OWASP Cambridge Chapter Security Seminar

Tuesday 21st October 2014 17:30 – 20:30, Lord Ashcroft Building (LAB003), Anglia Ruskin University, Cambridge.

Hosted by the Department of Computing & Technology, Anglia Ruskin University, OWASP (Open Web Application Security Project) Cambridge Chapter

Guest speakers: Eireann Leverett

Eireann Leverett is a Senior Consultant at IOActive where he focuses on Smart Grid and SCADA systems. He studied Artificial Intelligence (AI) and Software Engineering at Edinburgh University and went on to get his Masters in Advanced Computer Science at University of Cambridge. He studied under Frank Stajano and Jon Crowcroft in Cambridge's computer security group. In between, he worked for five years at GE Energy and did a six-month engagement with ABB in their corporate research department

Title : Switches get Stitches

This mini workshop is based on the successful 44Con talk this year and will introduce you to Industrial Ethernet Switches and their vulnerabilities. These switches are used in environments with industrial automation equipment, like substations, factories, refineries, and ports; in other words, SCADA and ICS switches. You will become familiar with how these switches are used and do some light traffic analysis and firmware reverse engineering, **bring your laptop with Wireshark installed!!** During this workshop, Eireann will discuss several vulnerabilities and share the methods used to discover them as well as techniques for exploitation.

This is partially a hands-on workshop, with pcaps, network forensics, binary analysis, web application vulnerabiities, etc. It teaches about bad session entropy, sidejacking, CSRF, brute forcing MD5, DoS in the context of industrial processes, and carving default private keys from firmware images. Essentially, this is "how I found the bugs in my CVE list for 2013-2014", breaking industrial ethernet switches.

Bring along your laptop with Wireshark installed.

Background

OWASP (Open Web Application Security Project is a 501(c)(3) not-for-profit worldwide charitable organization focused on improving the security of application software. Their mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks.

The Department of Computing & Technology at Anglia Ruskin University is enhancing its curricula and capabilities in information security following its successful BSc(Hons) Information Security and Forensic Computing pathway. Establishing a joint professional networking group with OWASP concentrating on

aspects of computing and application security is a key part of this enhancement. A key aim the department is working towards is developing a MSc Information Security specialising in Application Security and as part of this activity looking to develop and a local Information Security Student Society.

Agenda

17:30 – 17:45 Welcome from the OWASP Cambridge Chapter Leader, Adrian Winckles, Course Leader in Information Security & Forensic Computing, Anglia Ruskin University

17:45 – 19:15 Eireann Leverett – IOActive – Switches got Stitches

19:15 – 19:30 Q & A – Further meetings and ideas.

19:30– 20:30 Refreshments & Networking in LAB027

Registration

To register for this free event, please register online at

https://www.surveymonkey.com/s/OWASPoct2014

Please note there is no automatic notification or confirmation.

The meeting will be held in the Lord Ashcroft Building, Room LAB003 (Breakout Room LAB027 for networking & refreshments).

Please enter through the Helmore Building and ask at reception.

Anglia Ruskin University
Cambridge Campus
East Road
Cambridge
CB1 1PT

Get further information on travelling to the university.

http://www.anglia.ac.uk/ruskin/en/home/your_university/anglia_ruskin_campuses/cambridge_campus/find_cambridge.html