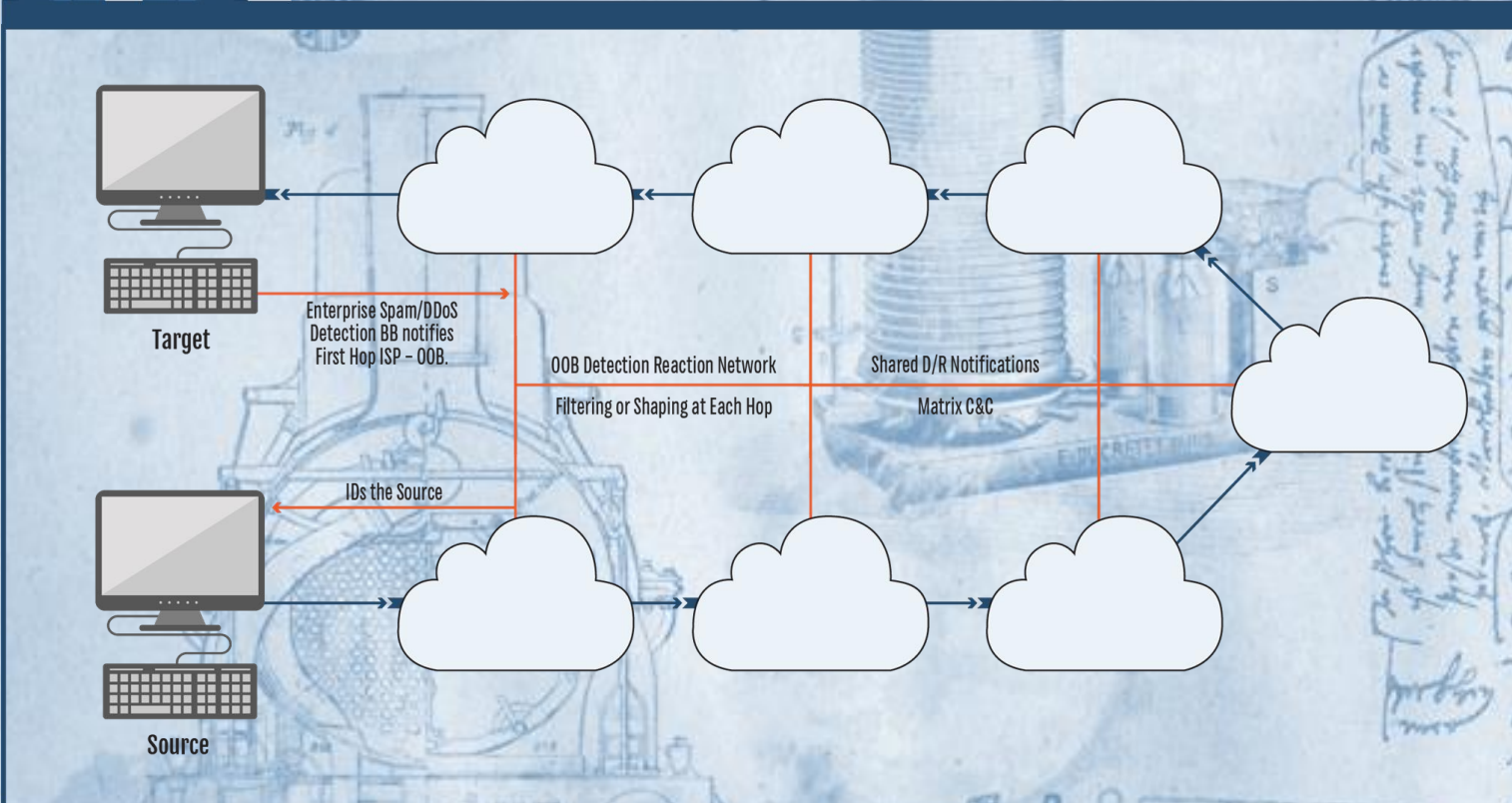
Example 1	Alice	Bob	Alice & Bob
TF	0.900	0.900	0.990
Risk	0.100	0.100	0.010
Risk Improvement			90.0%

Example 2	Alice	Bob	Alice & Bob
TF	0.90	0.95	0.995
Risk	0.10	0.05	0.005
Risk Improvement			95.0%

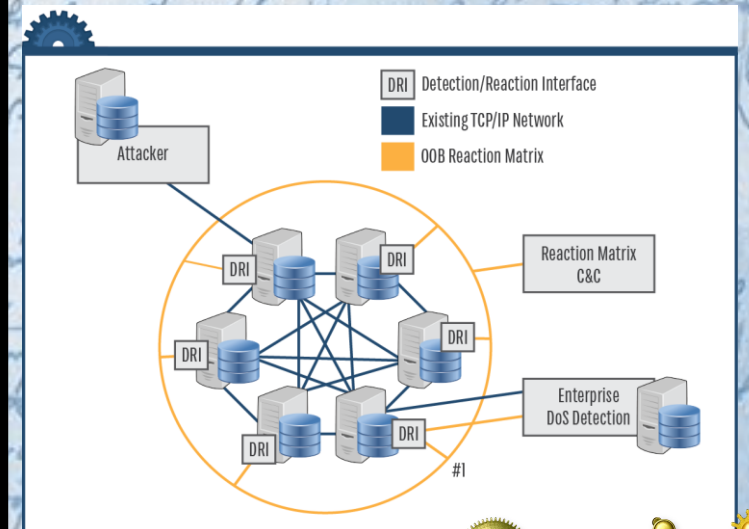
Example 3	Alice	Bob	Alice & Bob
TF	0.70	0.80	0.940
Risk	0.30	0.20	0.060
Risk Improvement			80.0%



Stop DDoS & Spam With Time

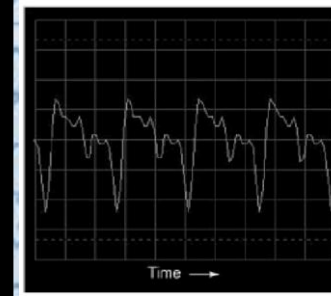
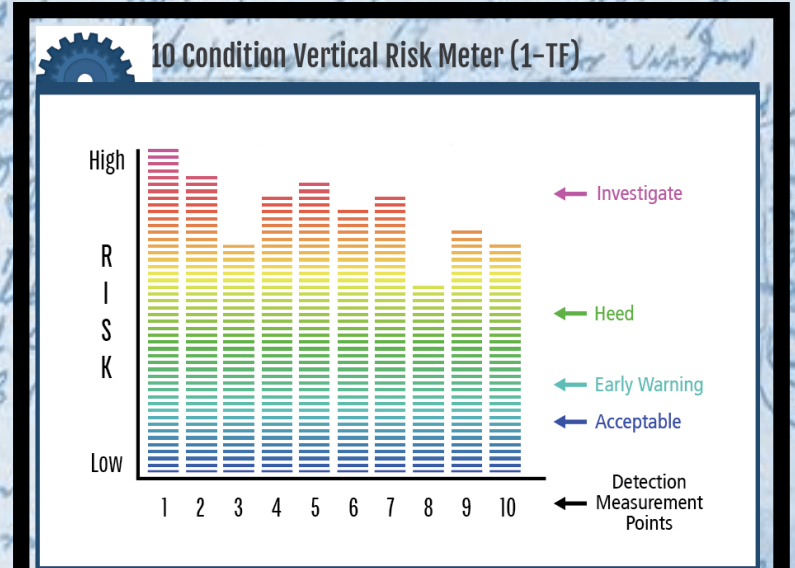
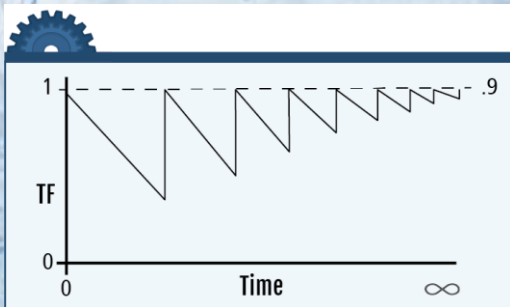
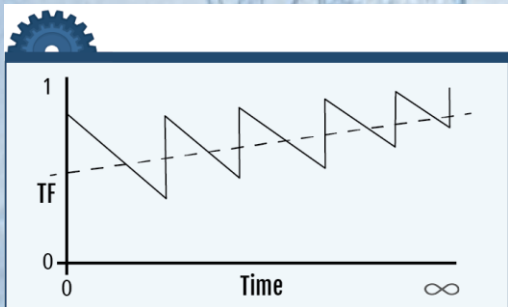
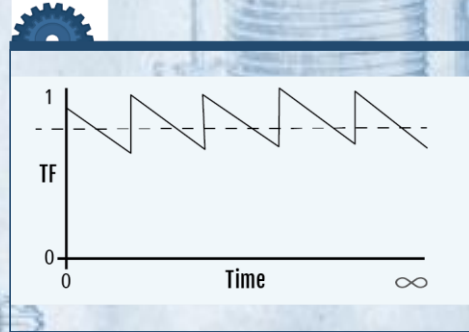
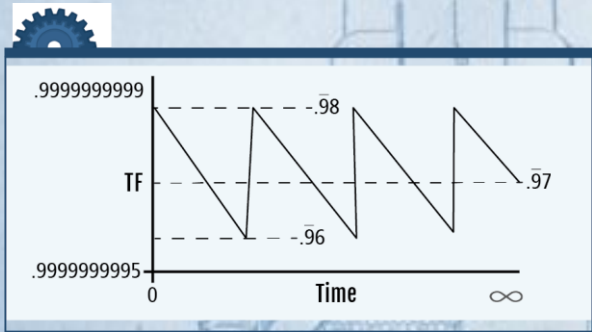
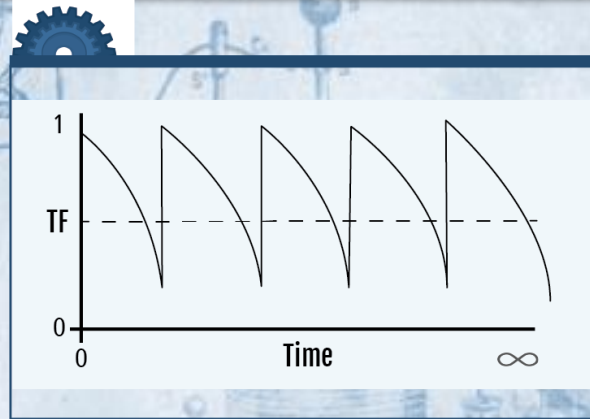
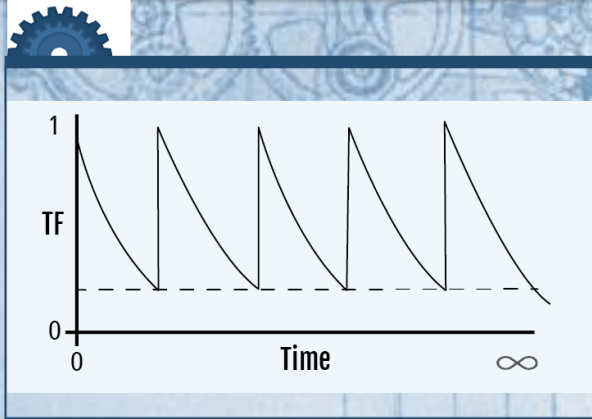


- Closed System
- OOB Comm
- Reaction Matrix

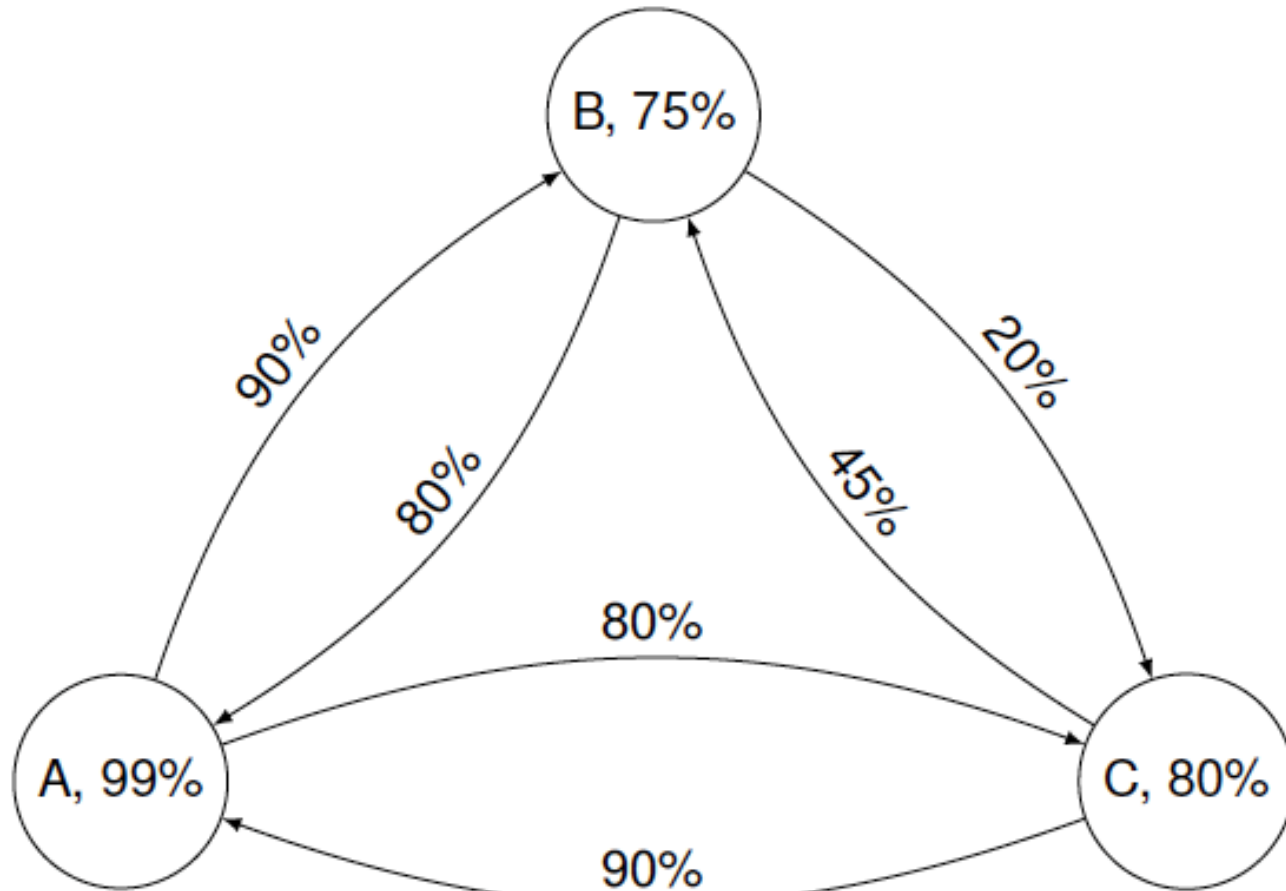


What Does Security Look Like?

Metric: $(.995 \pm .003)/\text{msec}$



Security Looks Like...Trusted Relationships



Where $TF(a) > TF(b)$

2MR - AND - No Feedback

Example 1	Alice	Bob	Alice & Bob
TF	0.90	0.90	0.9900
Risk	0.10	0.10	0.010
Risk Improvement			90.0%

Example 2	Alice	Bob	Alice & Bob
TF	0.90	0.85	0.7500
Risk	0.10	0.15	0.250
Risk Improvement			-150.0%

Example 3	Alice	Bob	Alice & Bob
TF	0.90	0.60	0.5000
Risk	0.10	0.40	0.500
Risk Improvement			-400.0%

The Formulas

$$TPR(T) = \int_T^\infty f_1(x) dx$$

1. $\delta(t, t+1) = rTF_t(A)$
2. $\delta(t, t+1) = e^{-(t/S)} - e^{-(t+1/S)}$
3. $\delta(t, t+1) = s \cdot \log_e(1-t)^8$

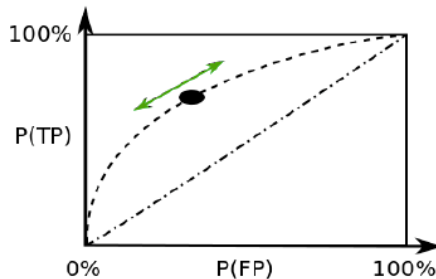
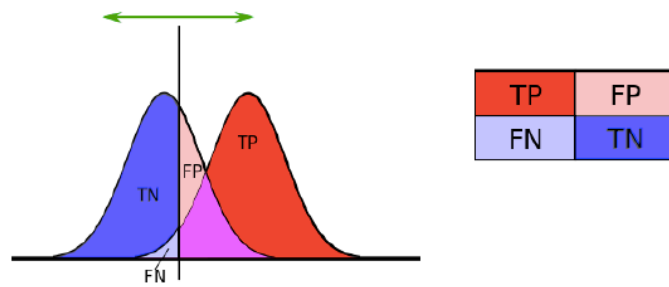
$$\frac{1}{n} \sum_{i=1}^n x_i \text{ and } \sqrt[n]{\prod_{i=1}^n x_i}$$

$$s = \sum_{i=1}^n \binom{n}{i} = \sum_{i=1}^n C(n, i)$$

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

We can now add in our weights from $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}$ as follows:

$$P_{ANS}(A \cup B \cup C) = \sigma_1 P(A) + \sigma_2 P(B) + \sigma_3 P(C) - \sigma_4 P(A \cap B) - \sigma_5 P(A \cap C) - \sigma_6 P(B \cap C) + \sigma_7 P(A \cap B \cap C)$$



$$\text{for } 1 \leq j \leq s, \sum_{k=1}^n \left((-1)^{k-1} \sum_{\substack{I \subset \{0,1,\dots,n\} \\ |I|=k}} \sigma_j P\left(\bigcap_{i \in I} A_i\right)\right)$$

$$TF_{t+1}(A) = TF_t(A) + D(TF_t(A))$$

$$D(TF_t(A)) = \frac{dTF_t(A)}{dt} = -\delta(t, t+1) + I(TF_t(A), x_1, x_2, \dots, x_n)$$

Now What Policy Makers?

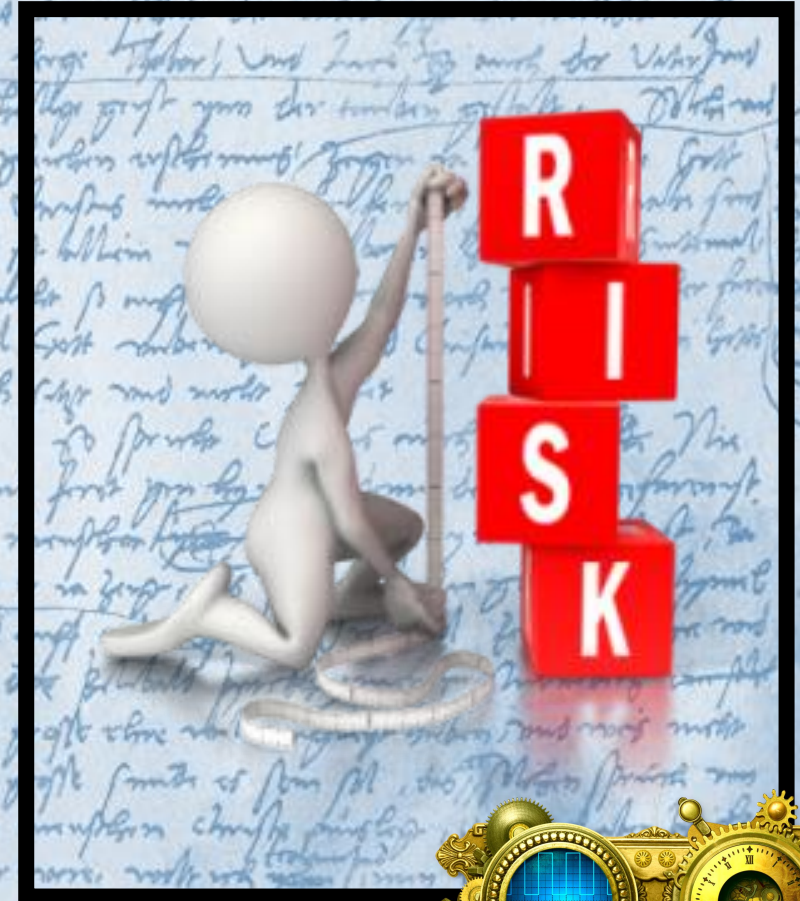
- Policy Driven Boundaries
- Strong Mathematical Justifiability
- Creates a Single Metric for
 - Risk, Privacy, Security & Trust
- Scalable
 - Code, networking, internetworking, human
- Vendor Performance Accountability
- Provable Systems Accountability
- Measurement
 - Code, Networking, People, Process



Let's Make Policy

The Top-10 Notional Policies

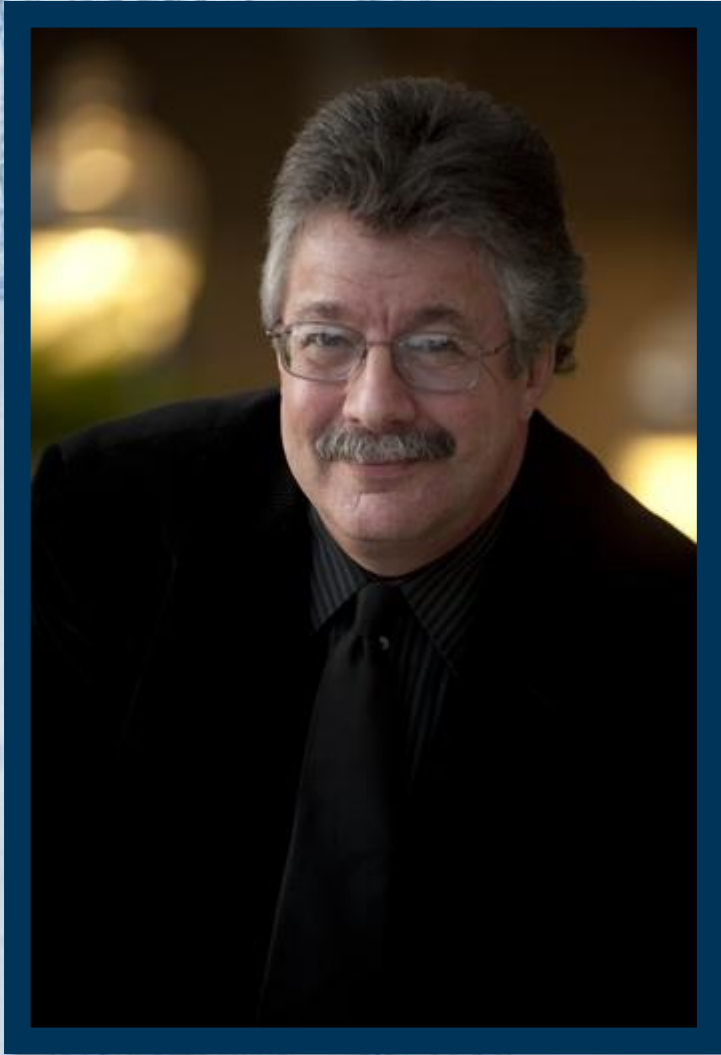
- Privacy
- Security
- Risk
- IoT
- New Technology



What's Next?

- The foundational mathematical formalization is firm.
- Determine initial privacy applications
- POC in VMs
- Research & Application
- Open Source
 - Commercial, Academic, Government
- Develop Standardized Protocols
 - Integrate with existing TCP/IP
 - Develop IoT





Comments? Questions? Responses?

Office: 615.541.6121

www.WinnSchwartzau.com

winn@securityexperts.com

