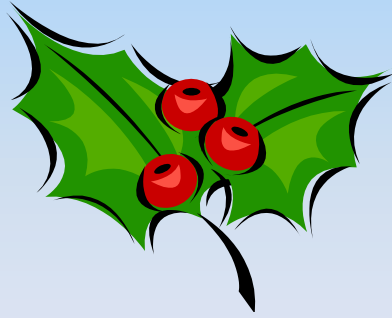
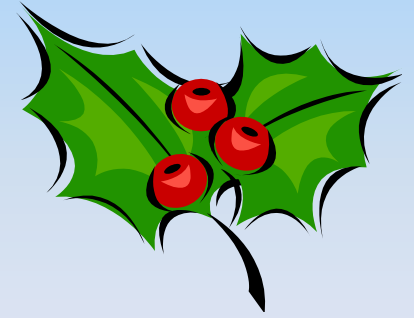


# Mainframe Computing Security Myths



Fact or Fiction?



millennia...

Julie-Ann Williams  
[julie@sysprog.co.uk](mailto:julie@sysprog.co.uk)

# agenda

## Introductions

Host: Julie-Ann Williams, Mainframe Security Specialist

25 anniversary of the infamous 3270 mainframe hacking

IBM XMASCARD EXEC

RACF, ACF2 & Top Secret

Top 10 Security Exposures within a z/OS environment

Q & A Session

# who am I?

MVS Systems Programmer

Special interest in security

aka Hacker

only do White Hat work

Appeared in several series of Robot Wars!

won Sportsmanship Trophy

working alongside my Brother



millennia...

# agenda

## FICTION:

The mainframe is dead

Mainframes only run legacy applications

System z is delivered with B2 levels of security

System z is the most secure, 24x7 platform available

Mainframes are expensive

Mainframes can only be run by old people



# agenda

## FACT:

We have never come across a mainframe that we couldn't hack!



# the mainframe is dead

## Rumours of the platform's demise

3 decades of lack of focus on mainframe because of a rumour!

## Increased market share

Not all "classic" workloads

Linux on z

zEC12



# the mainframe is dead

## The new zEC12



Proven hybrid computing design  
able to manage workloads on  
multiple platforms

5.5 GHz processors deliver  
increased performance

Cross platform virtualization

Help address server sprawl

Cutting edge, pattern recognition  
analytics

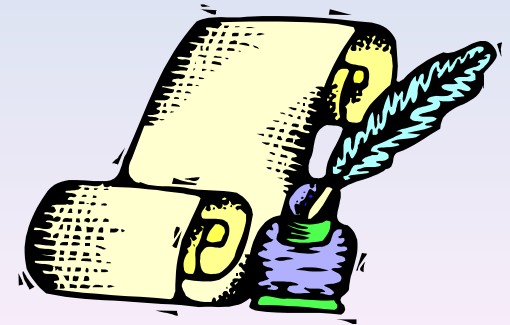
Smarter computing



# mainframes only run legacy applications

**From Wikipedia:** a term for out-of-date hardware and/or software still in use.

**From the OED:** a sum of money, or a specified article, given to another by will.  
a tangible or intangible thing handed down by a predecessor.  
a long-lasting effect of an event or process.  
give or leave as a legacy.





# system z is delivered with B2 levels of security

## Top 10 Findings...

- 1) Not all resources are protected
- 2) Many data set rules offer insufficient protection
- 3) Organisation using USS but without defining any security
- 4) Unprotected APF libraries
- 5) Access control repository not adequately protected



# system z is the most secure, 24x7 platform available

## Top 10 Findings continued...

- 6) Many users have higher levels of administration rights than they need
- 7) Many users are inactive (typically a problem when greater than 20%)
- 8) Over reliance on defaults
- 9) Only one production batch id and it has too much access
- 10) Little or no security event reporting



# mainframes are expensive

## Initial outlay vs TCO

**The Register**<sup>®</sup>

IBM warns mainframe shops of 2013 price hike 10 per cent jump coming next July for flat-priced wares  
When your customers pay millions of dollars for your machines and then spend many tens to hundreds of thousands of dollars per month – and sometimes much more – on monthly license fees for your software, you can't just spring a price increase on them one day. You have to give fair warning so they can budget for the price increase. IBM has always been good about these things, and generally gives customers the heads up on software or maintenance price hikes. But with the uncertainty of the global economy and with the System z mainframe currently in transition from to a new set of processors, Big Blue is giving its mainframe shops a little more warning that a price increase is coming by next summer.

True

False



# mainframes are expensive

Typical scenario for increased and decreased numbers of VMs on x86 and zCloud...

\* Published WWW pricing  
2012-05-28

		zCloud	x86	Typical Public Clouds*	
z114	100 VMs	£148.21	£ 112.50		
	250 VMs	£81.18	£ 89.39		
	400 VMs	£62.35	£ 73.99		
				£ 97.09	£ 89.90
z196	400 VMs	£66.76	£ 68.36		
	1600 VMs	£40.33	£ 65.23		
	3200 VMs	£35.54	£ 65.23		



# mainframes are expensive

## Sample Oracle Deployment

Model	Size of Config	Number of IFL's	Enterprise Linux Servers	With Service Management setup	x86 Cores non virtualised	X86 Cores Virtualised	Oracle Non-virtualised	Oracle virtualised	Oracle on Linux for z
z114	small	2	£143,037	£166,893	80	16	£2,000,000	£400,000	£50,000
	medium	6	£260,177	£328,167	240	48	£6,000,000	£1,200,000	£150,000
	large	10	£358,731	£463,697	400	80	£10,000,000	£2,000,000	£250,000
z196	expandable	6	£448,000	£515,990	300	72	£7,500,000	£1,800,000	£150,000
	supersized	32	£1,600,000	£1,823,054	1600	384	£40,000,000	£9,600,000	£800,000

N.B – All IBM Pricing is subject to Special Bid and is **purely** for indicative purposes  
N.B – Oracle cost are assumed to be £25K per core



# mainframes can only be run by old people

IBM Academic Initiative

University of Canberra

GSE UK Conference

101 Sessions in all streams

Students invited

Our real legacy must be to make sure System z runs for another 50 years



# we've never met a mainframe we couldn't hack!

Frightening but TRUE!

Major Financials

Small Specialists

ISVs

Manufacturing

Retail

Governments

Military



# recent news...

## Swedish Central Administration

IBM mainframes outsourced to Logica (now renamed CGI)

Elevated Access due, in part, to weak password rules

- Did **NOT** use full capabilities of RACF

**Failure:** Massive data loss including multiple “Confidential” databases

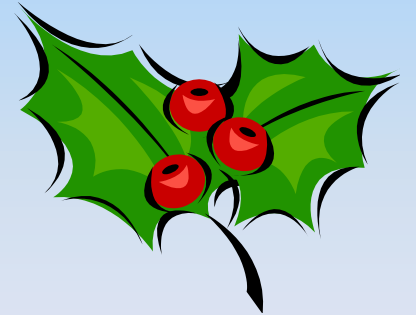
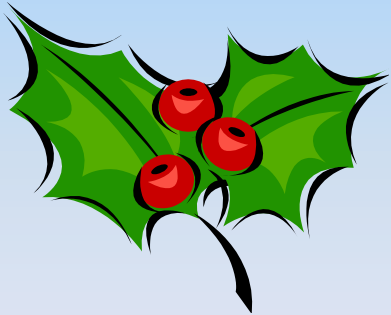
Problem not inherently caused by using a mainframe

- Security is security whatever the platform
- Implement appropriate levels of security
- Make sure current technology is applied frequently
- No platform running critical apps or hosting confidential data can be outside of scope

Ensure you know that your outsourcer’s approach to security includes mainframe!



q&a



# thank you for listening



My contact details in case you think of any questions after the event: Email: [julie@sysprog.co.uk](mailto:julie@sysprog.co.uk)

Mobile: 07770 415102