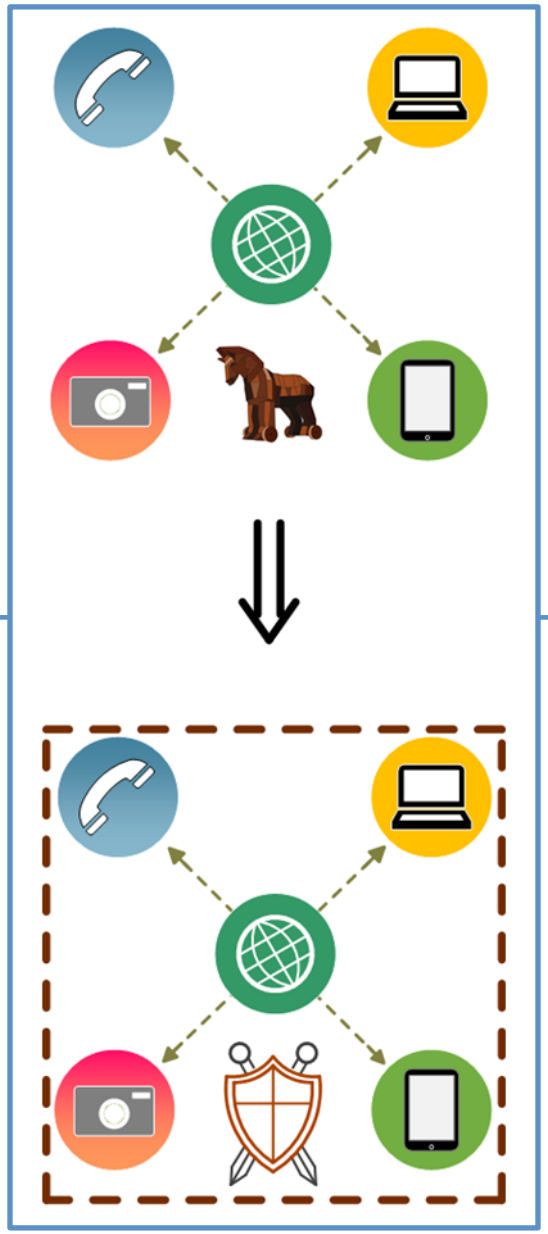
Hardware Trojans in Wireless Networks: Risks & Remedies

Challenge:

- Wireless networks exchanging valuable information over public channels are vulnerable to attacks
- Our challenge is to:
  - Expose "Gap" between wireless transceiver operating point and physical limits of communication
  - Highlight the risk that hardware Trojans pose in wireless networks
  - Develop appropriate remedies



Solution:

- Investigate hardware Trojan attack models
- Develop Trojan-agnostic remedies
- Experimental demonstration in 802.11a/g networks

Award: NSF 1514050
PIs: Yiorgos Makris, Aria Nosratinia

Scientific Impact:

- Focus on unexplored threat models: hardware root of trust
- Secure deployment of wireless networks in a broad range of applications, fostering technology trustworthiness
- Proposed remedies can eliminate the "Gap"

Broader Impact:

- Improvements in future wireless standards
- Module on Trusted and Secure Wireless Networks will be included in existing courses
- Outreach via Cybersecurity Research and Educational Institute at UT Dallas targeting high school students