A Critical Analysis of Fifth Generation (5G) Mobile Network Security

PRESENTER:
Jack Grieve

SUPERVISOR:
Dr Laith Al-Jobouri

BACKGROUND:

The fifth generation (5G) of mobile networks employ many innovative and advanced technologies to meet the high-level demands of the modern world. Doing so, they leave themselves vulnerable to a plethora of attack vectors commonly used by cyber-criminals.

METHODS:

To develop an accurate and informative threat analysis paper, a strict methodology was chosen. The Process for Attack Simulation and Threat Analysis (PASTA) methodology, along with the STRIDE threat models were chosen for this project as they were tailored the risk-based scope of the paper.

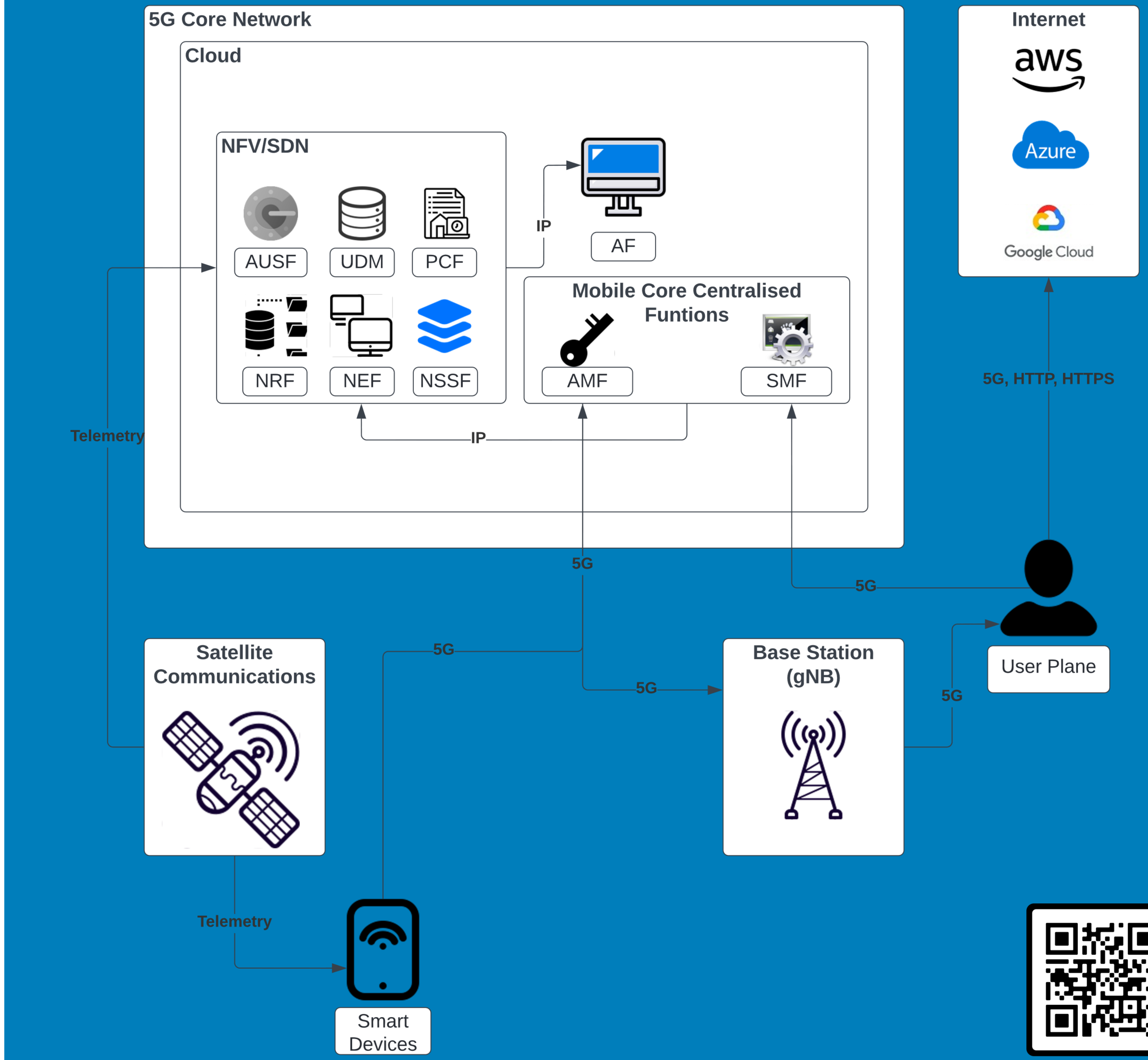
RESULTS:

Results showed that the 5G network was still vulnerable to many forms of cyber-attack. However, the successful completion of these attacks was gauged to be unlikely due to the novel technology requiring a considerable sum of technical and specialist knowledge prior to a potential exploitation of the network. It was also discovered that the 5G network's connection to the Internet Protocol (IP), various insecure IoT devices, bundled with the network carrier's choice to enable or disable certain security features would be a major downfall to the network and its overall security.

CONCLUSION:

The work conducted as part of this project effectively exhibited informative and accurate threat analysis documentation for the 5G network. This work hopes to educated users and network carriers regarding the security issues facing this novel technology.

The 5G network leaves itself vulnerable to a plethora of attack vectors commonly used by cyber-criminals. This is partly due to its connection to the Internet Protocol (IP), various insecure IoT devices, and the carrier's choice to enable or disable certain security features.



SCAN ME TO DOWNLOAD PAPER

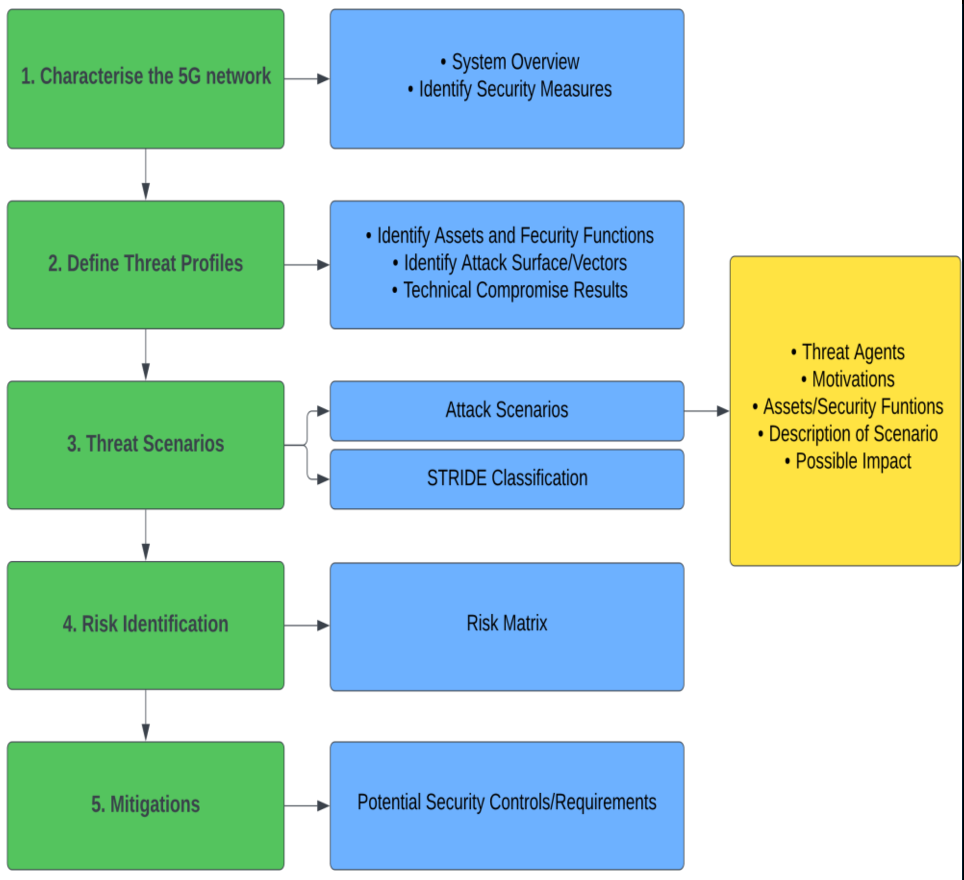

1. Characterise the 5G network
• System Overview
• Identify Security Measures
2. Define Threat Profiles
• Identify Assets and Fecurity Functions
• Identify Attack Surface/Vectors
• Technical Compromise Results
3. Threat Scenarios
Attack Scenarios
STRIDE Classification
• Threat Agents
• Motivations
• Assets/Security Funtions
• Description of Scenario
• Possible Impact
4. Risk Identification
Risk Matrix
5. Mitigations
Potential Security Controls/Requirements

Figure 1 – PASTA Threat Model

Security Feature	4G	5G
User Plane Encryption	Yes (Operator Choice)	Yes (Operator Choice)
International Mobile Subscriber Identifier (IMSI) Obfuscation	No	Yes (Uses Elliptic Curve Integrated Encryption Scheme (ECIES))
User Plane Integrity Protection	No	Yes (Operator Choice)
Radio Resource Control (RRC) message integrity protection	Yes	Yes
Radio Resource Control (RRC) message encryption	Yes (Operator Choice)	Yes (Operator Choice)
Non-Access Stratum (NAS) message integrity protection	Yes	Yes
Non-Access Stratum (NAS) message encryption	Yes (Operator Choice)	Yes (Operator Choice)
Authentication of User Equipment (UE) to serving network	Yes	Yes
Authentication of User Equipment (UE) to home network	No	Yes
Network slicing to provide segregated usage	No	Yes

Figure 2 – 4G vs 5G Security Features

REFERENCES:

Shevchenko, N. (2018) *Threat Modelling: 12 Available Methods, Insights*. Available at: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ (Accessed: 6 April 2022).

Hewko, A. (2021) *STRIDE Threat Modeling: What You Need to Know, Software Secured*. Available at: https://www.softwaresecured.com/stride-threat-modeling/ (Accessed: 5 April 2022).

Abertay University