Platforms EOI: Platform-as-a-Service for Cybersecurity Applications in Industry 4.0 Networks

Project title

Platform-as-a-Service for Cybersecurity Applications in Industry 4.0 Networks

Field of Research code(s)

- 08 INFORMATION AND COMPUTING SCIENCES
- 09 ENGINEERING
- 10 TECHNOLOGY
- 17 PSYCHOLOGY AND COGNITIVE SCIENCES

EOI Lead Name

Dr Nour Moustafa

EOI lead Research Group

Dr Nour Moustafa - School of Engineering & Information Technology, UNSW Canberra Cyber

EOI lead Organisation

University of New South Wales @ADFA – Canberra

EOI lead Email

Collaborator details

<table>
<thead>
<tr>
<th>Name</th>
<th>Research Group</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr Benjamin Turnbull</td>
<td>School of Engineering &amp; Information Technology, UNSW Canberra Cyber</td>
<td>University of New South Wales @ADFA – Canberra</td>
</tr>
<tr>
<td>Dr Timothy Lynar</td>
<td>School of Engineering &amp; Information Technology, UNSW Canberra Cyber</td>
<td>University of New South Wales @ADFA – Canberra</td>
</tr>
<tr>
<td>Dr Elena Sitnikova</td>
<td>School of Engineering &amp; Information Technology, UNSW Canberra Cyber</td>
<td>University of New South Wales @ADFA – Canberra</td>
</tr>
<tr>
<td>Professor Monica Whitty (Chair of Human Factors in Cyber Security)</td>
<td>School of Culture and Communication</td>
<td>University of Melbourne</td>
</tr>
<tr>
<td>Dr Seyit Camtepe</td>
<td>Distributed Systems Security</td>
<td>Data61 (CSIRO)</td>
</tr>
<tr>
<td>Dr Amin Beheshti</td>
<td>Department of Computing</td>
<td>Macquarie University</td>
</tr>
<tr>
<td>Dr Ibrahim Radwan</td>
<td>School of Information Technology and Systems</td>
<td>University of Canberra</td>
</tr>
<tr>
<td>Superintendent Frank Schiliro</td>
<td>Protection Operations</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>Associate Professor Kim-Kwang Raymond Choo</td>
<td>Colleague of Business and Cyber Security</td>
<td>University of Texas at San Antonio (USA)</td>
</tr>
</tbody>
</table>
### Project description

The project will develop an Industry 4.0 cybersecurity Platform-as-a-Service to solve the current challenge of protecting physical and network systems. Since industry 4.0 is the fourth revolution of computing and manufacturing to form smart systems, its complex nature produces new cyber threats.

The platform will integrate current open-source tools, including the tools of Security Onion and Kali. This platform, freely accessible to end-users, will be a web-based system for cybersecurity researchers to experiment and enhance usability, with securing Industry 4.0 implementations. These outcomes will positively impact cybersecurity nationally and globally, enhancing the Australian cybersecurity ecosystem.

### Existing technology

#### Adopt

The project will adopt open-source and existing tools developed and used at the UNSW Cyber Range and IoT Labs and by collaborators. Tools will be accessible to end-users via a public website or remote API. The tools that will be adopted in three-years are discussed as follows:

**Year 1:**
- Data logging, monitoring and management.
- Machine learning and human factor techniques.

**Year 2:**
- Intrusion detection and prevention solutions.
- Capture The Flag (CTF) technologies.

**Year 3:**
- Digital forensics tools.
- Security of computer vision applications based Deep Learning.

#### Adapt

Network security tools will require adaptation or configuration to be suited to Industry 4.0 environments. Additionally, the interconnection of these tools will also be considered. This will include the writing of additional collection and analysis algorithms, for effective integration. New algorithms generated will be released to the cybersecurity research community.

The project will utilise a layered approach to integrate the multitude of tools necessary. This approach will adapt existing Artificial Intelligence algorithms to allocate suitable security services to the layers of Industry

#### Build

The platform will build the following five components, free for end-users:

1. An intelligent service and group-based policy which will be used to disseminate knowledge on current threat vectors.
2. Automated configuration to open-source security solutions, involving intrusion detection and prevention, firewalls, and intelligence, for IoT servers and services.
3. Infrastructure-as-code Industry 4.0 simulation deployment templates.
4. Real-time monitoring and reporting showing active incidents.
5. Integration of machine learning into the real-analysis of the platform.

### Anticipated requirements

#### Annual funding

$100,000 - $199,000

#### Proposed length

3 years

### Other information

#### Other information you wish to provide

The team has proven the capability of the following:
- Winning and delivering research grants such as ARDC grant, US Naval Research Labs, CyberCRC;
- Creating benchmark datasets such as ToN_IoT (ARDC), UNSW_NB15, Bot_IoT; and
- Developing cybersecurity techniques such as threat models, intrusion detection, privacy preservation.

The team's outcomes have been widely used throughout the world in academia and industry. Based on their successful track record, the outcomes of this project will be widely used for addressing various security challenges.

<table>
<thead>
<tr>
<th>Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>I agree to the terms</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>