THE UNIVERSITY OF NORTHAMPTON

An Embedded Pedagogic Model for Computer Forensics within an Undergraduate Programme

Proposed by the Computing Division, University of Northampton

The 7th Annual Teaching Computer Forensics Workshop

University of Sunderland – 10th Nov 2011

Presented by Ali Al-Sherbaz

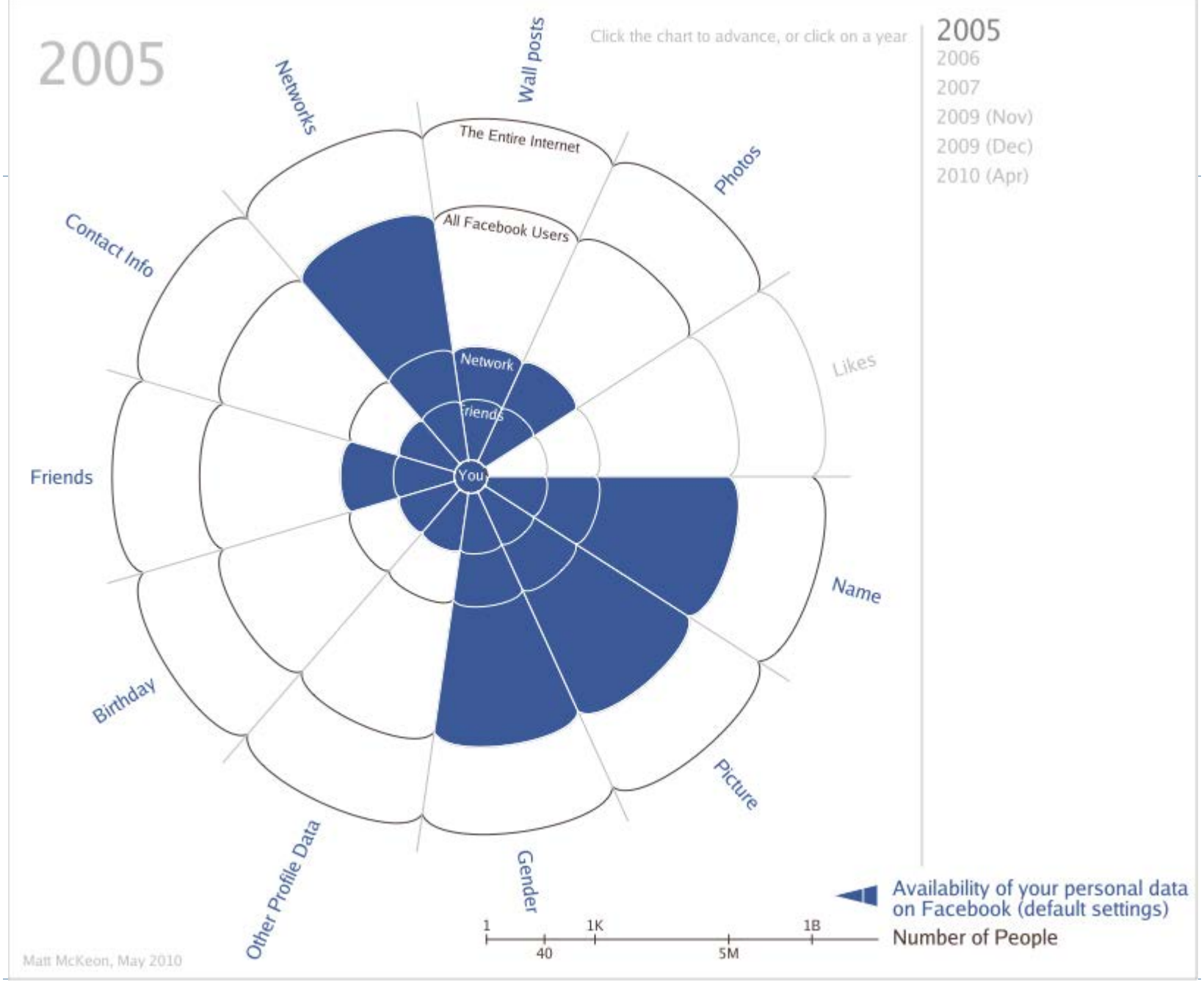
Authors: Amir Minai, James Xue, Rashmi Dravid , The University of Northampton

Overview:

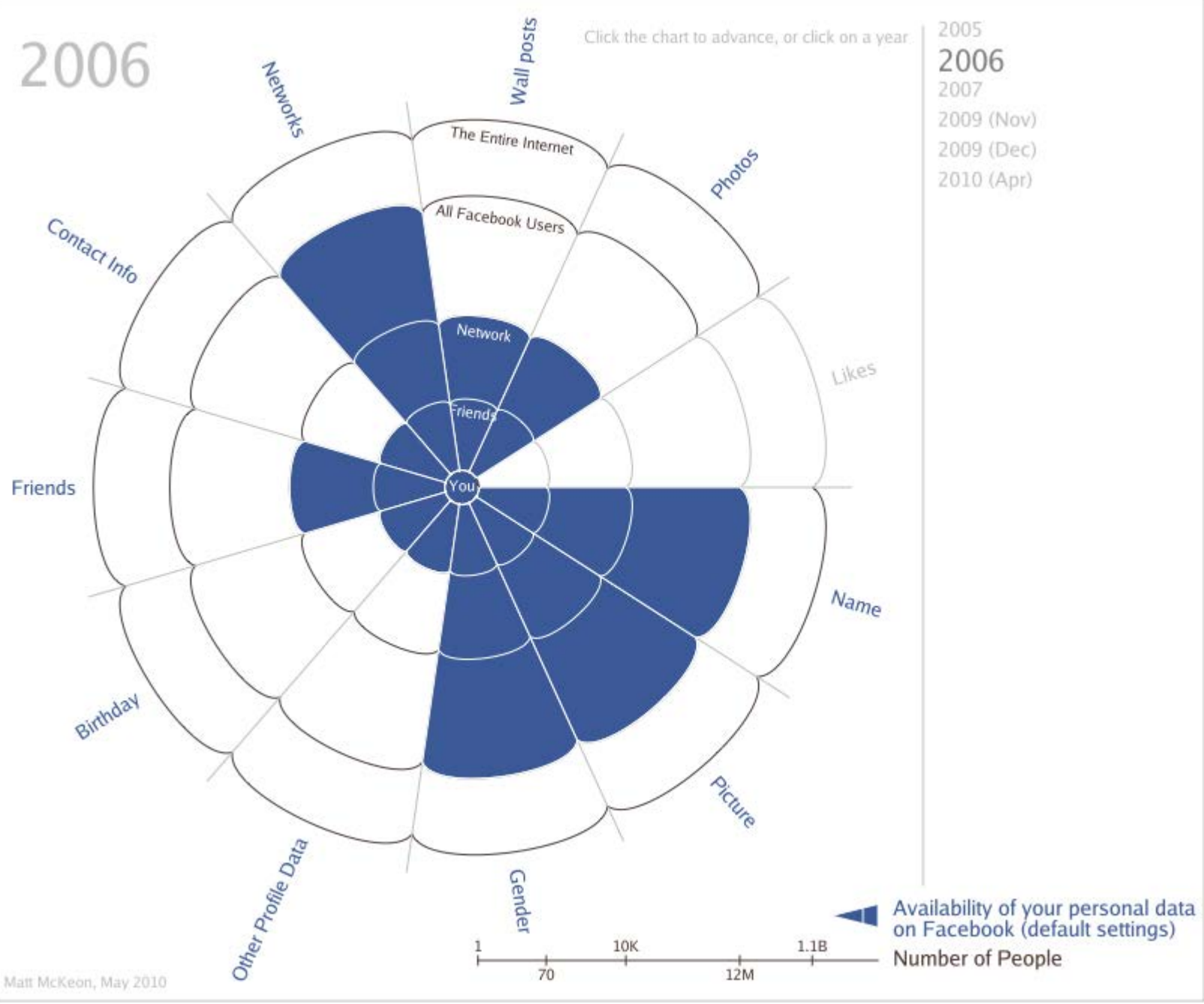
- **Facts -** Cybercrimes
  - The Evolution of Privacy
- **Dale's Cone** of Experience in learning
- **The Proposed Model:** present an embedded computer forensics/cyber security materials within an undergraduate Programme
- **Conclusion**

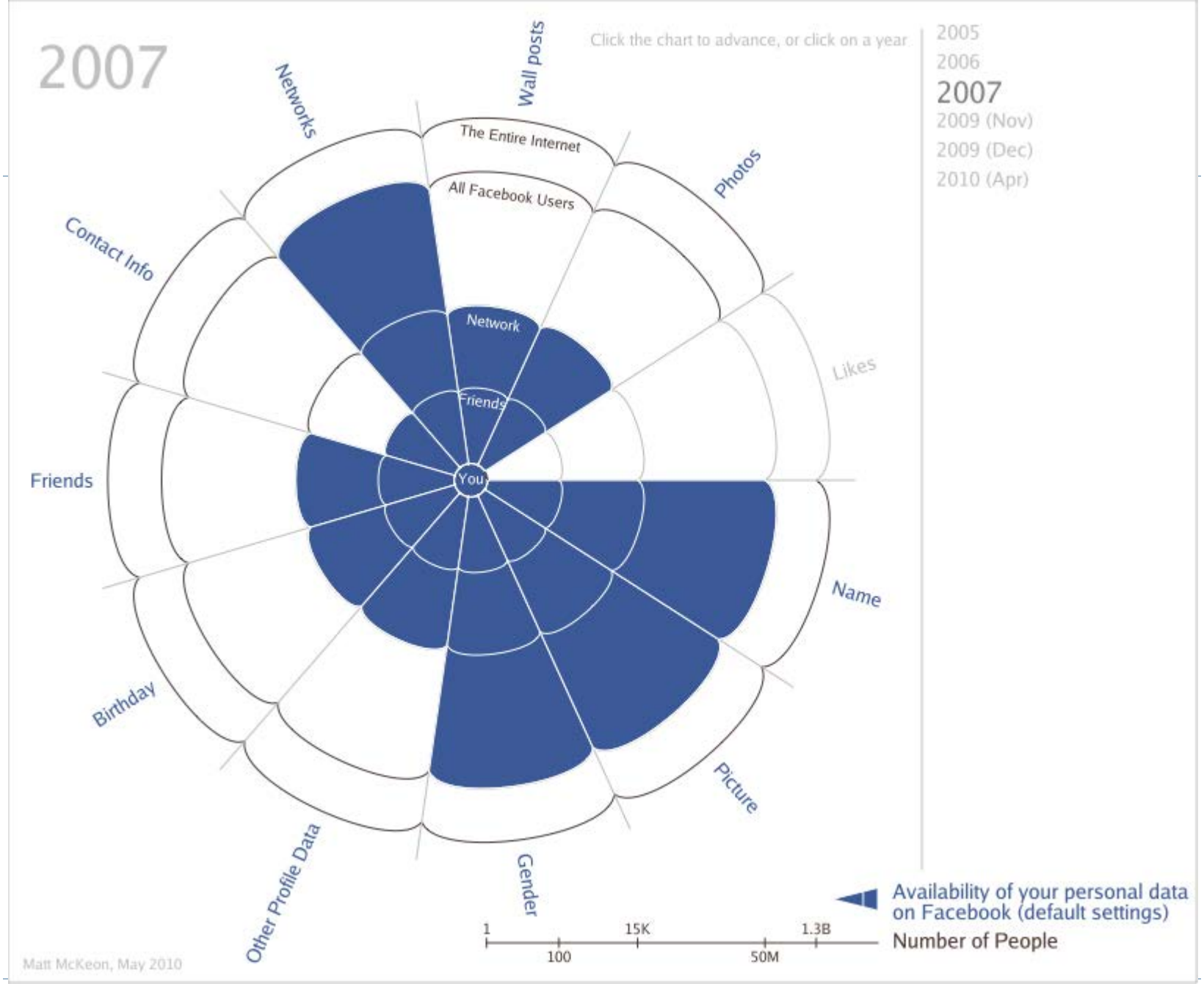
Facts

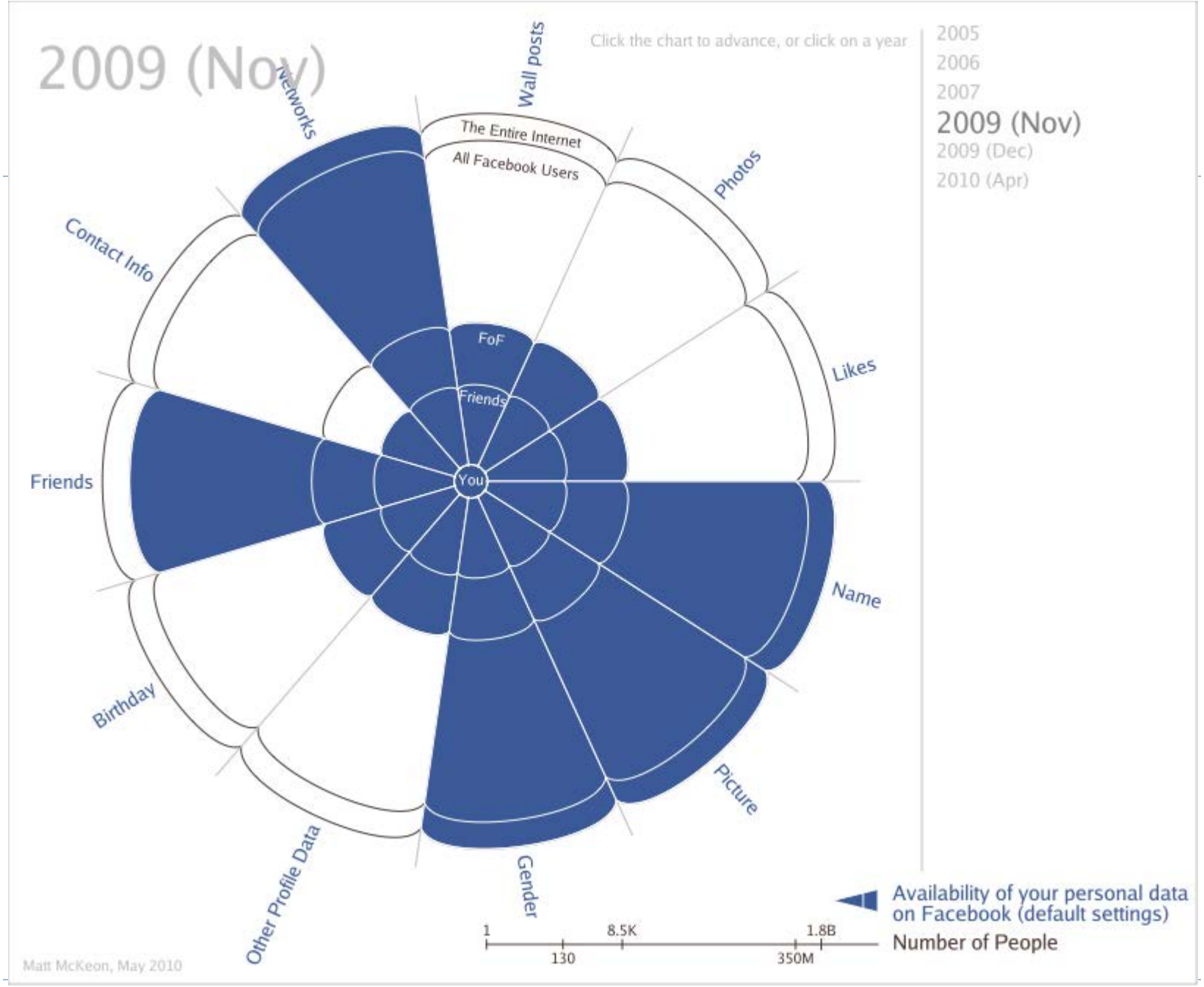
- Computer forensics / Cyber-Security which has a strong mutli-disciplinary background derives from the computing subjects in networking, programming, security and mathematics.
- Cyber crimes are on the rise, however, Cyber security professionals are in depressingly low numbers.
- Reflecting the technological fluctuations, it is seen as essential for students to be continuously updated.
- The evolution of privacy on Social Networking is changing

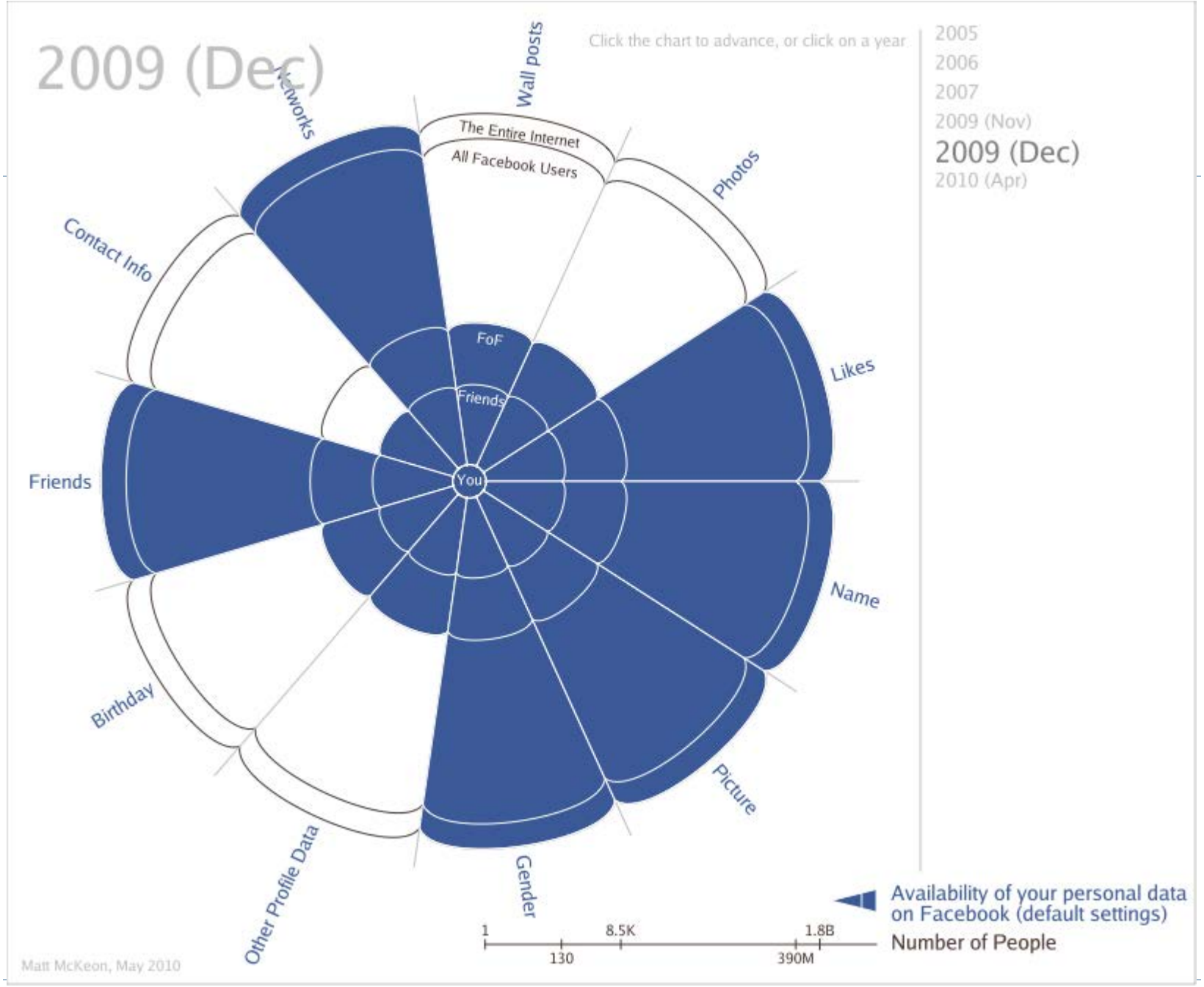


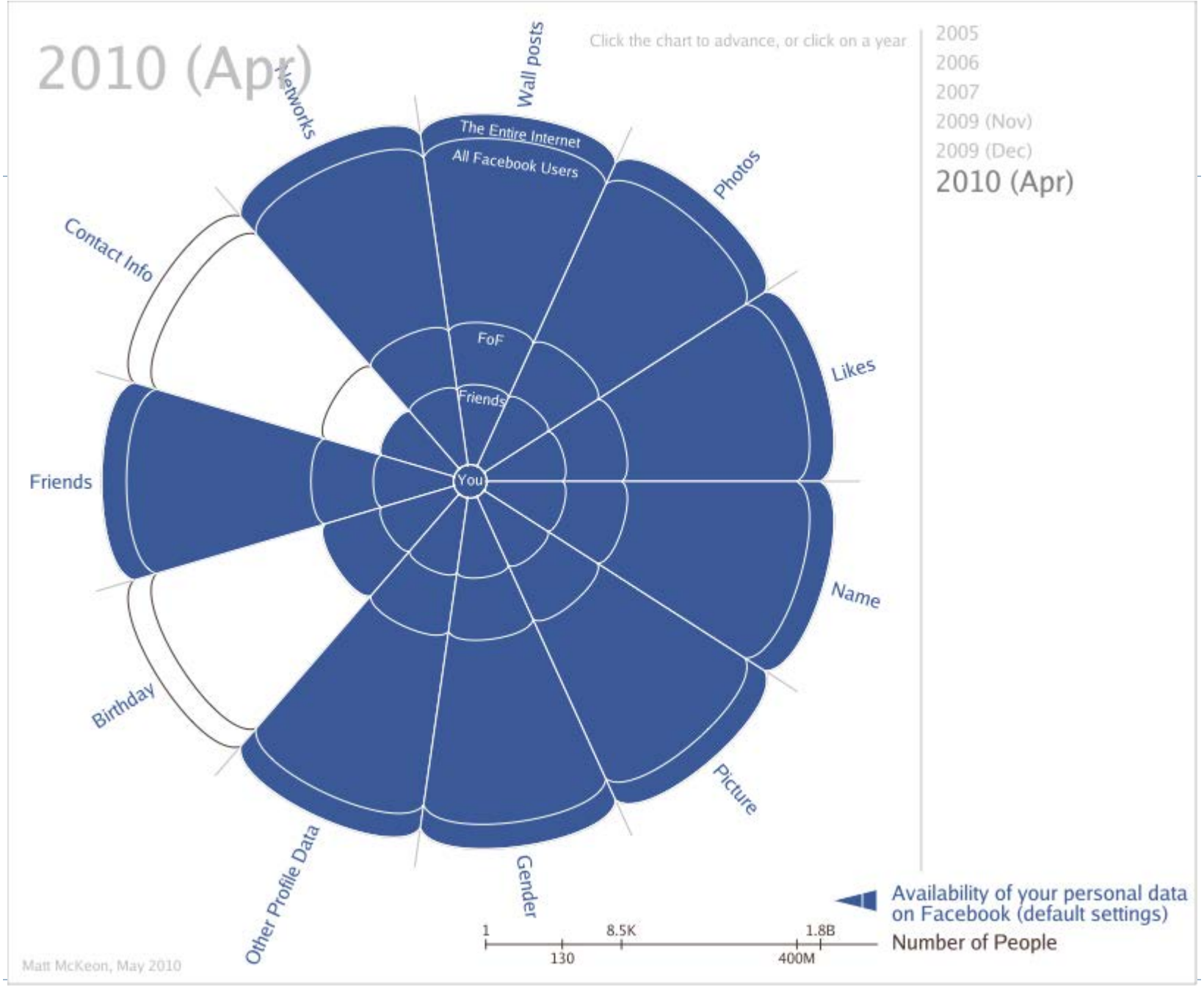
The Evolution of Privacy on Facebook


2006
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Contact Info
Likes
Friends
Name
Birthday
Picture
Other Profile Data
Gender
The Entire Internet
All Facebook Users
Network
Friends
You
1
10K
1.1B
70
12M
Availability of your personal data on Facebook (default settings)
Number of People
Matt McKeon, May 2010


2007
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
Networks
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
100
15K
50M
1.3B
Number of People
Matt McKeon, May 2010


2009 (Nov)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
FoF
Friends
You
1
130
8.5K
350M
1.8B
Availability of your personal data on Facebook (default settings)
Number of People
Matt McKeon, May 2010


2009 (Dec)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
8.5K
1.8B
130
390M
Number of People
Matt McKeon, May 2010

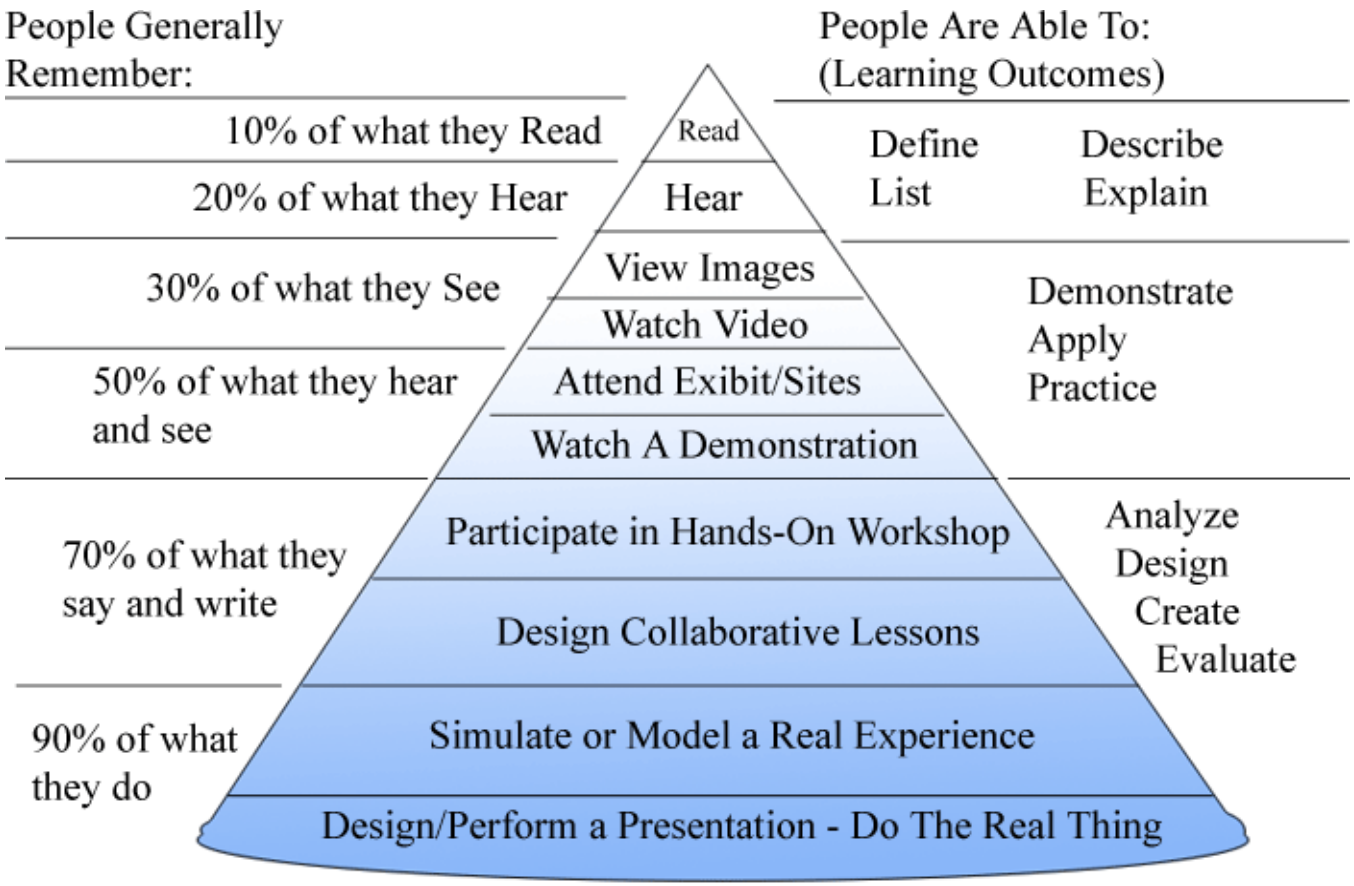


http://www.mattmckeon.com/facebook-privacy/

Learning From Experience Model

- **Least effective learning results from**
  - **listening to spoken words**
- **Most effective methods**
  - **Hands-on lab activities based on real, everyday life experiences**
- **Best learning methods use perceptual styles**
  - **Perceptual learning styles are sensory based**
- **Action-learning techniques result in up to 90% retention**
- **More real-life experiences.**
- **A tool** to help instructors **make decisions about designing Learning Activities and Resources**

Dale's Cone of Experience



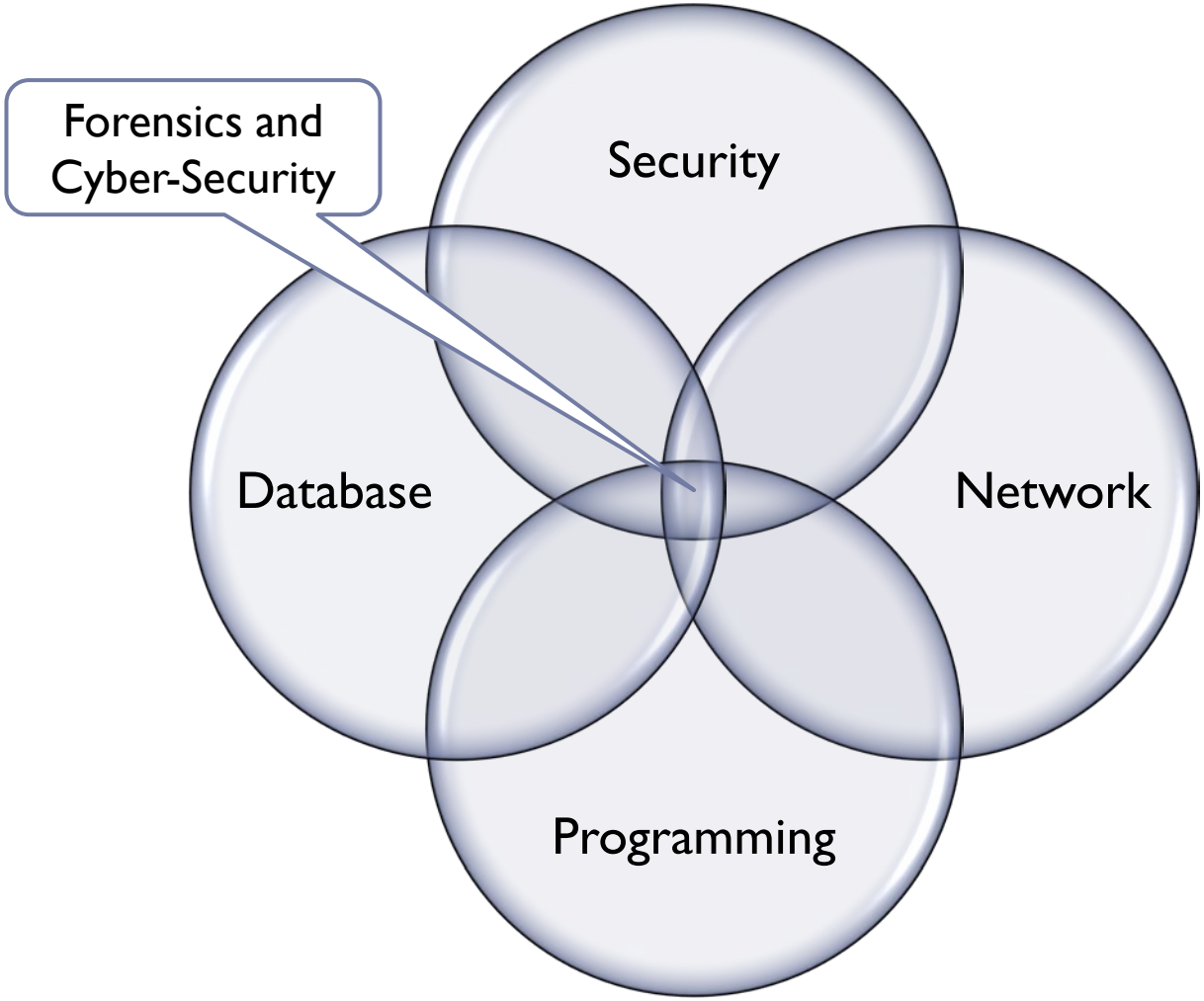
The Proposed Model

- The depth of knowledge required for learning such topics as forensic and cyber security should be offered from the underlying principles to their abstraction
- Increasing awareness of cybersecurity and emphasising the need for a common vision among students addresses the challenges
- Some of the modules already cover part of computer forensics implicitly

The Proposed Model

- Focuses on the delivery and assessment of certain computing modules, with an evaluation of its efficiency on the use of time and effort in order to satisfy the minimum requirements of the curriculum.
- Embed the computer forensics materials within the undergraduate modules to extend students' knowledge and skills in a practical context
- Highlighting these topics to the students and making them more visible as computer forensics is one of the main objectives
- Enhance the existing computing modules by dedicating certain amount of lecture time on computer forensic related concepts

The Proposed Module



Internet & Computer Security Module

Security in Context	Cryptography	Cryptographic Systems	Network Security	Application Security
• Security Awareness • Security technology in context • Security Vulnerabilities • Security (Hardware & Software) • Security Management	• Cryptographic systems • Crypto Algorithms • Crypto analysis	• Pki • SSL • IPSec • VPNs • Kerberos	• Firewalls • IDS & IPS	• Internet • Database • Enterprise

Internet & Computer Security Module
(Practical)

Footprinting the network (Pen test)	Cryptography	GNUPG	Network Security tools
• Security Analysis • Network threat testing	• Encryption basics • Encryption software • PKI exercise	• Email security	• Firewall • SNORT

Network Module

Logging

- Cisco devices
- Windows hosts
  - Syslog
- SNMP traps
- Enterprise Log and Search Archive (ELSA)

Monitoring

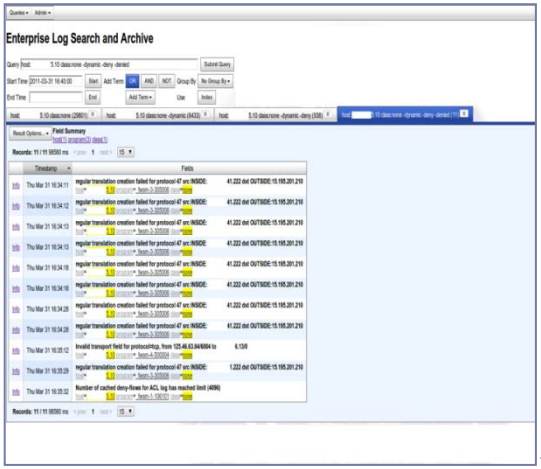
- Wireshark for packet capture and analysis of security threats

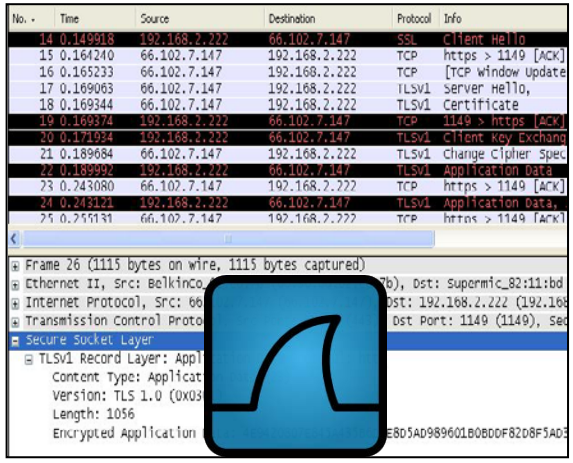
Capturing and Analyses

- Track packets and bytes at flow level
- Nmap and OpenVAS for port scans
- Ping sweeps

Action

- Routers and Switches
  - Network Address Translations
  - Access Control Lists
  - Stateful packet Inspection.
  - Intrusion detection/Prevention (IDS) Systems





DataBase Module

Ensure the right privileges are granted.

- During SQL DDL lecture/practical session
- Lower system and database privileges.

Firewall the database (GreenSQL)

- Prevent malicious attach (SQL Injection)
- Install and test how it works

Apply Best Practices

- Physical location, Antivirus, Regularly apply software patches.
- Rename root to a new name.
- Disable LOCAL INFILE in MySQL.
- Remove anonymous accounts.
- Remove test database.

Internet Programming Module

Invalidated Input	Broken Access Control	Broken Authentication	Cross Site Scripting (XSS) Flaws
Buffer Overflows	Injection Flaws	Improper Error Handling	Insecure Storage
Denial of Service (DoS)	Insecure Configuration Management	Session Management	Malware Attack

Conclusion

- To raise Cyber-Crime awareness it is imperative that computing courses within universities increase the level of student knowledge and skills by providing professional education.
- The teaching and learning of computer forensics and cyber-security can be integrated within a modular scheme without the need to add to an existing over loaded module pool.
- The proposed embedded model is founded on learning methods that reinforce learning through activities within technically related fields.
- The model can be adopted by Universities when considering to develop integrated modules.

THE UNIVERSITY OF NORTHAMPTON

Thanks

Any Question ?

Looking for Feedback