UPISC UNIVERSITY OF PITTSBURGH INFRASTRUCTURE SENSING

COLLABORATION WORKSHOP

NATIONAL ENERGY TECHNOLOGY LABORATORY

Simplifying the Deployment of Intrusion-Tolerant SCADA by Leveraging Cloud Resources

Maher Khan (maherkhan@pitt.edu) and Amy Babay (babay@pitt.edu)
Computer Science, SCI, University of Pittsburgh

What is SCADA?

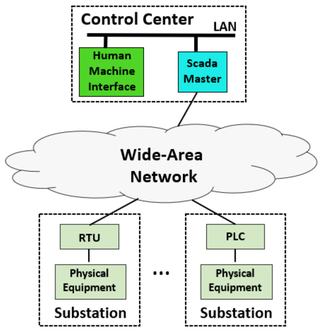


Fig 1: SCADA system

- ***Supervisory Control and Data Acquisition (SCADA)*** systems provide monitoring and control for the power grid:
  - Collecting and processing data from various sensors
  - Allow human operators to view the system state
  - Execute control commands to manage equipment in power substations
- SCADA systems must be continuously available and correct:
  - Any failures or downtime can lead to equipment damage and prolonged power outages [BTAPA18].
  - However, they are increasingly subjected to nation-state-level attacks

Intrusion Tolerance through BFT

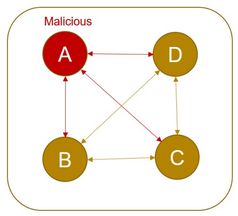


Fig 2: BFT system with 4 replicas (*f=1*)

- ***Intrusion tolerance*** is the ability to operate correctly even while partially compromised by an attacker.
- ***Byzantine Fault Tolerant Replication (BFT):*** Enables the system to work correctly as long as no more then ***f*** out of ***3f+1*** replicas are compromised

Deploying and Managing Intrusion-Tolerant SCADA is Challenging

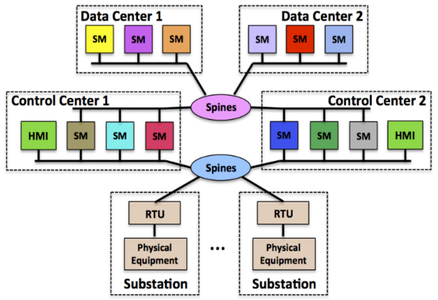


Fig 3: SCADA Architecture with 3 replicas in each of the two control centers and two data centers (configuration 3+3+3+3) [BTAPA18]

- Intrusion tolerance in practice requires more than just BFT replication
- We need to support the assumptions that BFT replication rely on such as:
  - Ensuring diversity of replicas
  - Supporting Proactive Recovery [CL02]
  - Network Attack Resilient Architecture [BTAPA18]
- This leads to a complex SCADA with multiple sites and numerous replicas that is difficult to deploy and manage.

Our Approach: Leverage Cloud Resources to Simplify Deployment and Management of SCADA

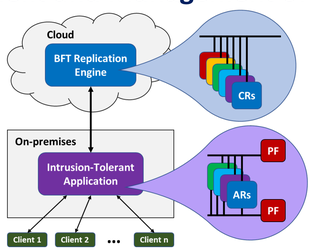


Fig 4: Cloud-based Hybrid Management Intuition

- ***Cloud providers*** may manage additional sites to make SCADA deployment more feasible, while ***system operators*** deploy and manage their on-premises site(s).
- Application state and requests in the cloud are encrypted with keys only available in the on-premises replicas

Our Solution: Cloud-based Hybrid Management

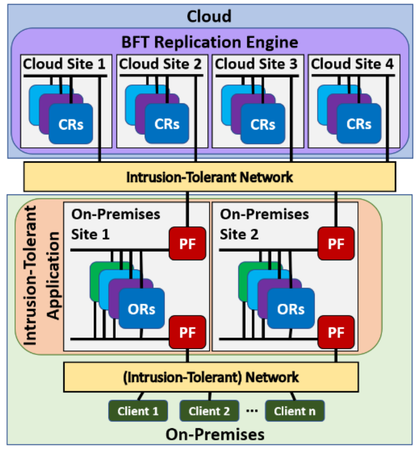


Fig 5: Decoupled Architecture

- System operators manage their applications, while leveraging ***intrusion-tolerant ordering*** and ***encrypted storage services*** from a cloud provider
- Cloud and On-Premises domains are separated such that BFT replication is completely offloaded to the cloud.
- We use ***threshold signatures*** to simplify the communication and trust interface between the domains.

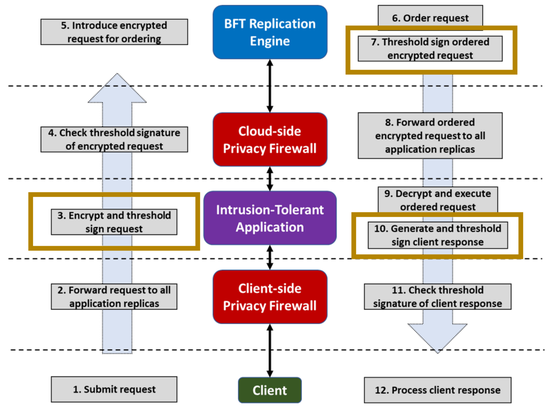


Fig 5: Client Request Flow

- **Additional benefits:**
  - Domains don't require knowledge of each other's internals, simplifying communication and management.
  - Introduces management diversity between on-premises and cloud domains

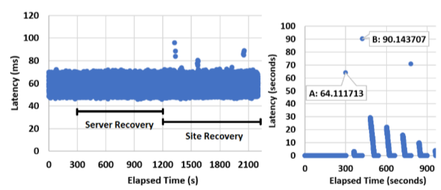
Implementation and Evaluation

- We implemented ***Decoupled Spire***, power grid SCADA system, using our cloud-based hybrid management solution.
- It is built on open-source Spire version 1.2.

	Avg Latency	99^{th} percentile
Decoupled Spire (f_o=1, f_c=1)	58.9 ms	69.6 ms
Confidential Spire 2021 [KB21] (f=1)	50.1 ms	60.9 ms
Spire 2018 [BTAPA18] (f=1)	49.9 ms	60.5 ms
Decoupled Spire (f_o=2, f_c=2)	62.0 ms	74.3 ms
Confidential Spire 2021 [KB21] (f=2)	56.5 ms	69.8 ms
Spire 2018 [BTAPA18] (f=2)	53.4 ms	64.1 ms

Table 1: Normal Operation Performance on LAN with emulated latencies between sites for 36000 updates over 1 hour

- **Normal Evaluation**:
  - Decoupled Spire has an average 9ms (18%) overhead compared to Confidential Spire and Spire at ***f=1***.
  - Furthermore, no request crosses 100ms latency which meets the SCADA application's requirements



(a) Server and Site Recovery (b) Domain Recovery

Fig 6: Performance during Attack Recovery

- **Attack and Recovery Evaluation**:
  - Server Recovery: no latency increase (recovery happens in-site)
  - Site Recovery: some spikes in latency (state is sent over WAN).
  - Domain Recovery: request processing halts until enough on-premises replicas catches up.
- **Diversity Evaluation**:
  - Decoupling greatly reduces the degree of diversity needed for the application.
  - The cloud service provider can use the same set of (diverse) replicas to serve many applications (amortizing the cost)

References:

- [BTAPA18] Babay, A., Tantillo, T., Aron, T., Platania, M., & Amir, Y. (2018, June). Network-attack-resilient intrusion-tolerant SCADA for the power grid. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 255-266). IEEE.
- [CL02] Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), 20(4), 398-461.
- [KB21] Khan, M., & Babay, A. (2021, June). Toward intrusion tolerance as a service: Confidentiality in partially cloud-based BFT systems. In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 14-25). IEEE.