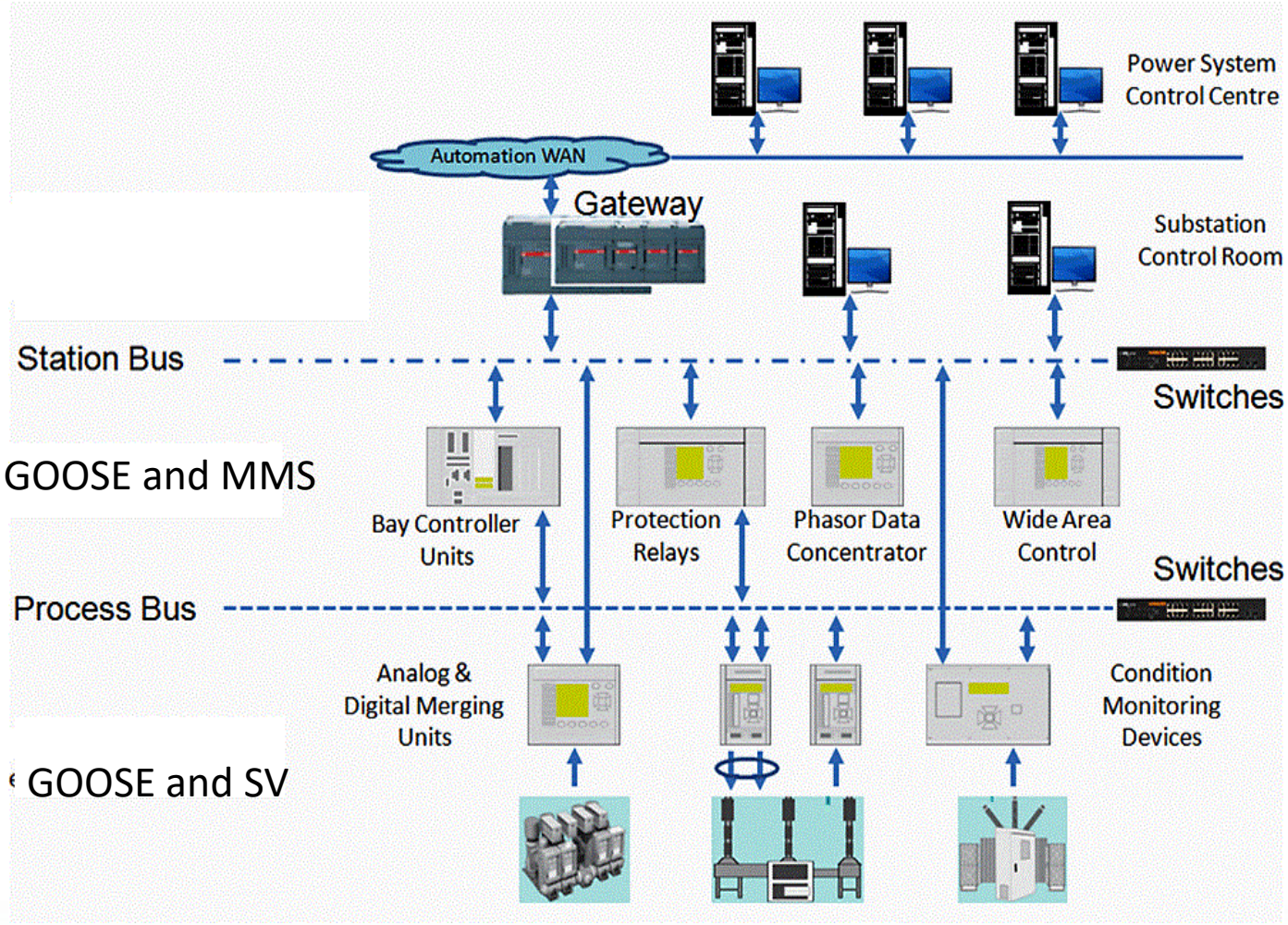
Framework for VAPT in Digital Substation

Speaker : *Dr. Devika Jay*

CTO/CEO

Gridsentry Pvt Ltd

Introduction



Context

- Defense-in-depth
- Vulnerability Assessment
- Penetration Testing

Relevance

Challenges

- No standardized procedure
- Risk on Live system

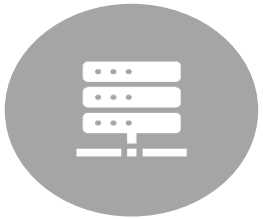
Approach

- VA based on standards
- PT based on MITRE ATT&CK

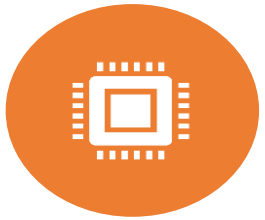
VAPT Framework

Create → Map → Analyse

Create Exploits



HOST DEVICES



SOFTWARE APPLICATIONS

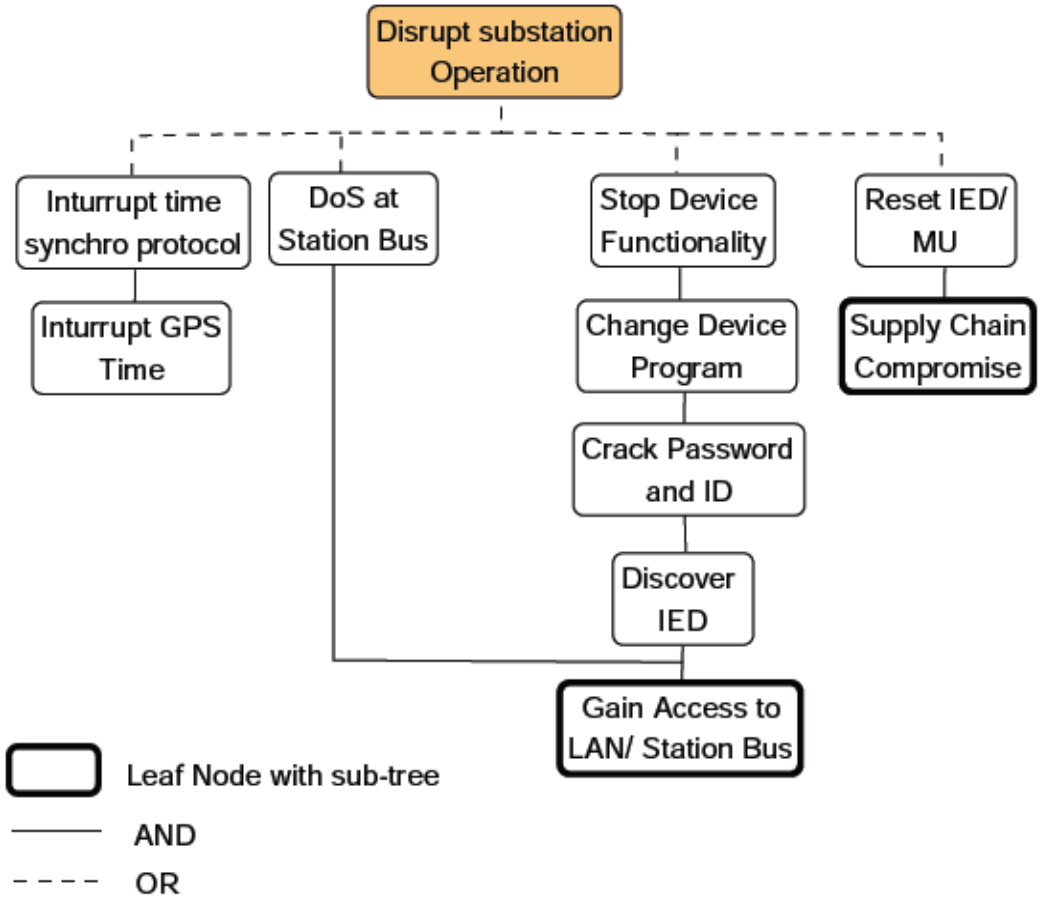
EMBEDDED DEVICES

NETWORK DEVICES

EMS & SCADA system

Protection and Control

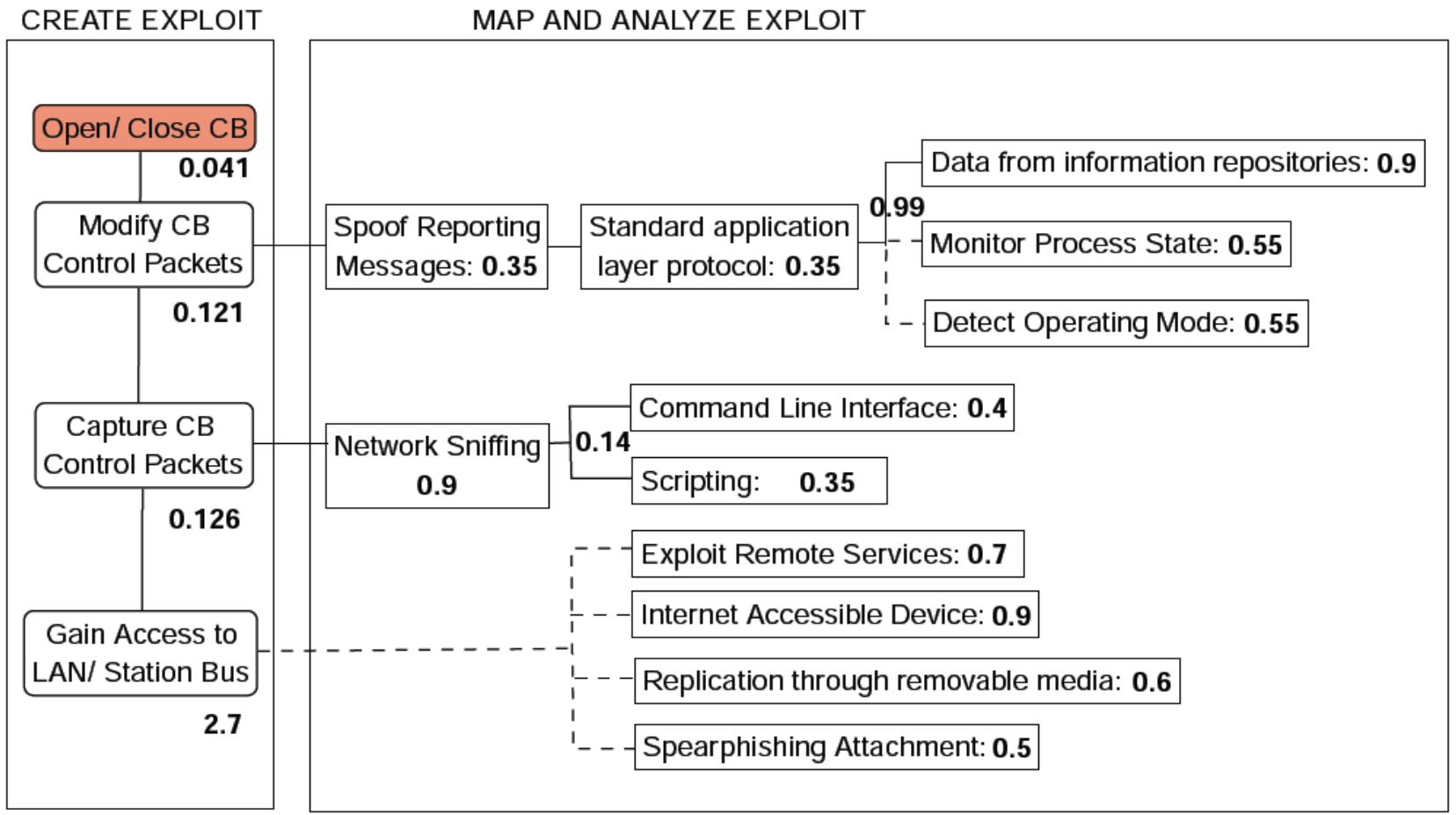
Map and Analyse



Criterion	Sub-criterion	Scores
Skill Required	Deep knowledge on domain and cyber attacks	0.3
	Insider knowledge required	0.5
	Basic domain and cyber skills	0.9
Accessibility	High expertise required to gain access	0.3
	Publicly accessible but not known commonly	0.5
	Common knowledge	0.9
Attack Vector	Attack knowledge available theoretically	0.3
	Past history of attack but with no attack scripts available	0.5
	Attack scripts/tools directly available in public domain	0.9
Common Vulnerability	Isolated occurrence	0.3
	More than one utility	0.5
	More than half of the utilities	0.9

TABLE III
LIKELIHOOD SCORES

Case study


CREATE EXPLOIT
MAP AND ANALYZE EXPLOIT
Open/ Close CB
0.041
Modify CB Control Packets
0.121
Capture CB Control Packets
0.126
Gain Access to LAN/ Station Bus
2.7
Spoof Reporting Messages: 0.35
Standard application layer protocol: 0.35
0.99
Data from information repositories: 0.9
Monitor Process State: 0.55
Detect Operating Mode: 0.55
Network Sniffing
0.9
0.14
Command Line Interface: 0.4
Scripting: 0.35
Exploit Remote Services: 0.7
Internet Accessible Device: 0.9
Replication through removable media: 0.6
Spearphishing Attachment: 0.5

Key Takeaways

- Vulnerability assessment: NIST, IEC, and NESCOR
- Penetration testing: MITRE ATT&CK
- Likelihood and impact scores

Thank You

For discussions/suggestions/queries email: ***isuw@isuw.in***

www.isuw.in

Links/References (If any)