International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2020)
in conjunction with SecSE 2020 Workshop
June 15-17, 2020
Dublin City University, Dublin, Ireland
https://www.c-mric.com/cs2020

Theme: Advancing a multidisciplinary approach to Cyber Security.

The submission deadline is 26th January 2020

We are pleased to invite you to submit a paper to the IEEE Technically Co-Sponsored (TCS) International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2020), an international refereed conference dedicated to the advancement of Cyber Security, information security, network security, application security and business transformation of digital services, and the protection of public digital services, especially high value bearing online services.

The aim of the Cyber Security 2020 is to encourage participation and promotion of collaborative scientific, industrial and academic inter-workings among individual researchers, practitioners, members of existing associations, academia, standardisation bodies, and including government departments and agencies. The purpose is to build bridges between academia and industry, and to encourage interplay of different cultures.

Cyber Security 2020 invites researchers and industry practitioners to submit papers that encompass principles, analysis, design, methods and applications. All submitted papers are independently peer-reviewed.

The conference proceedings will be submitted for consideration for listing in the IEEE Xplore Digital Library and other reputable bibliographic indexes.
The organisers will accept registration of up to 5 IEEE UK&I Student and YP Members at 75% discounted rate, and will offer up to 20% registration discounts for all IEEE, BCS, IET & IISP members.

Details

Cyber Security 2020 is co-located with other conferences as part of Cyber Science 2020.

- **SecSE 2020 Workshop** will be presented at the conference.
- **Posters & Presentations** will be presented at the conference.
- **Industry track** is available for discussing and publishing pilot and proof of concepts (PoC).
- **Work in Progress track** is available for preliminary work.
- **Research Ideas track** is available for ideas in early stages assessment.
- **PhD Seminar track** is available for discussing and publishing synopsis of early PhD research.

Submission Deadline

Deadline for all paper submissions, that is, both **full papers** and **extended abstracts** for Poster, WIP, PoC, Research Idea and PhD Seminar presentations is 26th January 2020.

All Industry track, Work in Progress track, Research Ideas track and PhD Seminar track will be published in the conference proceedings. Interested participants, please submit your proposal using the online submission system hosted by [EasyChair Conference Portal](#).

Submission Instructions

Both long (8 pages max., roughly 8,000 words) and short (4 pages max., roughly 4,000 words) paper submissions should be written in English and be **submitted electronically** via the EasyChair Conference System. Submission file formats are PDF and Microsoft Word using the C-MRiC Word/PDF templates that can be found at the corresponding [C-MRiC website](#).

Authors wishing to present a Poster, Industry Proof of Concept (PoC), Work in Progress (WIP), Research Ideas & PhD Seminar may submit a 2-page extended abstract using the [online submission systems](#) hosted by EasyChair Conference System, which, if accepted, will appear in the conference proceedings.

Topics of Interest

Original papers are invited on recent advances in Cyber Security, Online Services, and Protection Mechanisms for Digital Services. The topics in **Cyber Security 2020** include but not limited to:

**Cyber Security**
- Information Security
- Computer Network Security
- Application Security
- Web Services Security
- Mobile Security
- Protective Security
- Software Security
- Wireless & Sensor Network Security
- Software Coding Security
- Barcode Scanner Security
- Security in Middleware, Interface and Interaction
- Security Services in Authentication, Authorisation, Accountability, Automation, Availability, Integrity and Non-repudiation
- Security Management
- Security Operations
- Digital Trust and Reputation
- Geographical Location (IP Geo-location) and Cyber Travel

**Digital Services**
- Web Services
- Internet Banking
- E-Booking
- Cloud Computing
- E-Government
- Electronic Commerce
- Citizens Public Online Services
- Mobile Commerce
- E-Postal Services
- E-Health
- Online & Virtual Education
- E-Learning
- Web Chats
- Secure Protocols, Coding and Development
- Security Principles, Theory and Analysis
- Security Policy, Standards and Procedures
- Security in Business Processes
- Security Enforcing Function (SEF) Gateways
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Firewalls
• Geospatial Intelligence Networks (Centralised, Distributed & Hybrid)
• Policy, Legal, Legislation & Compliance
• Security Standardisation
• Law, Legal and Ethics

Protection of Digital Services
• Protection of Business Information Systems
• Protection of Online Services
• Energy Sector Security, Oil and Gas and SCADA Networks
• Protection of E-Currency & E-Money Transactions
• Security, Trust, Privacy
• Security in Online Gaming Systems
• Security in e-Government and Electoral Systems
• Content Security
• Protection of Public Online Content Distribution Systems
• Secure practices, processes and procedures in Public Online Services
• Cryptography - PKI, HSMs, Symmetric and Asymmetric Crypto, Crypto Custodian & Crypto Standards and Practices
• Digital Forensics and Investigations
• HoneyPots and Honey Nets
• Critical National Infrastructures (CNIs)
• Critical Network Systems (CNS)

Security Operations Centre
• Cyber Security Operations Centre (CSOC)
• Joint Security Operations Centre (JSOC)
• Strategic Security Operations Centre (SSOC)
• Virtual Security Operations Centre (vSOC)
• Cyber SOC Designs
• SOC Design Architecture Patterns
• Threat Intelligence
• Fusion Centre & Cyber Centre
• Operations Monitoring Centre
• Security Monitoring
• Transaction Monitoring
• Web Fraud Detection (WFD)
• Incident Management
• Cyber Incident Response
• Anomaly Detection
• Heuristic Learning
• Intrusion Detection
• Computer Misuse and Abuse

Network Operations Centre
• Functions of NOCs
• Design Principles
• Design Architectures and Design Requirements
• Monitoring and Analysis
• Coordination
• Incident Response & Handling
• Incident Management
• Operations Management
• Models of Operations
• System Interfaces and Automation
• Asset Management
• Data Leak Prevention (DLP)
• Denial and Distributed Denial of Service (DDoS)

Remediation and Optimisation
• Remedial Action Plans
• Risk Management
• Business Process Optimisation
• Security Management
• Policy and Standards Compliance
• Vulnerability Management
• Accreditation & Assurance
• Security Assurance and Certification
• Process, Procedure and Standardisation
• Global IT Outsourcing
• Supplier Management

Blockchain
• Cryptocurrency
• Bitcoin & Bit-everything
• Blockchain in Manufacturing
• Blockchain in Banking & Financial Systems
• Blockchain in Aviation
• Blockchain in Pharmaceuticals
• Blockchain in IoT
• Blockchain in Defence

STEM & Cyber Security Education
• Cyber Security in childhood education
• Code - Teaching Education for Kids, Teens and Colleges
• Secure by Code
• Secure by Design
• Secure by Default
- Blockchain in Cybersecurity Operations
- Blockchain in Publications
- Blockchain Education Curriculum

**Automation and Robotics**
- Autonomous & Self-driving
- Self-Healing
- Domestic Assistance
- Autonomous Healthcare and Assistance
- Industrial Manufacturing Robotics
- Search and Rescue Operations
- Robotics Process Automation (RPA)

**Security Operations Centre Management**
- Design Requirements
- Principles and Operations
- SOC Security Operating Procedures (SOC SyOPs)
- Architectures and Design Considerations
- Implementation of SOC Centres
- Monitoring and Security Analysis
- Security Information and Event Management (SIEM)
- Log Analysis & Analytics
- IDS/IPS & Firewall Administration
- Alerting and Event Prioritisation
- Log Management
- Analysis Tools and Techniques
- Incident Triage
- Incident Analysis, Management, Reporting and Escalation
- Management Reports and Management Information (MI) Reports
- Coordination and Containment
- Collaboration and Incident Investigation
- National CERT Liaison
- Model of Operations
- Intelligence Interfaces and Threat Intelligence Feeds
- Asset Management, Prioritisation and Categorisation
- Investigation & Forensic Readiness

**Application and Container Platform Security**
- Application and Container Platform (ACP)
- Container Technologies
- Security Concerns Associated with Container Technologies
- Apps
- Cultural and Technical Processes for Managing Containers & Apps
- Microservices
- Kubernetes
- Docker
- Cloud Computing
- Container Technology Architecture
- Approaches to Management, Maintenance and Processing of Containers, Apps and HostOS
- CI/CD
- Risks & Issues
- OWASP
- Open Web Application Security

**Vulnerability Management**
- Vulnerability Scanning, Ranking and Prioritisation
- IT Health Checks (ITHC)
- Vulnerability Analysis
- Vulnerability Management
- Asset Management & Configuration Management Database
- Asset Classification, Categorisation & Prioritisation

**DevSecOps**
- Virtualisation (Network, OS, Container & Apps)
- DevOps
- API
- HostOS
- Microservices security
- Agile and Scrum Methodologies
- Issues, practices and challenges
Important Dates

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended Abstracts submissions for Posters / Demo, Work in Progress</td>
<td>January 26, 2020</td>
</tr>
<tr>
<td>(WIP), Industry Proof of Concepts (PoC), Academic Research Ideas &amp; PhD Seminar presentation</td>
<td></td>
</tr>
<tr>
<td>Full Paper Submissions (Long and Short papers)</td>
<td>January 26, 2020</td>
</tr>
<tr>
<td>Notifications of Special Tracks, Extended Abstracts &amp; Full Papers</td>
<td>March 24, 2020</td>
</tr>
<tr>
<td>Acceptance / Rejection</td>
<td></td>
</tr>
<tr>
<td>Conference Dates</td>
<td>June 15-17, 2020</td>
</tr>
</tbody>
</table>

Best Papers

- The best paper of each section will be selected, and their author(s) will receive a corresponding Award Certificate.
- Authors of the Best papers and 20%-25% papers presented at the conference may be invited to adapt their papers for their publication in one of the special issues peer reviewed journals.

Sponsors/Partners

[Images of sponsor logos]

Previous Conferences

1. [Cyber Security 2019](#): International Conference on Cyber Security and Protection of Digital Services, held at the University of Oxford, UK on 3-4 June 2019
2. [Cyber Security 2018](#): International Conference on Cyber Security and Protection of Digital Services, held at the Victoria, Wellington and Buchanan Suites, Grand Central Hotel, Glasgow, Scotland, UK on 11-12 June 2018
3. [Cyber Security 2017](#): International Conference on Cyber Security and Protection of Digital Services, held at the Ampthill and Holborn Suites, De Vere Grand Connaught Rooms, London, UK on 19-20 June 2017
5. [Cyber Security 2015](#): International Conference on Cyber Security and Protection of Digital Services, held at the Hotel Russell, Central London, UK on 7-8 June 2015

Thanks,
Cyber Security 2020 Conference Co-Chair