Foundation for Science and Technology-debate

"How can UK intellectual property be better protected from cyber theft".

Queen's University Belfast

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Professor John McCanny CBE FRS FREng

Research Challenges

- Everyday we create 2.5 quintillion bytes of data = 10^{18} or 2.5 million trillion bytes
- 90% of world's data today apparently created in the past two years alone
- "Internet of Things" – 50 billion interconnected devices by 2020
- 6% of the UK's GDP is enabled by the Internet with this continuing to grow
- 93% of large corporations and 76% of small businesses reported a cyber breach last year
- Future systems must provide ability to extract high levels of meaningful information whilst providing assured levels of PRIVACY and TRUST

UK University Research in Cybersecurity

- RCUK funding currently £82M across 96 research projects
- Significant other funding for other national and international sources including major multinationals, EU FP7, other government sources etc.

11 EPSRC/GCHQ Academic Centres of Excellence

- Imperial College London
- Lancaster University
- Newcastle University
- Queen's University Belfast
- Royal Holloway, University of London
- University College London
- University of Birmingham
- University of Bristol
- University of Cambridge
- University of Oxford
- University of Southampton

Source: RCUK Cybersecurity Research and Innovation for a More Secure Britain 2013

UK University Research in Cyber Security

EPSRC-GCHQ Research Institutes

•Science of Cyber Security – involves seven universities, led by UCL

•Automatic Programme Analysis and Verification – Imperial

Doctoral Training Centres (~ 60 PhDs over 7 years)

•Royal Holloway, University of London

•University of Oxford

Innovation and Knowledge Centre (IKC)

•Queen's University Belfast

•Funded by EPSRC, TSB, InvestNI and industry

•£30M+ over initial 5 years , now 80+ people

•6PhDs graduated, 25 in pipeline

Source: RCUK Cybersecurity Research and Innovation for a More Secure Britain 2013

Open Innovation / Tiered Membership

Full Members

ALTERA, BAE SYSTEMS, THALES, CISCO, Roke, Q1 Labs (Total Security Intelligence), IBM, QinetiQ, Infosys, McAfee

Associate Members

QOSMOS, RepKnight, titanic systems, tyco, NETRONOME

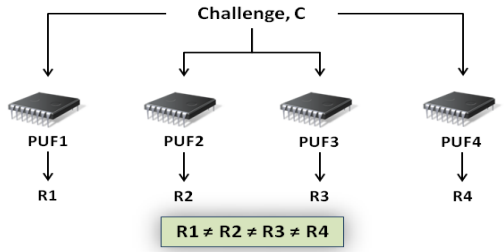
Government Agencies

GCHQ, CPNI (Centre for the Protection of National Infrastructure), [dstl], Ministry of Defence, Home Office, EPSRC, Technology Strategy Board (Driving Innovation), Invest Northern Ireland

Physical Unclonable Function (PUF)

A PUF (*Physical Unclonable Function*) is a circuit that uses manufacturing process variation to generate a unique digital fingerprint

Since every chip is different no two chips give the same response when supplied with the same challenge



Can be used to uniquely identify IP and detect counterfeit devices

Applications:
•*IP Protection/Anti-counterfeiting, Secure Key Storage, Key Generation, Tamper Evidence*

Sample Application

PUF & Public Key Infrastructure (PKI)

CSIT's **PUF** is being integrated into **Vehicle to Grid (V2G)** Communication Interface (ISO/IEC 15118-2) for use in an Electric Vehicle (EV) charging system to improve the security and **detect cloned or tampered devices** within an EV charging infrastructure.

Can also be used in Smart Meters

More generally for anti-counterfeiting and IP protection

Network Security Systems

Network Security
- IDS / IPS
- DDoS mitigation

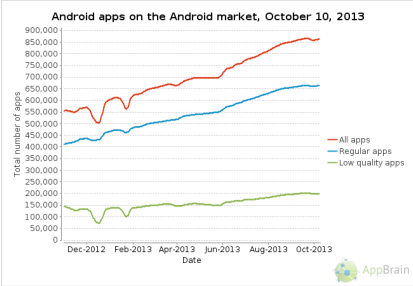
Cloud Security
- SDN
- Virtualisation

SCADA & Smart Grid Security
- Customised instruction
- DDoS mitigation

Mobile Malware Analysis
- Zero day attacks
- Reverse engineering
- Signature extraction

Prof. Sakir Sezer – Research Director

Mobile Network Security

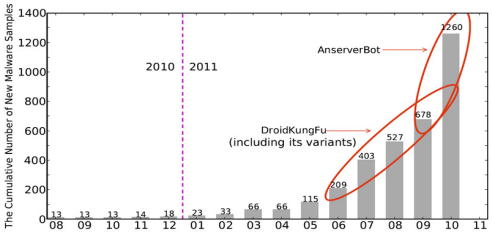


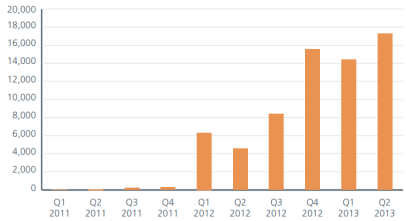
- Over 865,000 Google Android apps and rising
- Estimated downloads in excess of 25 billion
- Growing in number and sophistication

⇒ 23% low quality apps ~2% malware

⇒ 100 x increase of malware over the past 24 months

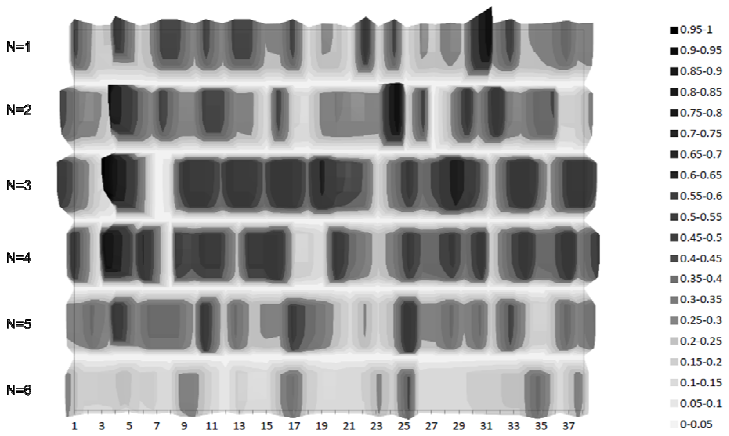
Source: AppBrain





Source: McAfee Threats Report: Second Quarter 2013

Op Code "DNA fingerprint"



Distribution map of Op Code combinations of a Software

Networked SCADA Security

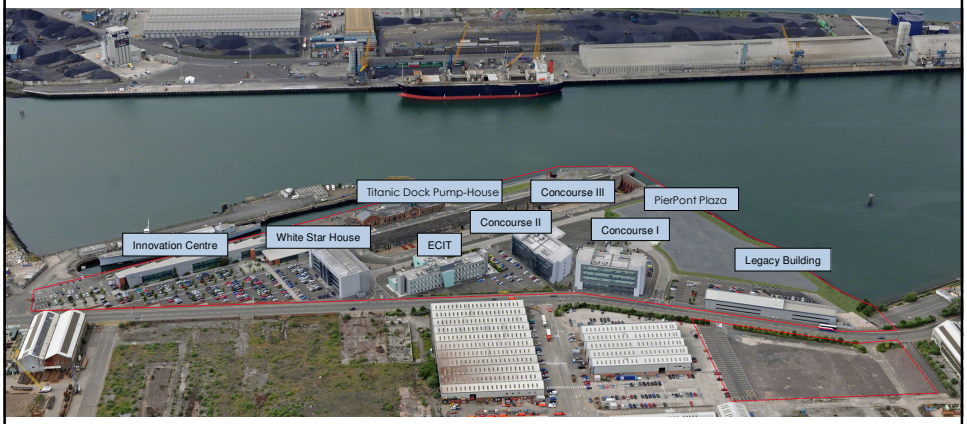
Enhanced connectivity of SCADA systems are essential for optimise use of assets, improve efficiency and monitoring, enhanced automation

Networked SCADA Security
is central for the protection of
Critical Infrastructures and Assets

CSIT: A Global Cyber Innovation Hub

Thought leader in Secure Information Technology Research
Network of Commercial & Research partnerships
Portfolio of successful Technology Transfer

Northern Ireland Science Park - 2013



- CSIT is based in Queen's University's ECIT Research Flagship – 175 people
- Science Park now 119 companies – now full, new buildings planned
- Over 2000 new jobs created since 2004
- £80M pa to local economy in salaries alone

Cybersecurity research : a vision for the UK

Professor John McCanny CBE FRS FREng

THE ROYAL SOCIETY

Royal Society – Cyber Security Research: a vision for the UK

- Cyber Security a major international issue – transcends international borders
- Many national Cyber Security strategies
  - US International Strategy for cyberspace - 2011
  - European Commission Cyber Security Strategy – part of the Digital Agenda for Europe, July 2013
  - Cyber Security Strategy for Germany - 2011
  - Information Strategy for protecting the Nation – Japan
  - UK Cyber Security Strategy – 2011, £650M allocated
- Royal Society – Science Policy project
  - Set out a high level vision to help frame a "cross sector research agenda" to complement these other initiatives

Terms of reference

What are the major cybersecurity research challenges emerging in the next 5 to 10 years?

What policy frameworks are needed in the UK to address these cybersecurity research challenges?

Government aims for cyber research

'strengthen the UK's academic base by developing a coherent cross sector research agenda, building on work done by the GOSCI'

'supporting the application of research, working with GOSCI and others to build innovative cybersecurity solutions'

Policy Frameworks

- Research priorities - current status
  - Where are the major research gaps and interdependencies between these research challenges?
- Research co-ordination
  - What new policy frameworks, if any, are needed
  - Enhancing research partnerships between academia, government and industry?
- International collaboration
  - Enhanced international research collaboration, who are the UK's priority partners, means to support and promote such partnerships
- Commercialisation
  - What needed to 'support the application of research ... to build innovative cybersecurity solutions … in support of the UK's national security interest and wider economic prosperity'

Cyber Security Research Challenges – Examples

- Sustainability of Cyberspace
- Cyber Privacy and Trust
- Bio-inspired Cyber Security
- Privacy and on-line surveillance
- Cyberphysical Systems/Internet of Things
- Cyber security in its wider socio-economic context.

To find out more, visit
royalsociety.org

THE
ROYAL
SOCIETY