Spectrum Security & Enforcement in Spectrum Sharing

Jerry Park
(jungmin@vt.edu)

Dept. of Electrical & Computer Engineering
**Virginia Tech**

Jan. 2014

VirginiaTech

Security and Privacy Threats

- When different stakeholders share a common resource, such as spectrum, security and enforcement become critical considerations that affect the welfare of all stakeholders.

- Threats to spectrum sharing often exploit the mechanisms which enable coexistence
 - Viz, spectrum sensing and geolocation databases

Taxonomy of Threats to Spectrum Sharing
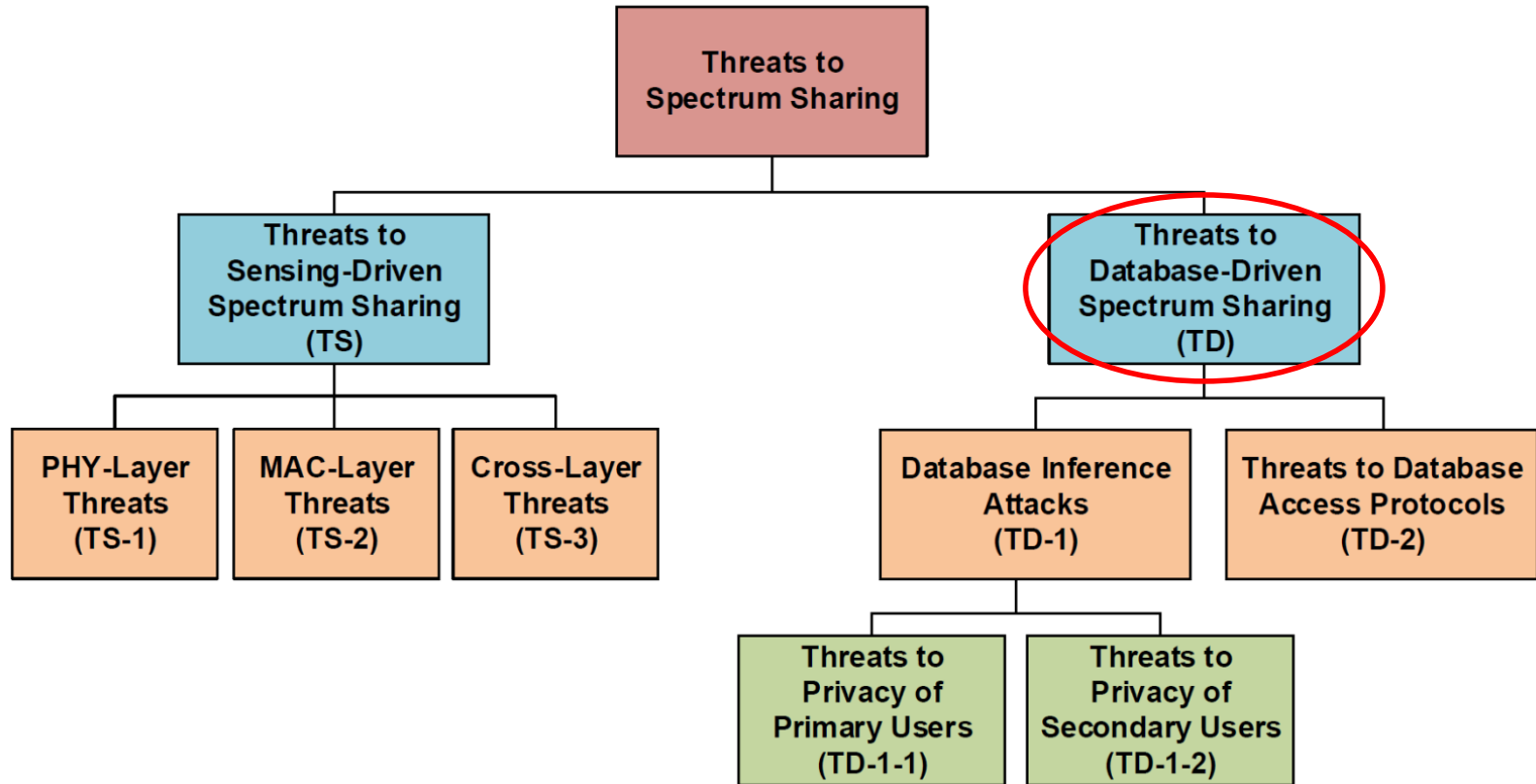
Database Inference Attacks

- ## Threats to the privacy of primary users (PUs)

  - Through seemingly innocuous queries to the database (DB), SUs can determine / infer the type, location, and operating characteristics of PU transmitters

  - A critical concern when the PU transmitters are nodes in a military or intelligence gathering network

- ## Threats to the privacy of secondary users (SUs)

  - Location privacy
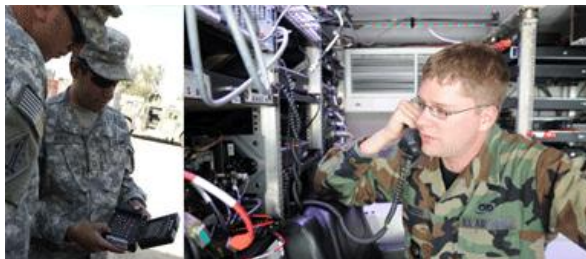
Threats to the Database Access Protocol

- Internet Engineering Task Force (IETF) and others are studying security concerns specific to DB access protocols
  - E.g., *Protocol to Access White Space database* (*PAWS*)
- Known security issues
  - Modifying a device to masquerade as another certified device
  - Spoofed database
  - Modifying or jamming a DB query
  - Modifying or jamming a DB response
  - Masquerading as a DB to terminate access or unfairly limit spectrum access to other devices

VirginiaTech

Threat Countermeasures & Enforcement

- Ex ante (preventive) approaches
  - Mechanisms for "spectrum access control"
  - Ex) policy-based radios (w/ policy reasoner), secure radio middleware, tamper resistance techniques, radio integrity assessment techniques, hardware-based compliancy modules

- Ex post (punitive) approaches
  - Remediate malicious or selfish behavior *after* a harmful interference event has occurred
  - Ex) schemes for uniquely identifying rogue transmitters (e.g., PHY-layer authentication), localization of non-compliant transmitters, punishment of non-compliant transmitters

VirginiaTech