The Immortal Retrofuturism of Mainframe Computers

and how to keep them safe!

Who am I?

Michelle Eggers

Security Consultant @ NetSPI

- Mainframe, Web App, Network Penetration Testing
- Background in accounting/finance and project mgmt
- Passionate about legacy tech security

Overview

1. History Debrief
2. Mainframes Today
3. Modern Threats
4. Tips to Secure

What is Mainframe??

- They are computers!
- More specifically, they are high-performance computer systems with immense processing and storage power that have unique operating systems, like z/OS or Linux on IBM Z.

Myth vs. Fact

Myth: Mainframe is Outdated

Mainframes continuously evolve and were among the earliest systems to adopt virtualization and built-in encryption

Myth: Cloud Replaces Mainframe

Regulatory compliance, barriers to transition.

Hybridization is more likely! ELT approach is developing to load mainframe data into lakes for analysis

Myth: It's too specialized!

Changes underway to make mainframes more accessible. WatsonX AI Code Assist for translation of COBOL to Java and initiatives to enlist early career professionals.

A Brief History!

1937

US Navy Bureau of Ships

- Pre-mainframe technologies in use: Analog computers, mechanical calculators, electrical tabulating machines

- Used for gunnery calcs, navigation, and engineering tasks

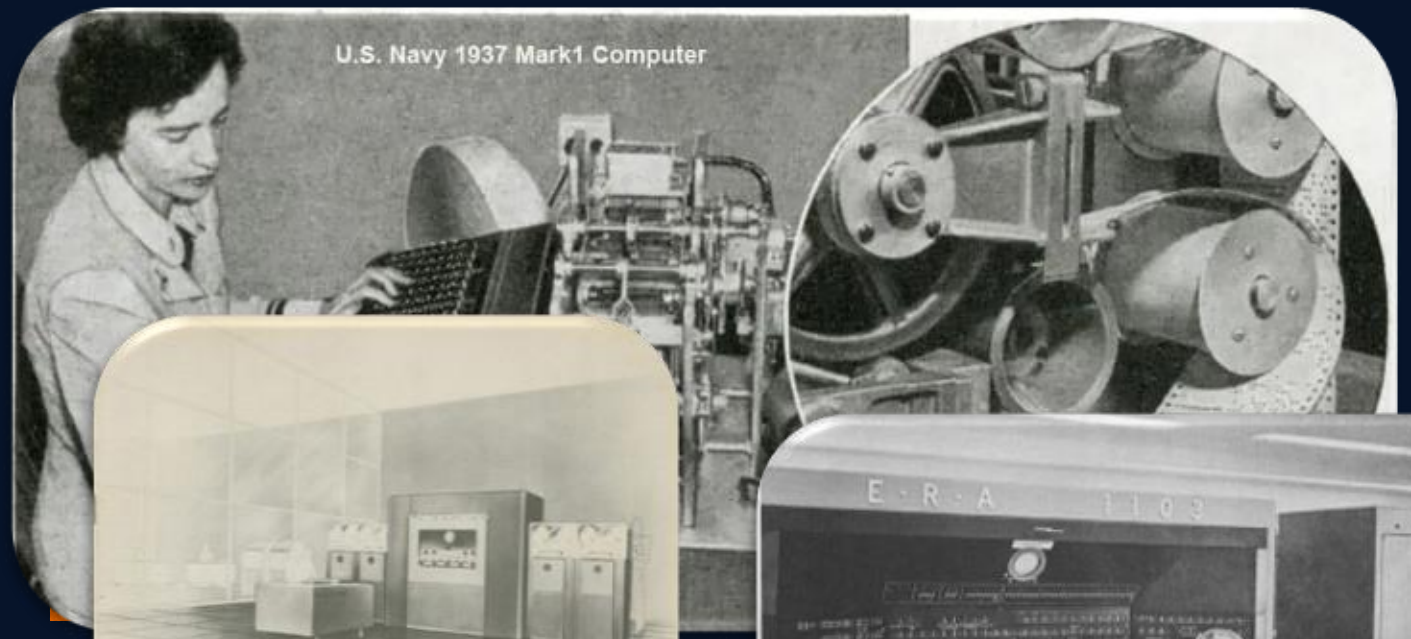
1951

Eckert-Mauchly Computer Corp

- Commercialization Occurs

- UNIVAC created to process census data

- Magnetic tape, faster than punch cards

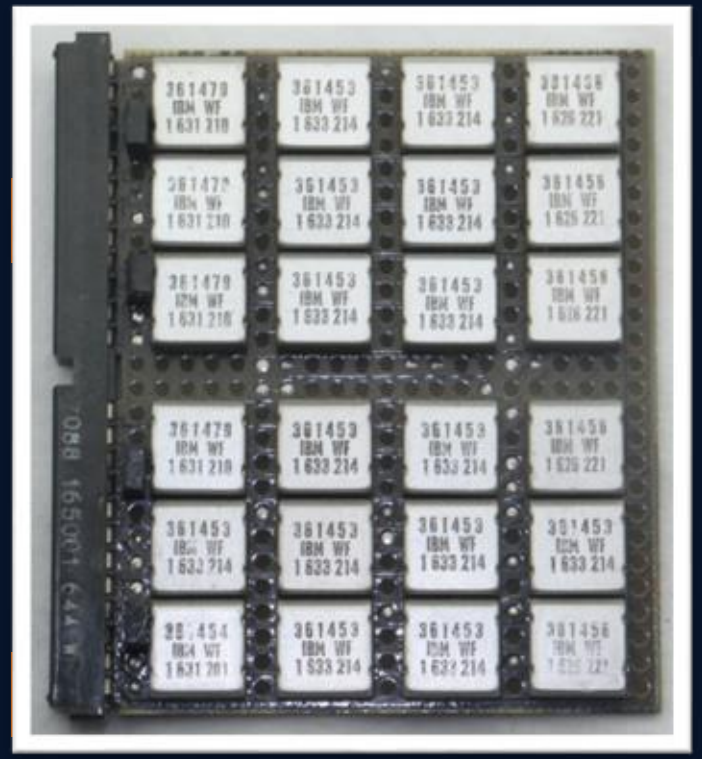


Time Marches On!

1965

IBM

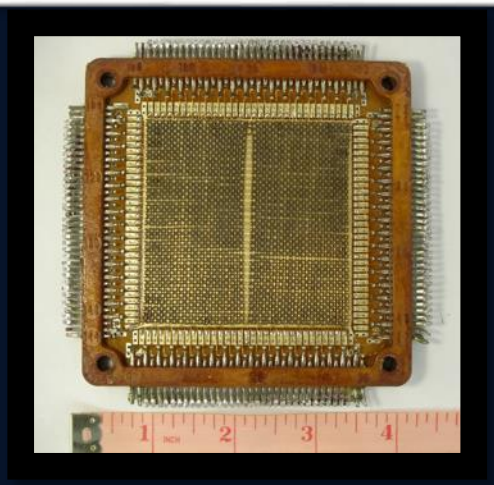
- Modern IBM Z System/360 released with unified architecture
- First computers designed to cover a complete range of applications, unified architecture
- Solid state tech replaced vacuum tubes

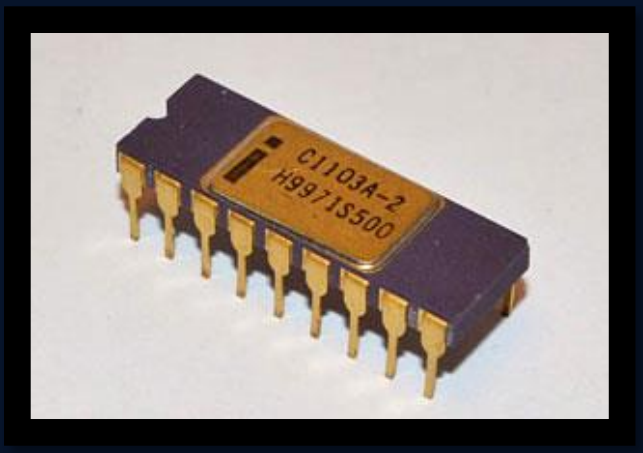


1970

Innovation Continues!

- Magnetic ferrite cores were replaced by silicon DRAM memory chips
- Virtual memory introduced
- Dynamic address translation





The Saga Continues!

1991

Death Announcement

- Mainframes were publicly stated to have only a few more years of relevance

- "I predict that the last mainframe will be unplugged on March 15, 1996.“ Stewart Alsop

2024

The Future is Now

- Mainframe is STILL IN USE by finance, healthcare, government, and aviation industries

- New developments include implementing AI to improve real-time fraud detection capabilities

Amazing Mainframe

Five nines of reliability!
Less than 5.36 minutes of downtime!

- Reliability

  - Built-in redundancy across various hardware levels (I/O paths, power supply, memory, processors)
  - Error detection/correction of data corruption.
  - Can handle up to 7 magnitude earthquakes!

- Availability

  - Transaction rollback
  - Checkpoint restart
  - Complex job scheduling
  - z15 offers 190 configurable cores = finely tuned; “bespoke”

- Serviceability

  - Modular by design
  - In-depth logging – problem solving that much easier
  - Onsite, accessible for repair and maintenance
  - Tightly controlled access

Environmental Threats

Expanded attack surface = more potential vulnerabilities

TJX Companies Data Breach (*2005-2007*)

- Payment card data breach
- Exposed 45.7 million credit/debit card number
- Weakness in wireless network used to pivot into mainframe

Heartland Payment Systems (*2008-2009*)

- 100 million cards compromised
- Global cyber fraud operation
- Combined attack of network and application vulnerabilities that the attackers exploited to access data stored on the mainframe

Equifax Data Breach (*2017*)

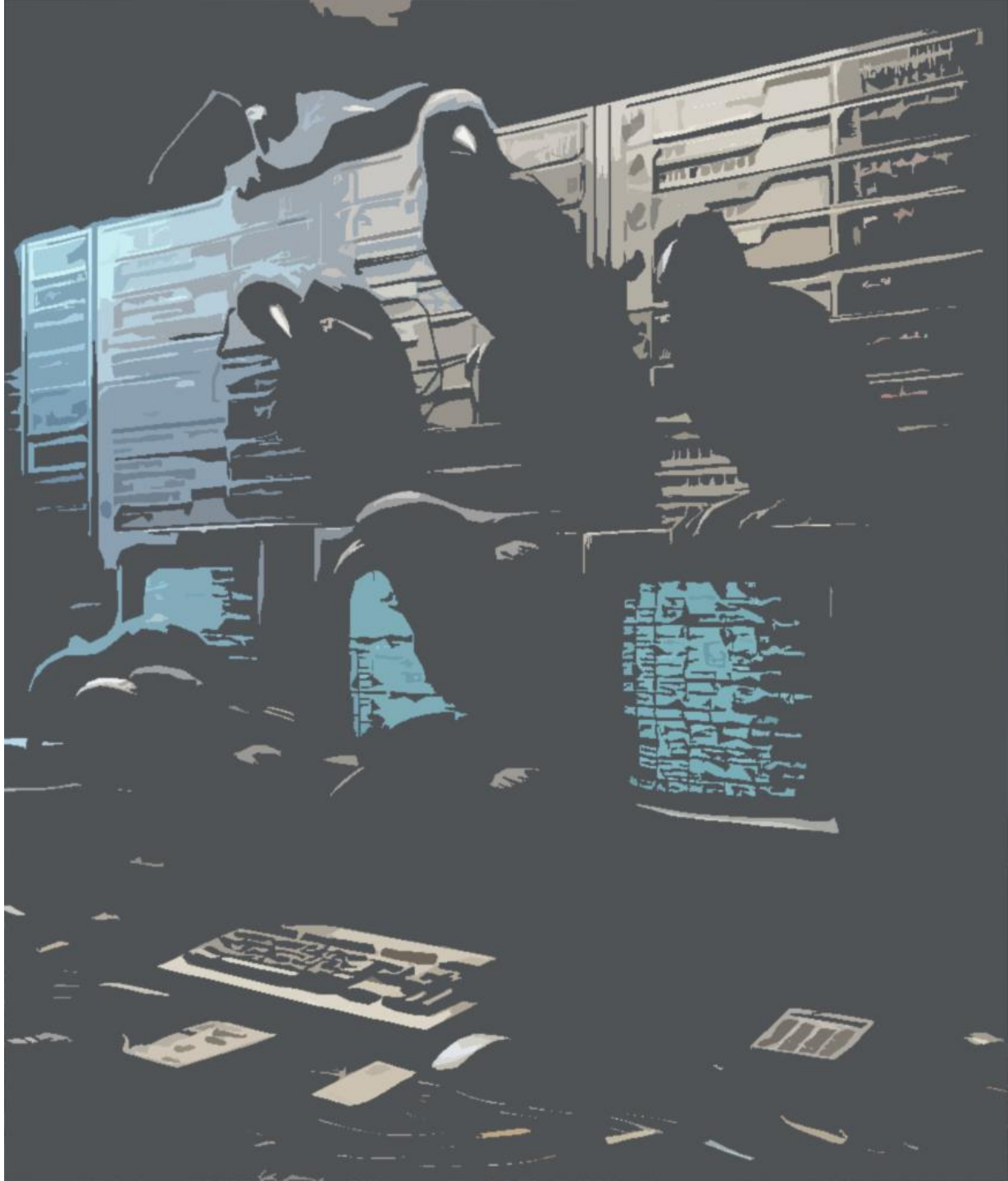
- Private data of 147 million users exposed
- Web application provided the initial access

Environmental Threats

Small Mistakes, Big Problems

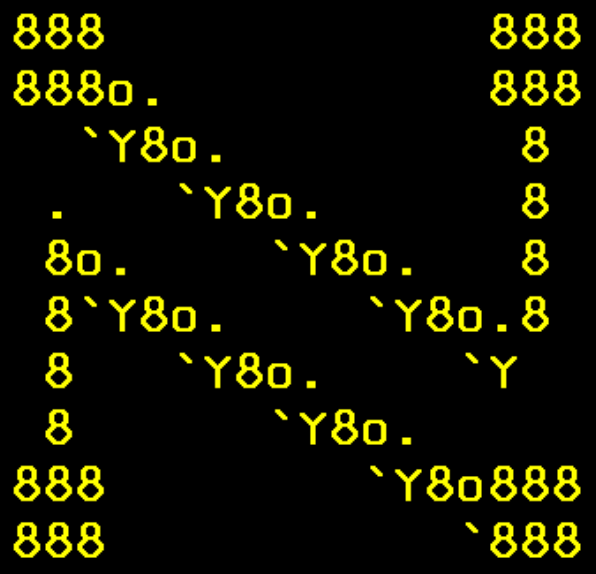
Logica Data Breach (*2012*)

- Swedish data breach that dramatically changed how the federal government viewed mainframe security
- The entire investigation was made public
- What happened?
    - Initial access via insecure FTP network connection
    - Likely, hackers used Hercules (mainframe emulator) to run z/OS and download files and tax-processing source code from the Logica servers
    - Attack included 0-day vulnerabilities that leveraged default configurations and sysadmin command execution
    - 120k Usernames were stolen from RACF and corresponding passwords cracked using John the Ripper
    - Funds were also stolen from banking institutions by the primary hacker, based in Cambodia



Next up: Simulated real-world attack

- Authentication to the logical partition (LPAR)
- Endpoints have already been enumerated in this walkthrough
- Access is restricted for low-level users to specific resources
- Is there another way to access?



```
888b     888
8888b    888                888      .d8888b.  8888888b. 8888888 tm
8SoF8b   888                888     d88P  Y88b 888   Y88b  888
888Y88b  888                88888888 Y88b.      888    888  888
888 Y88b 888  .d888b.       888      "Y888b.   888   d88P  888
888  Y88b888 d8P   Y8b      888          "Y88b. 8888888P"   888
888   Y88888 888888888      888            "888 888         888
888    Y8888 Y8b.    .      Y88b.  Y88b  d88P 888         888
888     Y888  "Y8888P        "Y888  "Y8888P"  888       8888888
```

Welcome to the NetSPI development mainframe. Type 'TSO' to access TSO:

Internal Threats

Broken Access Control

Local file include of datasets/unix files

Insecure file transfer protocols (e.g. FTP)

Unauthenticated access

Injections

SQL injection in DB2 databases

Job Control Language injections

Rexx scripts injection

Security Misconfigurations

Default credentials

Weak password policies

NOT using an external security manager (ESM) like RACF, Top Secret, or ACF2 to control user access

Ways to Secure

Secure with Network Controls

Properly configure your network topology as a whole

Make appropriate use of logical partitions, regions, and ESM tools

Disallow unencrypted protocols and keep up with patches/updates

Secure with Compliance

Implement CIS benchmarking, secure configuration guidelines

Follow DISA STIGS, DoD guides derived from NIST 800-53

Secure with Ongoing Reviews

Monitor traffic with a SOC; logs are robust, take advantage!

Audit identity and access management on a regular basis and implement MFA

Establish recurring audits for all features and conduct frequent penetration testing both internally and through third-parties

Summary

- ✓ Mainframe is not going away anytime soon!
- ✓ We rely on it globally to support finance, healthcare, government, and other critical industries.
- ✓ There are more possible vulnerabilities now due to increasing integrations.
- ✓ With diligence, we can combat these threats together.

When I figure out my dads computer password:

Thank You!

Please stay connected (:

Michelle Eggers

Security Consultant @ NetSPI

Mainframe, Web Application, Network Penetration Testing

michelle.eggers@netspi.com

@saltymiche