University of Glasgow

School of Computing Science

Developing pedagogy to optimise forensic training in safety-related applications

Chris Johnson, Charlie Rutherford, Marco Cook, Tania Wallis, Kelsey Collington

c.rutherford.2@research.gla.ac.uk

Contents

- Forensics pedagogy overview/update
  - The project
  - Progression of work
  - Lessons learned from last session
  - What's next?
- Pedagogy research with respect to network discovery in ICS
  - Session contents
  - Methods of presentation
  - Evolving session design
  - 5Ws and 1H

Forensics Pedagogy project

What is the aim/purpose of the study?

- Research into best-practices for teaching ICS forensics to professional systems engineers working in CNI
- Focus on unique challenges demanded by safety-critical systems and domains of cyber security such as digital forensics in ICS
- How can existing ICS cyber test beds be used effectively outside of the technically-focused security research?
- We are opening our labs up to various orgs to run training workshops for professionals working in CNI industries

University of Glasgow

School of Computing Science

Day One – 24th September	Day Two – 25th September	Day Three – 26th September
	09:00 – 09:15 Previous day review/questions	09:00 – 09:15 Previous day review/questions
12:00 – 12:30 Arrival, coffee	09:15 – 10:45 Team task: Analyzing a device using the Emphasis methodology	09:15 – 10:30 Discussion on Forensic Applications within ICS – 404
12:30 – 14:00 Welcome, introductions and objectives Introduction to ICS research at Glasgow Open discussion on industry's view on threats and challenges	10:45– 11:00 Coffee	10:30 – 10:45 Coffee
	11:00 – 12:00 Chris Presentation - 203	10:45 – 12:00 ICS Forensics
14:00 – 14:15 Coffee Break	12:00 – 13:00 Lunch	12:00 – 13:00 Lunch
14:15 – 16:00 Initial lab exercises I – taking IT cyber security into the context of ICS	13:00 – 14:30 ICS Network Asset Discovery	13:00 – 13:30 Feedback and Review Session
		13:30 – 14:00 Summary and Session Close
16:00 – 16:15 Coffee Break		14:00 – 15:00 Additional lab time if required
16:15 – 17:00 Initial lab exercises II – taking IT cyber security into the context of ICS - discussion	14:30 – 14:45 Coffee	
17:00 – 17:15 Feedback Session	15:45 – 16:30 ICS Network Asset Discovery Exercises 16:30 – 17:00 Discussion	
	17:00 – 17:15 Feedback Session	
	Evening: Team Social	

2nd & 3rd training workshops

Training workshops – network discovery

Session Contents

- Issues with network discovery in ICS
- Tools for performing network discovery – passive & active
  - The tools which already exist (from IT)
  - The limitations and problems with these tools
- Our tool for network discovery in ICS
- Research into the topic
  - Serial comms protocols, heterogeneous networks
  - Tool development
  - Utilising ICS application level protocols for discovery/information gathering

Teaching methods

- Lecture/classroom style (powerpoint/whiteboard), could be structured or semi-structured
- Demonstration - showing some technical concept on a projected screen
- Peer learning - expert-novice, or novice-novice
- Lab exercises and questions
- Written walkthrough - e.g. Do A, you should see B as the result...
- Open discussions - peer and near peer group sharing of knowledge

Evolving session design

1st session –	Lecture style presentation. Discussion about challenges in ICS network discovery. Largely unstructured sandbox hands on session.
2nd session –	Initially lecture style. Less group discussion, more individual discussion. Structured walk through.
3rd session –	No lecture, no walkthrough. Live demo and ongoing discussion. More focus on research at Glasgow vs broader concepts.

The 5 Ws and 1 H

Who? - The participants

What? - The course and session content

Where? - Location/facilities

When? - Structure of the course

Why? - Course aims

How? - Teaching styles

Lessons learned

- Manage expectations ("If you try and please everybody, you'll please nobody")
- For max benefit, content and presentation style should be tailored for a given group (within reason!)
- Need to re-think course aims – what do we want them to come out of this course with?

Thank you

Charlie Rutherford

Email: c.rutherford.2@research.gla.ac.uk

Office: 0141 330 7232