"On the all UR base are to be considered harmful for fun and profit is the new cool trick, hackers hate it. Redux."

Ekoparty 2023
November 1st, 2023

Iván Arce - Chief Research Officer at Quarkslab

What is this about ?

It’s a keynote

“I can talk about anything with total impunity!”

…

“ ok, but what do I talk about ?”

…

“nothing! I got nothing..”

What was I thinking ?!

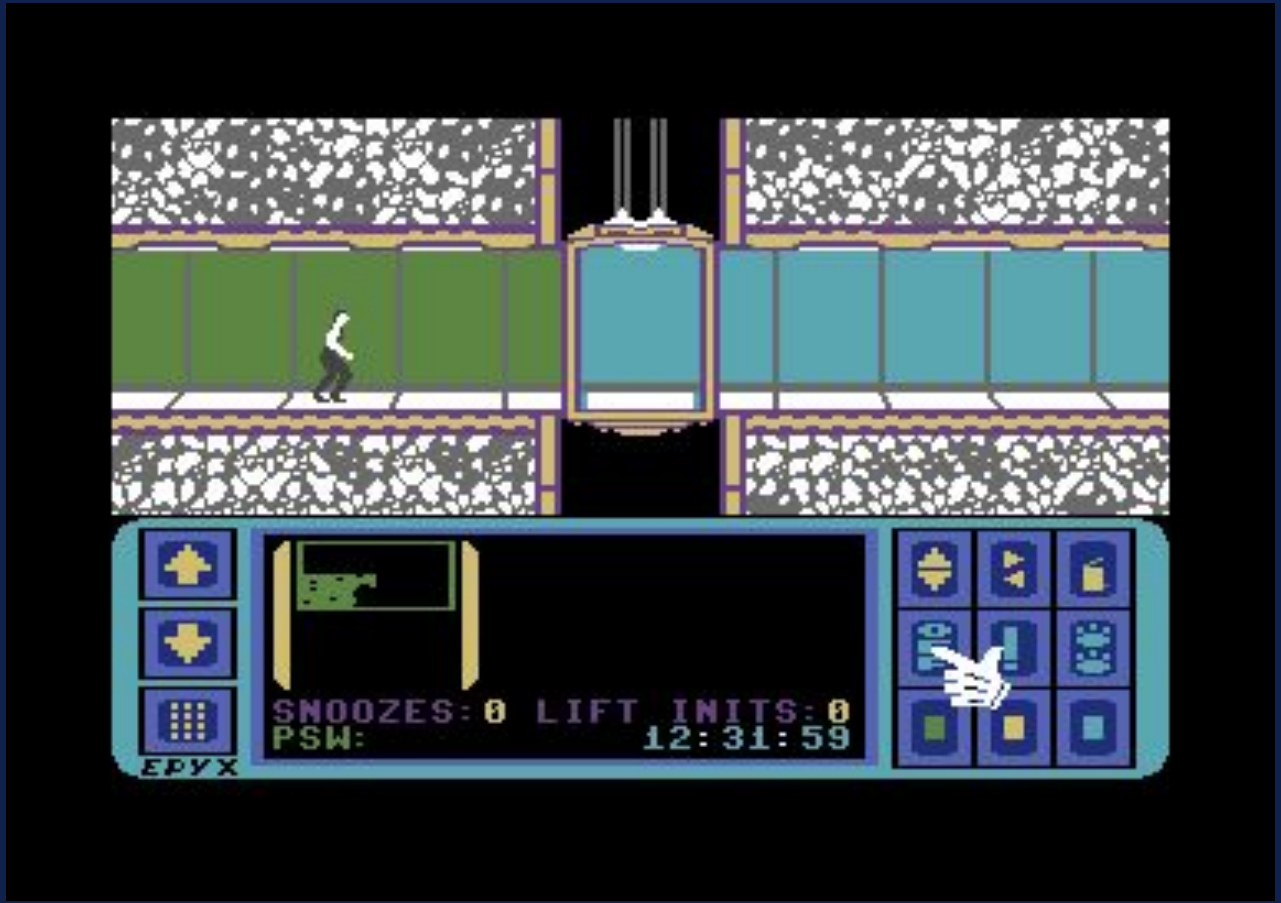
Talk about the only thing I know a lot about

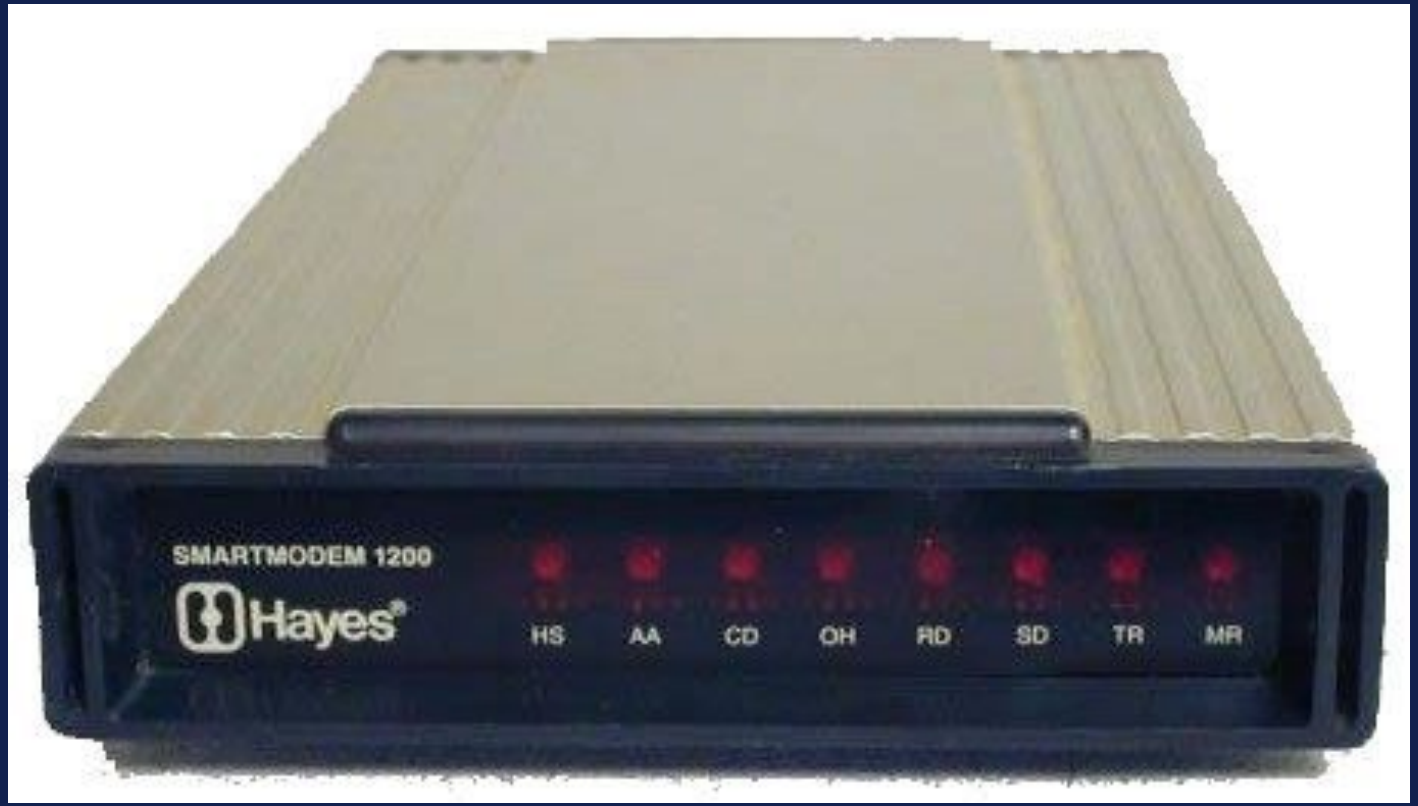
1982/3


**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM 38911 BASIC BYTES FREE
READY.

1982/3

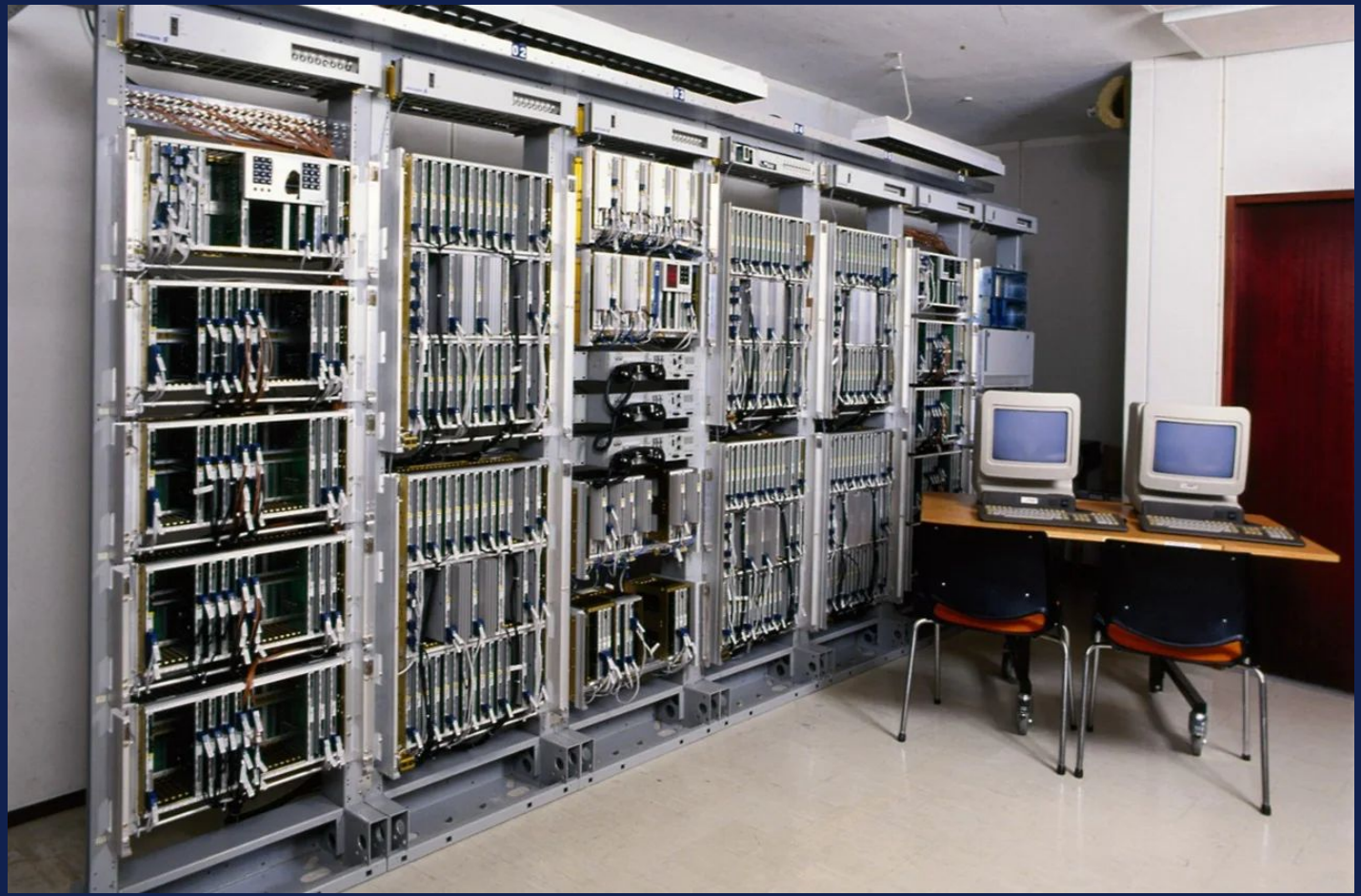
In the future, being able to "speak" a computer language will give you a tremendous advantage over those who can't, not because you can write a computer program but because you'll have a better understanding of what a computer is and does, and you will make better use of computing at the school, on the job and at home..


SNOOZES: 0 LIFT INITS: 0
PSW:
12:31:59
EPYX



~1988

~1992



1994-1996

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 27 of 28

****

International Scenes

There was once a time when hackers were basically isolated. It was almost unheard of to run into hackers from countries other than the United States. Then in the mid 1980's thanks largely to the existence of chat systems accessible through X.25 networks like Altger, tchh and QSD, hackers world-wide began to run into each other. They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles.

With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there. If you want to contribute a file about the hacking scene in your country, please send it to us at phrack@well.com.

This month we have files about the scenes in Argentina, Australia and Greece.

Argentina: Hacking at the ass of the world

by: OPii.

Yeah, i know, it's something you just can't stop, whenever you try to sleep that recurrent idea comes and recurses through your very brain, you are blind, it happens to be worse than MTV, you just can't get to sleep, you stay up for hours, you forget to feed yourself, you can't even remember your name, you turn catatonic, you stand still stretching every nerve and mumbling "hhmmpff..sc.eenn...arghh..teennn..ahhh..." and then you explode in a terrifying scream...

"ARRRGHHHHHH, WHAT THE FUCK IS GOING ON IN ARGENTINA??????"

Right?

NO????

Internet

The Internet is rarely know and even less used in the student, professor, computer and communications professionals circles. It's a depressive experience to explain the workings of "telnet","rlogin","ftp" and such "eccentricities" to people who were supposed to know about them from their TCP/IP books, courses and lectures. You, reader, could allege that a networked unix system is enough to explain this, but despite the technical explanations, the political, economic and social implications of the Internet will remain unknown until a vast amount of persons actually USE and EXPERIENCE it. And I'm not talking about "Joe citizen" here, I'm talking about people that would actually NEED the net if they were to improve their work.
It's like describing the taste of an apple to someone, he'll surely understand what you say but don't expect him to understand what it tastes like until he actually bites it.

The Internet top level authority in Argentina is the Foreign Relations Ministry and its link to the rest of the world is sponsored by the 'United Nations Development Programme'. 'whois' output follows:

```
 United Nations Development Programme (NET-ARNET)
    Ministerio de Relaciones Exteriores y Culto
    Reconquista 1088 1er. Piso - Informatica
    Buenos Aires
    ARGENTINA

    Netname: ARNET-NET
    Netnumber: 140.191.0.0

    Coordinator:
      Amodio, Jorge Marcelo  (JMA49)  PETE@ATINA.AR
      +54 1313 8082

    Domain System inverse mapping provided by:

      ATINA.AR   140.191.2.2
      ATHEA.AR   140.191.4.10

    Record last updated on 06-May-91.
```

Argentina has only an UUCP link (well, once again this is just the publicly known info...) to the Internet through UUNET, connecting several uucp linked networks to it (RAN,RECYT,etc). Atina.ar is the most important host in this scheme, seconded by the Science and Technology Secretary's host (SECYT) and the University of Buenos Aires (UBA) host located at the Exact and Natural Sciencies Faculty in a dependency known as the "CCC".
There's also a company the offers Internet connectivity bypassing atina and uunet. 'whois' output:

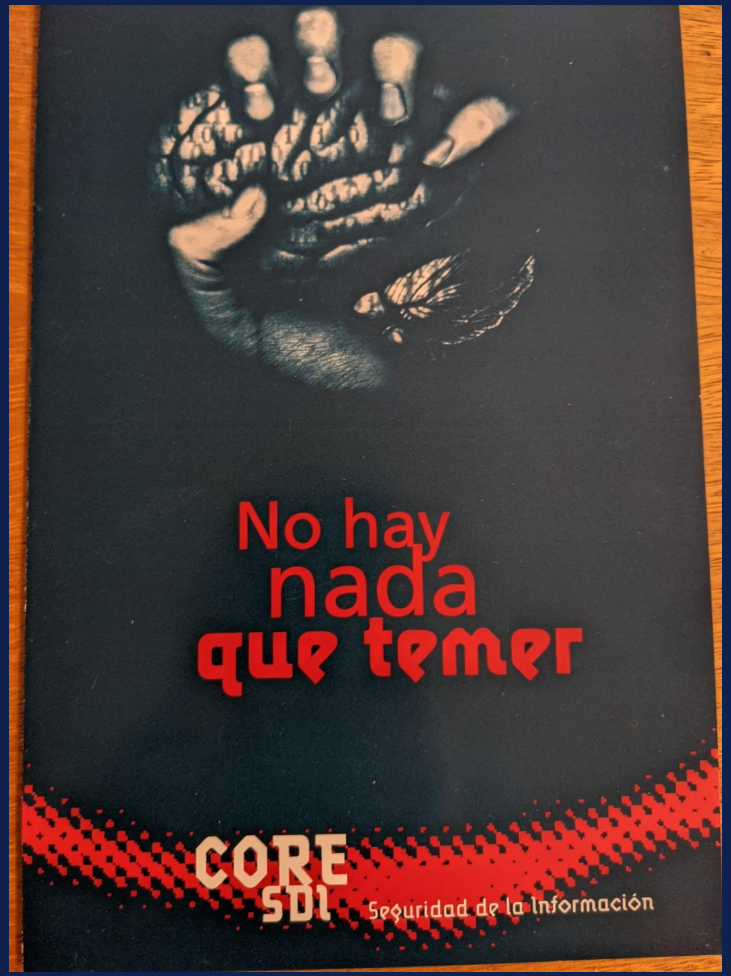
```
 SatLink Uucp/Internet (SATLINK-DOM)
    Casilla de Correo 3618
    (1000) Correo Central
    Buenos Aires
```

http://phrack.org/issues/45/27.html

1994

“Buy the ticket. Take the ride.”

- Hunter Stockton Thompson


No hay
nada
que temer
CORE
SDI
Seguridad de la Información


CORE
SDI
Nuestros Servicios
Diagnóstico
Optimización de seguridad
Diseño de políticas de seguridad
Capacitación
Análisis de proyectos que comprometan información sensible
Equipo de respuesta frente a emergencias
Desarrollo de herramientas para seguridad informática
Nuestros Productos
Ballista Network Auditing System
Network Scanner, representantes exclusivos de SNI en Latinoamérica
OpenBSD
SO Unix de perfil ultra seguro, distribuidores en Argentina
ICE³ Intrusion Detection System
Alpha2
Complemento de seguridad para sistemas operativos monousuarios
Versor
Sistema de identificación y seguridad para transferencia de información
Santa Fe 2861 5to C
(1425) Capital, Argentina
Telfax: (54-1) 821-1030
core@secnet.com
www.secnet.com/core
Seguridad de la Información

~1996

Propuesta para la implementación de un esquema de seguridad informática para el Banco de Boston.

Introducción

La presente propuesta contempla la implementación de un sistema de seguridad en el ámbito de las redes el Banco de Boston de acuerdo a las especificaciones y características técnicas surgidas de la reunión mantenida por Iván Arce, de CORE SDI S.A. y José P. D'Ambrosio de Banco de Boston el 17 de Julio de 1997.
En ella se determinaron las necesidades básicas de seguridad y las plataformas y el entorno de operación sobre las que se implementará una solución.
En este sentido, la propuesta de CORE SDI S.A. incluye una esquema de solución a implementarse sobre las siguientes plataformas, sistemas operativos y software de aplicación:

- Estaciones de trabajo (clientes) con sistemas operativos MS-DOS, MS Windows 3.1, 3.11, 95 y OS/2.
- Servidores Novell Netware 3.12 y 4.x
- Servidores UNIX AIX v3.2.5 o superior
- Bases de datos SYBASE y xBASE (dBAse,FoxPro, Clipper)
- 24 aplicaciones 'críticas' desarrolladas en diversos lenguajes.
- 80 aplicaciones de uso regular desarrolladas sobre diversos lenguajes.
- Redes locales corriendo protocolos IPX/SPX y TCP/IP.

Dada la complejidad del ambiente operativo y imposibilidad práctica de realizar modificaciones a todas las aplicaciones en uso a fin de que cubran los requerimientos mínimos de seguridad, CORE SDI S.A. plantea una solución alternativa que proporcionará los mecanismos necesarios para un funcionamiento transparente e independiente de las distintas plataformas y aplicaciones.
Dicha solución se detalla en el punto <> "Propuesta técnica".
Es importante destacar que la presente propuesta es de carácter general y a fin de elaborar una especificación técnica detallada y un presupuesto final será necesaria una etapa de relevamiento del ambiente de operación sobre el que se implementará la solución.

Normas mínimas de seguridad y control de acceso

1. Administración de Seguridad.
2. Listado de usuarios y perfiles.
3. Passwords.
4. Suspensión de passwords.

seguridad de la información
Lucio N. Mansilla 3355 10º 'B' - (1425) Buenos Aires - Argentina - Tel/Fax: 822-2364 - Email: core@silence.secnet.com

1997

IS YOUR NETWARE CONSOLE EXPOSED?

NetWare administrators know all too well that it's either all or nothing when it comes to providing access to your NetWare file server console. So if you've been hesitating to delegate chores in order to keep security tight, you can now turn to Protocom's Secure Console for NetWare 3.0 to grant selective console views and controls to others. See our review of the hot-off-the-presses beta version on page 58B.

PROACTIVE HELP-DESK MANAGEMENT

Whether you're looking to manage a high volume of help-desk calls or to strengthen your external customer support system, ProAmerica

offers a sophisticated solution with a proactive approach. Its Service Call Management 5.1 software package ties a relational database of call tracking and customer data to an easy-to-use interface. See our review on page 58D for more.

HOW WE REVIEW

Enterprise Networking Product Reviews examine new products, focusing on their usability, features, and suitability to task. Our expert reviewers rate shipping products on a scale of cold to hot. The authors do not employ the extensive analyses used in Test Center Comparisons, so their conclusions may be different.

TALK BACK

Questions, comments, kudos? Send a message to the editor at renee_gotcher@infoworld.com. Please include "Talk Back" on the subject line. To reach a staff author, use this format: firstname_lastname@infoworld.com.

▸Security-auditing software

Ballista 2.3 fortifies networks

By Stuart McClure

If securing your network from hackers is important to you, sooner or later you're going to want to arm yourself with Ballista 2.3 for Solaris from Secure Networks. Even if you already own another auditing tool from Internet Security Systems (ISS) or Cisco, this advanced network-security auditing tool is so complete that once you use it, you'll wonder how you ever got along without it.

We've tested numerous network and system scanners in the InfoWorld Test Center, but we can't get over how much Ballista still outpaces its competitors in overall flexibility and functionality.

Girded with password tools

Among the most notable additions to this version is a GUI front end for its powerful Unix-cracking and Server Message Block (SMB)-grinding utilities. As most security

administrators know, checking your Unix and Windows NT accounts for easy-to-guess passwords is one of the first steps in any good security plan. But you usually have to rely on a separate password-cracking application such as Crack and L0phtCrack. Ballista includes this functionality for free.

However, if there was any chink in Ballista's armor, it was here. We compared Ballista's cracking utility with that of Crack 5.0 and discovered a small reporting discrepancy. The issue surfaced when it tried to crack the password "mellow." Ballista told us the password was "mellow" with an "o" and not a "0" as Crack correctly reported. Ballista ended up cracking the password but failed to report it correctly.

The SMB-grinding utility is excellent and a must for any Windows NT security administrator. Ballista remotely attempts to break into an NT server trying the user names and passwords you desire. Aside from this flexibility, the grinder could guess a typical administrator password within minutes.

Solid attack-testing protection

Besides great Unix and NT password cracking, the single greatest built-in feature is Ballista's custom packet engine and scripting language, Custom Auditing Packet Engine (CAPE) and Custom Attack Scripting Language (CASL). Together, they allow you to create any attack packet your mischievous heart desires. But only CAPE comes with a GUI in the Sun Solaris version; the NT version offers the CASL GUI. A CASL GUI will be available for Sun Solaris soon, according to company officials.

I cannot say enough about the CAPE-CASL combination. For years I have yearned for an easy way to test packet-filtering routers, proxy servers, and firewalls. With CAPE and CASL, you can create a variety of legal and illegal TCP/IP packets to test the effectiveness of the security policies within your routers and firewalls, plus you can test how vulnerable your servers are to attack. All this without relying on hacker code that can leave back doors open in your network.

CAPE and CASL give you the power to simulate attacks on your network as they are discovered on the Internet. (See diagram, above.) For example, a popular attack that was discovered recently called "newtear" allows a hacker to send an invalid TCP packet to an NT server, which forces the unpatched box to blue-screen. By developing the attack yourself, you'll know the test is accurate and free of back doors.

Ballista provides more than 310 vulnerability checks out of the box, and more are added every two weeks. In fact, along with Axent's SWAT Team, Secure Networks is one of the only commercial vendors that actually discovers security holes before the hackers do.

All the necessary port-scanning capabilities are also available, including TCP, UDP, RPC, and FTP. Ballista uses stealth port scanning, which does not wait for the TCP three-way handshake to complete and speeds up the scans.

Securing the fort

The first stage in any hacker's attack plan is to gather loads of information about your network and the systems on it. Ballista checks for those devices and programs that give away this critical information. Services such as Finger, Telnet, FTP, Whois, Ident, the Web, and Sendmail are some of the most chatty services around. Almost anyone can connect to each of these services and dig up essential information about your host systems — almost everything a hacker would need to break into your computers.

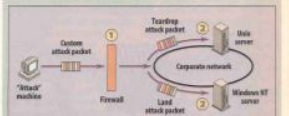
SNMP also holds priceless information about your network, including routing tables, network protocols, router hops, a system administrator's name and phone number, and much more. Ballista checks your SNMP devices for poorly chosen community strings and shows you what hackers can easily discover about your network. Ballista also provides unique vulnerability modules for discovering what Windows NT data can be detected from the outside.

Ballista's reporting capabilities are

▸BALLISTA page 58G

Ballista identifies security holes without opening vulnerabilities

Using Ballista's Custom Auditing Packet Engine (CAPE) and Custom Attack Scripting Language (CASL), you can create known or custom attacks to audit your network security.



With an "attack" machine running CAPE and CASL from outside your firewall, you can generate various attacks and send them to your network to 1. test the strength of your firewall's security policy, and 2. discover weaknesses in your network OSes.

THE BOTTOM LINE

Ballista 2.3 for Solaris

This security-auditing package is a silent force to be reckoned with, continuing to lead in overall flexibility and functionality while adding unique gems.

- **Pros:** Unix and Server Message Block password-cracking; custom packet-creation tools (Custom Auditing Packet Engine and Custom Attack Scripting Language); network mapping; more than 310 vulnerability checks.
- **Cons:** Reporting options limited.

- **Secure Networks Inc.,** Calgary, Alberta; (403) 262-8277; fax (403) 262-8227; sales@securenetworks.com; http://www.securenetworks.com.
- **Price:** $4,000 for C-class network; $1,500 for 11 to 50 licenses; flat-rate license pricing available.
- **Platforms:** Sun Solaris 2.6.

1998

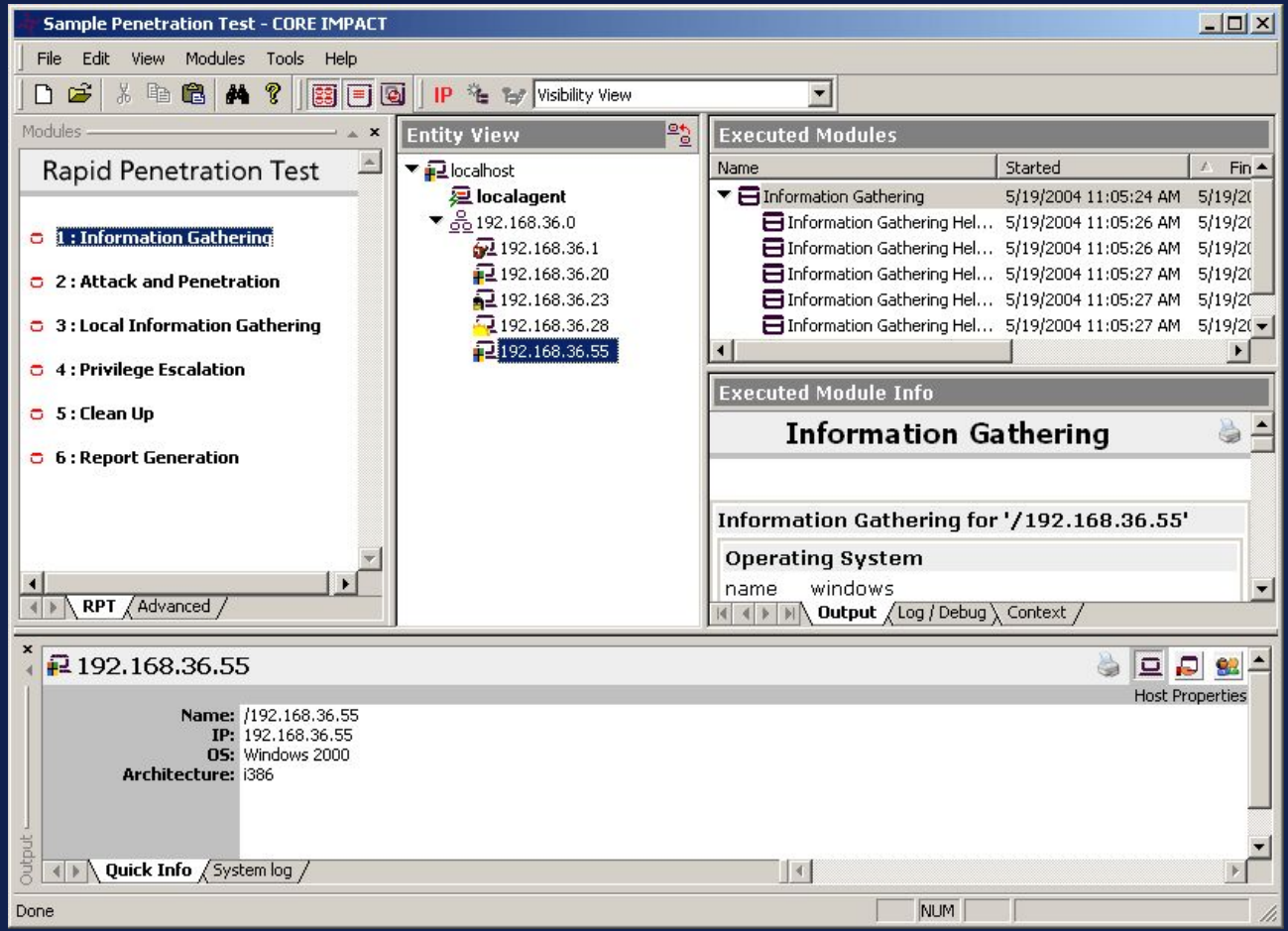

NASDAQ 100 Index, 1M, TVC
4500.0
4250.0
4000.0
3750.0
3500.0
3250.0
3000.0
2750.0
2500.0
2250.0
2000.0
1672.6
1500.0
1250.0
1000.0
750.0
500.0
250.0
93
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005

2000-2002

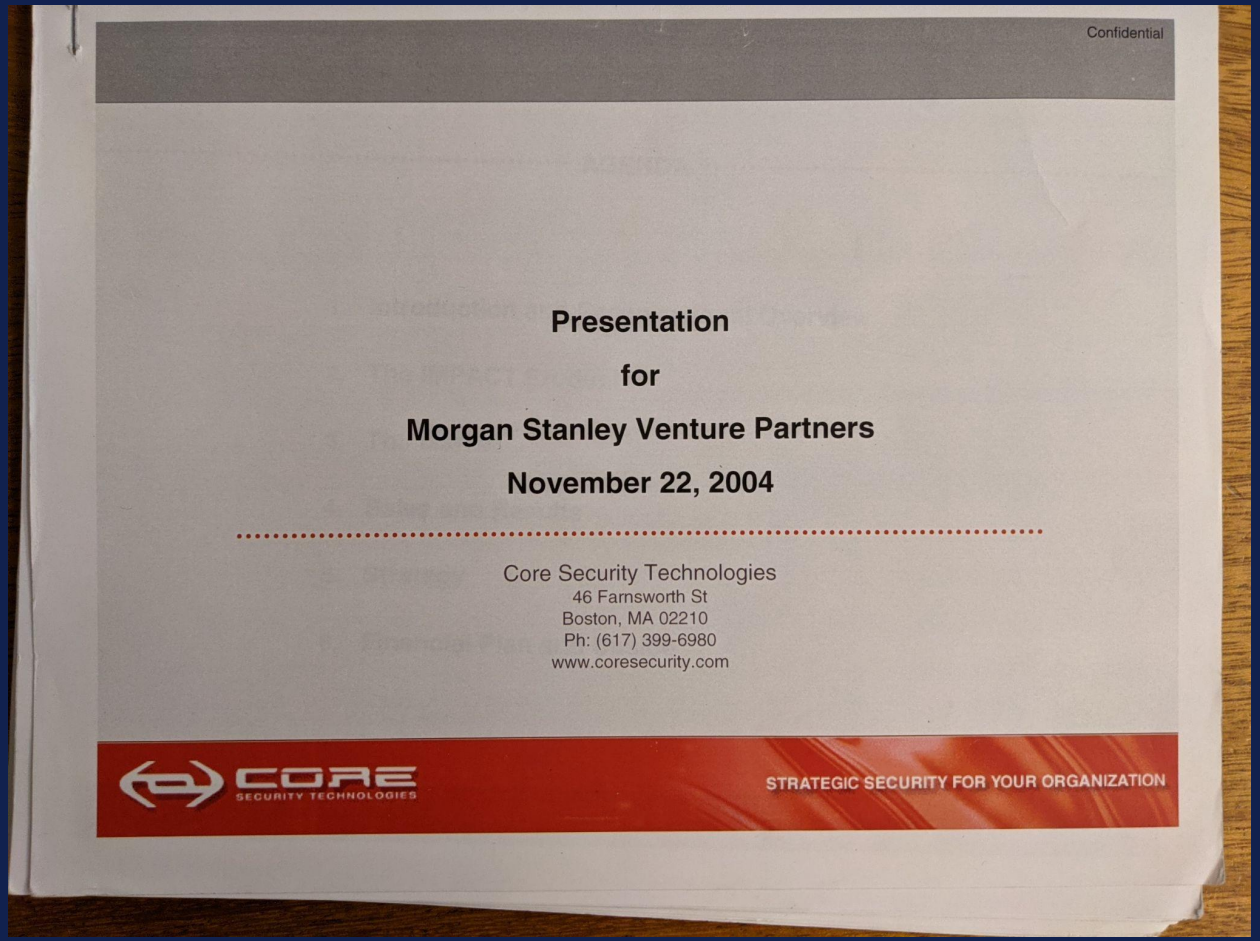
2001

“When the going gets weird, the weird turn pro.”

- Hunter Stockton Thompson


Sample Penetration Test - CORE IMPACT
File Edit View Modules Tools Help
IP
Visibility View
Modules
Rapid Penetration Test
1 : Information Gathering
2 : Attack and Penetration
3 : Local Information Gathering
4 : Privilege Escalation
5 : Clean Up
6 : Report Generation
RPT Advanced
Entity View
localhost
localagent
192.168.36.0
192.168.36.1
192.168.36.20
192.168.36.23
192.168.36.28
192.168.36.55
Executed Modules
Name Started Fin
Information Gathering 5/19/2004 11:05:24 AM 5/19/2(
Information Gathering Hel... 5/19/2004 11:05:26 AM 5/19/2(
Information Gathering Hel... 5/19/2004 11:05:26 AM 5/19/2(
Information Gathering Hel... 5/19/2004 11:05:27 AM 5/19/2(
Information Gathering Hel... 5/19/2004 11:05:27 AM 5/19/2(
Information Gathering Hel... 5/19/2004 11:05:27 AM 5/19/2(
Executed Module Info
Information Gathering
Information Gathering for '/192.168.36.55'
Operating System
name windows
Output Log / Debug Context
192.168.36.55
Host Properties
Name: /192.168.36.55
IP: 192.168.36.55
OS: Windows 2000
Architecture: i386
Output
Quick Info System log
Done
NUM

2001


Confidential
Presentation
for
Morgan Stanley Venture Partners
November 22, 2004
Core Security Technologies
46 Farnsworth St
Boston, MA 02210
Ph: (617) 399-6980
www.coresecurity.com
CORE
SECURITY TECHNOLOGIES
STRATEGIC SECURITY FOR YOUR ORGANIZATION

2004

15th USENIX Security Symposium | July 31st – August 4th 2006 | Vancouver, B.C. - Canada

Security vulnerabilities, exploits and attack patterns: 15 years of art, pseudo-science, fun & profit

Iván Arce

Core Security Technologies
Humboldt 1967 2do Piso
Buenos Aires, Argentina
(+54-11) 5556-2673
www.coresecurity.com

2006

Where do we go from here?

15 years in the information security world

A new generation entered the information security discipline in the early 90s

- Hands-on practitioners with their foundations on home computing
- Computers, and security, perceived as a “game”
- Internet networking, open standards, low cost HW/SW and the “Web” was not taken for granted

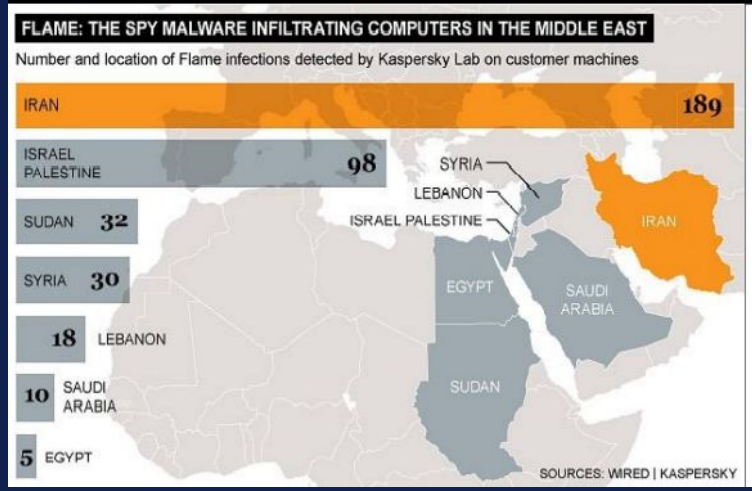
And what have they done ?

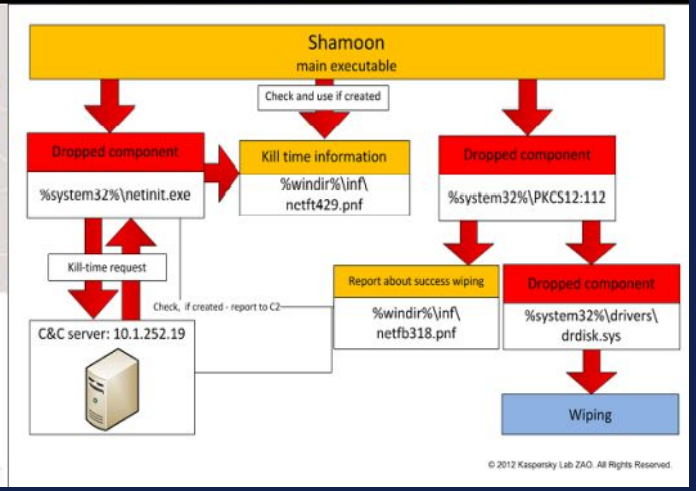
- Contributed to create an information security market and an industry to service it
- Pointlessly re-invented the wheel (several times)
- Embraced and promoted open and unmediated discussion about security issues
- Advanced and industrialized offensive security technology
- Got rich, famous and/or to jail
- Delved for 15 years at the intersection of Art, Science & Business

Did it make any difference?

What should we do to help the next generation?

https://www.usenix.org/legacy/events/sec06/tech/slides/arce.pdf


FLAME: THE SPY MALWARE INFILTRATING COMPUTERS IN THE MIDDLE EAST
Number and location of Flame infections detected by Kaspersky Lab on customer machines
IRAN 189
ISRAEL PALESTINE 98
SUDAN 32
SYRIA 30
18 LEBANON
10 SAUDI ARABIA
5 EGYPT
SYRIA
LEBANON
ISRAEL PALESTINE
IRAN
EGYPT
SAUDI ARABIA
SUDAN
SOURCES: WIRED | KASPERSKY


Shamoon
main executable
Check and use if created
Dropped component
%system32%\netinit.exe
Kill time information
%windir%\inf\
netft429.pnf
Dropped component
%system32%\PKCS12:112
Kill-time request
Check, if created - report to C2
Report about success wiping
%windir%\inf\
netfb318.pnf
Dropped component
%system32%\drivers\
drdisk.sys
C&C server: 10.1.252.19
Wiping
© 2012 Kaspersky Lab ZAO. All Rights Reserved.

2009+

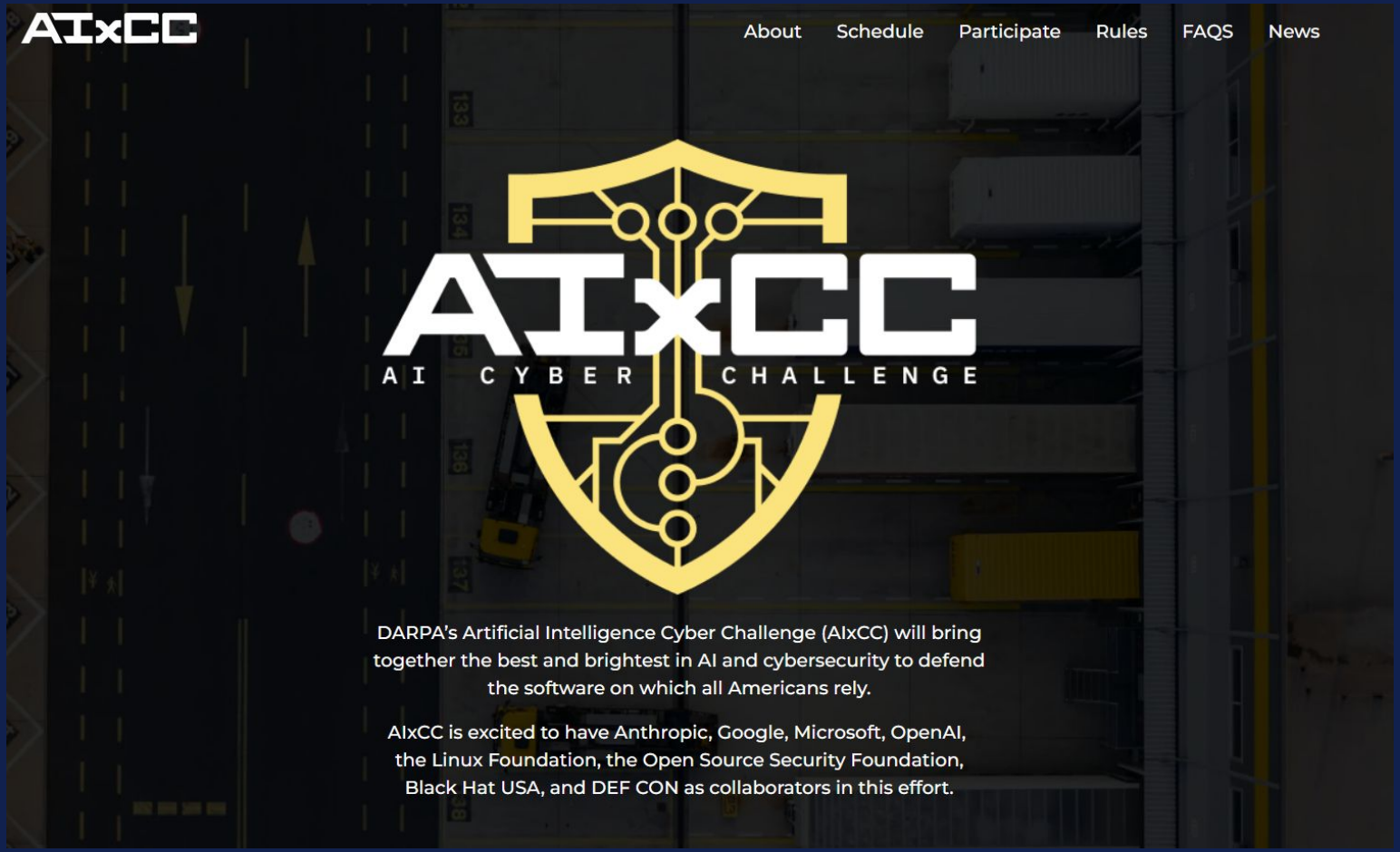
2013

Winter is coming… (se nos viene la noche)
Ekoparty 11 – Octubre 2015- Buenos Aires, Argentina

2016


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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 GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.
Contact
If you need our assistance, send a message by clicking <Contact Us>.
We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!
Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $600 worth of bitcoin to this address:
Copy
Check Payment
Decrypt

2017


AIxCC
About
Schedule
Participate
Rules
FAQS
News
AIxCC
AI CYBER CHALLENGE
DARPA's Artificial Intelligence Cyber Challenge (AIxCC) will bring together the best and brightest in AI and cybersecurity to defend the software on which all Americans rely.
AIxCC is excited to have Anthropic, Google, Microsoft, OpenAI, the Linux Foundation, the Open Source Security Foundation, Black Hat USA, and DEF CON as collaborators in this effort.

2024


...the doomsday machine
is terrifying.

What I think I learned

Specialization is for insects

“A human being should be able to change a diaper, plan an invasion, butcher a hog, conn a ship, design a building, write a sonnet, balance accounts, build a wall, set a bone, comfort the dying, take orders, give orders, cooperate, act alone, solve equations, analyze a new problem, pitch manure, program a computer, cook a tasty meal, fight efficiently, die gallantly.
Specialization is for insects.”

- Robert Heinlein, Time Enough for Love (1988)

Generalists or Specialists ?

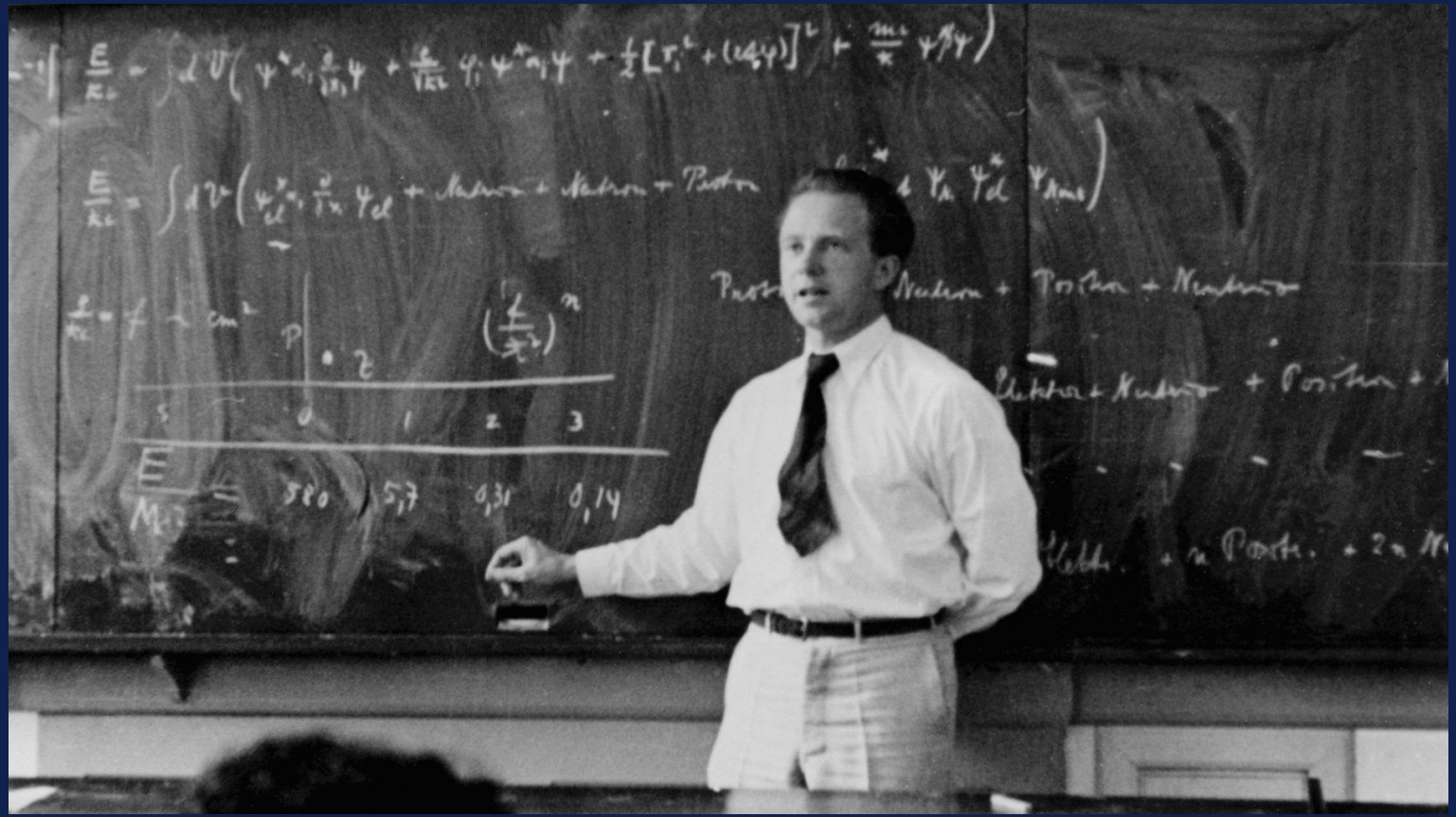
Artists, craftsmen|women or scientists?

“T.S. Kuhn Revisited”, Dan Geer, NSF, 2015 http://geer.tinho.net/geer.nsf.06i15.txt

Enter The Kelvinists

“When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science.”

- William Thomson, Lord Kelvin, 1883



Werner Karl Heisenberg (1901-1976)

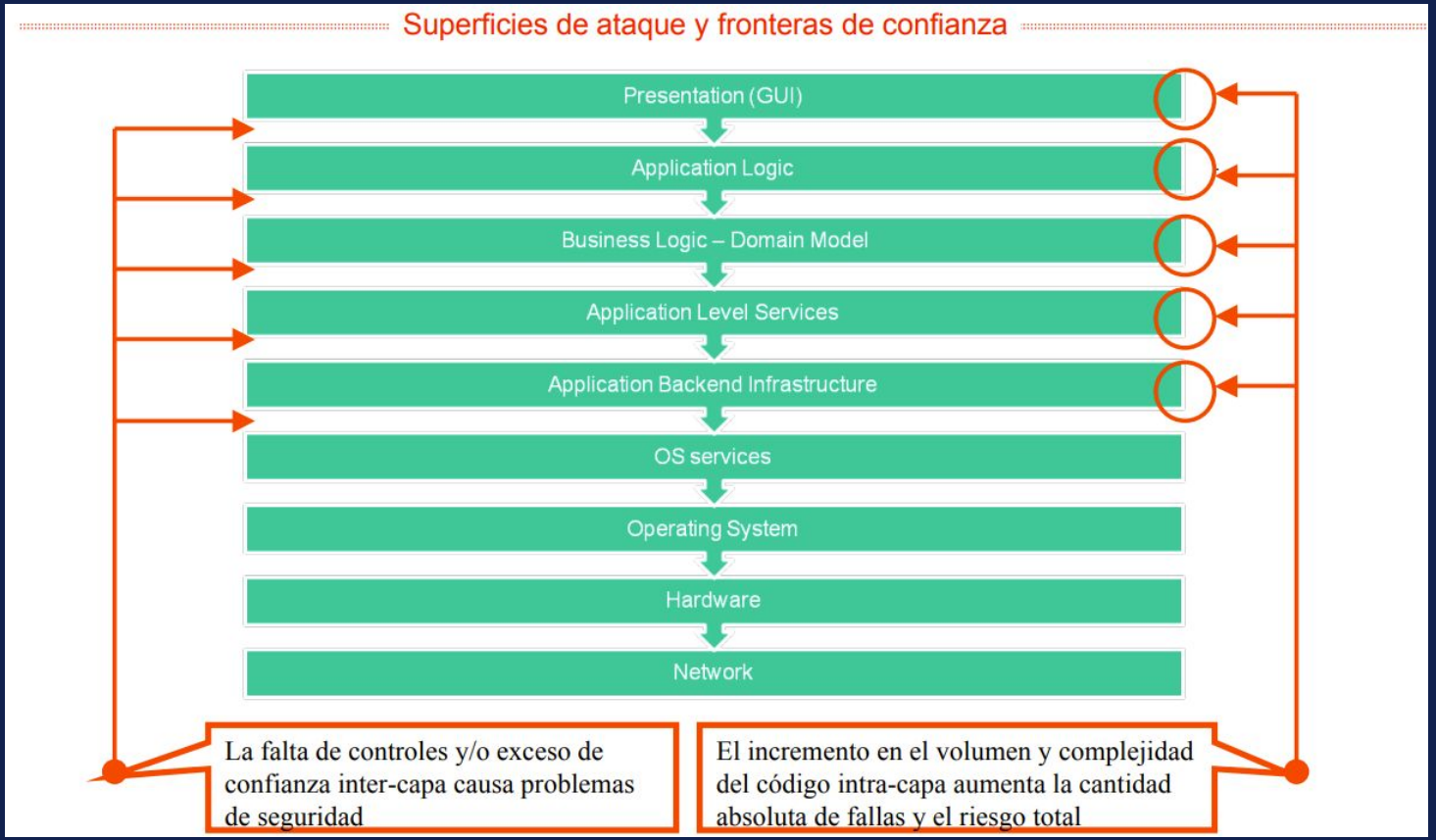
“Not everything that is important is measurable, not everything measurable is important.”

- Elliot Eisner.

OK SO HOW CAN HAZ ZECURITAY?

Security is about Thickness and Boundaries

Superficies de ataque y fronteras de confianza



“Tecnologías emergentes y tendencias de seguridad”, Iván Arce, WSEGI, 38va JAIIO, 2009.

Its Weird Machines all way down

“What hacker research taught me”, Sergey Bratus, Dartmouth College, 2009.
https://www.cs.dartmouth.edu/~sergey/hc/rss-hacker-research.pdf

Attack Surface >> Mitigations

Vulns are like cockroaches

“The Legacy of Stagefright”, Ben Hawkes, 2023. https://blog.isosceles.com/the-legacy-of-stagefright/

PoC || GTFO

“International Journal of Proof of Concept or Get The Fuck Out” https://www.alchemistowl.org/pocorgtfo/

You are not a genius*

* This may not apply to actual geniuses

Best > First*

* This may not apply to academic research

Standing on the shoulders of giants

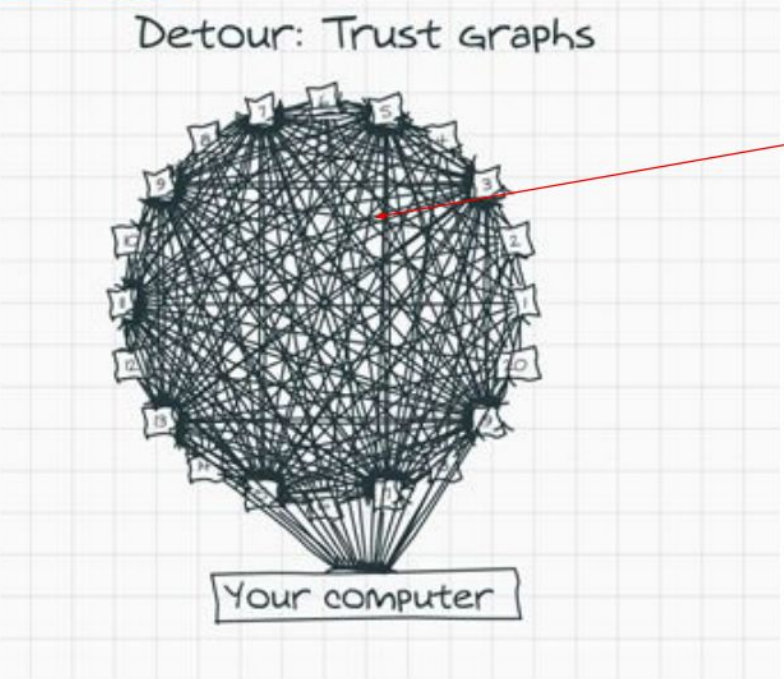
The Willie Sutton Principle

Pick your fights

Use the force (multiplier) Luke!

The Sub-zero Trust Problem

..BUT FIRST : SUPPLY CHAIN SECURITY TRUST GRAPH



YOU
ARE
HERE

Trust graph != dependency graph
The trust graph is not a tree
but if it was..
what would be the root?

Image courtesy of:
Thomas Dullien (Halvar Flake), *Re-architecting a defendable Internet*, O'Reilly Security Conference, Amsterdam 2017
https://drive.google.com/file/d/0B5hBKwqSqYFacC1jejJYSE1LTlk/view?resourcekey=0-JaTOSUC_e5A7yzCkPeEGHQ

https://github.com/quarkslab/conf-presentations/blob/master/Confs/CERT2023/20230424-CERTvendors-conf-Reflections_on_Supply-chain_security-iarce.pdf

Infosec problems that remain unsolved

- How to build software without vulnerabilities
- How to find vulnerabilities efficiently
- How to exploit vulnerabilities efficiently
- How fix vulnerabilities efficiently and effectively
- How to determine if a program is goodware or malware
- How to measure information security risk
- How to keep a secret
- How to compute in secret
- Who do we trust

The Future

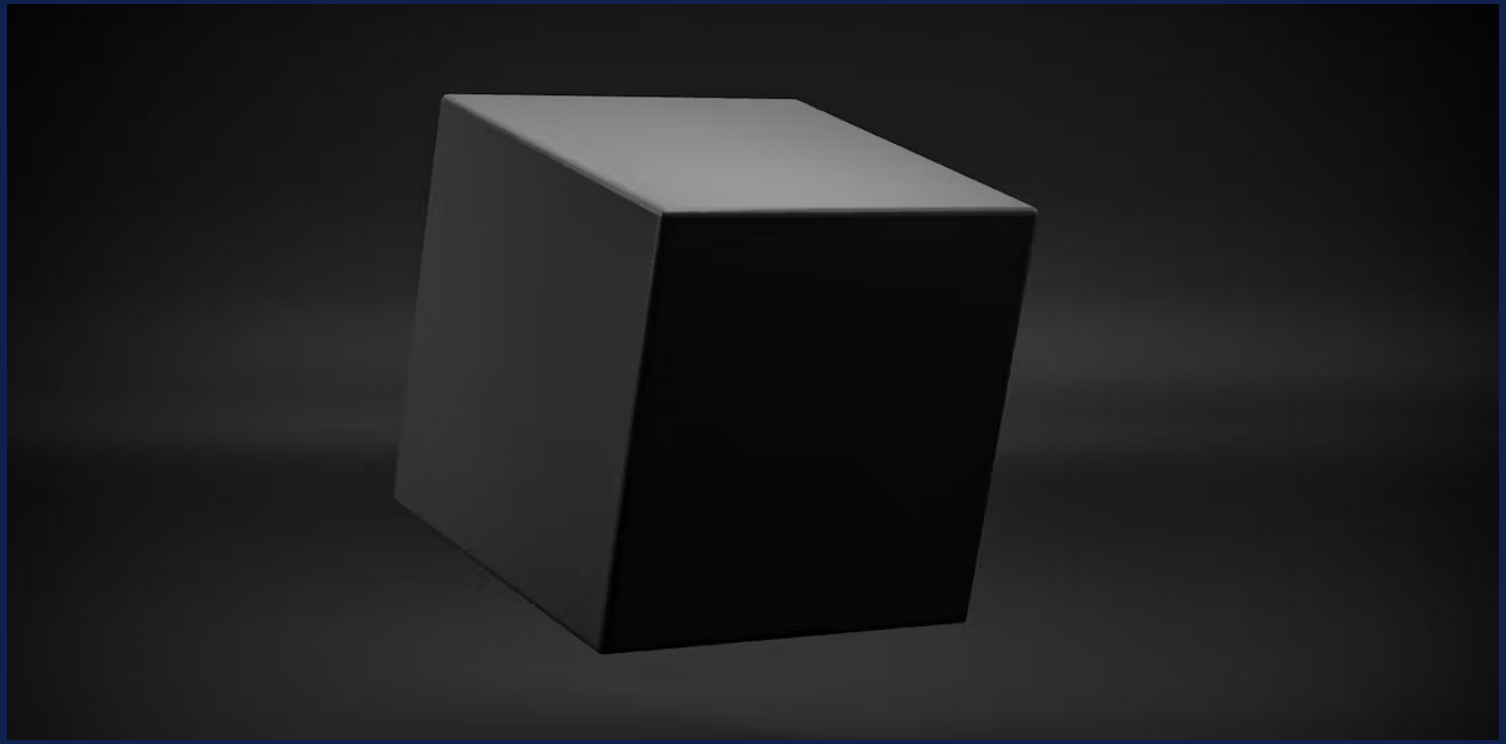
“Prediction if very difficult, especially if it’s about the future”

- Niels Bohr

Compute(Big Data)->Intelligence

Church of the AI

Crypto Engineering FTW



- Partition of the global dependency graph.
- The End of Abundance ?
- Continuous, autonomous, automated attack and defense.
- It is still weird machines. Look deeper.
- Old bugs never really die, they reincarnate.
- Are we plumbers or are we medics ?
- Are we human or are we dancers?

“The best way to predict the future is to invent it.”

- Alan Kay

Gracias Totales