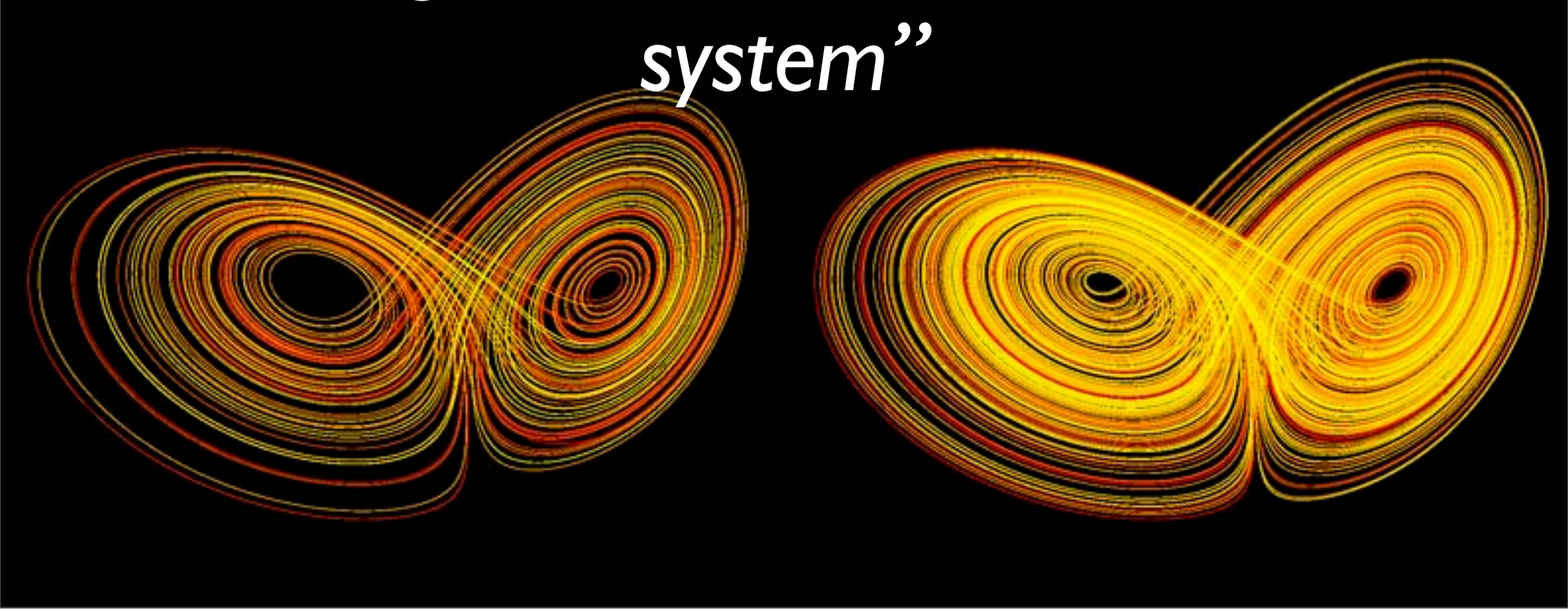
The Security Butterfly Effect

Cat Okita

"Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?"

"Small variations in the initial condition of a system may produce large variations in the long term behaviour of the system"



The Butterfly Effect Is...

Subtle

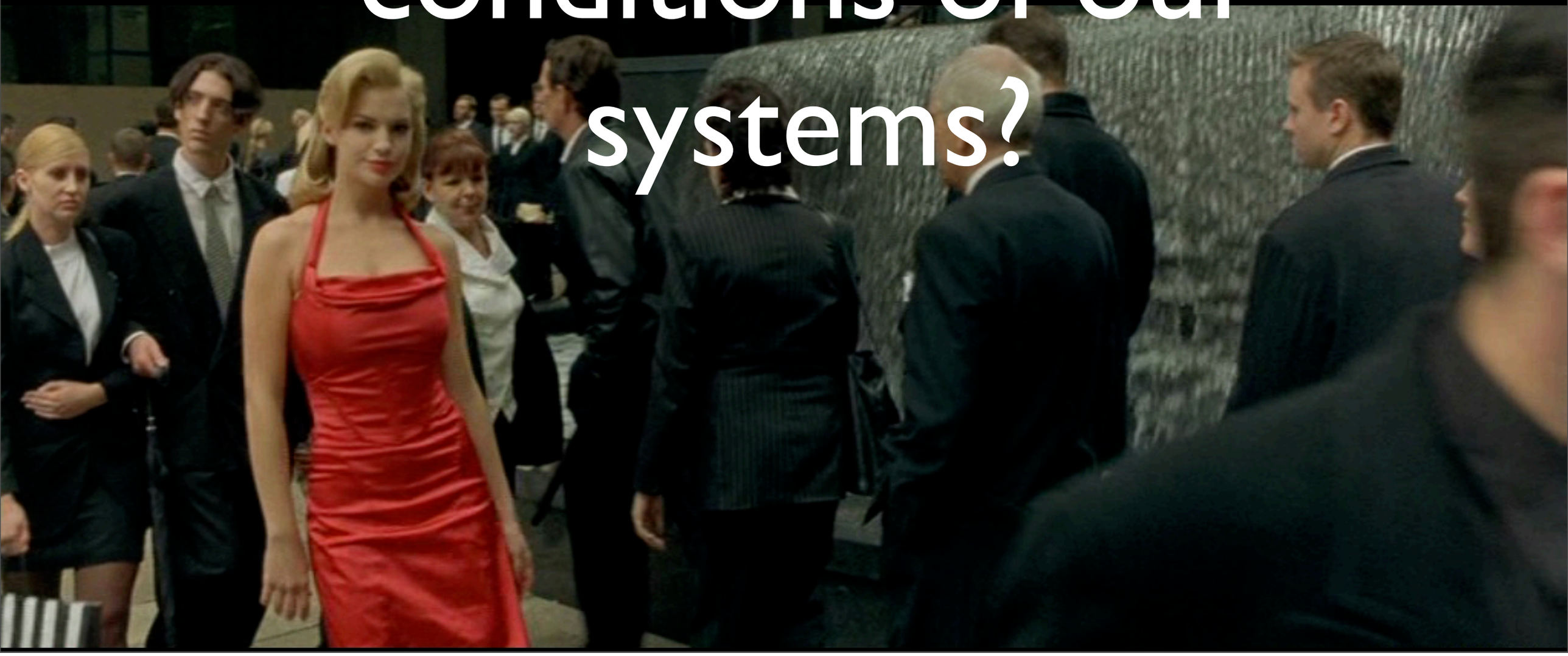
The Butterfly Effect is

Not ...

The Domino Effect

Linear or Cascading

What are the slight variances in the initial conditions of our systems?




One bad assumption
can be fatal

… But …


It’s not that simple

Do we even know the initial conditions of our systems?

Does anybody?

Assumptions

Environment

Behaviour

Blind Spots

Storytime

Disclaimer

THERAC-25

```
PATIENT NAME  : TEST                              A     1
TREATMENT MODE: FIX    BEAM TYPE: X ENERGY (KeV):  25

                                                 ACTUAL          PRESCRIBED
          UNIT RATE/MINUTE                            0             200
          MONITOR UNITS                      50    50            200
          TIME (MIN)                                0.27            1.00

GANTRY ROTATION (DEG)                        0.0             0  VERIFIED
COLLIMATOR ROTATION (DEG)                   359.2           359  VERIFIED
COLLIMATOR X (CM)                            14.2            14.3  VERIFIED
COLLIMATOR Y (CM)                            27.2            27.3  VERIFIED
WEDGE NUMBER                                    1               1  VERIFIED
ACCESSORY NUMBER                                0               0  VERIFIED

DATE  : 84-OCT-26  SYSTEM: BEAM READY   OP.MODE: TREAT   AUTO
TIME  : 12:55. 8   TREAT : TREAT PAUSE           X-RAY     173777
OPR ID: T25VO2-RO3 REASON: OPERATOR     COMMAND:
```

CAST OF CHARACTERS

AECL
Atomic Energy of Canada Ltd, An Atomic Power Company

CGR

A French Company

AECL Engineers & Computer Programmers

The THERAC-25
A (medical) linear accelerator

THERAC-25 Machine

Operators

Medical Physicists

An Assortment of Medical Patients

A Bit Of History

AECL and CGR made medical accelerators together

AECL and CGR called their accelerators the

THERAC-6 and THERAC-20

CGR made the software

AECL made the hardware

AECL and CGR had a falling out

AECL developed a new linear accelerator, the THERAC-25

AECL knew their THERAC-25 was Better than the THERAC-6 and THERAC-20

The THERAC-25 was Smaller and More Powerful

The THERAC-25 used All New Advanced Software

Actually, the THERAC-25 Reused Software from the THECAC-20 and THERAC-6

The THERAC-20 and THERAC-6 used hardware and software controls

The THERAC-25 only used software controls

AECL Engineers and Programmers had to write Special Software to Control the THERAC-25

The Problem

An Assortment of Medical Patients were experiencing Bad Effects after Treatment with the THERAC-25

AECL explained this could not be a problem with the THERAC-25

The THERAC-25 often did Unexpected Things

Medical Patients were underdosed

Medical Patients were overdosed

Sometimes the THERAC-25 produced Strange Errors

Other times the THERAC-25 didn't want to work

AECL explained this could not be happening

Medical Physicists and THERAC-25 Operators were not convinced

Some Medical Patients died

Some Medical Patients experienced radiation overdoses

AECL did not want to hear about THERAC-25 problems

AECL was in disgrace

Finally, AECL agreed to add hardware controls

Assumptions

“SAMY IS MY HERO”

Cast of Characters

MySpace, a social networking site

A concupiscent teenager named Samy Kamkar

A bit of background

Samy was fascinated by the fairer sex

The fairer sex was not fascinated by Samy

Samy wanted to fascinate the fairer sex.

The fairer sex was fascinated by popular people

Popular people on MySpace have lots of friends

Samy wanted to be popular

The Problem

Samy did not have a lot of friends on MySpace

Samy decided to get more friends

Samy needed a lot of friends to be popular on MySpace

Samy took advantage of his friends

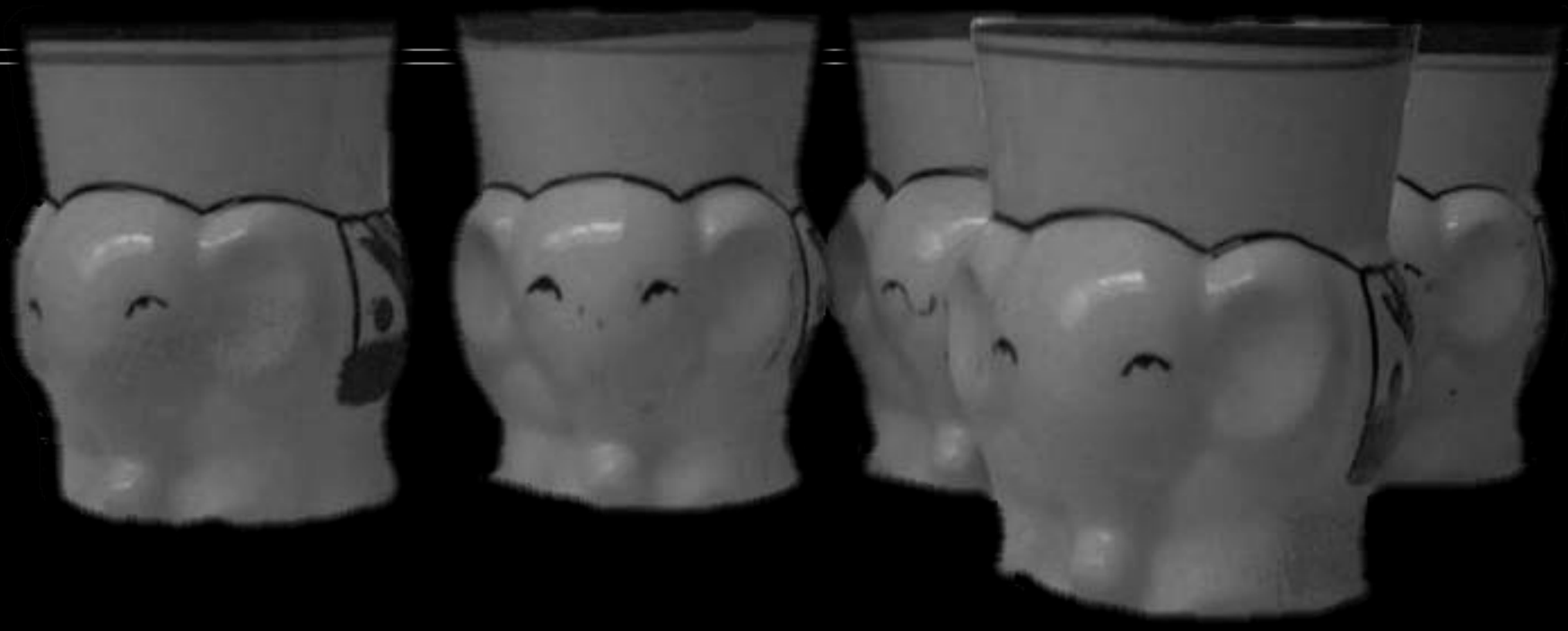
Samy made his friends make their friends his friends

Samy's 'popularity' grew exponentially

MySpace was not amused

Assumptions

HOW TO FIT AN ELEPHANT INTO A TEA CUP



Cast of Characters

Secure Datacenter

World Class

Access Controls

Talented Staff

The Problem

The Secure Datacenter was experiencing Impressive Growth

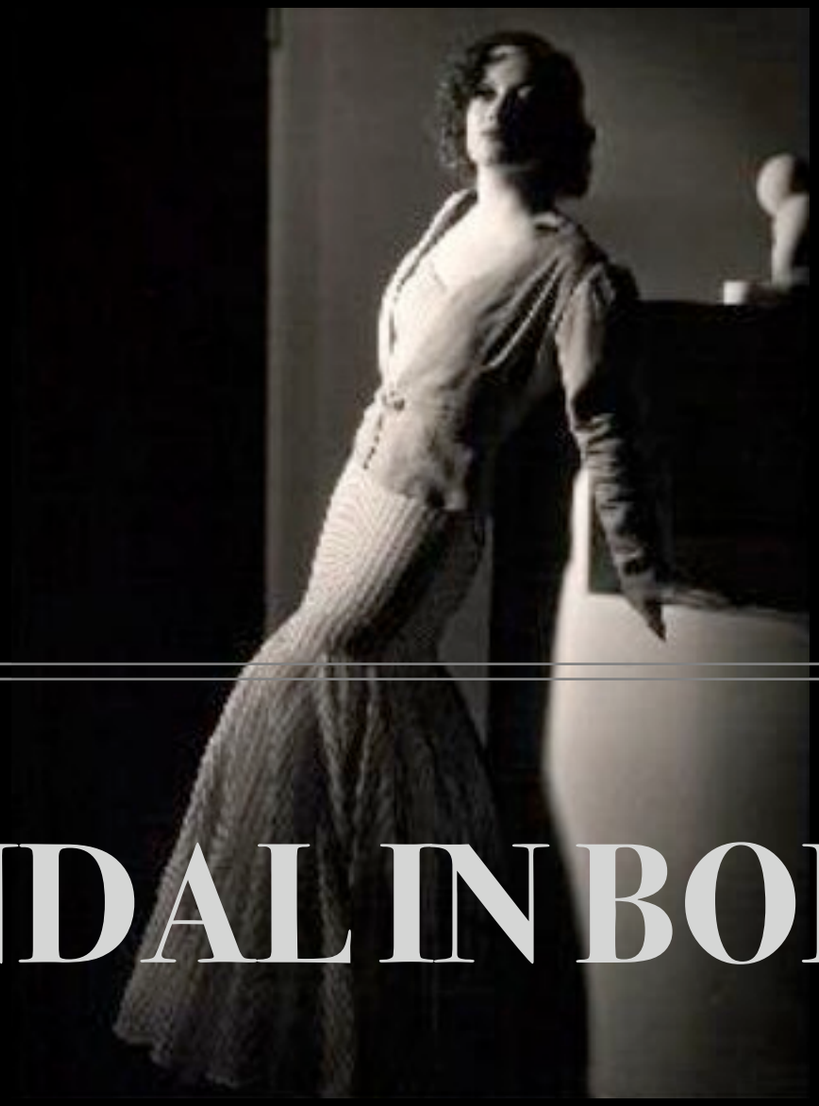
The Talented Staff were constantly visiting the Secure Datacenter at Peculiar Hours

The World Class Access Controls will only admit one person at a time

The World Class Access Controls knew the Talented Staff Member was more than one person.


The Talented Staff Member was beside himself with consternation!

Assumptions



A SCANDAL IN BOHEMIA

Cast of Characters

Paranoid Privacy Enthusiasts

A “Security Researcher” named Dan Egerstad

A Piece of Privacy Enhancing Software called Tor

A Bit of Background

Tor is Privacy Enhancing Software written by Paranoid Privacy Enthusiasts

Tor makes it hard for other people to find where you are on the Internet

Tor also makes it hard for other people to block your traffic to the Internet

... but ...

You need to read the fine print

"First, Tor does not protect you if you do not use it correctly. Read our list of warnings and make sure to follow the instructions for your platform carefully. Second, even if you configure and use Tor correctly, there are still potential attacks that could compromise Tor's ability to protect you. Third, no anonymity system is perfect these days, and Tor is no exception: you should not rely solely on the current Tor network if you really need strong anonymity."

Problem

Dan Egerstad posted details of sensitive email accounts

Paranoid Privacy Enthusiasts were disturbed

Where had Dan found the sensitive account details?

Had Dan Egerstad broken into critical systems?

Was there a dangerous vulnerability in the wild?

No.

It appeared that Dan Egerstad had read the Fine Print

Dan knew that traffic was only encrypted inside Tor

Dan admitted that he had been examining Tor exit traffic

Dan claimed he was performing a public service

Paranoid Privacy Enthusiasts were not amused

Apparently, the Police were not amused either

Assumptions

Fire in the hole!

Cast of Characters

Demanding Users

Helpful Engineers

The Problem

IO was slow

Users could not access their ‘data’

Assumptions

THERE'S NO PLACE LIKE HOME

Cast of Characters

An Unnamed Company

A Virtual Private Network

IT

A Teleworker

The Vendor

Problem

The Teleworker could not connect to the Virtual Private Network

The error message was not helpful.

IT Confirmed that all of the settings were correct.

The Vendor Confirmed that the platform was supported.

Everybody was puzzled.

Further Investigation revealed a File could not be Renamed

Assumptions

THE BURNING ZONE

Cast of Characters

A Shiny New Datacenter

An Important Customer

A Band of Electricians

A Bored Security Guard

An Attention of NOC Staff

A Fire Suppression System

A Bit Of History

A Band of Electricians were Installing Power in A Shiny New Datacenter for an Important Customer

The Datacenter was Secure

The Band of Electricians Must be Watched at All Times

A Bored Security Guard Watched the Band of Electricians

Suddenly there was an Alarming Noise!

The Fire Suppression System had become Perturbed

The Attention of NOC Staff knew A Band of Electricians was in the Shiny New Datacenter

The Attention of NOC Staff could not see Fire (or Smoke) on their Monitors

Sometimes, the Fire Alarm System didn't like Electricians

The Attention of NOC Staff wanted to Investigate Further

Unfortunately, the Fire Suppression System Override did not work

The Fire Suppression System was Incompatible with Breathing

RUN!!!

The Problem

There Was No Fire!

Nobody knew why the Fire Suppression System had become Perturbed

Nobody knew why the Fire Suppression System Override had Failed

The Band of Electricians argued with the Attention of NOC Staff

The Attention of NOC Staff argued with the Important Customer

The Important Customer argued with the Band of Electricians

Everybody was
Unhappy

Finally, some
Information Emerged

The Fire Alarm had been Manually Activated

Assumptions

TEST, BUT VERIFY

Cast of Characters

A Software Company

The Development Team

A Web-based Application

The QA Department

Users

A Bit of History

The Software Company makes a Web-based Application

Somebody told the Software Company that HTTP is Not Secure

The Software Company was Shocked and Dismayed

The Software Company told the Development Team to Make Things Secure

The Development Team Implemented HTTPS

HTTPS is Secure

The QA Team Tested The Web-based Application

The Web-based Application Passed the Tests

The Problem

The Users were Puzzled

The Software Company said the Web-based Application was Secure

The Users Could Not Connect Securely

The Users Complained to the Software Company

The Software Company Complained to the Developers

The Developers Combed through The Code

Everybody knew HTTPS had been Implemented

The Developers Complained that it Worked For Them

QA Displayed the Test Results

Everybody knew the Web-based Application had passed QA

QA Complained about The Users

Nobody knew why The Users were Puzzled

Then, A Developer Examined the Test Suite

Somebody was in Disgrace

The Tests were not Testing what should have been Tested

It appeared that cut and paste had been abused

Assumptions

MONKEY BUSINESS

Cast of Characters

Intrepid University Researchers

Doughty System Administrators

VAX 11/780

A Digital Field Service Engineer

Monkeys

The Problem

The VAX Crashed

... so the System Administrators called A Digital Field Service Engineer to fix the VAX

The System Administrators *did not* call the University Researchers

After all, there was nothing unusual about the VAX.

The Digital Field Service Engineer ran Diagnostics on the VAX

There were Unexpected Consequences!

It seems the VAX had Monkeys not hard drives

Monkeys Crash when you run Diagnostics on them.

Some Monkeys can be recovered

Some Monkeys
experience fatal errors

Assumptions


Future Directions

Specialized Knowledge

Rise of the Machines

Questions?