ARMOR: BUILDING A COMMUNITY FOR PROTOCOL RESILIENCE

SIDE MEETING TWO
IETF 124
NICK SULLIVAN, CDT

NOTE WELL

HTTPS://WWW.IETF.ORG/ABOUT/NOTE-WELL/

BY PARTICIPATING IN THE IETF YOU AGREE TO FOLLOW IETF PROCESSES AND POLICIES. THIS NOTE WELL IS A REMINDER OF SOME OF THOSE POLICIES.

ARMOR: A NEW MAILING LIST

Existing IRTF groups each cover part of the space

- MAPRG does measurement
- HRPC handles policy/human-rights
- PEARG focuses on privacy enhancements
- GAIA explores global access and architectural connectivity

No single forum is dedicated to end-to-end technical resilience and deployment research in adversarial or disrupted environments.

END-TO-END CONNECTIVITY

Deep-packet inspection systems actively block or modify protocol handshakes, with studies showing up to 15 % of TLS connections are manipulated by on-path devices.

Traffic throttling and injection degrade performance or inject fake responses, causing application failures.

Targeted protocol blocking forces services to fall back to less efficient or less secure methods, fragmenting end-to-end reliability.

WHICH RESEARCH ACTIVITIES COULD ARMOR DRIVE?

- Documentation of current tampering landscape
- Measure current tampering systems and their evolution
- Improve and harden protocols against interference
- Operational guidance and best practices
- Generalizable insights and recommendations for future IETF work

- Experimental specifications and software??
- Build testbeds, tools, and guidance??

WHAT COULD BE USEFUL OUTPUTS?

Initial:

- Minimal terminology and threat model
- Operator survey: pain points and desired mitigations

Long-term:

- Experimental IRTF drafts: taxonomy, test methods, fallback guidance
- Draft recommendations to relevant WGs (TLS, MASQUE, DNSOP)

WHAT IS THE UNIQUE FOCUS?

Close the loop: measure>design>build>validate

- ARMOR: mitigation engineering, testbeds, operator guidance, cross-protocol insights
- MAPRG: large-scale measurement methods and results
- PEARG/HRPC: privacy or human-rights framing and implications
- Coordination, not duplication

WHAT ARE RELEVANT ACADEMIC COMMUNITIES AND VENUES?

- IMC, PAM, FOCI, PETS
- USENIX Security, NDSS, IEEE S&P, ACM CCS, SIGCOMM, CoNEXT, HotNets?
- Practitioner communities: CDNs, ISPs, browser/networking teams

Do we have sufficient thrust in doing real, continuous work in the group?