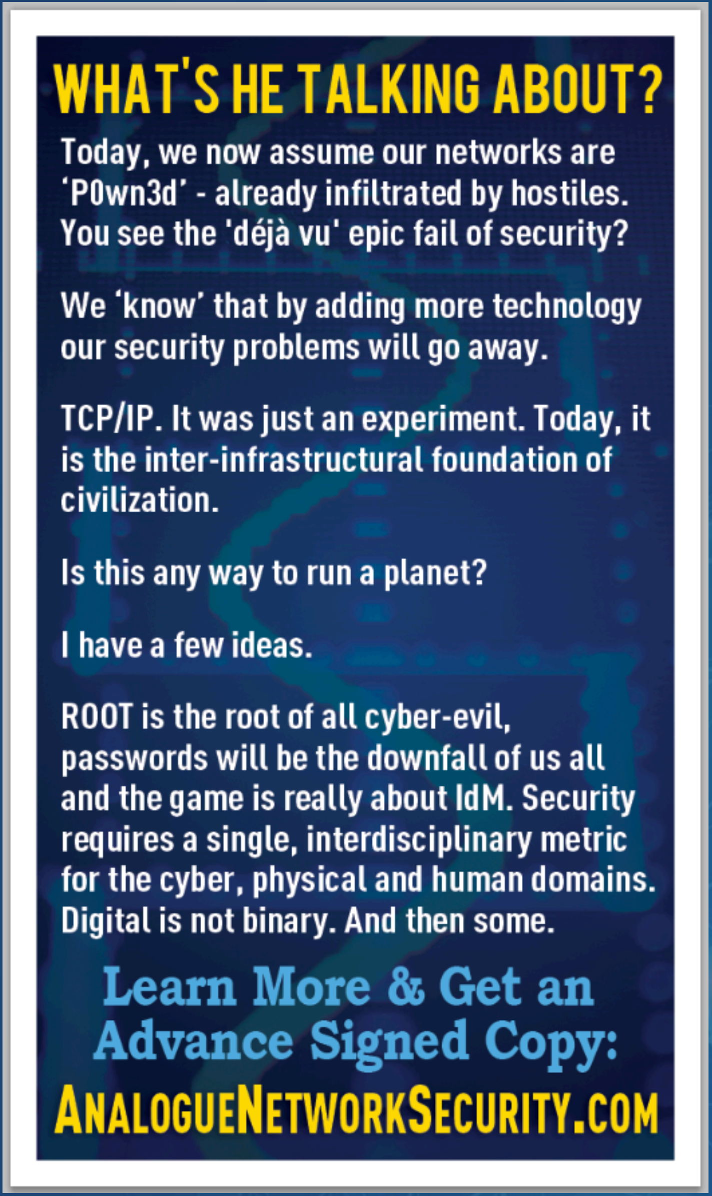
ANALOGUE NETWORK SECURITY

The Premise: Hack in Paris, 2015

- I may be right on some stuff. Probably wrong on other bits.
- Analogue is meant to help people think differently.
- This is the Hack in Paris 2015 version, and is subject to all sorts of changes as the book is finished.
- Please send me your ideas.
- Thanks! See you next year.
- For first edition signed copies of the book:

1ST Edition Signed Copies



WHAT'S HE TALKING ABOUT?

Today, we now assume our networks are 'P0wn3d' - already infiltrated by hostiles. You see the 'déjà vu' epic fail of security?

We 'know' that by adding more technology our security problems will go away.

TCP/IP. It was just an experiment. Today, it is the inter-infrastructural foundation of civilization.

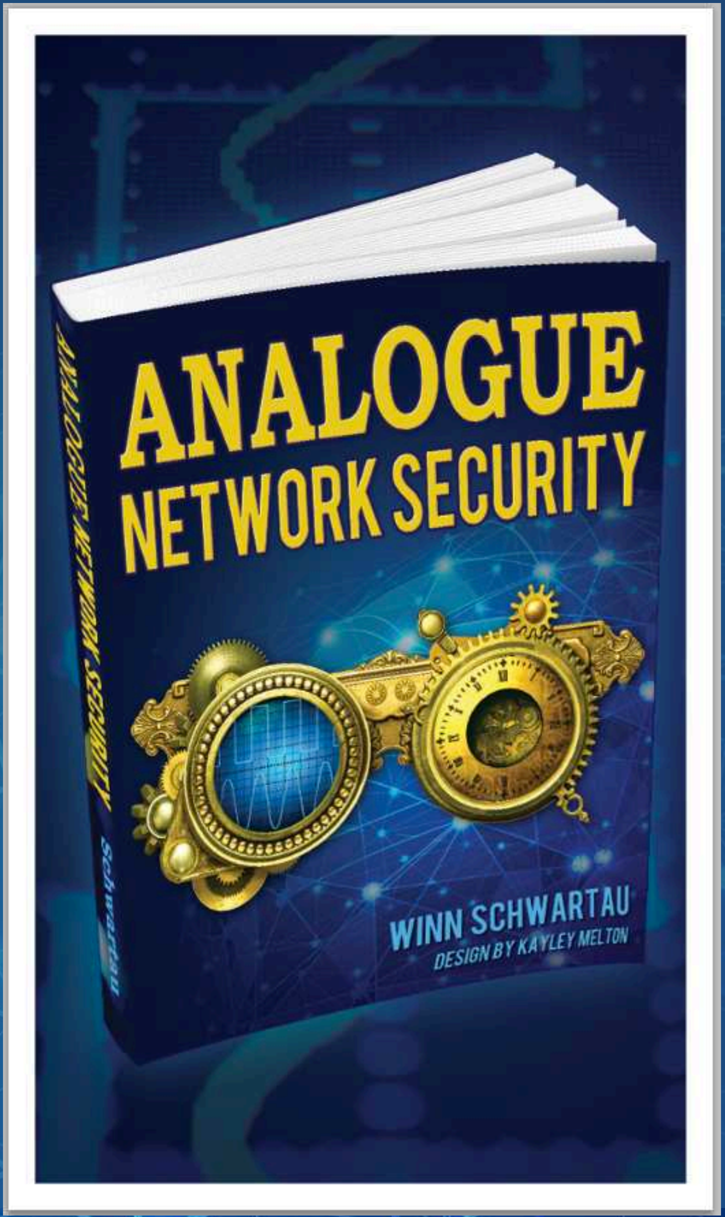
Is this any way to run a planet?

I have a few ideas.

ROOT is the root of all cyber-evil, passwords will be the downfall of us all and the game is really about IdM. Security requires a single, interdisciplinary metric for the cyber, physical and human domains. Digital is not binary. And then some.

Learn More & Get an Advance Signed Copy:

ANALOGUENETWORKSECURITY.COM



The World As It Is
<Le Sigh>

- Security is Broken. Abysmally so.
- TCP/IP was just an experiment.
    - We run the planet on it.
- Assume the bad guys are inside already.
- We 'know' newer, faster technology will *protect* networks and data.
    - (Same promises since 1980s)
- If You Can't Measure It, You Can't Manage It.

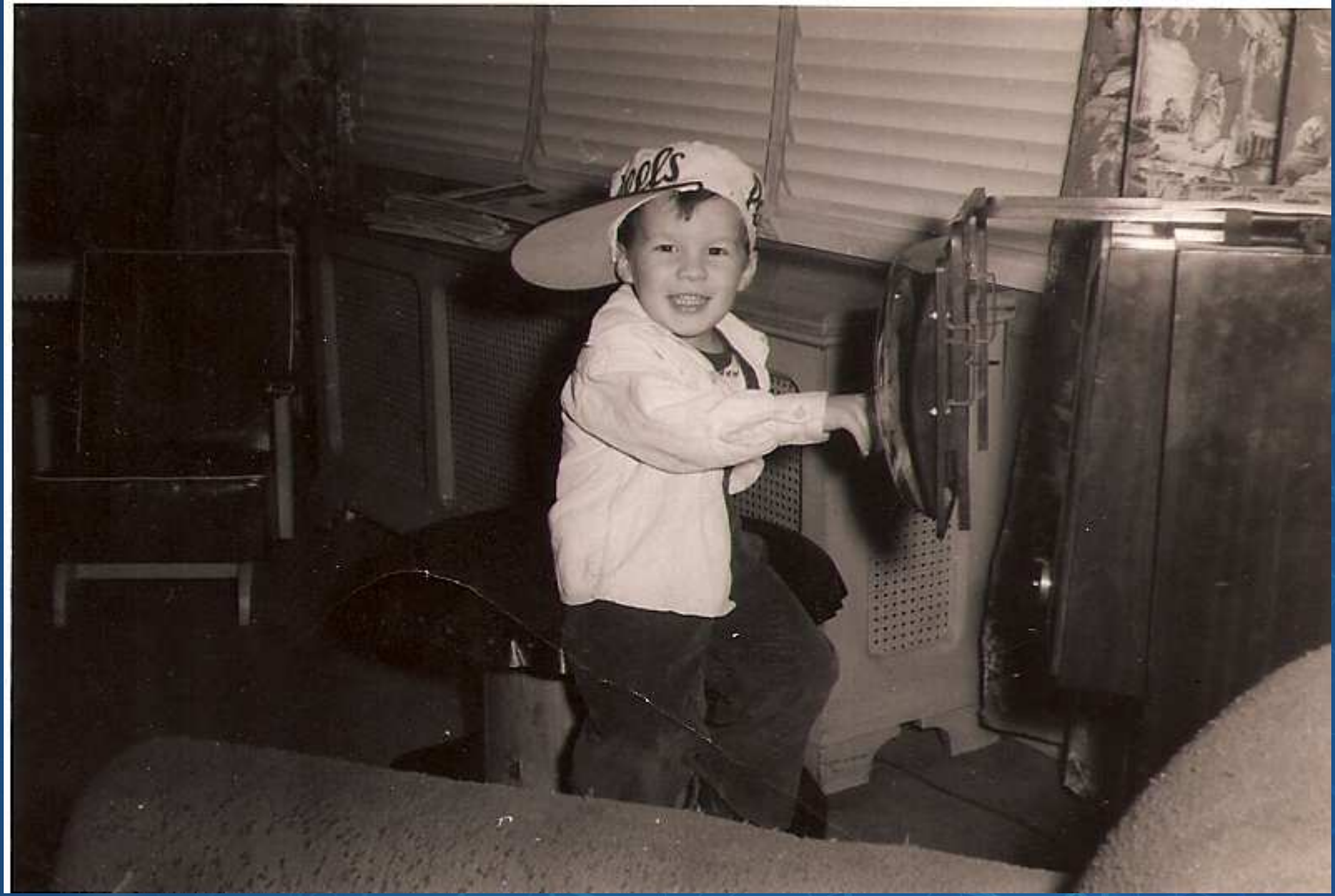
My Analogue Assessment

- Digital is Not Binary
- Security is Not Static
- No Common Metric: Risk, Security & Privacy
- We “Can’t” Measure Security. Or can we?
- Defense > Offense Is ‘Almost’ Possible

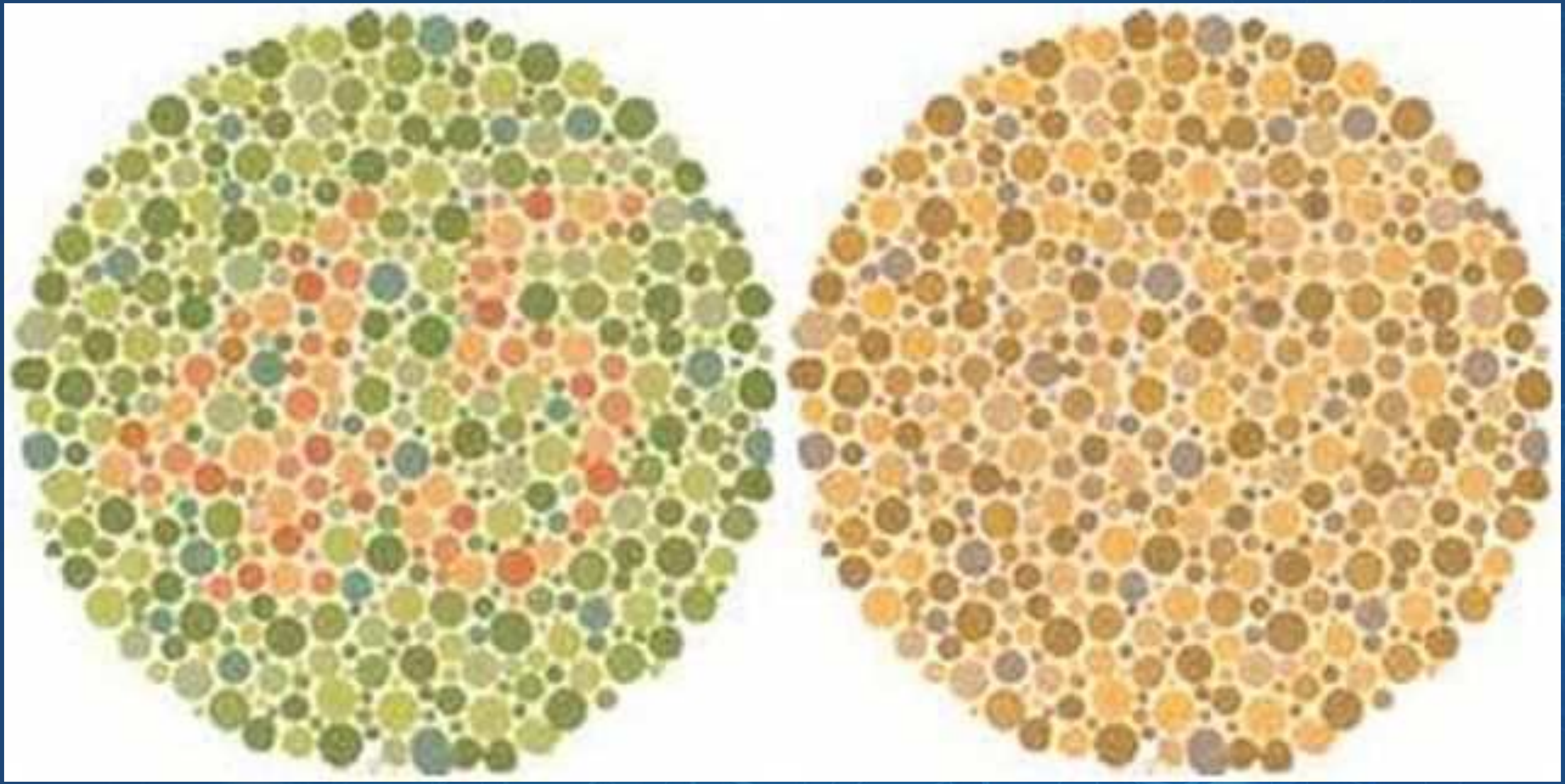
My Political Assessment

- Security Only Keeps the Good Guys Honest.
- Legislation, Regulations and Governance Require *Willingness* to Follow the Rules.
- Here Comes the IoT
- International Cooperation Can Solve Many Security Issues… if, and only if, Technology Comes First. Politics, Second.

Winn As Young TV Repairman



And Color Blind

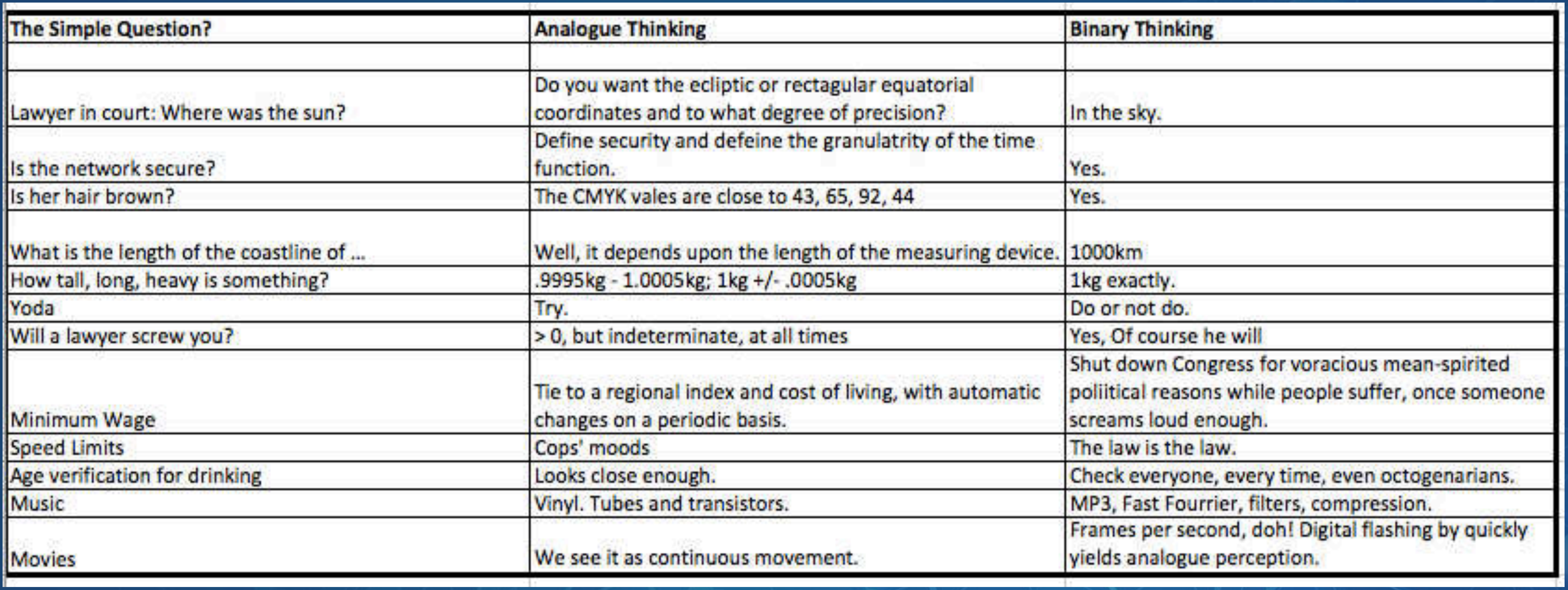


I Grew Up Analogue Rock'n'Roll: Complex Systems

Analogue: WTF?

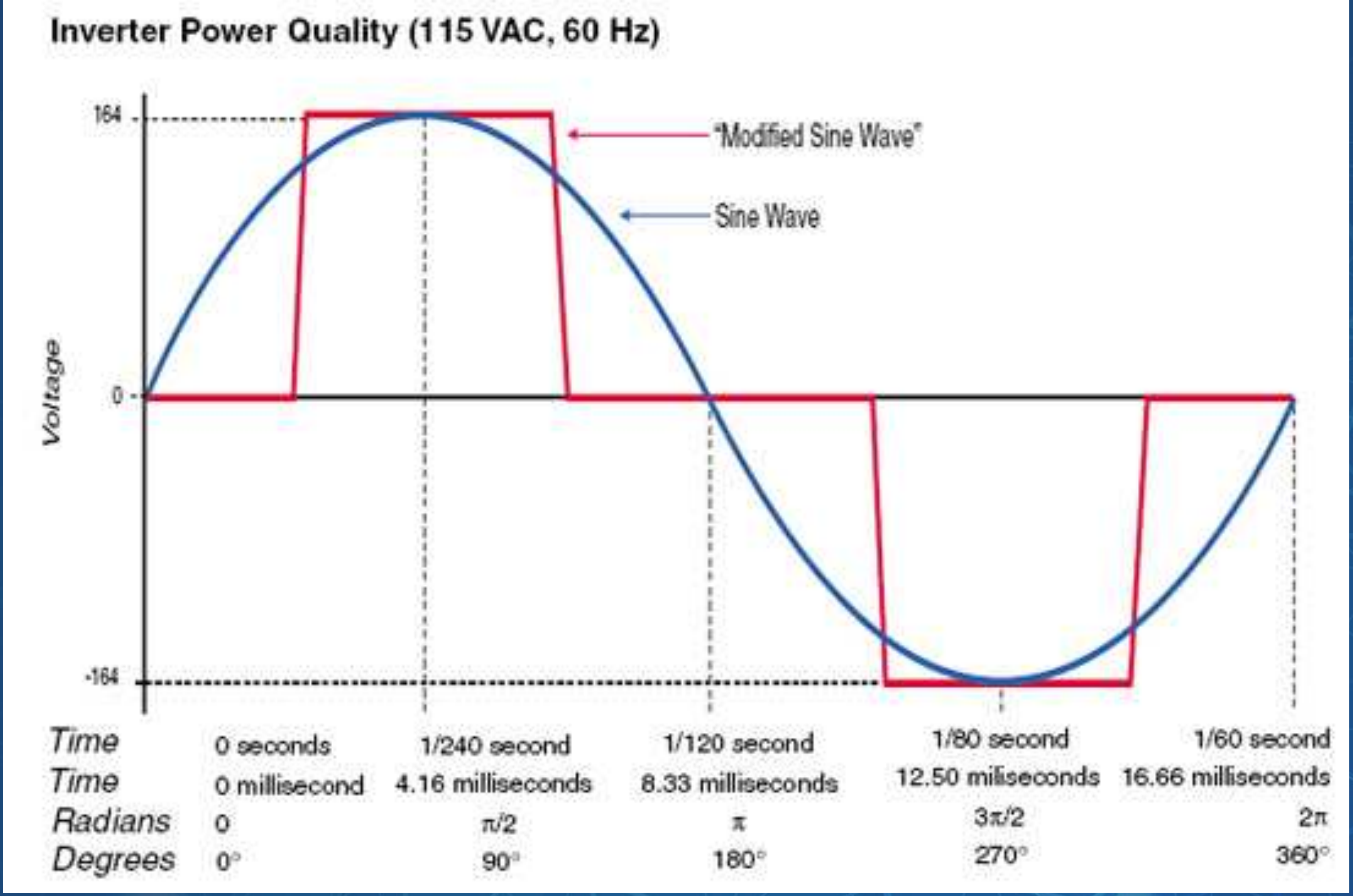
Continuously Variable & Dynamic

Is It Analogue?

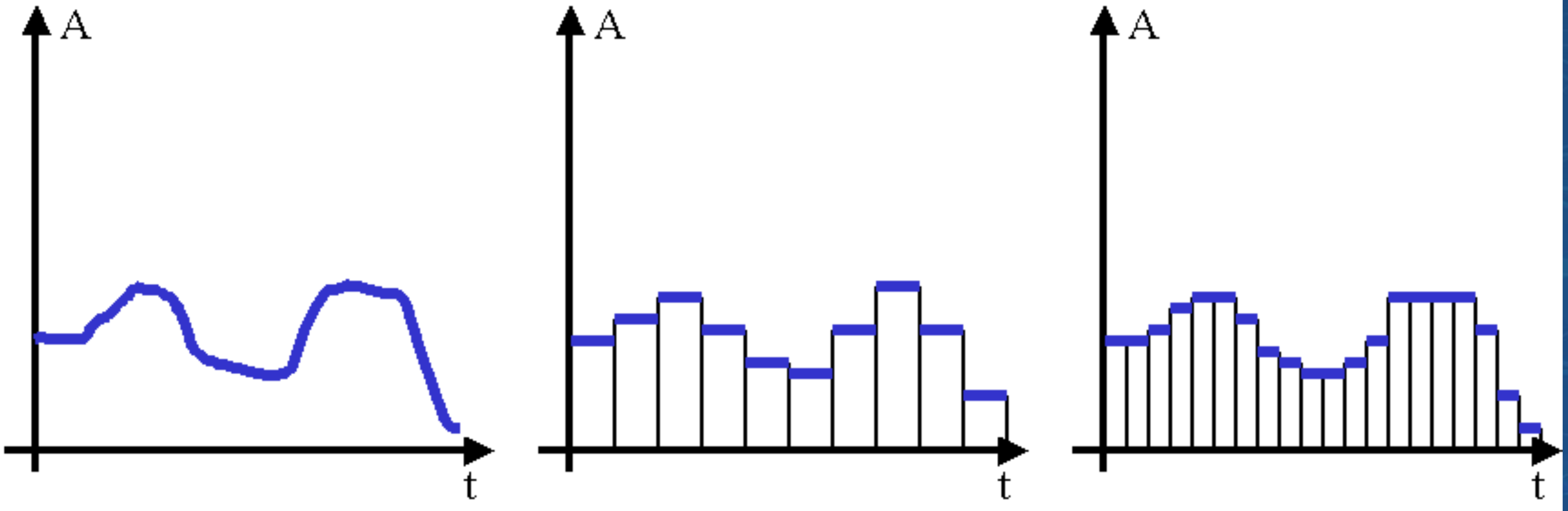


The Simple Question?	Analogue Thinking	Binary Thinking
Lawyer in court: Where was the sun?	Do you want the ecliptic or rectagular equatorial coordinates and to what degree of precision?	In the sky.
Is the network secure?	Define security and defeine the granulatrity of the time function.	Yes.
Is her hair brown?	The CMYK vales are close to 43, 65, 92, 44	Yes.
What is the length of the coastline of ...	Well, it depends upon the length of the measuring device.	1000km
How tall, long, heavy is something?	.9995kg - 1.0005kg; 1kg +/- .0005kg	1kg exactly.
Yoda	Try.	Do or not do.
Will a lawyer screw you?	> 0, but indeterminate, at all times	Yes, Of course he will
Minimum Wage	Tie to a regional index and cost of living, with automatic changes on a periodic basis.	Shut down Congress for voracious mean-spirited poliitical reasons while people suffer, once someone screams loud enough.
Speed Limits	Cops' moods	The law is the law.
Age verification for drinking	Looks close enough.	Check everyone, every time, even octogenarians.
Music	Vinyl. Tubes and transistors.	MP3, Fast Fourrier, filters, compression.
Movies	We see it as continuous movement.	Frames per second, doh! Digital flashing by quickly yields analogue perception.

Analogue = Continuously Variable



Averaging Quanta: Plank’s ‘d’

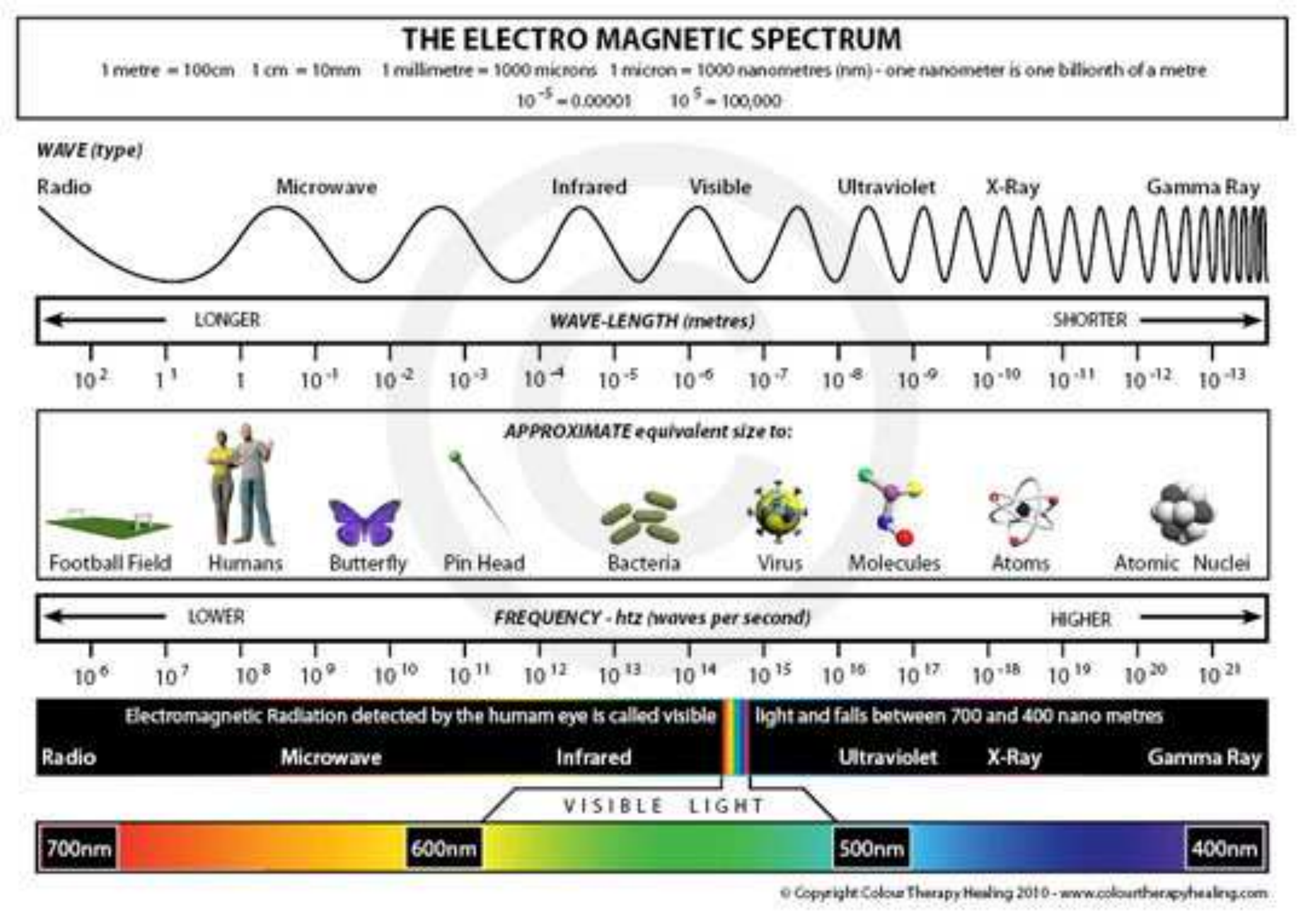


Analog signal – continuously varying

Digital signal – large time divisions

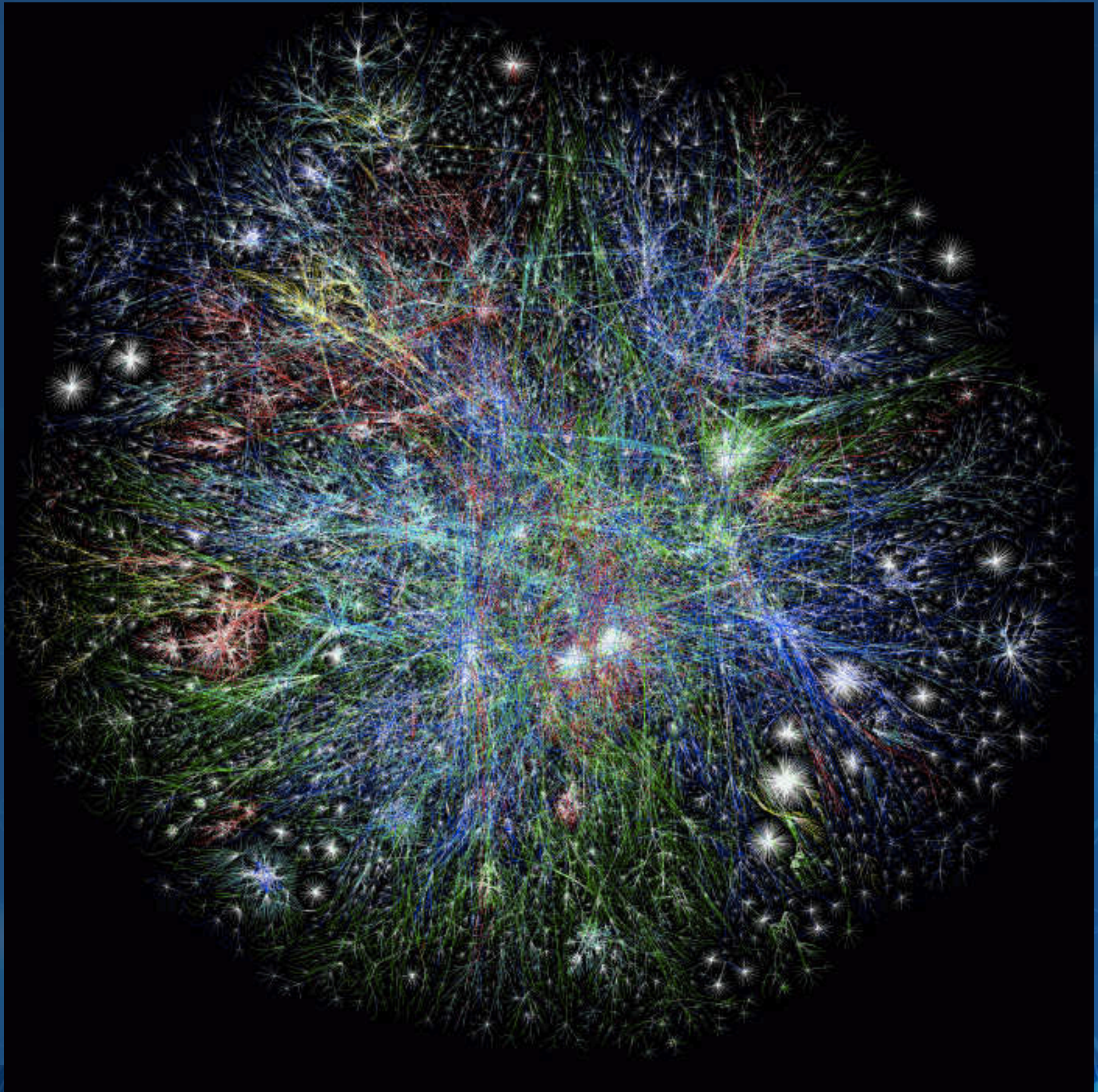
Digital signal – small time divisions

Continua (Not Binary)

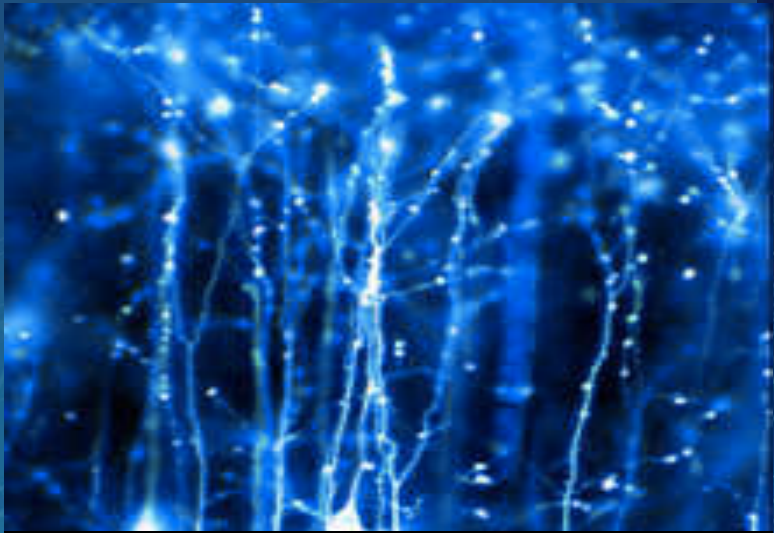


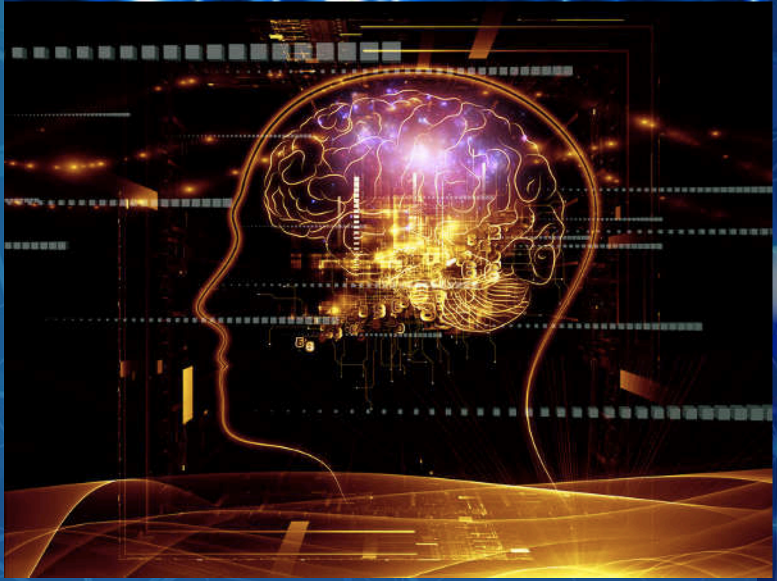
Sine Waves: Analogue

The Internet Is Analogue & Alive



The Brain is Analogue





Analogue Bio-Computers (Neural Interface / IoT)

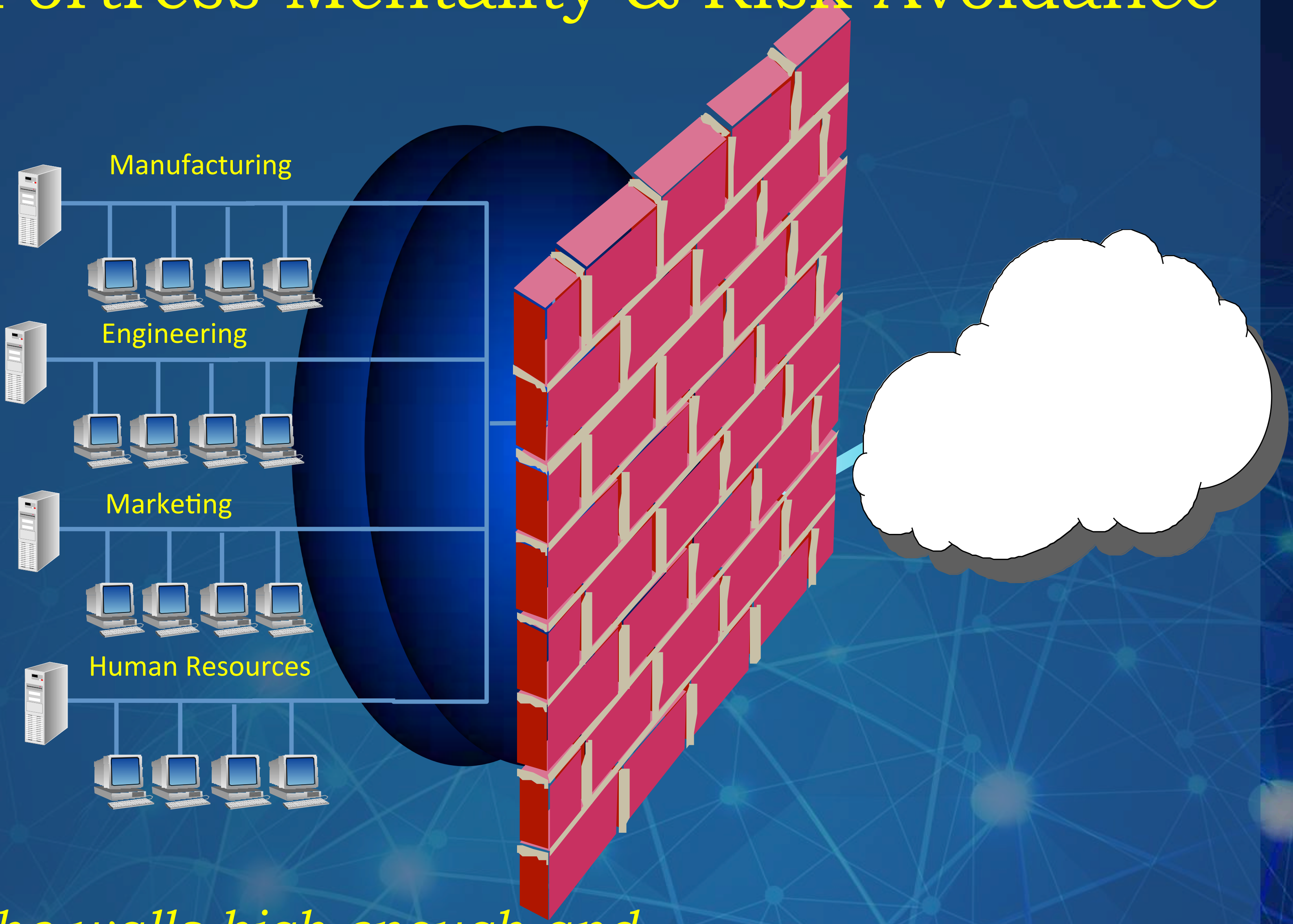
Picture: John Hopkins

Security Models

Static Security Models

- Expensive
- Not Prone to Communication/Commerce
- Models from 1970’s
  - Bell LaPadula
  - Bibi
  - Analyze/Decide Prior to Permission

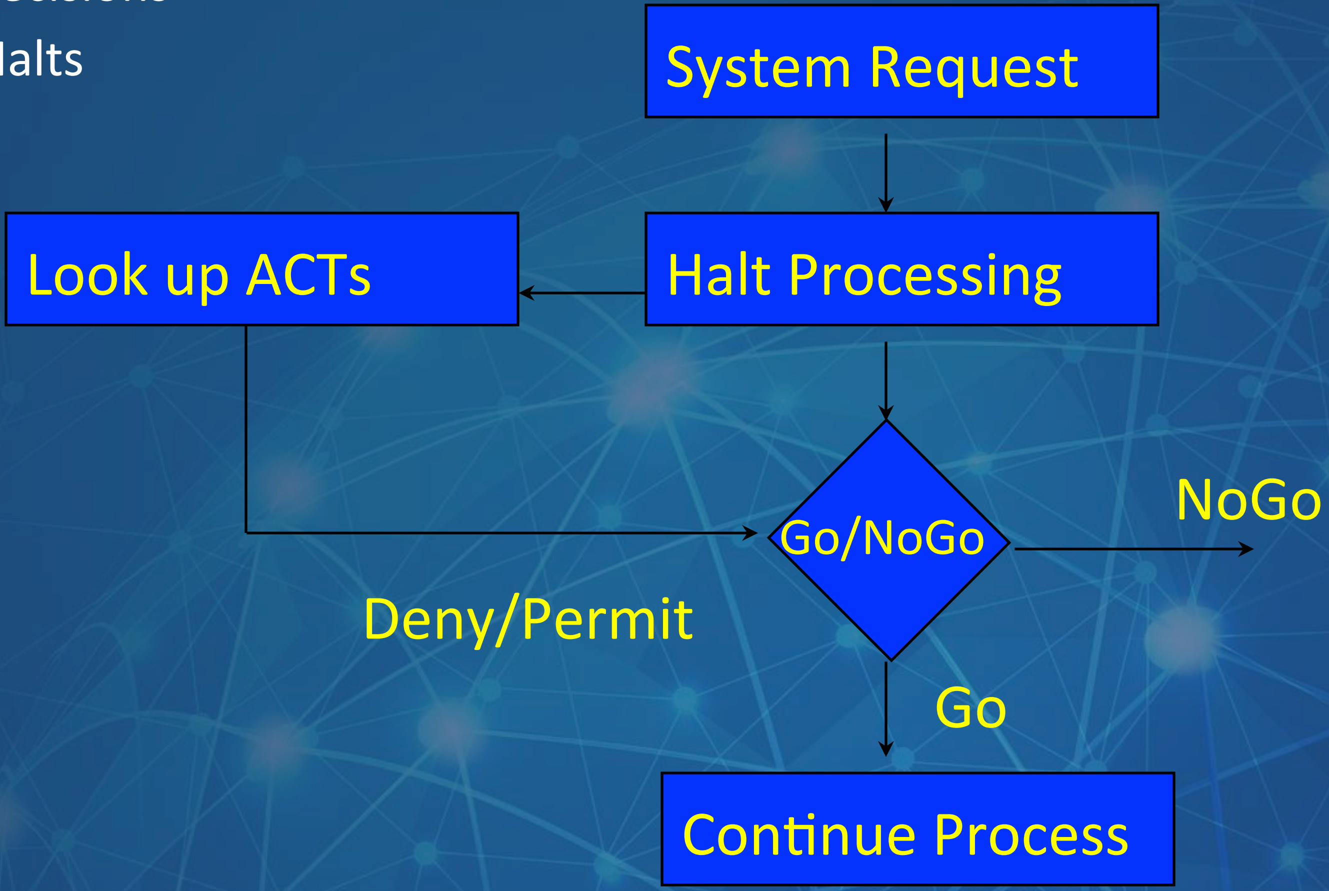
Fortress Mentality & Risk Avoidance



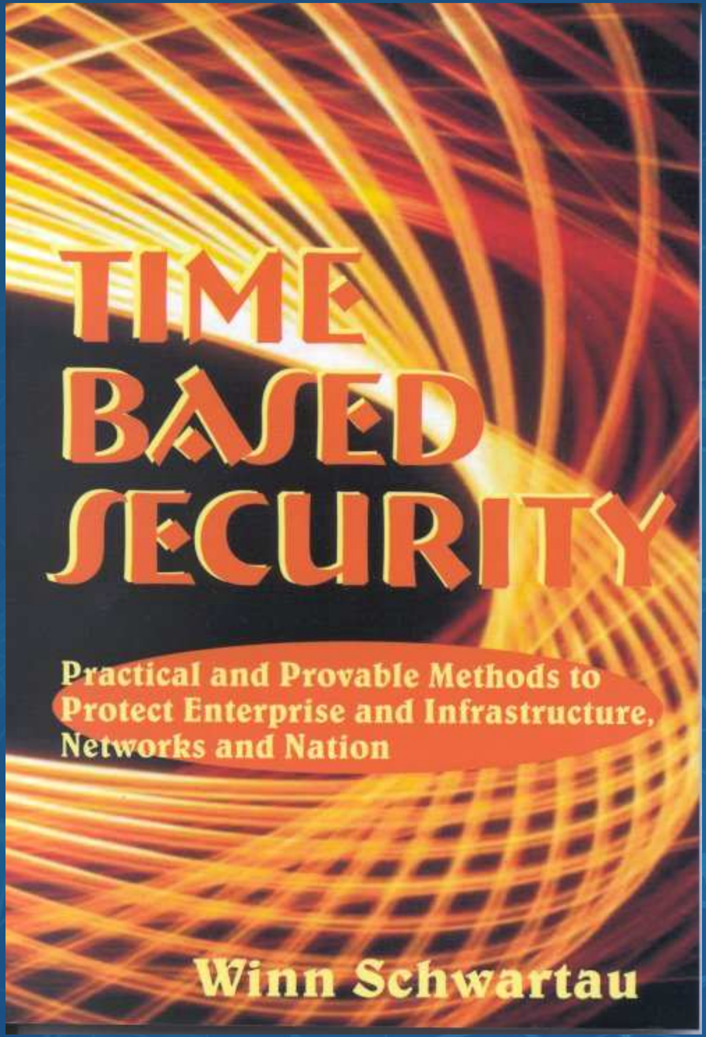
"Build the walls high enough and the computers are secure."

The Reference Monitor

- Each System Request Is Mediated
- Yes/No Decisions
- Process Halts



Protect-Detect-Respond’
The Original ‘Model: 1994



TIME BASED SECURITY

Practical and Provable Methods to Protect Enterprise and Infrastructure, Networks and Nation

Winn Schwartau

Is The Vault Secure?

VAULT DOOR
WEIGHT 22 1/2 Tons
THICKNESS 22 Inches
STEEL 11 Layers of Special Cutting and Drill Resistant
LOCKS 4 Hamilton Watch Movements for Time Locks

Safe Ratings

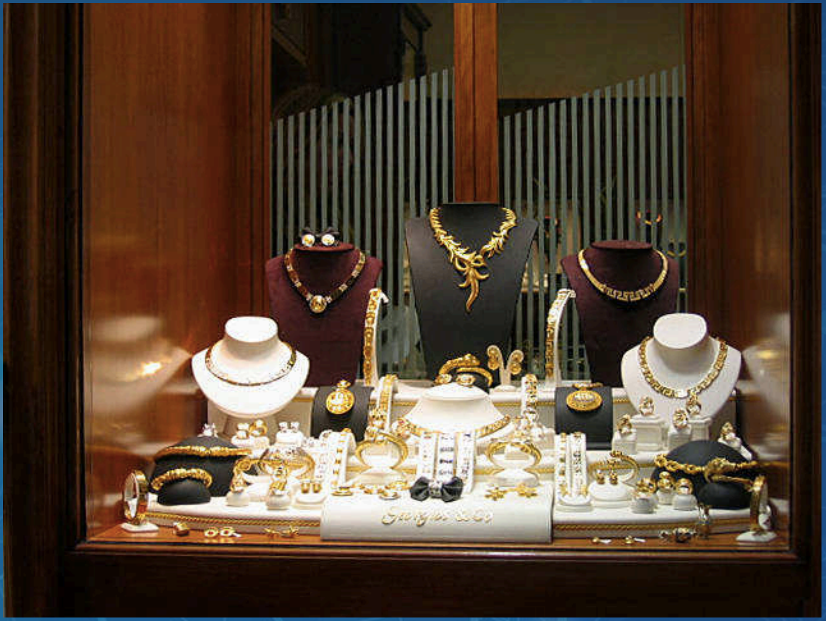
- This terribly expensive burnished steel vault is secure against:
  - 3200C Oxyacetylene torch for 92 Hrs.
  - 5.2kg of 3.8 Rated TNT

It’s About Time

Can You Rate Your Firewall? (0-10)

Why We Can't Rely on Protection

- No Product Guarantees
- Networks are highly dynamic
  - Most protection is highly static.
  - The security posture changes continuously
  - Network maps are 'iffy'. Especially ingress/egress
  - Partner networks are often security suspects.
  - Complexity breeds vulnerability
- New hacks & '0'-Days
- Patches take time
- Improper configuration
- Insiders (Errors & Intent)



How Much Protection Does The Window Provide (Time)?

What *Can* We Measure?

Detection

+

Reaction

Time Based Security Formula

- Protection (The glass/bank vault)
- Detection (The sensors and alarms)
- Reaction (The cops)
- Two Analogue Components:
  - **Time** (Dynamic)
  - **>** (Versus '=' which is static)

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

Measure Your Network Security … Now!

MAD Cold War = Time

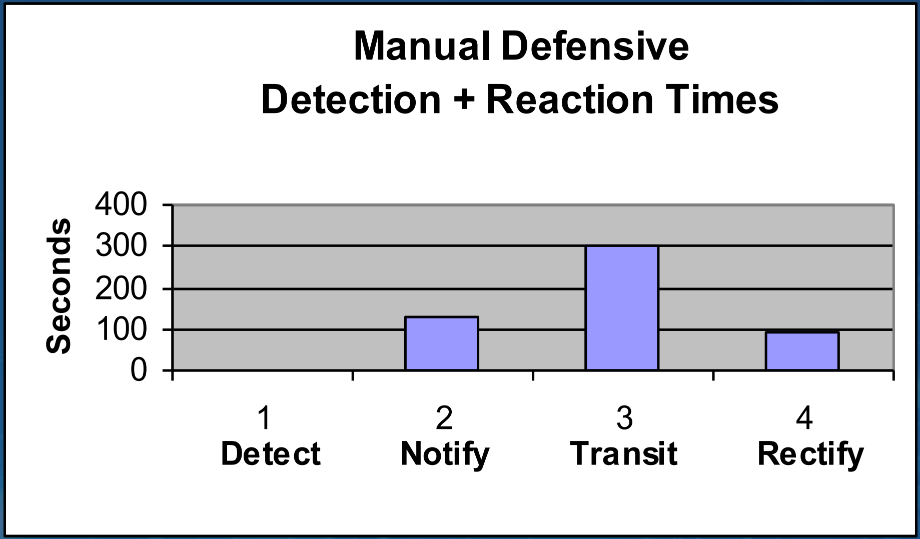
Adding It All Up: $D_{(t)} + R_{(t)}$

D + R = 527 Secs.

E = 8.8 Mins

F = 81.3MB. (T-1)

F = 6.7MB (512)

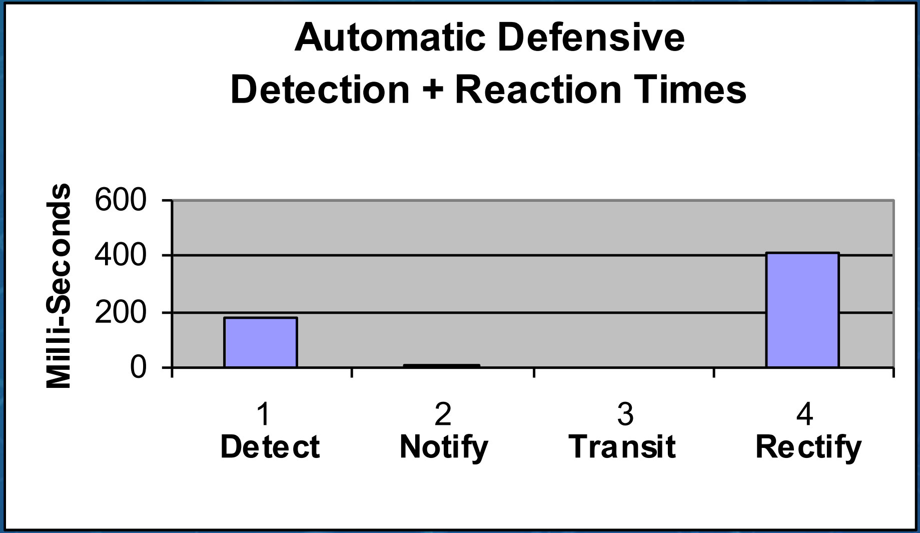


D + R = 600ms

E = .6 Secs

F = 92K (T-1)

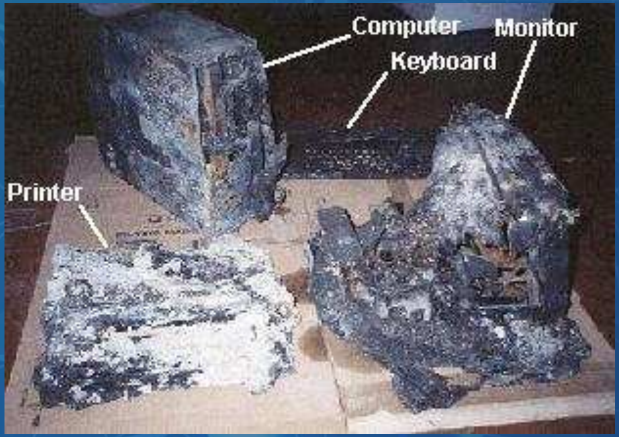
F = 7.7K (512)



Evaluating Exposure: $E_{(t)}$

- Assume No Protection:
  - If P = 0,
    - Then $E_{(t)} = D_{(t)} + R_{(t)}$
  - If P > 0,
    - Then $E_{(t)} = [P_{(t)} – (D_{(t)} + R_{(t)})]$
- Given Total Access to Your Networks -
  - How much ‘Value’ can be stolen in 1 minute?
  - How about 10 minutes?
  - What about 2 hours?
- Cost in $ of DOS/DDoS?
- Best-Case Metric of Security

$$\mathop{\mathrm{Lim}}_{t >> 0} E_t = \mathop{\mathrm{Lim}}_{t > >0} (D_t) + \mathop{\mathrm{Lim}}_{t >> 0} (R_t)$$



Data Evaluation

Stop Treating Networks As Single Objects!

Date				
Location				
Server				
If this data is released, modified or destroyed:	**Company Proprietary**	**Employee Private**	**Customer Private**	**Partner, Government, Other**
The results will be absolutely disasterous with no chance of economic or politcal recovery.				
There will be severe financial, political or other undesirable results, but we will survive.				
but spin doctoring will take care of it.				
Negligible effects, but we still really don't want it to happen.				
Publish it all you want. It's free, please take it!				

Defense in Depth
(Yes, but…)

$$P > D + R$$

$$\Downarrow$$

$$P_{(d1)} > D_{(d1)} + R_{(d1)}$$

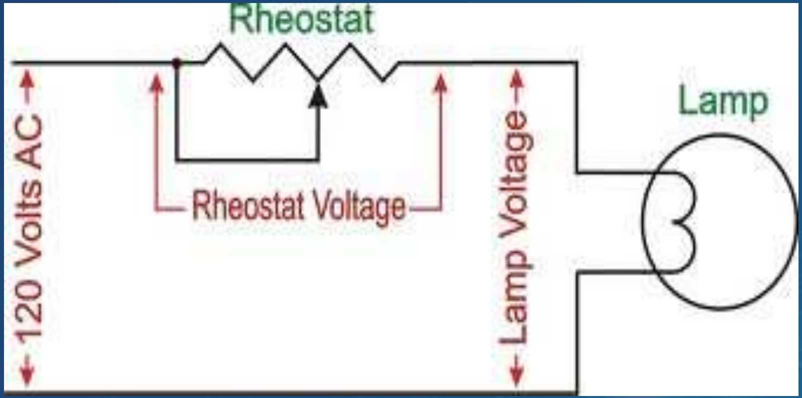
$$\Downarrow$$

$$P_{(r1)} > D_{(r1)} + R_{(r1)}$$

Measuring Which Files Are Targets

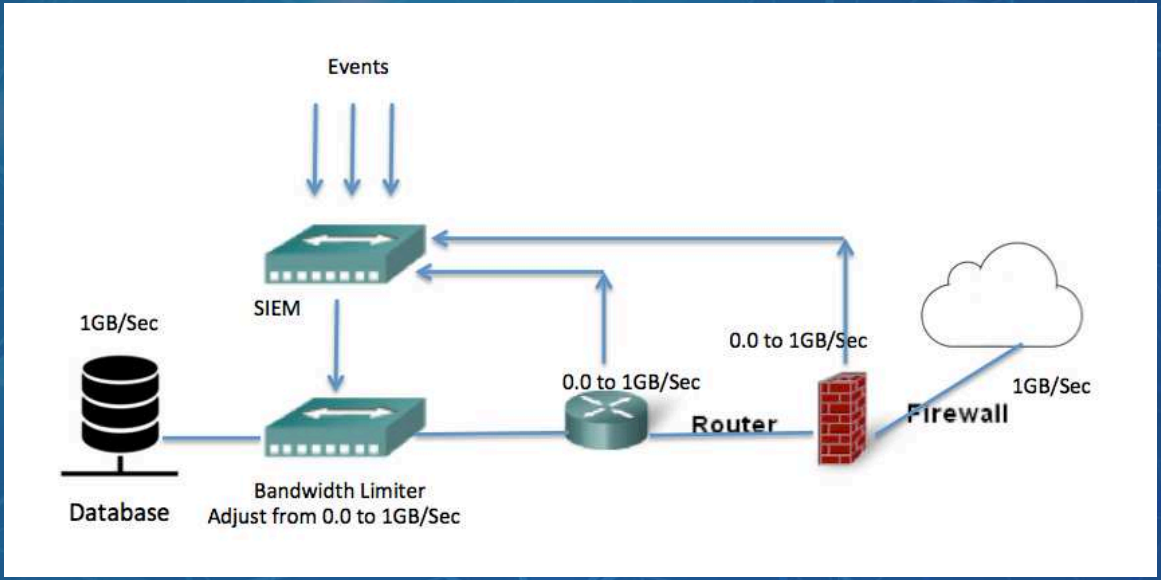
- $P > D + R$
  - If $P = 0$, then $D + R = E$
- $F / BW = T$
  - $BW(mb)/{\sim}10 = BW(MB)$
- 1Gb/sec ~ (100MB/Sec)
  - F = 100MB
- If $E > 1$sec, or $E > T$, F is Vulnerable

Dim All The Data

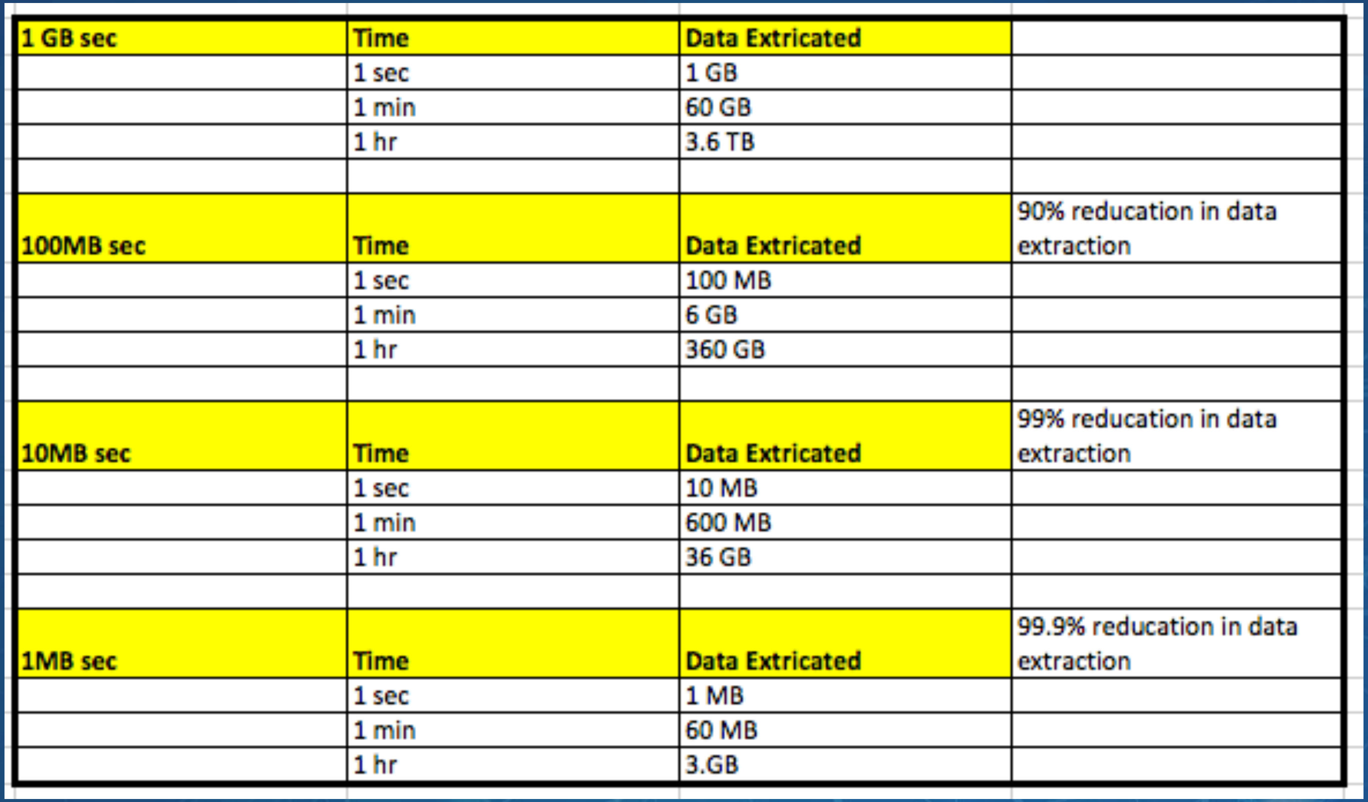


I = E/R

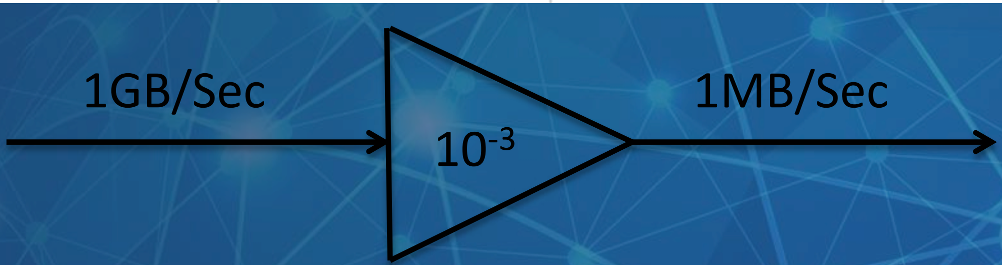
- T = F / BW



Bandwidth Compression



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



The Bad Guys Know Math, Too

- Offense: Think
- $1/[P = (D+R)]$
- If Defense $P > 0$
  - then Offense $A > P$ for success,
  - iff $(D + R) > P$
- If Defense $P = 0$,
  - then Offense $A < (D + R)$ or $A < E$ (Defense)

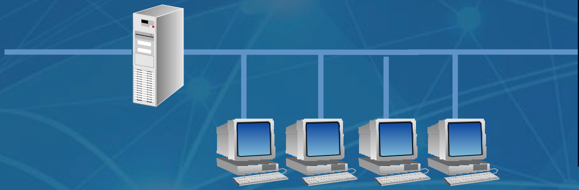
Kill Root

Multiple Admins

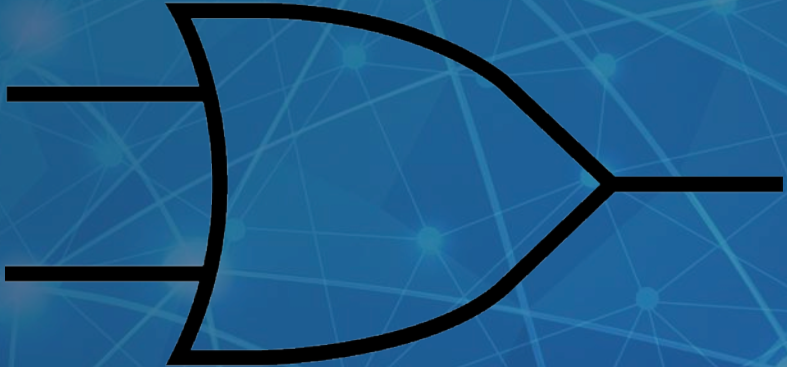
A

- With Multiple Individuals, What Happens to Trust Factor?
- Improves? Worsens?

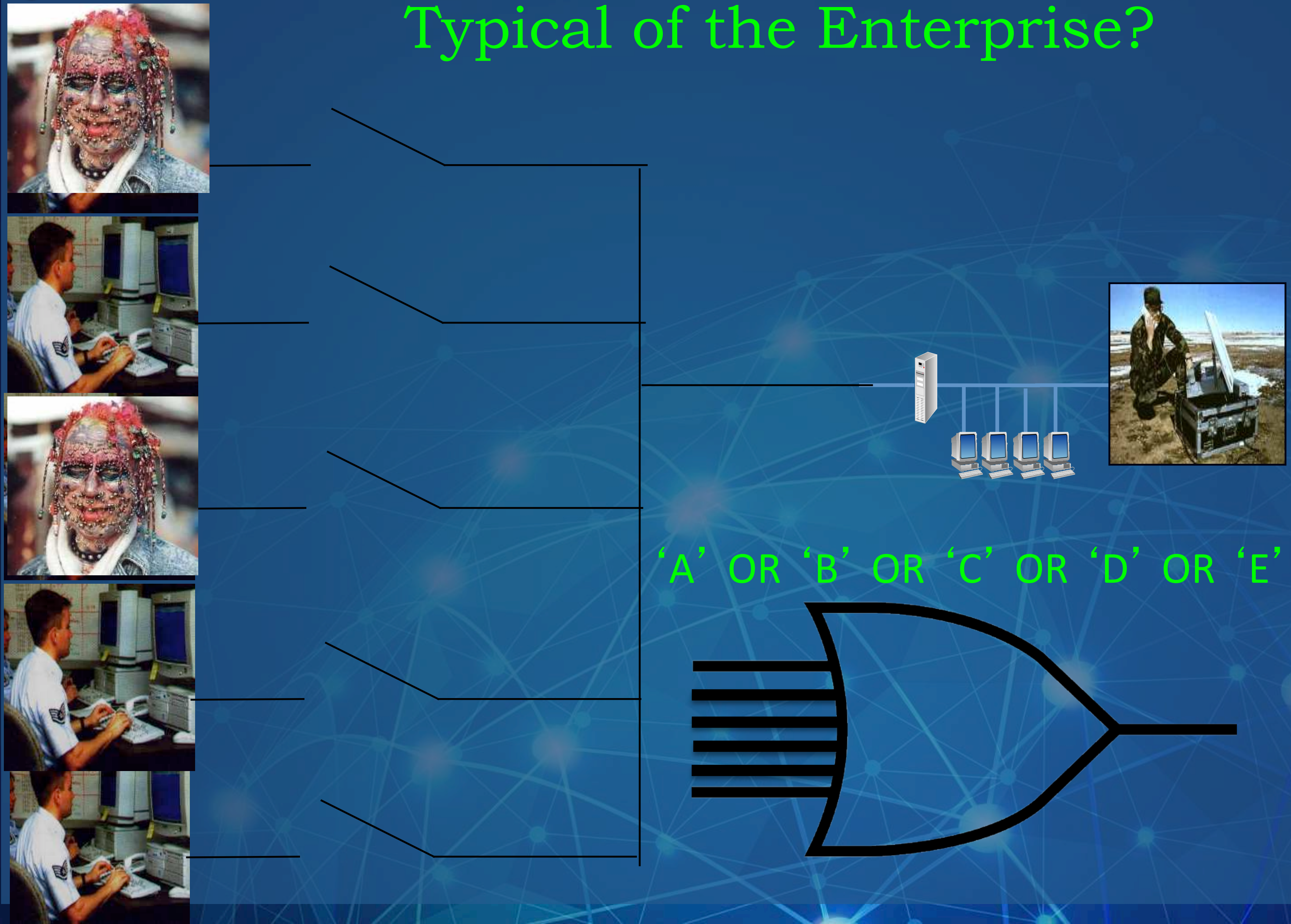
‘A’ OR ‘B’



B



Typical of the Enterprise?



‘A’ OR ‘B’ OR ‘C’ OR ‘D’ OR ‘E’

Admin Weakens Security
Trust Factors: ‘OR’

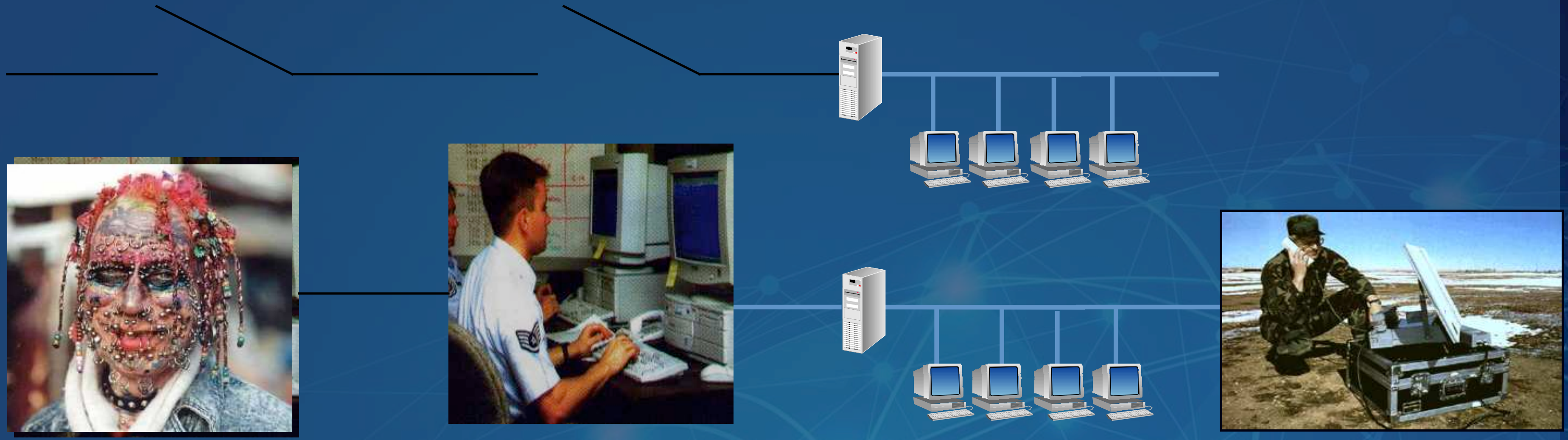
- If 2 Admins (OR)
  - Admin 1 and Admin 2 TF = .9 Each
  - Total TF = TF1 * TF2 = .81 (<.9)
- If 2 Admins (OR)
  - Admin 1 TF = .9
  - Admin 2 TF = .5
  - Total TF = .9 * .5 = .45!
- Lower TF than the Weakest Link!

2MR

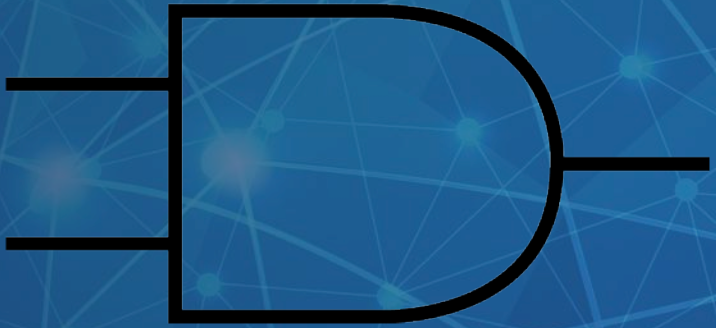
2MR Goal

- Ensure that Administrators Do Not Exceed Authority
- Ensure They Do Not Cause Intentional or Accidental Damage
- Reduce Risk From Insiders With Authority

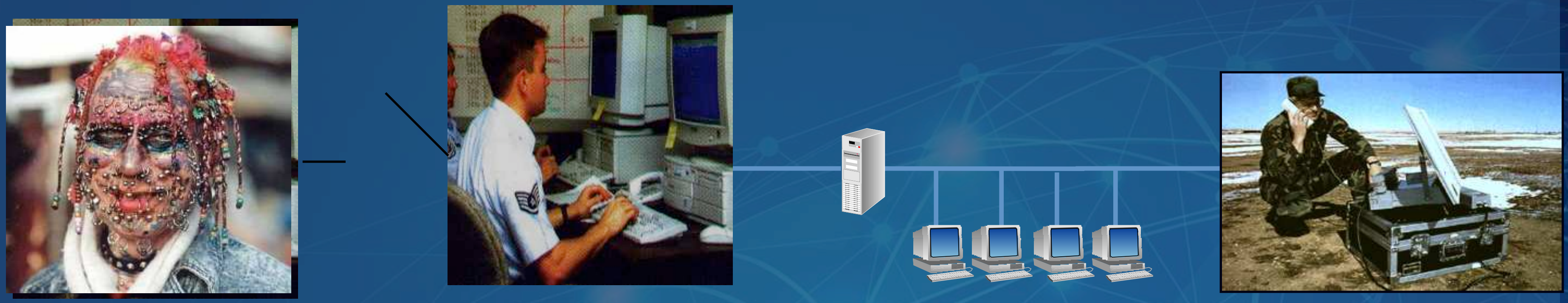
Two Man Rule: #1



- Admin 1 + Admin 2 = Security Relevant Changes
- Must Have 2 Authorized Admins Prior to Change

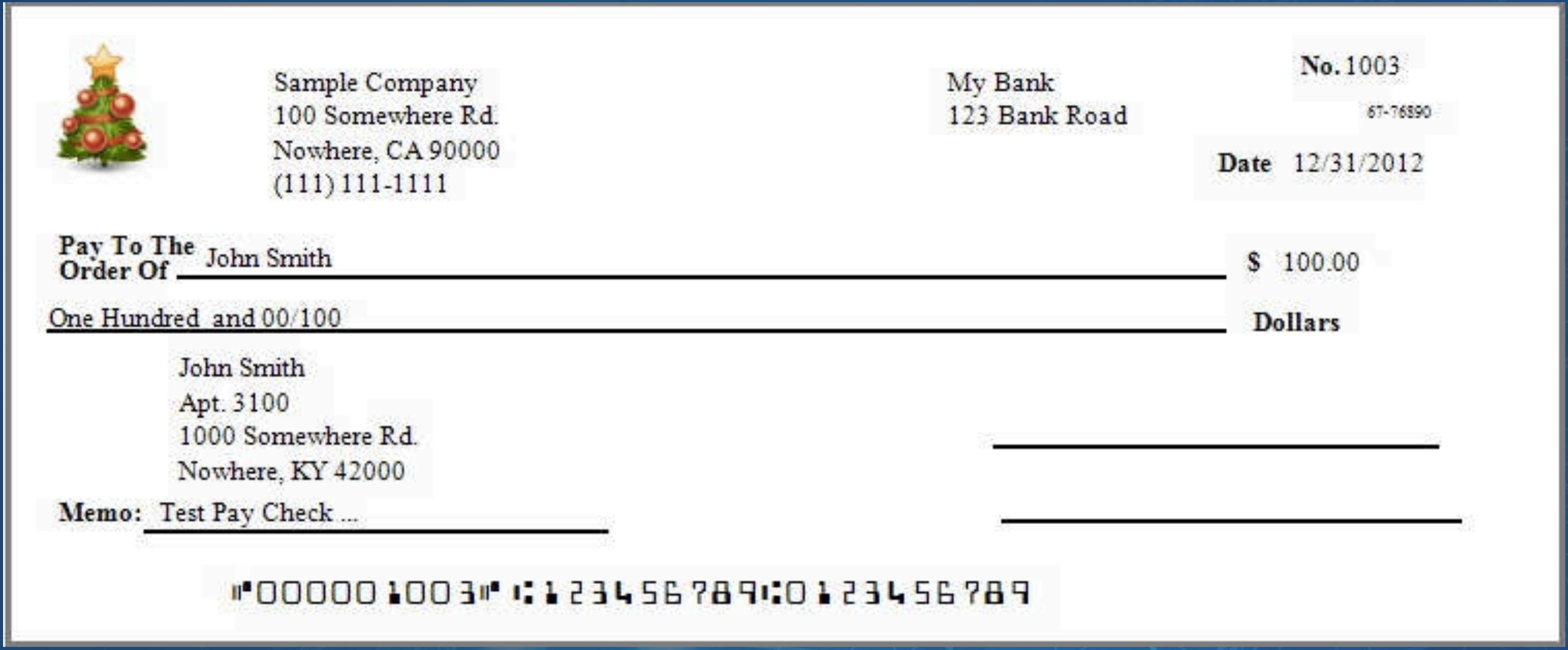


Problems With Two Man Rule



- Forces Hierarchal Administration for Security Relevant Changes
  - Good!
- Slows Down Process/Functionality
  - Bad!
- How Do We Achieve Balance?
  - Time, of course!

Do You Trust Your Partner?



Sample Company
100 Somewhere Rd.
Nowhere, CA 90000
(111) 111-1111

My Bank
123 Bank Road

No. 1003

67-76890

Date 12/31/2012

Pay To The Order Of John Smith

$ 100.00

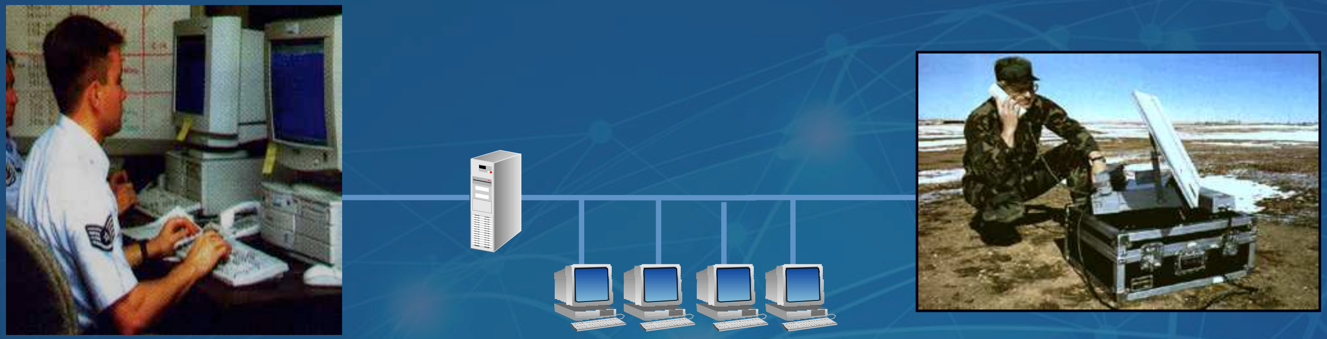
One Hundred and 00/100 **Dollars**

John Smith
Apt. 3100
1000 Somewhere Rd.
Nowhere, KY 42000

Memo: Test Pay Check ...

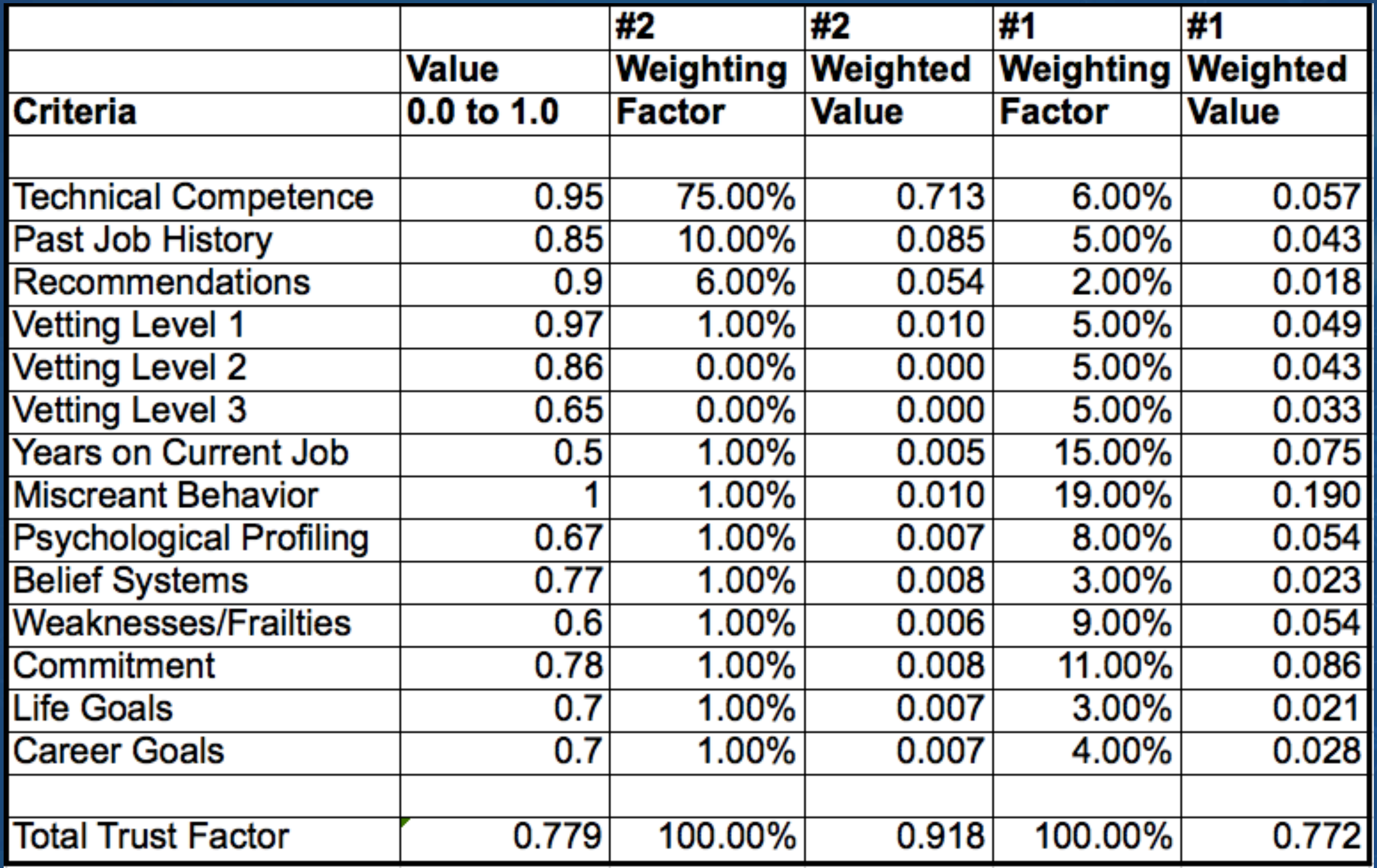
⑈00000 1003⑈ ⑆123456789⑆0123456789

Binary Trust



- Complete Trust is Placed in One Individual Over A Network
- What is Your Trust Factor?

TRUST FACTORS (Analogue)



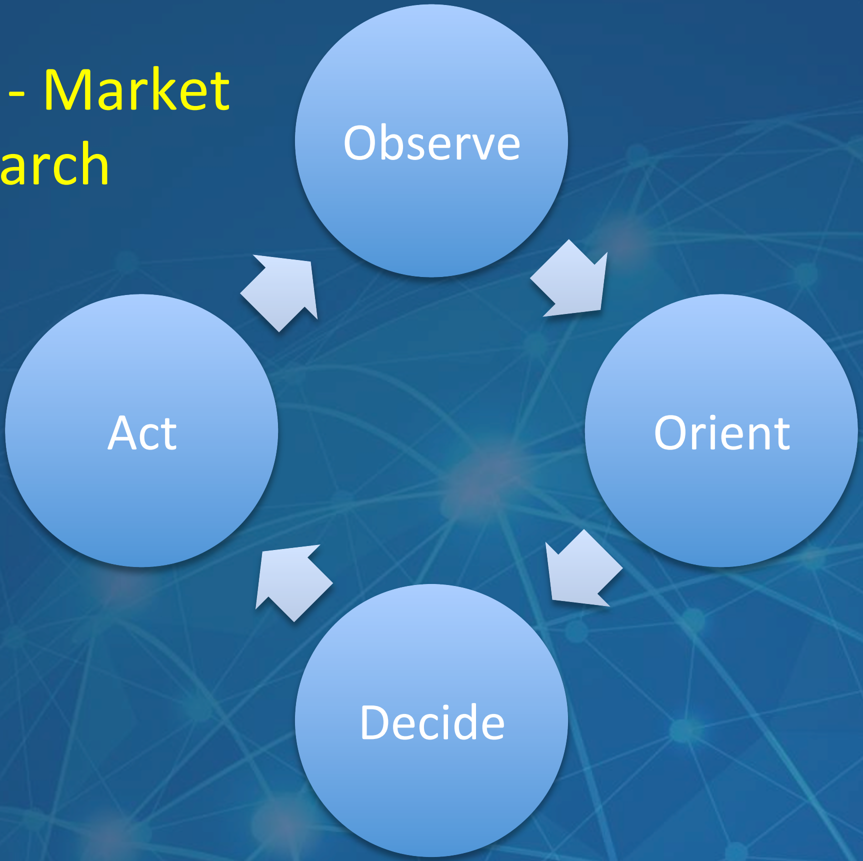
		#2	#2	#1	#1
	Value	Weighting	Weighted	Weighting	Weighted
Criteria	**0.0 to 1.0**	**Factor**	**Value**	**Factor**	**Value**
Technical Competence	0.95	75.00%	0.713	6.00%	0.057
Past Job History	0.85	10.00%	0.085	5.00%	0.043
Recommendations	0.9	6.00%	0.054	2.00%	0.018
Vetting Level 1	0.97	1.00%	0.010	5.00%	0.049
Vetting Level 2	0.86	0.00%	0.000	5.00%	0.043
Vetting Level 3	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 Behavior	1	1.00%	0.010	19.00%	0.190
Psychological Profiling	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

FEEDBACK

OODA Loop (JIT-Supply Chain)

Intel - Market Research

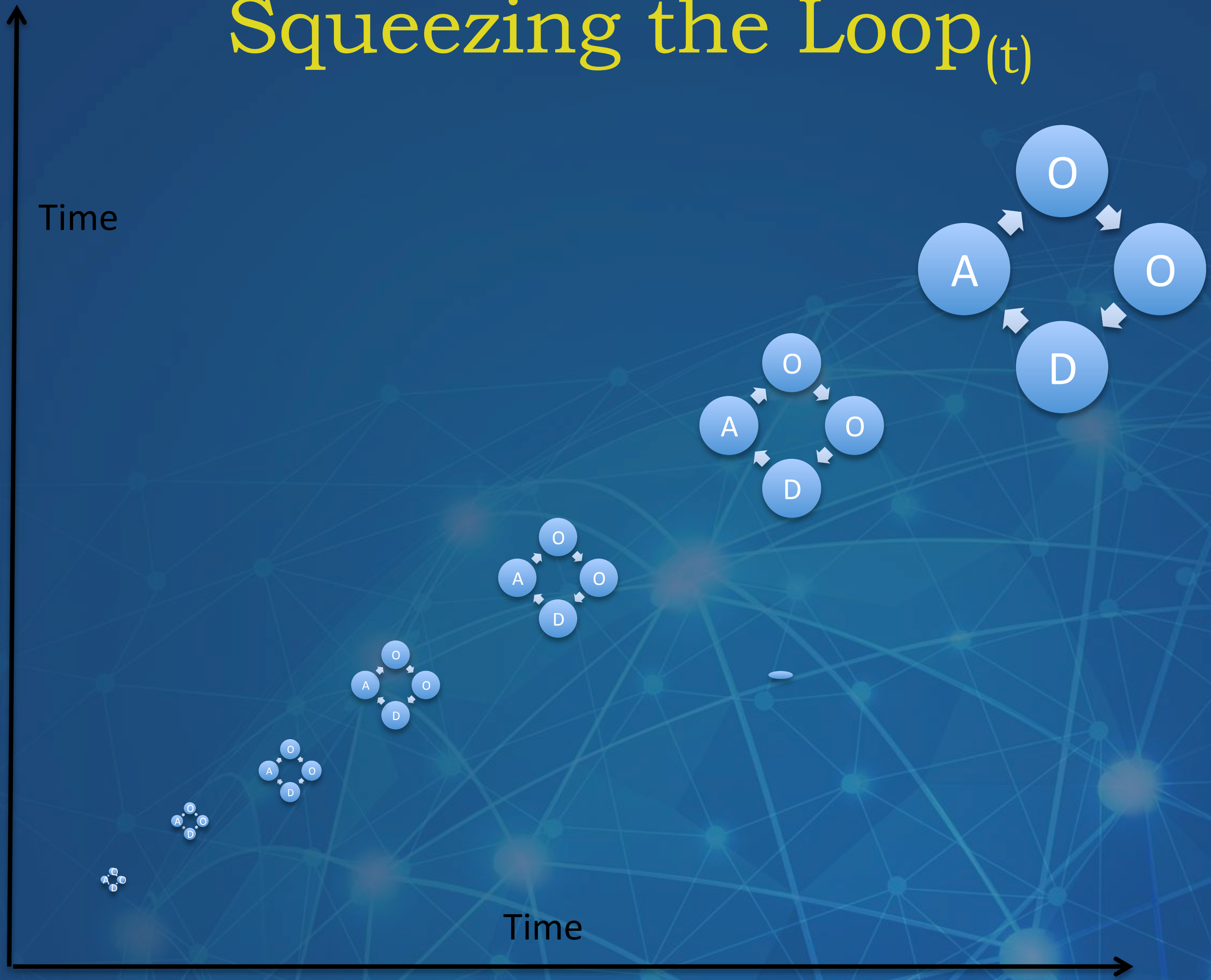
War fighting/ Deployment – Product/Service Launch



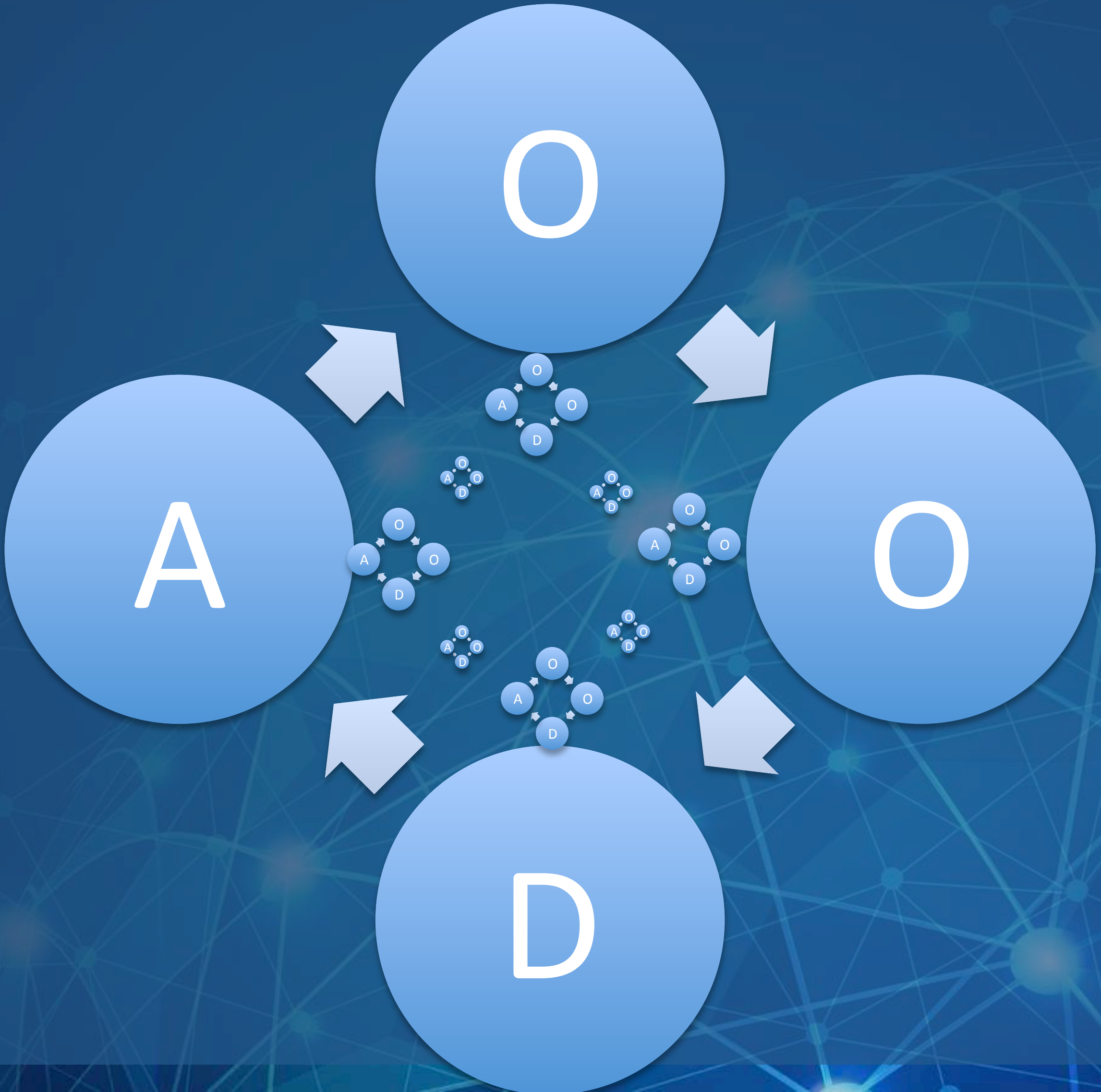
Contextualize

Decision Making (C3I)

Squeezing the Loop$_{(t)}$

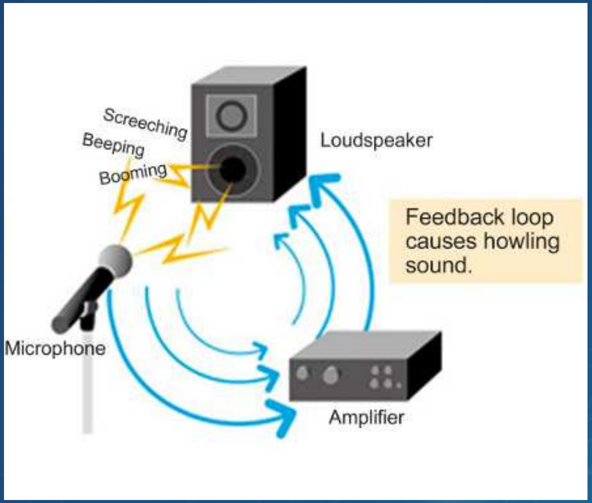


Defense in Depth - OODA

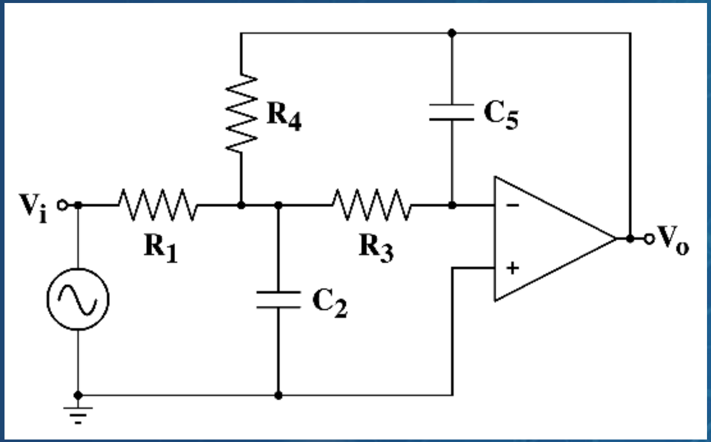


Feedback Is Analogue (Equilibrium vs. Chaos/Tipping Point)

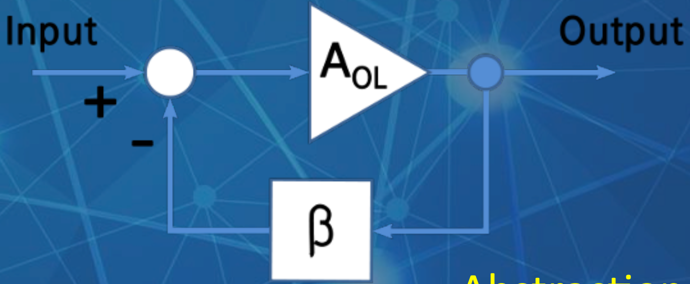
Acoustic



Mechanical

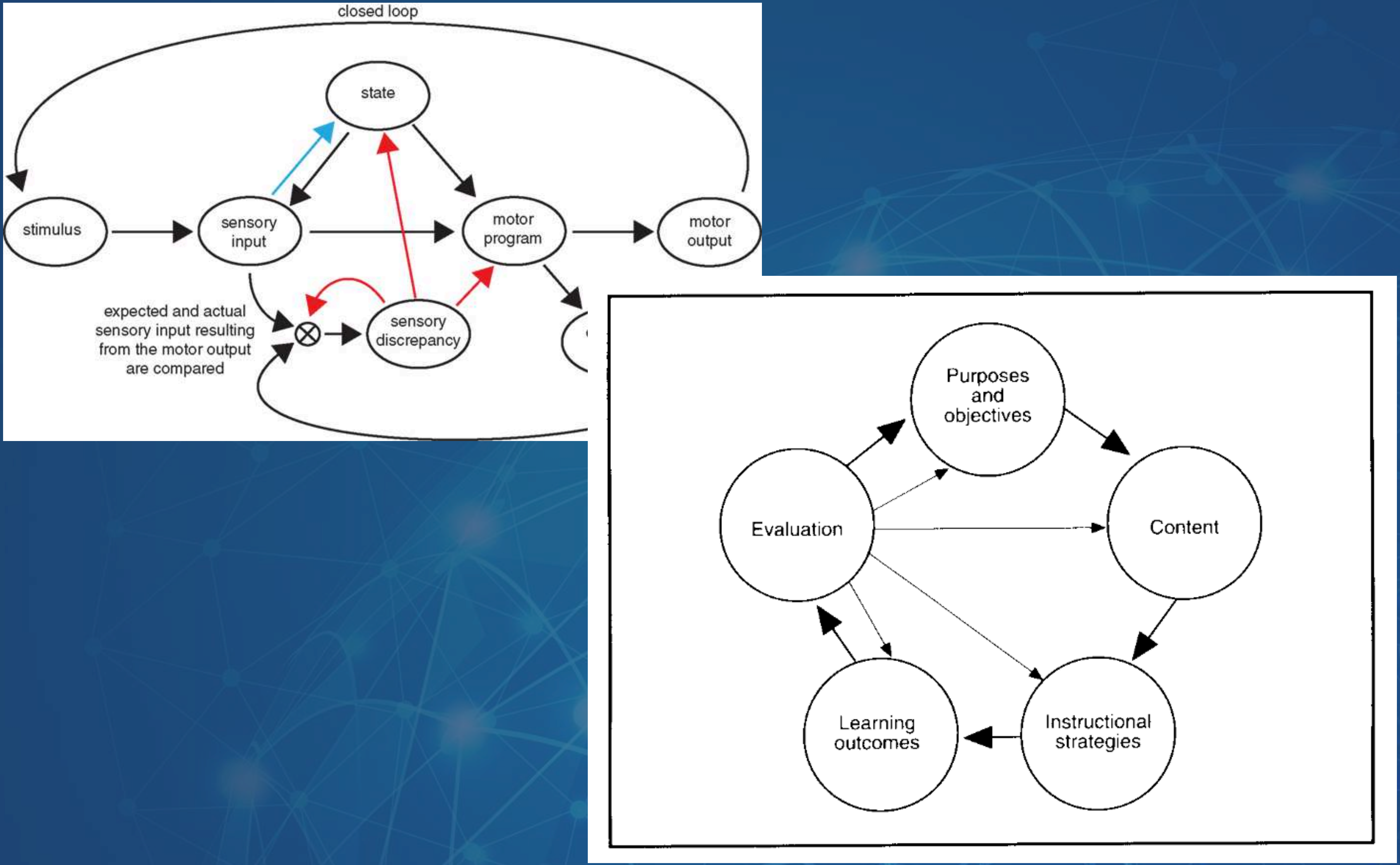


Electrical

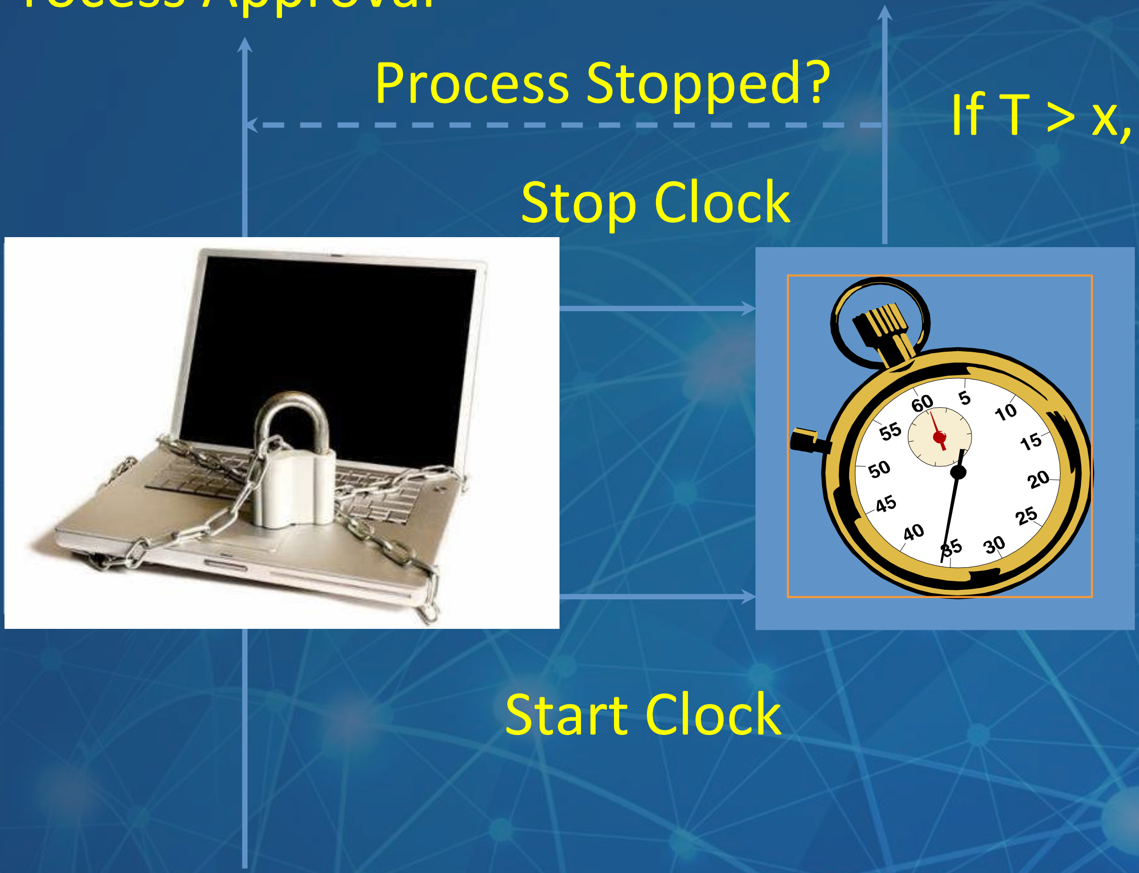


Abstraction

Haptics/Learning



Adding Time Based Security to Protection Products



Process Approval

Reaction Channel

Process Stopped?

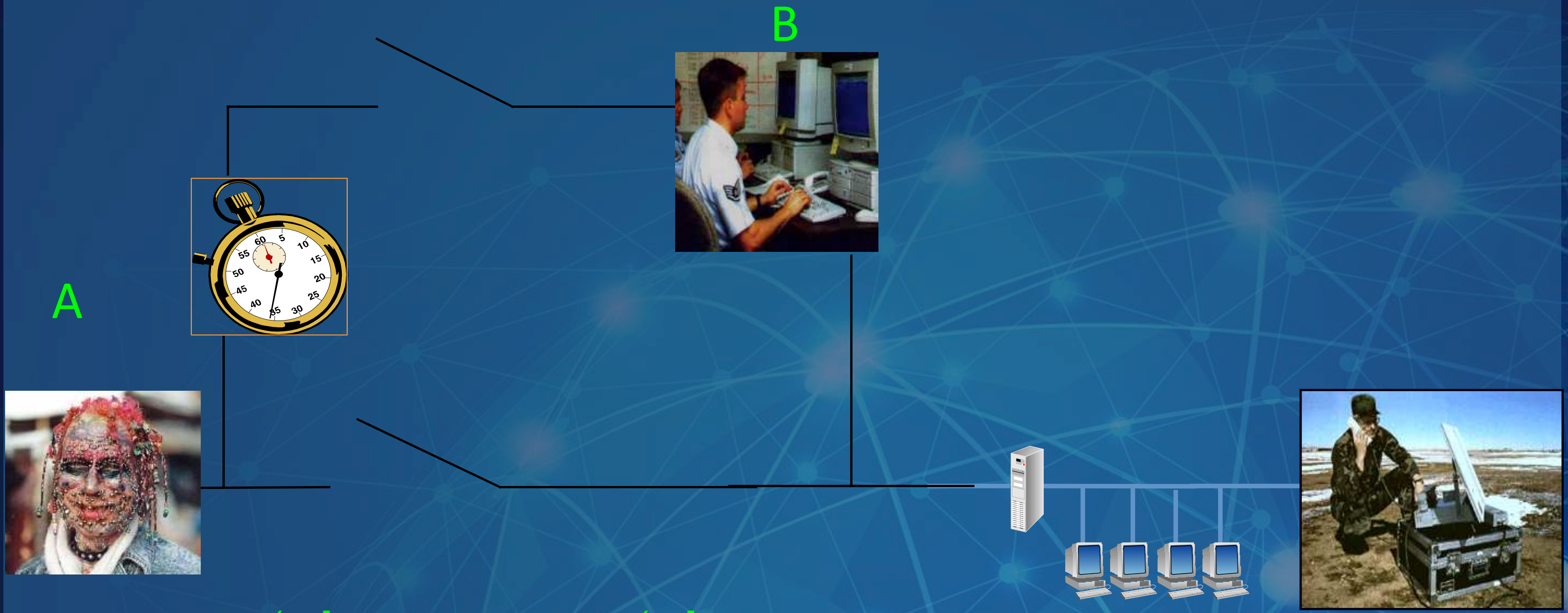
If T > x, then R

Stop Clock

Start Clock

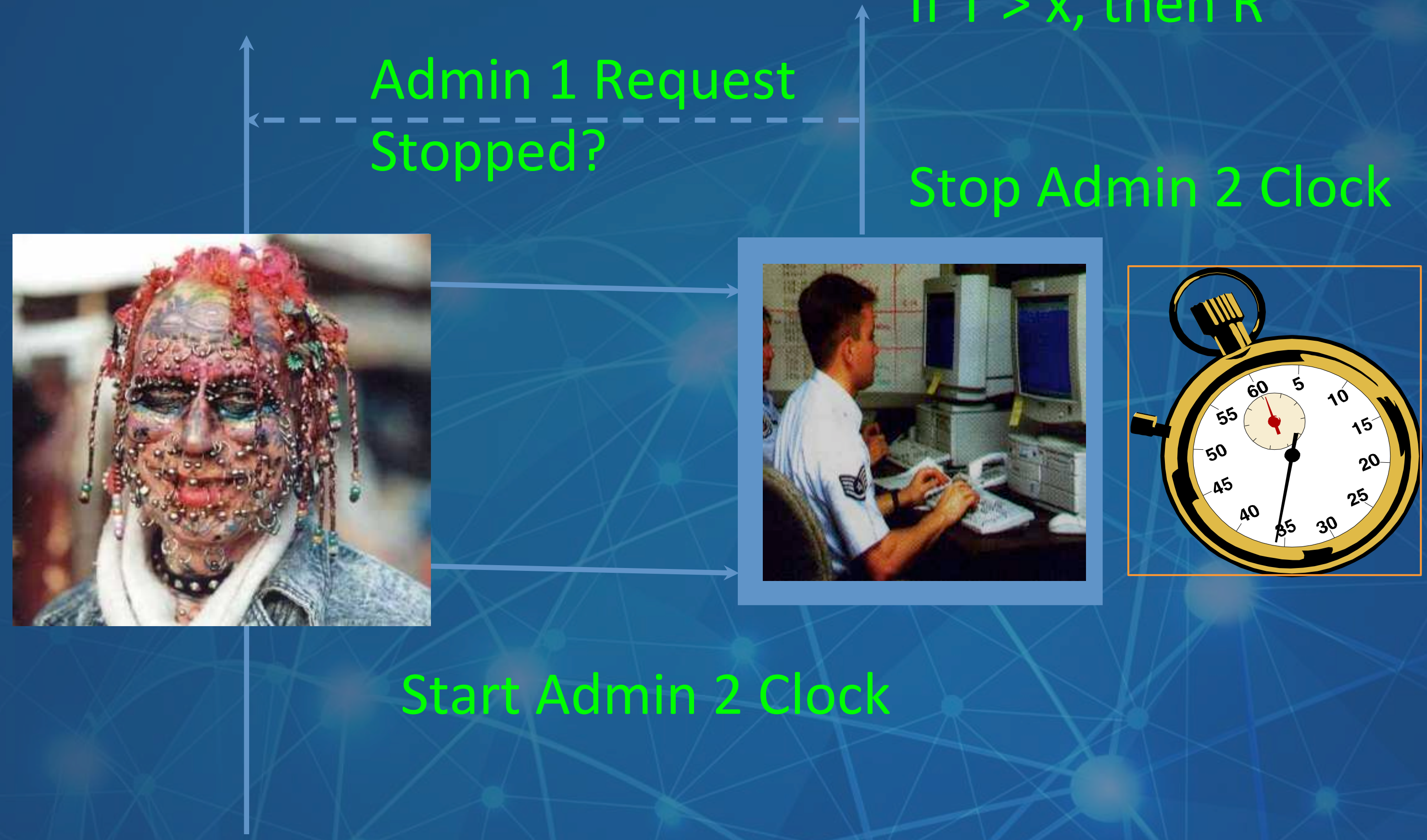
Process Request

TBS Feedback



- Admin ‘A’ AND Admin ‘B’ Must Agree, but. . .
- Security Action Can Occur Before ‘B’ Agrees
- Saves Time, Increases Exposure & Vulnerability

Using TBS to Enforce 2MR



Admin 1 Request Approval

Reaction Channel

If T > x, then R

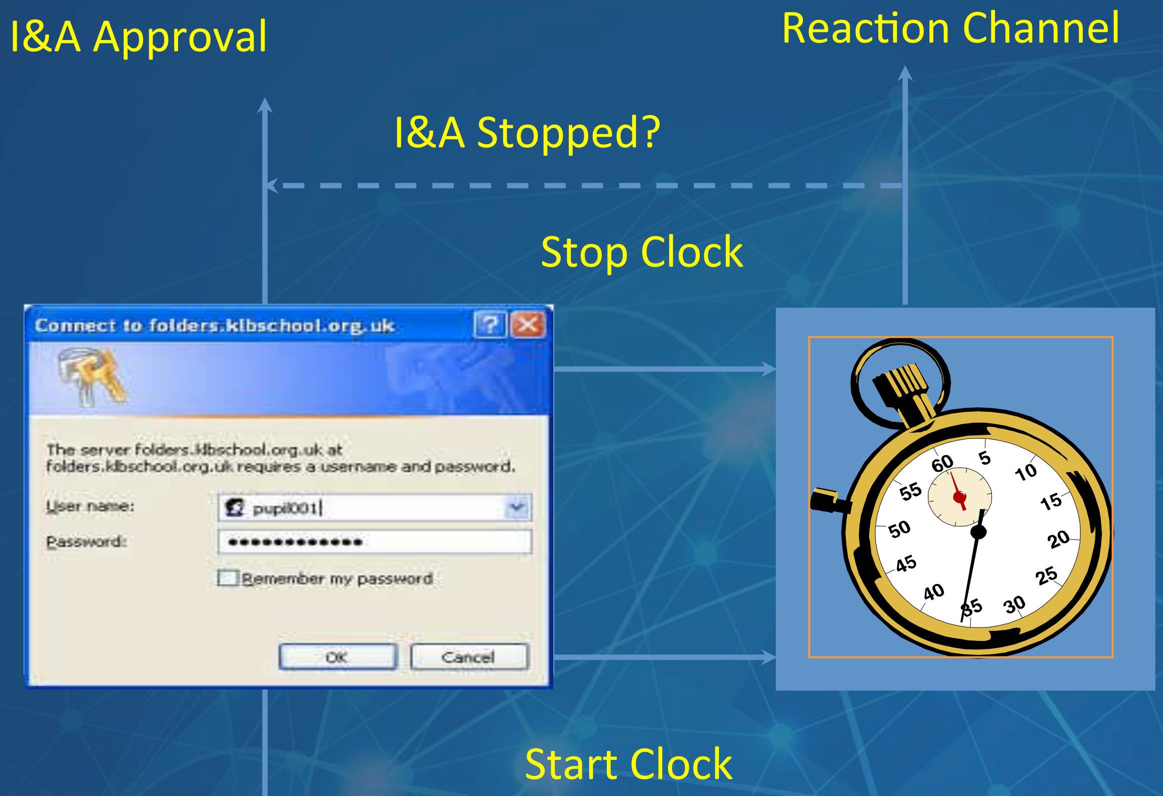
Admin 1 Request Stopped?

Stop Admin 2 Clock

Start Admin 2 Clock

Admin 1 Request

Adding TBS to I&A Mechanisms



I&A Approval

Reaction Channel

I&A Stopped?

Stop Clock

Connect to folders.klbschool.org.uk

The server folders.klbschool.org.uk at folders.klbschool.org.uk requires a username and password.

User name: pupil001

Password: •••••••••••••

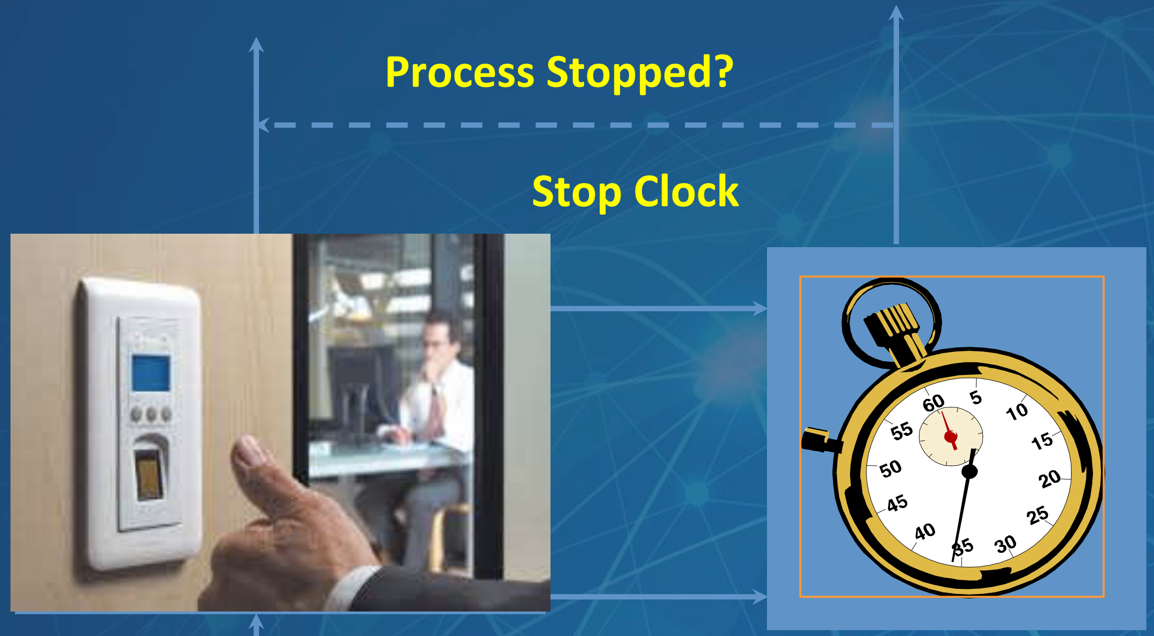
☐ Remember my password

Start Clock

I&A Request

P = Maximum Window for Authentication.
D = Amount of Time It Takes to Detect a User' s Sign-on
R = Amount of Time It Takes to Sever a Connection

Adding TBS to Access Control



Process Approval

Reaction Channel

Process Stopped?

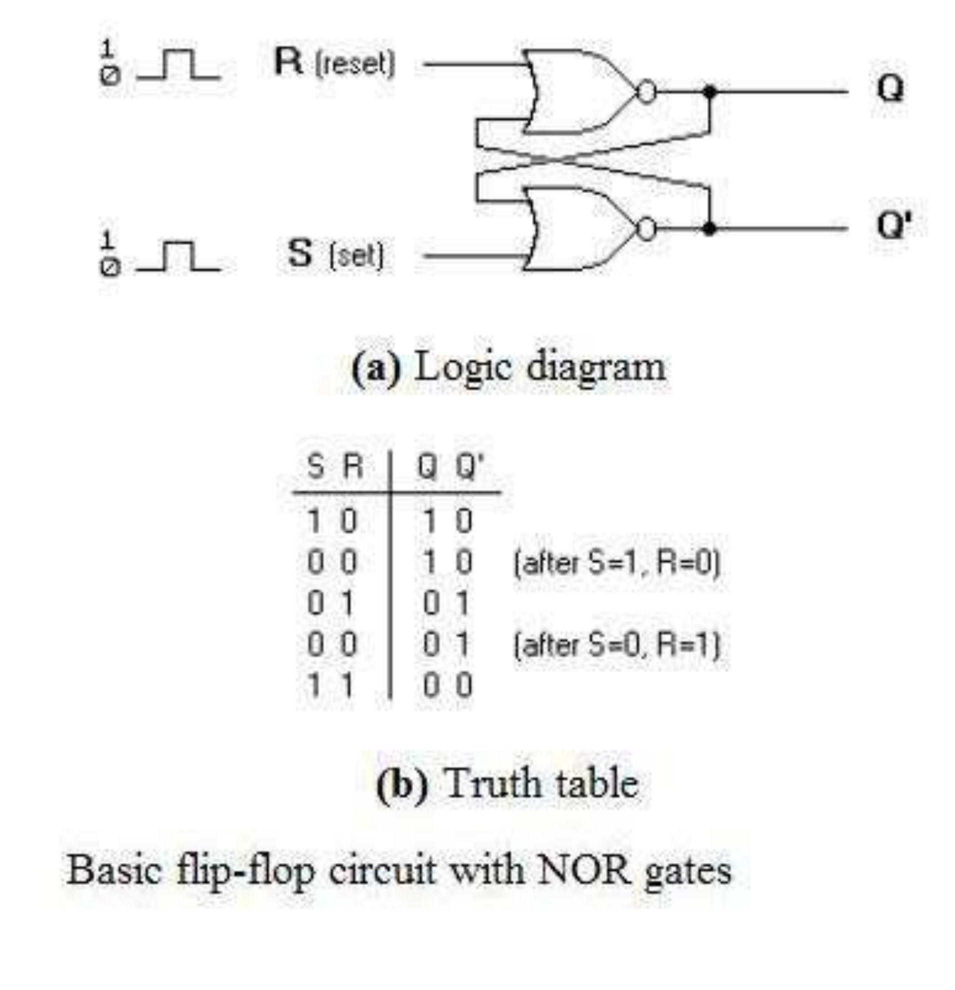
Stop Clock

Start Clock

Process Request

P = Time To Provide Legitimate Access To Resources
D = Time To Detect
R = Time To Respond

Fundamental ‘Bit’ of Feedback



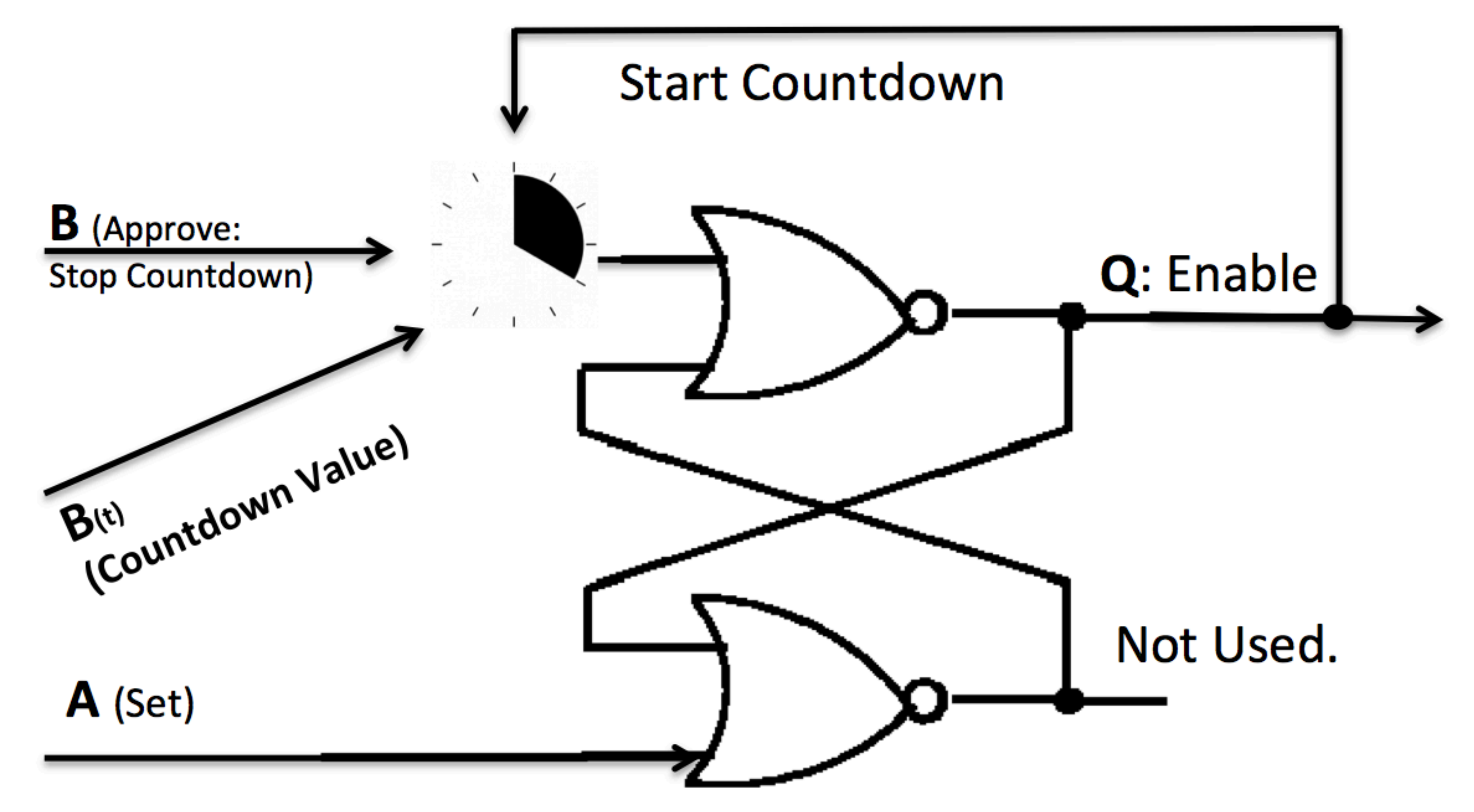
(a) Logic diagram

S	R	Q	Q'	
1	0	1	0	
0	0	1	0	(after S=1, R=0)
0	1	0	1	
0	0	0	1	(after S=0, R=1)
1	1	0	0	

(b) Truth table

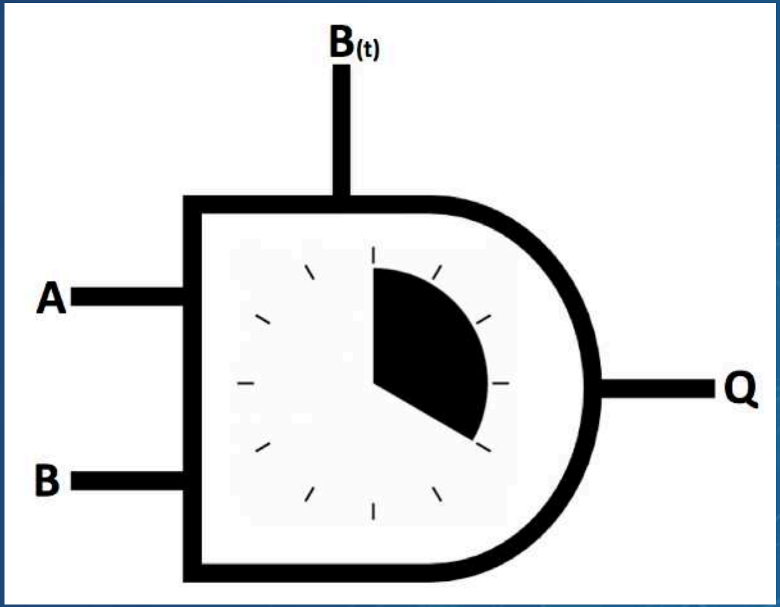
Basic flip-flop circuit with NOR gates

Adding Analogue Feedback (Time)



T-AND Gate

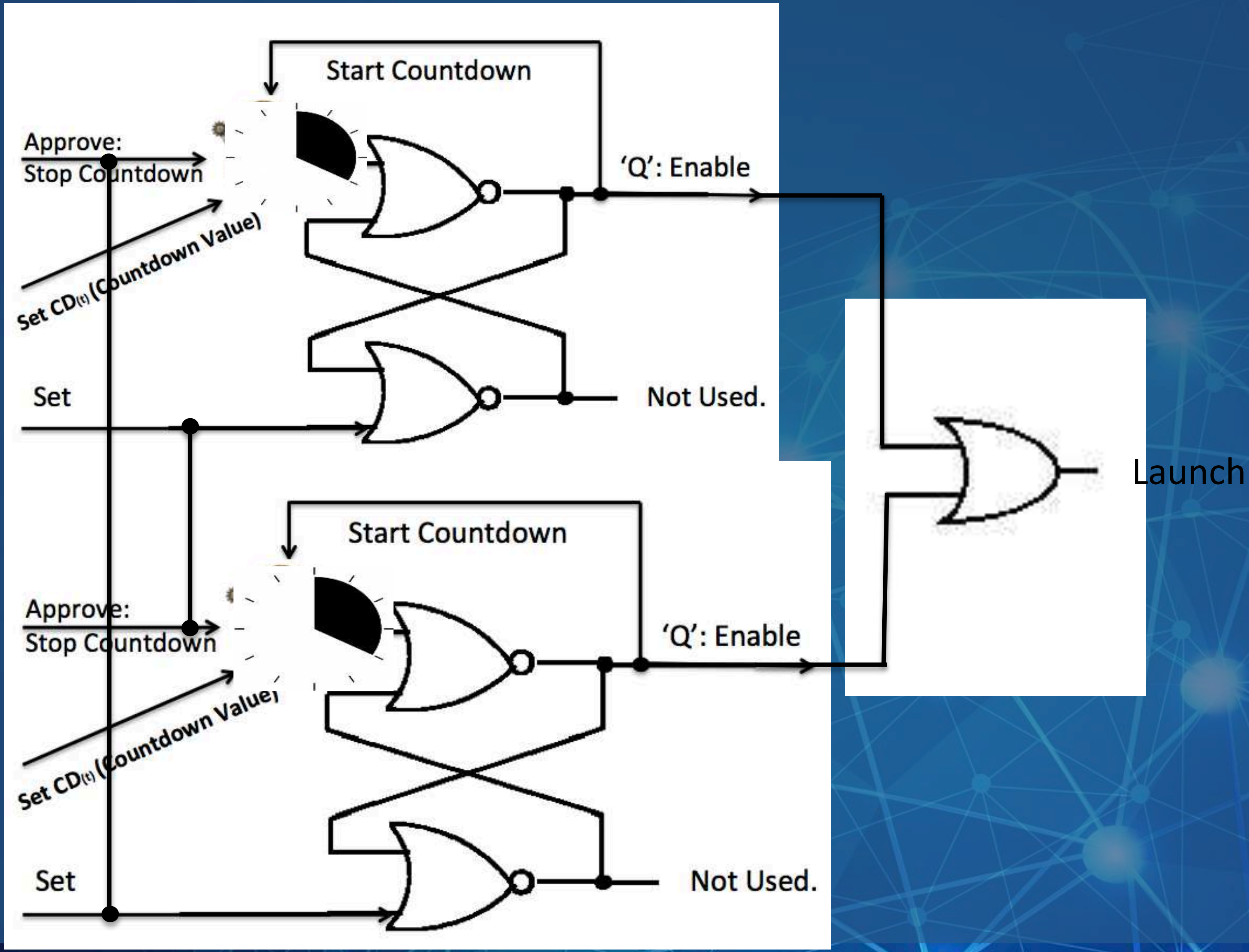
Truth Table



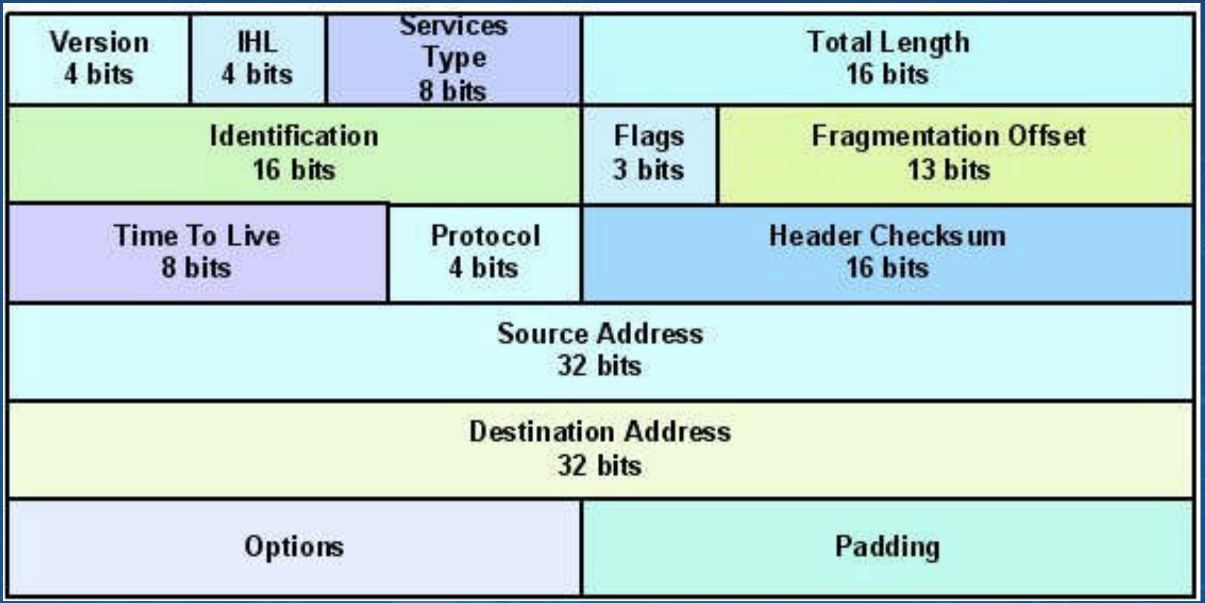
A = Set	B = Approve	B(t)	Q = Enable
0	0	OFF	0
0	0	t > 0	0
0	0	t = 0	0
1	0	OFF	1
1	0	t > 0	1
1	0	t = 0	0
1	1	OFF	1
1	1	t > 0	1
1	1	t = 0	1
0	1	N/A	0
0	1	N/A	0
0	1	N/A	0

How Do You Launch A Nuclear Missile?

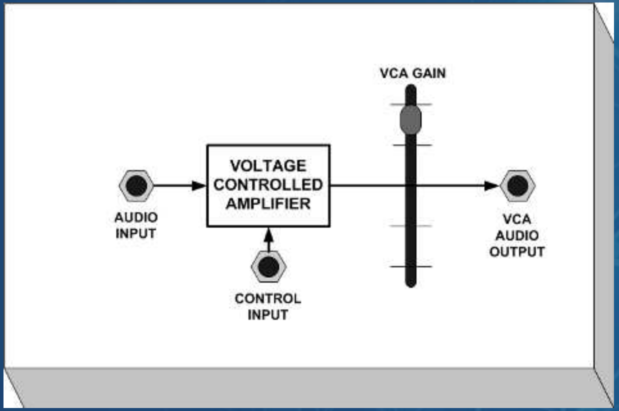
Launch a Nuke Circuit



Go Out of Band (OOB)

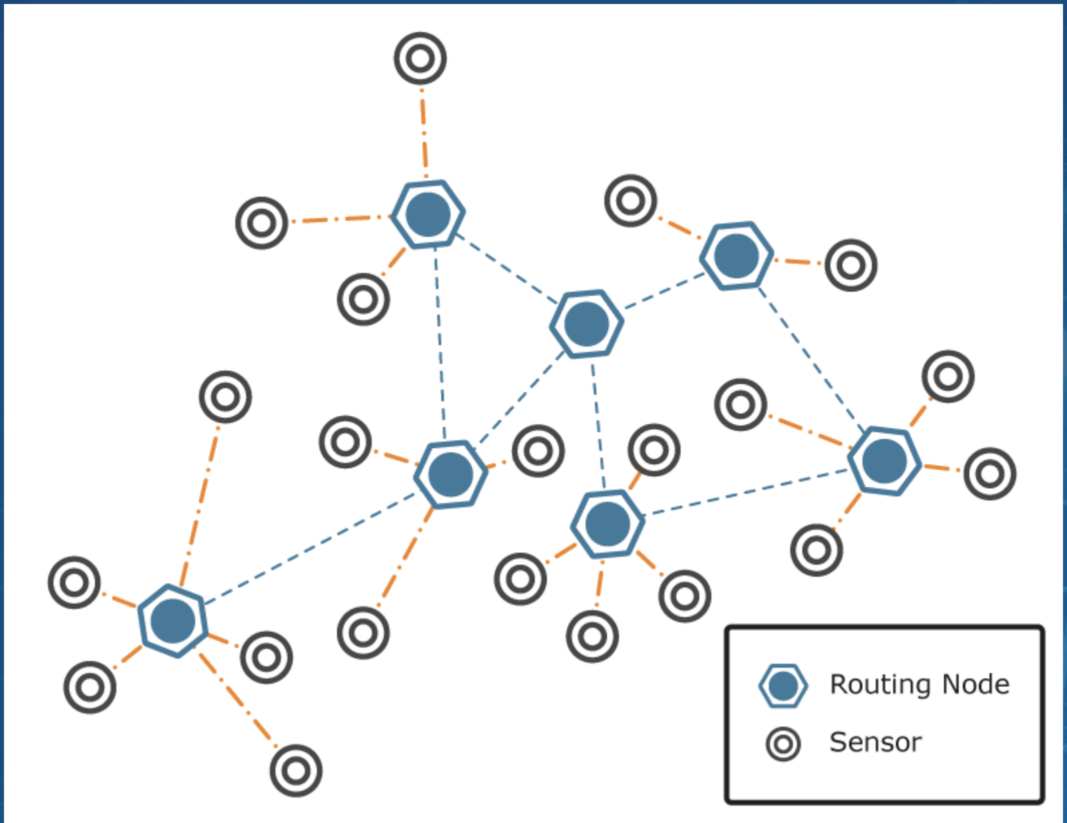


<table>
<tr><td>Version
4 bits</td><td>IHL
4 bits</td><td colspan="2">Services Type
8 bits</td><td colspan="2">Total Length
16 bits</td></tr>
<tr><td colspan="4">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation Offset
13 bits</td></tr>
<tr><td colspan="3">Time To Live
8 bits</td><td>Protocol
4 bits</td><td colspan="2">Header Checksum
16 bits</td></tr>
<tr><td colspan="6">Source Address
32 bits</td></tr>
<tr><td colspan="6">Destination Address
32 bits</td></tr>
<tr><td colspan="4">Options</td><td colspan="2">Padding</td></tr>
</table>



O.O.B. - Time Based Escalation

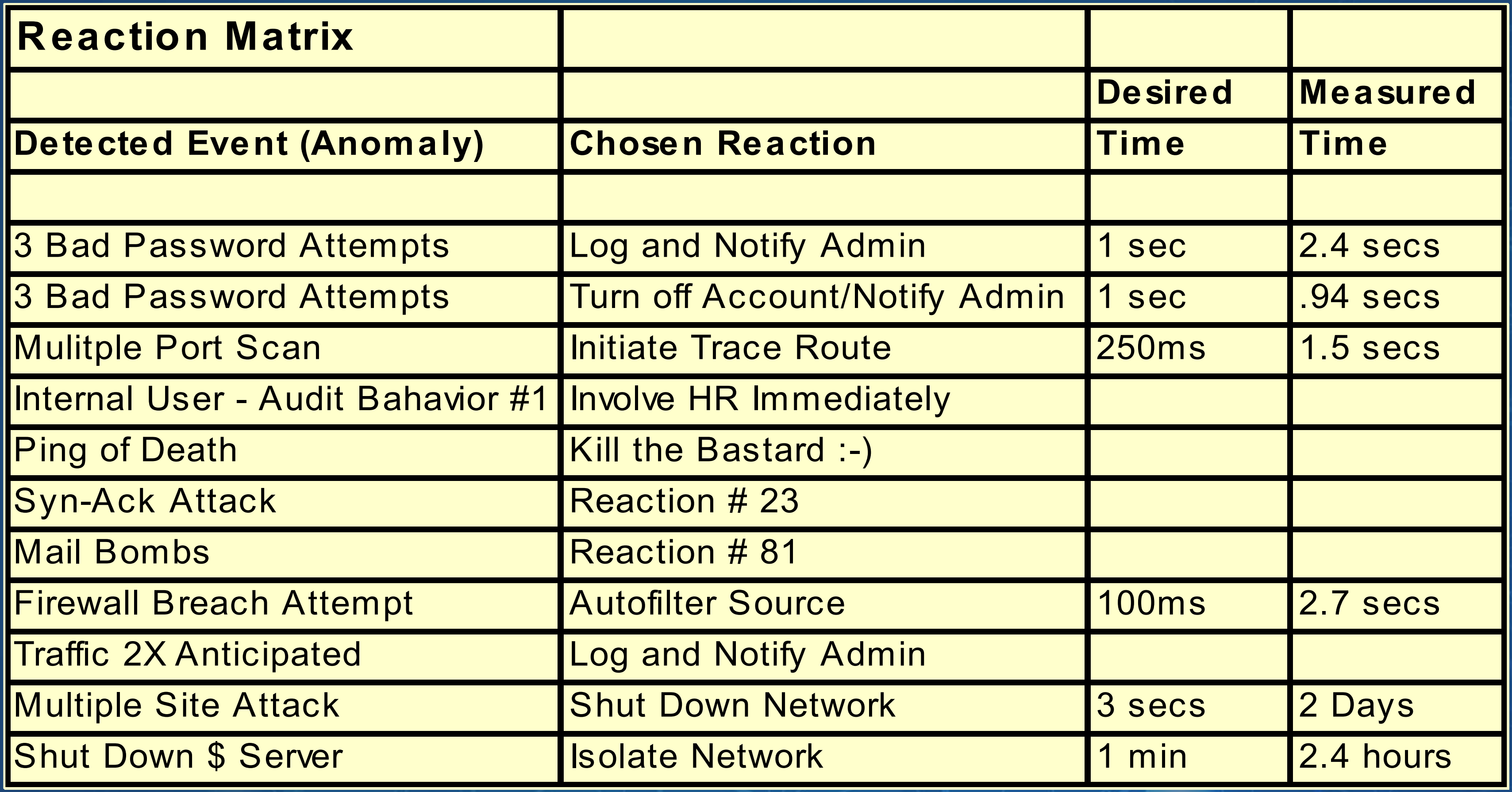
APT: 400+ Days… Seriously?



As Sensors $\to \infty$, $[D_t + R_t] > 0$

Common OOB Security Protocol

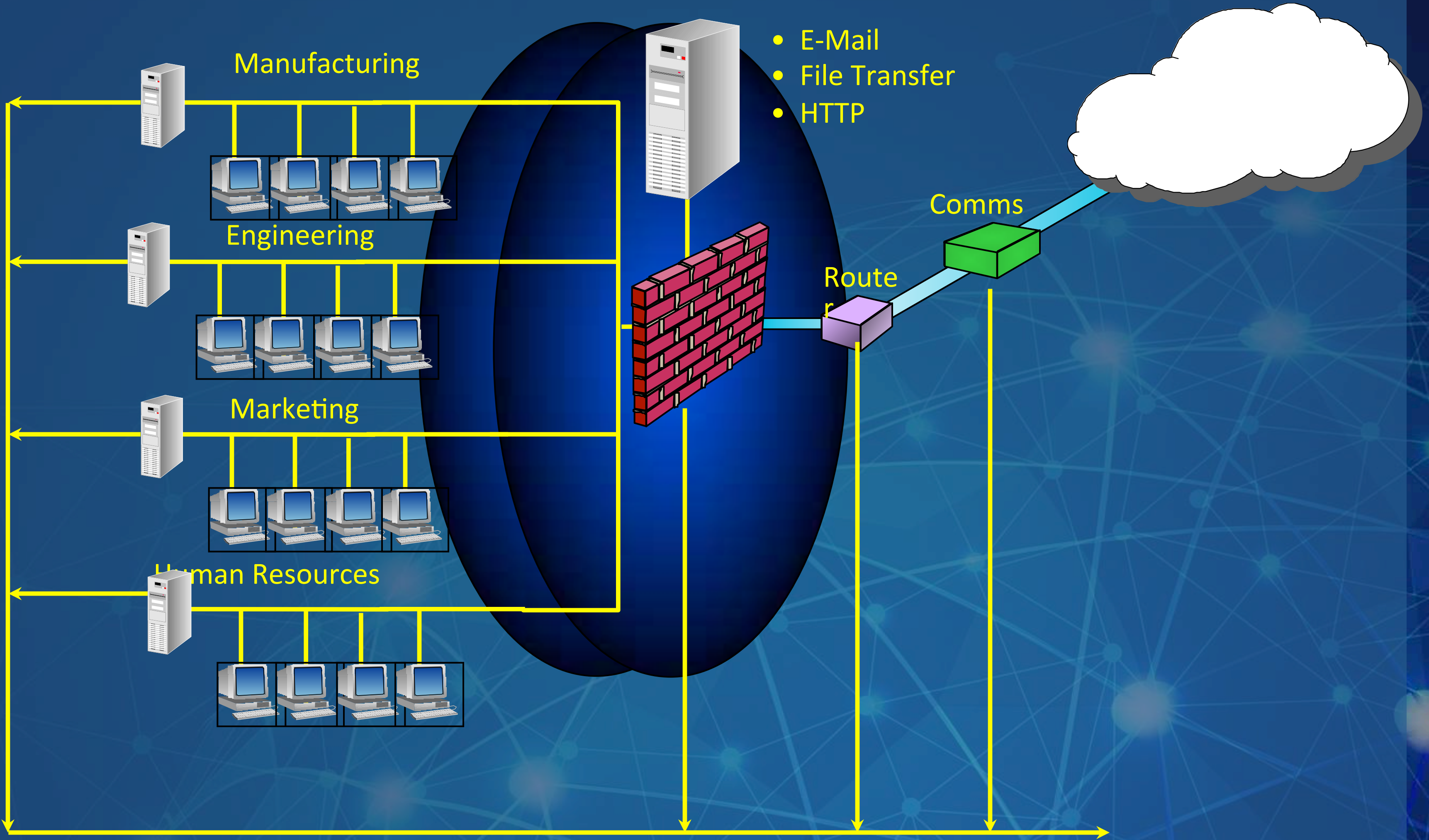
Sample Reaction Matrix



Reaction Matrix			
		Desired	**Measured**
Detected Event (Anomaly)	**Chosen Reaction**	**Time**	**Time**
3 Bad Password Attempts	Log and Notify Admin	1 sec	2.4 secs
3 Bad Password Attempts	Turn off Account/Notify Admin	1 sec	.94 secs
Mulitple Port Scan	Initiate Trace Route	250ms	1.5 secs
Internal User - Audit Bahavior #1	Involve HR Immediately		
Ping of Death	Kill the Bastard :-)		
Syn-Ack Attack	Reaction # 23		
Mail Bombs	Reaction # 81		
Firewall Breach Attempt	Autofilter Source	100ms	2.7 secs
Traffic 2X Anticipated	Log and Notify Admin		
Multiple Site Attack	Shut Down Network	3 secs	2 Days
Shut Down $ Server	Isolate Network	1 min	2.4 hours

What events matrix build

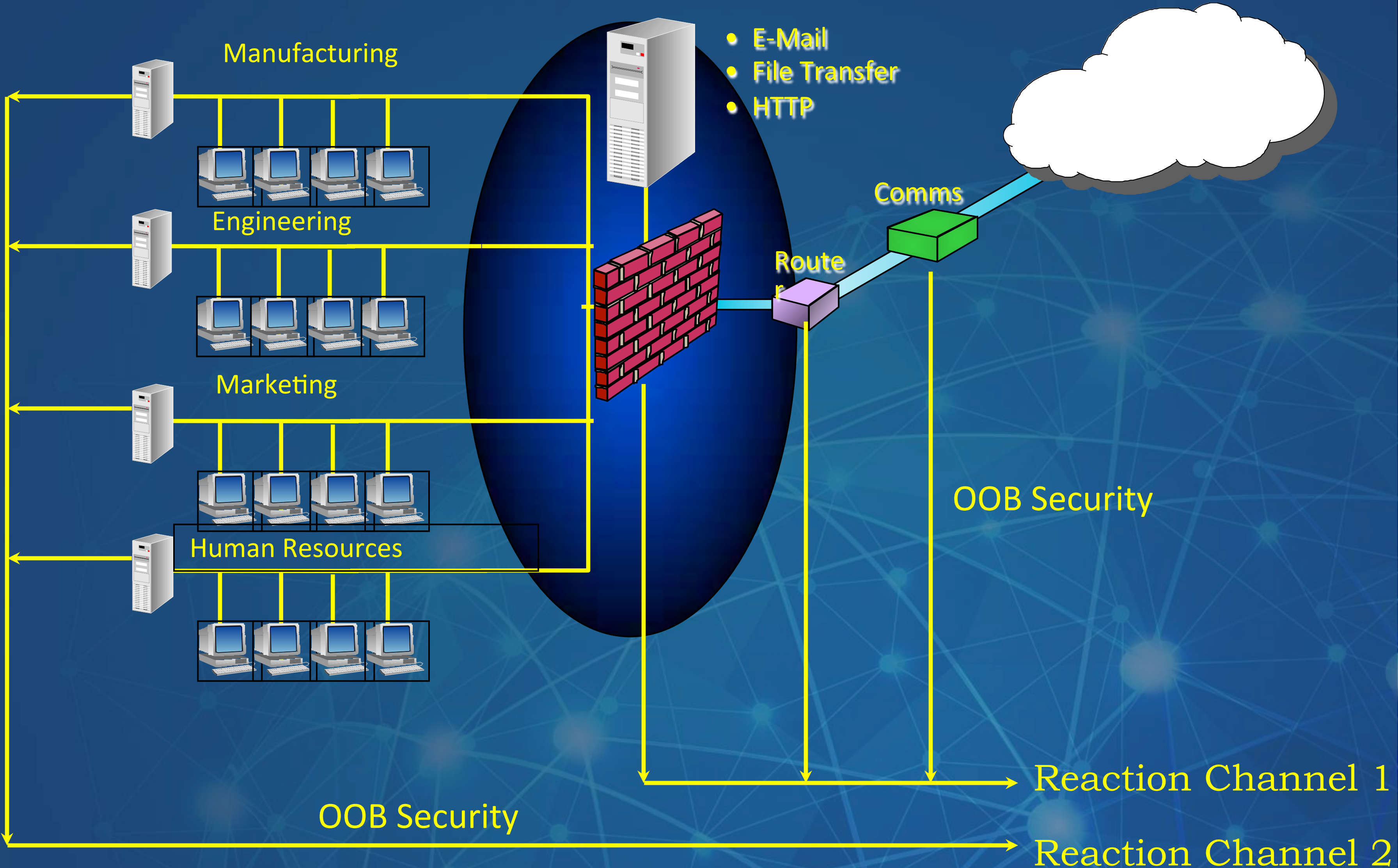
Single Reaction Channel



- E-Mail
- File Transfer
- HTTP

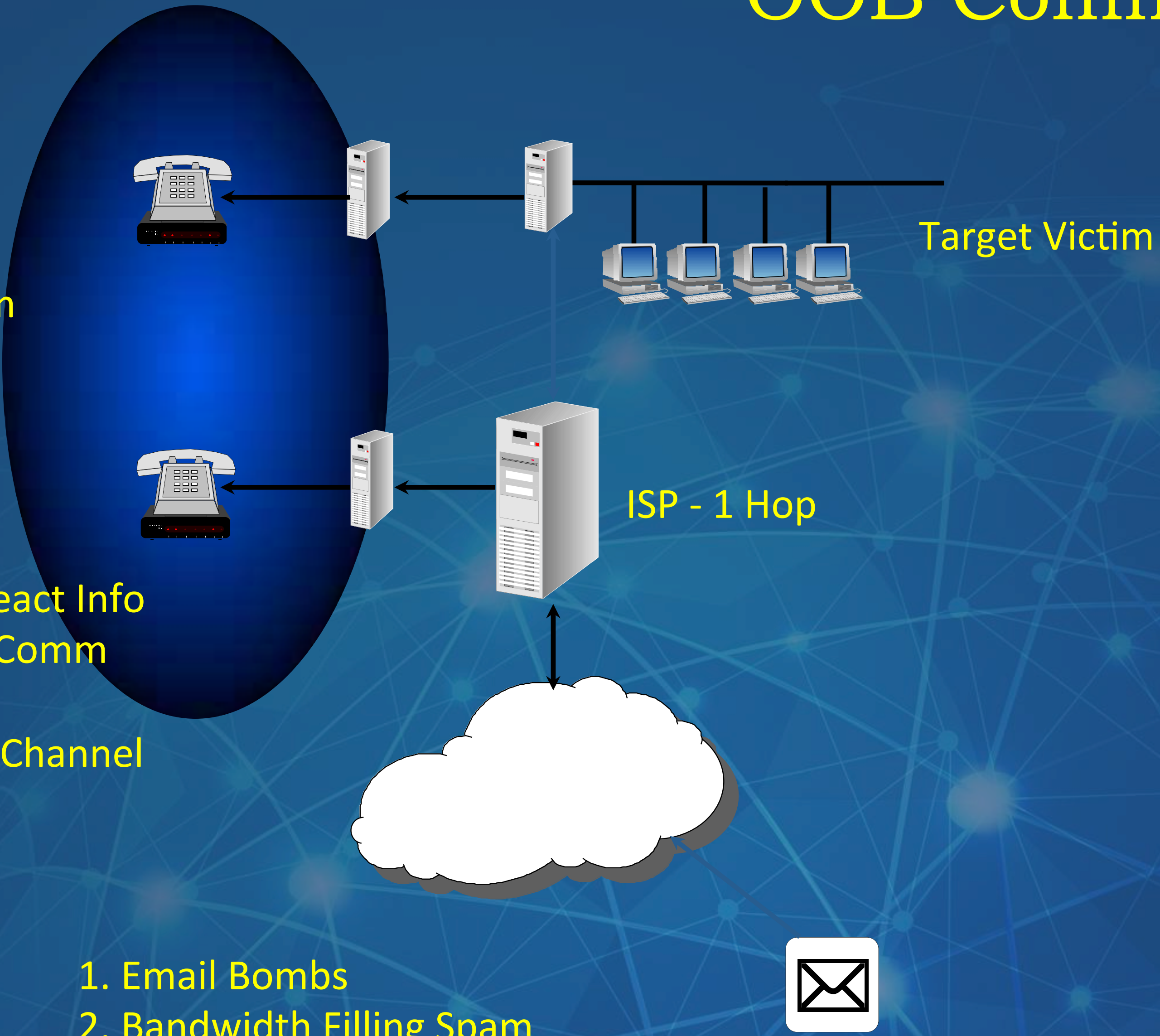
Reaction Matrix: $R_1....R_n$

Detection in Depth



Solving Denial of Service: OOB Comm

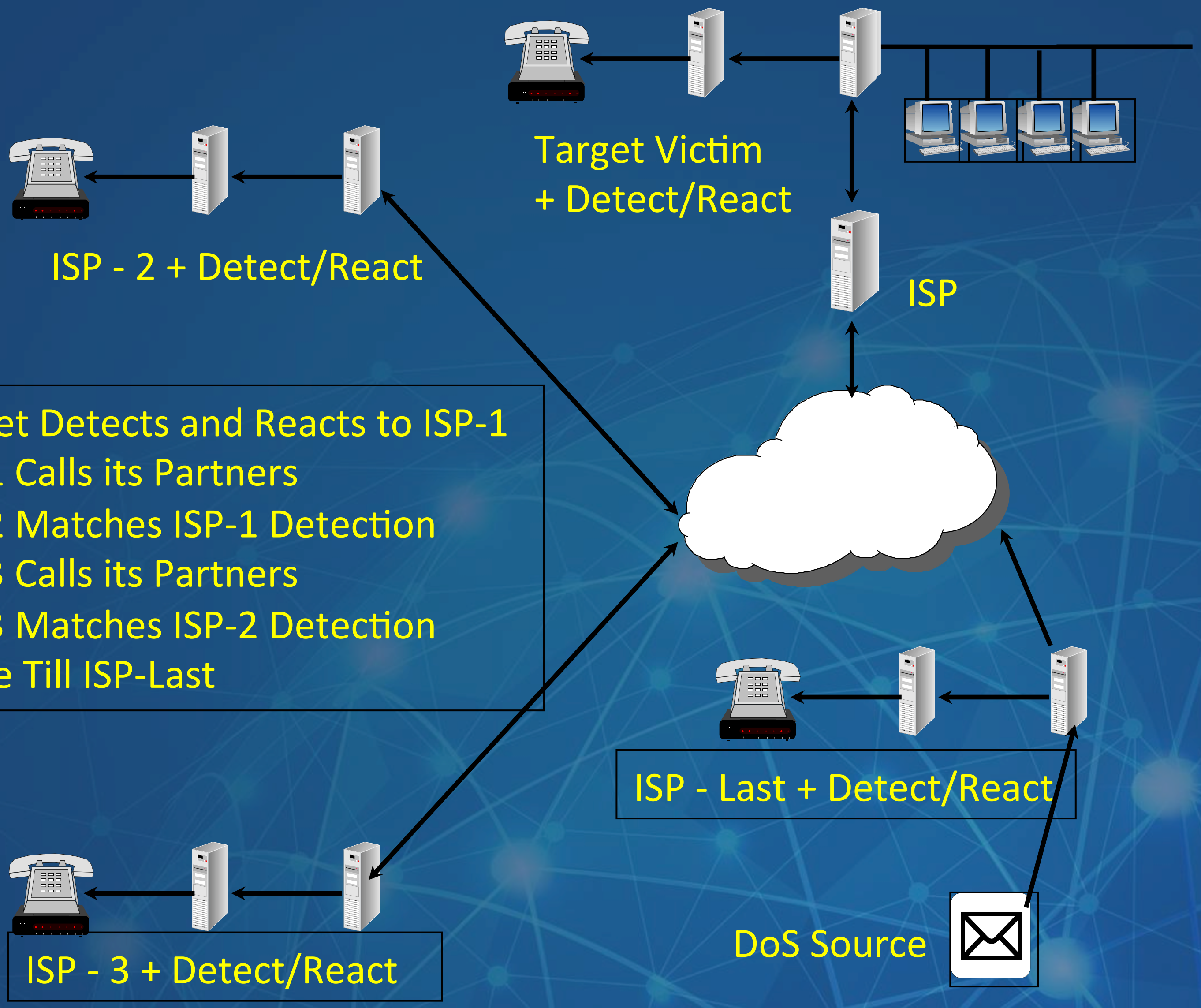
1. Detect Attack
2. React
3. Contact ISP
4. Out-of-Band Comm
5. Filter Attack @ISP



1. Receive Detect/React Info
2. Process/Validate Comm
3. Filter Attack
4. Establish Primary Channel

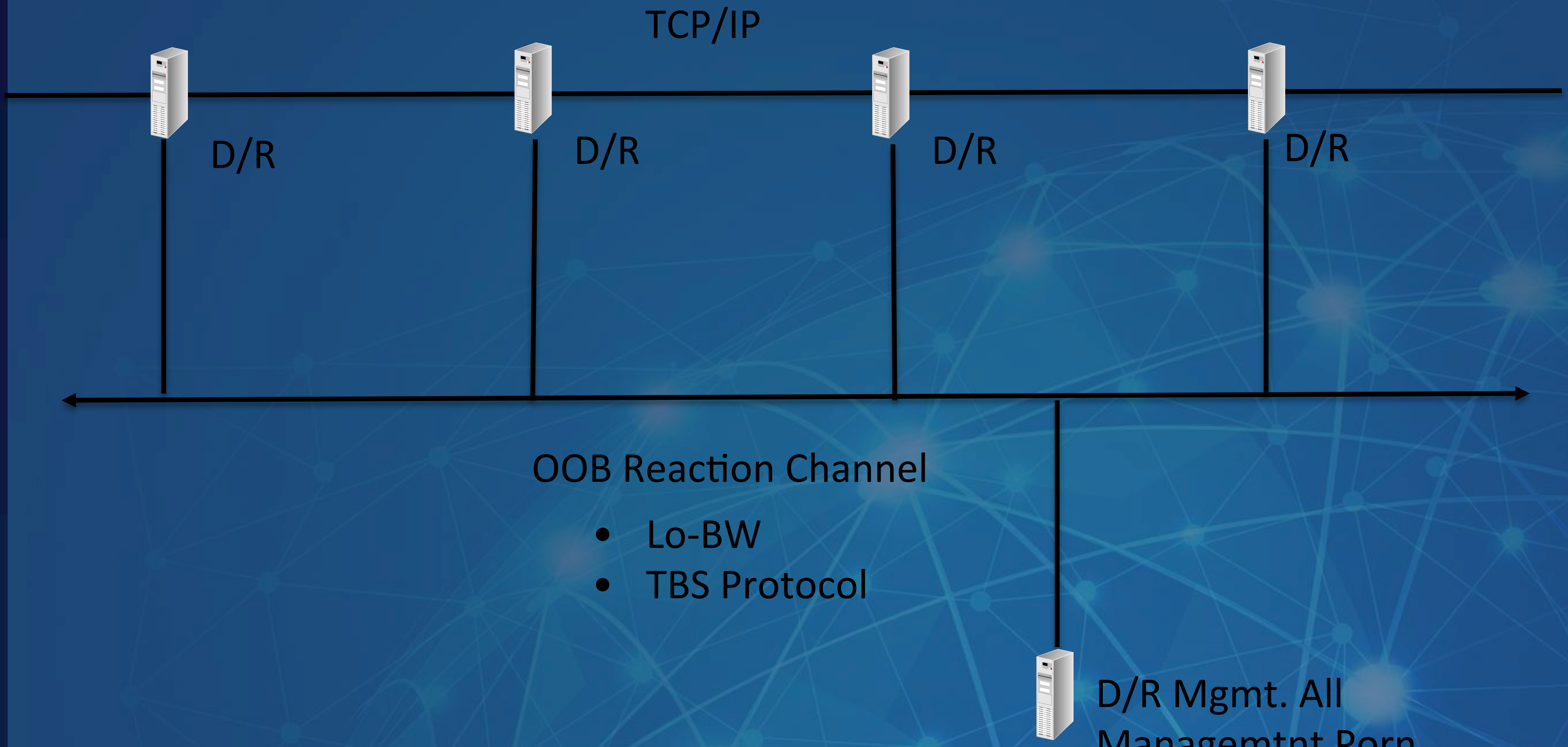
1. Email Bombs
2. Bandwidth Filling Spam
3. Other Denial of Service

Getting at the Source of DoS/CnC/Botnet



1. Target Detects and Reacts to ISP-1
2. ISP-1 Calls its Partners
3. ISP-2 Matches ISP-1 Detection
4. ISP-3 Calls its Partners
5. ISP-3 Matches ISP-2 Detection
6. Trace Till ISP-Last

Out of Band Analogue Security Detection in Depth & Reaction Channel



TCP/IP

D/R

D/R

D/R

D/R

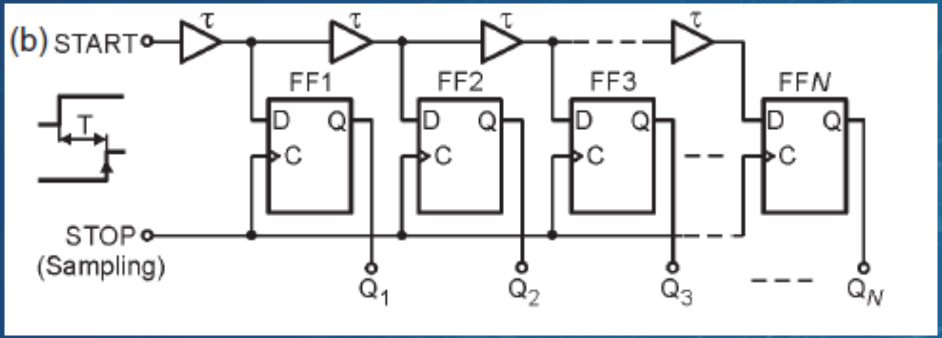
OOB Reaction Channel

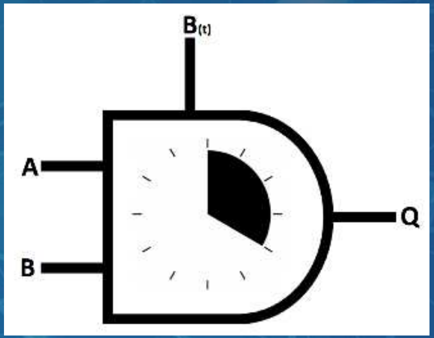
- Lo-BW
- TBS Protocol

D/R Mgmt. All Managemtnt Porn in English clear. Carbon unit analysis and subsequent reactions

Apply ‘Negative’ Time in Sensor & Reaction Based Networks

- Write (Input)
- Delay Time
- Read (Output)





Use Delay Lines to match D(t) + R(t) or T-AND Gates

Optimize for $\underset{t>0}{\textbf{Lim}}\ \mathbf{E_t} = \underset{t>0}{\textbf{Lim}}\ \mathbf{(D_t)} + \underset{t>0}{\textbf{Lim}}\ \mathbf{(R_t)}$

Time Difference < 0, thus perfecting security.

Virtual Queue Stability Theorem:

Recall: $Q_i(t+1) = \max[Q_i(t) + y_i(t), 0]$

Theorem: $Q_i(t)/t \rightarrow 0$ implies $\overline{y}_i \leq 0$.

Proof: $Q_i(\tau+1) = \max[Q_i(\tau) + y_i(\tau), 0]$

$\geq Q_i(\tau) + y_i(\tau)$.

Thus: $Q_i(\tau+1) - Q_i(\tau) \geq y_i(\tau)$ for all τ.

Use ***telescoping sums*** over τ in $\{0, \ldots, t-1\}$:

$$Q_i(t) - Q_i(0) \geq \sum_{\tau=0}^{t-1} y_i(\tau).$$

Divide by t and take limit as $t \rightarrow \infty$. □

What Else Can Analogue Network Security Do For You?

- Encourage International Cooperation
- Measure NW Security … Now!
- Talk to Risk Folks
- Added Resilience
- Stop Bots
- Malware Scanning w/NW-Delay Line
- Stop Click Through Infections (NW-DL)
- IoT – End Point 'Intelligence'
- Improved Mobile/Remote Security
- Enhanced Two Factor

I have not figured it all out yet…

Analogue Network Security Tenets

Nothing is Absolute (‘0’ or ‘1’)

Digital is Not Binary

Dynamic Approach (vs. Static)

Time is the Security Metric

All Data (NWs) Are Not Equal

Security is Fractal

Use Trust Factors

Apply Two Man(+) Rule

Feedback/OODA

Apply Detection in Depth

Sensor Based Granularity

OOB Comm

Fundamental New Logic Elements

Comments? Questions? Responses?

Winn Schwartau

- www.AnalogueNetworkSecurity.Com
- +1 727 393 6600
- CEO/Founder
- TheSecurityAwarenessCompany.Com
- Winn@TheSecurityAwarenessCompany.com

facebook.com/TheSACompany

twitter.com/SecAwareCo

linkedin.com/company/the-security-awareness-company

The Security Awareness Company

Entertaining. Educational. Effective

Winn Schwartau, Founder & CEO
+1.727.393.6600