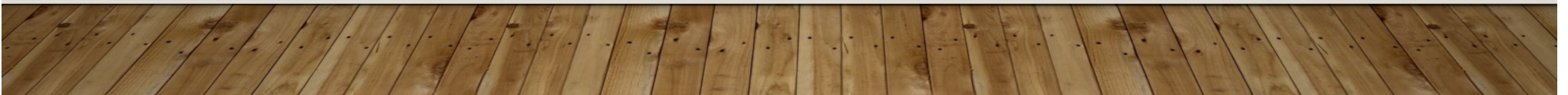# THREAT MODEL

UNIT 4 SEMINAR ACTIVITY

XUE LING TEH

CONCEPT

Qualitative vs Quantitative

- Open FAIR

- Threat Modelling Manifesto

- OWASP Threat Modelling Cookbook

- Mitre Att&ck Techniques

READING

Shostack (2018)

- STRIDE

- DREAD

- Attack trees, libraries

Spring et al. (2021)

- CVSS history, failings

SCENARIO

- A large nuclear power station in France

- Threat Model technique: Attack Tree

Attacks are represented in a tree structure as shown on the diagram (right). The power station, which is the attacker's goal is at the root node. The leaf nodes represent different ways to achieve the goal using various attack techniques.
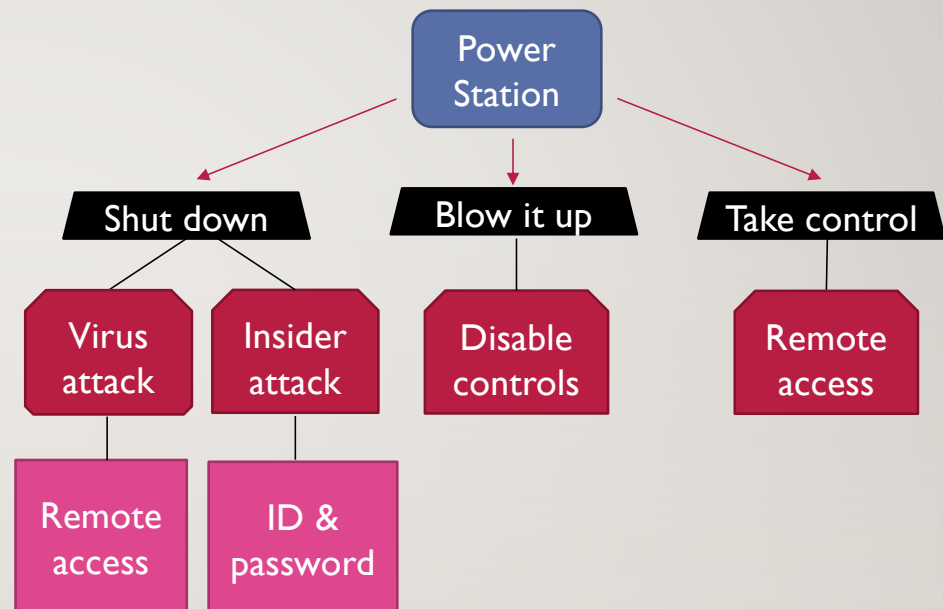
*The attacks shown in diagram are main examples but not exhaustive

```
                          Power
                          Station
              ┌──────────────┼──────────────┐
         Shut down      Blow it up     Take control
          ┌────┴────┐        │              │
        Virus   Insider   Disable        Remote
        attack   attack   controls       access
          │         │
        Remote    ID &
        access  password
```

REFERENCES

- Josey, A., Hietala, J. & Jones, J. (2014) Introducing The Open Group Open FAIR™ Risk Analysis Tool.

- Shostack, A. (2018). Threat modeling : designing for security. Wiley & sons ltd.

- Shostack et al (2020) *The Threat Modelling Manifesto.*

- Spring, J., Hatleback, E., Householder, A., Manion, A. & Shick, D. (2021) Time to Change the CVSS? *IEEE Security & Privacy*, 19(2), pp.74–78.

- Threat Modelling CookBook (OWASP).