WHITE PAPER:

Availability of Open Source Tool-Sets for CNI-ICS

Availability of Open Source Tool-Sets for CNI-ICS

23rd March 2018

Authors

Chris Hankin (editor), Imperial College London
Tom Chothia, University of Birmingham Peter M3, National Cyber Security CentrePeter Popov, City University of London
Awais Rashid, Lancaster University and University of Bristol
Sakir Sezer, Queen's University Belfast

1 Introduction: Rationale/Justification

Industrial Control Systems (ICS), composed of combinations of hardware, software and IT networks, orchestrate the myriad of functions needed to execute complex tasks such as the delivery of utility services and the operation of intricate and disparate manufacturing processes. ICS are examples of cyber-physical systems which are increasing in importance as techno-social components of the Critical National Infrastructure (CNI) of the future and as they extend their scope, becoming ubiquitous, accessible and transformative to wider society and the economy.

The cyber security of CNI ICS enterprises is actively studied worldwide and in the UK through academia, cyber services industry, CNI asset owners, and Government Departments. There is a wide range of tools available to enable this, some are widely known and commonly used while some have been developed for in-house application or as the output of academic research and await wider exploitation. There is an opportunity to bring together the wider ICS community to define what tools are available for use, what is the breadth of their scope and where future activities should be focussed.

The major benefit of creating an open source tool set repository is that it will raise efficiency across the community through the sharing and preventing the need to re-invent what is already in the community.

This paper will *catalogue* and assess the open source tools and processes available for securing or testing/evaluating of ICS products.

2 The NIST Framework

The NIST framework for improving cybersecurity of critical infrastructure[1] identifies five main functions:

- **Identify** – Develop the organisation's understanding to manage cybersecurity risk, including: asset management; appropriate governance; risk assessment; and a risk management strategy.

[1] https://www.nist.gov/cyberframework

- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services, including: access control mechanisms; user awareness and training; anti-virus software; firewalls; patch management.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, including: anomalies detection; security continuous monitoring.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event, including: response planning; communications; forensics; mitigation strategies.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event, including: recovery and business continuity planning; communications.

We will review the tools used by the RITICS partners and other activities indicating which functions they address.

3 Survey of the Current State of the Art

A survey of the RITICS partners has identified the following open source tools and systems produced by the research activity:

	NIST Framework Areas				
Tool Name	*Identify*	*Protect*	*Detect*	*Respond*	*Recover*
ADVISE	X				
ADVISE Meta	X				
AEGIS Protocol Fuzzer	X				
Attack Tree with Sequential Conjunction	X				
Automated SCADA attack scripts	X				
CVE-search	X				
FinkWinPP	X				
Hugin Lite 8.3	X				
IEC104 PCN TestBed	X				
NetLogo	X				
PIA:FARA	X				
QTester104	X				
SimaticScan (Vulnerability Scanner)	X				
Bettercap		X			
Ettercap with IEC104 plugin		X			
OpenMUC		X			
Scapy Modbus		X			
TRW-S		X			
ADTool	X		X		
Allium	X	X	X		
Clingo 3.0.2	X		X		
DigitalBonds Network enumeration	X		X		
SCADAStrangeLove	X		X		
Security Onion	X	X	X		
SENAMI (IDS)			X		
Tensorflow		X	X		
Wireshark	X		X		
IEC104 Application NSM SIEM	X		X	X	
SNORT		X	X	X	
SCADA Anomaly Detection System (SANDS)	X		X		X
SILK	X		X		X
Wireshark dissector for IEC61850-90-5	X			X	X
ElasticStack					

ADTool: The Attack-Defense Tree Tool (ADTool) allows users to model and analyze attack-defense scenarios represented with attack-defense trees and attack-defense terms. It supports the attack-defense tree methodology developed within the ATREES, TREsPASS, and ADT2P projects.

ADVISE: The ADVISE (ADversary VIew Security Evaluation) formalism is a part of the Mobius suite (https://www.mobius.illinois.edu/), a software tool well known in academia used for model-based quantitative evaluation of performance, dependability, performability, etc. The ADVISE formalism was added to the Mobius suite relatively recently (from 2012 onwards). It was developed to model in detail the steps taken by an Adversary attacking the assets of a computer network or of a cyber-physical system. The underlying modelling formalism is the theory of competitive Markov Decision Processes.

The modeller can state explicitly, although fairly abstractly, the motivation and the skills of an Adversary. Once a model is built, the tool allows for a stated utility function to be maximised, e.g. via Monte Carlo simulation. The tool was developed and applied to a range of cyber-security applications, documented in the academic literature. Some of these examples are from case studies made available by the Department of Energy, i.e. are ICS related.

The Perform group at the University of Illinois at Urbana Champaign, led by Prof. Bill Sanders, emphasise that the tool makes cyber-risk assessment *repeatable*, and reduces the impact of assessor's subjectivity on the risk assessment results. This claim, of course, is true to an extent - the assessor is responsible for the parameterisation of the model.

ADVISE Meta: This tool is an incremental improvement/enhancement of the ADVISE formalism. It includes a couple of major innovations. 1) The tool supports an ontology of modelling fragments, which can be reused in building new Adversary models. 2) The tool may generate a complete Adversary model from a given description of a network topology (e.g. of an ICS). The idea is that the

generated model will include the steps that the Adversary could take to exploit every known vulnerability in the particular computer network. The other aspects of the tool are similar to the standard ADVISE.

These concepts have been demonstrated and a working version of the tool can be obtained from the developers with non-trivial examples. The tool, however, has not matured yet and is being used mainly for research.

AEGIS Protocol Fuzzer: A smart fuzzing framework for a growing number of protocols that can identify robustness and security issues in communications software before it is deployed in a production system.

Allium: Snort and ElasticStack for network analysis – lightweight security onion VM.

Attack Tree with Sequential Conjunction: Script to generate visual representations of attack trees.

Automated SCADA attack graphs: An automated script to initiate a complex sequence of attacks with varying temporal spacing between attacks. Used for generating packet captures on testbed.

Bettercap: Man-in-the-Middle tool.

Clingo 3.0.2: Clingo is an answer set solver for (extended) normal and disjunctive logic programs. It combines the high-level modeling capacities of Answer Set Programing with state-of-the-art techniques from the area of Boolean constraint solving. Imperial used it to represent and reason about rule-based safety and security requirements in ICS to identify various interdependencies between them.

CVE-search: CVE-search is a tool to import CVE and CPE into a MongoDB to facilitate search and processing of CVEs. The main objective of the software is to avoid doing direct and public lookups into the public CVE databases. Local lookups are usually faster and you can limit your sensitive queries via the Internet. Imperial mainly used it for fetching data from CVE and sorting relevant vulnerabilities of products to estimate vulnerability similarities.

DigitalBonds Network enumeration: Collection of namp script to enumerate SCADA protocols.

ElasticStack: Dashboard and persistent storage.

Ettercap with IEC104 Plugin: Ettercap Plugin to modifiy IEC104 packets.

FinkWinPP: The WinPP family of software products by Fink Industrial Engineering enables simulation of standard protocols as well as widely used proprietary protocols.

Hugin Lite 8.3: The Hugin Graphical User Interface is an interactive tool enabling you to construct Bayesian networks and use the facilities of the Hugin Decision Engine. Imperial has mainly used it for visualization and interactions with Bayeisan attack graphs.

IEC104 Application NSM SIEM: Built with vagrant, ansible and ElasticStack. Provides graphical representation of network packets at an application layer, with intuitive misuse detection.

IEC104 PCN Testbed: Built with vagrant, ansible and OpenMUC, a scalable process control network with realistic topology and real-world emulation.

NetLogo: NetLogo is an agent-based modelling tool that enables a programmable modelling environment for simulating natural phenomena and behaviours of complex systems over time.

Imperial uses NetLogo to construct the networked ICS model and simulate the propagation of malware.

OpenMUC: OpenMUC is a software framework based on Java and OSGi that simplifies the development of customized monitoring, logging and control systems. Collection of libraries for field bus protocols: Modbus, IEC61850, IEC104.

PIA:FARA: This is an open source software tool developed at City University for risk assessment of complex cyber-physical systems (CPS). The tool allows one to build a hybrid model of a CPS, which includes a number of sub-models:

- an agent-based probabilistic model of the real assets (e.g. of a power transmission network, a gas/oil facilities, etc.),
- a set of deterministic models, which allow one to compute in detail the losses in the "physical world" due to changes in state of the physical assets (e.g. caused by accidental failures or by malicious activities), and
- an Adversary model built as a stochastic state machine.

The hybrid model is "solved" using a highly performant Monte Carlo simulation engine, designed to work on a range of hardware platforms: from a laptop, to a computer cluster and computing cloud (e.g. AWS infrastructure). The current version of the tool is written in Golang supported on all major computer platforms.

The measures of interest are specified separately from the model itself and can vary from recording full simulation traces of events and state of the modelled system to defining to defining aggregated measures, e.g. the average losses due to accidental failures/malicious events within a single simulation run. The tool also allows one to specify the required statistical significance of the results (e.g. of the losses).

A unique feature of the tool is the mixture of models - stochastic (to model the discrete events in the system) and deterministic (to establish the losses due to the adverse events in physical/cyber world). A possible integration of PIA:FARA with ADVISE (META) was discussed with the US colleagues, as the two tools clearly complement each other.

QTester104: This software implements the IEC60870-5-104 protocol (client side) for substation data acquisition and control via TCP/IP network using the QT UI Framework. It can be compiled on Linux and Windows platforms. It's possible to poll and view data from the substation system (RTU/concentrator) and also send commands.

SANDS: Uses OCSVM to build a model on a clean dataset and detect unseen network traffic using application layer features.

SCADAStrangeLove: Collection of namp script to enumerate SCADA protocols.

Scapy Modbus: Mobus library writen for SCAPY – Python packet craftiing library.

Security Onion: Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools.

SENAMI: Selective non-invasive intrusion detection mechanism - that combines passive monitoring with active approaches. SENAMI is a bespoke IDS for Siemens S7 ICS environments. SENAMI combines traditional NIDS methodologies with "active" intrusion detection, which requests values directly from the PLC to monitor; it introduces the concept of "selective, non-invasive active

monitoring" to avoid overloading legacy ICS devices by only actively polling a small number of pertinent variables. Combining passive IDS with an active IDS, SENAMI generates alerts, reported live in the IDS terminal, and saves them to a logfile for further analysis with the SIEM. SENAMI should work in all Siemens S7 environments that have their PLC memory configuration set up as above - a standard way amongst many ICS vendors.

SiLK: SiLK, the System for Internet-Level Knowledge, is a collection of traffic analysis tools developed by the CERT Network Situational Awareness Team (CERT NetSA) to facilitate security analysis of large networks. The SiLK tool suite supports the efficient collection, storage, and analysis of network flow data, enabling network security analysts to rapidly query large historical traffic data sets. SiLK is ideally suited for analyzing traffic on the backbone or border of a large, distributed enterprise or mid-sized ISP.

SimaticScan: A specialised vulnerability scanner specific to Siemens SIMATIC PLCs; can be used to determine if any PLCs found using the SHODAN search engine are vulnerable to specific attacks.

SNORT: Snort is an open source Intrusion Detection / Intrusion Prevention tool, executed on Intel Platforms. It is widely used for IT infrastructure protection and is estimated that approximately 60% worldwide IDS/IPS deployments are based on SNORT. Snort can operate with commercial rules (provided by CISCO and a number of smaller companies, such as Anomali, etc.), community rules (open source), and custom rules developed by the end user. QUB has been developing many custom-purpose rules for Snort and Suricate targeting the protection of SCADA protocols.

TensorFlow: Tensorflow is an open source software library to develop machine learning algorithms. It was developed by Google and is one of the most widely adopted machine learning frameworks. It uses data flow graphs for efficient computation, and utilises any available GPUs and TPUs on a machine. There are other higher level APIs used which utilise Tensorflow as a backend, of which Keras is one of the most popular.

TRW-S: TRW-S stands for tree-reweighted max-product message passing, which is an effective algorithm to minimizing energy in multi-label Markov Random Field/Conditional Random field optimization. Imperial has developed an effective approach based on this algorithm to produce optimal diversification strategy to improve ICS resilience.

Wireshark: Wireshark is a widely used packet analysis tool. It utilises pcap to capture packets and supports a range of integrated sorting and filtering options. It can capture traffic from different types of networks such as Ethernet or IEEE 802.11. Finally it is able to integrate and capture packets with network simulation tools.

Wireshark dissector for IEC61850-90-5: Dissector to enable viewing of application layer data for this network protocol for synchrophasor communications.

The SCEPTICS Tool – University of Birmingham

The Birmingham SCEPTICS Tool can be used to discover new, previously unknown threat vectors against ICSs, and understand all the possible threats from a range of different types of attackers. As a front end, the tool uses Visio, making it easy to use. The back end uses a purpose-built Java engine that analyses the models. The tool fits into a standard risk assessment process as part of the hazard discovery phase.

The SCEPTICS tool uses concepts such as hardware components, data profiles and process operations to model the behaviour of ICS systems. The modelling of hardware components is very flexible, they can be real physical entities such as embedded system boards, networking equipment,

or physical sensors, but also more abstract components such as BUSes, network interfaces or even software. Profiles are numerical values that describe either some individual aspect of the security of a system or an overall aggregated value for a component. These numerical values are used by the process operation to derive the aggregate security characteristic of the analysed model.

Thus, a complete SCEPTICS model includes all of the possible types of data and data flows in the system, as well as details of the system components and communication protocols. CVSS values, vulnerabilities and other information about the components can be added by the modeller, or automatically fetched from databases. Based on a model and list of assets, the SCEPTICS tool can automatically find possible attacks against the ICS, and then order them based on a modeller-defined ranking. In particular, the tool can discover new possible attacks that include chaining together a cascade of compromised components.

Rather than using a simulation or sampling technique, the SCEPTICS tool uses advanced mathematics to calculate the exact probabilities of attacks, via all possible paths. Using this the tool can:

- Find and rank attack vectors. The tool is able to enumerate all possible paths between a system asset and any possible attacker starting point, and rank them based on the probability of that path being successfully leveraged in an attack.
- Discover how attacks can propagate. By specifying a specific starting node and data type, the tool will establish how an attack of one node propagates if an attack were to take place over a specific medium, giving the owner an appreciation of how an attack can affect systems which may not have been originally believed to be possible to affect.
- Identification of critical assets. Given a specific data type or graph, the tool will identify critical assets, where the exploitability is either high, given some threshold supplied by the ICS owner.
- Ability to vary attack probabilities for security analysis. Our tool supports the ability to assess the security impact that affecting the exploitability of a given node has on the system, so highlighting possible weak points in an ICS.

5G UK Hub System

DCMS have a large multi-phase program to develop and innovate 5G technologies [1].

An initial activity has been to create a sustained long-term UK Hub for 5G experimentation and innovation. The UK Hub has been built by project partners at the University of Surrey, University of Bristol, and King's College London. They have each created an interconnected virtualised testbed island which is integrated to the 5GUK Exchange (5GUKEX) sub-system to provide access for the End User to the 5G UK Hub network services. The testbed follows ETSI standards on Cyber Security [7].

Further DCMS led competitions will determine the experiments that will use the 5G Hub which may include infrastructure and mobility, health and social care, and smart communities.

Each sub-system is scalable and sustainable providing the End Users with the ability to create and experiment with new virtual network services offered by the testbed islands. Thus it has been specifically designed to be interoperable with other testbeds.

The 5GUKEX exposes User interfaces to experimenters to launch experiments using ETSI MANO OSM APIs [2]. The interface between the 5GUKEX and the islands is compatible with the ETSI NFV MANO

[3] standard. The information elements (IE) used by the 5GUKEX have been determined and will be available to experimenters from Apr18 onwards.

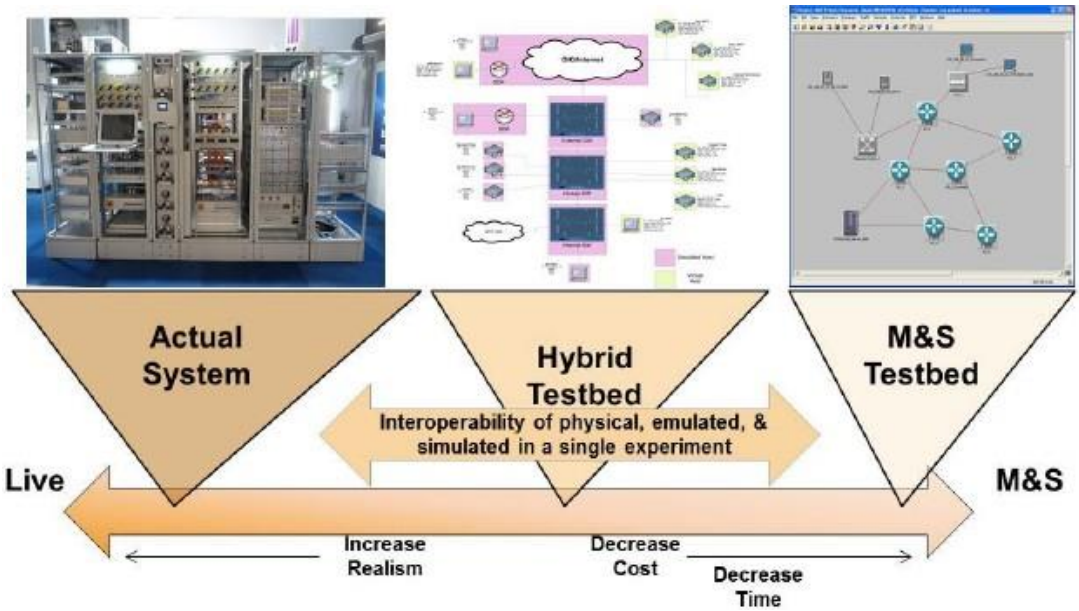
Significant functions in the 5GUKEX component include User Authenticator, Network Service Composer, Manager, Request Broker and Inter-domain Connectivity Manager (ICM). The ICM directly engages with the set of programmable switches at the fabric interconnection point (Slough Data Centre) to enforce the island interconnection. The underlying network uses JANET [4].

USA Grid Protection Alliance

The Grid Protection Alliance is a not-for-profit corporation specializing in the development and support of innovative software solutions for the electric industry. Since its inception in 2010, they have developed a production-grade open source code base which is incorporated in their Grid Solutions Framework. A recent project has been the open ECA project (extensible Control and Analytics) focused on enabling the production use of analytic systems that incorporate high fidelity synchrophasor data.

Emulytics™

Sandia National Laboratories has developed the Emulytics™ system to provide tools for emulation and analytics in a variety of different domains including SCADA systems. The approach involves an element of virtualisation but has the capability of including real hardware in the loop. The paper by Van Leeuwen et al [5] describes a spectrum from live system through to one based purely on modelling and simulation as shown in the Figure:



Emulytics™ allows a tradeoff to be made along this spectrum by allowing the inter-mixing of physical devices with emulated and simulated components. At the heart of the Emulytics™ toolset is the open source minimega tool for launching and managing virtual machines.

Spire

The group of Prof. Yair Amir at Johns Hopkins University in Baltimore, US, has developed an intrusion tolerant SCADA, which is designed to continue to work even if some of the critical components are compromised. The software (including a non-trivial demo system) is available as open source from http://dsn.jhu.edu/spire.

Spire relies on a number of other well-known open-source components, developed by the group over the years such as Spine (http://spines.org), an advanced Byzantine agreement protocol with liveliness guarantees, Prime (http://dsn.jhu.edu/prime), and on software components developed by others, such as SCADAMaster, RTC/RTU Proxy, OpenPLC and Multicompiler (which applies code obfuscation to the executable), etc.

The solution is quite intriguing because it was compared with the NIST-compliant SCADA architecture. The colleagues from Baltimore report that the NIST compliant solutions and Spire were attacked by the Sandia National Labs Red team. The red team was given access to the Spire source code. The NIST–compliant architecture was taken over and direct access to the PLC was obtained from the operational network. Spire, however, withstood the attack and continued to work unaffected. The Sandia National Labs Red team gave up trying to compromise the Spire after a few days.

Spire was deployed successfully in industrial settings, too: (https://hub.jhu.edu/2018/02/21/hacker-resistant-software-hawaii-power-grid/)

Further technical details on this work can be found at: http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/72/ResearchReports/Amir-2017_06_Spire_IFIP.pdf .

Open source tools from the INL Survey

The following additional open source tools were identified in [6].

Binwalk – Binwalk is a tool for analyzing, reverse engineering, and extracting firmware images. It can be used to quickly find offsets to filesystem sections in a binary image, extract files from within the image and perform entropy analysis on images.

CHIPSEC – CHIPSEC is a framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components. Originally developed by Intel to help internal teams find and fix vulnerabilities in platform hardware and software, the now open source tool includes a security test suite, tools for accessing various low level interfaces, and forensic capabilities. It can be run on Windows, Linux, Mac OS X, and UEFI shell.

CodeDNA – CodeDNA detects families of attacks and supports a navigable means of exploring attack family development, leading to insights and predictions about what a broad range of future zero-day attacks may look like, so that the defenders can detect them. It generates unique DNA-like fingerprints from incoming files and computes similarity scores across a database of fingerprints to automate the identification of related malware binaries and link variants.

Conpot – Conpot is an ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting ICS. This dockerized ICS specific honeypot includes Modbus, s7, http, snmp, bacnet, snmp, and Ipmi protocols. Conpot has built-in support for HPFeeds, a generic data sharing protocol used by the Honeynet Project.

Digital Ants – Digital Ants uses dynamic, decentralized mechanisms inspired by nature to provide mobile, resilient cybersecurity for protecting large enterprise IT networks and critical infrastructures. Individual ant-like sensor programs swarm to the location of anomalies and enable human operators to focus on areas and issues of concern

fcd – fcd is a burgeoning LLVM-based native program decompiler. Most of the code is licensed under the GNU GPLv3 license, though some parts, such as the executable parsing code, are licensed under

a less restrictive scheme. Currently, fcd works best with executables that follow the x86_64 System V ABI. Fcd 13 supports ELF executables out-of-the-box, but also ships with Python scripts that can be used as plugins to parse Mach-O and PE executables.

GridPot – GridPot is a Symbolic Cyber-Physical Honeynet Framework. Its symbolic simulation of cyber-physical systems emulates SCADA/HMI and ICS protocols. GridPot uses ETSY's skyline project for anomaly detection and shows real-time attacks.

Hyperion – Hyperion is a cyber security technology designed to "look inside" an executable program and determine software's function or "behavior" without the use of the software's source code. It generates associated program behaviors and the complete set of conditions under which they occur; these behaviors can be automatically checked for known malicious signatures and inspected by domain experts to assure correct operation and the absence of malicious content.

Radare – Radare is a portable reversing framework that can: disassemble (and assemble for) many different architectures; debug with local native and remote debuggers; run on Linux, *BSD, Windows, OSX, Android, iOS, Solaris, and Haiku; perform forensics on filesystems and data carving; support collaborative analysis using the embedded webserver, visualize data structures of several file types; and patch programs to uncover new features or fix vulnerabilities.

Snowman – Snowman is a native code to C/C++ decompile that supports ARM, x86, and x86-64 architectures. It reconstructs functions; their names and arguments; local and global variables; expressions; integer, pointer, and structural types; and all types of control-flow structures, including switch. The GUI allows one-click navigation between the assembler code and the reconstructed program. It includes a command-line interface for batch processing and offers an IDA Plug-in.

T-Pot – T-Pot combines the dockerized honeypots conpot, cowrie, dionaea, elasticpot, emobility, glastopf, and honeytrap with suricata, a NSM engine and the ELK stack to visualize all events. Events are correlated by T-Pot's data submission tool ewsposter which also supports Honeynet project HPfeeds honeypot data sharing.

TruffleHog – Started as a university project at the Karlsruhe Institute of Technology, TruffleHog requires a modified version of Snort including a PROFINET-preprocessor to collect "Truffles" representing a semantic analysis of one PROFINET-network package. It keeps track of all incoming Truffles, uses the semantic information to build a network topology (or rather a network map), and displays it to look at in quasi real time.

Volatility Framework – The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License (GPL), for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer visibility into the runtime state of the system.

WeaselBoard – WeaselBoard is a PLC backplane analysis system that connects directly to the PLC backplane; it provides zero-day exploit protection for PLCs. WeaselBoard captures and analyzes backplane traffic among PLC modules, thereby detecting changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates.

X64dbg – Using a single interface, X64dbg can debug both x64 and x32 applications. Built on opensource libraries (Qt, TitanEngine, capstone, Yara, Scylla, Jansson, Iz4, XEDParse, Keystone,

asmjit, and Snowman), X64dbg is customizable and extendable and offers executable patching and analysis.

YARA – YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. YARA users can create descriptions of malware families (or others) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a Boolean expression which determine its logic.

Feasibility/Barriers

The majority of the tools that we have identified are available at the following URLs:

ADTool	http://satoss.uni.lu/members/piotr/adtool/
ADVISE	https://www.mobius.illinois.edu/
ADVISE Meta	https://www.mobius.illinois.edu/wiki/index.php/ADVISE_Meta_Alpha_Tutorial
AEGIS Protocol Fuzzer	https://www.automatak.com/aegis/
Allium	
Attack scripts for IEC61850-MMS	https://project-sparks.eu/wp-content/uploads/2016/09/04-multi-stage-attack-scada-ids-belfast-workshop-20160826.pdf
Attack Tree with Sequential Conjunction	
Automated SCADA attack scripts	
Bettercap	https://www.bettercap.org/
Clingo 3.0.2	http://potassco.sourceforge.net/
CVE-search	https://github.com/cve-search/cve-search
DigitalBonds Network enumeration	https://github.com/digitalbond/Redpoint
ElasticStack	https://www.elastic.co/
Ettercap with IEC104 plugin	https://github.com/PMaynard/ettercap-104-mitm
FinkWinPP	http://www.ipcomm.de/product/FinkWinPP/en/sheet.html
Hugin Lite 8.3	https://www.hugin.com/index.php/hugin-lite/
IEC104 Application NSM SIEM	
IEC104 PCN TestBed	
NetLogo	https://ccl.northwestern.edu/netlogo/
OpenMUC	https://www.openmuc.org/openmuc/
PIA:FARA	https://github.com/AlexAtNet/nordic32
QTester104	https://sourceforge.net/projects/qtester104/
SCADA Anomaly Detection System (SANDS)	
SCADAStrangeLove	https://github.com/atimorin/PoC2013
Scapy Modbus	
Security Onion	https://securityonion.net/
SENAMI (IDS)	https://github.com/WilliamJardine/SENAMI http://eprints.lancs.ac.uk/81642/1/senami.pdf
SILK	https://tools.netsa.cert.org/silk/
SimaticScan (Vulnerability Scanner)	https://ewic.bcs.org/content/ConWebDoc/56473
SNORT	https://www.snort.org/
Tensorflow	https://www.tensorflow.org/
TRW-S	https://github.com/johannesu/stereo/tree/master/imrender/vgg/trw-s
Wireshark	https://www.wireshark.org/
Wireshark dissector for IEC61850-90-5	

One of the main issues concerning the feasibility of an open source tool repository centres on assurances about the validity of tools. It may be unrealistic to expect formal verification of all tools in the repository but some level of assurance should be provided. Some follow-up work should look at various certification standards such as Common Criteria and the various CESG schemes (CTAS and CCT Mark) to assess what might be practicable. Some related work has been done by the European Reference Network on Crititical Infrastructure Protection (ERNCIP) Thematic Group on Industrial and Automated Control Systems (IACS) who have looked at certification of individual IACS components (https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC102550_introduction-to-iccf_erncip-iacs-tg-onlineversion.pdf).

There is also the issue apparent in the RITICS table that there is less coverage in the respond and recover columns. This is something we saw in another piece of work for the CPNI iDATA programme on data exfiltration where there was poor coverage of recovery: http://security-centre.lancs.ac.uk/data-exfiltration.

Conclusions and Recommendations

We make the following recommendations:

1. It is worthwhile cataloguing the open source tools available to the UK OT community.

2. CISP could be a suitable platform for hosting the catalogue.
3. Some guidelines for inclusion in the catalogue should be developed, possibly similar to the policies for Kali Linux[2] or commercial stores such as Apple's.
4. Follow-up work could consider an approach to providing assurances of the quality of tools in the repository either through moderated user feedback or some more formal mechanism. However, this would require significant investment.

References

[1] https://www.gov.uk/government/news/three-universities-to-develop-16m-5g-test-network

[2] ETSI Open Source MANO (OSM), http://www.etsi.org/technologies-clusters/technologies/nfv/opensource-mano [5] ETSI Network Functions Virtualisation (NFV) Management and Orchestration, ETSI GS NFV-MAN 001 v1.1.1, December 2014, http://www.etsi.org/deliver/etsi_gs/NFVMAN/001_099/001/01.01.01_60/gs_NFV-MAN001v[4] ETSI Open Source MANO (OSM), http://www.etsi.org/technologies-clusters/technologies/nfv/opensource-mano

[3] ETSI Network Functions Virtualisation (NFV) Management and Orchestration, ETSI GS NFV-MAN 001 v1.1.1, December 2014, http://www.etsi.org/deliver/etsi_gs/NFVMAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf

[4] The JANET network, https://www.jisc.ac.uk/janet

[5] Emulytics at Sandia National Laboratories, B. Van Leeuwen, V. Urias, W. Stout, and B. Wright, MODSIM World 2015.

[6] A Survey of Security Tools for the Industrial Control System Environment, C. M. Hurd, M. V. McCarty, INL/EXT-17-42229, Revision 1, May 2017.

[7] http://www.etsi.org/technologies-clusters/technologies/cyber-security.

[2] https://docs.kali.org/category/policy