SUMMER RESEARCH 2024/25
PROJECT ABSTRACT

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

PROJECT # 28

SUPERVISOR/S: Dr Marinho Barcellos

PROJECT TITLE: Using an Internet-in-a-box Approach to Experimentally Study Attacks against Networks

FIELD: Cybersecurity

DIVISION/SCHOOL: HECS - Au Reikura School of Computing and Mathematical Sciences

PROJECT LOCATION: Hamilton

PROJECT ABSTRACT:

Internet cybersecurity. The Internet has become an essential part of the critical infrastructure of any country, with societies becoming increasingly digital. The high impact it has on the lives of citizens is undeniable due to the usage of numerous services accessed through the Internet, such as health care and public transport. Because of this fact, there is an inevitable rise in cybercrime and cyberwarfare that we have already begun to observe.
Study attacks against networks. This project aims to study experimentally some of the most relevant cybersecurity attacks that affect the Internet nowadays and assess the effectiveness of existing defences. The attacks are (a) against routing, such as BGP prefix hijacking and route leaks, and the use of RPKI to mitigate them; (b) scanning looking for vulnerabilities in other networks, and how packet filtering can add some level of protection; (c) botnets, comprised of bots controlled by a botmaster to launch an attack; and DDoS attacks (e.g. at Layer-4 and Layer-7) and how FlowSpec, Blackholing, Anycast, and packet filtering can help mitigate the impact of attacks. Botnets and DDoS attacks will be explored together.
Internet-in-a-box. The methodology consists of constructing scenarios representing each of the attacks using a controlled environment called “mini-Internet”. The mini-Internet environment was introduced in 2020 by ETH Zurich (https://github.com/nsg-ethz/mini_internet_project) and has been used widely to teach students how the Internet works, including at the University of Waikato (COMPX304 2021-2024). The software platform creates an “Internet-in-a-box” with a high level of realism. Networks are comprised of hosts and routers, running virtualised Linux and FRR software routers, the same software that equips many routers on the Internet nowadays.
Approach and challenges. The project will explore the feasibility and level of realism the environment can use for investigating the named attacks and mitigations on scenarios with over 100 independent networks (called Autonomous Systems). The creation of such scenarios poses many challenges or limitations, both functional and non-functional. Functional limitations refer to the impossibility of mimicking accurately certain attacks or protections, whereas non-functional refers to limitations in system size and performance (the environment will be running on a single machine, e.g. a multi-core server).
Outcomes. The scenarios created, as well as the results generated, have potential uses in research and teaching.

STUDENT SKILLS:

- A or A+ in COMPX304, which covers the subjects in this SRG: Mini-Internet environment, Internet infrastructure (OSPF/BGP routing, DNS, etc), and cybersecurity.
- Programming skills: Python and C/C++ or Java
- Development using a Linux environment and GitHub

PROJECT TASKS:

1. Create a “baseline” Internet infrastructure on mini-Internet. (Week 01)
2. Create prefix hijacking experiments, exploring attack variations and degrees of sophistication. Extend the scenarios to include mitigations, such as RPKI and BGPsec, assessing their positive impact. (Weeks 02-03)
3. Deploy scanner tools (nmap and masscan) inside the environment. Explore scanning scenarios, in which networks are tested for vulnerabilities (ports with vulnerable services). Apply combinations of packet filtering rules at networks to assess how this strategy can block scanning. (Weeks 04-05)
4. Implement a simple “lightweight version of a bot” to run on hosts or routers of the environment and take commands from a botmaster, to be implemented as well. Create botnet-based DDoS attack experiments using this bot, with bots flooding a chosen web server (part of the environment) with HTTP(S) requests. Extend the scenarios to include DDoS mitigations, namely packet filtering, blackholing, anycast, and BGP FlowSpec. (Weeks 06-09)

5. Write online documentation about the system. Publish the system with documentation in a public repository, such as GitHub, allowing the research community to engage and contribute. (Weeks 02-10)
6. Create a research poster summarising the results. (Week 10)

EXPECTED OUTCOMES:

- Student's Research Poster (as per clause 6 of the Scholarship regulations)
- Project implementation (source code, configuration files, scripts, documentation) is shared on GitHub and available to the academic community.
- Environment to be available to 300- and 500-level students to study Internet cyberattacks, for any demonstrations we (Cybersecurity group) need to do in public events, as well as cybersecurity papers in Waikato.