Threats and Security Requirements for SMRs

Lon Dawson, Mike Rowland, Chris Lamb
{ ladawso | mtrowla | cclamb }@sandia.gov

SMR Use Cases

Prefab NPP

More sites, users

Better team players

Different fuels

Integrated security

Passive Safety

Use → Threat

Prefab NPP	***Transportation***
More sites, users	***Proliferation***
Better team players	***Single Target***
Different fuels	***Different Goals***
Integrated security	***Target Mobility***
Passive Safety	***Active Security***

Threat Actors

Not much of a change.

Attack Surface

Diluted

- More SMRs

Extended

- Factory to plant

Novel

- Standard Misalignment
- Regulatory guidance

Threat Types

Physical/Cyber

- Understand physical attacks
- Getting better with cyber
- Cyber multiplier for physical attacks

Inside/Outside

- Good operator reliability programs
- Adversaries have more operator access
- Pre-established cyber staging

New Vectors

Remote security and control systems

- What would this even look like?
- AuthN/Z? Encryption? Failover and fallback?
- Replay?

Reduced staffing

- Multi-person rules
- Centralization of roles

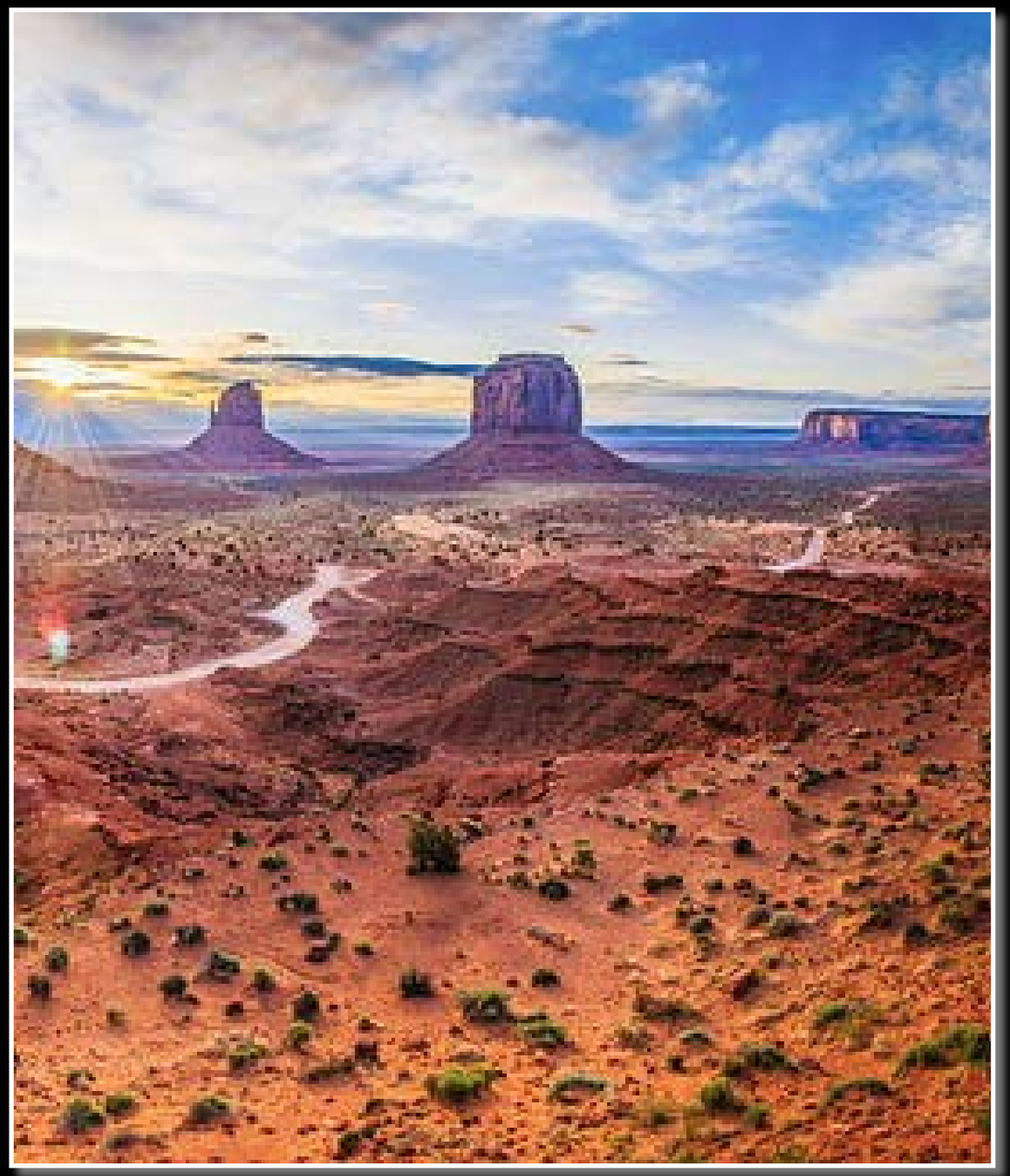
Passive Safety

$\not\rightarrow$

Passive Security

Scenario: Distributed Control

- SMR for mining company in American southwest
- Third party remote centralized management
- IPSEC VPN for monitoring



Scenario: Hybrid Attack

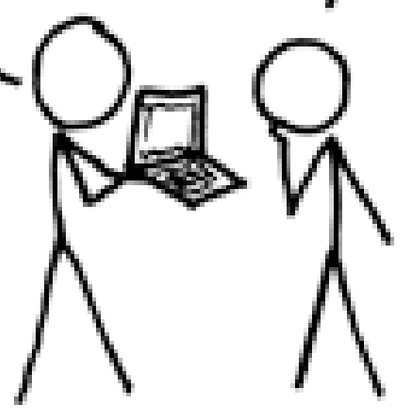
- SMR for small power coop
- High load during winter storm
- Pre-existing unknown implants
- Compromised insider

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

BLAST! OUR EVIL PLAN IS FOILED!

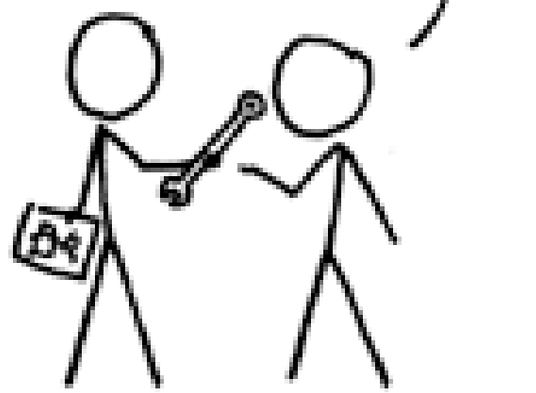
NO GOOD! IT'S 4096-BIT RSA!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.

GOT IT.



“The only constant is change.”

–Heraclitus

?