CYBERSECURITY 2020 AND BEYOND?

Matthew Roughan <matthew.roughan@adelaide.edu.au>

ACEMS and School of Mathematical Sciences

University of Adelaide

THE UNIVERSITY of ADELAIDE

SUB CRUCE LUMEN

ACEMS

AUSTRALIAN RESEARCH COUNCIL CENTRE OF EXCELLENCE FOR MATHEMATICAL AND STATISTICAL FRONTIERS

Shameless Plug

2nd ACDCN, Adelaide, 28-29th Nov
Workshop on Challenges of Data and Control of Networks

Keynote speakers:

- Walter Willinger
- Randy Bush
- Darryl Veitch
- Cristel Pelsser

http://www.maths.adelaide.edu.au/matthew.roughan/workshops/acems_workshop_2018/

or just Google me, and follow the links.

Three Grand Challenges for 2020 (-2050)

- Global Social Inequality
- Environmental Degradation and Collapse
- Cybersecurity (particularly of critical systems)

Why These Challenges?

- They are important!
  - If we don’t improve, people will die
  - Without fixes to these, other problems are more difficult
- They are interesting!
  - At least I think so
- They are hard!
  - Let’s talk about this some more in a minute

But 1st, should Cyber- be in this List?

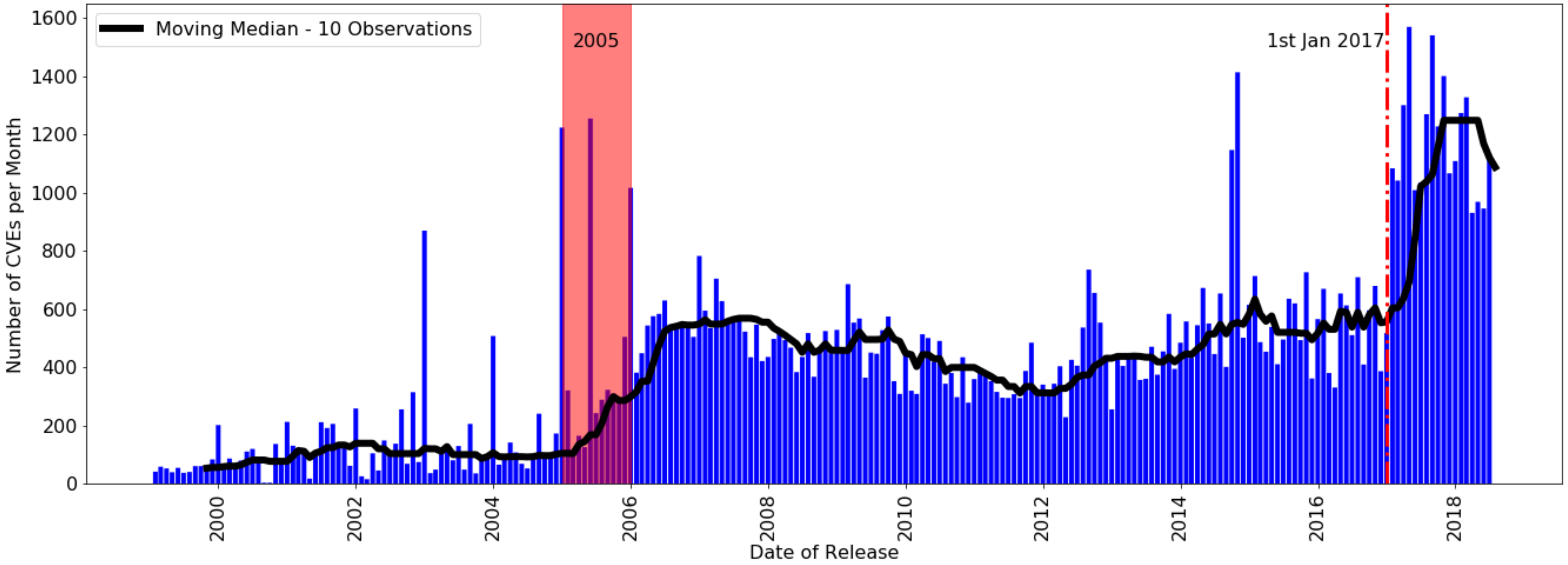
> *"To err is human; to really foul things up requires a computer"*
>
> Bill Vaughan, 1969

- Growing problem: target rich environment
  - IoT = embedded, networked devices everywhere
    - New attacks and new attack vectors
  - Autonomous cars
  - Power stations and networks
  - Hospitals and medical devices
  - Plus much, much more

- Resources allocated to cyber- aren't growing fast enough

Cybersecurity is Hot and Getting Hotter

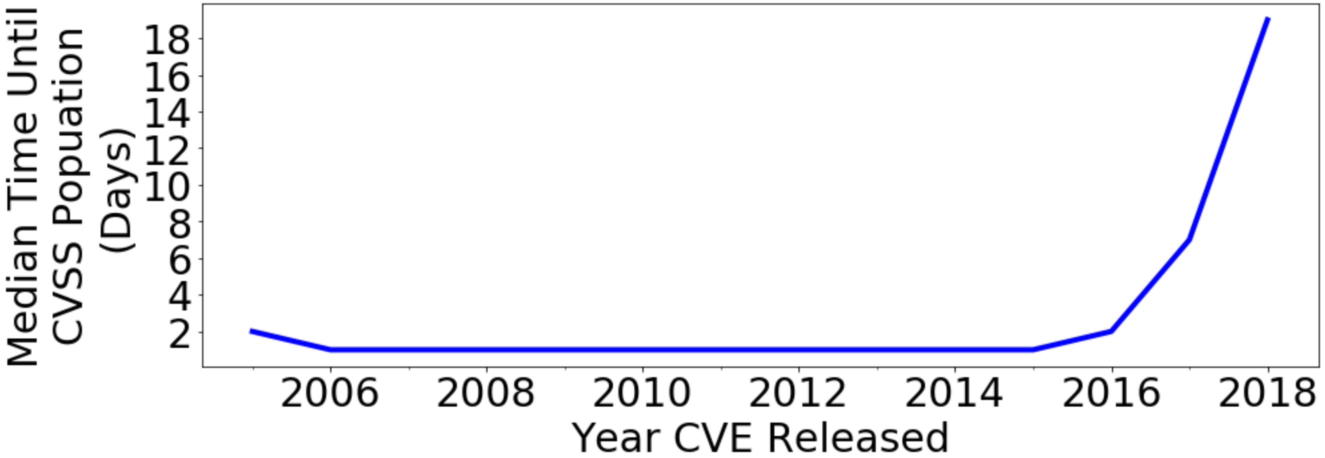
We’ve had decades to understand the problem, and improve it, but it’s getting worse [1]

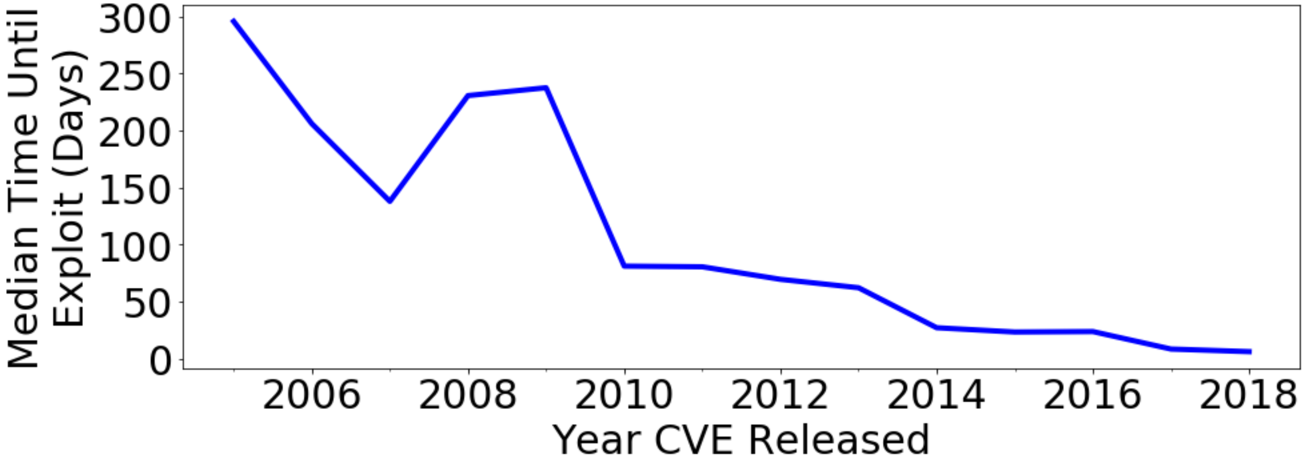


- CVE = Common Vulnerabilities and Exposures
- CVSS = Common Vulnerability Scoring System
- Data from cve.mitre.org and www.exploit-db.com

Cybersecurity is Hot and Getting Hotter

We've had decades to understand the problem, and improve it, but it's getting worse [1]





Why are these 3 Challenges so Hard?

- Technically difficult
- Economic incentives are wrong
- Politically problematic
- Psychology/Sociology

Psychology/Sociology

- The Law of Unintended Consequences (R.K. Merton, 1936)
  - *e.g.,*1920s prohibition creates organised crime
  - *e.g.,* think about passwords for a minute
    - Passwords that are “words” are too easy to crack
    - There aren’t enough symbols in the English alphabet
    - So let’s include numbers and symbols to increase the space of passwords
    - **BUT** We all know that “password” is the most common password
    - When you introduce these rules it becomes

p@ssword01

- This type of problem is rife in cybersecurity
  - If security is too inconvenient people find ways around it
  - People follow social norms, which are often counter to being secure

Pushing at these issues Is like trying to hold wet soap by gripping tighter!

Politics

- Politics and the law
  - Politicians aren’t technical experts => can’t write legislation about this stuff

    “*The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia.*”

    Malcolm Turnbull (ex-PM), 2017

- Western ideas of freedom are based around individual rights
    - *e.g.*, privacy, free speech, due process, …
  - Security would be easier without such niceties
  - Individual *vs* universal good
  - Local *vs* global optimisation

- Problems are global
  - You can’t (effectively) prosecute people scamming Australians from Nigeria

Economic Incentives are Wrong

- You don’t make money by fixing security
  - It costs a lot
  - It doesn’t create revenue
- You don’t lose much by failing
  - Zero tangible cost (often)
  - Reputation losses are overestimated
    - *e.g.*, Ashley Madison
- More and more devices, software, clouds, …
  - Too often, they are made down to a cost, not up to a standard

Technically Hard!

- You know many of the issues
  - IoT
    - According to the technology research firm Gartner, more than 25% of cyber-attacks will involve IoT by 2020
  - Baked-in backdoors in silicon
  - Software written without any security expertise

- But underlying these problems is complexity
  - Systems/software/networks are too big/complex for a single person to understand them
  - Correct behaviour is dependent on people understanding the systems

  These two can't both be true and still have it all work

Network Security Problem Example

- “Google goes down after major BGP mishap routes traffic through China”, Nov 12, 2018 arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/
- “Strange snafu misroutes domestic US Internet traffic through China Telecom”, Nov 7, 2018 arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/

BGP is the ‘glue’ that holds the Internet together

- It has long-known security (and other) flaws
- BGPsec (concatenated cryptographic authentication of paths)
  - Should fix
  - But it may not fix everything
  - And will anyone use it anyway?

Three Grand Challenges for 2020-50

- Global Social Inequality
- Environmental Degradation and Collapse
- Cybersecurity (particularly of critical systems)

There are a lot of other challenges in the future, but I don’t know too many with this combination of underlying issues. And there are additional tensions, e.g., between performance and security.

Complexity is Not a New Problem

“Seeing there is nothing that is so troublesome to Mathmaticall practice, nor that doth more molest and hinder Calculators, than the Multiplications, Divisions, square and cubical Extractions of great numbers, which besides the tedious expense of time are for the most parte subject to many slippery errors. I began therefore to consider in my minde by what certaine and ready Art I might remove those hindrances. And having thought upon many things to this purpose, I found at length some excellent briefe rules to be treated of (perhaps) hereafter.”

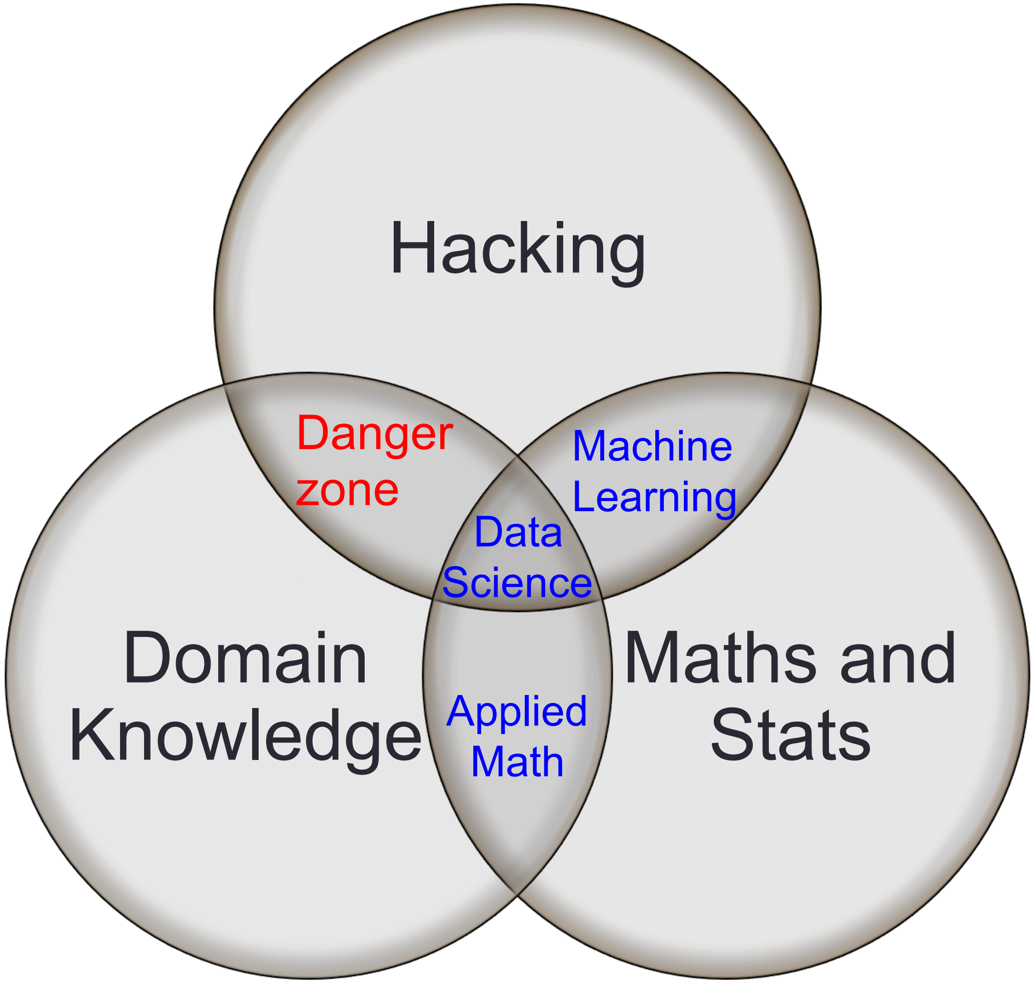
Mirifici logarithmorum canonis descriptio,
John Napier, 1614

This is Not a New Problem

“Seeing there is nothing that is so troublesome to Mathematicall **Network** *practice, nor that doth more molest and hinder Calculators,* **Operators** *than the Multiplications, Divisions, square and cubical* **Configuration of Routers and** *Extractions of* **Switches in** *great numbers, which besides the tedious expense of time are for the most parte subject to many slippery errors. I began therefore to consider in my minde by what certaine and ready Art I might remove those hindrances. And having thought upon many things to this purpose, I found at length some excellent briefe rules to be treated of (perhaps) hereafter.”*

Mirifici logarithmorum canonis descriptio,
John Napier, 1614

The Solution is Math

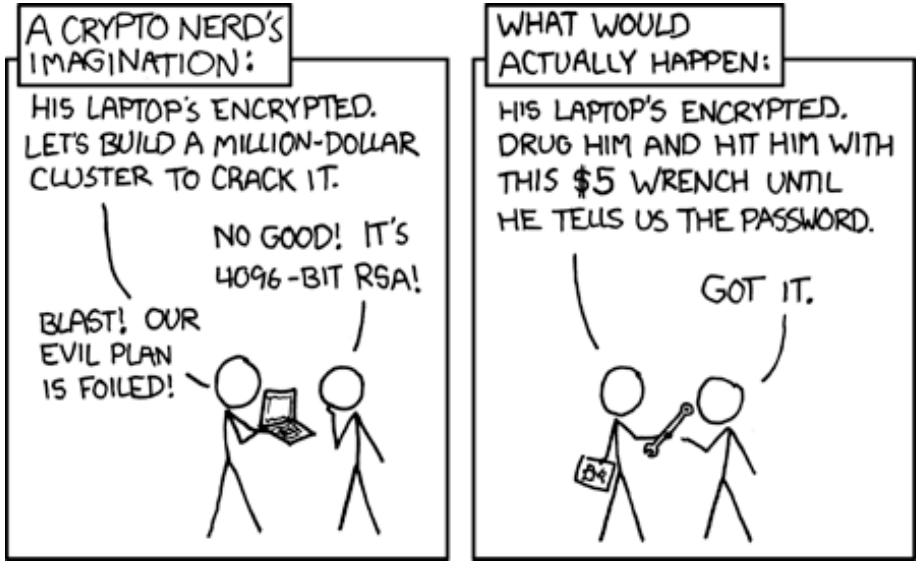


Conway’s data-science Venn diagram
http://drewconway.com/zia/2013/3/26/the-data-science-venn-diagram

- Note the danger zone
  - This is where most cybersecurity sits
  - It is too “hacky”
  - It is too reactive
  - It is too clever – it just increases complexity, which is the root problem!
- Plus, security is about weakest links
  - “cyber” still needs physical security
  - How can we be sure weakest links are secure?

But Math is Already Involved Isn't It?

- Cryptomath is a vital part of cybersecurity
  - It's so good, we don't try to break crypto, we break the bits around it


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

  - Cryptomath focus is on confidentiality and integrity, not availability
    - In critical systems, often the latter is most important
- I don't want more cryptomath

(actually I do, but that's not the main point today)

The Mathematical Sciences are Wide

- We use math a lot in communications networking
  - Cryptomath (number theory++)
  - Stochastic modelling (Queueing theory! ☺)
  - Statistical analysis
  - Graph theory
  - Optimisation

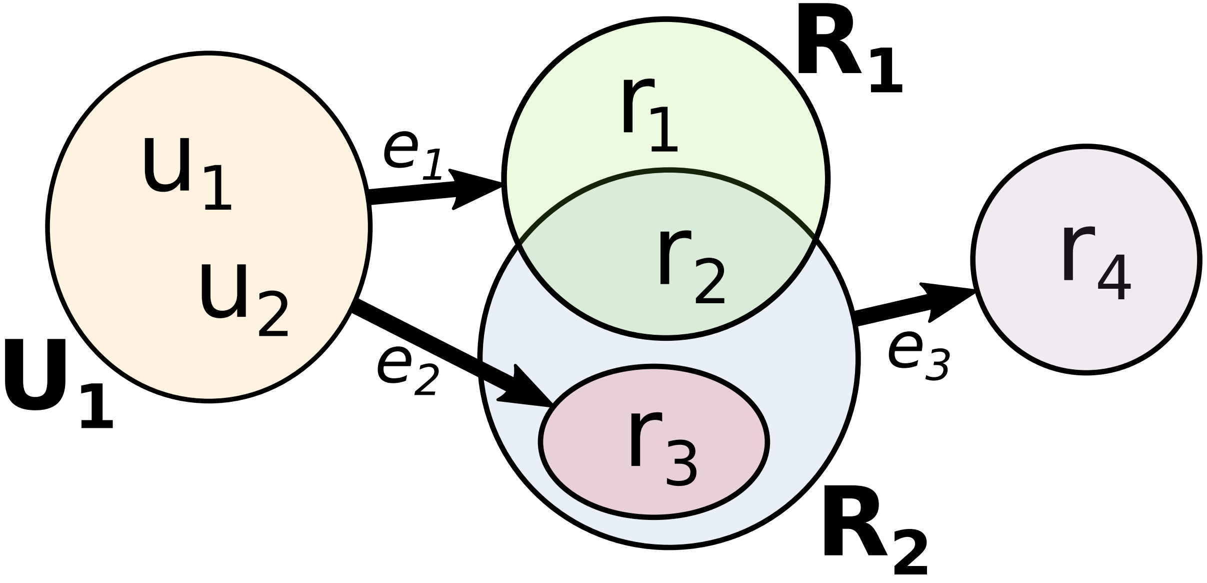
- What about algebra!
  - We don’t usually include this (beyond simple linear stuff, or the more obscure cryptography)
  - But there are cool things we can say and do with it
  - And it meshes well with the other techniques above

Semirings

- A semiring is a mathematical algebra where we redefine the meaning of + and x, so that they have a set of properties in common with traditional arithmetic
  - *e.g., (a+b) + c = a + (b +c)* (this is called associativity*)*
- Many network problems can be described by operations on a semiring on the network
  - *e.g.,* shortest-path routing protocols = min-+ semiring
- Given a precise mathematical abstraction of a network problem (e.g. a security criteria) we can prove the network satisfies the required criteria [2]
- We can then push the proven solution direct into network devices via a network compiler

Metagraphs

- Metagraphs use the same visual metaphor for networks we are familiar with, but group atoms: *e.g.*, resources and users



- We can do algebra on metagraphs as well, to do proofs, for instance of reachability of particular services [3]

An Example

- As Clear as MUD (Manufacturer Usage Description) [4]
  - IoT device description being drafted by the IETF
  - Machine readable
    - intention is to be used to automatically configure network to support device
  - We can
    - Validate a MUD profile
    - Compare a MUD profile to your security policy
  - So you can automatically decide whether a device is consistent with network policy (for the location you want to put it), and if not, see precisely how it violates the policy

Key points

- Software-Defined Networks are cool, but not enough
  - SDN is infrastructure, not an end in itself
- Good (mathematical) abstractions are needed
  - Express intent not details (Intent-Based Networking)
  - Tension between
    - Simplicity
    - Expressiveness
- Automation (SDN = Self-Driving Networks)
  - Forget about hand configuration of routers
  - Automated checks as part of the process
    - Never assume anything is working correctly
    - Check everything as many ways as you can
- Monitoring
  - Quality control requires knowledge
  - Monitoring isn’t an add on feature, its crucial

Conclusion

- I am not going to fix cyber security tomorrow
  - It’s a big and hard set of problems
  - I only really know about networks
  - I just want more people to work on it
  - And I want more people to think about it at a fundamental level not just by adding hacks on top of hacks on top of new vulnerabilities on top of hacks

- Math is good, do more math!!!

- Choose problems that are important! And interesting! And Hard! -- or at least two of these ☺

References

1. *The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay*, A Feutrill, D Ranathunga, Y Yarom and M Roughan, CANDAR 2018.
2. *Malachite: Firewall Policy Comparison*, D Ranathunga, M Roughan, P Kernick, N Falkner, IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, June, 2016.
3. *MGtoolkit: A python package for implementing metagraphs*, D Ranathunga, H Nguyen, M Roughan, SoftwareX, Vol.6, pp. 91-93, 2017.
4. *Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles*, A Hamza, D Ranathunga, HH Gharakheili, M Roughan, V Sivaraman, 2nd ACM Workshop on IoT Security and Privacy, 2018.