Ensuring Cyber Hygiene: Attack Vectors Analysis and Mitigation Strategies project

Cathal Lawlor, Mamoona Asghar, Computer Science

UROP Undergraduate Research Opportunities Programme funded through SFI Discover

Introduction

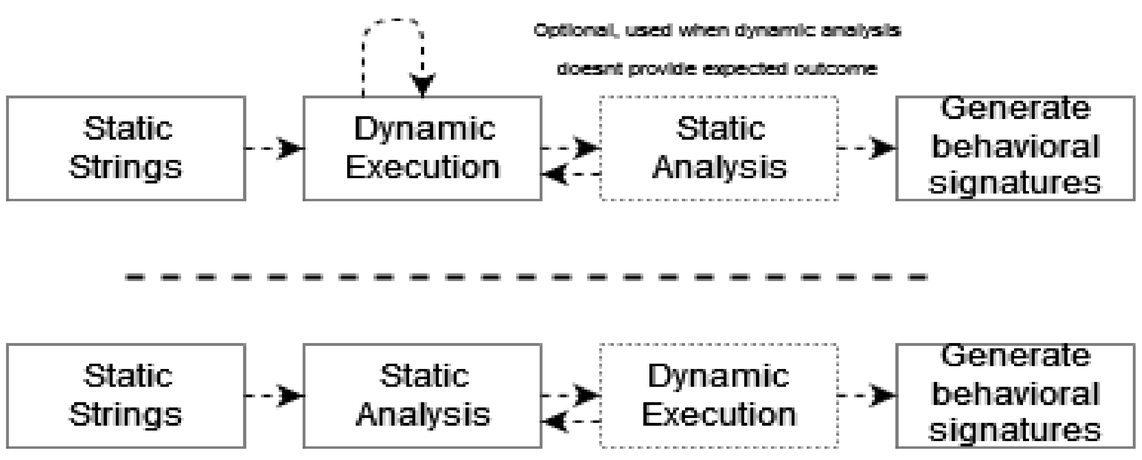
- I'm learning all about cybersecurity which is quite an interesting field to be in. There is plenty of stories about breaches/hacks, and how they are becoming more prevalent in the news nowadays.
- Cybersecurity is the protection of computer systems and networks from information being shared when it shouldn't be, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misleading users away from the services they provide. This is an interesting field to work in with new threats everyday changing the workspace.

Topics

My project is for me to learn about and put to use cybersecurity techniques, with how they are applied with practical use cases. This is learning how systems and networks are being attacked, and what we can do to stop and protect these systems.
I focused on the malware and encryption aspect of this for the internship.
I did nearly all my research online, using websites such as tryhackme.com where you can do actual hands on examples by yourself.
I covered topics in:

- Malware – The different types employed, various attack approaches and methods, the use of hashing to track the individual malicious software.
- Analysing – Use of sandboxing to protect your system
- The mitigation of any of malicious attacks.
- Vulnerabilities – How they can be exploited, how they could be mitigated, zero day exploits.
- Cryptography – The process of keeping information and links between computers secure and trustworthy.

Identification of malicious malware activity



For identification of malicious malware activity either of these process charts are the general approaches for identification. The main objectives of this is to extract malicious behaviour, write reports on the information gained and then label malware families.

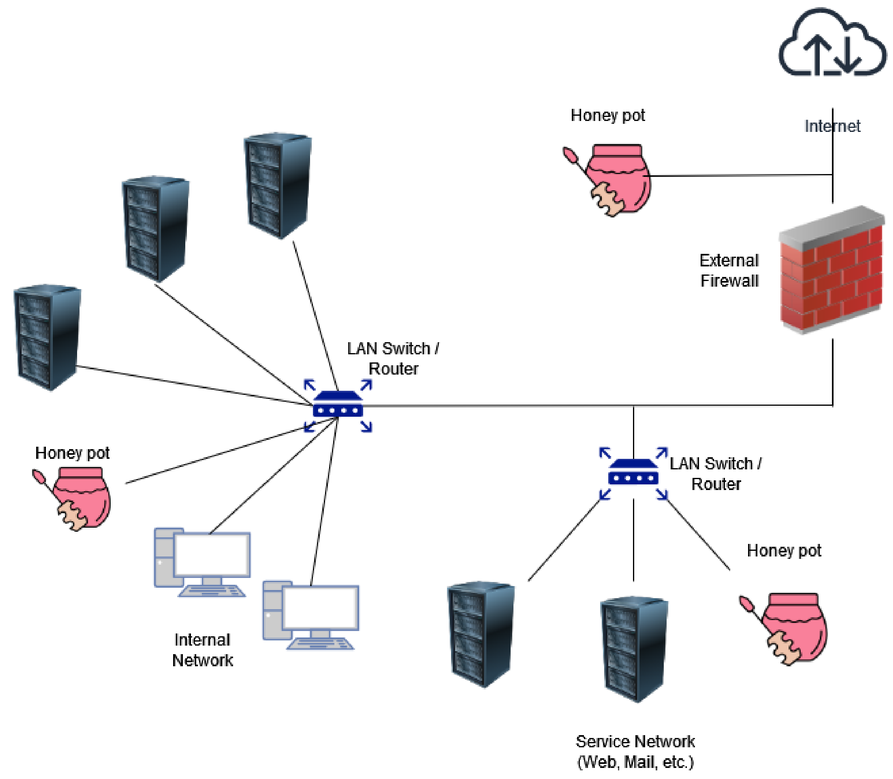
The malware samples used in this process are collected from sources, such as clients, honeypots, malware repositories and from there is prioritized and would be sent to the main analysis process like above.

REFERENCES

M. Y. Wong, M.Landen, M. Antonakakis, D. M. Blough, E. M. Redmiles, M. Ahamad, CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security November 2021 Pages 3053–3069 doi: 10.1145/3460120.3484759

O. Or-Meir, N. Nissim, Y. Elovici, L. Rokach, ACM Computing SurveysVolume 52Issue 5September 2020 Article No.: 88pp 1–48h doi: 10.1145/3329786

Honey Pot example



Above is a figure for a very simple network with honeypots in use. Honeypots are used to mislead hackers away from actual systems and data while gathering information in how they infiltrate a network.

This info can then be used to protect and upgrade networks and fix vulnerabilities it could have.

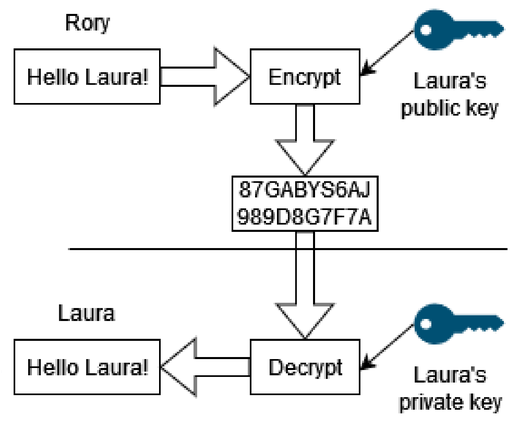
Honeypots have downsides if used as the only form of protection - relying on them means you're depending on techniques based in prevention, where eventually hackers will find a detection gap, e.g. get past a honeypot undetected.

Public Key Cryptography

This figure is an example of public key encryption.

With Rory using Laura's key, only Laura could actually open up Rory's message as Laura is the only one holding the private key able to decrypt message.

This can also be used to have a trust factor established by using ones private key first.



Conclusion

I found this internship to be really good in helping me develop my skillset and learn more about cybersecurity itself. It really has peaked my interest in the topic and I plan to keep learning more about it into the future.

I had great support from my supervisor; Mamoona Asghar and from all of the team behind the organisation of the internship in Cúram.

I've seen first hand myself that this is a great way to encourage and foster growth in groups that are underrepresented in STEM. We need to keep this push to foster learning for aspiring students. It is hard to see the steps to take to get to these research positions and programs similar in structure to this can really show how you get actually realise that vision.

ACKNOWLEDGEMENTS

Science Foundation Ireland (SFI 21/DP/9815) and the European Regional Development Fund (Grant Number 13/RC/2073_P2)

Put any additional logos here