Is This The Software Security Crisis?

Robert Postill
Privay

Acknowledgement of Country

I begin today by acknowledging the Wurundjeri people, Traditional Custodians of the land on which I stand today, and pay my respects to their Elders past and present. I extend that respect to Aboriginal and Torres Strait Islander peoples here today.

Agenda

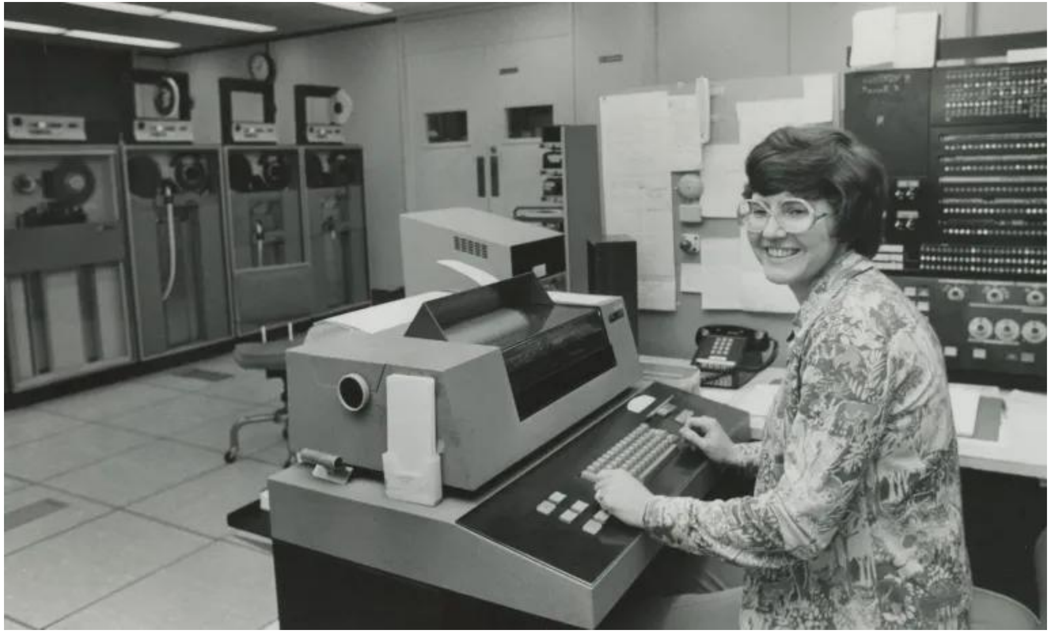
- Who Am I
- What Happened In The Software Quality Crisis?
- Signs We’re Heading In The Same Direction
- How Did The Crisis End?
- The Future

Who Am I?

- CTO for multiple startups (Ynomia, Greensync Donesafe)
- Consultant (Midnyte City, Dius)
- Ex MYOB

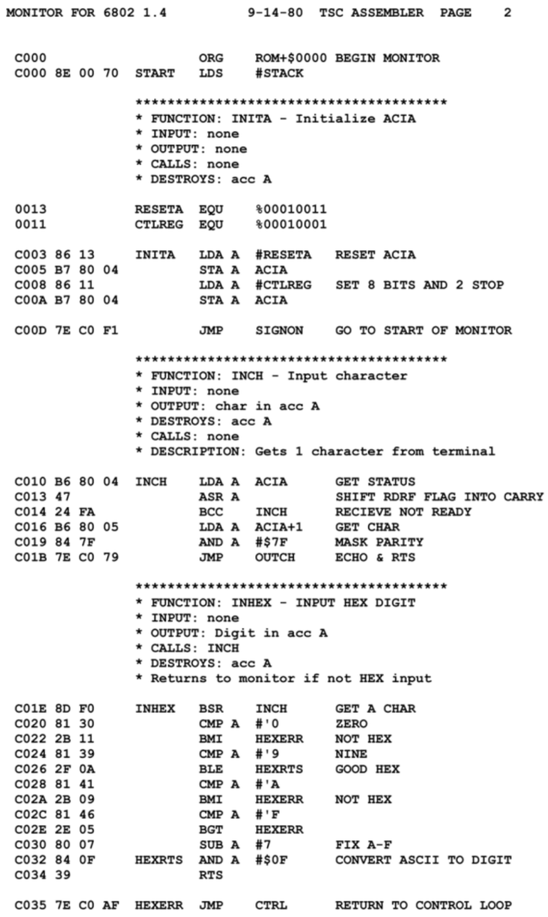
What Happened In The Software Quality Crisis?

Computers Were Different



Programming Was Different

- Intimately tied to the machine it was deployed upon
- Low-level - lots of code to get the outcome
- Optimised for memory efficiency not speed or maintenance



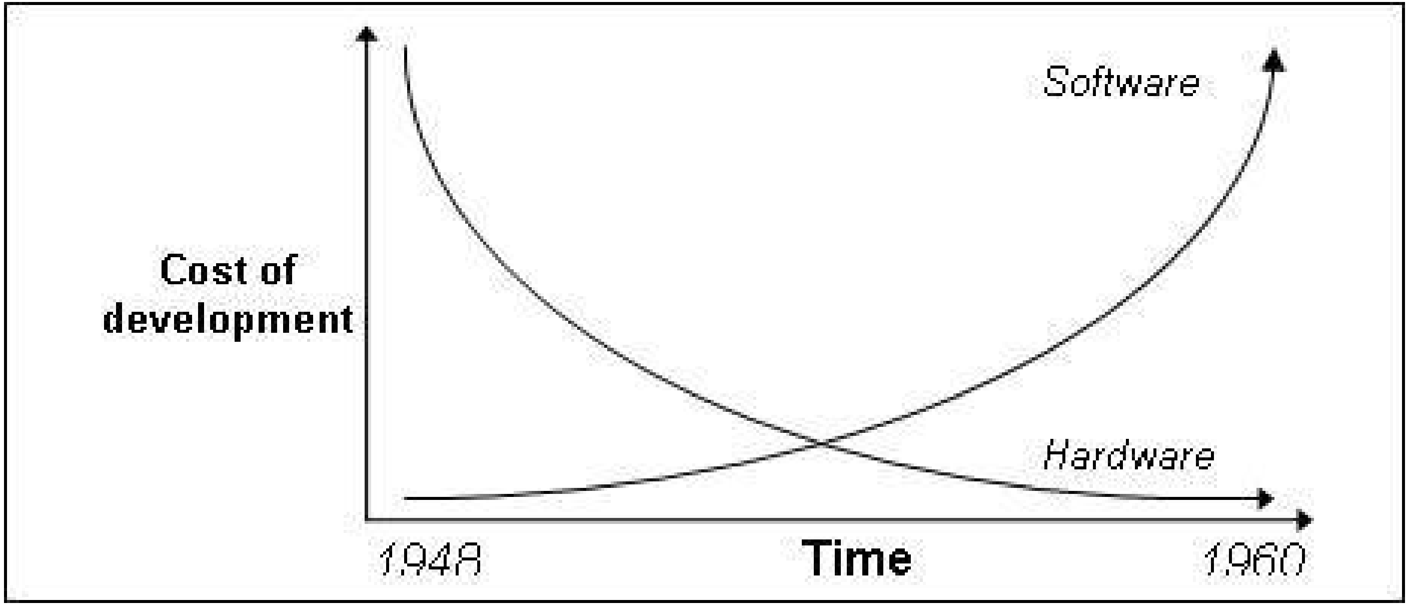
```
MONITOR FOR 6802 1.4          9-14-80  TSC ASSEMBLER  PAGE    2

 C000                  ORG    ROM+$0000 BEGIN MONITOR
 C000 8E 00 70  START  LDS    #STACK

                ****************************************
                * FUNCTION: INITA - Initialize ACIA
                * INPUT: none
                * OUTPUT: none
                * CALLS: none
                * DESTROYS: acc A

 0013           RESETA EQU    %00010011
 0011           CTLREG EQU    %00010001

 C003 86 13     INITA  LDA A  #RESETA   RESET ACIA
 C005 B7 80 04         STA A  ACIA
 C008 86 11            LDA A  #CTLREG   SET 8 BITS AND 2 STOP
 C00A B7 80 04         STA A  ACIA

 C00D 7E C0 F1         JMP    SIGNON    GO TO START OF MONITOR

                ****************************************
                * FUNCTION: INCH - Input character
                * INPUT: none
                * OUTPUT: char in acc A
                * DESTROYS: acc A
                * CALLS: none
                * DESCRIPTION: Gets 1 character from terminal

 C010 B6 80 04  INCH   LDA A  ACIA      GET STATUS
 C013 47               ASR A            SHIFT RDRF FLAG INTO CARRY
 C014 24 FA            BCC    INCH      RECIEVE NOT READY
 C016 B6 80 05         LDA A  ACIA+1    GET CHAR
 C019 84 7F            AND A  #$7F      MASK PARITY
 C01B 7E C0 79         JMP    OUTCH     ECHO & RTS

                ****************************************
                * FUNCTION: INHEX - INPUT HEX DIGIT
                * INPUT: none
                * OUTPUT: Digit in acc A
                * CALLS: INCH
                * DESTROYS: acc A
                * Returns to monitor if not HEX input

 C01E 8D F0     INHEX  BSR    INCH      GET A CHAR
 C020 81 30            CMP A  #'0       ZERO
 C022 2B 11            BMI    HEXERR    NOT HEX
 C024 81 39            CMP A  #'9       NINE
 C026 2F 0A            BLE    HEXRTS    GOOD HEX
 C028 81 41            CMP A  #'A
 C02A 2B 09            BMI    HEXERR    NOT HEX
 C02C 81 46            CMP A  #'F
 C02E 2E 05            BGT    HEXERR
 C030 80 07            SUB A  #7        FIX A-F
 C032 84 0F     HEXRTS AND A  #$0F      CONVERT ASCII TO DIGIT
 C034 39               RTS

 C035 7E C0 AF  HEXERR JMP    CTRL      RETURN TO CONTROL LOOP
```

We Hit A Limit For Complexity

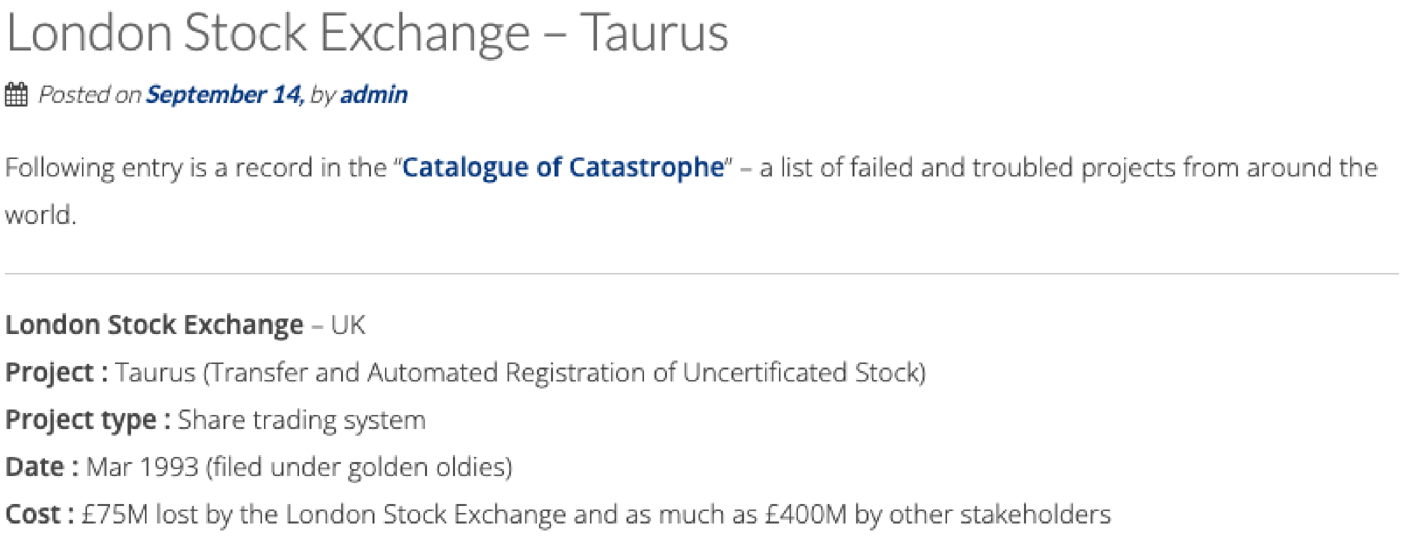
The major cause of the software crisis is that the machines have become several orders of magnitude more powerful! To put it quite bluntly: as long as there were no machines, programming was no problem at all; when we had a few weak computers, programming became a mild problem, and now we have gigantic computers, programming has become an equally gigantic problem.

Edsger Dijkstra, The Humble Programmers (1972)

We Began To Realise We Were In The Mire



We Failed… A L-O-T :grimace:



London Stock Exchange – Taurus

📅 *Posted on* ***September 14***, *by* ***admin***

Following entry is a record in the "**Catalogue of Catastrophe**" – a list of failed and troubled projects from around the world.

London Stock Exchange – UK

Project : Taurus (Transfer and Automated Registration of Uncertificated Stock)

Project type : Share trading system

Date : Mar 1993 (filed under golden oldies)

Cost : £75M lost by the London Stock Exchange and as much as £400M by other stakeholders

Signs We’re Heading In The Same Direction

We Haphazardly Implement Software

We Can't Seem To Find Anything To Make That Doesn't Require Exceptional Quality

We Don’t Seem To Know How To Price Software

How Did The Crisis End?

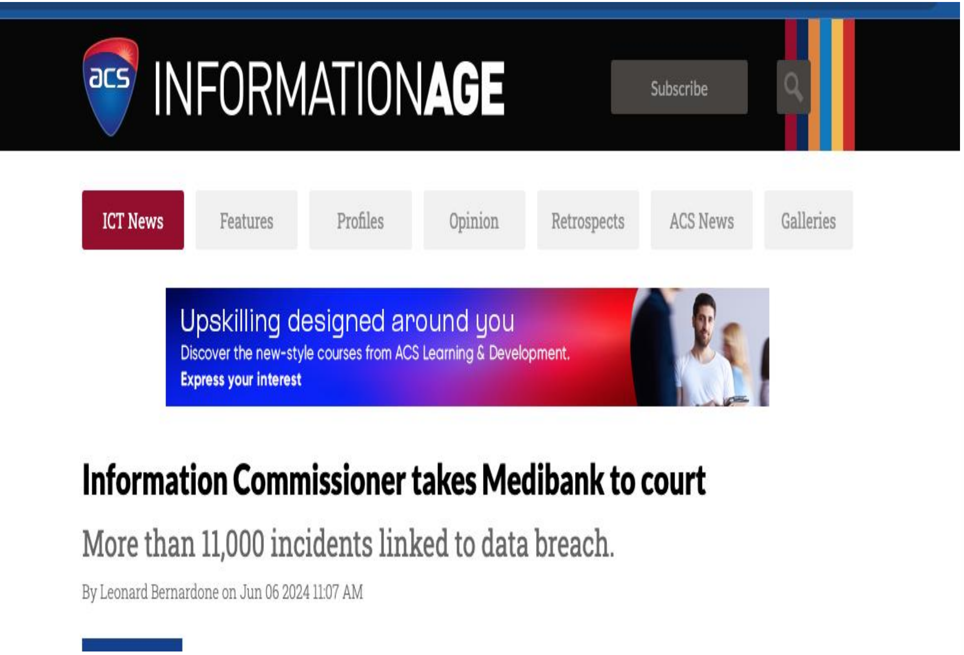
We Developed Better Tools

New Analysis Techniques

We Tried To Understand Delivery Better

The Future

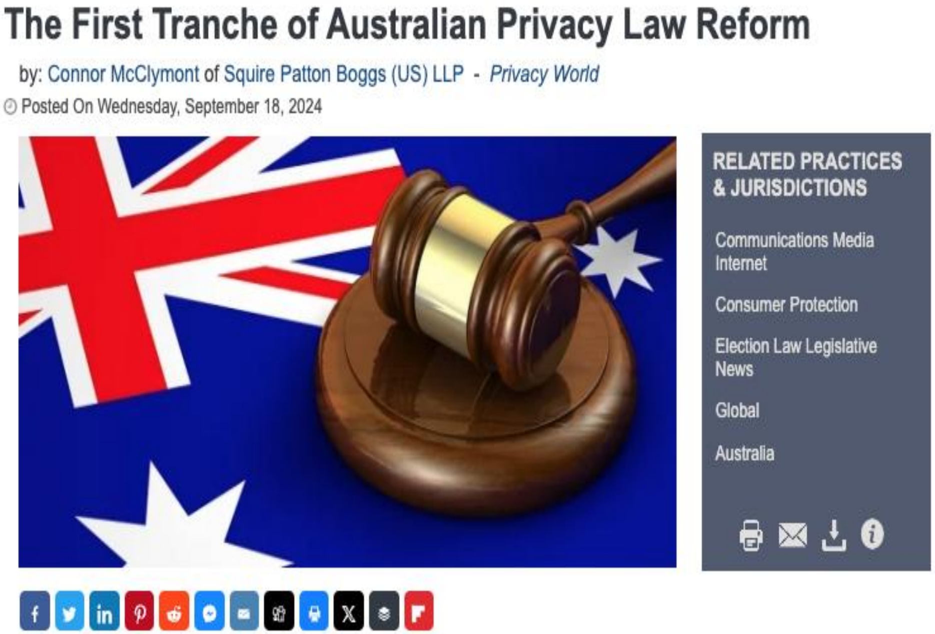
Regulation Is Coming



Information Commissioner takes Medibank to court

More than 11,000 incidents linked to data breach.

By Leonard Bernardone on Jun 06 2024 11:07 AM



The First Tranche of Australian Privacy Law Reform

by: Connor McClymont of Squire Patton Boggs (US) LLP - *Privacy World*

Posted On Wednesday, September 18, 2024

RELATED PRACTICES & JURISDICTIONS

Communications Media Internet

Consumer Protection

Election Law Legislative News

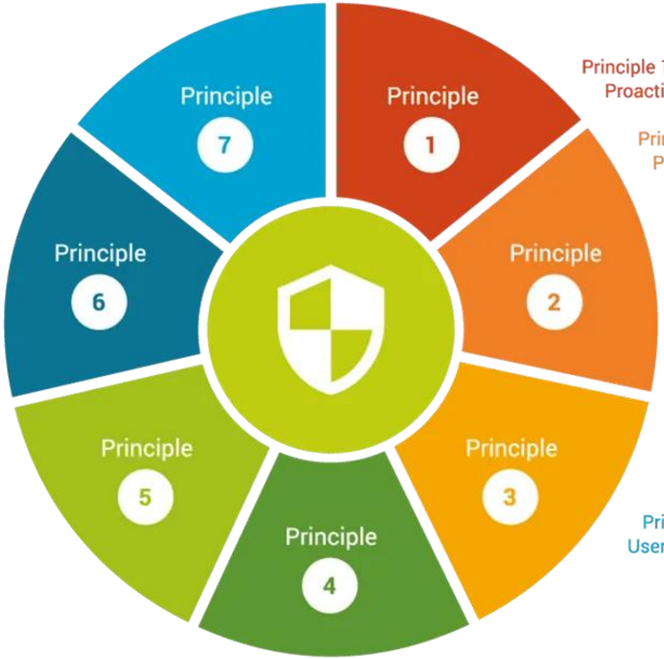
Global

Australia

We’re Going To Need To Price Software Differently

We’re Going To Need To Change The SDLC

SDLC Changes - Privacy By Design



Principle 1:
Proactive not Reactive; Preventative not Remedial

Principle 2:
Privacy as the Default Setting

Principle 3:
Privacy Embedded into Design

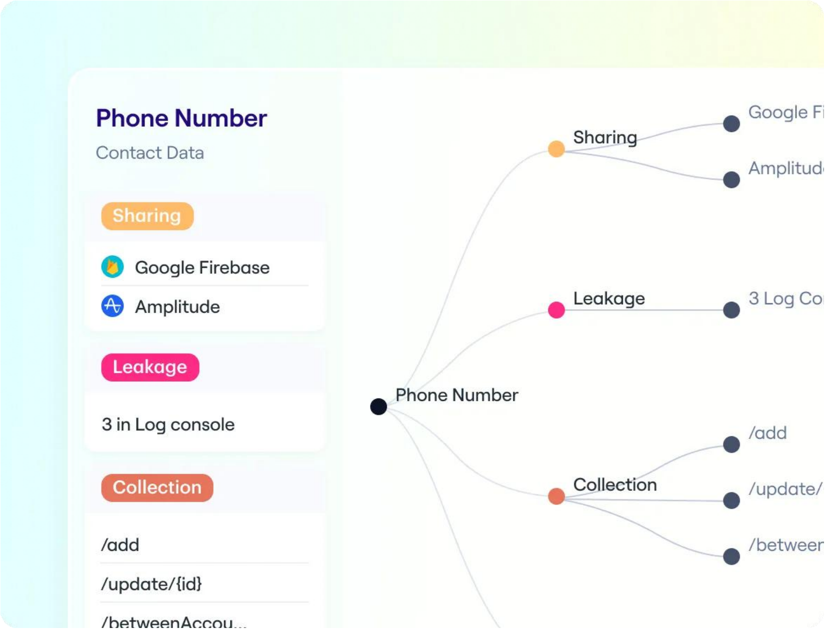
Principle 4:
Full Functionality – Positive-Sum, not Zero-Sum

Principle 5: End-to-End Security – Full Lifecycle Protection

Principle 6: Visibility and Transparency – Keep it Open

Principle 7: Respect for User Privacy – Keep it User-Centric

SDLC Changes - Data Mapping



Phone Number

Contact Data

Sharing

Google Firebase

Amplitude

Leakage

3 in Log console

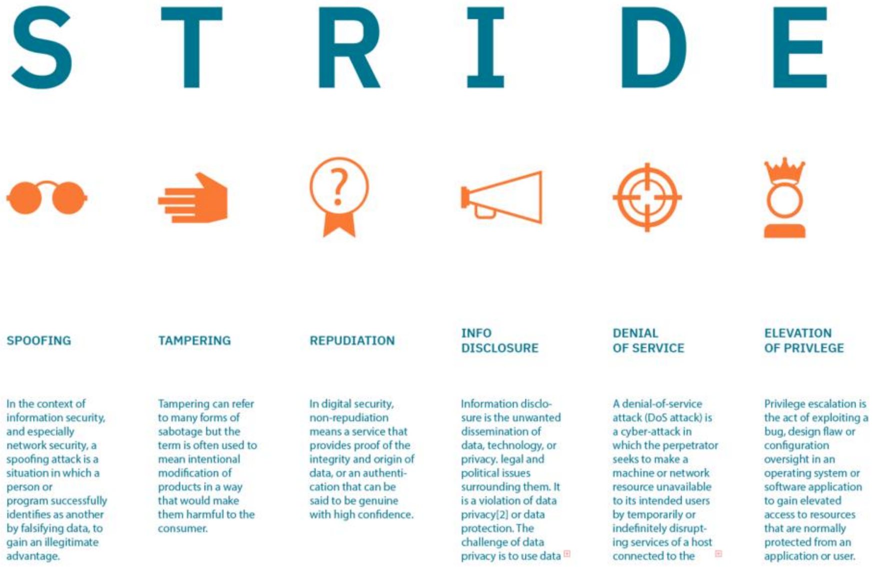
Collection

/add

/update/{id}

/betweenAccou...

SDLC Changes - Threat Modelling



SPOOFING

In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

TAMPERING

Tampering can refer to many forms of sabotage but the term is often used to mean intentional modification of products in a way that would make them harmful to the consumer.

REPUDIATION

In digital security, non-repudiation means a service that provides proof of the integrity and origin of data, or an authentication that can be said to be genuine with high confidence.

INFO DISCLOSURE

Information disclosure is the unwanted dissemination of data, technology, or privacy. legal and political issues surrounding them. It is a violation of data privacy[2] or data protection. The challenge of data privacy is to use data

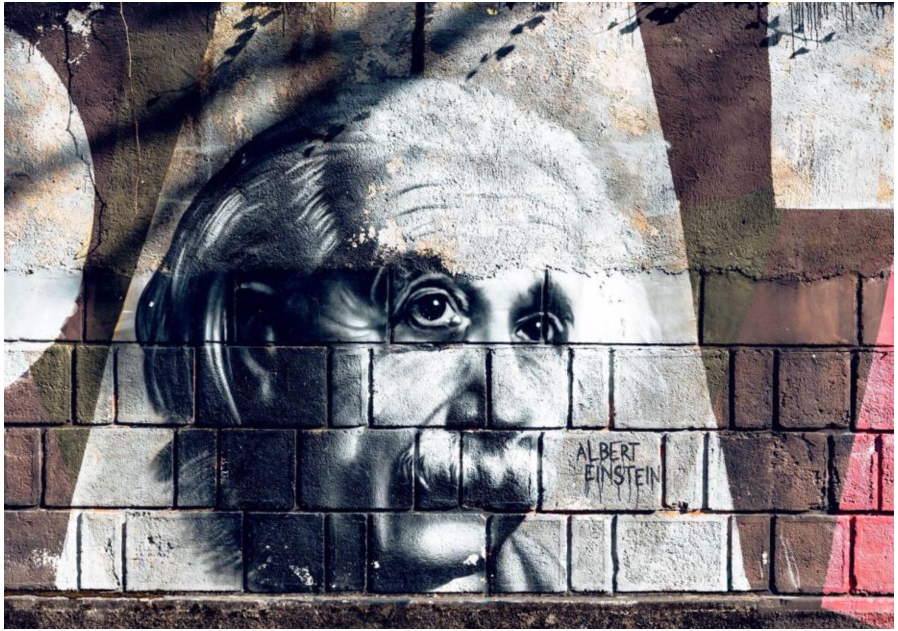
DENIAL OF SERVICE

A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the

ELEVATION OF PRIVLEGE

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

We Need To Step To Our Destiny



“In the midst of every crisis, lies great opportunity.”

Questions?

robert.postill@privay.net

https://www.linkedin.com/in/robertpostill/