(ISC)2 Twin Cities Area Chapter
2013 Annual Meeting
18 June 2013, 14.00 - 16.00

Cloud Security

Matthew J. Harmon
Security Researcher and Consultant
IT Risk Limited, LLC
CISSP, GSEC, GCIH

Hello!

- Matthew J. Harmon - 20 years of Information Security and 13 years of Virtualization experience
- Owner and Security Consultant for IT Risk Limited
- SANS Institute Mentor & Community Instructor
  SEC 401 - Security Essentials Bootcamp
  SEC 504 - Incident Handling, Exploits and Hacking Techniques
  SEC 464 - Hacker Guard for Systems Administrators
- Upper Midwest Security Alliance (UMSA) Board of Directors and Education Sub-Committee Co-Chair

Why we are here today.

- Raise awareness of the risks and benefits involved with "Cloud Computing" otherwise known as outsourced computing, third party services and third party database hosting
- We're talking about "Virtualization"
- These used to be called Mainframes

What we are going to talk about...

- Virtualization basics and types of virtualization
- Overview of Cloud Computing Benefits
- Details of Cloud Computing Risks

...and what not.

- This is not a complete course in Cloud Security, for that take Dave Shackleford's excellent six day class SANS SEC 579 named:
  "Virtualization and Private Cloud Security"
  https://www.sans.org/course/virtualization-private-cloud-security

- or... Dave Shackleford's two day fundamentals class, SANS SEC 542 named:
  "Cloud Security Fundamentals"
  https://www.sans.org/course/cloud-security-fundamentals

- or... Study for the Cloud Security Alliance's CCSK
  "Certificate of Cloud Security Knowledge"
  https://cloudsecurityalliance.org/education/ccsk/

Cloud Security Alliance's CCSK "Certificate of Cloud Security Knowledge"

- 15 Domains
- Cloud Architecture, Governance and Enterprise Risk, Legal and Electronic Discovery, Compliance and Audit, Information Lifecycle Management, Portability and Interoperability
- Traditional Security, Business Continuity and Disaster Recovery, Data Center Operations, Incident Response, Application Security, Encryption and Key Management, Identity and Access Management, Virtualization and Security-as-a-Service

https://cloudsecurityalliance.org/education/ccsk/

Terms and Definitions

- **Hypervisor:**
  A piece of computer software, firmware or hardware that runs virtual machines
    - Type 1: Native or Bare Metal
    - Type 2: Hosted or running within another OS

- **Guest:**
  A virtual machine running on top of a hypervisor

Reference: Gerald J. Popek and Robert P. Goldberg (1974).
"Formal Requirements for Virtualizable Third Generation Architectures". Communications of the ACM 17

Terms and Definition Reminder

- **Threat (or threat agent):**
  Anything that is capable of acting against an asset in a manner that can result in harm. [FAIR]
  The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. [NIATEC]
  A threat agent has Capability, Intent and History [OWASP]

- **Vulnerability:**
  A weakness that could be exploited by a threat. The presence of a vulnerability does not in itself cause harm. [NIATEC]

National Information Assurance Training and Education Center (NIATEC) niatec.info
Factor Analysis of Information Risk (FAIR) fairwiki.riskmanagementinsight.com
Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Category:Threat_Agent

Virtualization Basics

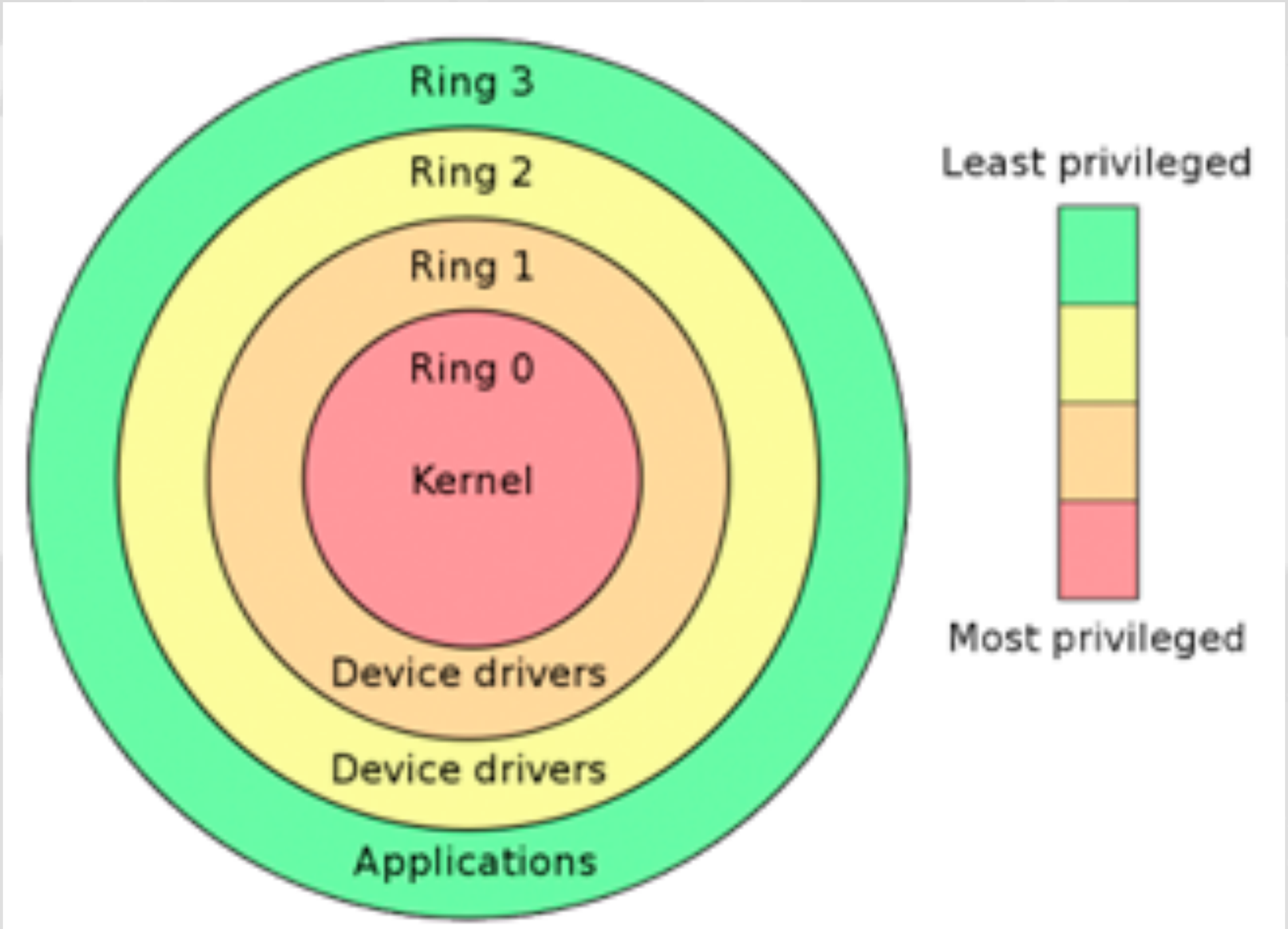


Image Credit: Miguel Santos Ribeiro, 2009

Virtualization Basics

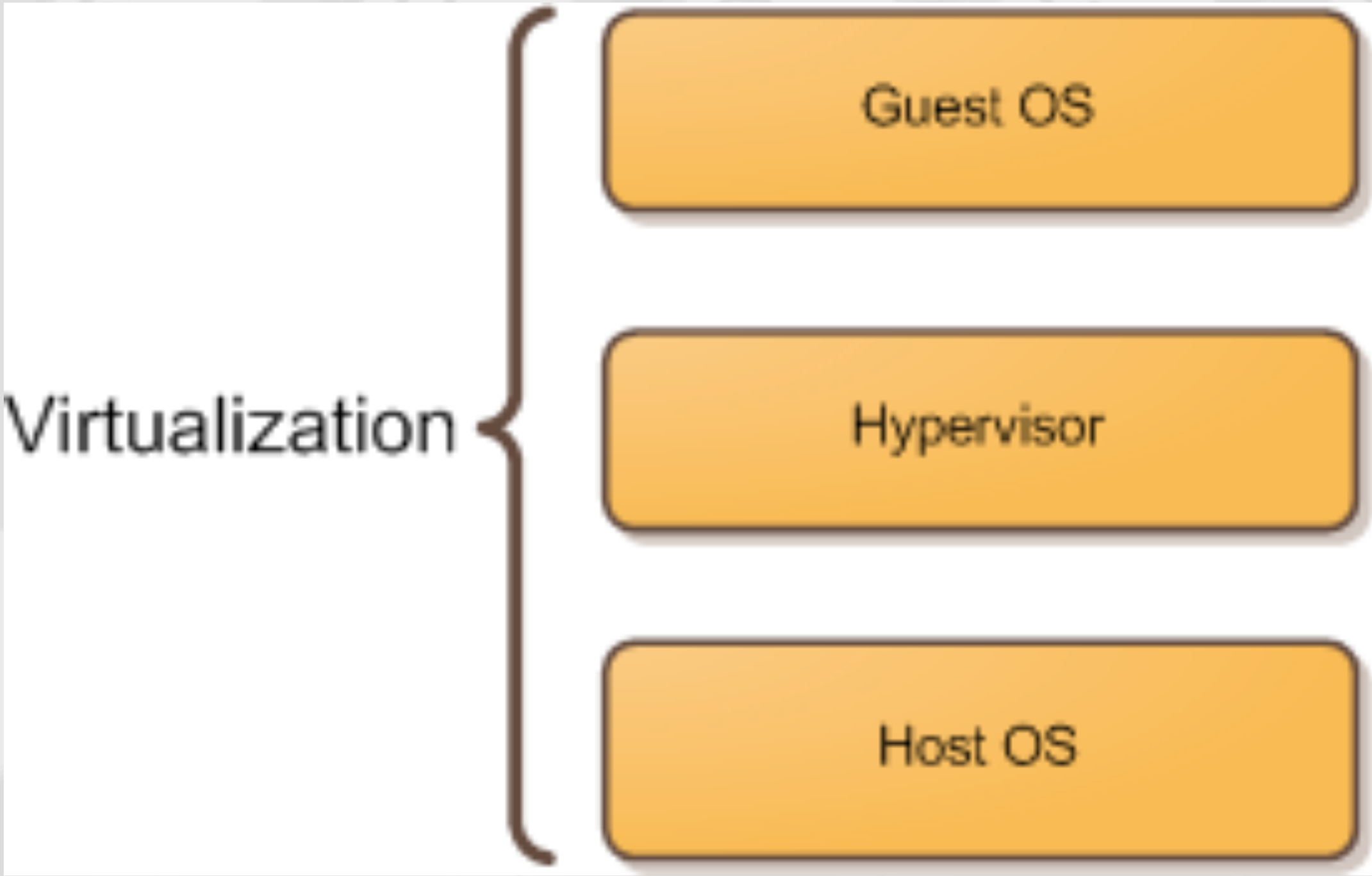
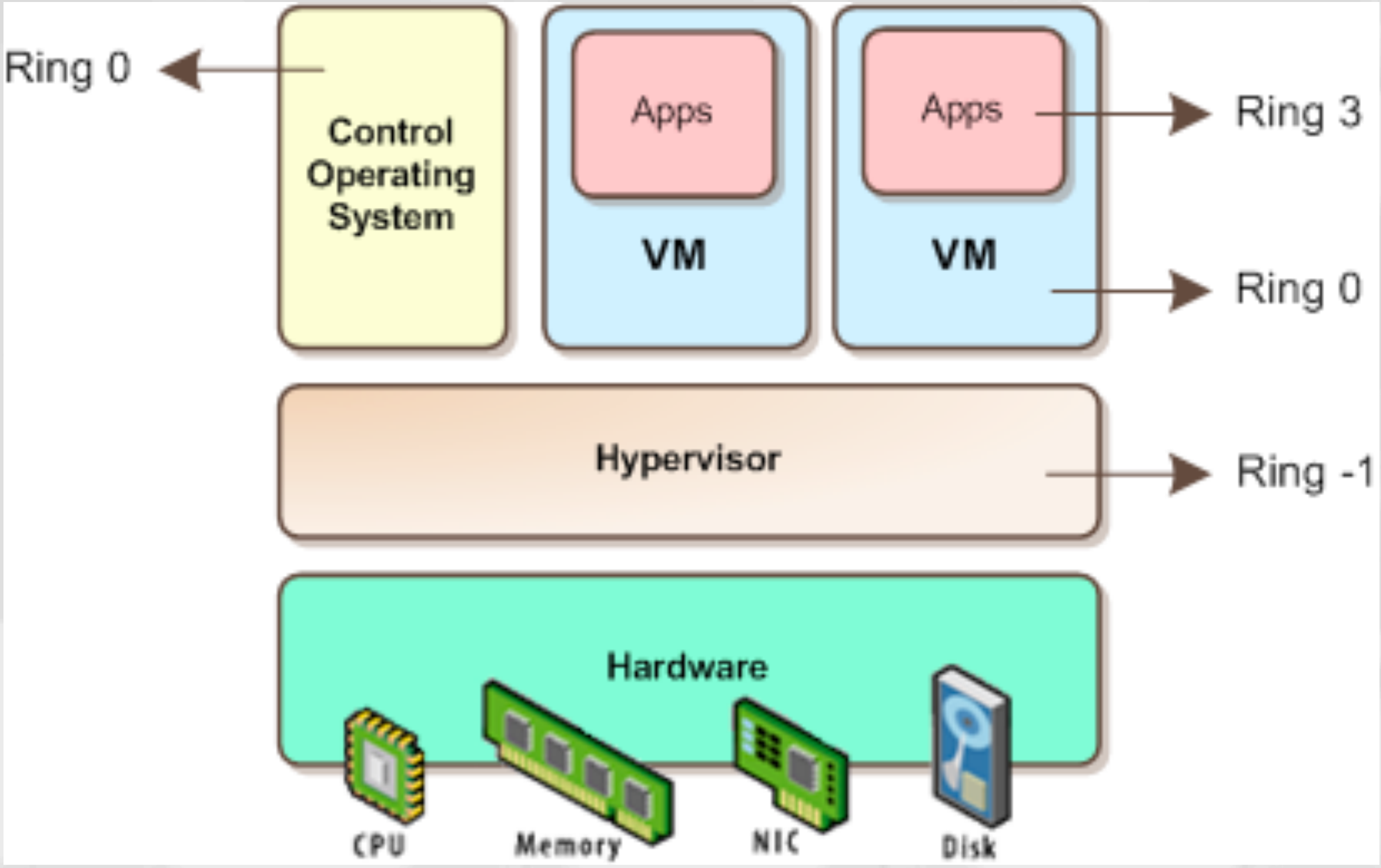


Image Credit: Miguel Santos Ribeiro, 2009

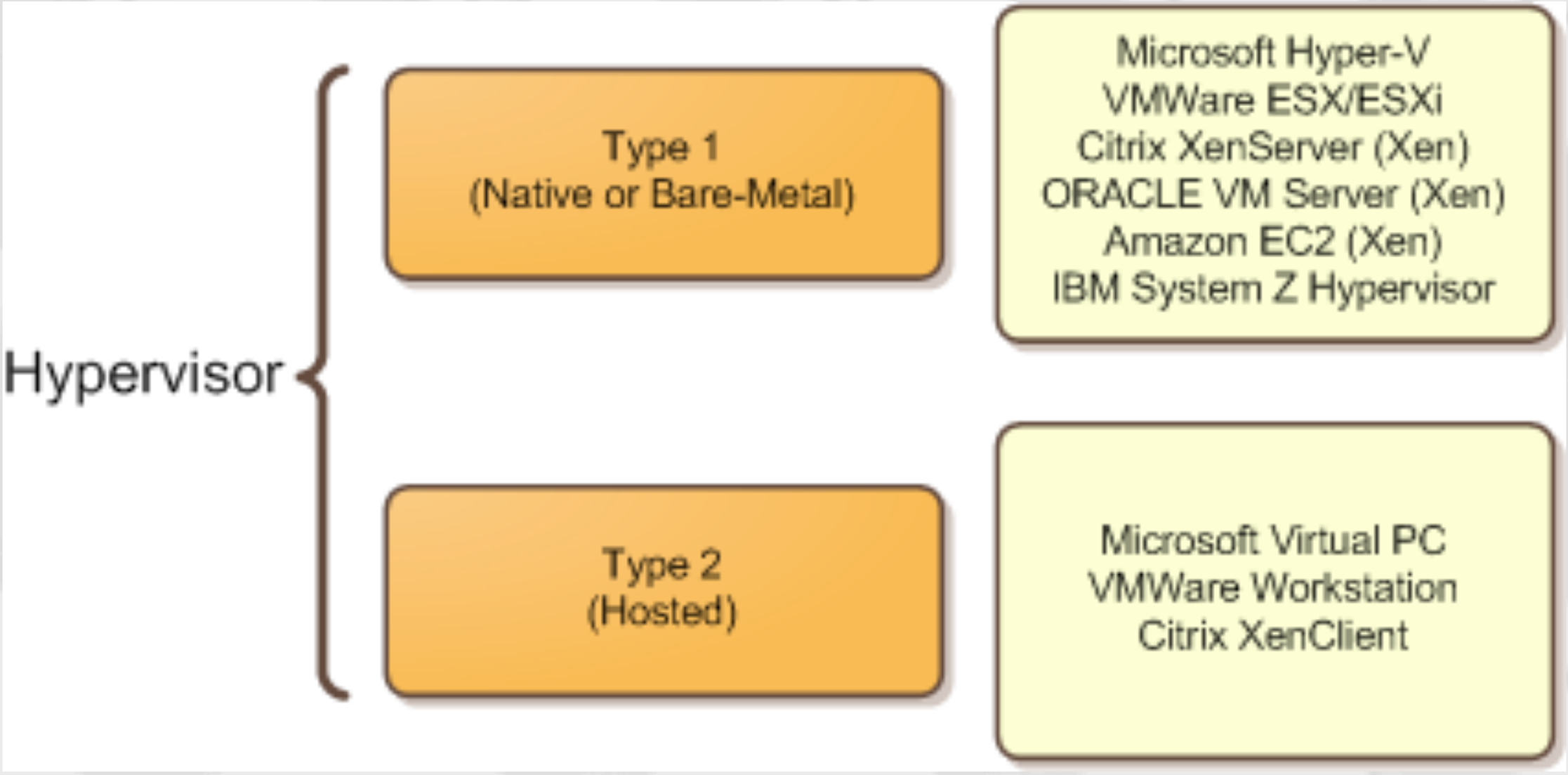
Virtualization Basics



Type 1 - Full Virtualization with Hardware/Processor Acceleration (VT-x, etc.)

Image Credit: Miguel Santos Ribeiro, 2009

Virtualization Basics



Big players are Microsoft, VMWare, Xen, Citrix and OpenStack

Image Credit: Miguel Santos Ribeiro, 2009

Benefits of Virtualization

- Server consolidation
  - Old 1U hardware reaching End-of-Life? Consolidate.
  - Better use of data center rack space, 20 blades in the same space as a single 3U rack mount server

Benefits of Cloud Computing

- Software as a Service
  - Auto-patching, silent upgrades, flexibility
- Infrastructure as a Service
  - Reduced operational overhead and issues become “somebody elses problem”
  - What you need, when you need it, as you need it with the option of rapid build outs and rapid decom
- [anything] as a Service
  - Easier requisition process, buying a service in most organizations is easier than buying and deploying hardware

Benefits of Cloud Computing

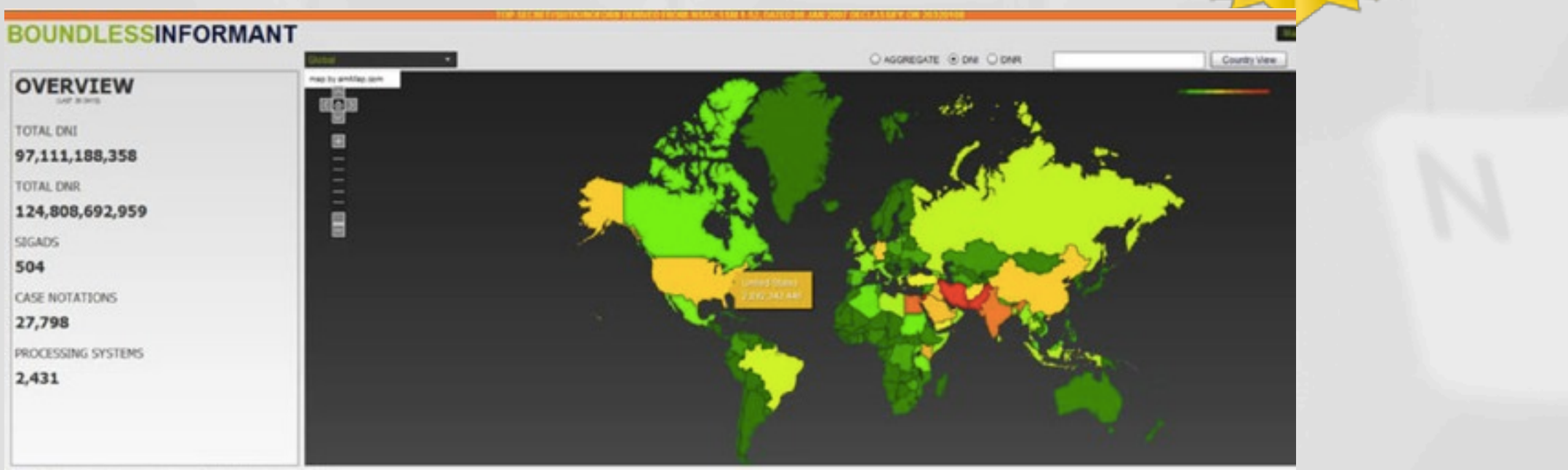
- Shims
  - Xlyrvisor (?)
  - McAfee Move AV
  - TrendMicro (Amazon)
- Encryption as a Service
  - Cipher Cloud
  - Perspecsys

Cloud Security Risks

If you're not paying (a premium) for a product,
you're the product that is being sold.

- Confidentiality and Privacy
  - Multi-tenant (low cost) systems co-mingle data from multiple customers
  - Few (no?) cloud providers encrypt your data
- Availability
  - Terms of Service violation? Data is locked away.
  - Internet access go down? No access to your data.
- Integrity
  - Lack of visibility into cloud provider operations
  - Insider threat at cloud vendor

Cloud Security Risks



I'm not saying what they are doing is against the law, I just think it's just a bit creepy that it isn't.

Cloud Security Risks

Threats played out in the media recently.

- Intel Corporation's Threat Agent Library References
  - Civil Activist, Data Miner, Sensationalist
  - Employee Disgruntled, Government Cyberwarrior
  - Radical Activist, (Possibly) Corrupt Government Officials
- Assume worst case scenarios
  - Who here has been or is a systems administrator?
  - What access did you have? Root? Domain Admin? Physical?

Privacy as Standard Operating Procedure

- Worst case scenarios, coming true:
  - What is being collected from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL and Apple?
  - E-Mail, Chat (Video and Voice), Videos, Photos, Stored Data, VoIP Interception, File Transfers, Video Conferencing, Notifications of Activity (Login, Logout), Online Social Networking details and other "Special Requests"
- Not too long ago these were called "paranoid fantasies"
  - Today they are reality being featured in the popular media

Privacy as Standard Operating Procedure

- Control your data
  - Encrypt end-to-end (in transit, during processing, and at rest)
  - Encryption at rest is a good first step
- Audit your vendors and third parties
  - Don’t be afraid to walk away if they don’t meet your requirements
  - Clearly state your needs and desires in your contract
  - Trust - but verify
  - Be careful with any personal data or regulated data such as the now viral HIPAA or PCI.

Final comments

"The Cloud" or Virtualization, gives us many opportunities to harvest significant processing power at a low cost.

However there are trade offs, your data is being hosted with someone else and you lose control of that data.

Do not assume that your price point includes any privacy of your data and frequently security is an afterthought for vendors.

You can transfer a lot of risk, but you cannot transfer the impact of a customer data breach.

IT Risk Limited, LLC

matthew@itriskltd.com
@mjharmon
+1 612.987.0115

IT Risk Ltd. performs IT risk assessments, advanced security testing, incident response, IT Security Training, forensics, International Standards Development and security team building

Thank you!

Questions?

I hope you enjoyed this presentation, it can be downloaded from:

https://github.com/itriskltd