



BSides Bristol 2023

On 4th November I attended BSides Bristol which is a community driven security conference. The conference has a schedule of speakers over two tracks along with Vendor stalls and other activities.

The day opened with some words from one of the organisers, swiftly followed by a keynote titled 'you're gonna need a bigger boat' from Lisa forte. Using a mountain climbing analogy Lisa explained why sometimes you have to change things up. Think about the problem differently to how it has been. Asking the question why several times can help realise you don't know something as thoroughly as originally thought. E.g., why do you breathe. Need to think about how to disrupt ransomware differently as people do pay and gangs do not generally renege on their promise to give data back. Diversity matters as when we view risks, we do it based on our own experiences so different views help.



After Lisa's presentation I moved to track 2 to for 'Securing AI' by Seth who talked us through a Generative AI and his experience over the past 9 months looking at ways to use Generative AI securely in an enterprise setting. One thing to particularly be aware of is to give lots of context for best results. He also talked about prompt injection, social engineering the computer to trick it into giving you answers it shouldn't, and about hallucination. Remember, you can't trust LLMs. Use response inspection to help ensure integrity. A beneficial use for it is to use it to write an exploit then ask it how we can prevent it. Seth provided the following resources for further Gen AI research.

<https://owasp.org/www-project-top-10-for-large-language-model-applications/>

<https://atlas.mitre.org/>

<https://github.com/nomic-ai/gpt4all>

<https://huggingface.co/>

Next up was 'Hey doesn't that look like your cloud data' presented by Shahnoor Kiani. This talk was about a methodology for finding exposed cloud assets. Shahnoor provided a new technique to find instances of most AWS services using AWS Cognito as an example of how an attacker could gain unauthorised access to an application. A tool called Katana was used to find URL's and httpx to make requests at scale. The responses could then be checked. Certificate transparency logs were then used to check the details of certificates as Certificate Log Monitoring tracks all publicly issued certificates. There is also a searchable database of certificate transparency logs which was used to view certs.

After that was a talk by Ryan Pullen on 'working against the clock cybersecurity the infinite game.' It was explained that Infinite game is keep the game going and stay in the game and the reference for this came from Simon Sinek's 'The Infinite Game.' Ryan focussed on how to adopt a sustainable approach to security taking into account we all make mistakes and it's what do we do when that thing goes wrong that counts.



Next up was Andrea Jones with 'Making consistent STRIDES with threat modelling templates.' Andrea explained how to start using the Microsoft Threat Modelling Tool which is free to use. She then went through maturity levels and then where you need to get to using the SAMM threat modelling level 3 descriptor which states – 'Regularly review and update the threat modelling methodology for your applications.' The

talk moved onto frameworks and STRIDE is the one we're looking at today. STRIDE is a model to identify threats which in this framework are Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. Andrea went through a few ways to tackle the threats such as using good authentication to counter spoofing, using hashes to ensure integrity and encryption to prevent information disclosure. As part of the threat modelling it's important to think of each of those components and how could they happen in the system. Andrea explained how to do this with the Microsoft threat modelling tool and went through the components needed to build a template focussing on AWS as an example, and then Andrea did a demonstration of using the template in the tool.

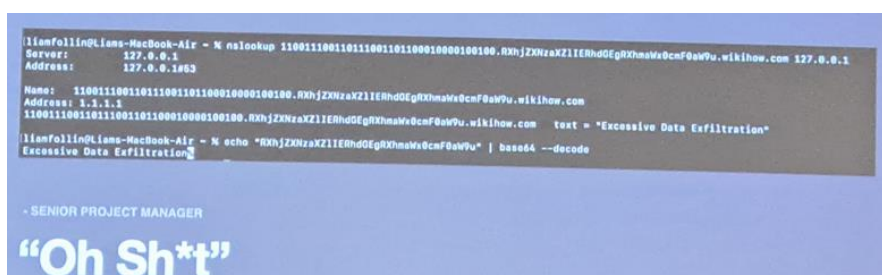
Time then for lunch which was a selection of Subway sandwiches. After eating I had a look at the other areas of the conference.



For infosec battlebots there is an arena where people can battle it out with custom built robots. Next door in the lock picking village is the opportunity to try your hand at picking a variety of locks which varied in difficulty. There's also a number of vendor stalls where you can find out about what the vendors have to offer and pick up a range of swag (promotional products).




After lunch it was back to the talks and 'Domain Name Stupidity' by Liam Follin. Liam went through one of his experiences as a pentester when he heard the challenge words 'our network is unbackable.' Liam explained how a new tool, Pervade, was created in their quest to prove them wrong. This tool abuses DNS lookups and this attack works because of how logging works with DNS. A lot of the logging ignores the destination address. In the 'unhackable' network Liam was working on they forgot to log the 2nd parameter and that allowed them to search for those domains. Reassuringly there needs to be a chain of things that have to line up to be successful with this so only a few networks would be susceptible however Liam provided information on what could be done to prevent this.



On to 'Human Error breaches are bullshit' by Marius Poskus. Marius explained that technology doesn't help if you don't have the right people and processes. To solve the problem we have in cybersecurity currently Marius believes we need to start by building security culture and ensure security is not a department of 'No' but instead it should be 'yes but these are the requirements.' We also need to move away from annual awareness training to frequent relatable trainings and also to document business processes to enforce repeatable behaviour.

Finally, the last talk I attended was 'Cognitive Defenders: How AI Transforms Cyber Security' by Rosalind Grindrod. This was about AI and what it is and that means something that is learning, reasoning and problem solving. AI is the broadest term for Artificial Intelligence. Anything that can learn is called AI. Rosalind then went through some use cases including fraud detection with isolation forest.

What sort of problems can AI solve?	
	Things AI are good at <ul style="list-style-type: none">• Data analysis and pattern recognition• Repetitive tasks• Natural language processing• Image & speech recognition• Predictive analytics• Automation
	Things AI are not good at <ul style="list-style-type: none">• Common sense & understanding context• Creativity & innovation• Ethical & moral decision making• Adaptation to unforeseen circumstances• High level & complex creative problem solving• Understanding intent

That was the end of the day of talks however the day did not end there. There was an afterparty where drinks and a space to catch up with other attendees was provided. A great way to end a fun interesting day.

