The Centre for Research on Engineering Software Technologies (CREST)
http://crest-centre.net
School of Computer Science, University of Adelaide

Summer Research Scholarships

Security by Design (Cyber Security+AI+Big Data)

List of the R&D challenges:

- **Challenge #1: Collaboration and Teamwork for CCOP**
- **Challenge #2: Intelligent Assistant for Executive Cyber Awareness**
- **Challenge #3: Metric recommendation based on organizational needs**
- **Challenge #4: Containerized application live updating with network-level services**
- **Challenge #5: Configurable Vulnerability Assessment in Docker Containers**
- **Challenge #6: Automatic coordination of software security patch management**
- **Challenge #7: Dependency analytics in software security patch management**
- **Challenge #8: Blockchain-based Tool for Security Patch Management**
- **Challenge #9: Automated security assessment for interconnected systems**
- **Challenge #10: Log file analysis and visual feedback generator**
- **Challenge #11: Security database mapping for meaningful mitigation**
- **Challenge #12: Modelling Support for Security of Operational Activities**
- **Challenge #13: Tool Support for Security by Design of C3i Systems**
- **Challenge #14: Comparison of AI (DL) methods for managing security patches**
- **Challenge #15 Protecting SDN of a C3I system from packet injection attacks**
- **Challenge #16 Evasion Attack on ML based Insider Attack Detectors**
- **Challenge #17 Accountable Artificial Intelligence (AI)**
- **Challenge #18 Securing Deep Leanring Based NLP Systems**
- **Challenge #19 Leveraging Deep Learning for Recommending Security Tools APIs**
- **Challenge #20 Human Decision-Making for Cyber Security**

Details:

Challenge #1: Collaboration and Teamwork for CCOP

Common Operational Pictures (COPs) have been used in the military domain as a powerful tool for gaining Situational Awareness (SA) and thus enabling appropriate decision-making in moments of crisis or attacks. Today, SA is also an essential part of the cybersecurity operations of many organisations, but particularly for Critical Infrastructures (CIs) and national agencies. A number of solutions have been proposed to enhance Cyber Situational Awareness (CSA) by means of Cyber Common Operational Pictures (Cyber COPs). A COP is defined as "a single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness".
Complete cyber situation awareness is implausible to achieve through interactions only between an individual analyst and their technology. Achieving complete situation awareness requires members of different teams and different organisational positions, working across

different work shifts to collaborate and share information with each other. Often each team member will have different, though perhaps overlapping, perspectives and hypotheses on the situation. In a complex and dynamic world, it is likely that two or more such perspectives will need to be combined to obtain complete SA that extends beyond a single analyst's knowledge. Unfortunately, there is a lack of technologies conducive to humans to collaborate, effectively communicate, and share information and knowledge with each other in the context of CCOP and CSA. The project's main aim is to enable people from different organisational teams and levels to share their knowledge and perspective in order to:

- collaboratively analyse alerts and observations related to the CCOP dashboard and;
- collectively make actionable decisions.

The expected outcomes for this research challenges are:

- Develop a functional prototype of this concept.
- Make the prototype usable for getting feedback from users on ways to improve the workflow and to identify additional requirements.

Challenge #2: Intelligent Assistant for Executive Cyber Awareness

Cyber Common Operating Picture (CCOP) comprises a set of metrics, coming from different security intelligence sources. One of the current means of displaying a CCOP is executive dashboards, which were carefully designed to display the right kind of metrics at an appropriate level of detail. Whilst dashboards can be tailored to individual organizations, or even individual executives, they can only narrow down the available information of the CCOP to a more manageable level instead of providing the very specific information that executives seek within a specific context. Moreover, when using these dashboards, executives need to examine and analyze the security status details themselves instead of having an assistant to offer them what they need and useful recommendations for making security decisions.
This research activity will explore the ways we can apply semantic modelling, logic reasoning, and information retrieval technique to retrieve and return the precise information that executives need within a context.

The key outcomes of will be:

- Develop a mechanism to understand natural language requests from executives and return an appropriate set of information from the CCOP model that satisfies the request.
- Integrate this mechanism into an open-source voice assistant platform such as Mycroft AI, Open Assistant, LinTO, Leon, etc.

Challenge #3: Metric recommendation based on organizational needs

Cyber Common Operating Picture (CCOP) comprises security metrics that reflect the cyber-health of an organization with respect to its historical performance and the industry standard. These metrics are populated with the data gathered through different security tools (e.g., SIEM, IDS, firewalls) as well as OpeN Source InTelligence (ONSIT) sources (e.g, Socail media platform or Vulnerability registries). Each organization has different level of access to these sources. Moreover, they have different requirements in terms of the metrics to be included in the CCOP and the relative importance of these metrics.
Given the large number of metrics that can be used for CCOP, it is difficult for organizations to map their current capabilities, in terms of the security intelligence sources that they have, to

the metrics. Moreover, the requirements of an organization might simply be insatisfiable given their existing capability. Thus, organizations need suitable recommendations about either extending their capability or modifying their requirements. However, there is little support for automatically recommending suitable metrics for an organisational specific CCOP.
This research activity aims at applying Artificial Intelligence (AI) techniques, such as semantic reasoning and collaborative filtering, to develop an intelligent recommendation mechanism that matches organizations's needs/preferences with suitable metrics in a CCOP model for extending capabilities or modifying requirements.

The expected outcomes will be:

- A Prototype of Intelligent Tool for Security Metrics Recommendation Services

Challenge #4: Containerized application live updating with network-level services

Software live updating can occur at different granularity, such as instruction-level, function-level, process-level, etc. This research challenge will focus on container-level software updating. Minimising or completely eliminating service downtime associated with vulnerable container updating is necessary for highly critical applications. An automated and transparent way to manage run-time updating of vulnerable containers would be beneficial for such critical environments. Traditional container updating approach involves multiple steps. Namely, a) stopping the existing vulnerable container, b) preparing a new updated/patched container, c) starting the newly created container. However, with the growth of modern software in terms of size and complexity leads to increased container creation and preparation times. Thus, in order to minimise the downtime of the service provided by a container, this research effort would focus on investigation of seamless downtime-free client migration from vulnerable to updated containers.

The expected outcomes for this research challenges are:

- A prototype tool for managing dynamic container updates at the network level.

Challenge #5: Towards Configurable Vulnerability Assessment in Docker Containers

Security is considered as one of the most challenging factors for migrating Small and mid-size enterprises (SMEs) services and applications to the cloud (containers). SMEs employ one or more open-source tools without properly configuring them to fit in appropriate context. This results in several issues: 1) waste of computing resources, 2) improper accuracy in vulnerability detection, 3) misidentification of security events. This challenge aims to explore the potential of multi-tools approach on vulnerability assessment of virtualised infrastructure.

The planned activities and deliverables are:

- Exploring the strengths and weaknesses of the performance and accuracy of existing vulnerability scanning tools in the context of containers.
- Identifying and using mechanisms for integrating and orchestrating various existing container security tools into a coherent container security enabling flow.
- Developing a multi-tools approach for automatically detecting vulnerabilities and configuring Docker containers.

Challenge #6: Automatic coordination of software security patch management

Keeping machines up to date by applying the critical security patches on time is critical security hygiene. Enterprise software security patch management involves the process of applying security patches to large and complex organization mission systems (i.e., Cyber Physical Systems or Industrial Control Systems), which is a challenging task. Efficient coordination of the tasks with multiple stakeholders of conflicting interests is a daunting task that could easily be neglected because of the inherent complexity and lack of technological support yet a critical success factor to security patch management. A typical manual approach to this problem would use discussion with several stakeholders to argue the different considerations and reach a consensus. This research challenge will analyse the activities, tasks, and artefacts generated and shared for supporting coordination of security practitioners for security patch management tasks in large and complex organizations. The research activities will identify the needs of automating the coordination tasks for better and timely decision making in the following areas:

- collaboratively analyse alerts related to patch application;
- gain and share situational awareness of the context of the patch being applied and;
- collaboratively make actionable decisions

The task/expected outcome is to:

- Develop a prototype tool for improving automation support of coordination in software security patch management process of Mission Systems

Challenge #7: Dependency analytics in software security patch management

Timely security patch installation in organizations is often impeded by the necessity to manually test and install patches to avoid the risks of unexpected system breakdowns caused by faulty and malicious patches. These manual tasks are often associated with misconfiguration and erroneous responses and consume a significant amount of time and human effort. Dependency and compatibility concerns cause severe problems for automation in these security patch management tasks. The research challenge is to evaluate suitable automation approaches for supporting security patch management. The R&D effort will look into Artificial Intelligence (AI) approaches' suitability for assessing patch dependencies and visualising the results. The automated detection and visualisation of the dependency of patches will help investigate the pre-requisites for patch application and identify any particular outliers (missing patches/patch information) that would streamline the patching workflow. The developed tool will also assist practitioners in decision-making for timely patch installation.

The expected deliver is:

- An Intelligent approach and tool for automatically track and visualise the patch dependencies for supporting patching decisions.

Challenge #8: Blockchain-based Tool for Security Patching Lifecycle Management

Software security patching plays a critical role in thwarting cyber security attacks. A security patch involves a change applied to the software code to correct the security weakness discovered by a vulnerability. Software security patch lifecycle management refers to the

application process of security patches to address the identified security vulnerabilities in the software code. Enterprise security patch management involves the process of applying security patches to large and complex organization systems with hundreds of servers, multiple operating systems, and heterogeneous applications, all interconnected through networking devices which is a challenging task. It important to have an automatic and trustworthy support infrastructure for the activities and artefacts of the software security patch lifecycle management.

This research challenge is aimed at exploring the suitability and viability of leveraging distributed ledger technologies to automate the process of software patch management in mission critical system, e.g., industrial control systems or healthcare systems. The research activities will design and implement a prototype for a blockchain enabled tool for supporting the software security patch lifecycle management.

The expected deliver is:

- A blockchain-enabled App for managing security patches from generation to application

Challenge #9: Automated security assessment for interconnected systems

Modern command, control, and communication systems are highly interconnected supported by advanced networks and Internet of Things (IoT). The hypberconnectivity of the such systems and the software underpinning exposes them to a large number of security vulnerabilities, which leads to an increase in the volume and sophistication of cyberattacks. These attacks potentially disrupt the cyber safety and operation of many organisations and enterprises with millions of users. Assessment of these cyber risks is important to prioritise to fix the ones that would have the highest impact on a system. The current techniques are mostly expert-based with manually crafted rules, and thus do not scale well to new vulnerabilities. The proposed research challenge aims to automate the security assessment process using Artificial Intelligence enabled technologies. The envisioned solution will support evaluation-based security modelling to analyse vulnerabilities in complex and dynamically changing computer systems and interconnected networks.
The expected deliverables of the project are:

- Enrichment of graphical security models with a variety of security metrics extracted from software vulnerability assessment
- Automated security analysis of the interconnected systems using a combination of machine learning-driven software vulnerability assessment and graphical security modelling techniques

Challenge #10: Log file analysis and visual feedback generator

Command, control, and communication systems are considered a type of Systems-of-Systems (SoS). Such systems are complex distributed and concurrent systems, bring many benefits, but also raise many security challenges. With the scalability and robustness characteristics, these systems are widely deployed to support mission critical processes and business functions such as search and rescue tasks, smart buildings, health care and transportation. However, heterogeneity, highly distribution and emergent behaviours of SoS also significantly increase their exposure to a large number of security vulnerabilities. A vulnerability in an individual constituent system (CS) usually makes that CS the weakest link for the whole SoS in cae of

cascading attack resulting from the interactions among the CSs. Moreover, SoS modification and vulnerability mitigation would be expensive when a system becomes mature. Thus, the security solution at the early stage becomes a critical challenge. To address this problem, our research has introduced a model-driven based method for designing and analysing security of Systems-of-Systems Security (SoSSec). The proposed research challenge will provide a tool support for automatically analyse and visual the log files generated based on the security model developed using the SoSSec. The envisioned automated analysis/visualisation tool will make the security vulernability models easy to understand for system designers.

The deliverables for addressing this challenge are:

- Automatically analyse the log file of execution/simulation results and extract the information, such as agents (CS), vulnerabilities, pre and post-conditions, and interactions/messages of the agents.
- Generate visual feedback by drawing the cascading attack diagram using model driven engineering techniques.

Challenge #11: Security database mapping for meaningful mitigation

When a vulnerability is found, the security architects need to take necessary actions to mitigate the attacks. To fix the system vulnerability, the architects need to know the root and the reason for the problem. Therefore, weaknesses and attack patterns can be employed to explore system vulnerabilities. With this information, the proposed security solutions and patterns can be provided to the architects as a guideline and references. This project explores the relationship between the vulnerabilities and weaknesses of the SoS, attack patterns, and potential mitigations. Based on the proposed mitigations, systems can return the security solution suggestions.
The expected outcomes for addressing this challenge will be:

- ML/NLP techniques for automatically linking the relevant CVE, CWE, CAPEC and security centric patterns.
- A web-based system to visual the mapping for support designers in understanding and mitigating security vulnerabilities by suggested the relevant security patterns.

Challenge #12: Modelling Support for Security of Operational Activities of C3I System

Command, Control, Communication, and Intelligence (C3I) system is a kind of System of Systems (SoS) that is increasingly leveraging ICT infrastructures. As C3I systems are becoming more pervasive in military and law enforcement organizations that are usually involved in search and rescue missions. There is a high risk of cyber-attacks on such systems. Given that it is inevitable that a cyber-attack will happen at one stage or another, it is important to be ready for promptly responding to the attack. This research challenge aims at providing tooling support for modelling the security of operational activities of C3i systems, particularly in the search and rescue mission domain. The provided modelling will underpin the identification of the response activities that is how the C3i system will response when it is under an attack. The availability of security modelling tool will greatly benefit the designer of C3i system in determining, planning, and testing the response of C3i system to various kinds of attacks at the design stage. The proposed work will leverage SysML based an Open Source tool, Papyrusm, semantic modelling, natural language processing and model-driven engineering for providing security modelling of the operational activities of C3I systems as SoS in a sub-set of search and rescue mission domian.

The expected outcome for addressing this challenge will be:

- A tool for modelling security of operational activities of C3I System.

Challenge #13: Tool Support for Security by Design of C3i Systems

This research action will build a design space for supporting security by design paradigm for next generation Command, Control, Communication and Intelligence (C3i) systems. Such design space is needed for building and/or improving organizational and individuals' competencies in embedded security by design paradigm in the design and evaluation phases of large-scale mission- and business-critical software intensive services. The research activities will identify and critically analyse the requirements of an integrated body of knowledge consisting of design principles, guidelines, patterns, reusable meta-models, and artefacts for collaboratively designing and evaluating secure C3i systems. The envisioned R&D activities will leverage intelligent approaches and tools for enabling the populating and usage of the design space for identifying, considering and incorporating security centric approaches in desiging and evaluating a C3i system. The developed tool will also be evaluated for customization to individual knowledge and preferences and the total cost of ownership perspectives.

The expected outcome from this research action will be:

- An intelligent tool for security by design of C3i software systems.

Challenge #14: Battle of the giants: Comparison of deep learning methods for managing security patches

Open-Source Software (OSS) is at the backbone of many large systems that are being used by millions of users worldwide. However, OSS is prone to ever-increasing security vulnerabilities, which can lead to huge risks of losing data and money for both organisations and users. It is important to apply vulnerability patches as soon as they are released, but these patches usually go undetected in code commits, which would delay the patch application. Code and artefacts of commits can be analysed to assist the retrieval of missing security patches. Recently, many deep learning and natural language processing techniques have been proposed to represent text for various applications. This project aims to investigate state-of-the-art deep learning techniques to extract commit features to predict patches for different types of vulnerabilities.

The expected deliverables of the project are:

- Implementation of state-of-the-art deep learning text-based feature extraction methods
- A systematic comparison of different feature extraction methods to predict security patches

Challenge #15: Protecting SDN of a C3I system from packet injection attacks

The networking architecture of the software-defined network (SDN) employed in a C3I infrastructure makes it easy to target the packet injection attack. The attacker can affect the services and performance of the SDN controller and can overflow the capacity of the SDN switch devastatingly, by injecting the malicious packets into the SDN network. That ultimately stops the network from functioning in real-time, leading to the situation of network breakdown. Thus, the packet injection attack is a primary threat to the software-defined enterprise network

of a C3I infrastructure, in which continuous connectivity and real-time network functioning are two essential requirements.

In this project, we will design and implement a packet injection attack mitigation technique that will detect and immediately block the malicious data packet flow at the gateway switch of the software-defined enterprise network of a C3I infrastructure. In our project, we want to guarantee that the core network does not stop functioning due to the packet injection attack. We want to shift the computational functionality of the controller to the edge switch, using the P4 based implementation, to thoroughly reduce the workload of mitigating the edge controller's packet injection attack.

The outcomes of this project will be:

- A tool for analysing SDN for protecting from packet injection attack.

Challenge #16: Evasion Attack on Machine Learning based Insider Attack Detectors

Insider threats are one of the most challenging attack models to deal with in practice. According to a recent report1, 30% of all cybercrime incidents were suspected to be committed by insiders and the overall cost of insider threats is rising, with a 31% increase from $8.76 million in 2018 to $11.45 million in 2020. Machine Learning (ML) based approaches are frequently used to detect insider attacks (see attached survey paper). Most of these approaches use anomaly detectors such as Hidden Markov Model (HMM), Gaussian Mixture Models (GMM), One Class SVM (OCSVM) and Isolation Forest Tree (IFT). In Deep learning methods, recently LSTM, Multistate LSTM and CNN and Autoencoders are used to detect insider threat with an average accuracy of more than 90%. However, there is no study done on testing the security of these detectors and assessing their practical applicability are against adversarial attacks such as Poisoning and Evasion. The goal of this project to assess the test-time security and practical applicability of these systems. To achieve this goal, this project aims to model an evasion attack against ML-based insider attack detection systems.

This project will answer following research questions

- Which models are more robust (hard to fool)? Based on time, number of perturbations and number of queries to the model?
- How transferrable adversarial examples generated by different models?
- Examining the impact of adversarial examples generated against a target model on other models. Studying which model adversarial examples are more transferrable.
- Identify the most sensitive features that impact the performance of all the models?

Challenge #17: Accountable Artificial Intelligence (AI)

Deep Learning-based models (DL) are increasingly adapted in security-sensitive applications such as Spam and toxic content detection. However, the datasets on which the models are trained are obtained from people, online sources or third-party such as threat intelligence feeds such as Phish Tank or social media. The end-user usually has some control over these data sources and an adversary can use this for poisoning the datasets.
DL models trained over poisoned dataset can shift the decision boundary of the model in accordance with the adversary will. A popular real-world example of poisoning the attack is Microsoft Tay. Tay was an artificial intelligence chatterbot that was originally released by Microsoft Corporation via Twitter on March 23, 2016; it caused subsequently controversy when the bot began to post inflammatory and offensive tweets through its Twitter account,

forcing Microsoft to shut down the service only 16 hours after its launch. According to Microsoft, this was caused by trolls who "attacked" the service as the bot made replies based on its interactions with people on Twitter.

This project aims to detect Poisoning attack on Spam and Phishing detectors. This will be done by first generating a log file to assess the security of DL systems by executing a list of poisoning attacks on spam and phishing detectors and logging the critical security events. After that, the generated log file will be used to develop a Machine Learning model that automated analyse the log files to detect poisoning attack against DL systems.

The expected deliverables of the project are:

- Knowledge and understanding of types of approaches to detecting poisoning attacks on spam and phishing DL models.
- A DL based tool for automating the detection of poisoning attacks

Challenge #18: Securing Deep Learning based NLP Systems

Deep Learning (DL) models have attained remarkable success in several tasks such as classification and decision analytics. However, DL models, are often sensitive to Adversarial Examples (AEs). AEs consist of transformed original training data samples that preserve the intrinsic utilities of the ML solutions, but influence target classifier's predictions between the original and the modified input. A recent popular and powerful attack against DL based NLP systems is synonym substitution, where a transforming a word in the original example with its semantically similar synonym changes the prediction of the target model. For example, transforming "The Fish N Chips are excellent" to "The Fish N Chips are first-class" changes the target model output from positive to negative.

This project aims to create a robust encoding method and train a robust model that is resilient to synonym substitution attack at test time. The NLP datasets that will be used to evaluate the method will be security critical datasets Enron (for spam email detection), Toxic comments (Kaggle jigsaw), Yelp (Positive/Negative reviews) and Fake News datasets. Three state-of-the-art synonym- substitution attacks will be considered to generate AEs against these systems.

The goals of this project will be achieved by answering the following questions:

- How effective Robust_Encoding is against synonym substitution attack?
- How well Robust_Encoding perform in comparison of state-of-the-art adversarial training?

The expected deliverables of the project are:

- The outcome of this project would be a robust encoding method to develop robust DL models against synonym substitution attack.

Challenge #19: Leveraging Deep Learning for Recommending Security Tools APIs

A wide variety of multi-vendor disparate security tools are used in a Security Operation Center (SOC) of an organization to defend and respond against emerging cyber-security attacks. Security Orchestration Platform (SecOrP) aims to integrate the activities performed by diverse types of security tools to execute an incident response process. While using this high number of diverse security tools in SecOrP, SOC team members require APIs from the varied tools to perform their activities. Searching appropriate APIs of a distinct tool for their specific task is challenging and time-consuming. Besides, in security tool domain the user contributed data

sources such as Stack Overflow and GitHub are not always available. Hence, the target of this project is to recommend API from documentation rather than depending on user contributed data sources. Recently, many deep learning and natural language processing techniques have been proposed for various text-based applications such as question answering, sentence classification etc. This project aims to investigate state-of-the-art deep learning techniques to recommend API for diverse security tools from documentation and provide an interface for API recommendation.
The expected deliverables of the project are:

- Implementation of Deep Laerning approaches for answering free form security tool API related query.
- Comparative analysis of DL approaches to recommending security tool API.
- An interface for answering security tool API related query.

Challenge #20: Human Decision-Making for Cybersecurity

Most people receive dozens of emails that contain attempts to phish their personal data each week. Phishing attacks cost approximately $10 billion each year, and incidence of coordinated phishing attempts directed to individuals and businesses is expected to increase. Safeguarding sensitive material and protecting personal finances against fraud relies on more than just protective software, but also on human behaviour.

This project investigates human decision making and learning processes in the context of targeted phishing emails. We are interested in identifying (i) visual and textual cues that may signal the presence of a phishing attack in simulated emails, (ii) the behavioural and cognitive processes that occur after correctly identifying, incorrectly identifying, or failing to identify such cues, (iii) methods by which such behavioural and cognitive processes may be trained in such cases where humans fail to identify cues, and (iv) quantifiable metrics that allow organisations to evaluate the efficacy of anti-phishing training programs in their staff.

The expected deliverables from the project are:

- A body fo knowledge about behavioural and cognitive processes that might be used to measure positive and negative phishing outcomes.
- Design and experiment for testing the efficacy of cueing participants in phishing email simulations based on the findings of that review.