

AUSTRALIA'S DIGITAL INNOVATION POWERHOUSE

DATA
61



1100+
employees
[including students]

415+
students

31
Government
partners

91
Corporate
partners

29
University
partners

190+
data-driven
projects

172
patents

ENGAGE WITH US



DATA 61+

- ◆ **ACADEMIA**
Enhanced industry-relevant PhDs
Contributed academic staff
- ◆ **CORPORATIONS**
Collaborative R&D
Contract R&D
New technology licensing
- ◆ **STARTUPS**
Business and tech mentoring
New technology licensing
- ◆ **FEDERAL AND STATE GOVERNMENT**
Trusted advisor for policy and technology
Contract R&D
- ◆ **Investors and entrepreneurs**
Access to deep tech startups

DATA
61



INVEST VICTORIA

HOME WHY MELBOURNE OPPORTUNITIES HOW WE CAN HELP RESOURCES

News & Events /

Data61 Cyber Security and Innovation Hub opens in Victoria

06 Oct, 2016

Victoria's new world-class cyber security centre [Data61 Cyber Security](#) is up and running and will create 140 jobs, including positions for PhD students, over the next three years.



Data61 Cybersecurity

Data61 Cyber Security and Innovation Centre



- Data61's Cyber Security and Innovation Centre opened in Melbourne in October 2016.
- The 135-seat Centre co-locates industry, government and research stakeholders with Data61, to drive collaboration and co-development.
- Data61 works directly with these partners – and our extended D61+ network - to identify applications in their fields.



D61+ Cybersecurity Network



Partnership with DST Group
15+ active research projects with universities

Collaborative research Projects with 15+ Uni
with access to researchers & PhDs

Partnership with Fed/State Governments on research projects

Partnership with AICD
Executive training for boards and executives

Collaboration with AustCyber & CRC
Seeding and scaling cyber security industry

Seeding New Industry with Deep Tech/Science & Collaboration



Build User Communities
around deep tech & science

Attract Talent
using deep tech & have a healthy turnover

Enable Meta-idea Innovation
on top of general-purpose tech

Incentivise Industry-Research Collaboration
around deep tech & science

Research Challenges & Themes



Research challenges, defined together with our defence partner, DST Group

- *Building trustworthy and resilient cyber systems.*
- *Risk-based cyber approaches and shared awareness.*
- *Strengthening the human and social dimension of cyber security.*

Research themes within D61+ network

- *Trustworthy Systems*
- *Automating Cybersecurity and Resilient Systems*
- *Cyber-Physical Systems Security*
- *Quantitative Cybersecurity Risk Management*
- *Data Security and Privacy*
- *Data and Decision Trustworthiness*
- *Usable Human-centric Security*

Cross-Domain Desktop Compositor



Building high-assurance and high-usability systems



Australian Government

Department of Defence

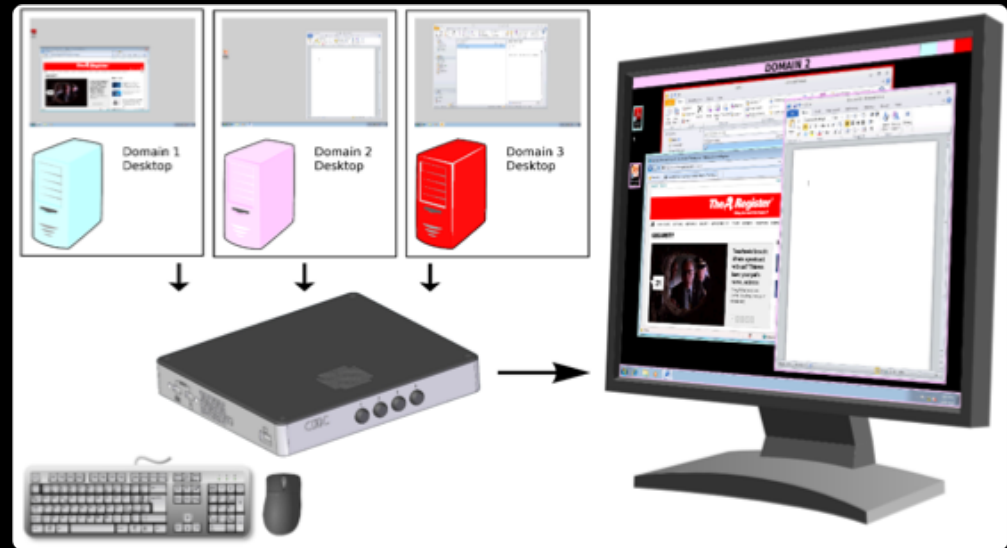
Defence Science and Technology Group

Problem

Cross domain solutions are **critical** for government and business productivity. Current solutions offer **very poor usability** (e.g. secure KVM switch) or have **known insecure foundations** (e.g. Xen).

Insight

Combine DST Group **secure hardware** compositing with Data61's **verified software** control and configuration to produce a solution that simultaneously **maximises both usability and security**.



Impact

- New partnership for in cybersecurity innovation.
- Trialed in defense & supported by defense innovation hub.
- Won 2 national and 3 state iAwards.

Cyber Physical Systems Security

Prevent/Detect/Recover from Physical Attacks



- New technologies for threat analysis and authentication and responses
- Technologies targeting several areas:
 - Drones and UAVs
 - Medical devices & wearables
 - Critical infrastructure: energy, water...

Partners: State governments

METRIC SCORE	DATA BREACH	DOS RELATED	DRONE-JACKING	MALICIOUS EXPLOITS	PASSWORD RELATED	PHISHING	REMOTE ACCESS	REMOVABLE MEDIA RELATED	SPAMMING	WEB SEEDING	Summed impact	Mean impact level
Services and/or facilities	1	3	4	4	3	1	2	4	2	1	25	2
Severity, intensity or magnitude	4	3	1	4	3	2	3	3	4	4	31	3
Scope or spatial distribution	4	4	4	4	4	3	4	4	4	4	39	4
Effects of time or temporal distribution	4	4	4	4	4	3	4	4	4	4	39	4
Public effect	2	2	3	4	3	4	1	1	1	2	22	2
Economic effect	4	4	3	3	3	3	4	4	4	3	35	3
Environmental effect	1	3	3	3	1	1	1	2	1	1	17	1
Political effect	2	1	3	2	2	1	3	3	3	2	23	2
Public safety	1	3	4	3	3	1	2	3	1	1	22	2
Interdependency	3	4	3	3	2	2	3	4	3	4	31	3
Contribution	4	4	4	4	4	4	4	4	4	4	40	4
Summed criticality	30	35	36	38	32	25	31	36	31	30		
Mean criticality level	3	3	3	4	3	2	3	3	3	3		

Adversarial Machine Learning

Robust Defence against Attacks on Learning Itself



New threat vectors

- ◆ Poisoning
- ◆ Adversarial examples
- ◆ Model inversion

Solutions

- ◆ Game theory
- ◆ Data integrity and provenance
- ◆ Random projection & noise injection



Australian Government
Department of Defence
Defence Science and Technology Group

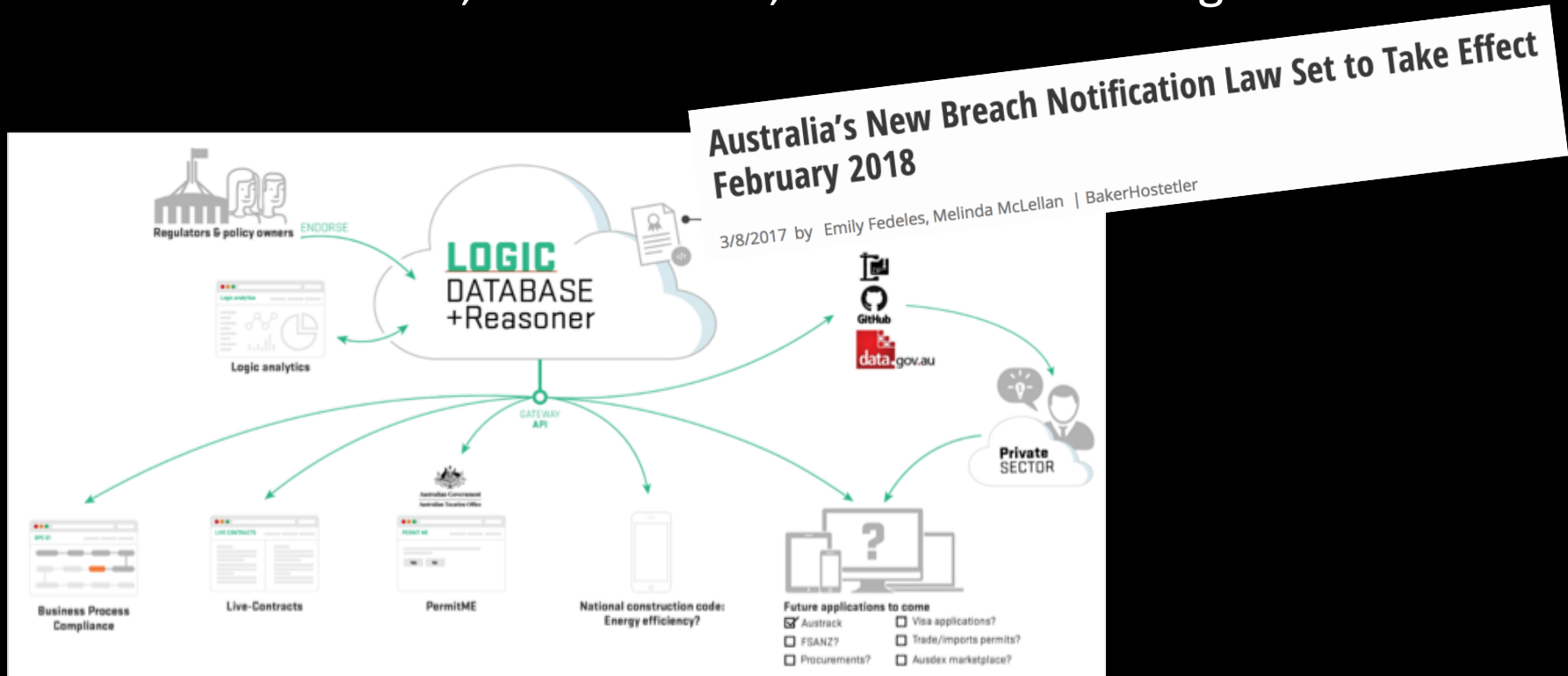


Digital Legislation Platform

Improving access and quality of legislation, as data



- Legislation as a fact base for compliance-by-automation
- Tools for access, visualisation, and understanding of the law





**DATA
61**

QUESTIONS?

Liming Zhu, Research Director
Liming.Zhu@data61.csiro.au

www.data61.csiro.au

