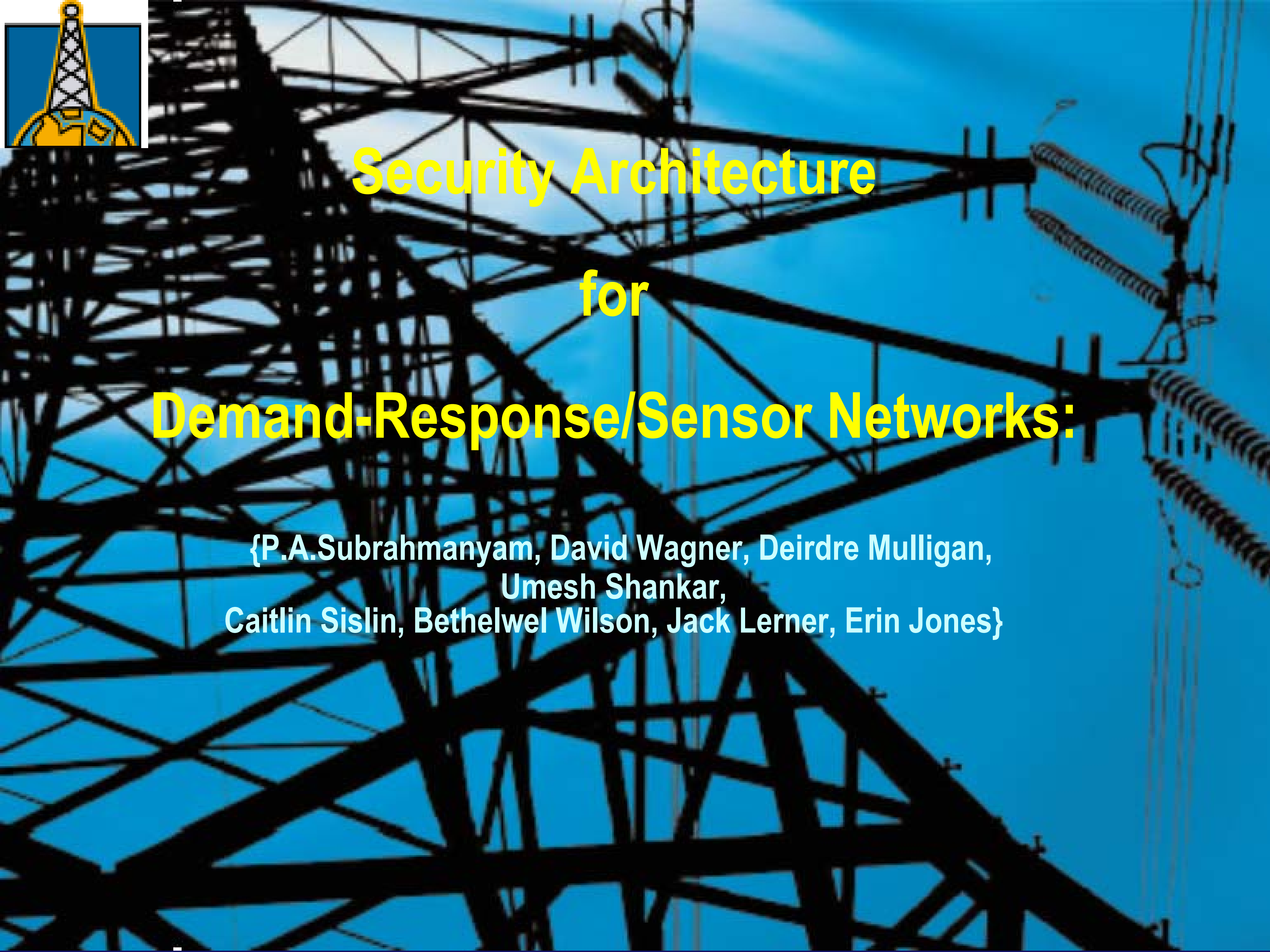


Security Architecture

for

Demand-Response/Sensor Networks:

{P.A.Subrahmanyam, David Wagner, Deirdre Mulligan,
Umesh Shankar,
Caitlin Sislin, Bethelwel Wilson, Jack Lerner, Erin Jones}

Acknowledgements

- Many thanks for their support!
  - CEC/CIEE
    - Gaymond Yee & Ron Hofmann
    - TAC
- Profs. Paul Wright, Ed Arens, Jan Rabaey, …
- Industry Partners
  - Bell Labs
  - Others

Introducing the Team

- P.A. Subrahmanyam
- David Wagner (UC Berkeley, CS)
    - Umesh Shankar
- Deirdre Mulligan (UC Berkeley, Law)
    - Jack Lerner (Clinic Fellow)
    - Caitlin Sislin
    - Bethelwel Wilson
    - Erin Jones

Agenda

- Introducing the team
- Project: Security Architecture for DR/Sensor Networks
  - Background & Motivation
  - Goals & Scope
- Task Status
  - Sensor Network Security & Privacy
  - Security Issues in Agile/Software Defined Radios
  - Legal and Public Policy Issues
- Summary
- Open discussion
  - Ways to maximize the impact of this project

Research Goals
Security & Privacy in DR/Sensor Networks

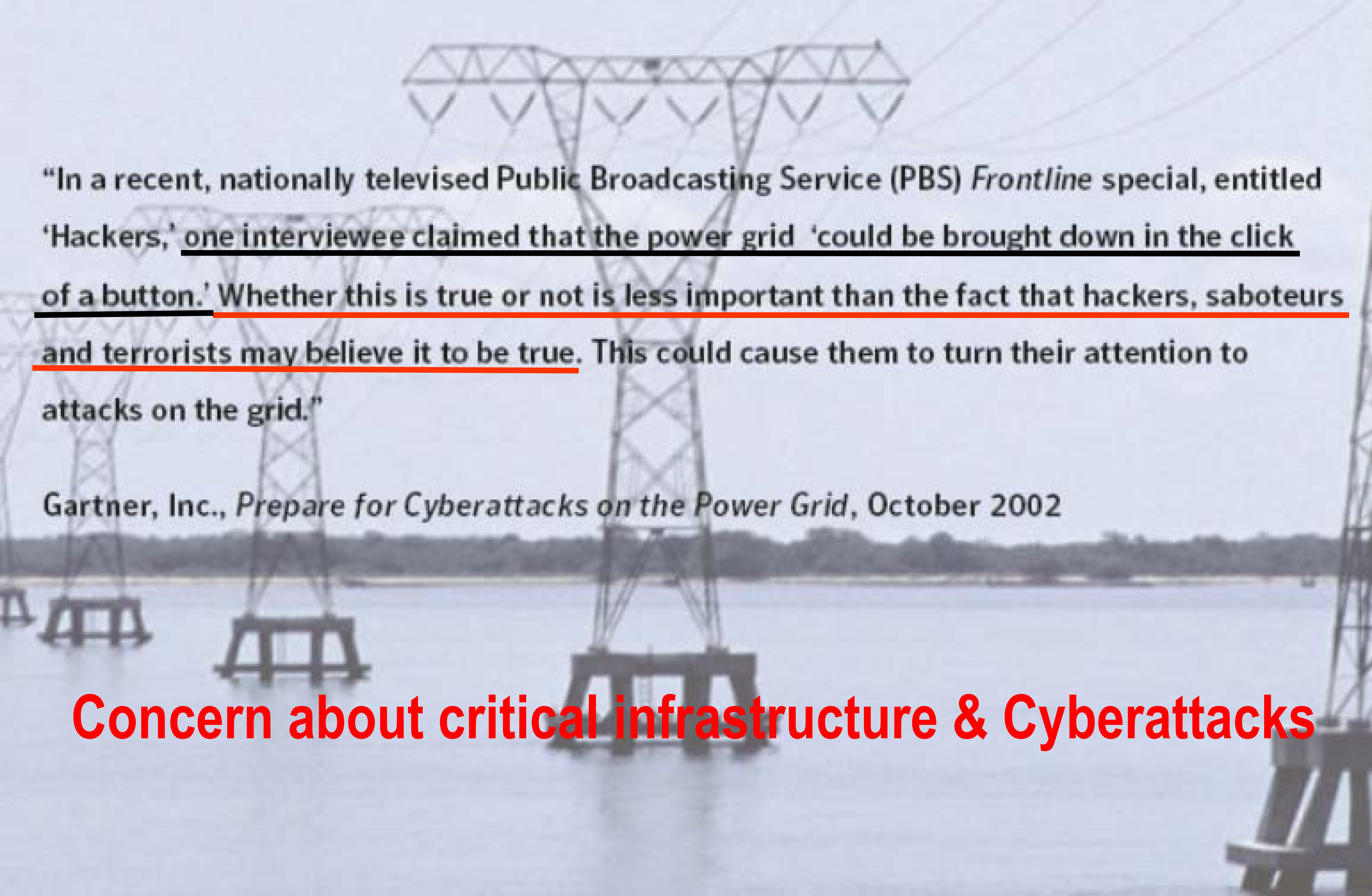
- Research Goal
  - Investigate Security and Privacy issues that are relevant in the context of Demand response/sensor networks
    - Identify and articulate relevant security issues.
    - Develop a holistic (framework for) DR network security architecture
      - Explication and validation of basic notions.
      - Establish a basis for further research & prototyping

- Aligned with imperatives under the “security” topic of the Network Management Research Opportunity Notice.
  - “Technologies (are needed) to ensure information cannot be either stolen, altered, or corrupted. Security also includes the ability to withstand attacks that attempt to partially or fully incapacitate the network.”
      - » Gaymond Yee & Ron Hofmann

Security Architecture
for
Demand-Response/Sensor Networks:

Background & Motivation

Even Before Demand-Response & Sensors…



“In a recent, nationally televised Public Broadcasting Service (PBS) *Frontline* special, entitled ‘Hackers,’ one interviewee claimed that the power grid ‘could be brought down in the click of a button.’ Whether this is true or not is less important than the fact that hackers, saboteurs and terrorists may believe it to be true. This could cause them to turn their attention to attacks on the grid.”

Gartner, Inc., *Prepare for Cyberattacks on the Power Grid*, October 2002

Concern about critical infrastructure & Cyberattacks

Security in DR/Sensor Networks: Background & Motivation

- Security is important
    - Infrastructure security is critical.

- Wireless security is tricky.

- Wireless Sensor networks and Demand-response technologies represent a new component being injected into a legacy system.

→ It is important to understand & address security in this context

- Since DR networks are intended for deployment in the public domain, and are eventually designed to target the majority of the state's population, privacy issues are very relevant in this context.

→ Security and privacy are key issues that need to be addressed in the context of Demand-Response/Wireless sensor-networks

Security & Privacy:
Early, System-level Perspective

- Security and privacy should be addressed early in the design.
- Security should be considered from a holistic perspective.
- Security and Privacy/legal issues are closely intertwined, so it is best to address them both, in the early stages.

Security Architecture for Demand-Response/Sensor Networks:

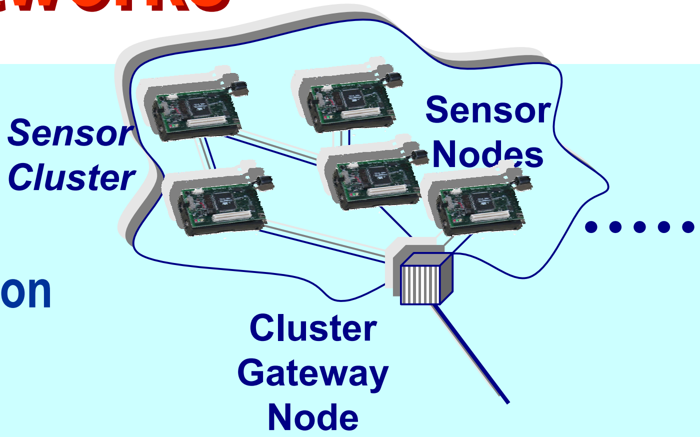
Goals & Scope

Representative Questions.

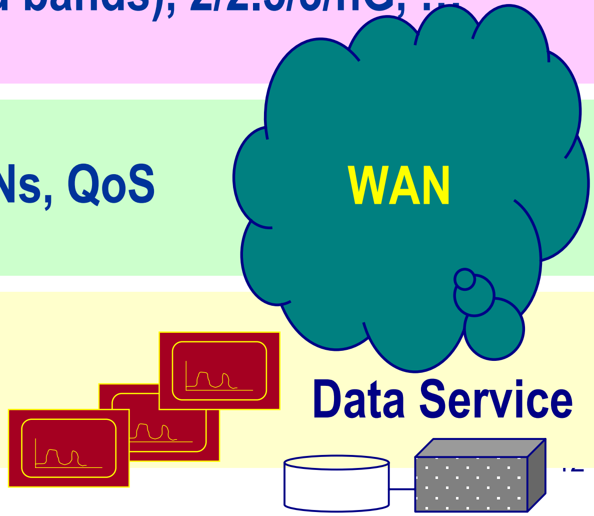
- What are the subsystems and networks that are representative of potential "typical" Demand-response networks?
- What are the potential sources of vulnerabilities in DR/sensor networks?
- What is a desirable/meaningful notion of security in this context?
- What are the legal and privacy concerns of relevance?
- What mechanisms are needed/available/should be developed to address the security issues?
- And how do these interact with the legal and privacy/public policy concerns?
- "Security in the small"
  - Investigate specific vulnerabilities and ways to address them
    - E.g. Link-layer routing algorithms/protocols
- "Security in the large"
  - Security services/abstractions that may be provided by sensor networks, independent of specific HW/SW/OS implementations
- Technologies, algorithms, organizational processes, …

Demand-Response Network Architecture: Typical Subsystems & Subnetworks

- Building level ("User premises")
  - Scalable Sensor clusters/ Sensor network
  - Cluster gateway node(s)
  - Building control subsystem with communication
    - Building gateway node(s)
      - Home meter
      - Enterprise monitoring & control system
    - Scalable LAN/WAN connectivity in the building gateway node
- Access networks
  - Wireless e.g., Mesh networks (Licensed/unlicensed bands), 2/2.5/3/nG, …
  - Wired e.g., DSL, Cable, Leased line, PON, …
- Backhaul
  - Private Enterprise Networks, e.g., leased lines/WANs, QoS
  - Public Internet
- Other Networks
  - Utilities e.g., PG&E
  - Power generators
  - SCADA



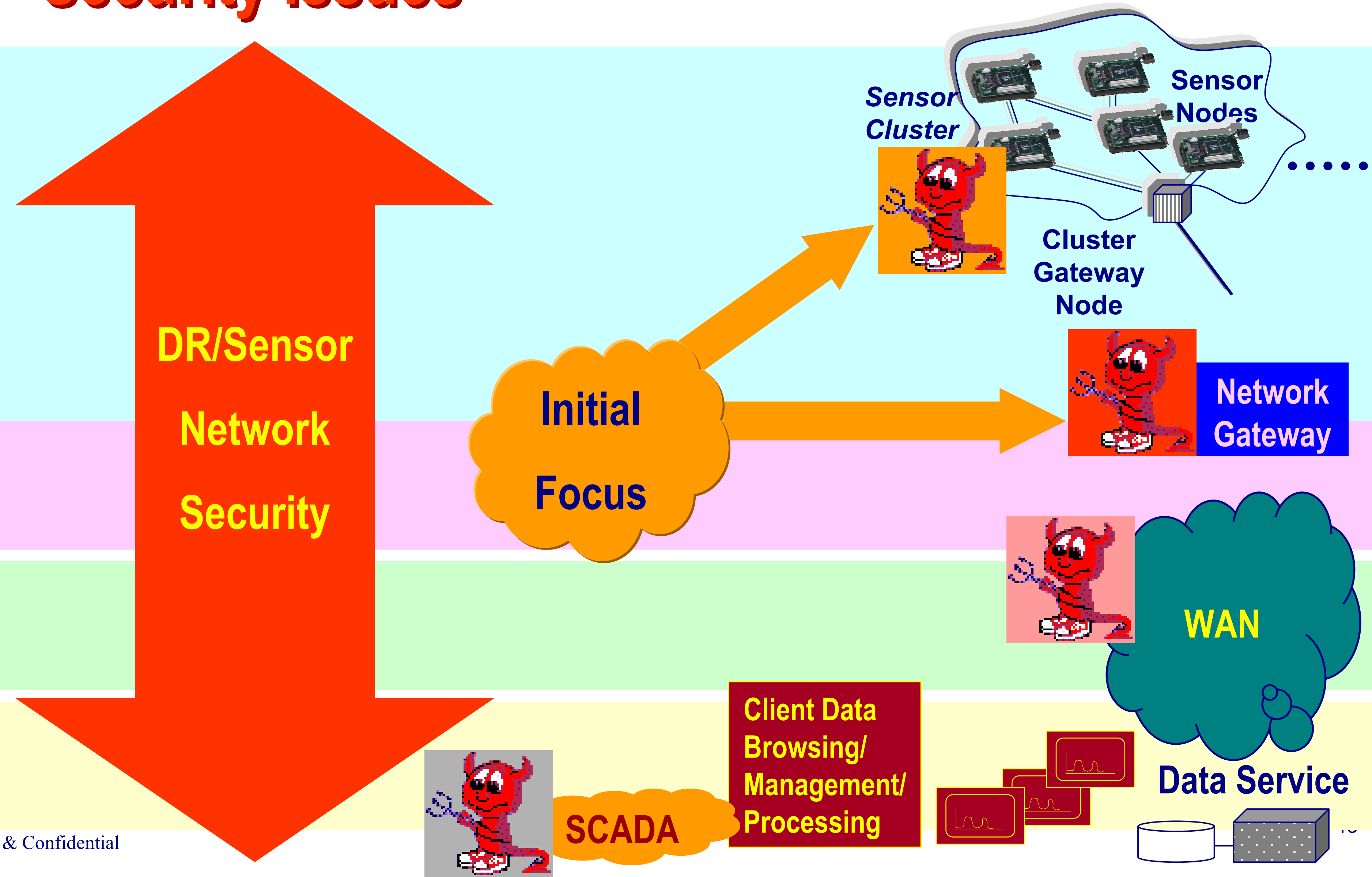
Network Gateway



Client Data Browsing/ Management/ Processing

SCADA

Security Issues



DR/Sensor

Network

Security

Initial

Focus

Sensor Cluster

Sensor Nodes

Cluster Gateway Node

Network Gateway

WAN

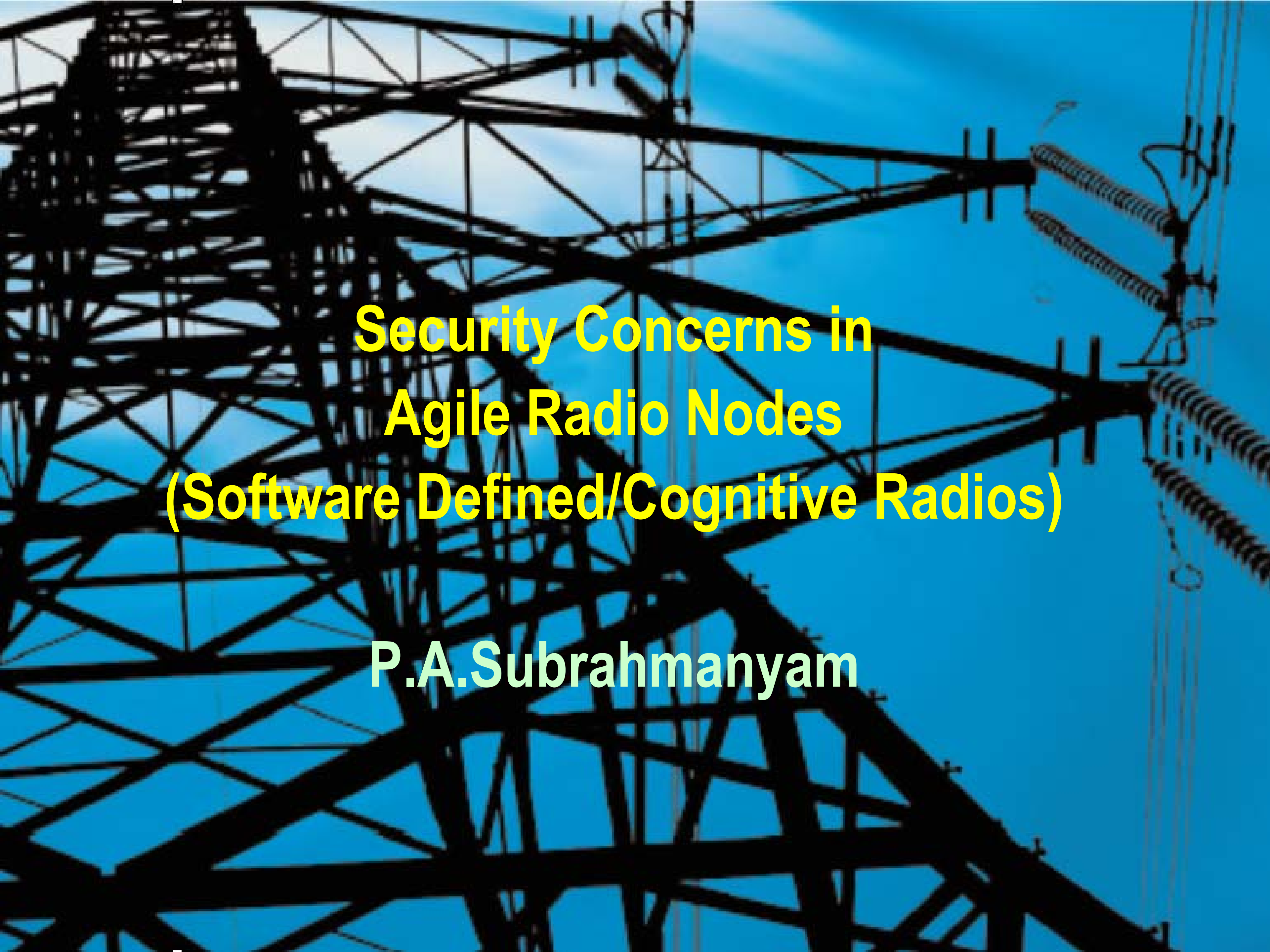
Data Service

Client Data Browsing/ Management/ Processing

SCADA

Agenda

- Introducing the team
- Project: Security Architecture for DR/Sensor Networks
  - Background & Motivation
  - Goals & Scope
  - Project structure & components
- Task Status
  - Sensor Network Security & Privacy
  - Security Issues in Agile/Software Defined Radios
  - Legal and Public Policy Issues
- Summary
- Open discussion
  - Ways to maximize the impact of this project



Security Concerns in Agile Radio Nodes (Software Defined/Cognitive Radios)

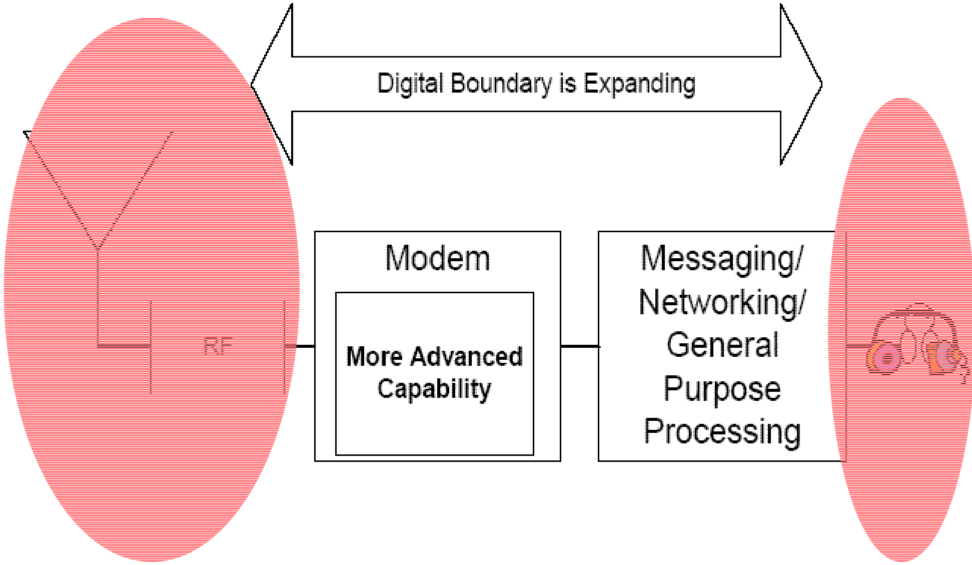
P.A.Subrahmanyam

Outline

- Agile Radios & Demand Response Networks
  - What is an Agile/Software Defined Radio (SDR)?
    - Why and where is technology useful?
  - What role can SDRs have in Demand-Response Networks?
- Security issues in Software Defined Radios (SDRs)
  - What are the security concerns introduced by SDRs?
  - What are the potential sources of threats, attack modes?
  - Is there a model that provides a framework for the discussion of SDR related security?
    - SDR Security Framework
- Summary
- Future Plans

What is a Software (Defined) Radio?

- Software (Defined/Based/…) Radios:
  - Radio systems whose functionality is partially implemented in software.



Digital Boundary is Expanding

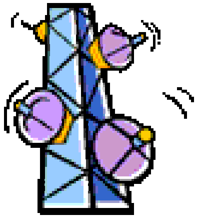
RF

Modem

More Advanced Capability

Messaging/ Networking/ General Purpose Processing

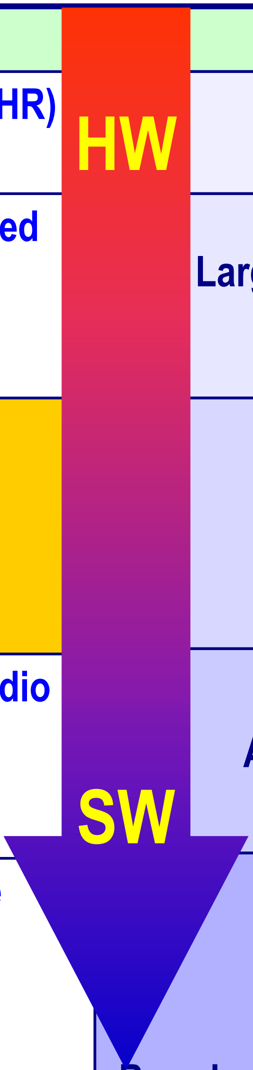
- Examples:
  - Basestations (today)
  - Military (leaders)
  - Commercial Handsets
    - Emerging (2005)
  - Several other applications



“Software Radio”: Tiers 0-4

(Courtesy SDR Forum)

Tier	Name	Description
Tier 0	Hardware Radio (HR)	Hardware only
Tier 1	Software Controlled Radio (SCR)	Largely HW, Software for a few controls (interconnects, power levels) Not frequency bands, modulation, …
Tier 2	Software Defined Radio (SDR)	Software plays a significant role: Modulation, protocols, … Antenna switch may still be required
Tier 3	Ideal Software Radio (ISR)	Analog only at the boundaries (Antenna, Microphone, Speaker)
Tier 4	Ultimate Software Radio (USR)	Extreme Reference Model. Fast switching across broad frequency spectrum Broader functionality than a typical phone (+ GPS, Smart card, Video, TV, etc.)



Advantages of Software Defined Radios

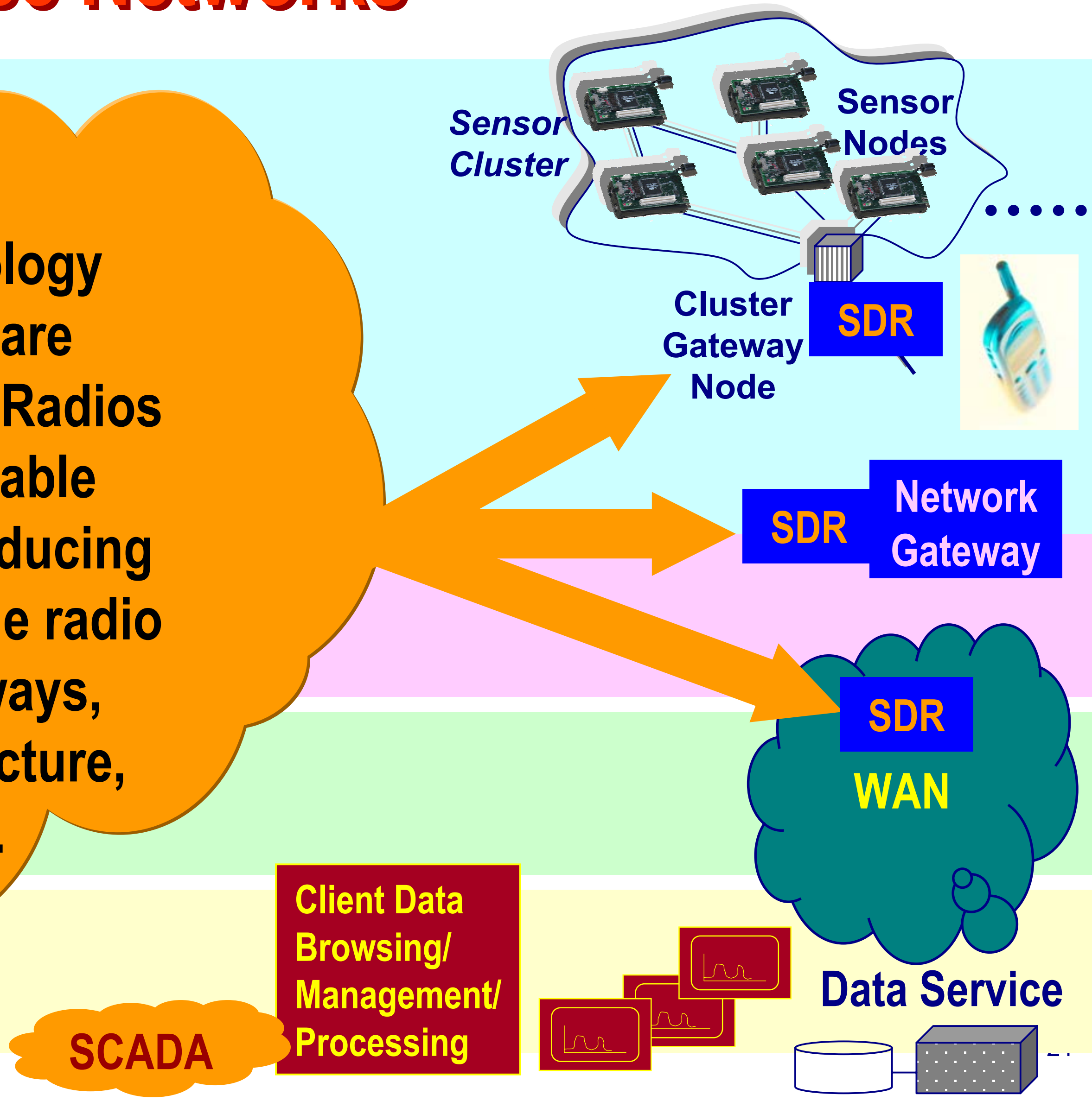
- Software Defined Radio (SDR) technology is a collection of hardware and software technologies that enable reconfigurable system architectures for wireless networks and terminal devices.
  - Efficient & comparatively inexpensive solution to the problem of building wireless devices that can be enhanced using software upgrades;
    - multi-mode e.g., Zigbee, Bluetooth, 802.11b/g/…,
    - multi-band, e.g., 2.4 Ghz, 5 GHz, 800/900 MHz, …
    - multi-functional
- SDRs:
  - Enabling technology applicable across a wide set of domains in the wireless industry

Agile Radios in Demand-Response Networks: Potential Benefits

- Agile Radio Technology enables ways to
  - Minimize “Stranded Assets”
  - Leverage a diversity of wireless channels, and to use the best available wireless channel/network
  - Preserve investment in Software Platforms
    - Leverage the hardware/technology/cost curve
  - “Future-proof” the network
  - Improve redundancy at the system level
  - ….

Software Defined Radios in Demand Response Networks

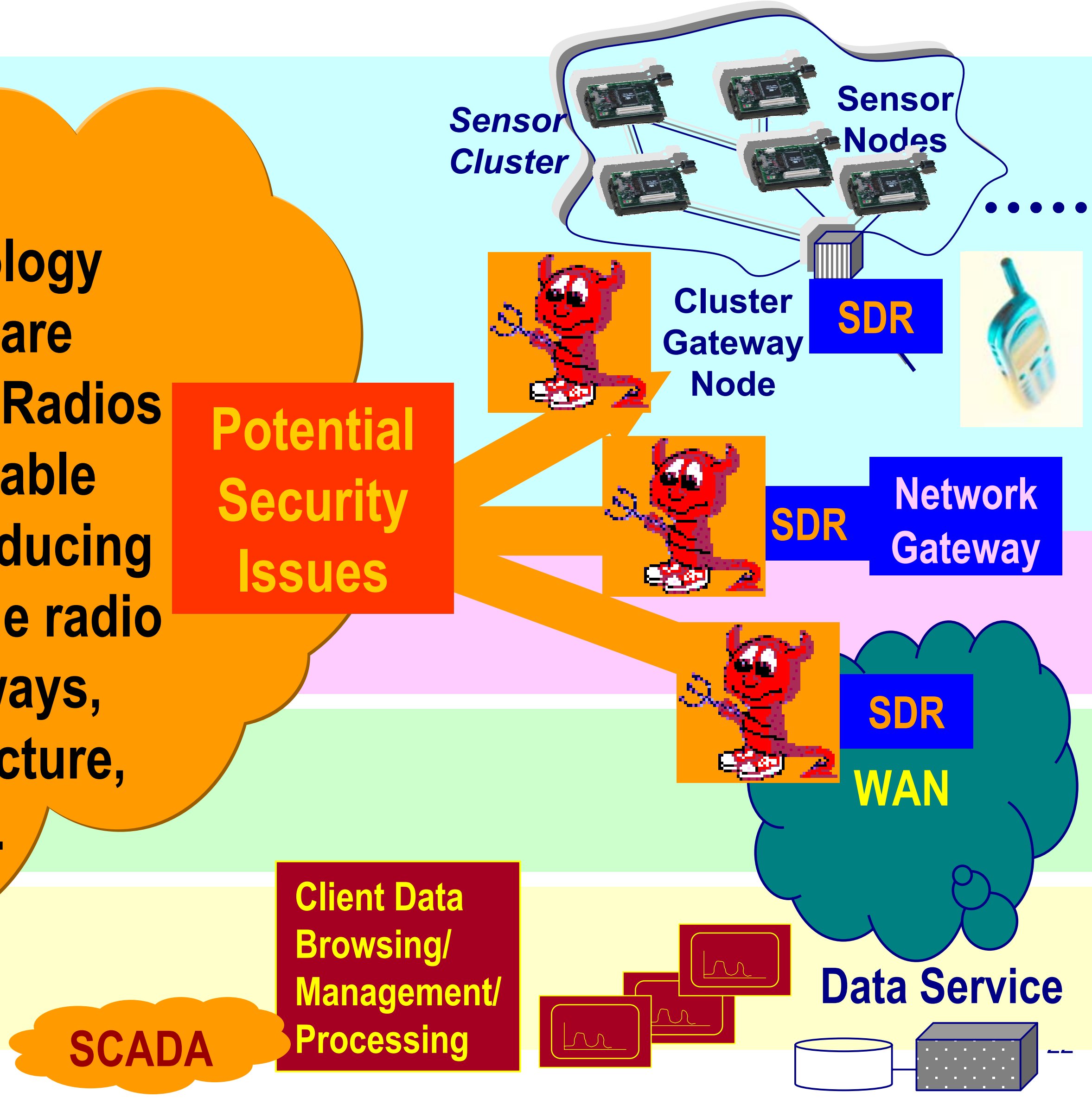
Emerging technology related to Software Defined / Cognitive Radios creates considerable incentives for introducing agility in some of the radio nodes e.g. Gateways, Wireless Infrastructure, Terminals, …



Software Defined Radios in DR Networks: Security Issues

Emerging technology related to Software Defined / Cognitive Radios creates considerable incentives for introducing agility in some of the radio nodes e.g. Gateways, Wireless Infrastructure, Terminals, …

Potential Security Issues



SDR-related Security Issues

- Security concerns associated with SDR wireless implementations:
  - (Conventional) Protection needed for content privacy and integrity, authentication, non-repudiation, …
  - (Wireless) RF links in mobile wireless …
    - interception of the signal cannot be prevented.
  - (New) Implementation of radio links with SDR technology …
    - requires further security measures to preclude introduction of software that can compromise existing security measures/systems.
    - The full cycle of download, storage, installation, and instantiation (DSII) for software over wireless links must be considered.

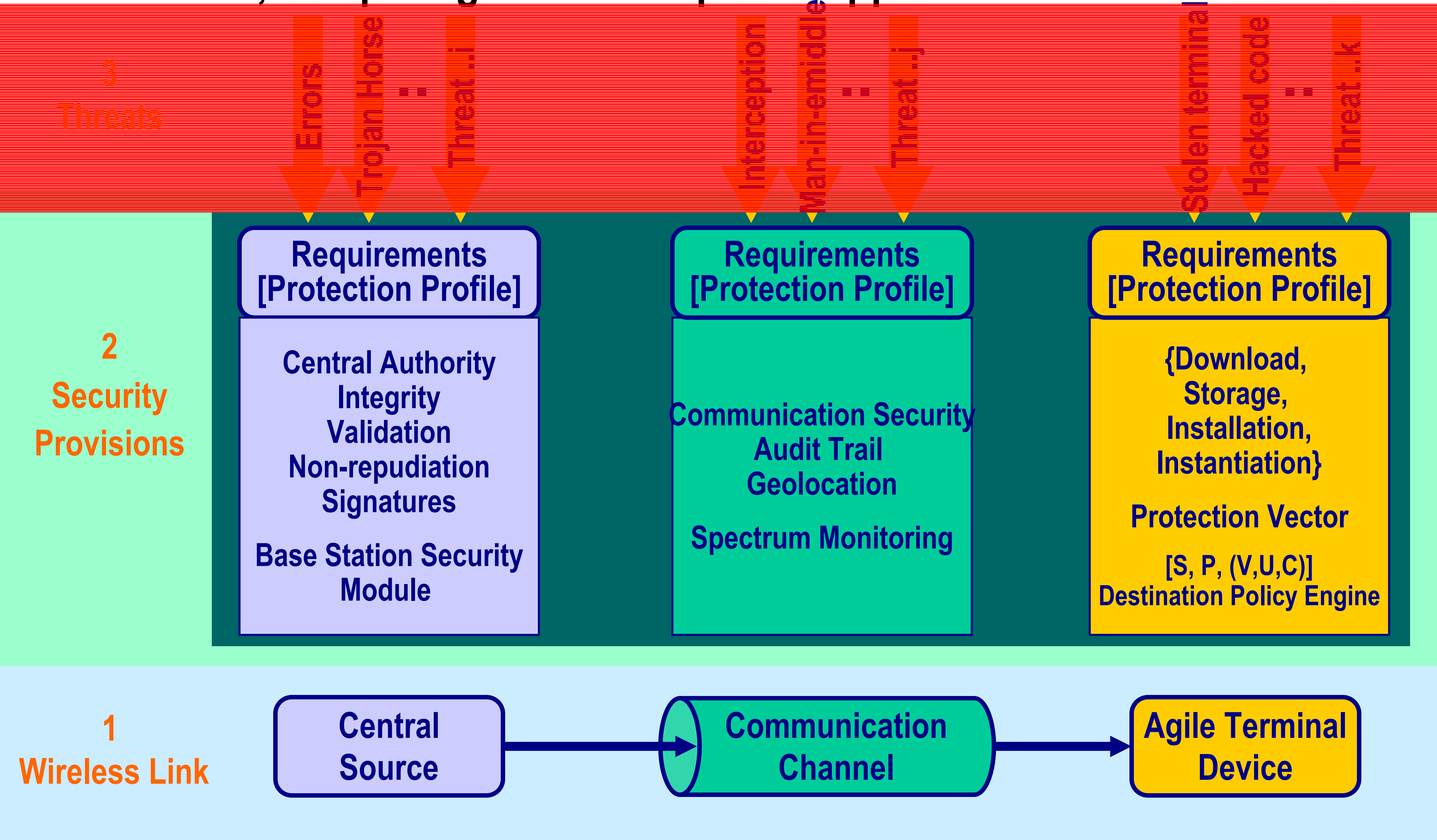
- Many of the issues have only relatively recently being identified and defined …

Software Download Security

- The ability to download software into terminals introduces several new security issues
  - Regulatory
    - New software can change transmitter characteristics
  - User
    - Protection of content
  - OEM
    - Assurance that the software load is appropriate for the target terminal and is unaltered
  - Wireless Service provider
    - Accounting for all billable time, …
  - Utilities, CallSOs, …
    - {User, OEM, …}

SDR Security Framework

- SDR Security Framework: A template for discussing specific issues, comparing different topics & approaches



3 Threats

Errors

Trojan Horse

...

Threat ...i

Interception

Man-in-emiddle

...

Threat ...j

Stolen terminal

Hacked code

...

Threat ...k

2 Security Provisions

Requirements [Protection Profile]

Central Authority
Integrity
Validation
Non-repudiation
Signatures

Base Station Security Module

Requirements [Protection Profile]

Communication Security
Audit Trail
Geolocation

Spectrum Monitoring

Requirements [Protection Profile]

{Download,
Storage,
Installation,
Instantiation}

Protection Vector

[S, P, (V,U,C)]
Destination Policy Engine

1 Wireless Link

Central Source

Communication Channel

Agile Terminal Device

Security Requirements

- Security Policy Enforcement/Management
- Information Integrity
- Authentication and Non-Repudiation
- Access Control (includes authorization)
- Encryption and Decryption
- Key and Certificate Management
- Standardized Installation Mechanisms
- Auditing and Alarms
- Configuration Management
- Memory Management
- Emissions Management

Security Related to Software Download: Areas of Concern

- The uniqueness of the media and the hardware and software flexibility in reconfigurable, software defined radio devices present some unique potential security threats and requirements including:
  - Security threats during the software creation process
  - Reconfiguration of hardware and software
  - Unique authentication, authorization, and accountability requirements
  - Trust relationship based on the type of software being downloaded
  - Resource constraints — limitations of processing power and memory
  - International roaming considerations
  - Device management aspects
  - Controlled access
  - Existing security download mechanisms (e.g., SSL) typically not flexible or not efficient enough to accommodate the wide range of devices

Summary: Work in Progress…

- SDR security is a *system level* problem.
- To design a system with appropriate defenses, one must first understand the system threat and defense requirements.
- Hackers use blended attacks against both the radio and computer layers of the SDR.
- To defend against the blended attack requires a multi-layered defense-in-depth which protects both the radio equipped (mobile) clients and servers.
  - This includes the mobile radio, mobile host, server radio, and server host components of an SDR network.
- The security architecture must:
  - Ensure integrity of the software applications and downloads including download, storage, installation and instantiation
  - Ensure integrity of the reconfigurable platform against blended attacks by employing defensive layers (firewalls, intrusion detection, virus protection)
  - Integrate biometric and radiometric assurance techniques
  - Employ trusted architecture, high assurance operating systems and middleware
  - Integrity of the analog signal or data from exploitation/compromise
- The SDR security framework is intended to serve as a model to describe relation between system elements, components, and functions

We are off to a good start…

- And have the opportunity to make some unique contributions
  - Security for Demand-Response/Sensor Networks
  - Privacy/legal/public policy issues
    - … important in this context, and
    - … can have long lasting societal implications.

Open Discussion