Some Thoughts on Zero-Trust, Resilience, and 5G…

Presented at ISART

13 August 2020

Wayne Phoel
Institute for Systems Research (ISR)
wphoel@umd.edu

With acknowledgment to the Applied Research Laboratory for Intelligence and Security (ARLIS)
Who (Doesn’t) Trust Whom?

Two Views for Zero Trust:

- Network Operators: No implicit trust of components, users, employees

- Users: All of the above + Network Operators
Strengthening Access Control

Observing behavior adds another dimension to trust.

Role-Based Access

Behavioral Monitoring

These basic Zero-Trust concepts re-define the moat around the castle.
If you’re in, you’re in.

Multifactor Authentication

Micro-segmentation

If you’re in, you’re in.
Resilience and Situational Awareness

- Resilience: the capability to recover after misfortune
- Internal network situational awareness needed to detect and react to undesired behavior
- Multi-level trust metric can aid adaptive network control
- Customized virtual network functions may enable monitoring, evaluating trust, and reconstitution
Thank you