Some Security Issues for the Future Wireless Internet and GENI

Contact: Wade Trappe
GENI Wireless Working Group
WINLAB, Rutgers University
trappe@winlab.rutgers.edu
Tel: (732) 932-6857 x644

Wireless Security Experiments for the FI

- *Forensics in the core:* The edge will be the point-of-entry for attacks on the broader network. Can the traffic analysis be performed in the backbone to identify/flag/filter/etc. traffic originating from the wireless edge?
- *Heterogeneity:* The FI will consist of a more heterogeneous collection of devices, with inherently disparate management domains. Issues of handoff and handoff, interworking, policy enforcement/translation/enforcement will be key to a seamless user experience. Issues of optimized AAA are possibly interesting, especially in support of new opportunistic communication paradigms.
- *Trustworthy Location-based Addressing:* Location is being explored as an alternative to traditional addressing. Can we ensure that location claims are verifiable? Can we set up location-restricted AC mechanisms (e.g. anti-email zones? or anti-VOIP zones?)
- *Cache-and-Forward:* The FI might consist of routers with extensive memory for caching. Such a paradigm is beneficial for Infostation, DTN, or even vehicular paradigms. A critical question is how trustworthy interactions can be quickly built and torn down (especially when client devices are resource limited). Fast authentication?

Some Security Challenges and Requirements for Wireless GENI

- The security challenges for the Wireless GENI portions include:
  - Ensuring the facility itself is secure and trustworthy
  - Ensuring the facility's security does not interfere with the quality and reliability of real experiments (especially security experiments)
  - Providing enough resources to facilitate interesting wireless, and wireless-to-wired security experiments
- Some notable hurdles that need to be addressed:
  - Securing Virtualization and Slicing
  - Providing measurement infrastructure to monitor behavior of wireless subnets
  - Specification of formal, operational security procedures for GENI (e.g. how frequently nodes should be re-imaged, etc.)
  - Key management across wired and wireless domains (key management should be compartmentalized to prevent theft of wireless devices from compromising broader GENI)
  - A set of certified security tools (e.g. crypto) should be provided, along with specifications

Dig-Down Discussion on Security Issues

- Securing Virtualization:
  - Virtualization will play an important role in both future testbed facilities and future networking technologies (programmable routers)
  - Cross-slice boundaries and enforcement is very challenging
  - Can a clever adversary exploit a non-obvious shared resource for an attack?
  - Addressing this issue will not only benefit the wireless portions of GENI, but will also benefit the core of GENI, where programmable routers are being considered
- Validity of Experiments in the Presence of GENI Security:
  - One concern is whether adding security needed to protect GENI might invalidate the science of experiments being conducted on GENI
    - Example: Would GENI's packet-level authentication mechanisms add extra latency and communication overhead that would mask true protocol performance outside of GENI?
  - Security mechanisms used to protect GENI should be explicitly explained to all experimenters
    - In particular, performance specifications of authentication and other cryptographic tools should be provided to experimenters.