Introduction to Cybersecurity Session 1

Phil Irving (philip.irving@sunderland.ac.uk)

House Keeping

- Fire
- Coffee
- First Aid
- Coffee
- Toilets
- Coffee
- Lunch
- Coffee

….. See a theme developing here?

Objectives

- Awareness of Cyber Security, digital forensics and the threats we face

Agenda

Time	Activity	Who
10.30	Outline of the day Intro to the area	Phil
11am -12pm	Penetration Testing	Paul Jenkins
12 – 12.30	Q&A's to Paul	Paul Jenkins
12.30 - 13.15	Lunch	
13.15	Pen Testing Hands on	Paul Jenkins
14.45 – 15:00	Comfort break	
15.00	CIA with exercises continued	Paul Jenkins
16.00	Finish and next steps	Steve Blanks

About Me

- Senior Lecturer in Networking, Network Security, Cyber Security and Telecoms.
- Cisco CCNP Instructor
- Cisco Network Security Instructor
- Cisco Cyber Security Instructor
- Access data Certified digital Examiner (ACE!)

Discussion: Cyber Security vs Digital Forensics – what is the difference?

- Thoughts on:
  - Cyber Security
  - Digital Forensics

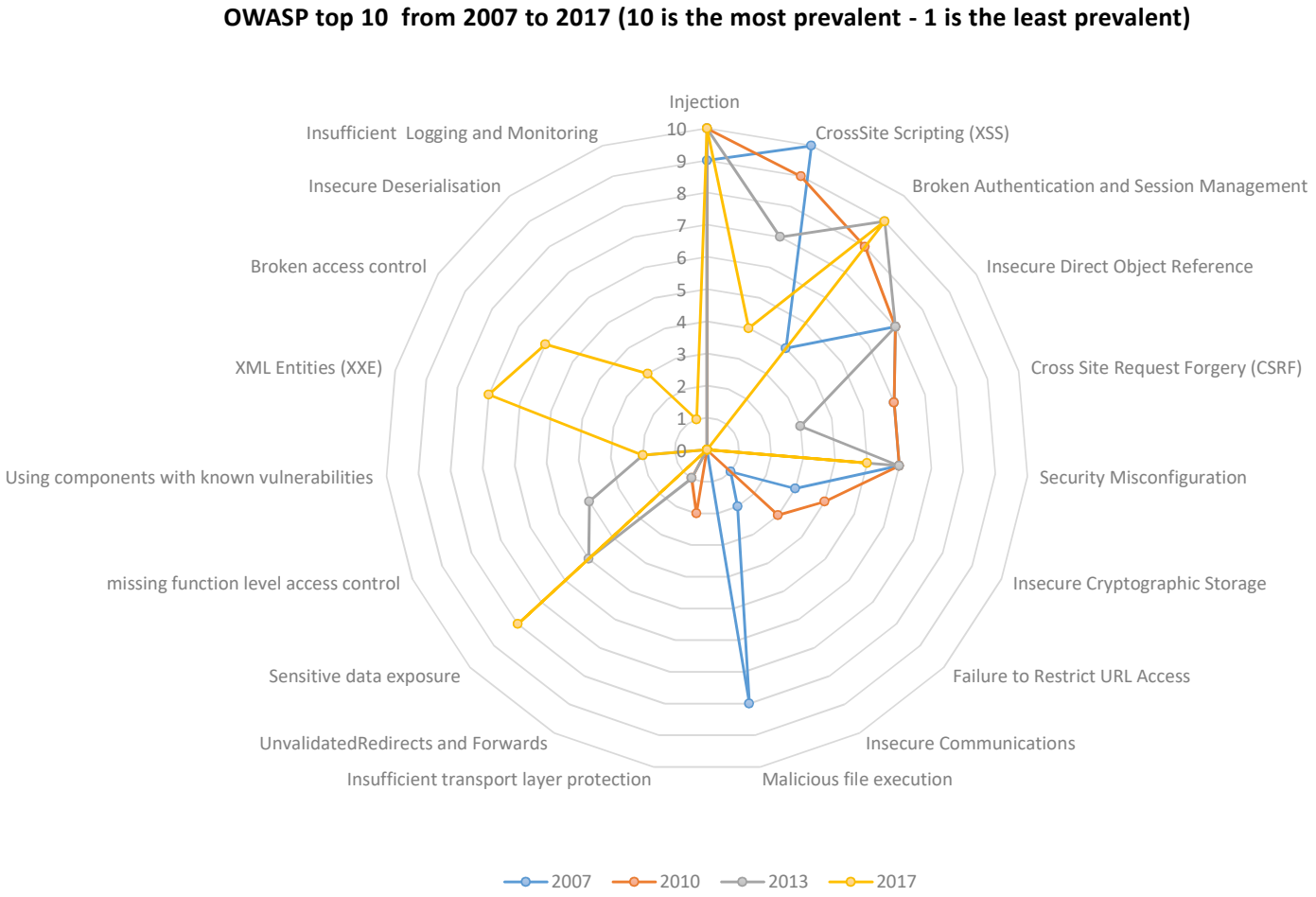
Cybersecurity

- “The protection of devices, services and networks — and the information on them — from theft or damage”. NCSC (National Cyber Security Centre). https://www.ncsc.gov.uk
- Harry Potter terms “Defense against the Dark Arts”
  - Remus Lupin (Prisoner of Azkaban) Severus Snape (Half-Blood Prince), Gilderoy Lockhart (Chamber of Secrets) Mad-Eye Moody/Barty Crouch Jr (Goblet of Fire), Amycus Carrow (Deathly Hallows), Dolores Umbridge (Order of **the** Phoenix), Professor Quirrell (Philosopher's Stone)
- A set of tools and techniques used to enhance systems security design
- Knowing and understanding what the bad guys are up to
- Using that knowledge to identify potential attacks and put in place preventative measures
- Using hacking tools and techniques to identify security weaknesses and then provide solutions on how to remove those weaknesses through systems design

Digital Forensics

- "*In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony*". Source: DoDD 5505.13E (https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf)
- "*Forensic science is generally defined as the application of science to the law. Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Data refers to distinct pieces of digital information that have been formatted in a specific way. Organizations have an ever-increasing amount of data from many sources. For example, data can be stored or transferred by standard computer systems, networking equipment, computing peripherals, personal digital assistants (PDA), consumer electronic devices, and various types of media, among other sources*". https://www.nist.org/nist_plugins/content/content.php?content.60
- ACPO Good Practice Guide (https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)

Change in the Open Web Application Security Project (OWASP) top 10 most critical web application security risks from 2007 to 2017.



Owasp.org. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Some of those involved

- Have a look at NCSC self help https://www.cyberessentials.ncsc.gov.uk/)
- Payment Card Industry (https://www.pcisecuritystandards.org/)
- Cyber-thieves set sights on hijacking payment data https://www.bbc.co.uk/news/technology-47279255
- National Institute of Science and Technology (https://www.nist.gov/cyberframework)

But, before I hand over …..

- Are we alone in this?
- Should we be worried?
- https://www.bbc.co.uk/news/technology-45823180