Panel on Cloud Services

Security and Safety in Cloud-based Systems and Services

Moderator
Dr Bob Duncan
Business School/Computing Science/Geology & Petroleum Geology
University of Aberdeen
Aberdeen, UK
Email: bobduncan@abdn.ac.uk

Special Track on Finding A Solution To – Cloud Forensic Problem
Cloud Computing 2018
19 – 20 February, Barcelona, Spain

1495 UNIVERSITY OF ABERDEEN BUSINESS SCHOOL

Panel on Cloud Services

Security and Safety in Cloud-based Systems and Services

Dr Bob Duncan has a background in accounting, with many decades of experience in industry, and has watched the development and implementation of IT systems over the decades. With a recent MA (Hons) in Computing and a PhD in Computing Science, specialising in Cloud Security, he has an avid interest in Cloud Cyber Security. He is particularly interested in Cloud systems from a security perspective, due to the possible opportunities offered by the flexibility of cloud systems, but is concernned as to how easy it is for corporates to lose sight of the security implications for their business. This is particularly problematic with the development of modern legislation and regulation concerning matters of data protection, and in particular, the forthcoming EU General Data Protection Regulation.

Moderator
Dr Bob Duncan

Special Track on Finding A Solution To – Cloud Forensic Problem
Cloud Computing 2018
19 – 20 February, Barcelona, Spain

Panel on Cloud Services

Security and Safety in Cloud-based Systems and Services

Panel Member 1

Prof. Dr. rer. nat. Nane Kratzke
Computer Science and Business Information Systems

Professor for computer science at Lübeck University of Applied Sciences in Germany.

His research focuses mainly cloud-native application engineering

and web-scale elastic systems.

He consulted the German Ministry of Defense and the German Air Force in questions concerning network centric warfare as a consulting software architect.

As former Navy officer (German Navy) he executed (in addition to military) functions as project leader, software-architect, and software engineer in several electronic warfare system and naval command and control system projects.

Panel Discussion: "Security and Safety in Cloud-based Systems and Services"

There is no impenetrable system

So, why we are just waiting to get breached?

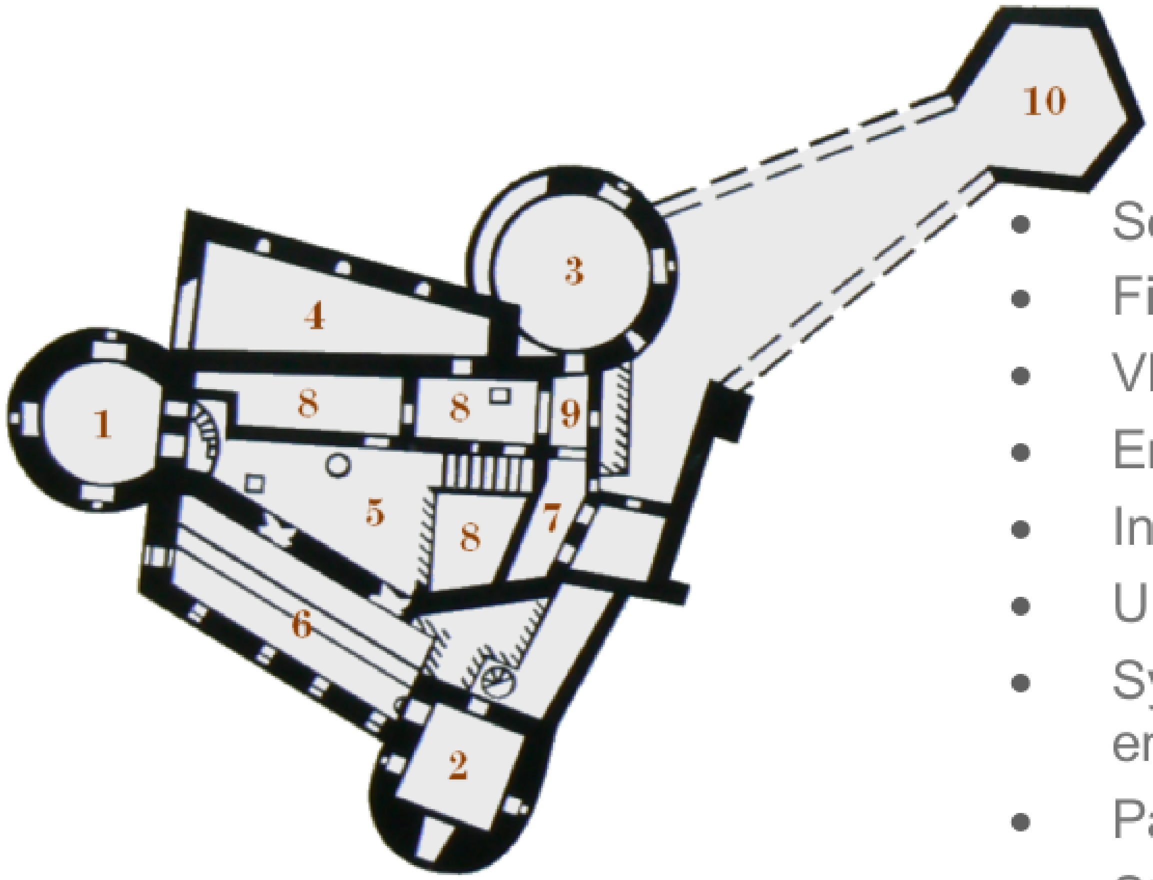
Nane Kratzke

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

CoSA
Center of Excellence

9th International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2018); Barcelona, Spain, 2018

The Fortress Walls of Cloud Applications



- Security Groups
- Firewalls
- VPNs
- Encryptable Overlay Networks
- Intrusion Detection Systems
- Unattended Security Updates
- Symmetric and asymmetric encryption
- Password (checks)
- SSH Keys
- Authentication
- Authorization
- Two (Multi) Factor Authentication
- …

How to defense against unknown vulnerabilities?

MELTDOWN

CVE-2017-5754

SPECTRE

CVE-2017-5715

CVE-2017-5753

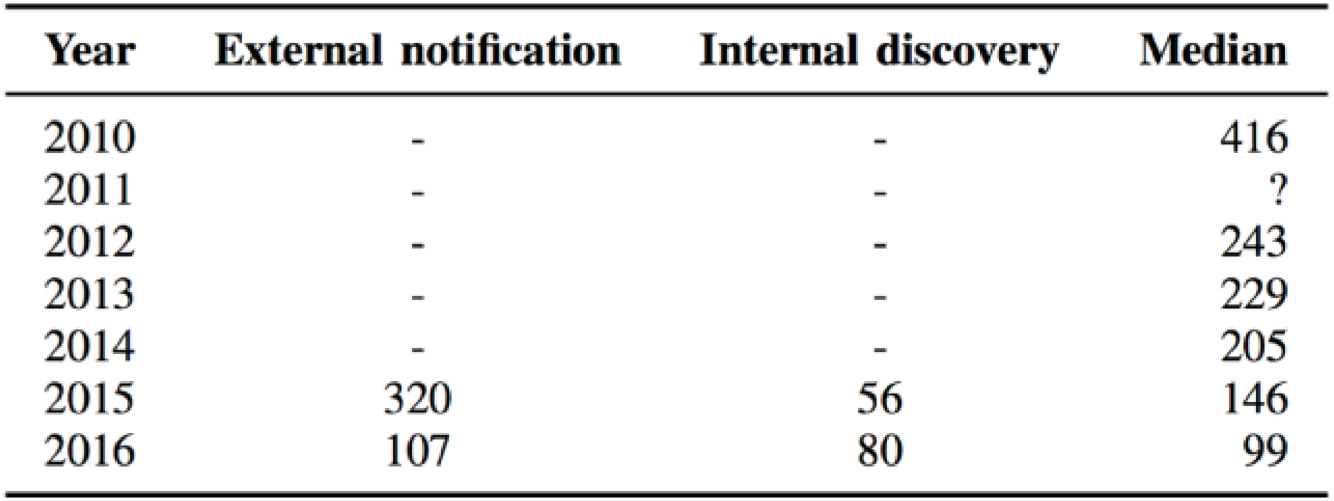
I started my computer science studies in 1996!

My microprocessor professor told me, out-of-order execution and branch-prediction is one of the coolest things on earth.

*Reported in January 2018. Mainly x86 microprocessors with **out-of-order execution** and **branch-prediction** affected since **1995** (says Google).*

How long can presence be maintained?

TABLE II. **Days that attackers were present on victim systems** Dwell times reported by M-Trends reports since 2010. External and internal discovery data is reported since 2015. No data could be found for 2011.



Year	External notification	Internal discovery	Median
2010	-	-	416
2011	-	-	?
2012	-	-	243
2013	-	-	229
2014	-	-	205
2015	320	56	146
2016	107	80	99

Answer: ***Surprisingly long!***

Some scary considerations

- **In principle attackers can establish footholds in our systems whenever they want (zero-day exploits)**
- Cloud application security engineering efforts focus to harden the fortress walls.
- Cloud applications rely on their defensive walls but seldom attack intruders actively.

We need a reactive component as well

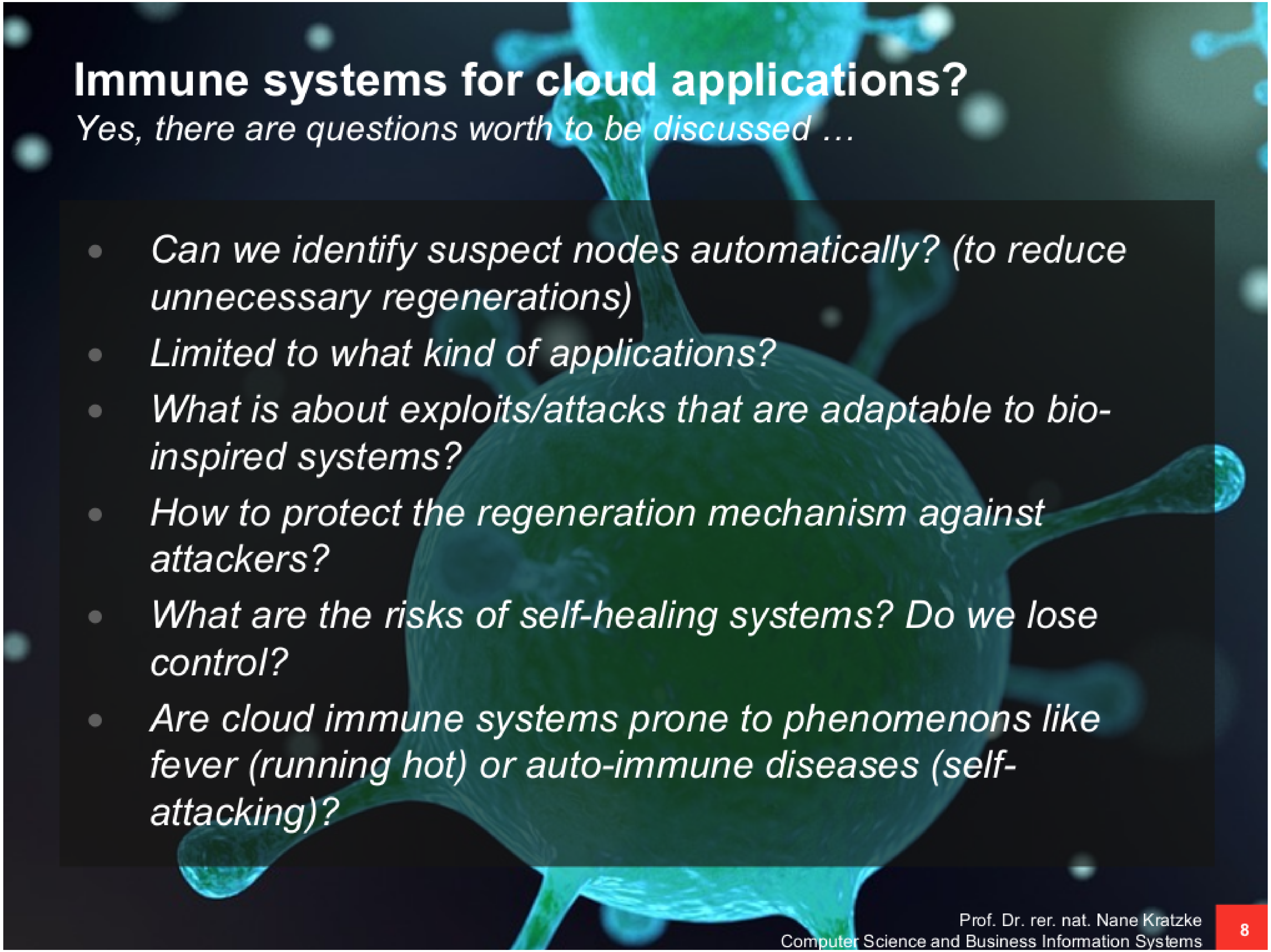
Biological systems are different.

Defensive “walls” can be breached at several layers.

An additional active defense system is needed to attack potential successful intruders - an immune system.

We presented a solution that follows a biological analogy of a cell regeneration (works fully automatic).

It could reduce these mentioned **3 month** easily down to **3 hours**.



Immune systems for cloud applications?

Yes, there are questions worth to be discussed …

- *Can we identify suspect nodes automatically? (to reduce unnecessary regenerations)*
- *Limited to what kind of applications?*
- *What is about exploits/attacks that are adaptable to bio-inspired systems?*
- *How to protect the regeneration mechanism against attackers?*
- *What are the risks of self-healing systems? Do we lose control?*
- *Are cloud immune systems prone to phenomenons like fever (running hot) or auto-immune diseases (self-attacking)?*

Acknowledgement

This contribution resulted as a side-effect from research that is funded by German Federal Ministry of Education and Research (Project Cloud TRANSIT, 13FH021PX4).

FORSCHUNG AN FACHHOCHSCHULEN

Presentation URL

Picture Reference

- **Ninja:** Pixabay (CC0 Public Domain)
- **Fortress:** Pixabay (CC0 Public Domain)
- **Bowman:** Pixabay (CC0 Public Domain)
- **Cattle:** Pixabay (CC0 Public Domain)
- **Cell:** Pixabay (CC0 Public Domain)
- **Air Transport:** Pixabay (CC0 Public Domain)

About

Nane Kratzke

CoSA: http://cosa.fh-luebeck.de/en/contact/people/n-kratzke

ResearchGate: https://www.researchgate.net/profile/Nane_Kratzke

Blog: http://www.nkode.io

Twitter: @NaneKratzke

GooglePlus: +NaneKratzke

LinkedIn: https://de.linkedin.com/in/nanekratzke

GitHub: https://github.com/nkratzke

Speaker Deck: https://speakerdeck.com/nkratzke

Panel on Cloud Services

Security and Safety in Cloud-based Systems and Services

Panel Member 2 Dr Aspen Olmsted

Dr Aspen Olmsted is an assistant professor and Graduate program director at the College of Charleston. He obtained a Ph.D. in Computer Science and Engineering from The University of South Carolina. Before his academic career, he was CEO of Alliance Software Corporation. Alliance Software developed N-Tier enterprise applications for the performing arts and humanities market. Dr Olmsted’s research focus is on the development of algorithms and architectures for distributed enterprise solutions that can guarantee security and correctness while maintaining high-availability. In his Secure Data Engineering Lab at the College of Charleston, Aspen mentors over a dozen graduate and undergraduate students each year. Aspen's research is primarily focused on providing secure transaction guarantees for Databases, Web Services, and Distributed Systems. He has contributed over fifty conference and journal papers in the domains of cloud computing, secure software development and distributed transactions in IARIA and IEEE publications. Aspen has delivered several keynote addresses, special sessions, tutorials at IEEE and IARIA conferences in the past few years. Aspen has also participated or hosted several panels at the same conferences.

COLLEGE of CHARLESTON

1770

Data Leakage through Cloud

Cloud Computing 2018

Aspen Olmsted

Problem

Organizations are the custodians of their patrons data

Ideal World

An organizations application would run as a uni-kernal with data available in a single interface.

The single interface would ensure access control,privacy and auditing.

Current Cloud

- Many layers each with their own access control, vulnerabilities, and auditing

Items that need to be controlled and audited.

- OS
- Source Code
- Private Keys
- Credentials
- Data
- Logs

Panel on Cloud Services

Security and Safety in Cloud-based Systems and Services

Panel Member 3 Dr George Weir

- Lecturer in Computer Science, University of Strathclyde, UK
- Adjunct Professor, School of Criminology, Simon Fraser University, Canada
- Published extensively on Security, HCI, e-learning, readability and Corpus Linguistics
- Current focus on Security and Digital Forensics in the Cloud
- Supervising 13 PhD students on aspects of Information Security

Special Track on Finding A Solution To – Cloud Forensic Problem
Cloud Computing 2018
19 – 20 February, Barcelona, Spain

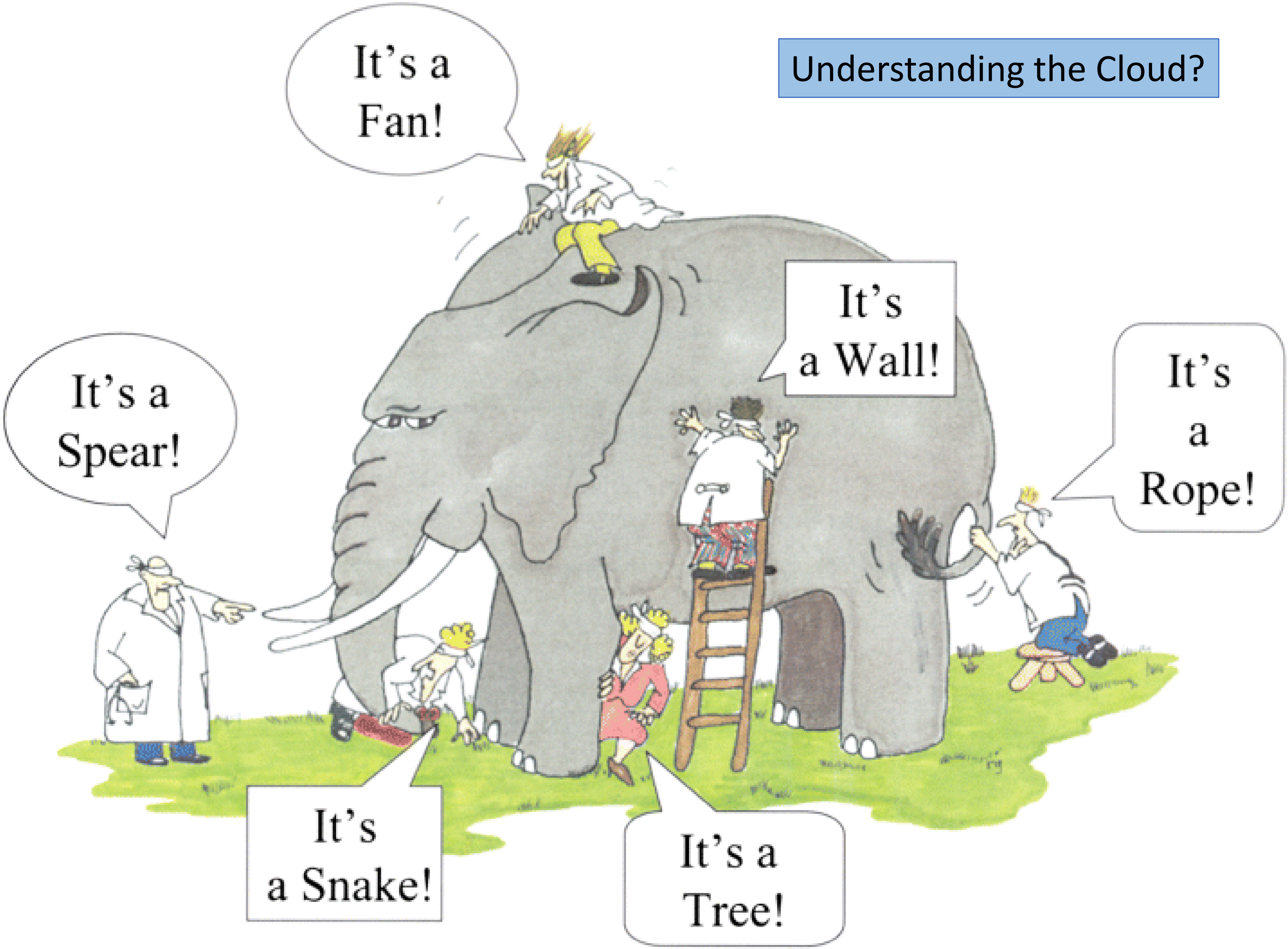
1495

UNIVERSITY OF ABERDEEN
BUSINESS SCHOOL

End user issues

- Understanding the systems we are using
- Risk tolerance
- Safety-critical systems?

Understanding the Cloud?

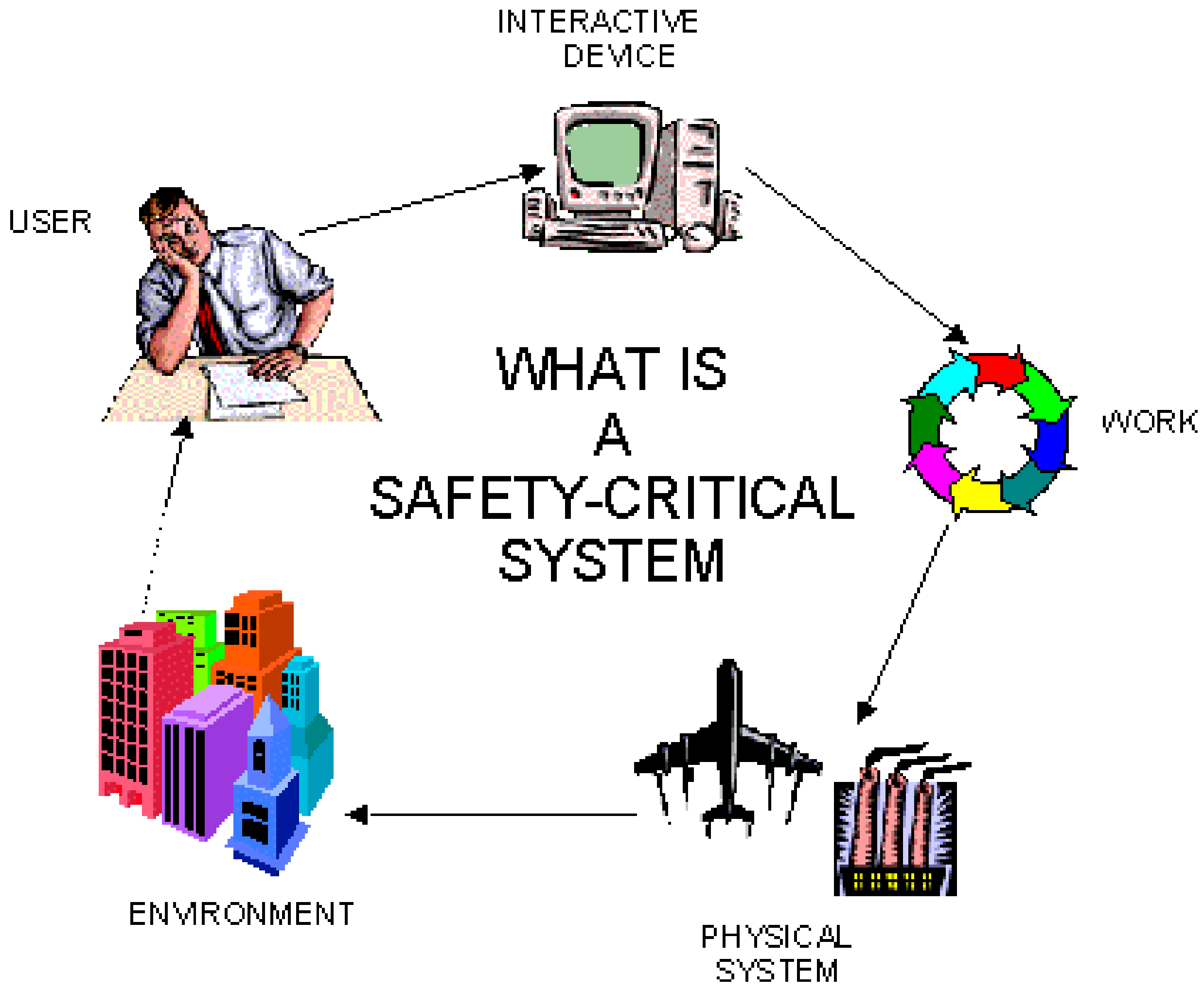


Risk tolerance

- We are accustomed to taking risks
- We will tolerate risks for the benefits

TOTALLY
Above the Fringe
01603
614989
V725 ETF

Safety-critical systems



Panel on Cloud Services

Security and Safety in Cloud-based Systems and Services

Summary of Panel Discussion

After each of the three panel members presented themselves, the panel got down to some serious discussion on impoartant matters of security and safety in cloud systems. There was a great deal of interest from the audience on the implications of security and safety on the use of cloud systems, and the whole panel constributed significantly to the discussion. A considerable range of interesting and challenging questions was brought up by the audience and discussed fully by the panel. Many audience members were surprised by how little many understood about the challenges presented by the forthcoming EU General Data Protection Regulation for cloud users, and were shocked at the level of potential fines. Altogether, a highly illuminating discussion, which was very well received by the audience.