BBVA
Creando Oportunidades

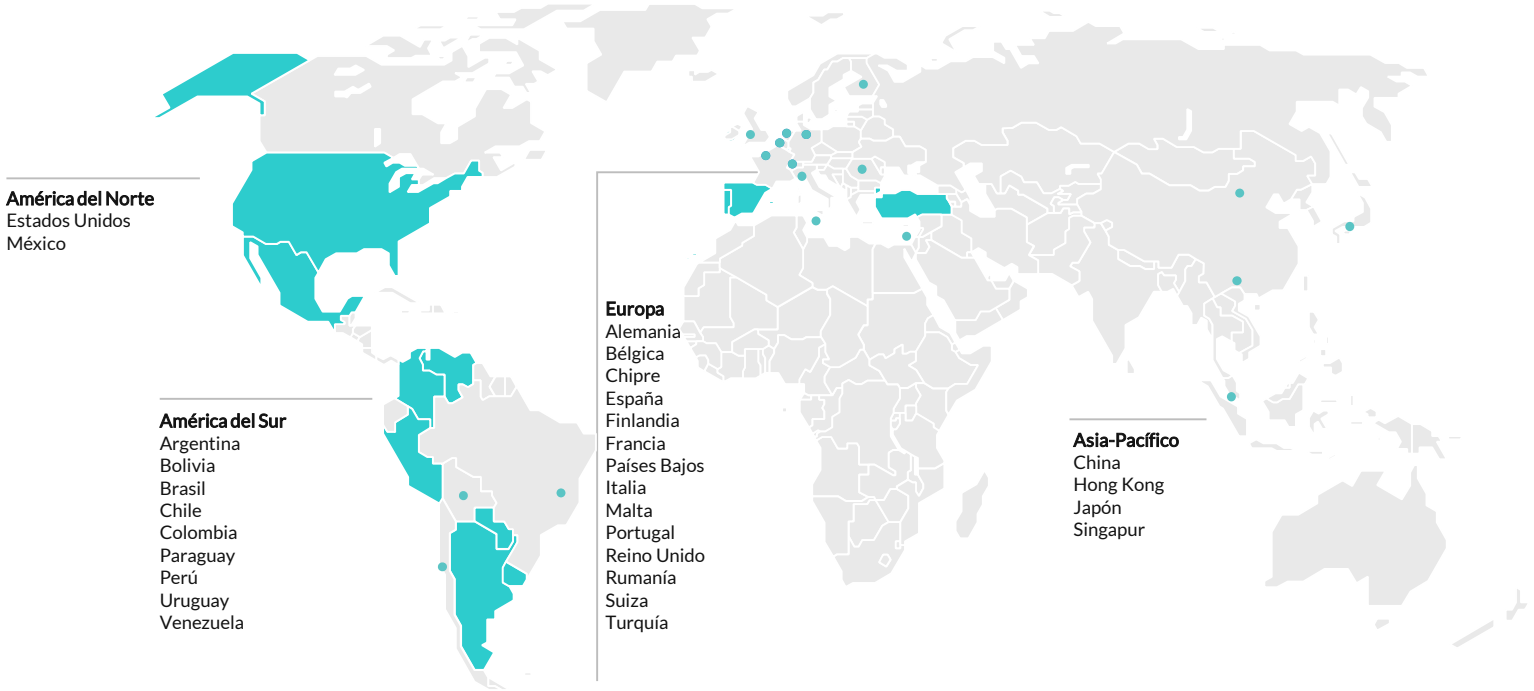
La seguridad ~~no~~ si es un juego

Teoría de juegos aplicada a seguridad
Dinámica de juegos para threat modeling

URJC
Febrero 2020

HackOn

BBVA en el mundo



€ 699
miles de millones de activo total

78,1
millones de clientes

>30
países

7.744
oficinas

32.658
cajeros

126.973
empleados

Información a cierre de diciembre 2019. El mapa excluye aquellos países en los que BBVA no tiene sociedad o el nivel de actividad es reducido

BBVA

Creando Oportunidades

MM0003CA:~ whoami luissaiz

Luis Saiz Gimeno

@lsaiz

Telecomm. Eng. - Cryptography - Sys.Sec - Info.Sec - Tech. Fraud Prevention - Fraud Prevention Tech. - Global Security Center - Innovation in Security @BBVA

Madrid

bbva.com/en/featured/bb…

Se unió en julio de 2010

BBVA
Creando Oportunidades

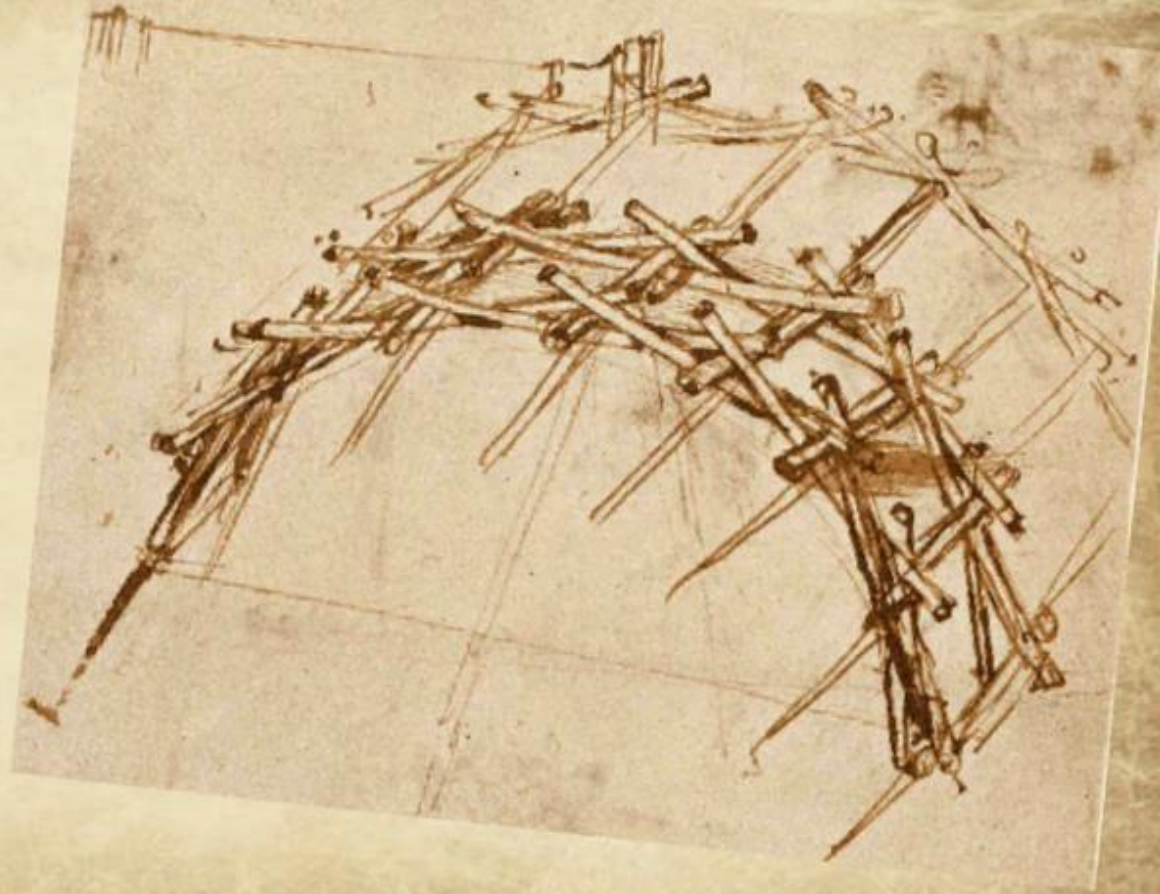
Índice

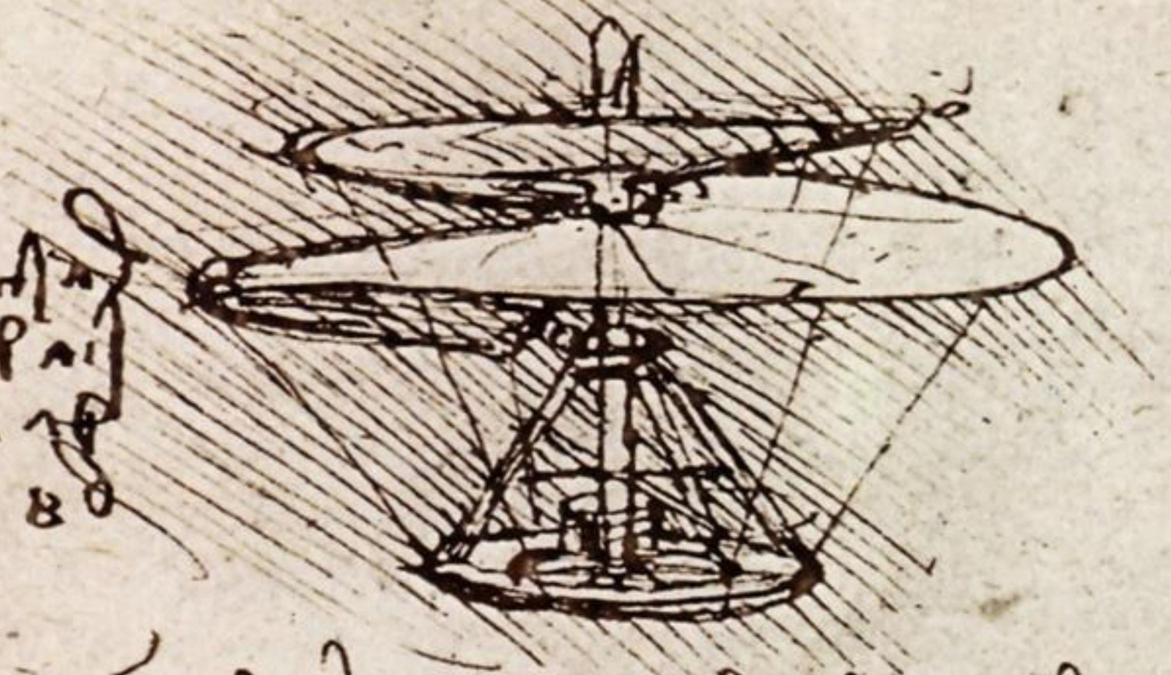
BBVA
Creando Oportunidades

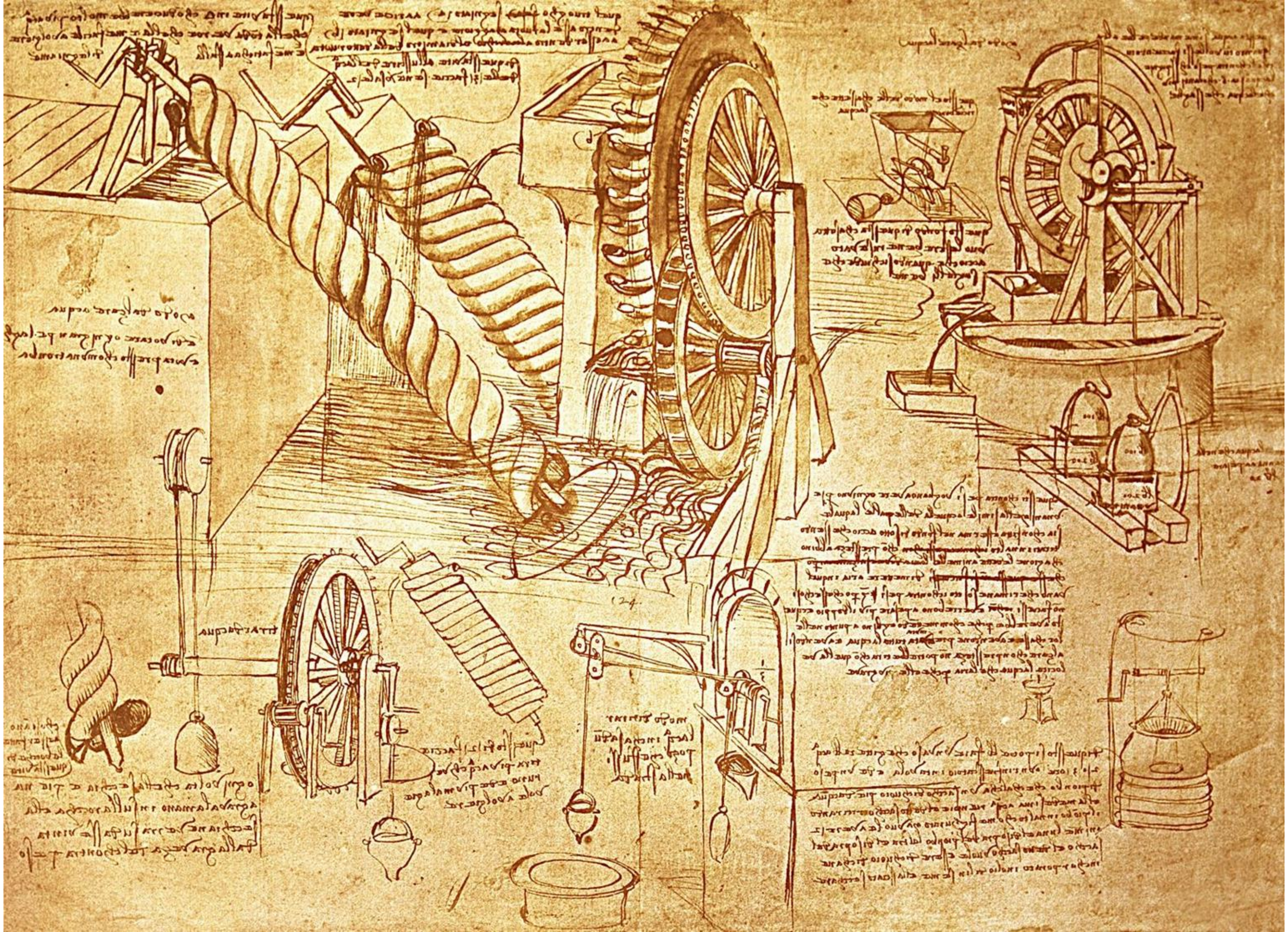
01

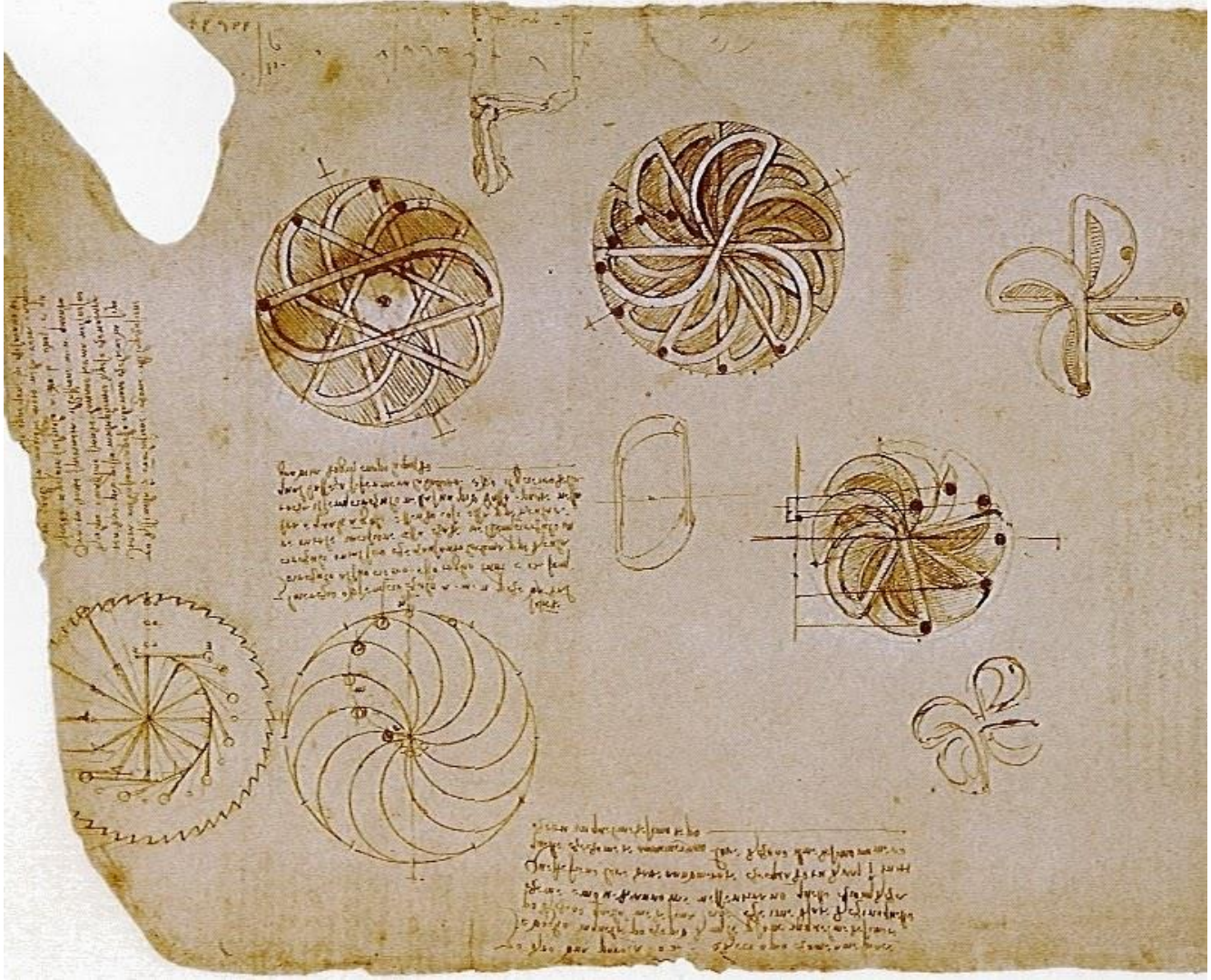
Adversarial Risk

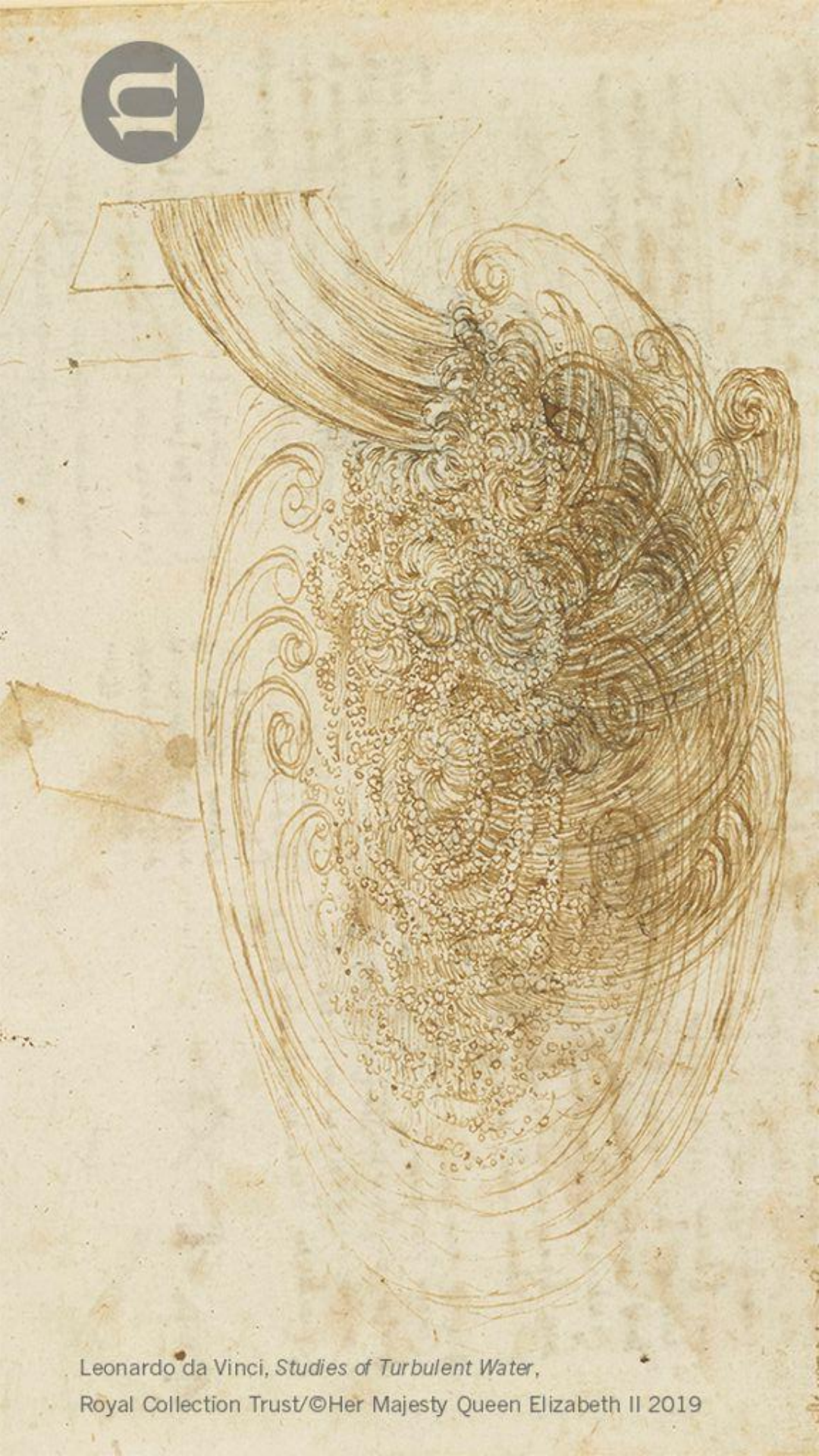
¿Contra qué lucha cada ingeniero?







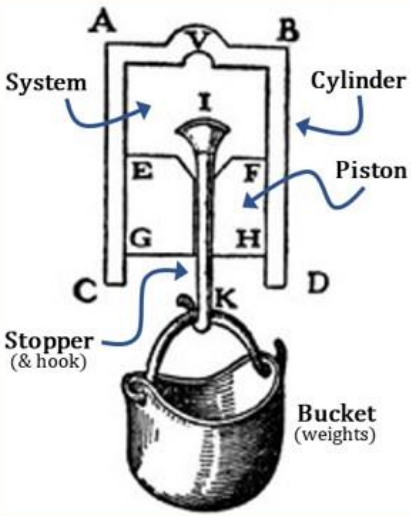




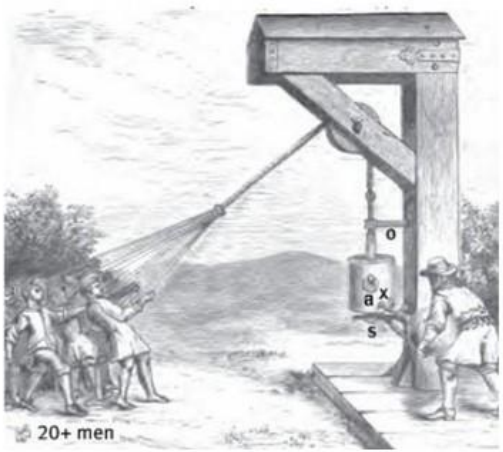
Leonardo da Vinci, *Studies of Turbulent Water*,
Royal Collection Trust/©Her Majesty Queen Elizabeth II 2019


Thug
Life

History of Thermodynamics

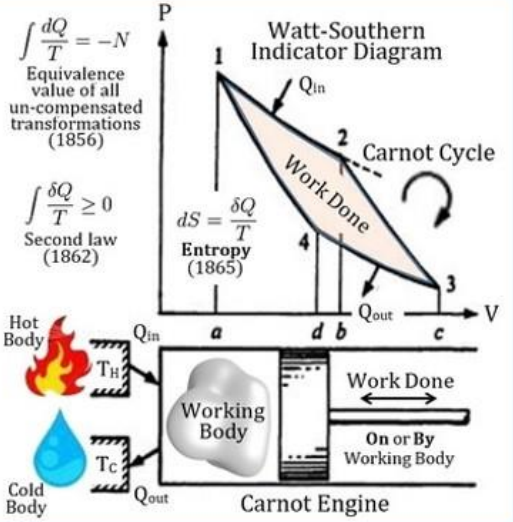


Galileo Vacuum Device
(1632)



Guericke Vacuum Engine
(c.1670)

Papin Engine
(1690)



Carnot Engine
(1824)

Information Theory: Shannon Information

The Mathematical Theory of Communication

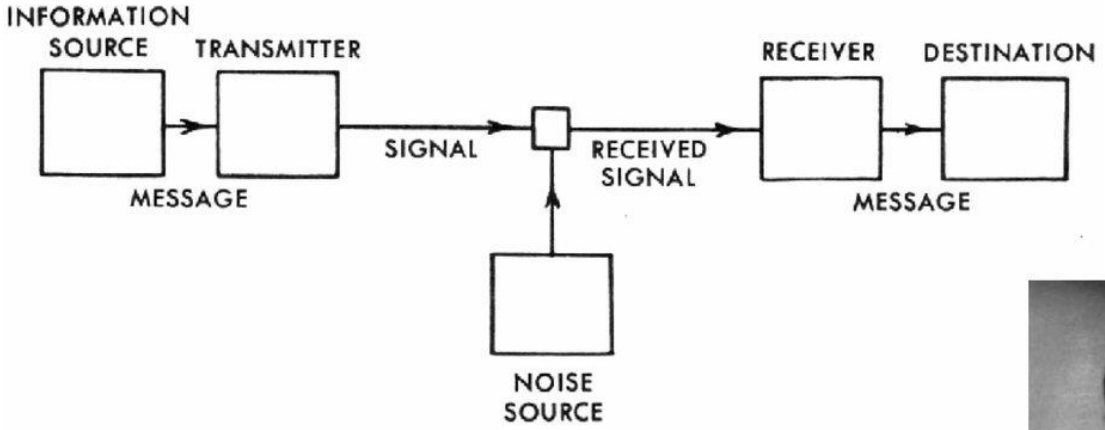
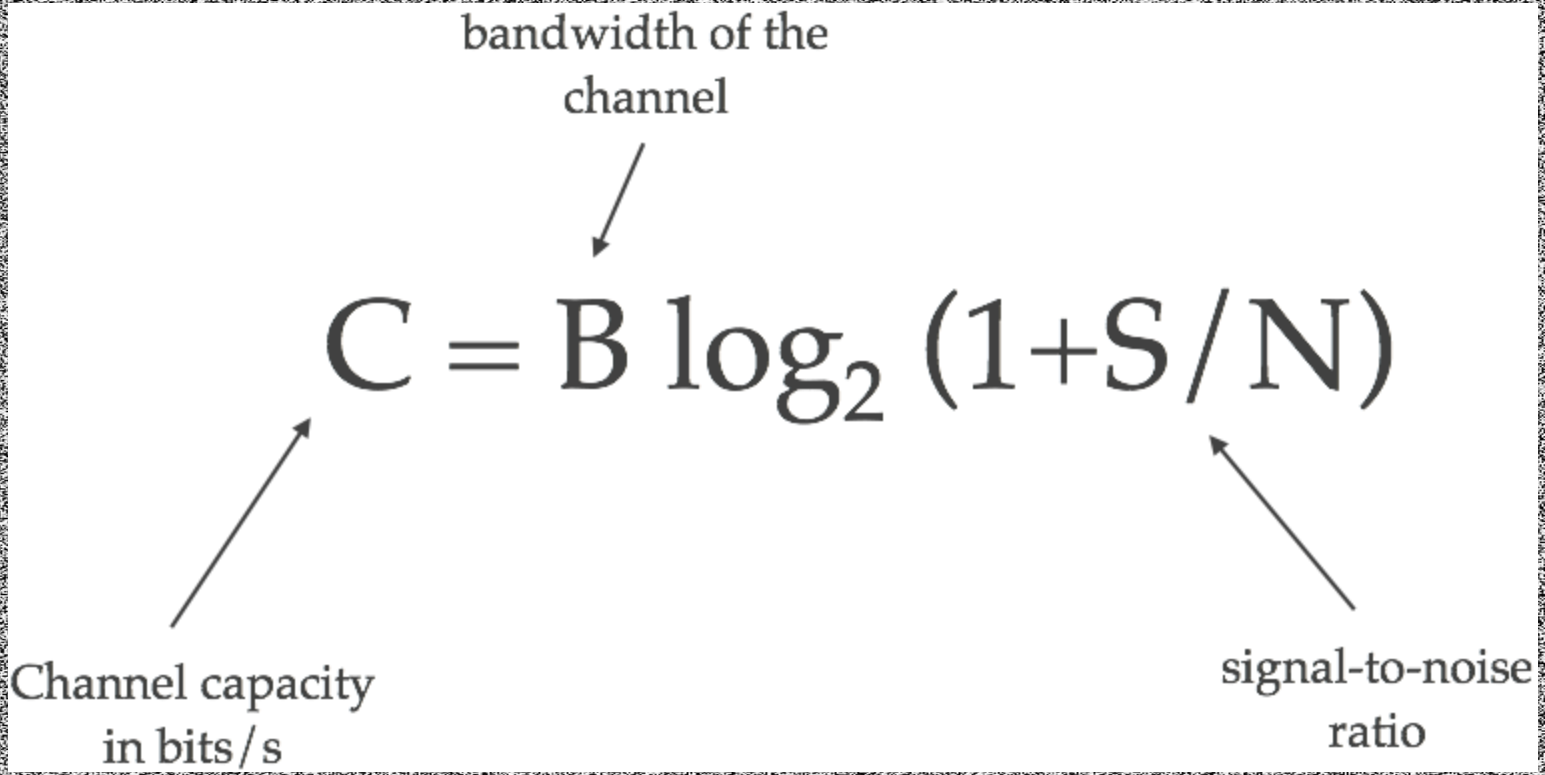


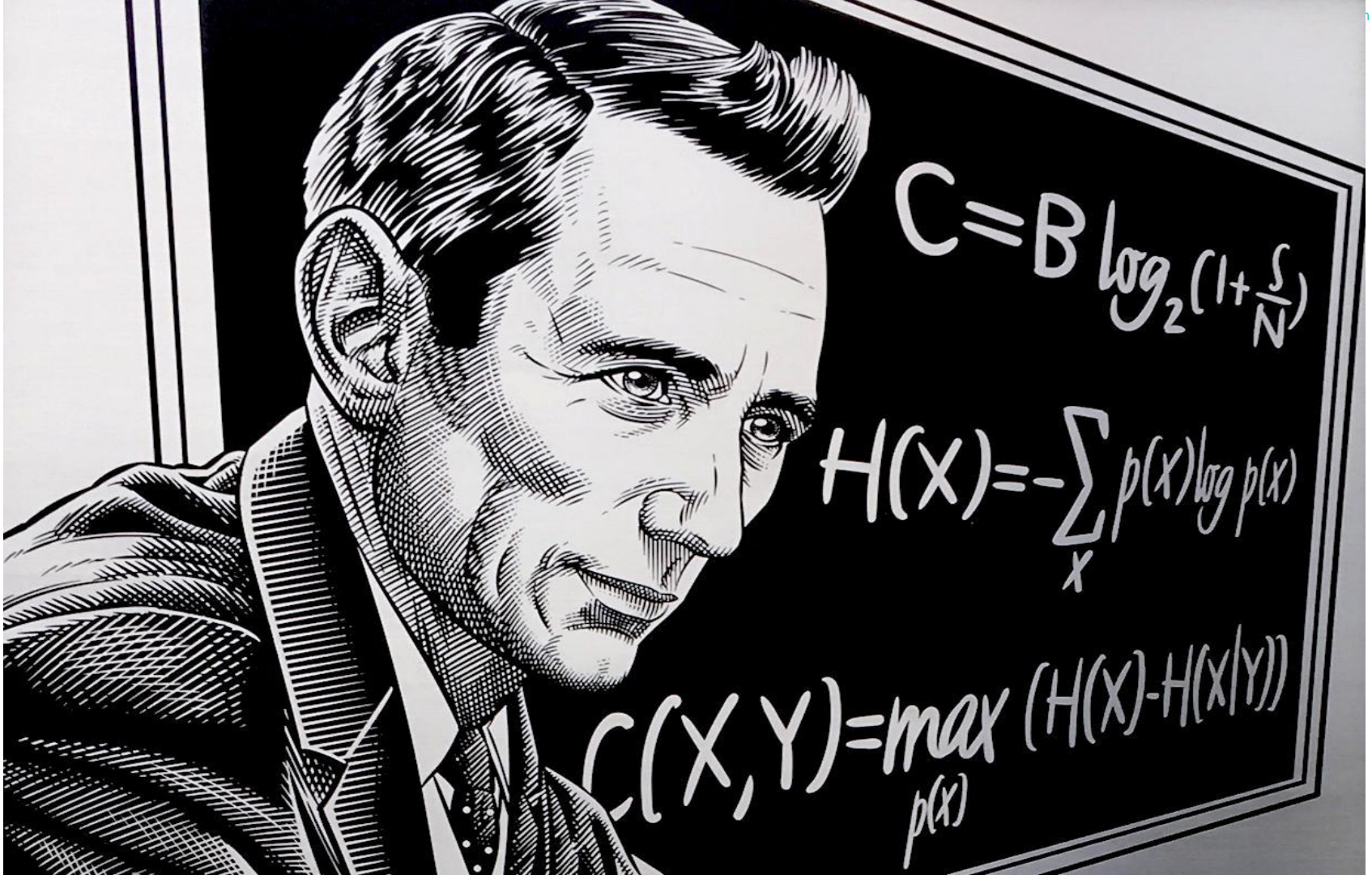
Fig. 1. — Schematic diagram of a general communication system.

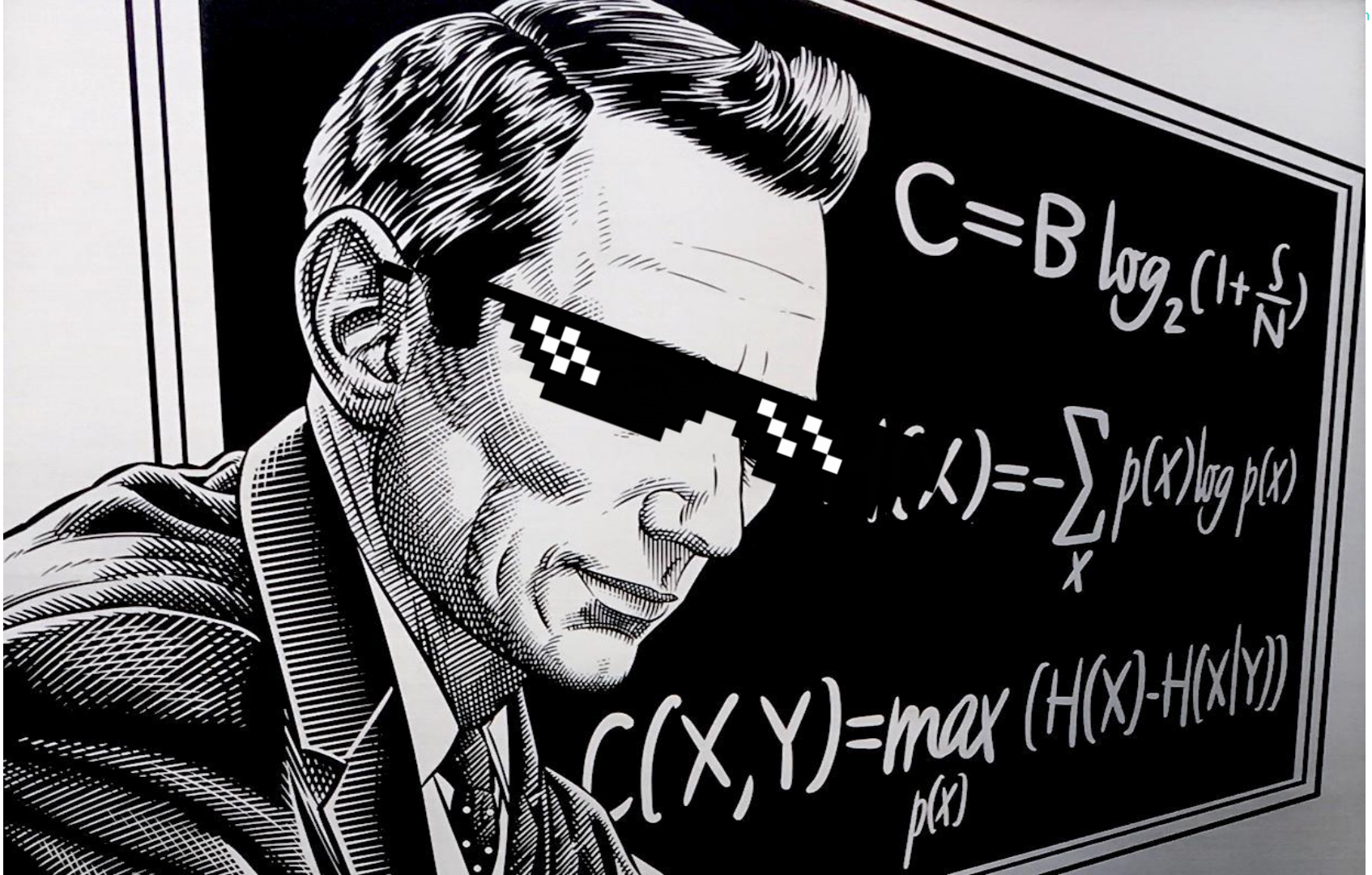
→ Shannon information can only be lost, never gained

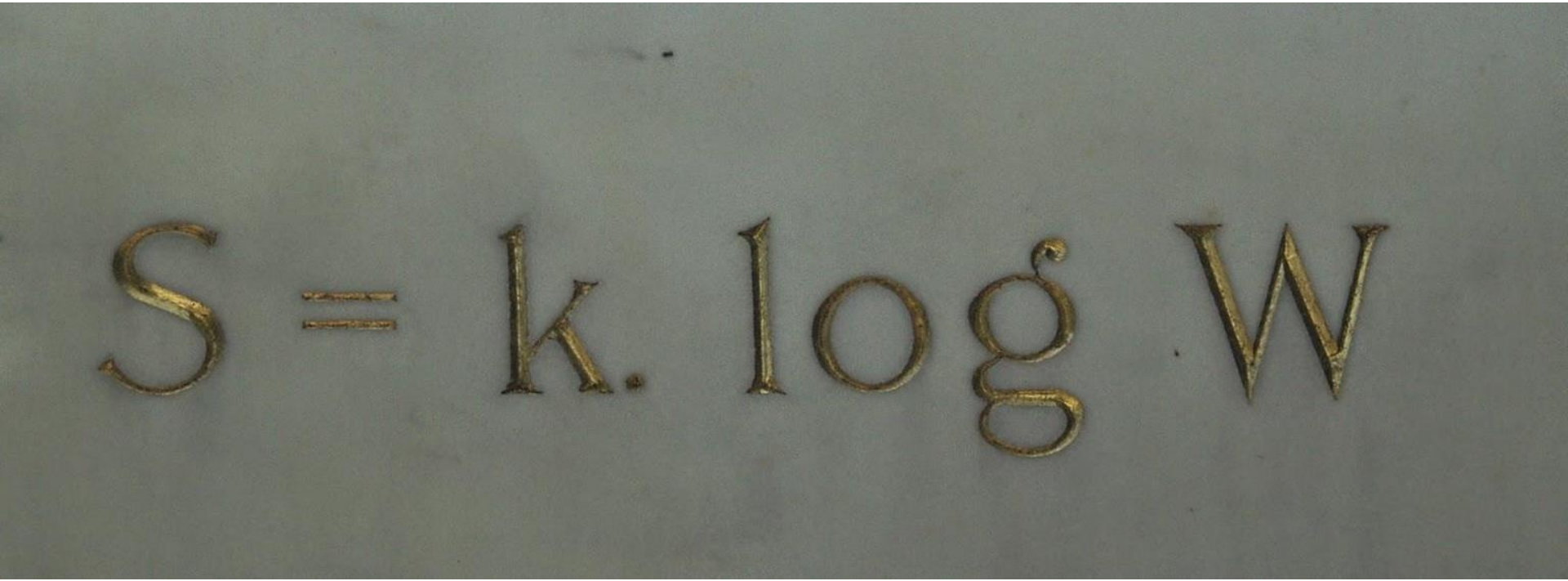
Claude Shannon
1916–2001

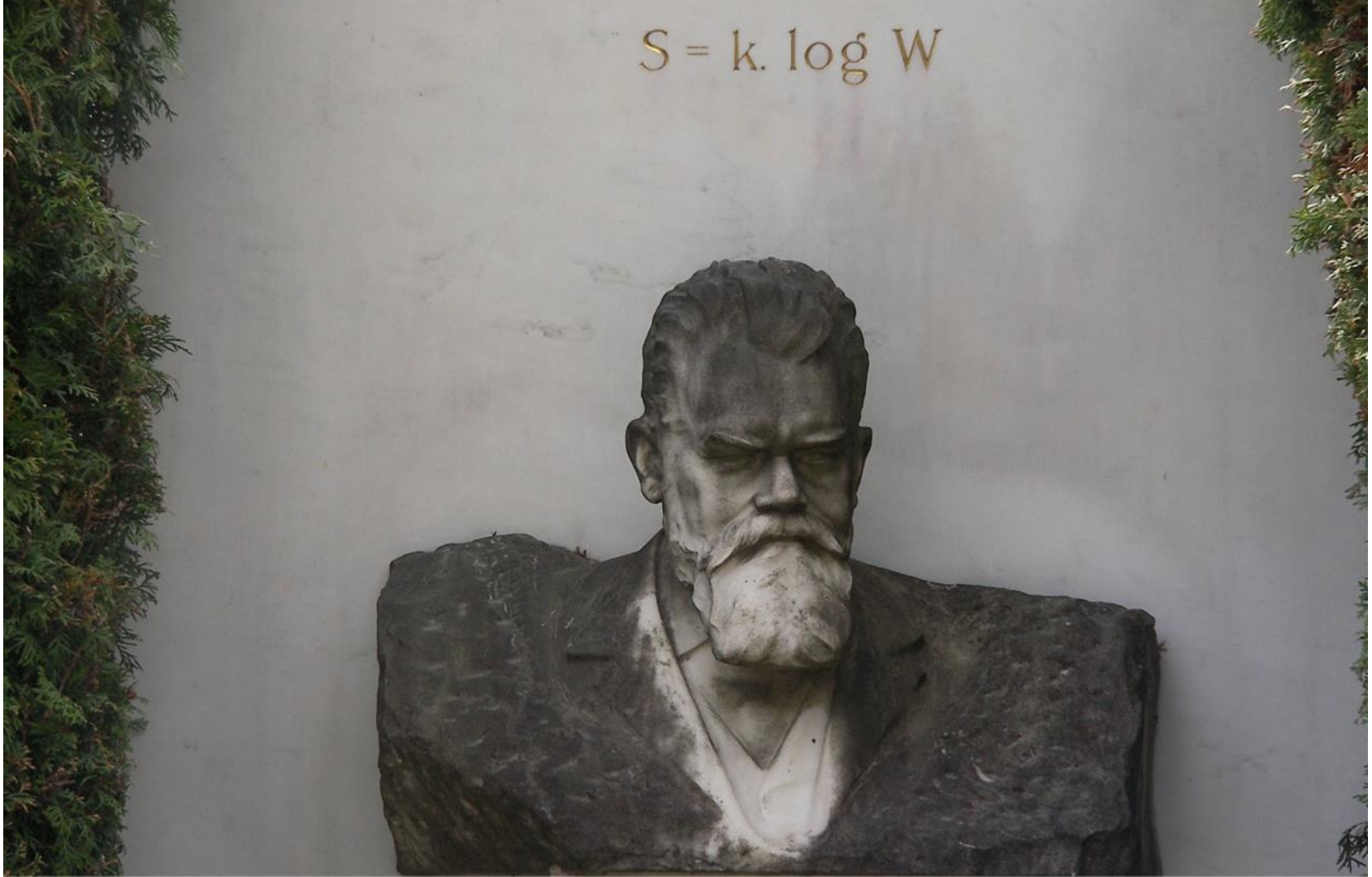
Shannon (1948). *Bell Systems Technical Journal* 27: 379.


bandwidth of the channel
$C = B \log_2 (1+S/N)$
Channel capacity in bits/s
signal-to-noise ratio

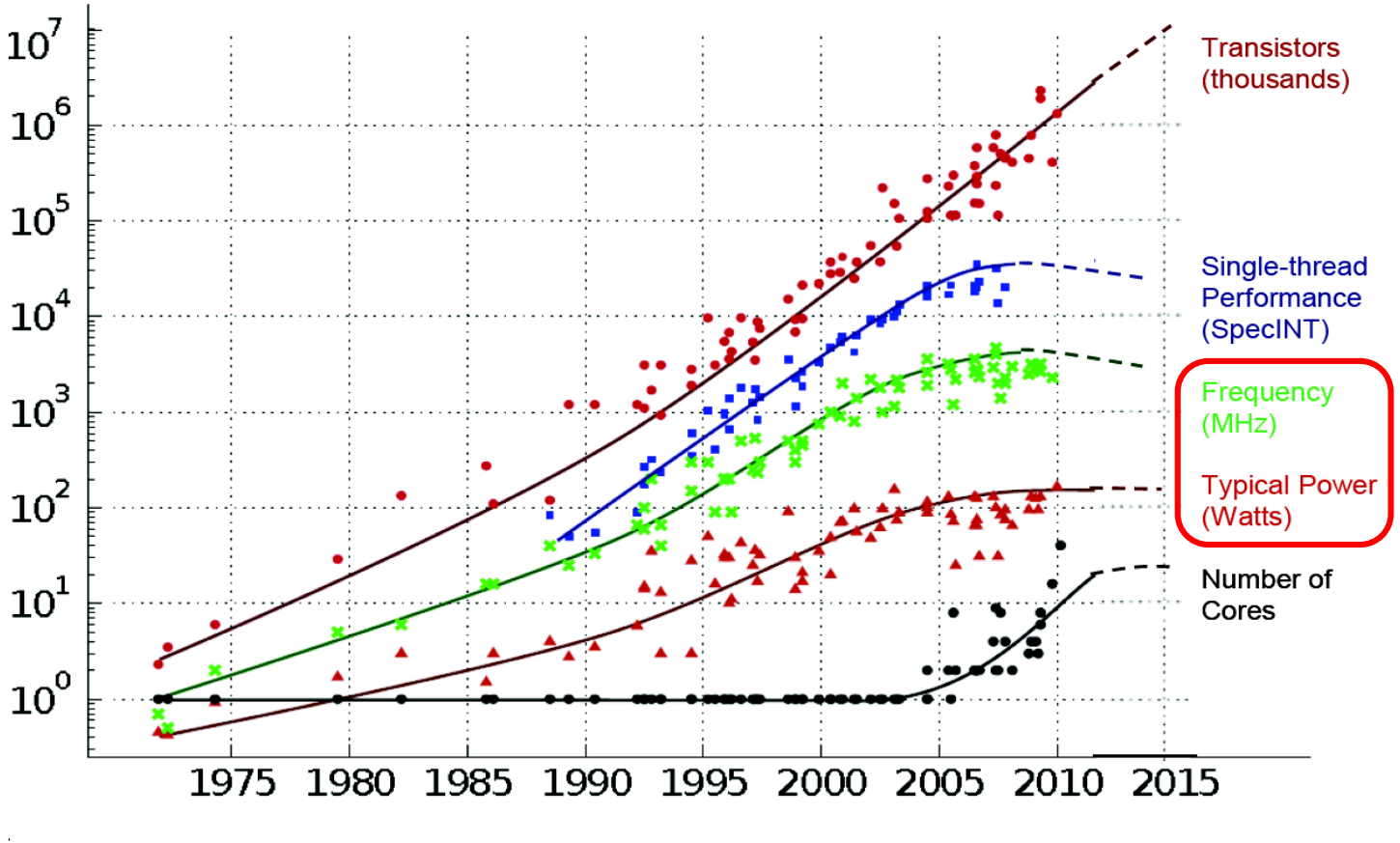

C=B log2(1+S/N)
H(X)=-∑x p(x)log p(x)
C(X,Y)=max p(x) (H(X)-H(X|Y))


C=B log2(1+S/N)
p(x)=-∑x p(x)log p(x)
C(X,Y)=max p(x) (H(X)-H(X|Y))


S = k. log W


S = k. log W

35 YEARS OF MICROPROCESSOR TREND DATA



Original data collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond and C. Batten
Dotted line extrapolations by C. Moore

I blame entropy!

Complex

the relationship between cause and effect can only be perceived in retrospect

probe – sense - respond

emergent practice

Complicated

the relationship between cause and effect requires analysis or some other form of investigation and/or the application of expert knowledge

sense – analyze - respond

good practice

novel practice

no relationship between cause and effect at systems level

act – sense -respond

Chaotic

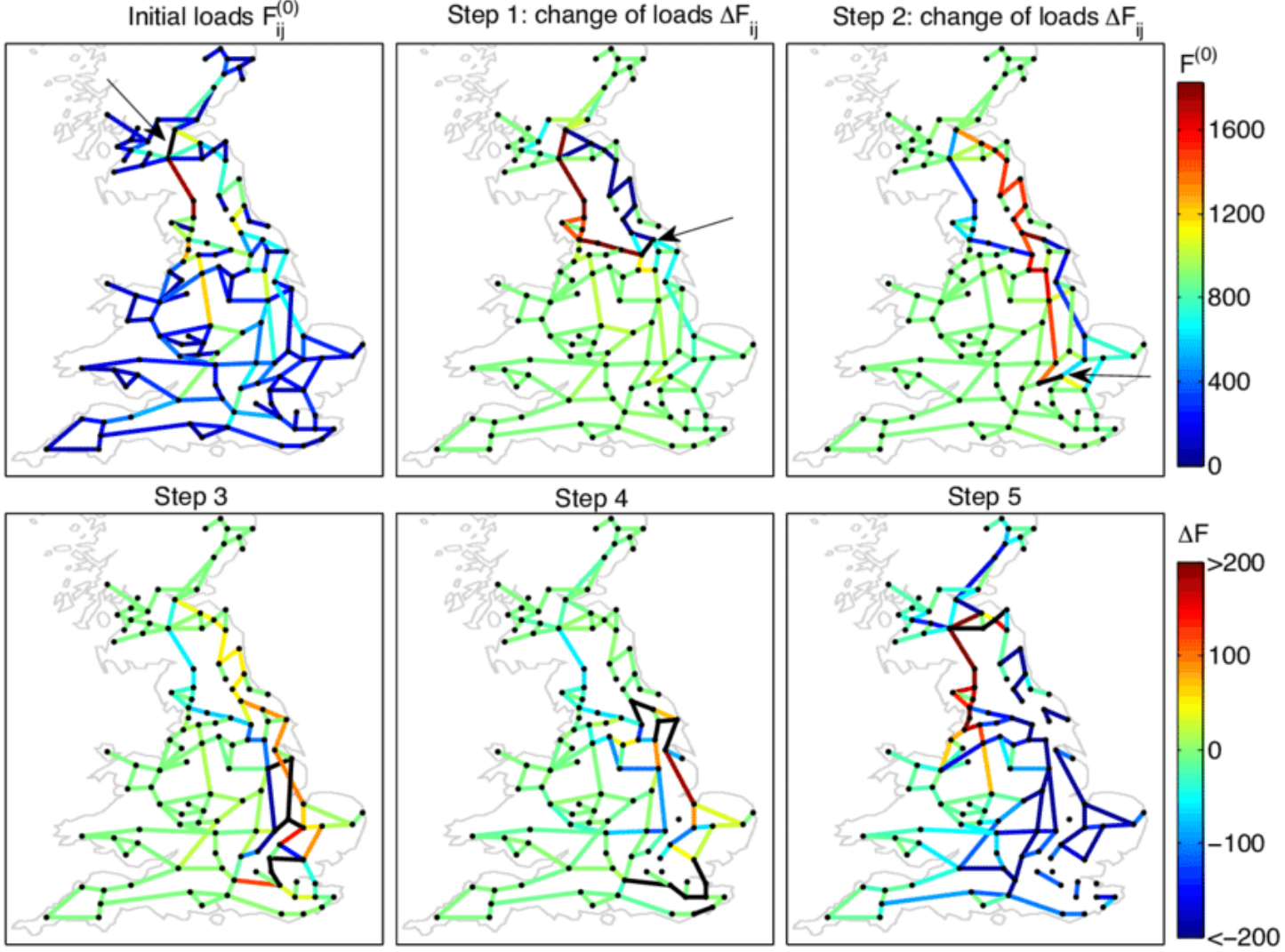
best practice

the relationship between cause and effect is obvious to all

sense – categorize - respond

Simple

The Cynefin Framework. Snowden, D.J. Boone, M. 2007. "A Leader's Framework for Decision Making". Harvard Business Review, November 2007, pp. 69–76.


Initial loads $F_{ij}^{(0)}$
Step 1: change of loads ΔF_{ij}
Step 2: change of loads ΔF_{ij}
$F^{(0)}$
1600
1200
800
400
0
Step 3
Step 4
Step 5
ΔF
>200
100
0
−100
<−200

Contra qué lucha cada ingeniero

Las Leyes de la Naturaleza

Contra qué lucha cada ingeniero

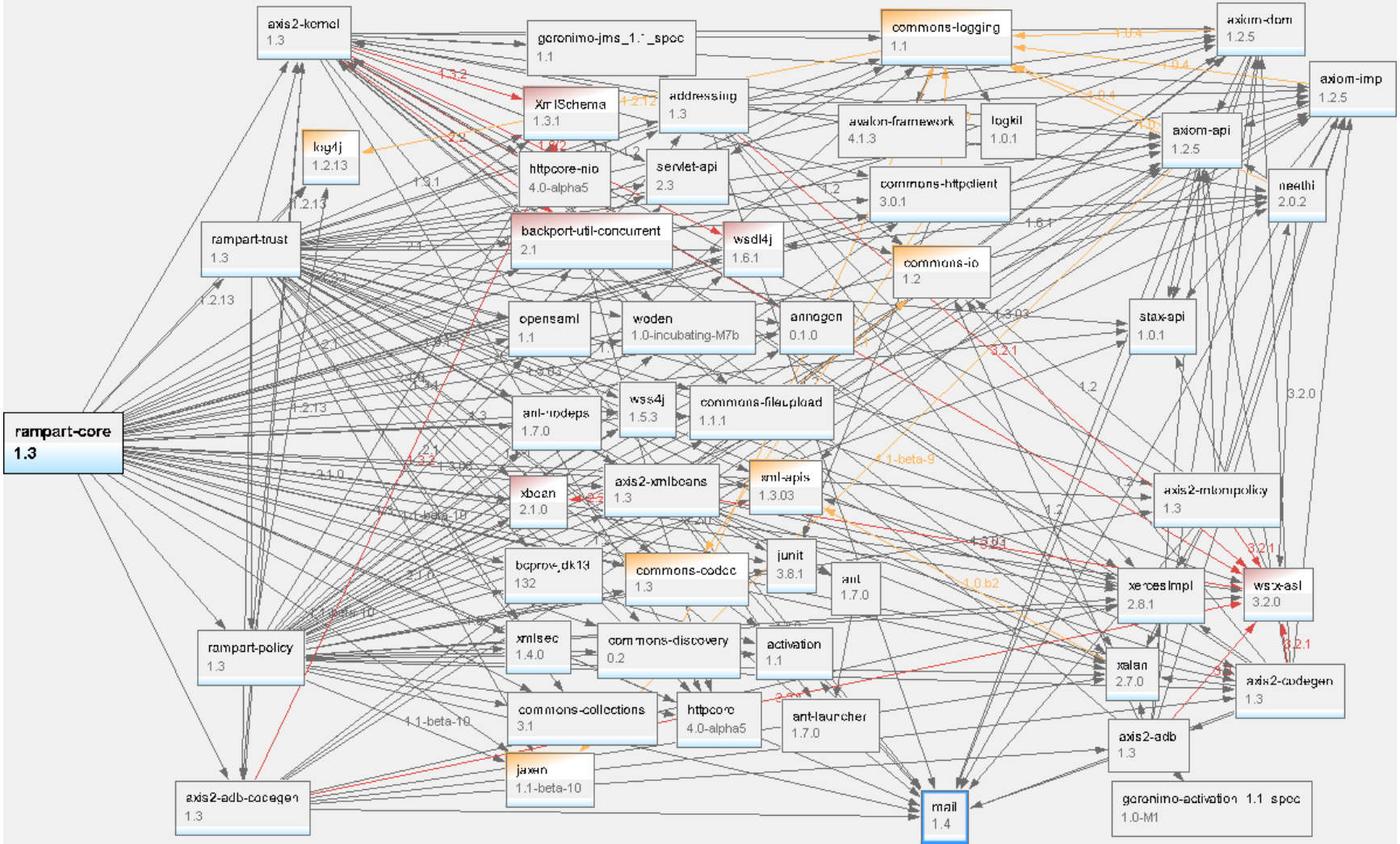
Las Leyes de la Naturaleza

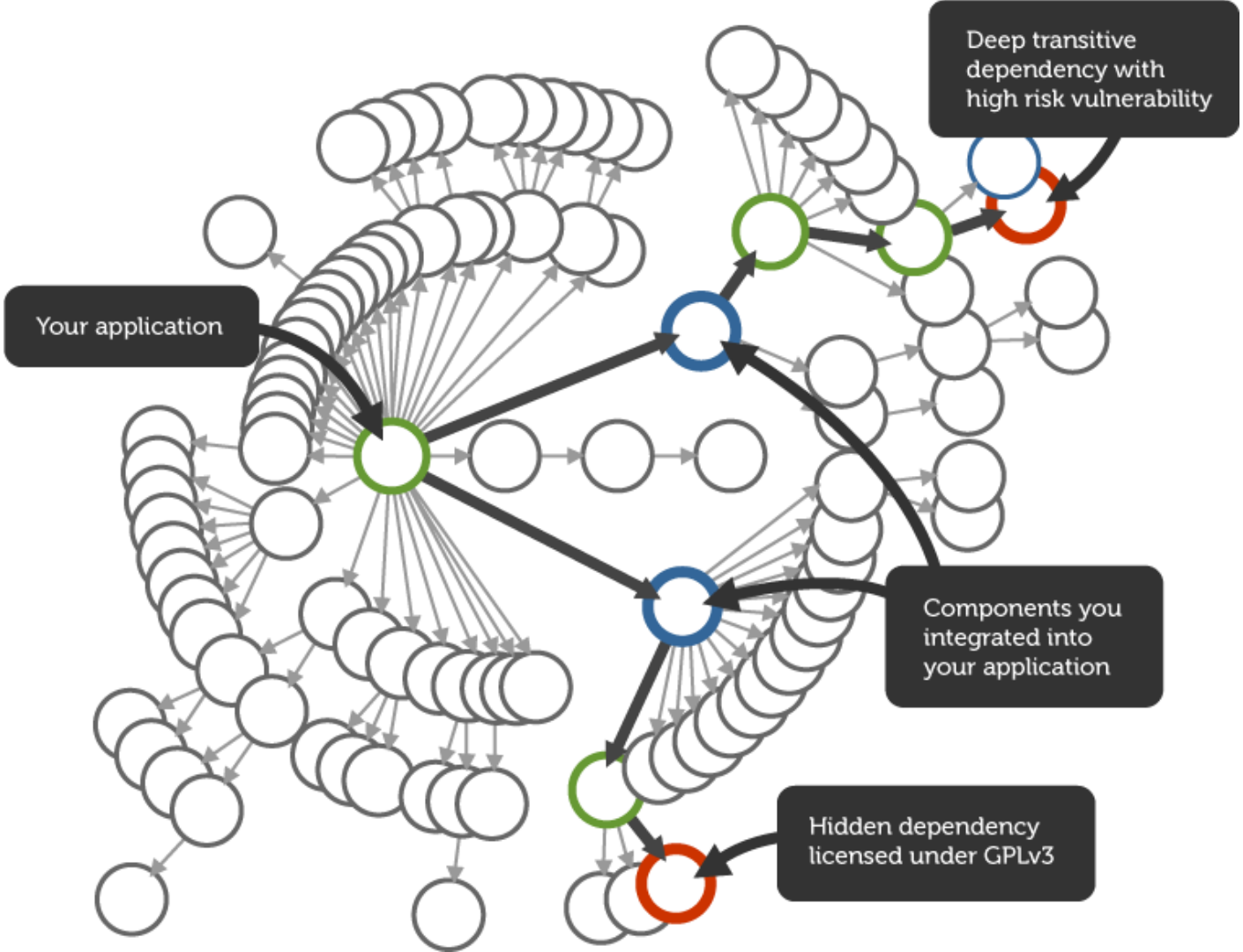
¿Y un ingeniero de Ciberseguridad?

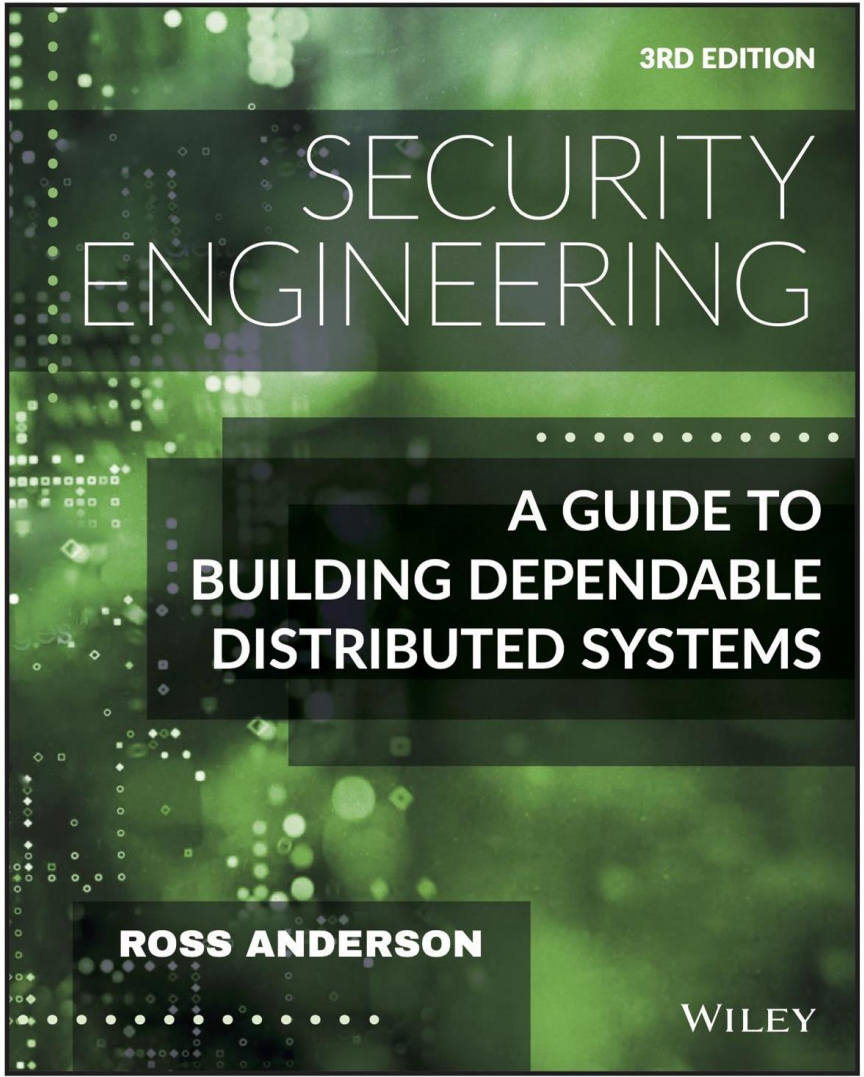
Adversarial

Intentional risk

https://pixabay.com/photos/window-window-grille-lattice-window-243074/

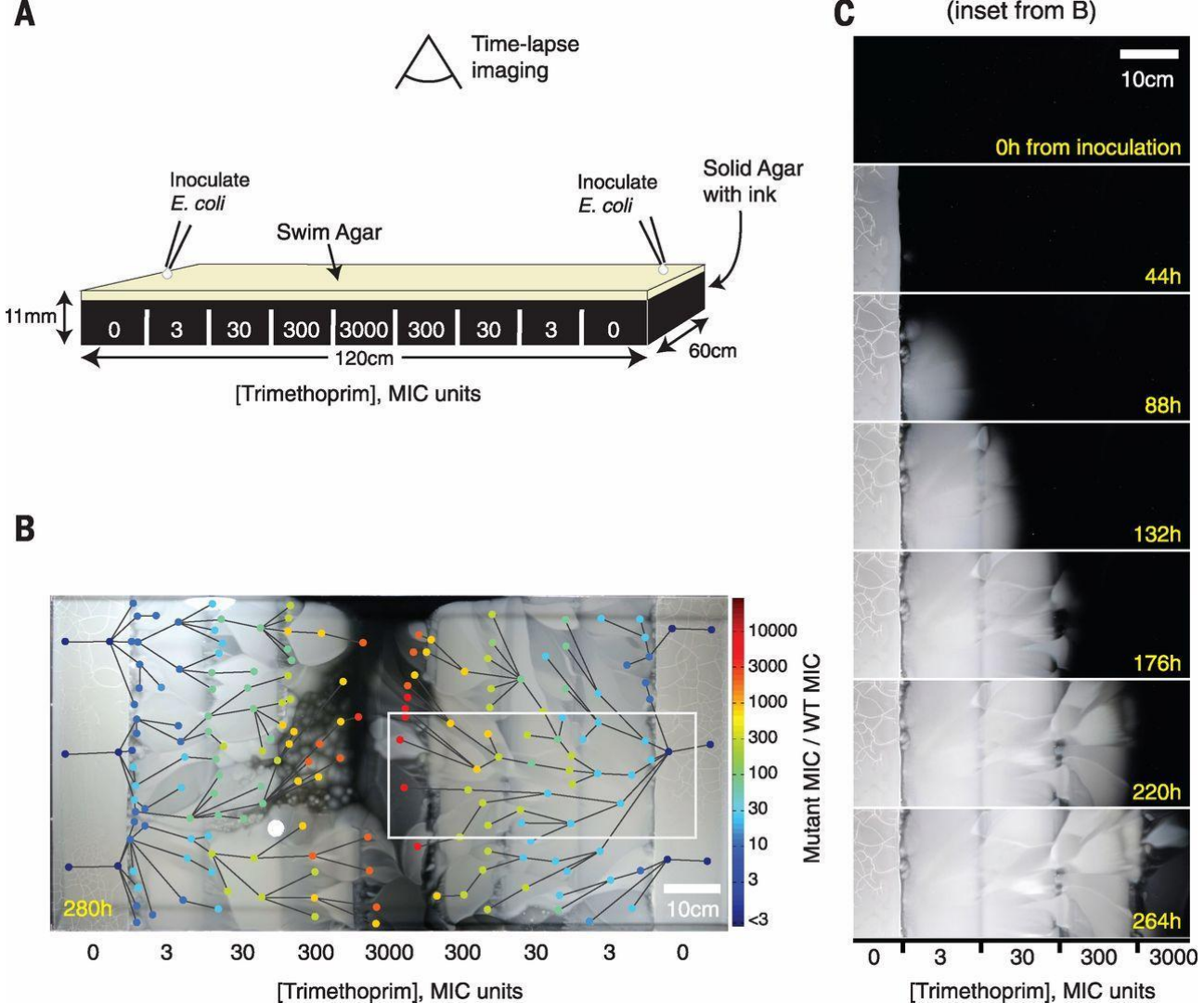

rampart-core
1.3
axis2-kernel
1.3
geronimo-jms_1.1_spec
1.1
commons-logging
1.1
axiom-dom
1.2.5
axiom-impl
1.2.5
XmlSchema
1.3.1
addressing
1.3
avalon-framework
4.1.3
logkit
1.0.1
axiom-api
1.2.5
log4j
1.2.13
httpcore-nio
4.0-alpha5
servlet-api
2.3
commons-httpclient
3.0.1
neethi
2.0.2
rampart-trust
1.3
backport-util-concurrent
2.1
wsdl4j
1.6.1
commons-io
1.2
opensaml
1.1
woden
1.0-incubating-M7b
annogen
0.1.0
stax-api
1.0.1
wss4j
1.5.3
commons-fileupload
1.1.1
axis2-xmlbeans
1.3
xml-apis
1.3.03
xbean
2.1.0
axis2-rmbonpolicy
1.3
bcprov_jdk13
132
commons-codec
1.3
junit
3.8.1
ant
1.7.0
xercesImpl
2.8.1
wsdx-asl
3.2.0
rampart-policy
1.3
xmlsec
1.4.0
commons-discovery
0.2
activation
1.1
xalan
2.7.0
axis2-codegen
1.3
commons-collections
3.1
httpcore
4.0-alpha5
ant-launcher
1.7.0
axis2-adb
1.3
jaxen
1.1-beta-10
axis2-adb-codegen
1.3
mail
1.4
geronimo-activation_1.1_spec
1.0-M1


Deep transitive dependency with high risk vulnerability
Your application
Components you integrated into your application
Hidden dependency licensed under GPLv3


3RD EDITION
SECURITY ENGINEERING
A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS
ROSS ANDERSON
WILEY

```
        hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
    hashOut.length = SSL_SHA1_DIGEST_LEN;
    if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

        err = sslRawVerify(ctx,
                        ctx->peerPubKey,
                        dataToSign,                     /* plaintext */
                        dataToSignLen,                  /* plaintext length */
                        signature,
                        signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                    "returned %d\n", (int)err);
                goto fail;
        }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
```

```
    if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

        err = sslRawVerify(ctx,
                           ctx->peerPubKey,
                           dataToSign,                  /* plaintext */
                           dataToSignLen,               /* plaintext length */
                           signature,
                           signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                    "returned %d\n", (int)err);
                goto fail;
        }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
```


A
Time-lapse imaging
Inoculate E. coli
Swim Agar
Inoculate E. coli
Solid Agar with ink
11mm
0 3 30 300 3000 300 30 3 0
120cm
60cm
[Trimethoprim], MIC units
B
280h
10cm
10000
3000
1000
300
100
30
10
3
<3
Mutant MIC / WT MIC
0 3 30 300 3000 300 30 3 0
[Trimethoprim], MIC units
C
(inset from B)
10cm
0h from inoculation
44h
88h
132h
176h
220h
264h
0 3 30 300 3000
[Trimethoprim], MIC units

Contra qué lucha un ingeniero de Cyberseguridad

BBVA
Creando Oportunidades

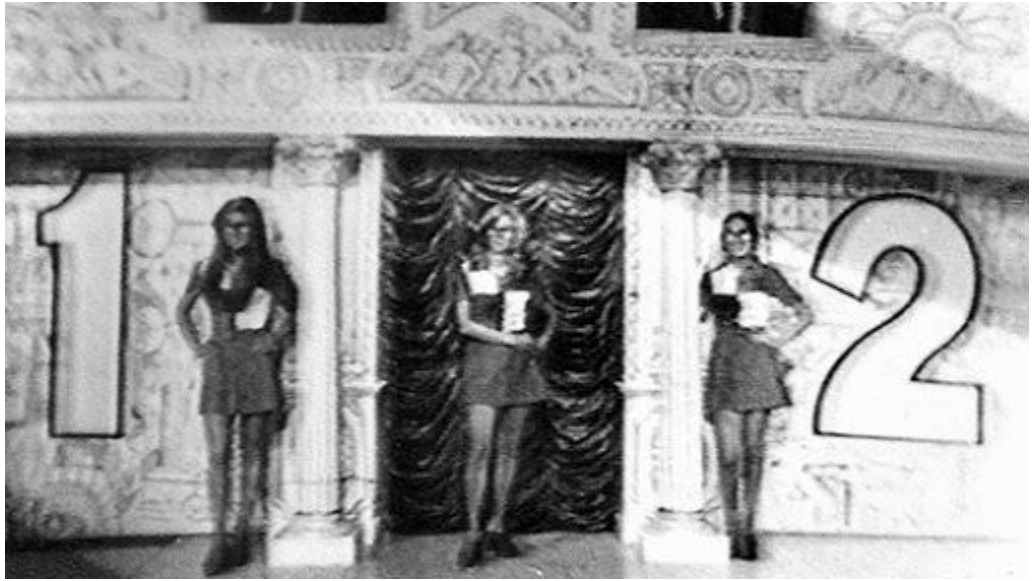
02

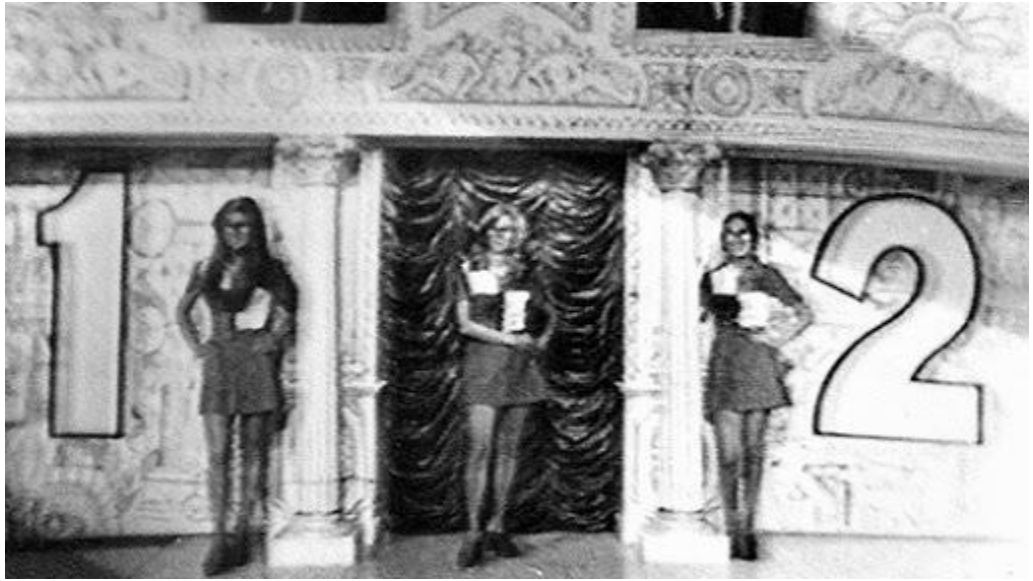
Game theory

Los juegos son algo muy serio

A beautiful mind

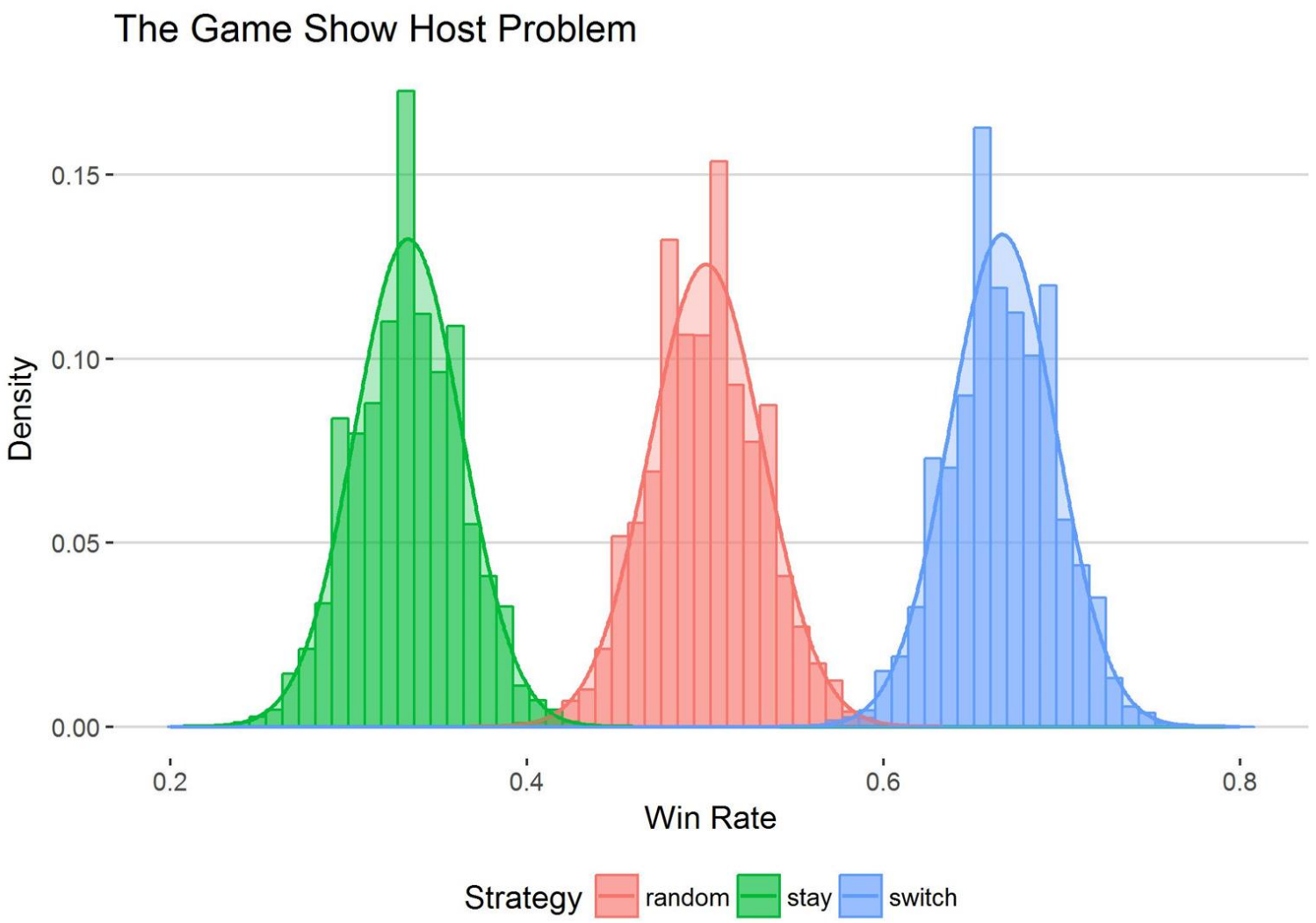

PAREJAS


1
2



#OKBoomer

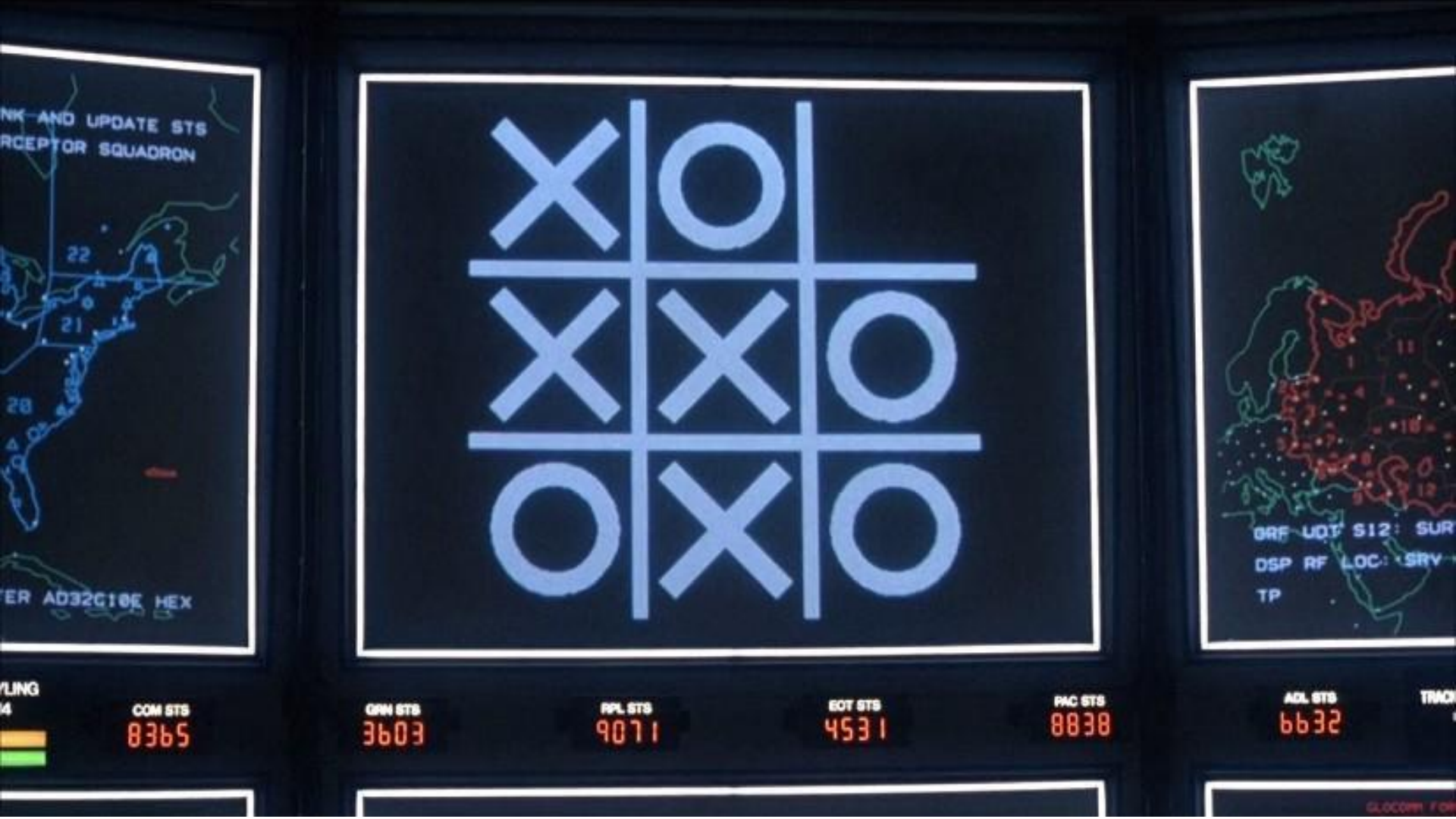
The Monty Hall Problem


The Game Show Host Problem
Density
0.15
0.10
0.05
0.00
0.2
0.4
0.6
0.8
Win Rate
Strategy
random
stay
switch

SHALL WE PLAY A GAME?

SHALL WE PLAY A GAME?

#OKBoomer

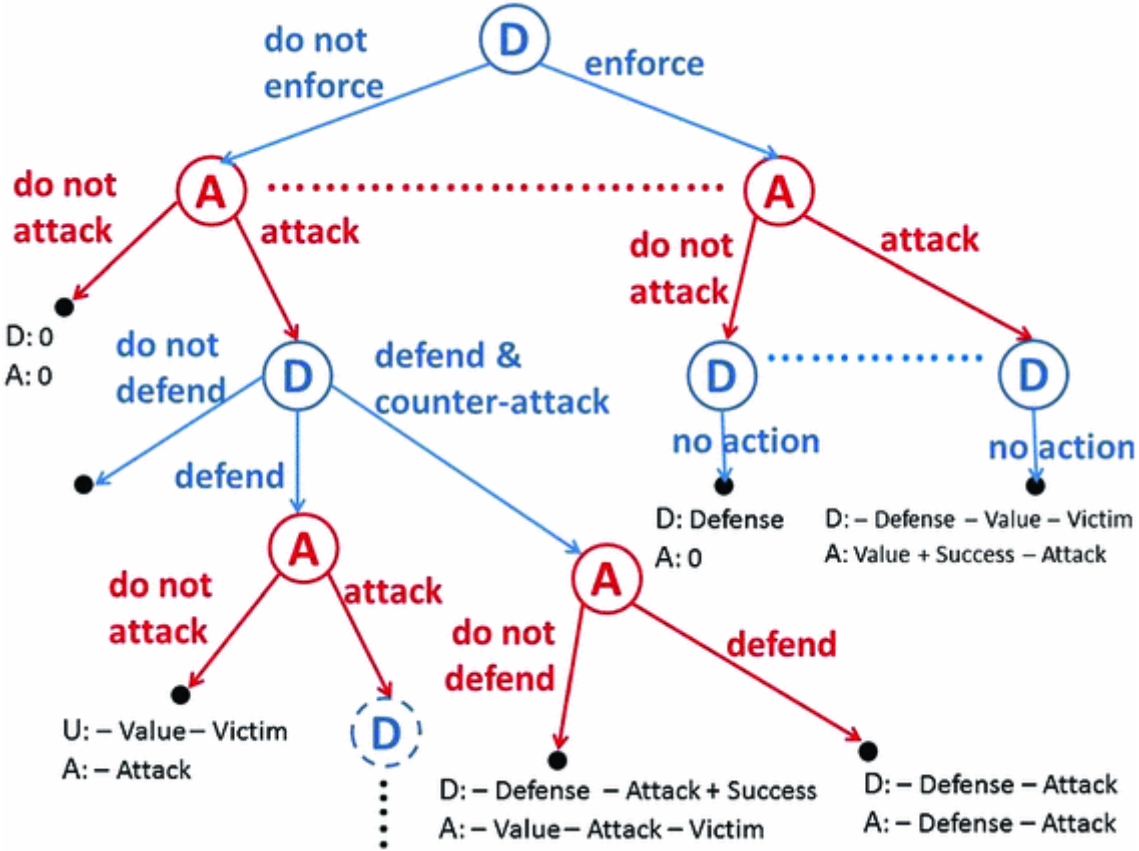

NK AND UPDATE STS
RCEPTOR SQUADRON
22
21
28
ER AD32C18E HEX
COM STS
8365
GRN STS
3603
RPL STS
9071
EOT STS
4531
PAC STS
8838
ADL STS
6632
DSP RF LOC:
TP

GREETINGS PROFESSOR FALKEN

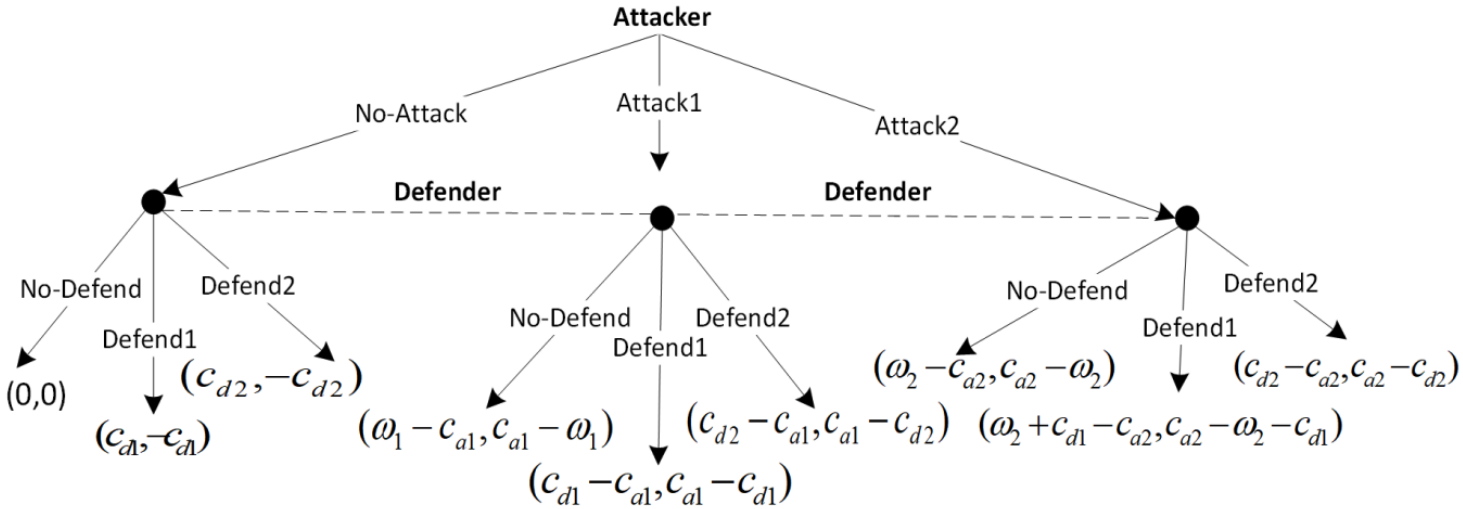
HELLO

A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.

HOW ABOUT A NICE GAME OF CHESS?

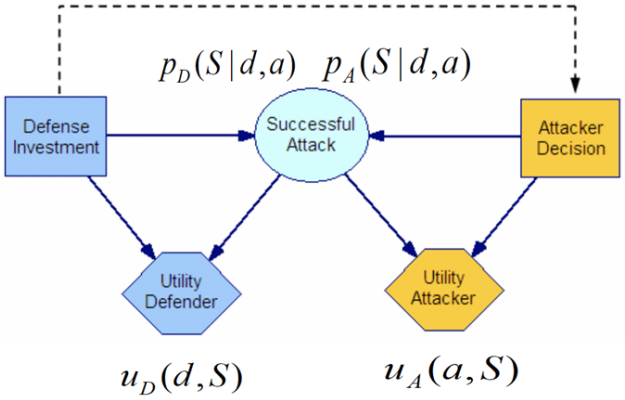

D
do not enforce
enforce
A
do not attack
attack
A
D: 0
A: 0
D
do not defend
defend & counter-attack
defend
A
do not attack
attack
U: – Value – Victim
A: – Attack
D
A
do not defend
defend
D: – Defense – Attack + Success
A: – Value – Attack – Victim
D: – Defense – Attack
A: – Defense – Attack
D
D
do not attack
attack
D
no action
D: Defense
A: 0
D
no action
D: – Defense – Value – Victim
A: Value + Success – Attack

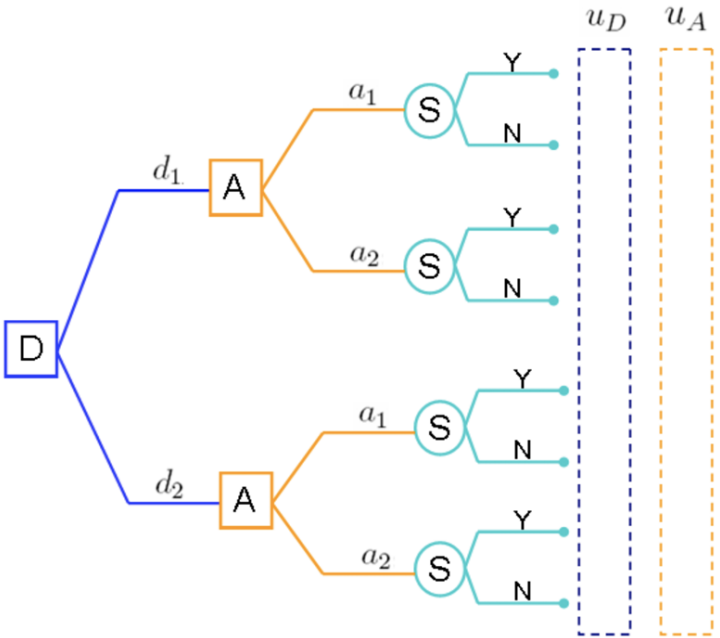
Attacker (A)	Defender (D): d_0	d_1	d_2
a_0	$0\ ,\ 0$	$c_{d1}\ ,\ -c_{d1}$	$c_{d2}\ ,\ -c_{d2}$
a_1	$\omega_1 - c_{a1}\ ,\ c_{a1} - \omega_1$	$c_{d1} - c_{a1}\ ,\ c_{a1} - c_{d1}$	$c_{d2} - c_{a1}\ ,\ c_{a1} - c_{d2}$
a_2	$\omega_2 - c_{a2}\ ,\ c_{a2} - \omega_2$	$\omega_2 + c_{d1} - c_{a2}\ ,\ c_{a2} - c_{d1} - \omega_2$	$c_{d2} - c_{a2}\ ,\ c_{a2} - c_{d2}$



Sequential Defend-Attack model

- Two intelligent decision makers
  - Defender and Attacker
- Sequential moves
  - First Defender, afterwards Attacker knowing Defender's decision





Game Theoretic Analysis

Expected utilities at node S

$$\psi_D(d,a) = p_D(S=0|d,a)\ u_D(d,S=0)\ +\ p_D(S=1|d,a)\ u_D(d,S=1)$$

$$\psi_A(d,a) = p_A(S=0\mid d,a)\ u_A(a,S=0)\ +\ p_A(S=1\mid d,a)\ u_A(a,S=1)$$

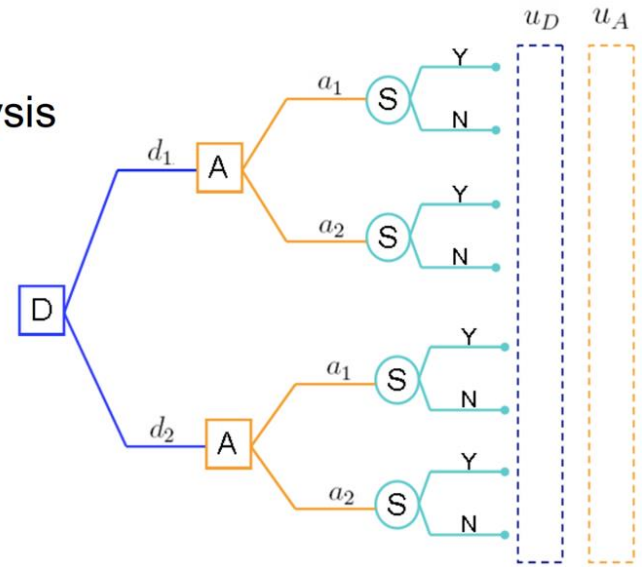
Best Attacker's decision at node A

$$a^*(d) = \text{argmax}_{a\in\mathcal{A}}\psi_A(d,a)$$

Assuming Defender knows Attacker's analysis
Defender's best decision at node D

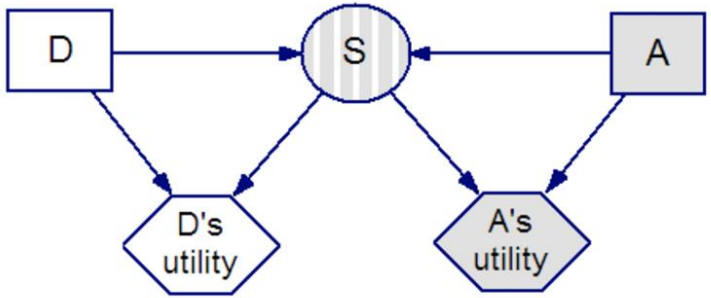
$$d^* = \text{argmax}_{d\in\mathcal{D}}\psi_D(d,a^*(d))$$

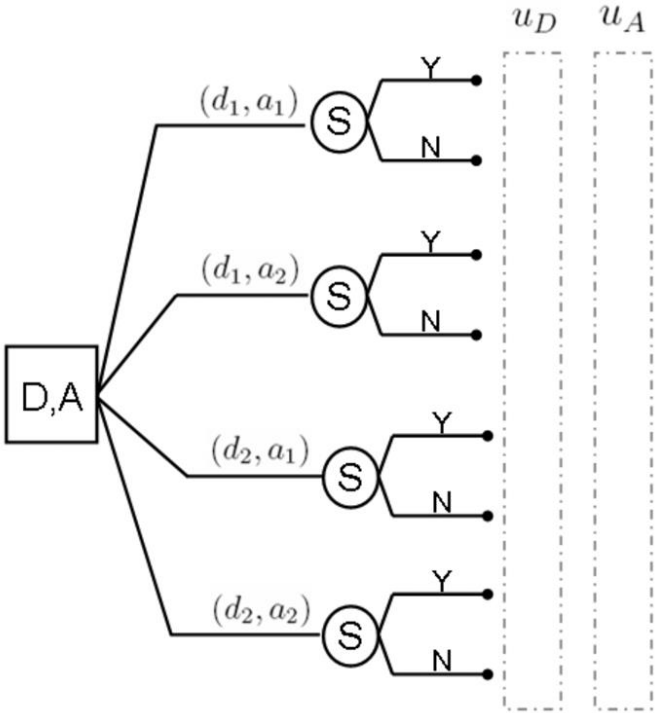
Solution: $(d^*, a^*(d^*))$

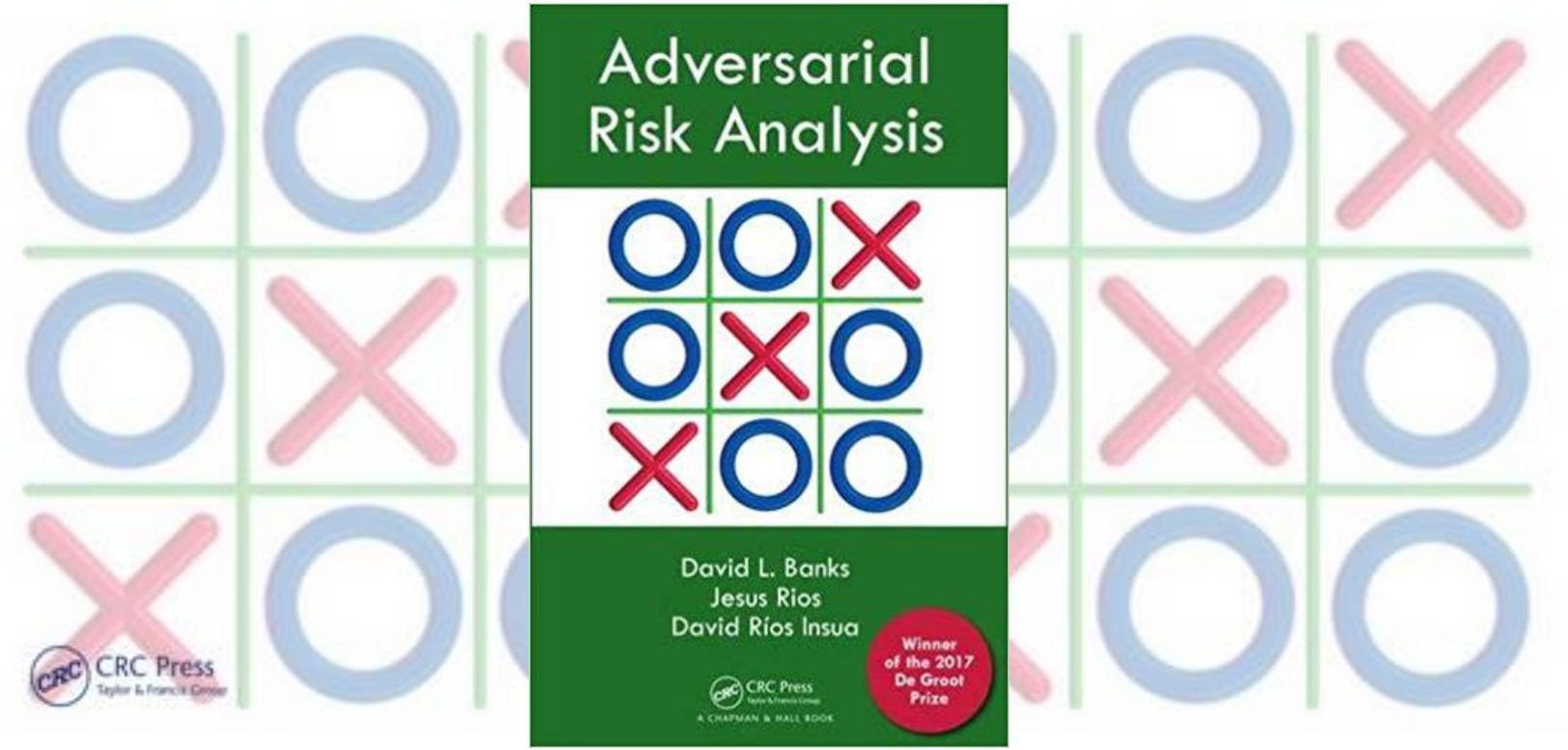


Simultaneous Defend-Attack model

- Decision are taken without knowing each other's decisions






Adversarial
Risk Analysis
David L. Banks
Jesus Rios
David Ríos Insua
Winner of the 2017 De Groot Prize
CRC Press
A CHAPMAN & HALL BOOK
CRC Press

Modeling Opponents in Adversarial Risk Analysis

David Rios Insua,[1] David Banks,[2] and Jesus Rios[3,*]

Adversarial risk analysis has been introduced as a framework to deal with risks derived from intentional actions of adversaries. The analysis supports one of the decisionmakers, who must forecast the actions of the other agents. Typically, this forecast must take account of random consequences resulting from the set of selected actions. The solution requires one to model the behavior of the opponents, which entails strategic thinking. The supported agent may face different kinds of opponents, who may use different rationality paradigms, for example, the opponent may behave randomly, or seek a Nash equilibrium, or perform level-*k* thinking, or use mirroring, or employ prospect theory, among many other possibilities. We describe the appropriate analysis for these situations, and also show how to model the uncertainty about the rationality paradigm used by the opponent through a Bayesian model averaging approach, enabling a fully decision-theoretic solution. We also show how as we observe an opponent's decision behavior, this approach allows learning about the validity of each of the rationality models used to predict his decision by computing the models' (posterior) probabilities, which can be understood as a measure of their validity. We focus on simultaneous decision making by two agents.

KEY WORDS: Adversarial risk analysis; Bayesian model averaging; decision analysis; opponent modeling; simultaneous games

Information Security Economics – and Beyond

Ross Anderson and Tyler Moore

Computer Laboratory, University of Cambridge
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
firstname.lastname@cl.cam.ac.uk

Abstract. The economics of information security has recently become a thriving and fast-moving discipline. As distributed systems are assembled from machines belonging to principals with divergent interests, incentives are becoming as important to dependability as technical design. The new field provides valuable insights not just into 'security' topics such as privacy, bugs, spam, and phishing, but into more general areas such as system dependability (the design of peer-to-peer systems and the optimal balance of effort by programmers and testers), and policy (particularly digital rights management). This research program has been starting to spill over into more general security questions (such as law-enforcement strategy), and into the interface between security and sociology. Most recently it has started to interact with psychology, both through the psychology-and-economics tradition and in response to phishing. The promise of this research program is a novel framework for analyzing information security problems – one that is both principled and effective.

1 Introduction

Over the last few years, people have realised that security failure is caused by bad incentives at least as often as by bad design. Systems are particularly prone to failure when the person guarding them does not suffer the full cost of failure. Game theory and microeconomic theory are becoming important to the security engineer, just as as the mathematics of cryptography did a quarter century ago. The growing use of security mechanisms for purposes such as digital rights management and accessory control – which exert power over system owners rather than protecting them from outside enemies – introduces many strategic issues. Where the system owner's interests conflict with those of her machine's designer, economic analysis can shine light on policy options.

Risk Assessments: Incentivos

ROI

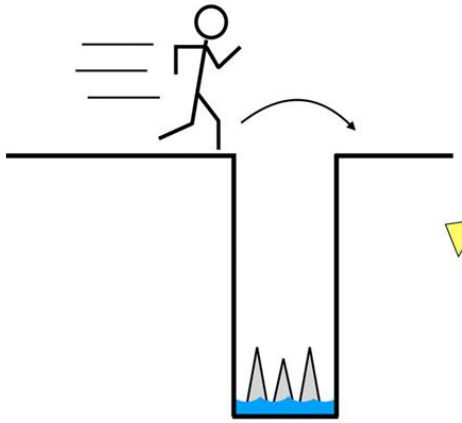
Propensión a la liquidez O.K. he's a billionaire, but how much of it is in cash?

Risks

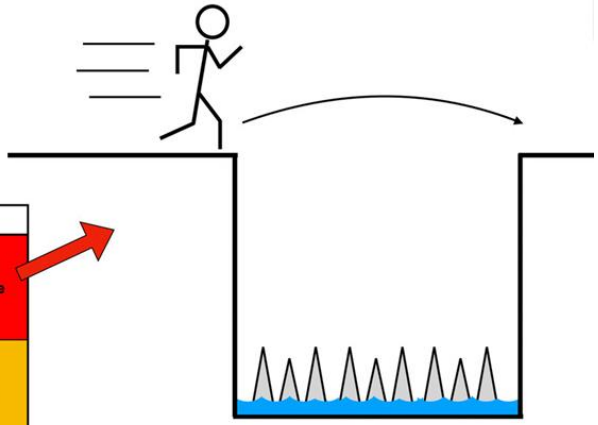
Recurrencia

Assessment of Risk Exposure = Risk Probability x Impact

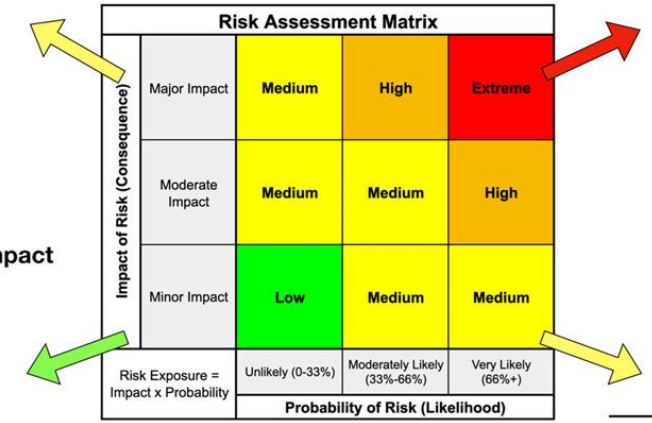
(Severity = Likelihood x Consequence)

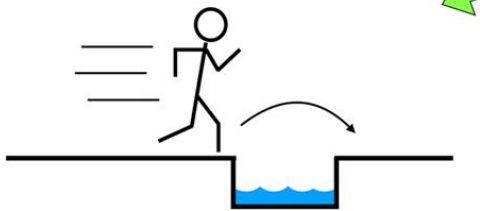


Low Probability & High Impact

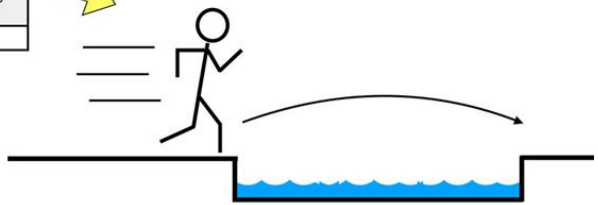


High Probability & High Impact





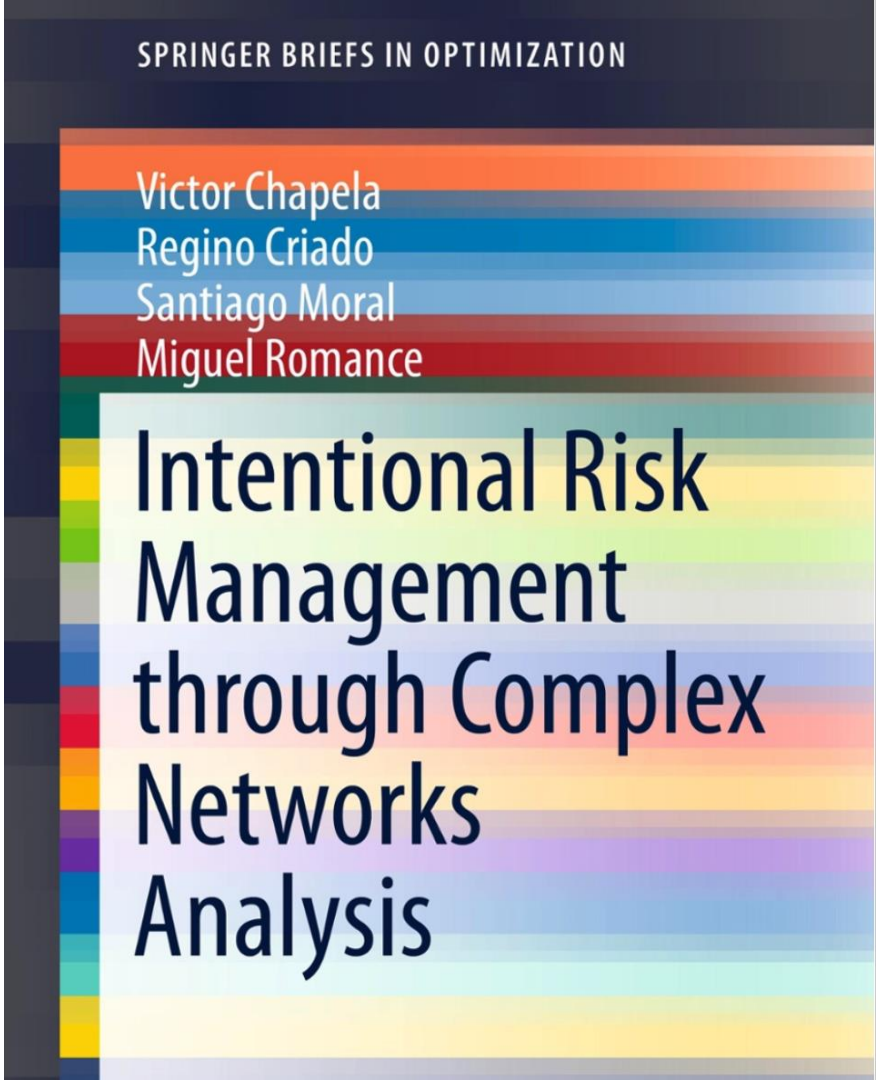
Low Probability & Low Impact



High Probability & Low Impact


Risk
No
Yes
Reward


O.K. he's a billionaire, but how much of it is in cash?

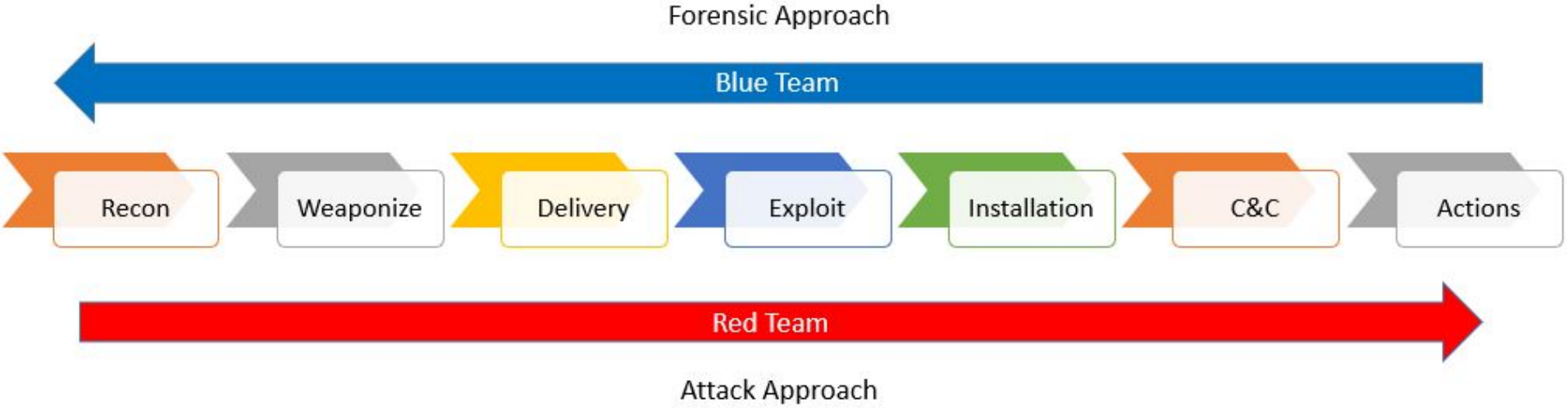

SPRINGER BRIEFS IN OPTIMIZATION
Victor Chapela
Regino Criado
Santiago Moral
Miguel Romance
Intentional Risk Management through Complex Networks Analysis

BBVA

Creando Oportunidades

Dinámica de juegos

Pasando de pantallas


Forensic Approach
Blue Team
Recon
Weaponize
Delivery
Exploit
Installation
C&C
Actions
Red Team
Attack Approach

PRE-ATT&CK

Priority Definition
- Planning, Direction

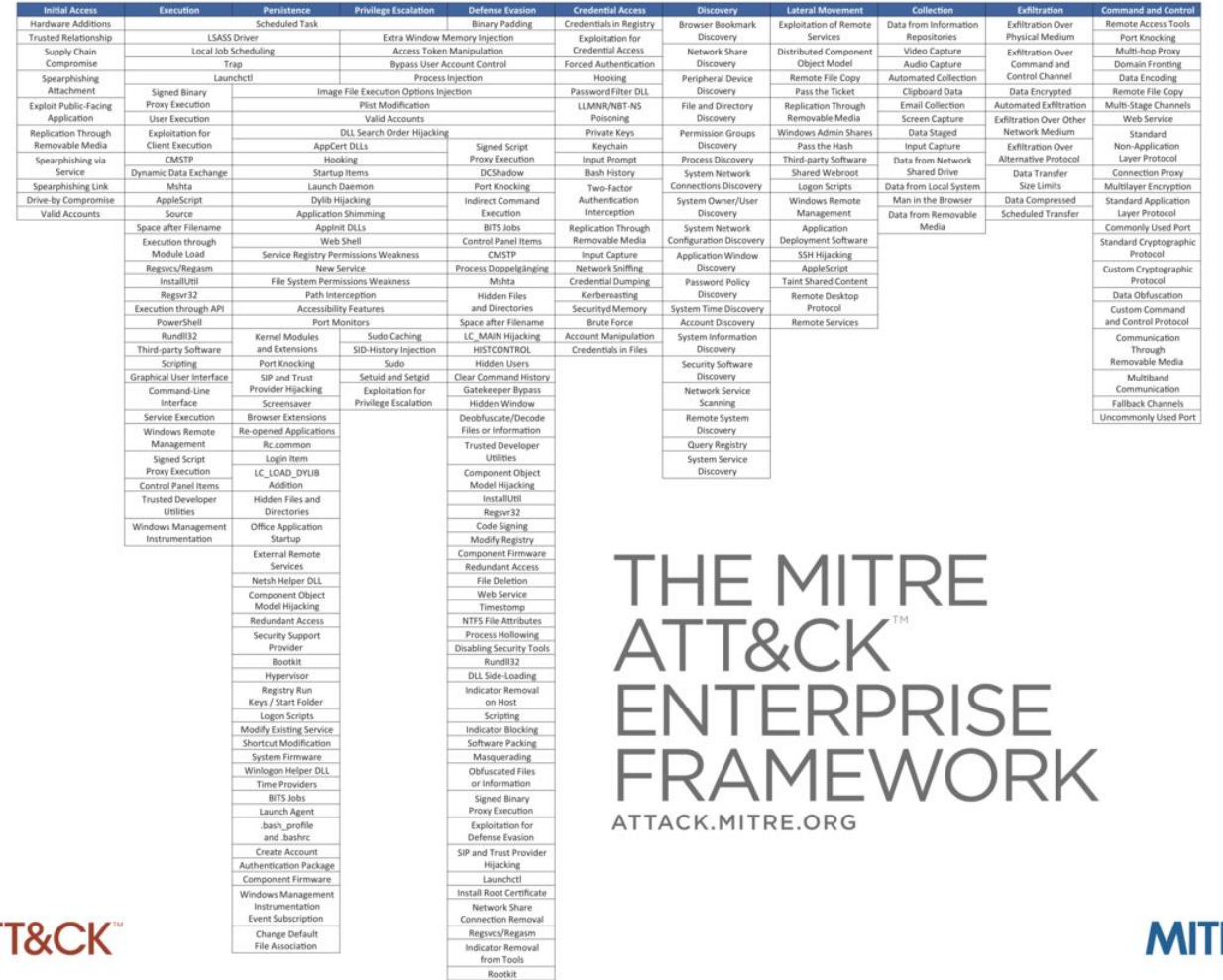
Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control



THE MITRE ATT&CK™ ENTERPRISE FRAMEWORK

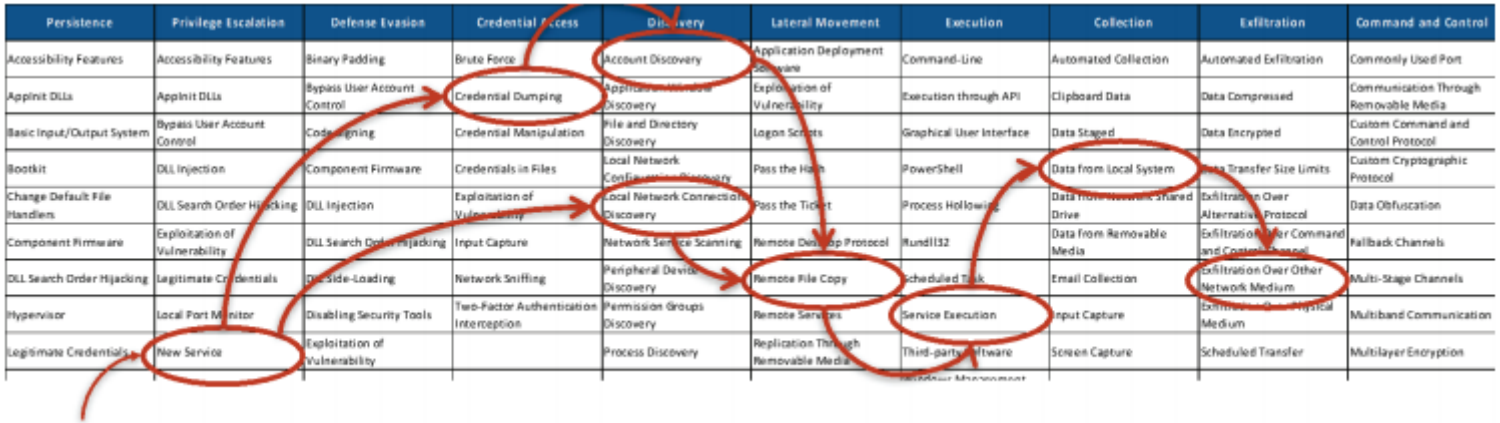
ATTACK.MITRE.ORG

ATT&CK™

MITRE

Use ATT&CK for Adversary Emulation and Red Teaming

The best defense is a well-tested defense. ATT&CK provides a common adversary behavior framework based on threat intelligence that red teams can use to emulate specific threats. This helps cyber defenders find gaps in visibility, defensive tools and processes—and then fix them.



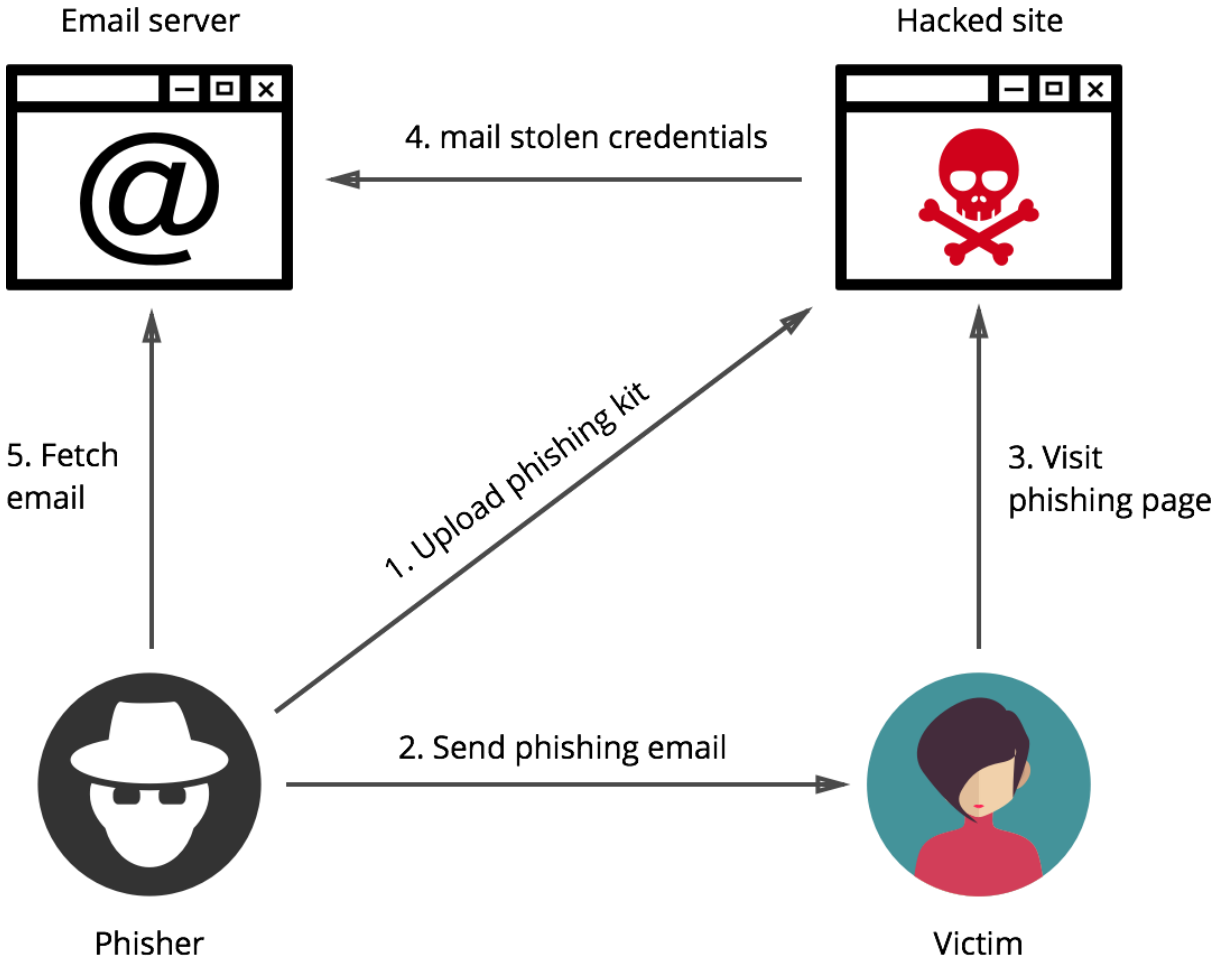
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connection Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption

BBVA
Creando Oportunidades

03

¡A jugar!

Simulación de casos reales

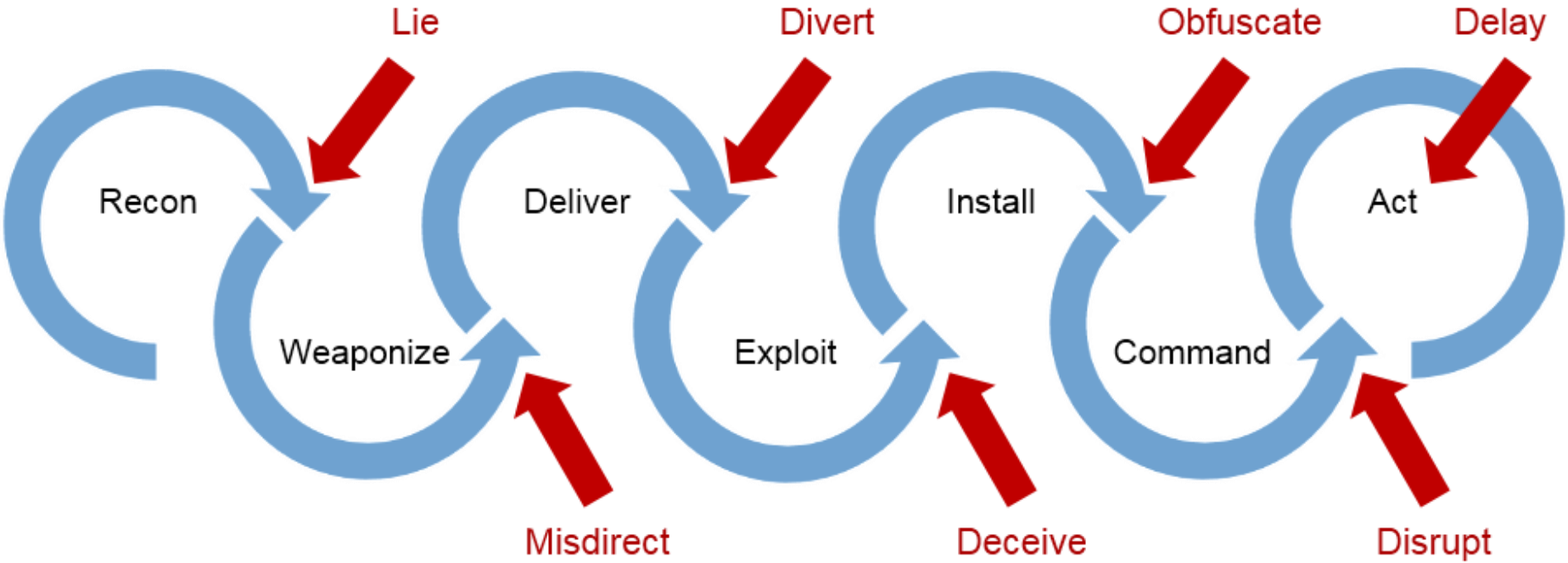

Email server
Hacked site
4. mail stolen credentials
5. Fetch email
1. Upload phishing kit
3. Visit phishing page
2. Send phishing email
Phisher
Victim

PHISHING

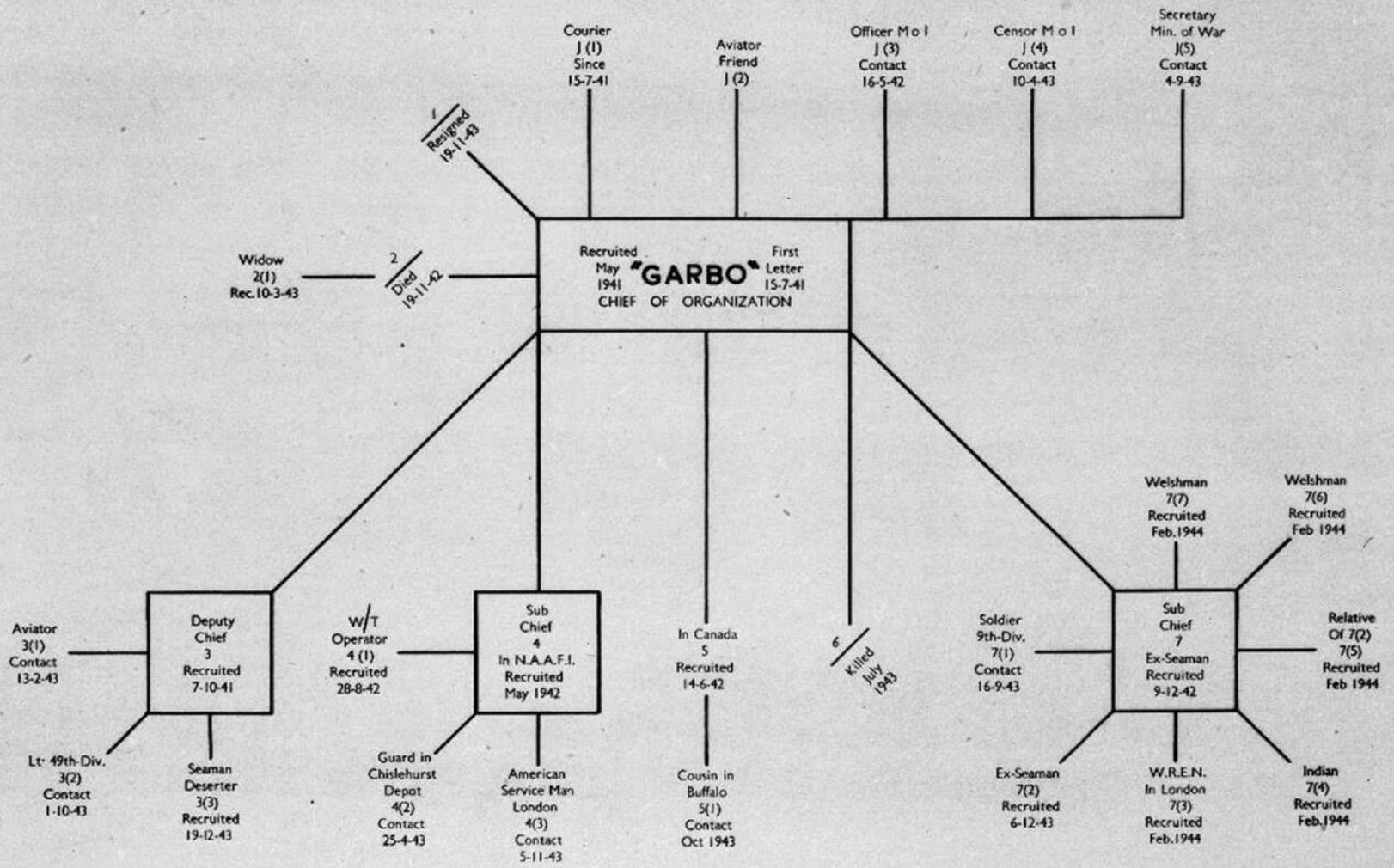
VS

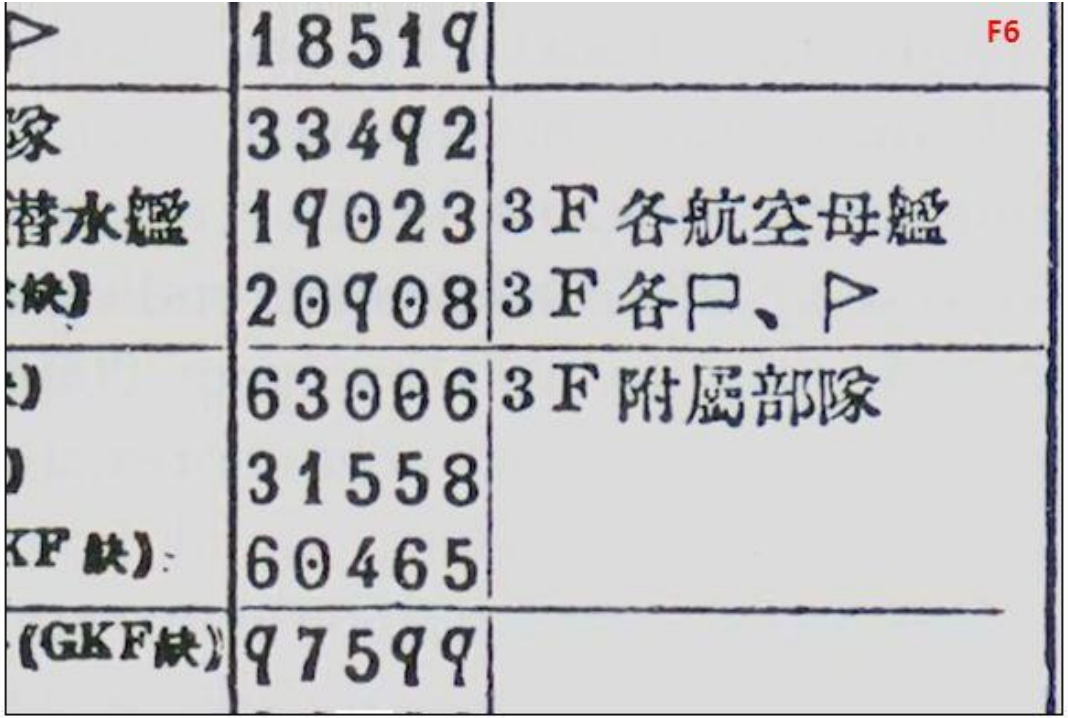
SMISHING


3
Luego de abierto el link, se instala un virus en el teléfono, replica toda la información almacenada y nueva al servidor del atacante
1
El atacante envía un SMS falso con un Link de una URL maliciosa
SMS
Internet
Usuario
El usuario abre el link contenido en el SMS
2
Teléfono inteligente
Atacante
Enlace celular
Servidor falso


Lie
Divert
Obfuscate
Delay
Recon
Deliver
Install
Act
Weaponize
Exploit
Command
Misdirect
Deceive
Disrupt


760


Courier
J (1)
Since
15-7-41
Aviator
Friend
J (2)
Officer M o I
J (3)
Contact
16-5-42
Censor M o I
J (4)
Contact
10-4-43
Secretary
Min. of War
J(5)
Contact
4-9-43
1
Resigned
19-11-43
Widow
2(1)
Rec. 10-3-43
2
Died
19-11-42
Recruited
May
1941
"GARBO"
First
Letter
15-7-41
CHIEF OF ORGANIZATION
Aviator
3(1)
Contact
13-2-43
Deputy
Chief
3
Recruited
7-10-41
Lt. 49th Div.
3(2)
Contact
1-10-43
Seaman
Deserter
3(3)
Recruited
19-12-43
W/T
Operator
4 (1)
Recruited
28-8-42
Sub
Chief
4
In N.A.A.F.I.
Recruited
May 1942
Guard in
Chislehurst
Depot
4(2)
Contact
25-4-43
American
Service Man
London
4(3)
Contact
5-11-43
In Canada
5
Recruited
14-6-42
Cousin in
Buffalo
5(1)
Contact
Oct 1943
6
Killed
July
1943
Welshman
7(7)
Recruited
Feb. 1944
Welshman
7(6)
Recruited
Feb 1944
Soldier
9th-Div.
7(1)
Contact
16-9-43
Sub
Chief
7
Ex-Seaman
Recruited
9-12-42
Relative
Of 7(2)
7(5)
Recruited
Feb 1944
Ex-Seaman
7(2)
Recruited
6-12-43
W.R.E.N.
In London
7(3)
Recruited
Feb. 1944
Indian
7(4)
Recruited
Feb. 1944



▷	18519	F6
隊	33492	
潜水艦	19023	3F 各航空母艦
缺)	20908	3F 各巳、▷
缺)	63006	3F 附屬部隊
)	31558	
KF 缺):	60465	
(GKF缺)	97599	

Vimeo: *Codebreaking Victory: The Midway Battle*
(9:50) – Jap code with Jap characters – F6

That vital information was hidden in coded Japanese Naval message traffic. The code was made up of 33,000 words, phrases and letters expressed in strings of numbers.

2a

F17

"WATER SUPPLIES ARE RUNNING LOW ON MIDWAY ISLAND."

"WATER SUPPLIES ARE RUNNING LOW ON AF."

Vimeo: Codebreaking Victory: The Midway Battle
(13:45) – telegraph of low water supply/CU of message – F15

The message that *"water supplies were running low on Midway Island,"* was intercepted by the Japanese. They advised their commanders, *"water supplies are low on 'AF'."*

8c

Vimeo: Codebreaking Victory: The Midway Battle
(13:45) – telegraph of low water supply/CU of message – F15

The message that *"water supplies were running low on Midway Island,"* was intercepted by the Japanese. They advised their commanders, *"water supplies are low on 'AF'."*


POLICIA NACIONAL
Mº INTERIOR

Contents lists available at ScienceDirect

Journal of Computational Design and Engineering

journal homepage: www.elsevier.com/locate/jcde

Donkey and smuggler optimization algorithm: A collaborative working approach to path finding

Ahmed S. Shamsaldin [a], Tarik A. Rashid [a,*], Rawan A. Al-Rashid Agha [a], Nawzad K. Al-Salihi [a], Mokhtar Mohammadi [b]

[a] Computer Science and Engineering Department, University of Kurdistan-Hewler, Erbil, Kurdistan, Iraq
[b] Department of Information Technology, University of Human Development, Sulaymaniyah, Kurdistan, Iraq

ARTICLE INFO

Article history:
Received 19 November 2018
Received in revised form 9 April 2019
Accepted 15 April 2019
Available online 19 April 2019

ABSTRACT

Swarm Intelligence is a metaheuristic optimization approach that has become very predominant over the last few decades. These algorithms are inspired by animals' physical behaviors and their evolutionary perceptions. The simplicity of these algorithms allows researchers to simulate different natural phenomena to solve various real-world problems. This paper suggests a novel algorithm called Donkey and Smuggler Optimization Algorithm (DSO). The DSO is inspired by the searching behavior of donkeys.

La Voz de Galicia

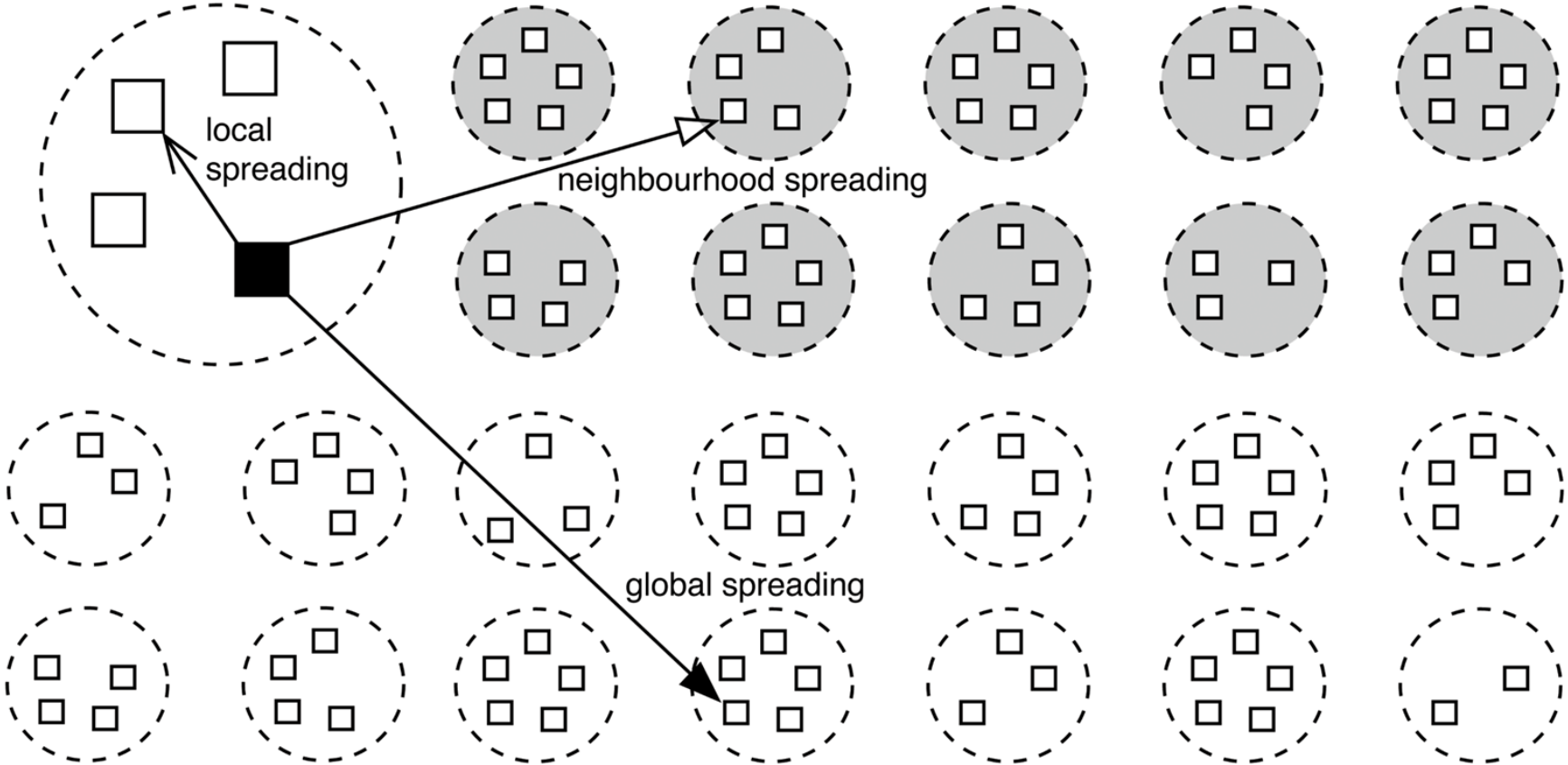
INTERNACIONAL

Argentina, en guerra contra el robo masivo de cables de cobre

En dos años desaparecieron 320.000 kilómetros de líneas teléfonicas. El Gobierno suspende las exportaciones de ese metal para intentar detener el expolio

Conficker's three probing strategies.

(1) global spreading, where it probes any computer on the Internet at random; (2) local spreading, where it probes computers in the same local network; (3) neighbourhood spreading, where it probes computers in ten neighbouring local networks.



doi: https://doi.org/10.1371/journal.pone.0127478.g002

English

Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:59:49

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:59:49

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

[redacted] Copy

About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

BBVA
Creando Oportunidades

04

Juegos de cartas

Crowd-threatmodeling


2
Spoofing
An attacker could squat on the random port or socket that the server normally uses.
2
J
Spoofing
An attacker could steal credentials stored on the client and reuse them.
3
Tampering
An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto.
3
K
Tampering
An attacker can load code inside your process via an extension point.
K
7
Information Disclosure
An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection.
7
6
Denial of Service
An attacker can make a server unavailable or unusable without ever authenticating, but the problem goes away when the attacker stops (server, anonymous, temporary).
6
Q
Repudiation
An attacker can say "I didn't do that," and you would have no way to prove them wrong.
I didn't do that.
R
K
Elevation of Privilege
An attacker can inject a command that the system will run at a higher privilege level.
K

Instructions 1

Elevation of Privilege Instructions

Draw a diagram of the system you want to threat model before you deal the cards.

Deal the deck to 3-6 players. Play starts with the 3 of Tampering. Play clockwise, and each player in turn follows in the suit if they have a card in the suit. If they don't have that suit, they can play another suit. The high card played takes the trick, with Elevation of Privilege taking precedence over the suit lead. Only Elevation of Privilege (EoP) or the lead suit can take a trick.

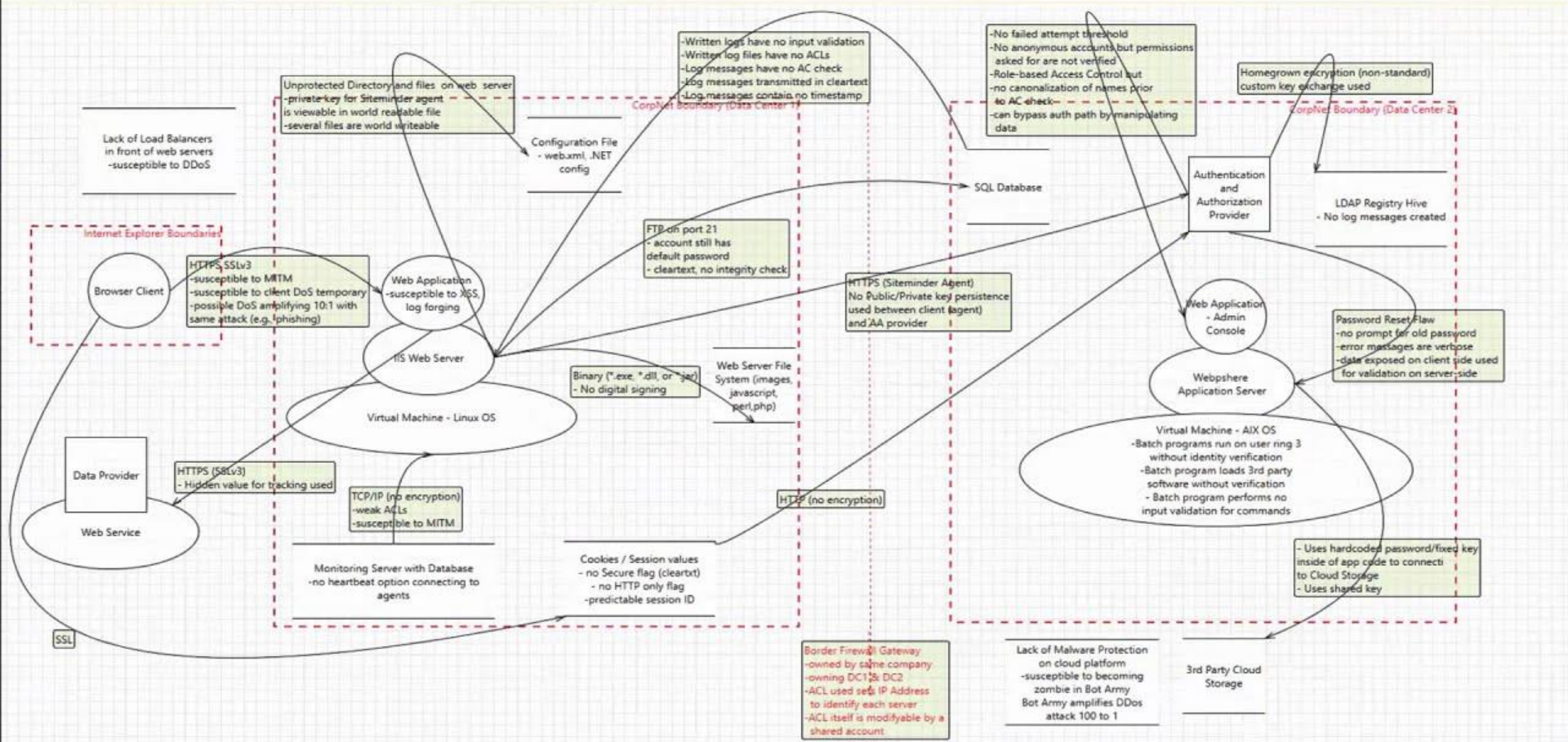
To play a card, read the card, announce your threat and record it. If the player can't link the threat to the system, play proceeds.

Take few minutes between hands to think about threats.

Points:
1 for a threat on your card, +1 for taking the trick

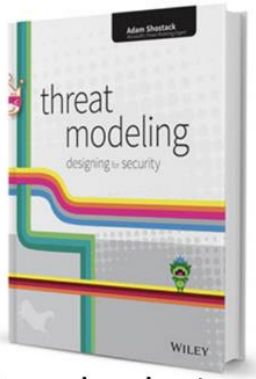
Instructions

ACME-Application



Resources

Threat Modeling: Designing For Security



Part I: Getting Started

1. Dive in and threat model
2. Strategies for threat modeling

Part II: Finding Threats

3. STRIDE
4. Attack Trees
5. Attack Libraries
6. Privacy Tools

Part III: Managing and Addressing Threats

7: Processing and managing threats
8. Defensive Building Blocks
9. Tradeoffs when addressing threats
10. Validating threats are addressed
11. Threat modeling tools

Part IV: Threat modeling in technologies and tricky areas

12. Requirements cookbook
13. Web and cloud threats
14. Accounts and Identity
15. Human Factors and Usability
16. Threats to cryptosystems

Part IV: Taking it to the next level

17. Bringing threat modeling to your organization
18. experimental approaches
19 Architecting for success

Appendices

- Helpful tools, Threat trees, Attacker Lists, Elevation of Privilege (the cards), Case studies

OWASP Cornucopia

CORNUCOPIA

K

Gareth can utilize the application to deny service to some or all of its users

OWASP SCP 41, 55
OWASP ASVS 2.9
OWASP AppSensor UT1-4, STE3
CAPEC 2, 25, 119
SAFECODE 1

OWASP Cornucopia Ecommerce Website Edition v1.04

CRYPTOGRAPHY

J

Justin can read credentials for accessing internal or external resources, services and others systems because they are stored in an unencrypted format, or saved in the source code

OWASP SCP 35, 90, 171, 172
OWASP ASVS 2.14, 12.1
OWASP AppSensor -
CAPEC 116
SAFECODE 21, 29

OWASP Cornucopia Ecommerce Website Edition v1.04

AUTHENTICATION

7

Cecilia can use brute force and dictionary attacks against one or many accounts without limit, or these attacks are simplified due to insufficient complexity, length, expiration and re-use requirements for passwords

OWASP SCP 33, 38, 39, 41, 50, 53
OWASP ASVS 2.3
OWASP AppSensor AE2, AE3
CAPEC 2, 16
SAFECODE 27

OWASP Cornucopia Ecommerce Website Edition v1.04

AUTHORIZATION

8

Tom can bypass business rules by altering the usual process sequence or flow, or by undertaking the process in the incorrect order, or by manipulating date and time values used by the application, or by using valid features for unintended purposes, or by otherwise manipulating control data

OWASP SCP 10, 32, 93, 94, 189
OWASP ASVS 4.1, 4.2, 4.3, 4.4, 4.6, 4.12
OWASP AppSensor ACE3
CAPEC 25, 39, 74, 162, 166, 207
SAFECODE 8, 10, 11, 12

OWASP Cornucopia Ecommerce Website Edition v1.04


CONTROL-ALT HACK
WHITE HAT HACKING
FOR FUN AND PROFIT
FRANZI
KARL
ATTENDANCE
ENTROPY
MISSION
$2K


ENTER THE
SPUDNET
A board game of potatoes, networking and cyber piracy

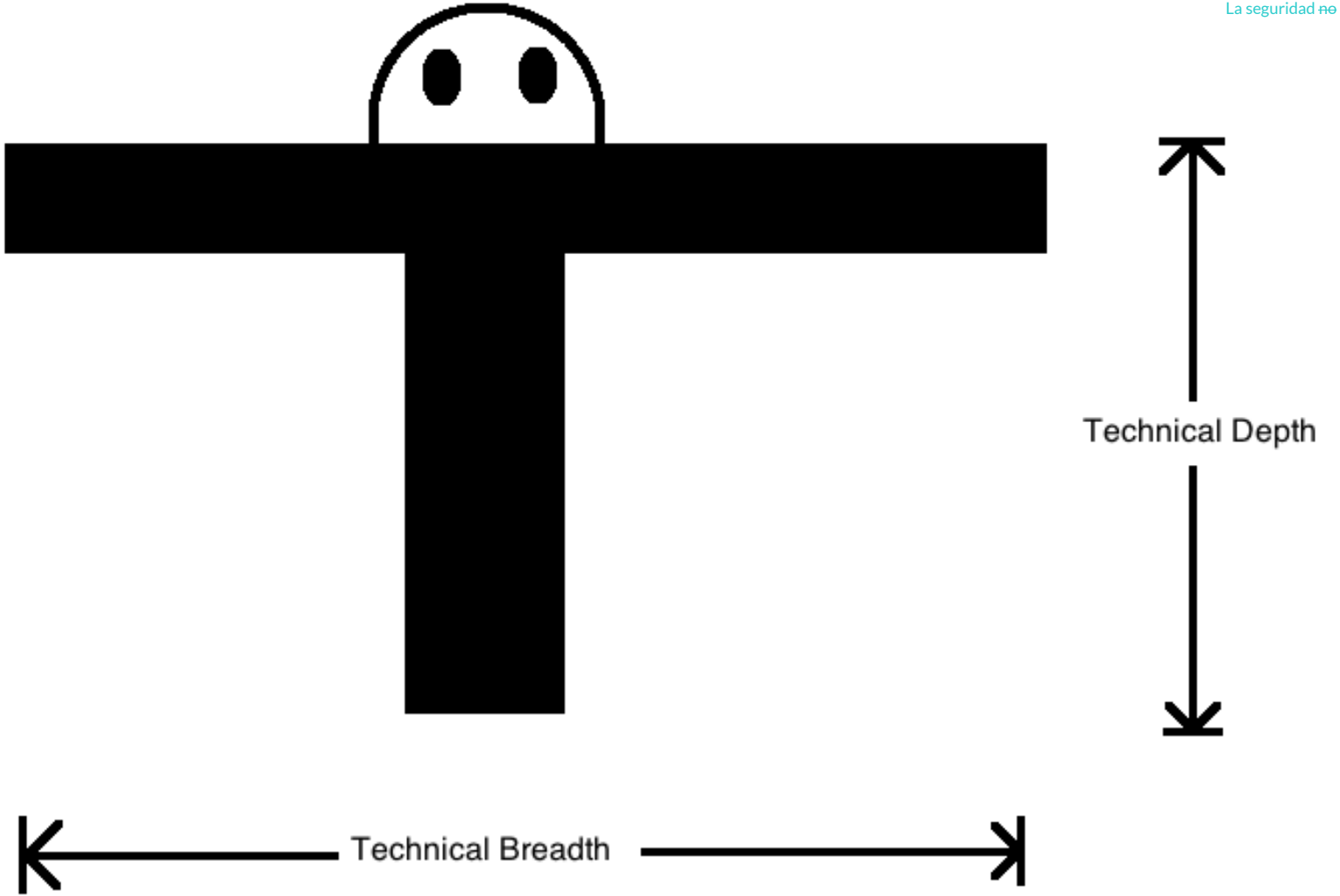

Crypto Go
Grow with t3chfest
HMAC
SALSA
20/20
AEFEX
SHA-3
2-8
14+
@cryptogogame

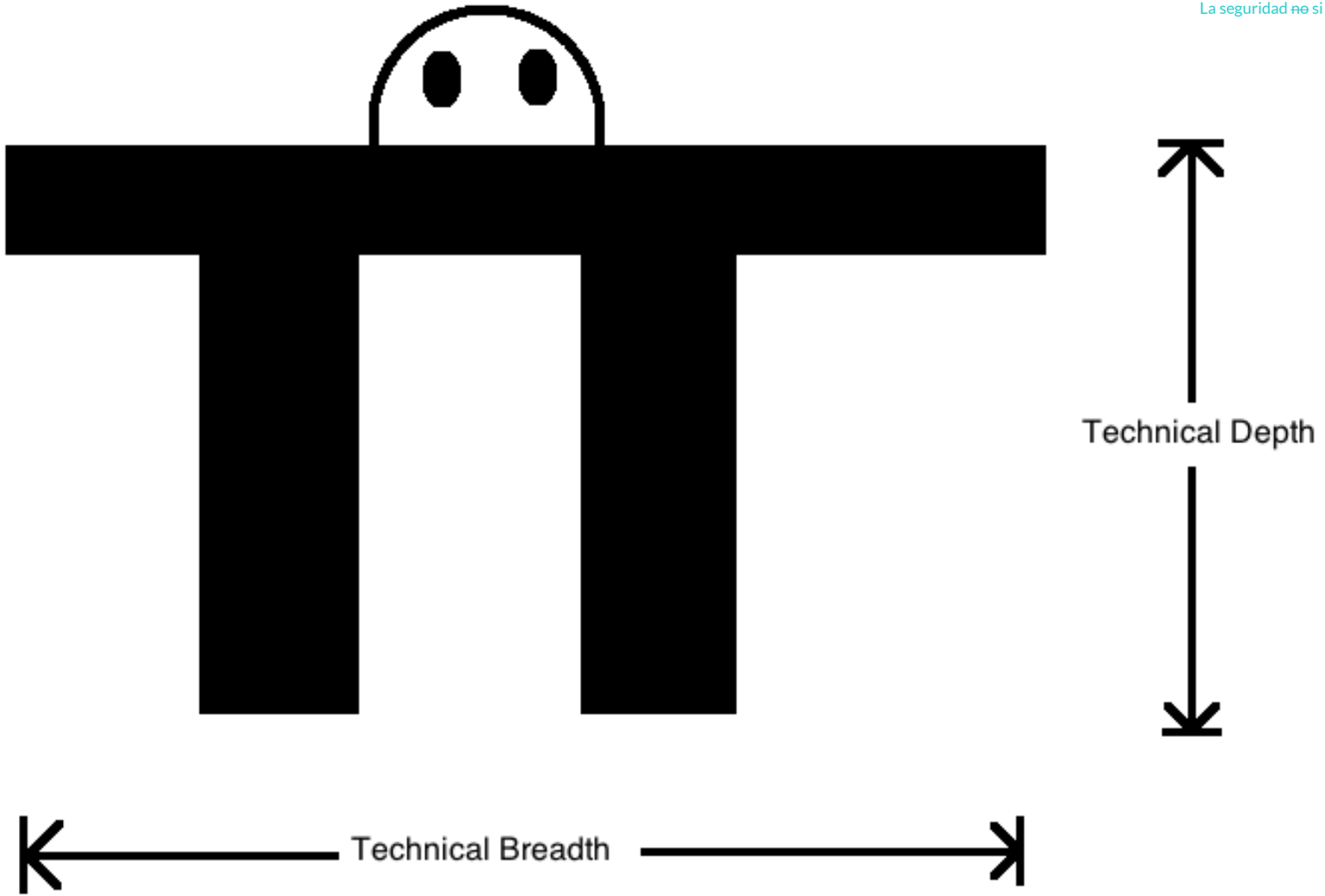
BBVA
Creando Oportunidades

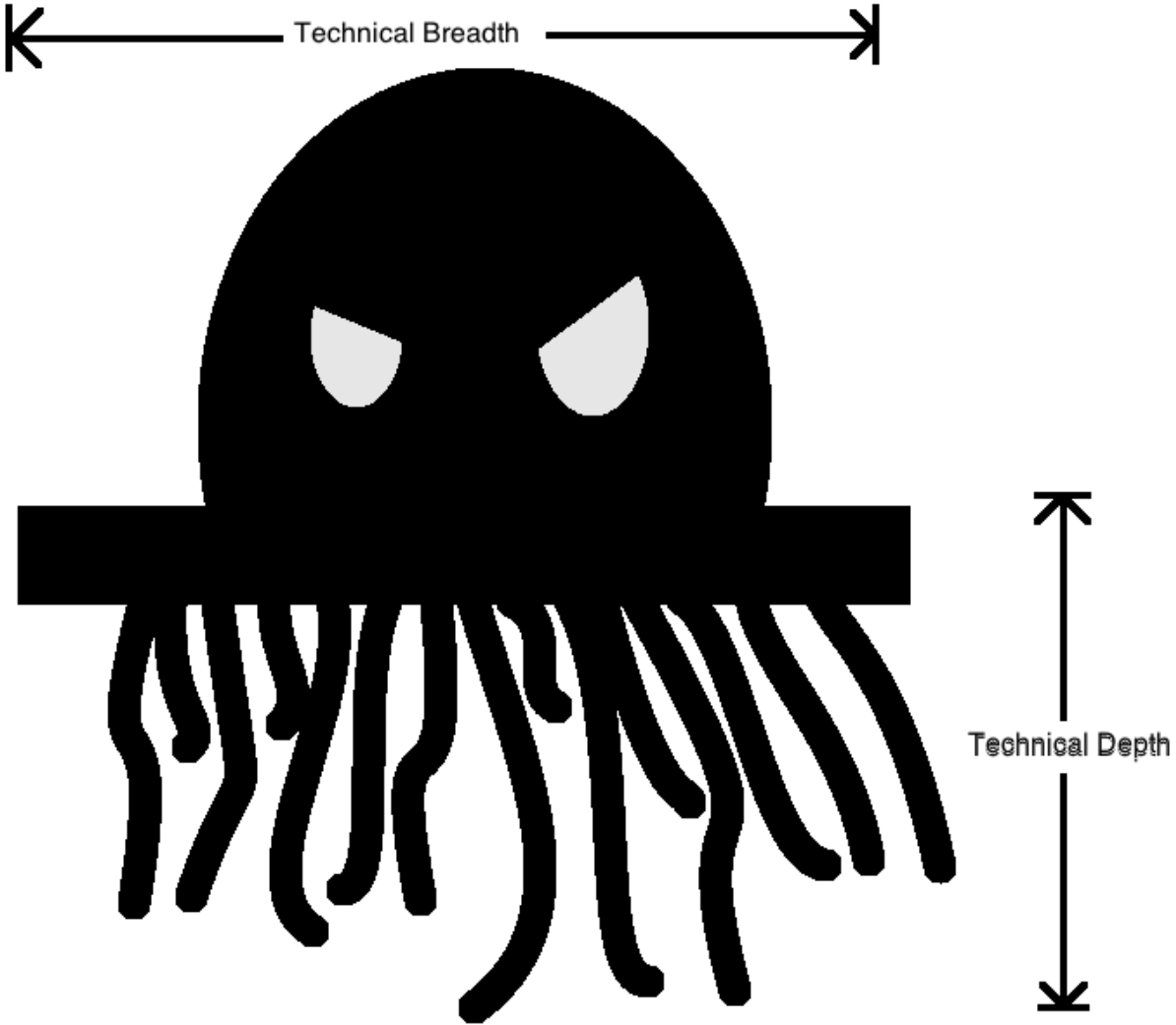
05

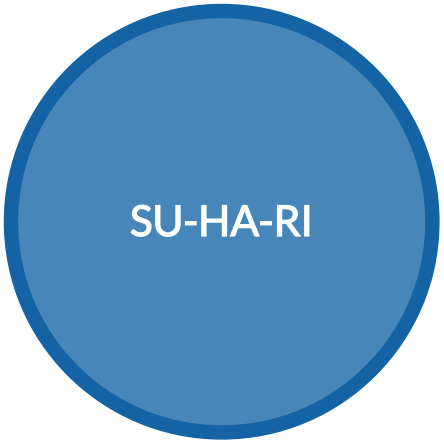
Conclusiones

Y consejos


Technical Depth
Technical Breadth


Technical Depth
Technical Breadth


Technical Breadth
Technical Depth


SU-HA-RI


CRITERIO


EXPERIENCIA

BBVA
Creando Oportunidades

GRACIAS

@lsaiz

URJC
Febrero 2020

HackOn