UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Consortium GARR

# Cybersecurity: siamo in guerra! (che ci piaccia o no)

**Pier Luca Montessoro**
*Dipartimento Politecnico di Ingegneria e Architettura*
*Università degli Studi di Udine*

**Conferenza GARR – Cagliari, 3 ottobre 2018**


WARNING
POLITICAL INCORRECTNESS
ZONE AHEAD


LET'S
START!


IMSAI


United Artists

anno: 1983

# CRIMINALITÀ ORGANIZZATA


The underground marketplace
Ransomware toolkit
$10 – $1,800
DDoS short duration (< 1 hr)
$5 – $20
Documents (Passports, utility bills)
$1 – $3
Android banking Trojan
$200
BANK
Credit cards
$0.5 – $30
Cloud service account
$6 – $10
GIFT
Gift card
20%– 40% (of face value)
Cash-out service
10%– 20% (of acct. value)
Where everything has a price


The Dark Web

**anno: 2017**


Surface Web
<10% of Internet
– Indexed Internet
Deep Web
>90% of Internet
– Unindexed Internet
Dark Web (Darknet)
- Subset of Deep Web
- Hidden Services

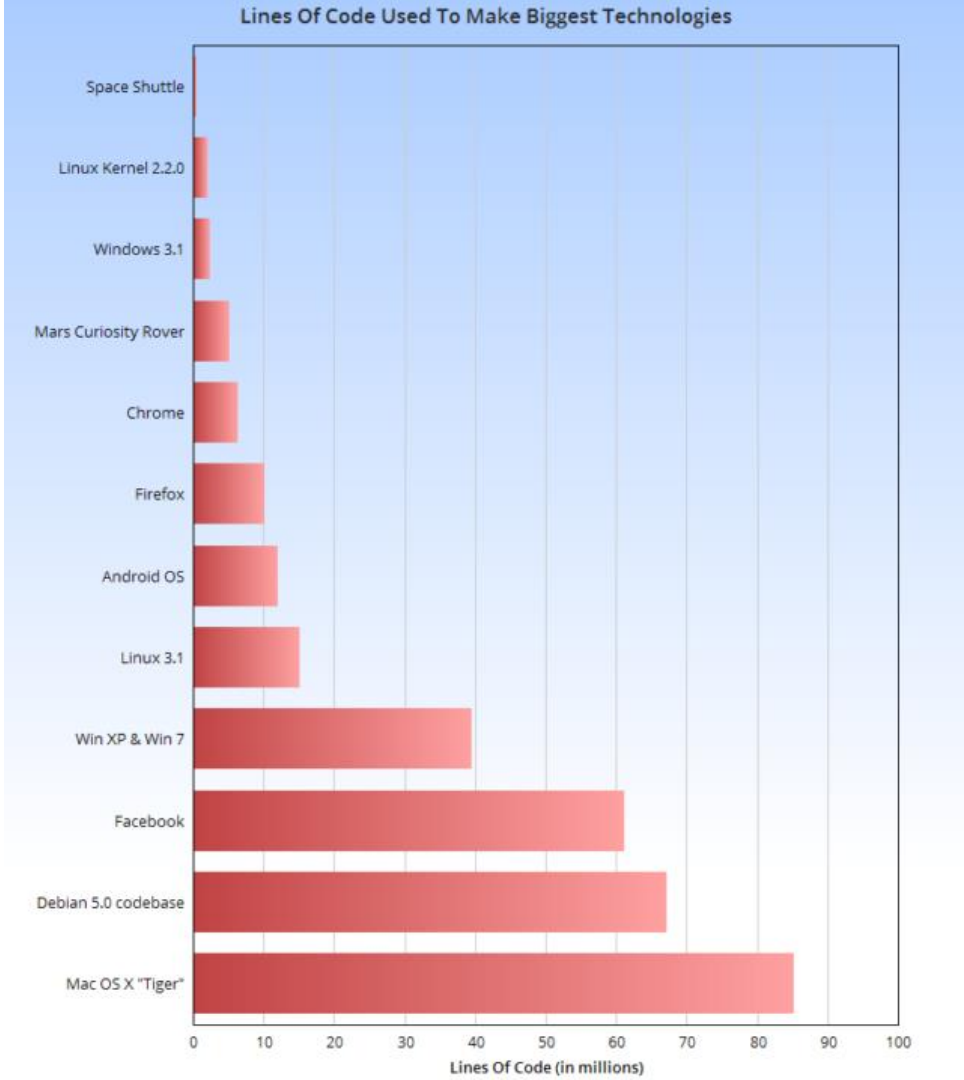
**Nel 2017 la cyber security è costata 600 miliardi di dollari (0.8% del PIL mondiale)**

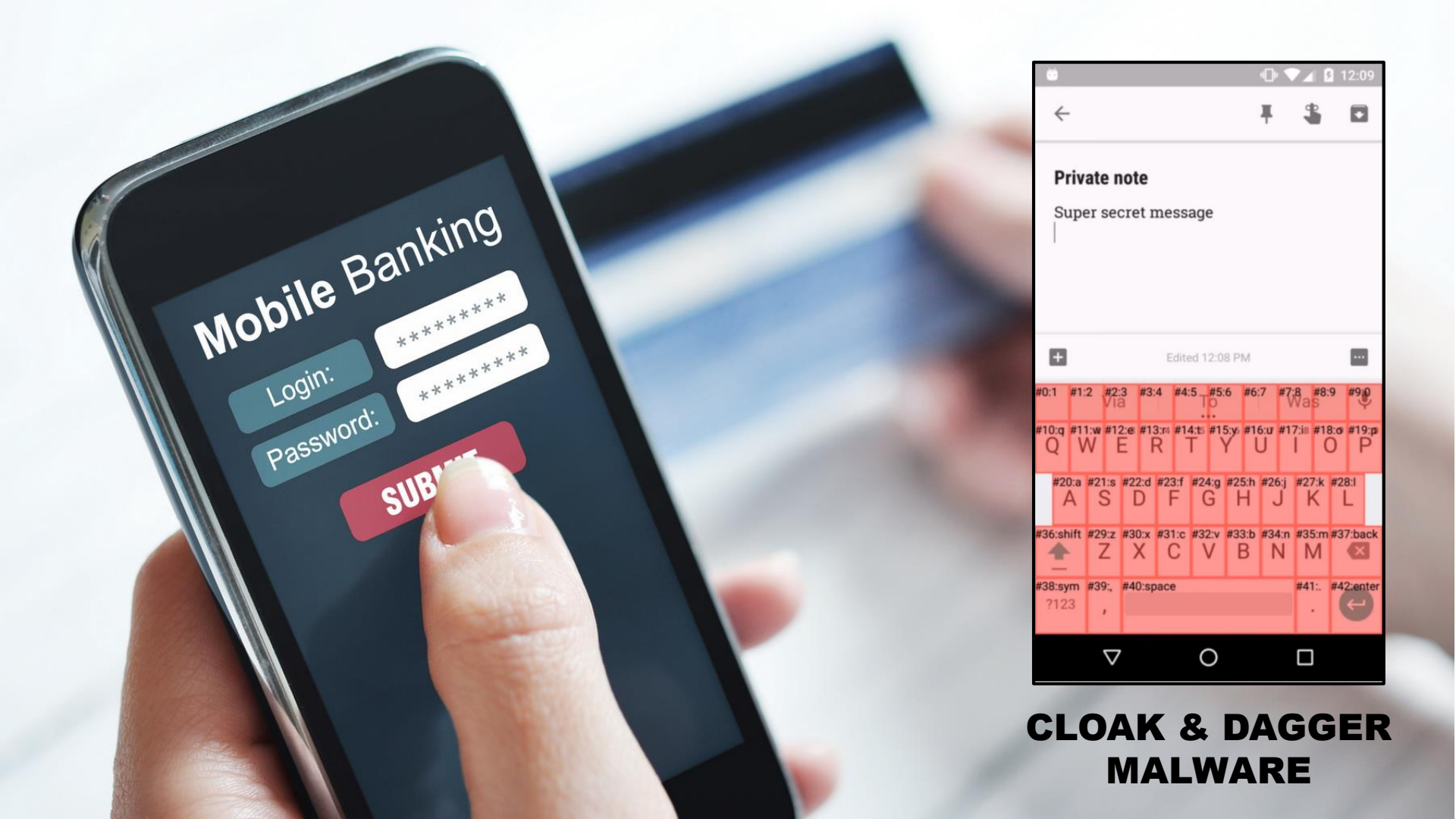
**Con lo 0.1% del PIL mondiale si potrebbe risolvere il problema della scarsità d'acqua potabile sull'intero pianeta**


PERCHÉ SIAMO
COSÌ VULNERABILI?

## *UNA COMPLESSITÀ OLTRE I LIMITI DEL CONTROLLO UMANO*

- Windows 10: ~ 50 milioni di linee di codice
- Mac OS X: ~ 85 milioni di linee di codice
- Google: 2 miliardi di linee di codice, 9 milioni di file sorgenti, 25.000 sviluppatori, 15.000 modifiche al giorno






# CLOAK & DAGGER MALWARE

# È QUESTIONE DI FIDUCIA

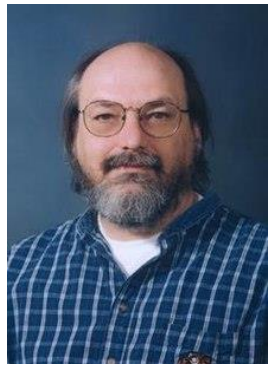
August 1984 Volume 27 Number 8
Communications of the ACM

TURING AWARD LECTURE

# Reflections on Trusting Trust

*To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.*

KEN THOMPSON



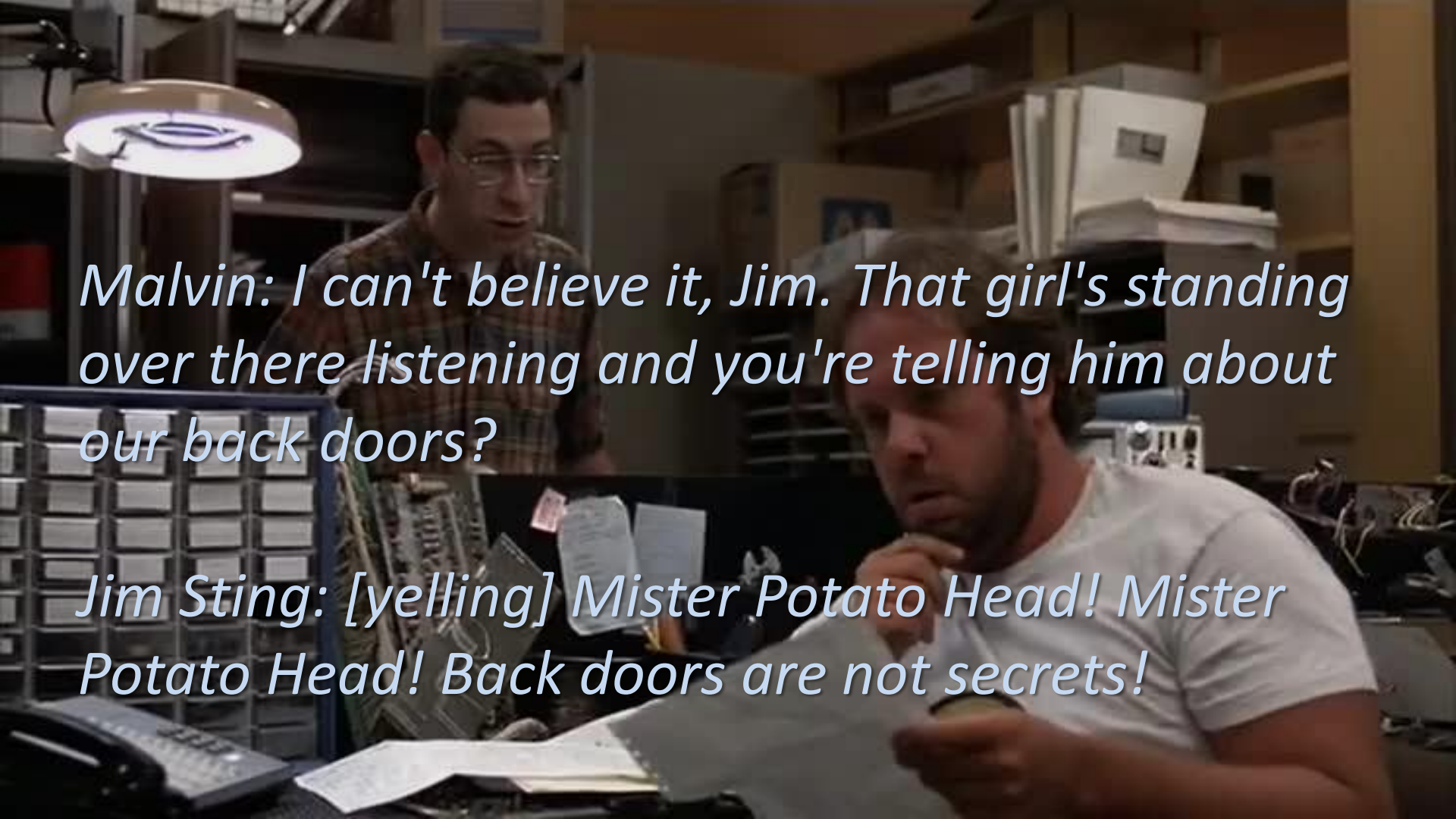
## INTRODUCTION

I thank the ACM for this award. I can't help but feel that I am receiving this honor for timing and serendipity as much as technical merit. UNIX[1] swept into popularity with an industry-wide change from central mainframes to autonomous minis. I suspect that Daniel Bobrow [1] would be here instead of me if he could not afford a PDP-10 and had had to "settle" for a PDP-11. Moreover, the current state of UNIX is the result of the

programs. I would like to present to you the cutest program I ever wrote. I will do this in three stages and try to bring it together at the end.

## STAGE I

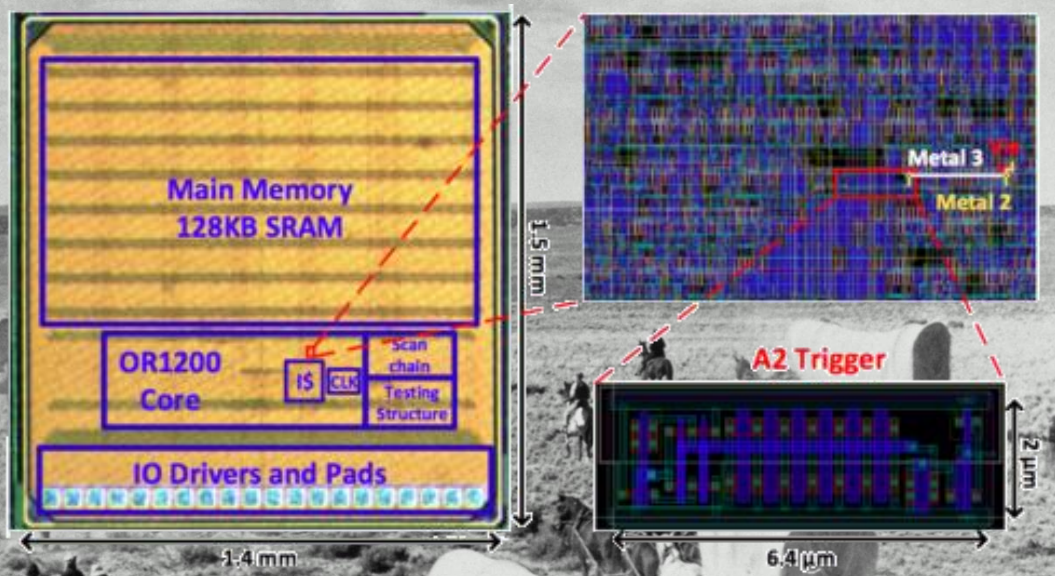
In college, before video games, we would amuse ourselves by posing programming exercises. One of the favorites was to write the shortest self-reproducing pro-

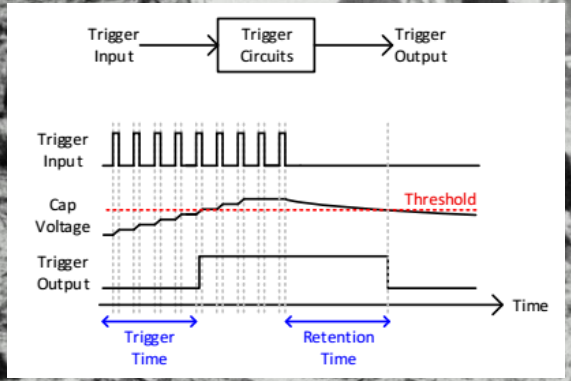

Malvin: I can't believe it, Jim. That girl's standing over there listening and you're telling him about our back doors?
Jim Sting: [yelling] Mister Potato Head! Mister Potato Head! Back doors are not secrets!

# LA PROSSIMA FRONTIERA

## BACK DOOR HARDWARE

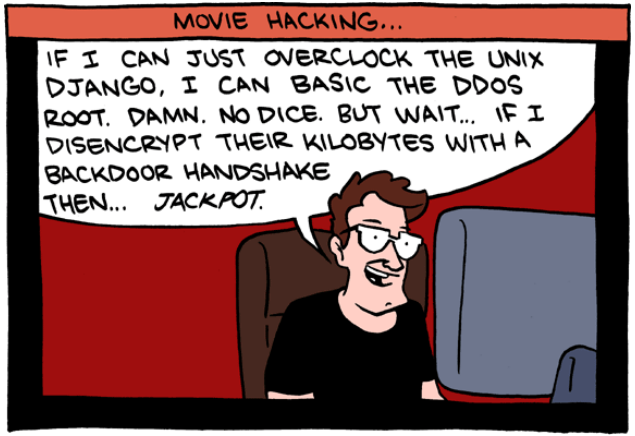
*(da una ricerca all'Università del Michigan, USA)*



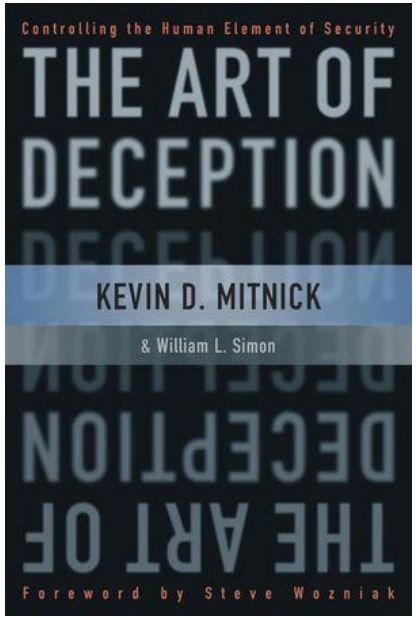



# NON SOLO TECNOLOGIA

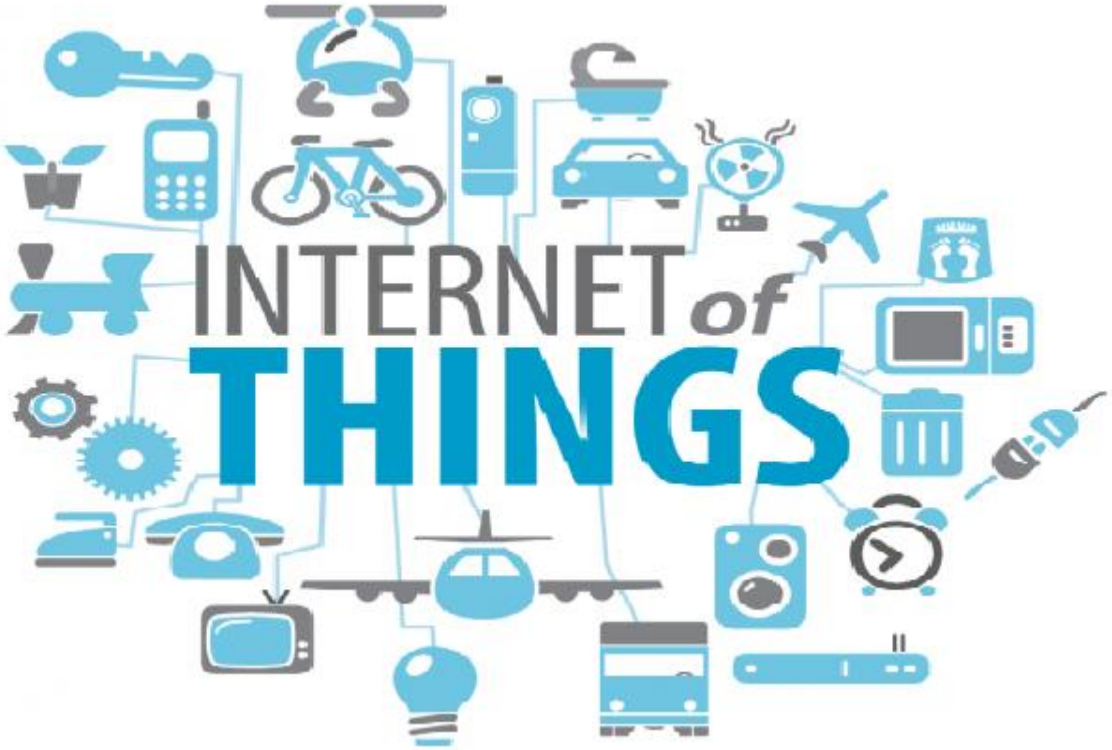

SOCIAL
ENGINEERING
The clever manipulation
of the natural human
tendency to trust.


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.


REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

# SIAMO PRONTI PER LA




?


# SHODAN un motore di ricerca per IoT hacking

https://www.shodan.io/explore

Shodan Developers Book View All...

SHODAN | Explore | Developer Pricing | Enterprise Access | Contact Us | New to Shodan? | Login or Register

## Explore

Discover the Internet using search queries shared by other users.

### Featured Categories

- Industrial Control Systems
- Databases
- Video Games

### Top Voted

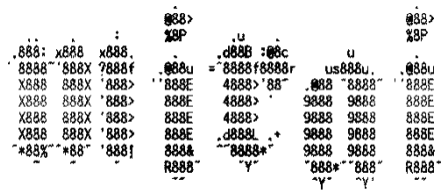
- 9,663 — Webcam — best ip cam search I have found yet. — webcam, surveillance, cams — 2010-03-15
- 3,776 — Cams — admin admin — cam, webcam — 2012-02-06
- 2,128 — Netcam — Netcam — netcam — 2012-01-13
- 1,385 — default password — Finds results with "default password" in the ba... — router, default, password — 2010-01-14
- 1,057 — dreambox — dreambox — dreambox — 2010-08-13

More popular searches...

### Recently Shared

- 1 — Brother Printers — Administration pages — printer — 2018-03-16
- 3 — Camera — 2018-03-15
- 3 — share — 2018-03-15
- 1 — share — 2018-03-15
- 1 — minecraft 895 online — 2018-03-15

More recent searches...



| USER: | PASS: | USER: | PASS: |
|---|---|---|---|
| root | xc3511 | admin1 | password |
| root | vizxv | administrator | 1234 |
| root | admin | 666666 | 666666 |
| admin | admin | 888888 | 888888 |
| root | 888888 | ubnt | ubnt |
| root | xmhdipc | root | klv1234 |
| root | default | root | Zte521 |
| root | juantech | root | hi3518 |
| root | 123456 | root | jvbzd |
| root | 54321 | root | anko |
| support | support | root | zlxx. |
| root | (none) | root | 7ujMko0vizxv |
| admin | password | root | 7ujMko0admin |
| root | root | root | system |
| root | 12345 | root | ikwb |
| user | user | root | dreambox |
| admin | (none) | root | user |
| root | pass | root | realtek |
| admin | admin1234 | root | 00000000 |
| root | 1111 | admin | 1111111 |
| admin | smcadmin | admin | 1234 |
| admin | 1111 | admin | 12345 |
| root | 666666 | admin | 54321 |
| root | password | admin | 123456 |
| root | 1234 | admin | 7ujMko0admin |
| root | klv123 | admin | 1234 |
| Administrator | admin | admin | pass |
| service | service | admin | meinsm |
| supervisor | supervisor | tech | tech |
| guest | guest | mother | fucker |
| guest | 12345 | | |
| guest | 12345 | | |



Internet of Things - number of connected devices worldwide 2015-2025

## Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)


The 'S' in IoT stands for security.
And yes, I'm aware there's no "S" in IoT.
Oleg Šelajev - Oracle Labs

# NO IOT?


**PROFITTI PER 1 MILIARDO DI DOLLARI NEL 2016**

**+250% NEI PRIMI MESI DEL 2017**

**+752% NUOVE FAMIGLIE DI MALWARE RANSOMWARE**

# MAN IN THE MAIL

*Text of spear-phishing email sent to John Podesta, the chairman of the 2016 Clinton presidential campaign*

*From:* Google <no-reply@accounts.googlemail.com>
*Date:* March 19, 2016 at 4:34:30 AM EDT
*To:* [redacted]@gmail.com
*Subject:* *Someone has your password*

Someone has your password
Hi John

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

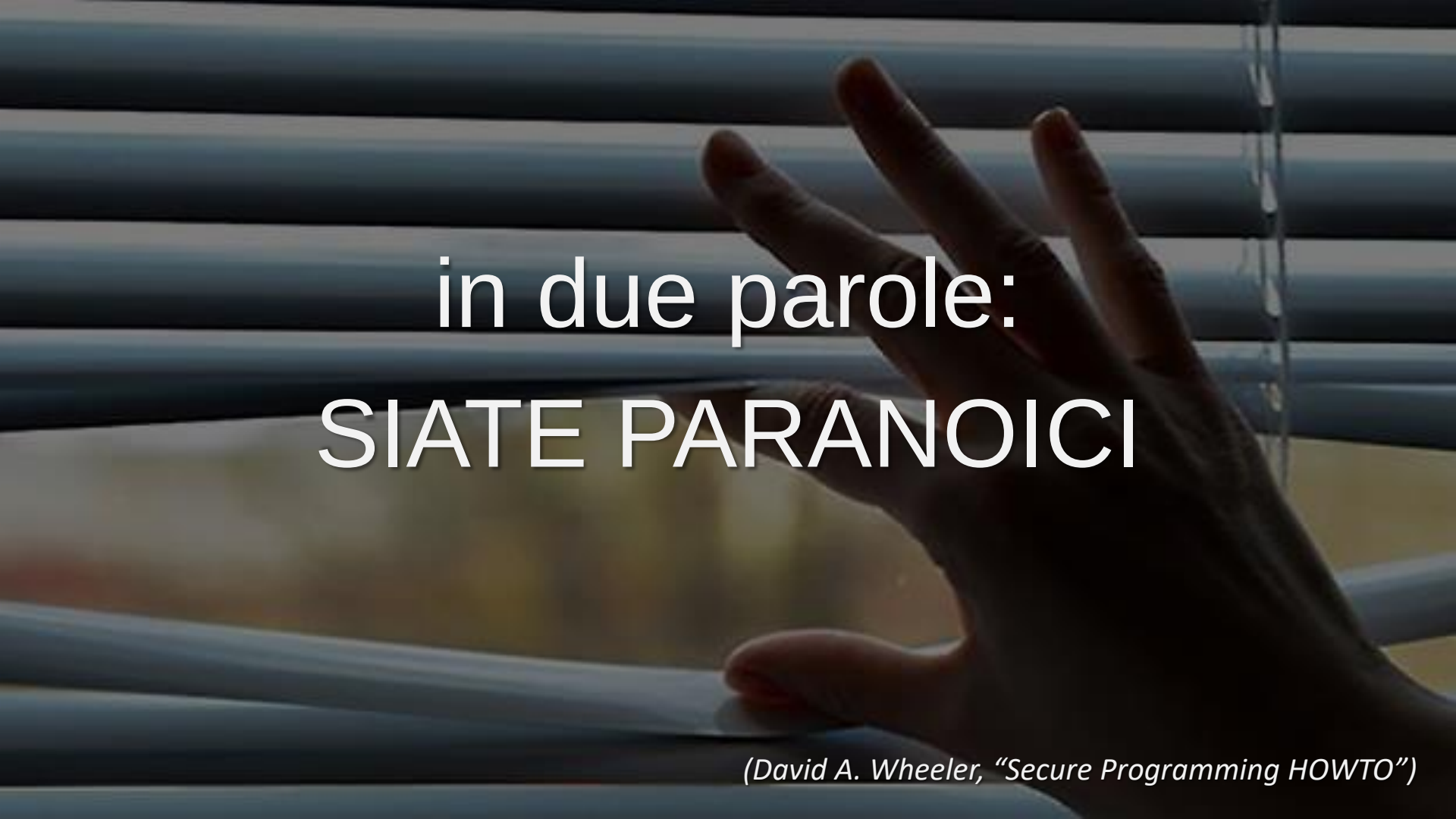
Best,
The Gmail Team
You received this mandatory email service announcement to update you about important changes to your Google product or account.


SO
WHAT?


# Manuale di sopravvivenza

Sappiate che:

- Molto probabilmente il vostro smartphone è infetto
- Molto probabilmente anche il vostro PC è infetto
- I vostri dispositivi sono sotto attacco
- Il vostro cloud/service/network provider è sotto attacco
- VOI siete sotto attacco



# in due parole:
# SIATE PARANOICI

*(David A. Wheeler, “Secure Programming HOWTO”)*

## SIATE PARANOICI!

- Abbiate un backup di tutto (non solo nei dati, ma anche nelle attività)
- Se possible, non fidatevi
  - di nulla
  - di nessuno
  - mai!
- Se dovete dare fiducia qualcuno/qualcosa, scegliete consapevolmente
- Gestite bene i vostri sistemi, la vostra rete, i vostri dispositivi IoT
- Siate cauti nel fornire dati on-line
- Siate cauti  nell'utilizzare e-mail, messaggistica and social network
- Abituatevi a comportamenti orientati alla sicurezza
- Diffondete la conoscenza tra familiari e amici


Pier Luca Montessoro - www.montessoro.it

## References


- Ken Thompson, "Reflections on trusting trust," Communications of the ACM, Volume 27, Number 8, August 1984, https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf
- David A. Wheeler, “Secure Programming HOWTO,” https://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO.pdf
- “Internet Security Threat Report,” Symantec, April 2017, https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
- “Economic Impact of Cybercrime – No slowing Down,” CSIS/McAfee, February 2018
- “Security 1:1,” Symantec, https://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms, https://www-secure.symantec.com/connect/articles/security-11-part-2-trojans-and-other-threats, and , https://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks