Motivation
- SDR/CR platforms expose the lower-layers of the protocol stack to the “public”
- Various attacks and spectrum policy (etiquette) violations are possible
- We aim to regulate the future radio environment and ensure trustworthy radio operation

Potential Threats
- Poor programming
- Greedy exploitation
- Simply Ignoring Etiquette
- Jamming
- Primary user emulation (PUE): adversaries emulate the incumbent signal’s characteristics
- Rogue terminals send tainted spectrum sensing reports to fusion center

Approach and Impact

<table>
<thead>
<tr>
<th>Our Approach</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Formulate regulation of cognitive radio behavior as an access control problem</td>
<td>• Cognitive Radios will be an important emerging wireless technology</td>
</tr>
<tr>
<td>• Onboard enforcement will employ a TCB. External regulation would employ anomaly detection</td>
<td>• Developing security mechanisms will help ensure they are not misused/abused</td>
</tr>
</tbody>
</table>

Spectrum Law Maker
- Define and disseminate the spectrum laws
- The laws may be defined by modifying XGPL to describe access control policies, i.e. what actions are allowed for a CR to perform (e.g. channel allocation)
- Action-reaction mechanisms (i.e. punishment) would describe onboard and external regulation

Trusted CR Platform
- TRIESTE-TCB (Trusted Computing Base) includes all the hardware and software that enforces universal laws and etiquette policies
- Monitor/verifier: a Controller which can interpret and enforce any well-formed Law
- Verify that current radio environment adheres to current spectrum policy and radio platform profiles
- Verify whether downloaded policy profiles conform to radio platform profiles
- Verify whether solution profiles generated by Cognitive Engine is in accordance w/ policy profiles
- A Wake up/Kill Switch would allow external enforcement of spectrum laws by allowing the CR to be commanded to shut down

External Law Enforcement
- Spectrum sensors, which may be other CRs or a special infrastructure, monitor the local radio environment
- The Distributed Spectrum Authority (DSA) is a fusion center that collect radio measurements and make punishments
- Localization of signal source can detect primary user emulation
- Ensuring the trustworthy of sensed data is important and robust fusion rules are being developed to protect against tainted data
- RF fingerprinting methods allow for the identification of rogue terminals