Sandia National Laboratories

Exceptional service in the national interest

NUCLEAR SYSTEM REMOTE OPERATIONS ATTACK SURFACES

Christopher C. Lamb
cclamb@sandia.gov

Shadya Maldonado
sbmaldo@sandia.gov

International Conference on Computer Security in the Nuclear World

Vienna, Austria, 19-23 June 2023

SAND2023-11697C

WHERE WE ARE, AND WHERE WE DON'T WANT TO END UP

Implementation

Remote operations and control saves money!

It provides new business opportunities!

Let's build it!

Ideation

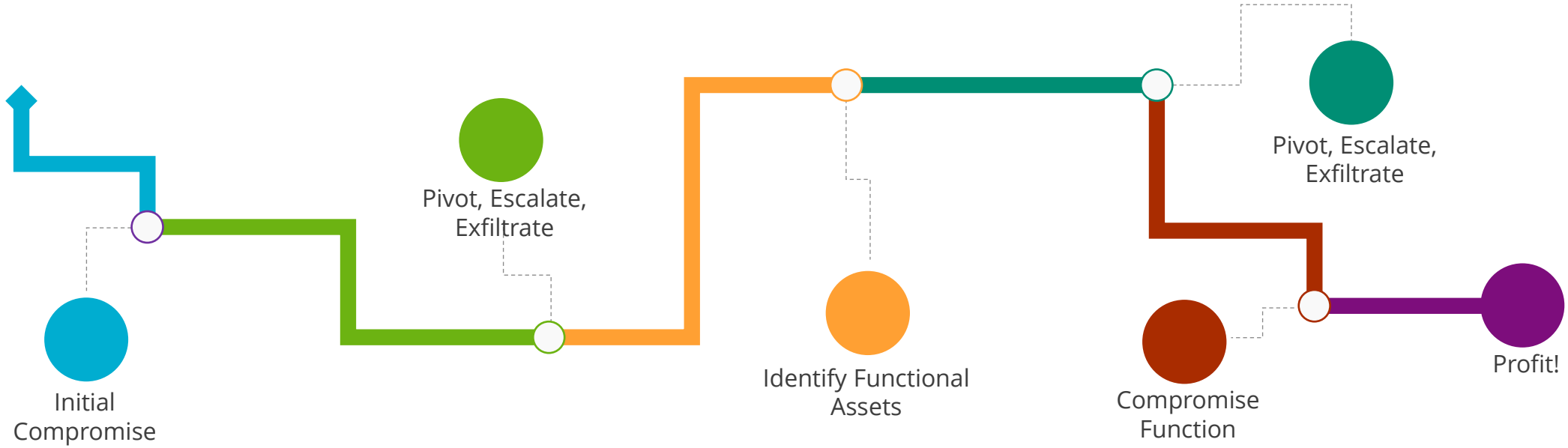
How can we control systems remotely?

Why should we?

What's the return on investment?

We missed security!

WHY DO WE CARE?



Initial attack surface in a remote system describes landscape of initial compromise

WHERE ARE WE NOW?

- Remote attacks and attack surface research mostly focused on cars [Plapper, Miller]
- Some attack surface work on general ICS systems exposed via Shodan [Leverett]
- Security comparisons between communication technologies used for power systems [Baime]

HOW DOES THIS HELP NUCLEAR ENERGY?

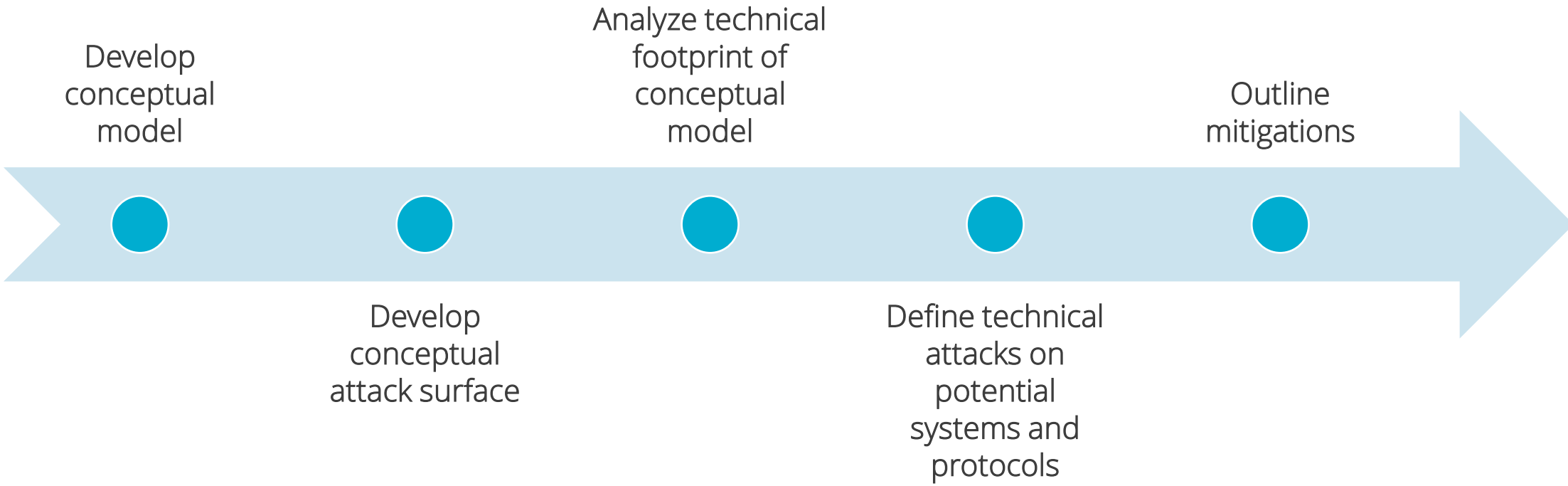
Provide guidance on preventing first step in compromising facility function

Clarify cybersecurity concerns in remote nuclear control systems

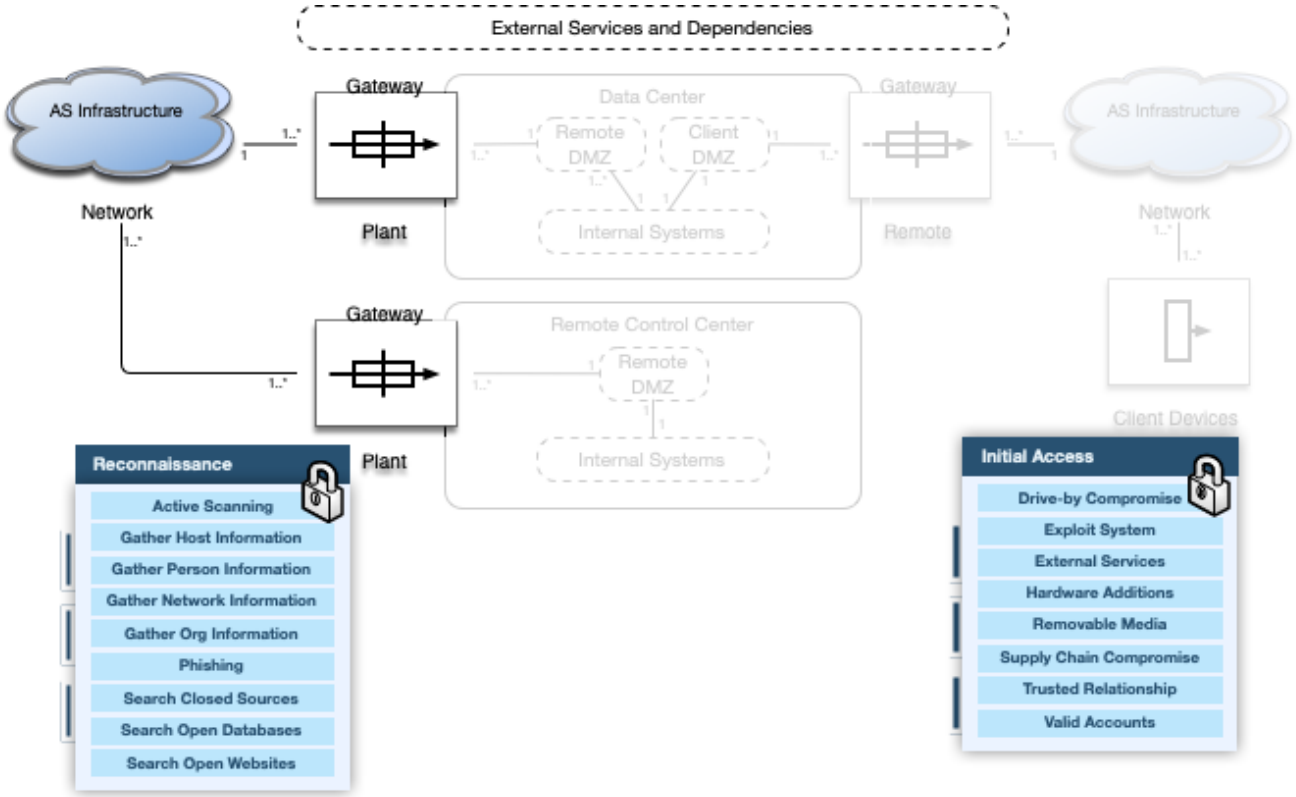
Codify possible attacks, linking them to specific attack classes

Define mitigations needed for identified attacks

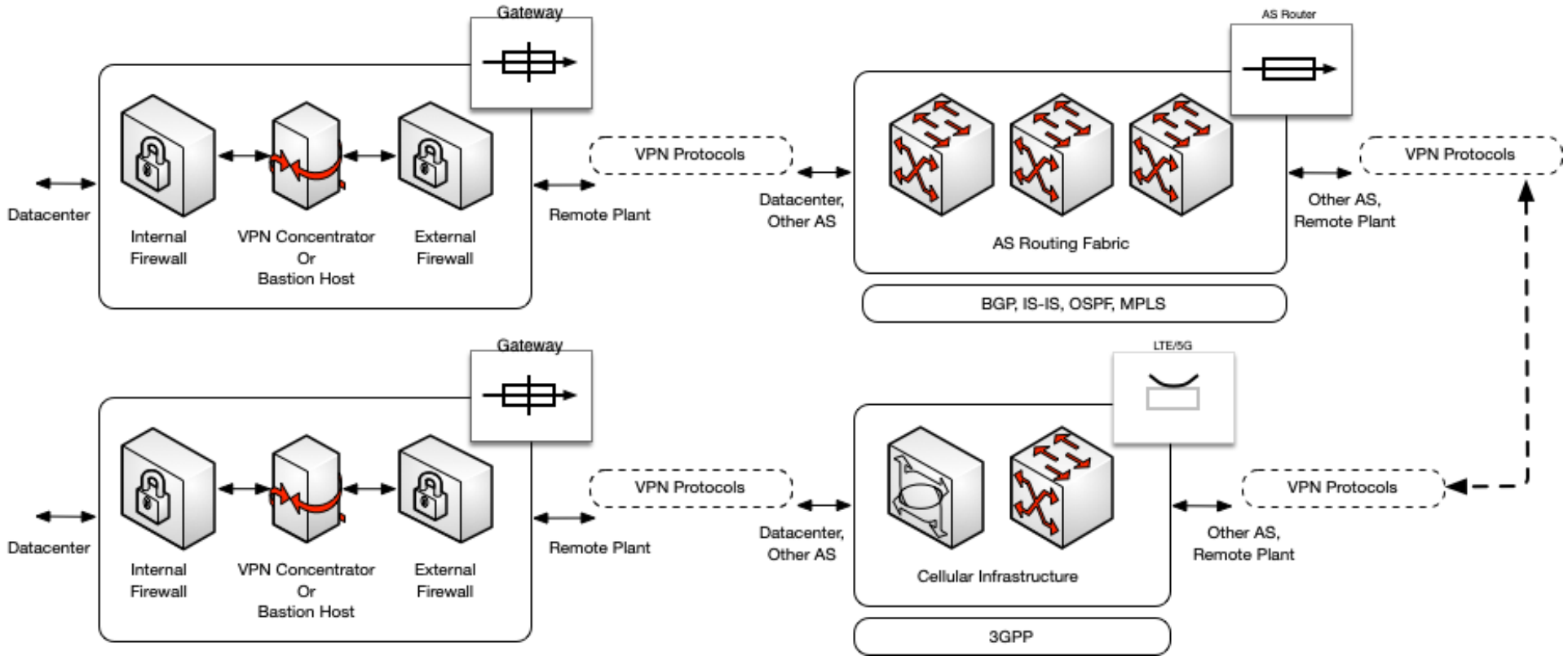
METHODOLOGY



CONCEPTUAL MODEL AND ATTACK SURFACE



CONCEPTUAL MODEL



TECHNICAL IMPLEMENTATIONS

Communications

VPN Configurations
- Site-to-site, MPLS, SD-WAN
- Remote Access

Infrastructure
- LTE/5G, wired internet, Power-line Comms

VPN Protocols
- IKEv2/IPSec, TLS, ***PPTP***, ***L2TP***, GRE
- OpenVPN
- TLS/SSH, TLS/HTTPS

Endpoints

Gateways
- Bastion Hosts
- VPN Gateways

Network Architecture
- Internal-, external-facing firewalls
- Isolated DMZ
- Segmented, with other services/systems

SYSTEM ATTACK SAMPLE

Attack

Exploiting Common Services

Class: Trusted Relationship

Action: If an attacker can compromise DNS records, that attacker can potentially redirect traffic to domains they control and either poison results or transfer information.

Mitigations

(1) **Firewall configurations** that do not allow traffic from the gateway to systems other than remote sites and required local services;

(2) Use of **secure protocols** like DNSSec [10] whenever possible to verify data and connections

(3) **Logging and monitoring** of packet traffic for anomalous behavior like larger than expected packet sizes

COMMUNICATION ATTACK SAMPLE

Attack

False Data Injection

Class: Trusted Relationship

Action: An adversary can leak information to other peering services resulting in redirection of traffic to malicious domains.

Mitigations

Operators have no technical means to prevent this kind of attack. They can only apply compensatory controls via strong integrity-preserving or confidentiality-preserving techniques.

MITIGATION SUMMARY

Logging, monitoring, SIEM and SOAR

Threat hunting

Adversarial pursuit

Network and host forensics

Honeypot/Honeynet

Equipment Replacement

MFA

Endpoint protection

System Hardening

Restrictive Configuration

Secondary DMZ/Zones

Clear trust relationships/dependencies

Secure, verifiable protocols

Patch and vulnerability management

HW/SW inspections

Third party liability

Autonomous systems

Heterogeneous ISP/secondary comms

Contingency travel to site

VPN Configuration

THANK YOU!