

# Security Architecture for Demand-Response/Sensor Networks:

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

# Acknowledgements

- Many thanks for their support!
  - CEC/CIEE (David Michel)
    - ◆ Gaymond Yee & Ron Hofmann
    - ◆ Technical Advisory Committee
- Profs. Paul Wright, Ed Arens, and collaborators at UCB
- Industry Partners: Bell Labs, Others
- Participants in the interviews


# The Team

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

# Agenda

- Introducing the team
- Project: Security Architecture for DR/Sensor Networks
  - Background & Motivation
  - Goals & Scope
- Executive Summary
  - Sensor Network Security & Privacy
  - Security Issues in Agile/Software Defined Radios
  - Network Security Framework
  - Legal and Public Policy Issues (Deirdre Mulligan)
- Open Discussion
  - Ways to maximize the impact of this project
  - Feedback, Future directions

# 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 Security of critical infrastructure & Cyberattacks**

# Security in DR/Sensor Networks: Motivation

- 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

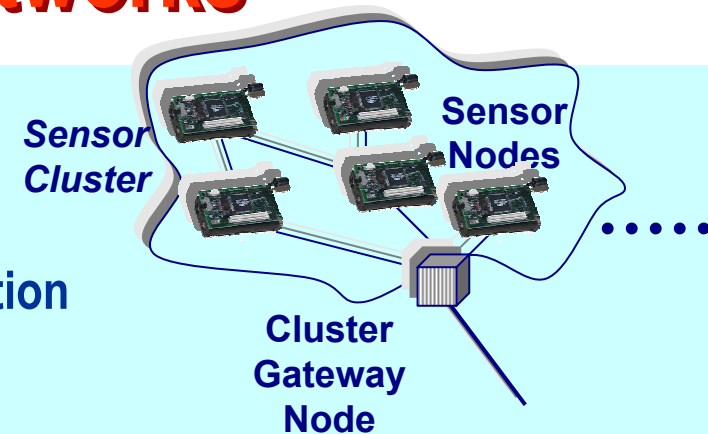


# Research: Objectives & Results

- Research Objective
  - Identify the specific security and privacy issues associated with demand response networks, and use this as a basis to
  - Develop an overall framework
    - ◆ For delivering security and privacy
      - Including Technical architecture and policy controls
- Research Focus
  - Demand response networks that employ
    - ◆ sensors and wireless communication networks
    - ◆ in conjunction with advanced metering technologies.
- Phase 1: Results couched in the context of
  - A short/medium/long-term framework for
    - ◆ Looking at likely demand response architectural features,
    - ◆ Understanding the attendant privacy and security issues,
    - ◆ Suggesting recommended solutions.

# 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, ...

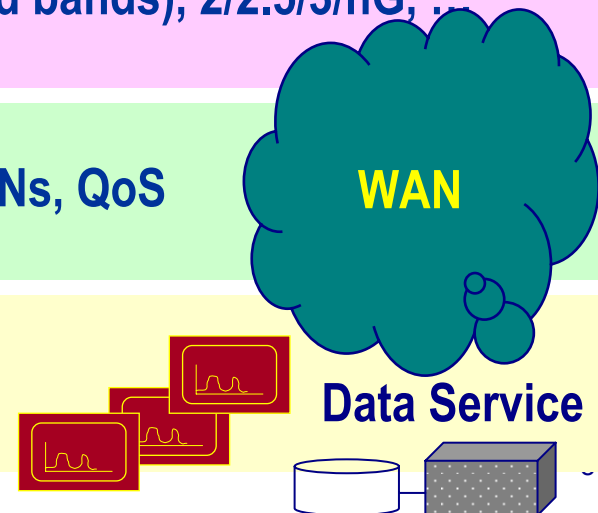
Network  
Gateway

- Backhaul
  - Private Enterprise Networks, e.g., leased lines/WANs, QoS
  - Public Internet

- Other Networks
  - Utilities e.g., PG&E
  - Power generators
  - SCADA

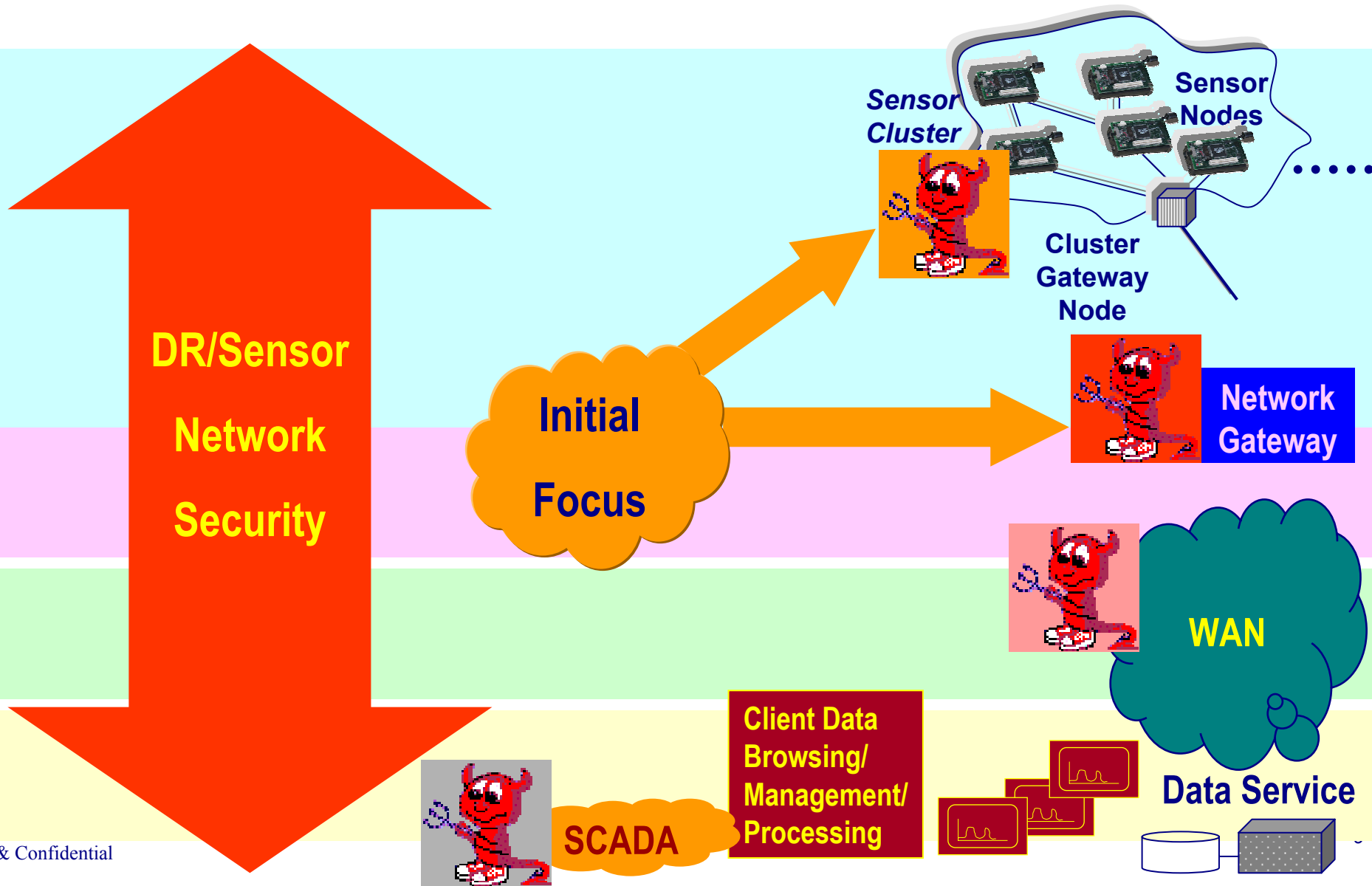
SCADA

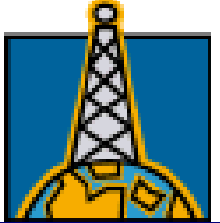
Client Data  
Browsing/  
Management/  
Processing



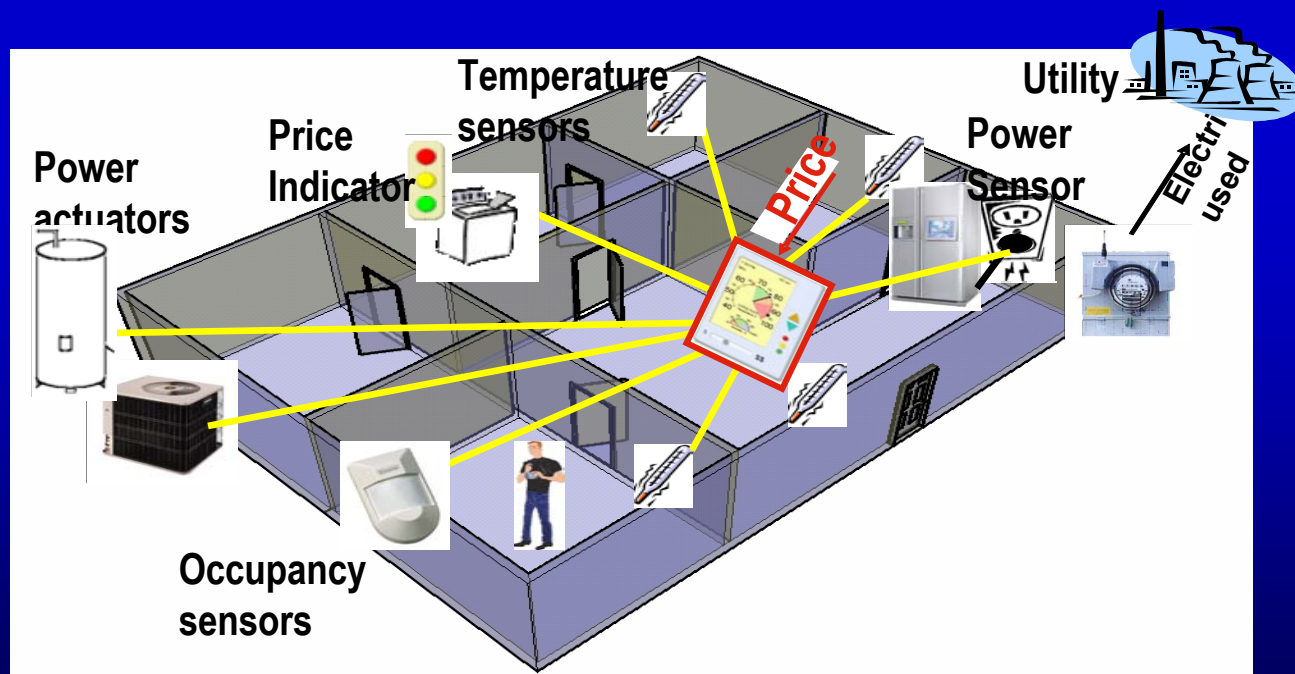


# Demand-Response Network Architecture: Subsystems & Subnetworks. Security Issues





# Sensor Network Security



# **Sensor Network Security:**

## **Potential vulnerabilities, Resource Constraints, and Security Implications**

- **Wireless sensor networks afford a natural and potentially cost-effective mechanism for the monitoring and control of appliances and energy management systems.**
- **However, sensor networks may suffer from many layers of potential vulnerabilities:**
  - **they are subject to the problems of computer networks in general;**
  - **ordinary wireless networks;**
  - **ad-hoc networks; and**
  - **additional physical attacks that take advantage of the sensor nodes' new form factor.**
- **Sensor nodes have limited resources, including slow CPUs, short battery life, and small memories.**
  - **These limitations both open up additional attack avenues for adversaries and make it difficult to use existing cryptographic techniques as defenses.**

# Sensor Network Security: Research focus

- Sensing/Actuation at customer site
  - Wireless sensors/actuators
  - Detailed data may be stolen
  - Actuators may be misused
- Data Sent from customer to utility
  - Privacy compromise
  - Customer activity may be inferred
  - Main Future Work

# Sensor Network Security: Recommendations

- **Encryption** is recommended over a manufacturers' proprietary format for securing data over the entire transmission path, from the meter to the utility.
- We recommend that designers adhere to published, well studied, and where possible, provably secure standards.
- We recommend the use of **authentication** for all data.
- We recommend that **spread-spectrum radios** be used if feasible.
- We recommend that a **single-hop network** be used if possible for sensor networks.

# Sensor Network Security: Privacy & Regulatory Aspects

- As it is expected that customer usage and demand response data are likely to be held, either temporarily or long-term, by both utilities and third party systems, current and updated rules covering data privacy and business record handling need to apply to both utilities and third-parties who hold the data.
- Access to hourly customer usage data should be limited within the utility, to systems that have a justifiable requirement for it.
- Guidelines for how much data is necessary and should be stored for the purposes of customer service and other functions should be set by the appropriate regulatory body.





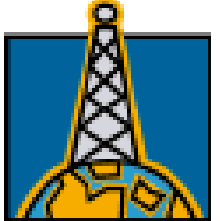
# **Sensor Network Security: Privacy & Regulatory Aspects (2)**

- **Separate data pathways (communication channels) for systems that do and do not require identifiable data should be built into the system. In other words, data that is tagged with information relating to the consumer that is private should be transmitted over a different (more “secure”) channel compared to data that is anonymous.**
- **The data mining of hourly usage data (or fine-grained usage data in general) should be carefully monitored and regulated.**
- **When significant computing capability exists inside the home, that processing capability should be developed to enable the customer or his smart equipment to perform necessary energy-related functions – energy monitoring, demand response control, self-education, and billing – at the home site.**

# Points to ponder

- Some of the “obviously good” attributes of ad-hoc sensor networks obtaining due to route discovery may have to be rethought because of potential security issues.
  - But improved solutions are possible, while still maintaining limited flexibility.





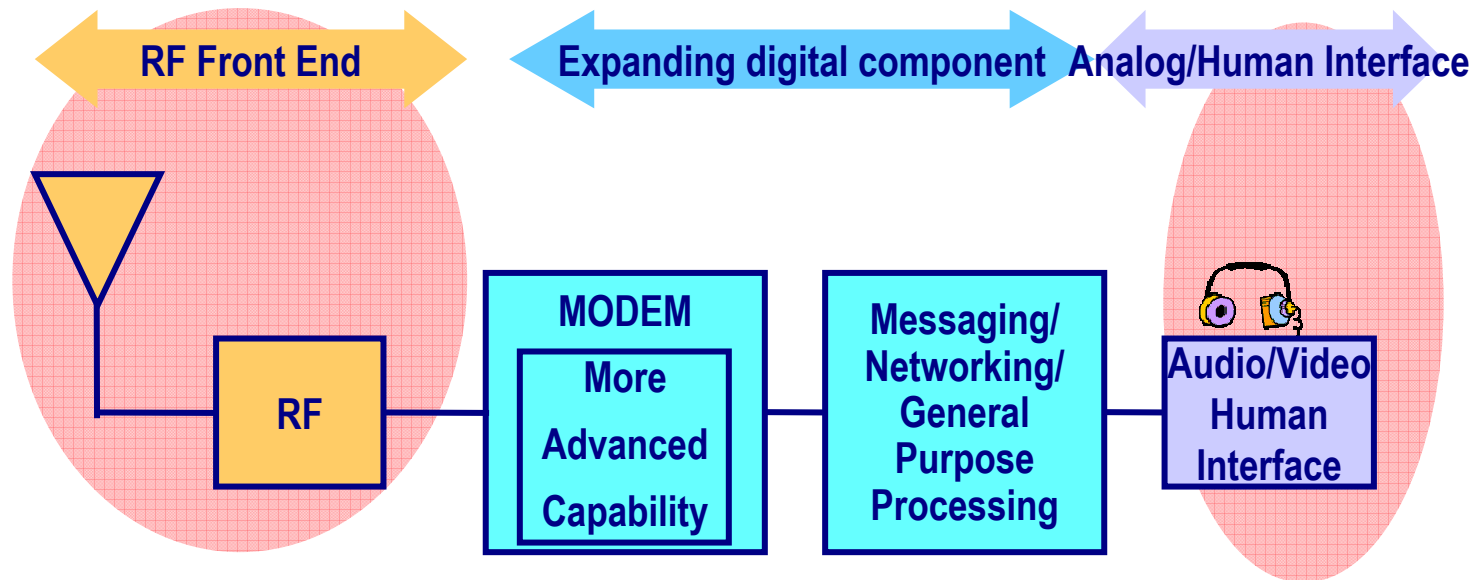
# Agile Radio Security

What?  
Why useful?  
Role in DR Networks?  
Security Issues?  
Solutions  
Future Work

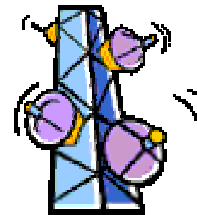


# What is a Software (Defined) Radio?

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



- Examples:
  - Basestations (today), Handsets (2006), others
  - Military (leaders)

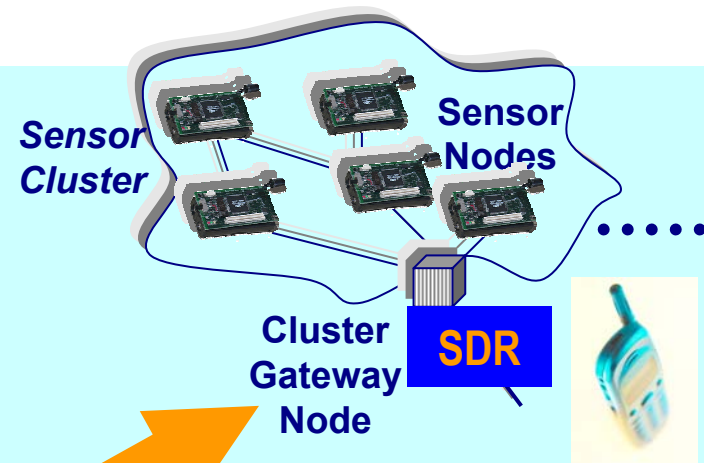


# What is an Agile Radio Node?... and Why it is useful in the Demand-Response Context?

- An Agile (Radio/Gateway) Node has the ability to communicate over more than one Air Interface (Wireless Protocol/Standard).
    - E.g., Bluetooth, IEEE 802.11 b/g, IEEE 802.15.4, ...
    - Flavors of agility:
      - ◆ Protocol Agility (choose from multiple networks/protocols)
      - ◆ RF Agility (operate in more than one frequency bands)
      - ◆ Cognitive (Spectrum) agility (leverage underutilized spectrum bands)
  - A Software Defined Radio node has the further ability to have its air interfaces defined and provisioned in the field.
- 
- The use of agile, software-defined radio nodes can
    - Help reduce stranded assets by supporting legacy radio/sensor interfaces, (Reduce Capex)
    - “Future-proof” deployments and reducing operational costs by enabling software download of new radio functionality, and enhanced services. (Reduced Capex & Opex)
    - Provide a superior ability to manage, upgrade and provision new services.

# Software Defined Radios in Demand Response Networks

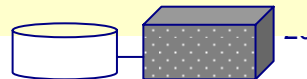
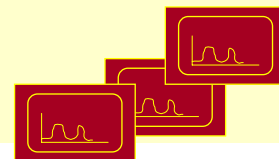
Emerging technology related to Software Defined / Cognitive Radios creates considerable incentives for introducing agility in some of the radio nodes e.g. Gateways, Wireless Infrastructure, Terminals, ...



Data Service

Client Data  
Browsing/  
Management/  
Processing

SCADA

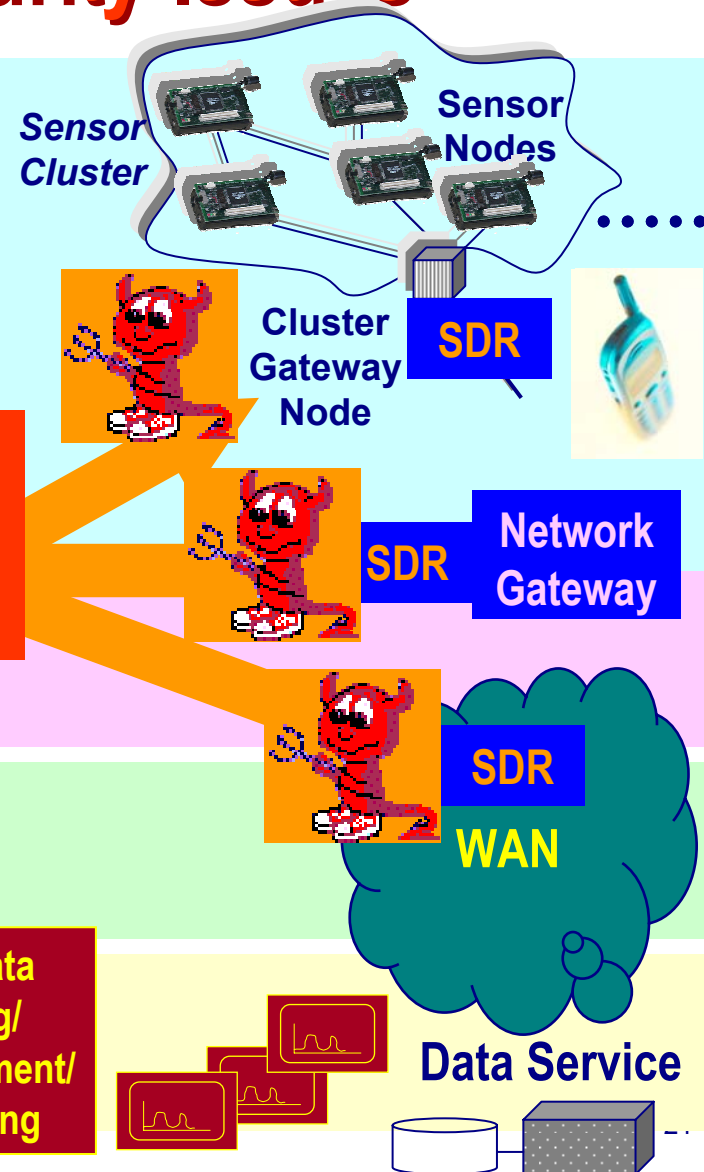




# Software Defined Radios in DR Networks: Deployment Locations & Security Issues

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

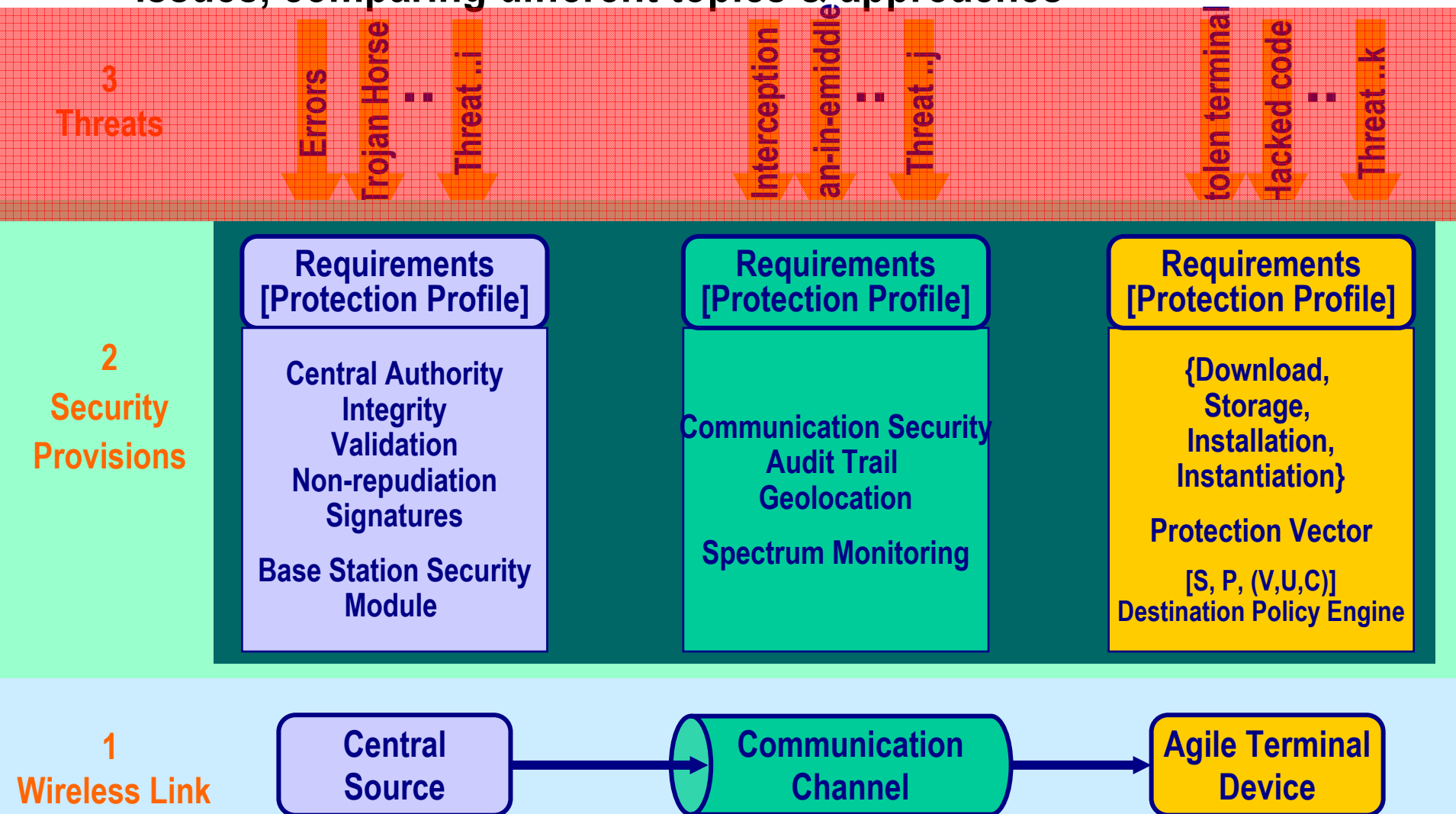


# SDR-related Security Issues

- 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 ...

# SDR Security Framework

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

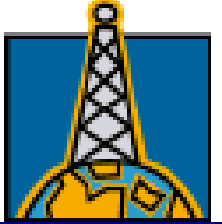


# Agile Radio Node Security Architecture: What is required?

- A high confidence 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 (e.g., fingerprint) and radiometric assurance techniques as appropriate;
  - Employ trusted architecture, high assurance operating systems and middleware
  - Preserve the integrity of the analog signal or data, and protect it from exploitation and/or compromise.
- An important open problem in this context relates to the security challenges arising from the need to accommodate third party software to be downloaded onto agile radio nodes.

# Agile Radio Node Security Architecture: Summary

- The security architecture provides a framework that addresses the following key questions with regard to the end-to-end security:
  - What kind of protection is needed and against what threats?
  - What are the distinct types of network equipment and facility groupings that need to be protected?
  - What are the distinct types of network activities that need to be protected?
- These questions are addressed by three architectural components: sets of security measures (also referred to as security dimensions), security layers and security planes. The principles described by the security architecture can be applied to a wide variety of networks independently of the network's technology or location in the protocol stack.
- We suggest that demand response systems should have an associated security program that consists of policies and procedures in addition to technology, and that progresses through three phases over the course of its lifetime: the Definition and Planning phase; the Implementation phase; and the Maintenance phase. The security architecture can be applied to security policies and procedures, as well as technology, across all three phases of a security program.



# Network Security Architecture: A Framework

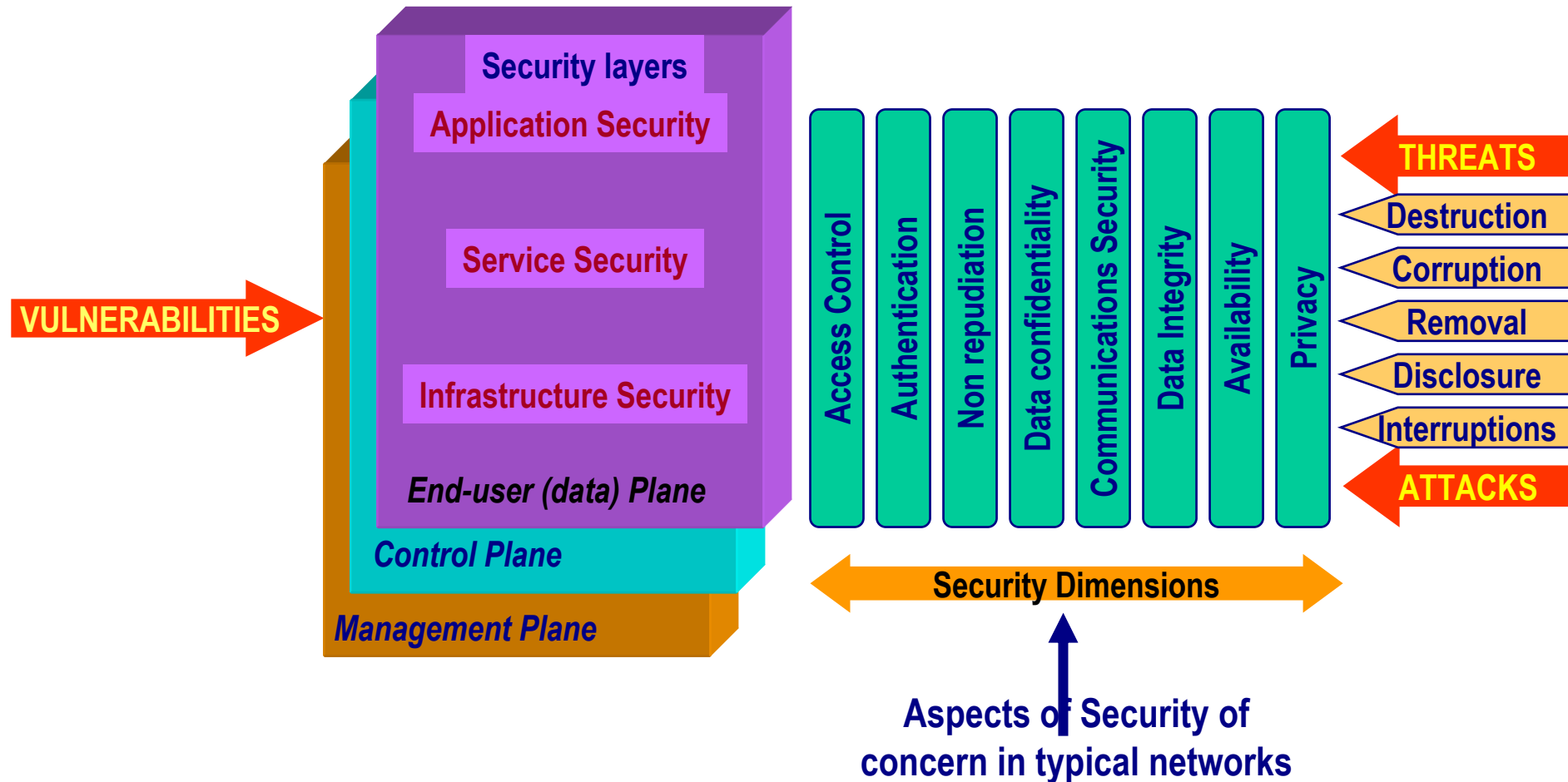


# Network Security Architecture Framework.

## Security measures, layers, planes

- The security architecture addresses the following key questions with regard to the end-to-end security:
  - What kind of protection is needed and against what threats?
  - What are the distinct types of network equipment and facility groupings that need to be protected?
  - What are the distinct types of network activities that need to be protected?
- These questions are addressed by three architectural components:
  - security measures (sets of security measures are sometimes referred to as security dimensions),
  - security layers and
  - security planes.
- The principles described by the security architecture can be applied to a wide variety of networks independently of the network's technology or location in the protocol stack.

# Network Security Architecture Framework: Threats, Security measures/dimensions, layers, planes



# Security Planes

- Security Planes
  - The security planes address the security of different categories of activities performed in a network.
  - The basic network security architecture consists of three Security Planes to address the three types of protected activities that take place on a network.
    - ◆ (1) the Management plane,
    - ◆ (2) the Control plane, and
    - ◆ (3) the End-User plane.
  - These Security Planes address specific security needs associated with network management activities, network control or signaling activities, and end-user activities correspondingly.

# Network Security Planes: “Orthogonality” Principle

- Networks should be designed in such a way that events on one security plane are kept totally isolated from the other security planes.
  - For example, in a regular network, a flood of DNS (Domain Name Service) lookups on the end-user plane, initiated by end-user requests, should not lock out the OAM&P interface in the management plane that would allow an administrator to correct the problem.
  - Demand Response Context
    - ◆ In a hypothetical demand response scenario, a burst of user level requests for energy related data should not disable the ability to manage and update the basic meter.
- Each type of network activity typically has its own specific security needs.
  - The concept of security planes allows the differentiation of the specific security concerns associated with those activities and the ability to address them independently.

# Orthogonality of Security Planes: Examples

- Consider, for example, the security of a DR service (e.g., the ability to transmit real time pricing signals), which is addressed by the services security layer.
  - Securing the management of the DR service (e.g., provisioning users) is independent of
  - securing the control of the service (e.g., initiating a service session) and also independent of
  - securing the end-user data being transported by the service (e.g., the energy usage and billing information).
- A communication service analogy is, for example, a VoIP service, which is addressed by the services security layer.
  - Securing the management of the VoIP service (e.g., provisioning users) has to be independent of
  - securing the control of the service (e.g., protocols such as SIP) and also has to be independent of
  - securing the end-user data being transported by the service (e.g., the user's voice).

# Recommendations

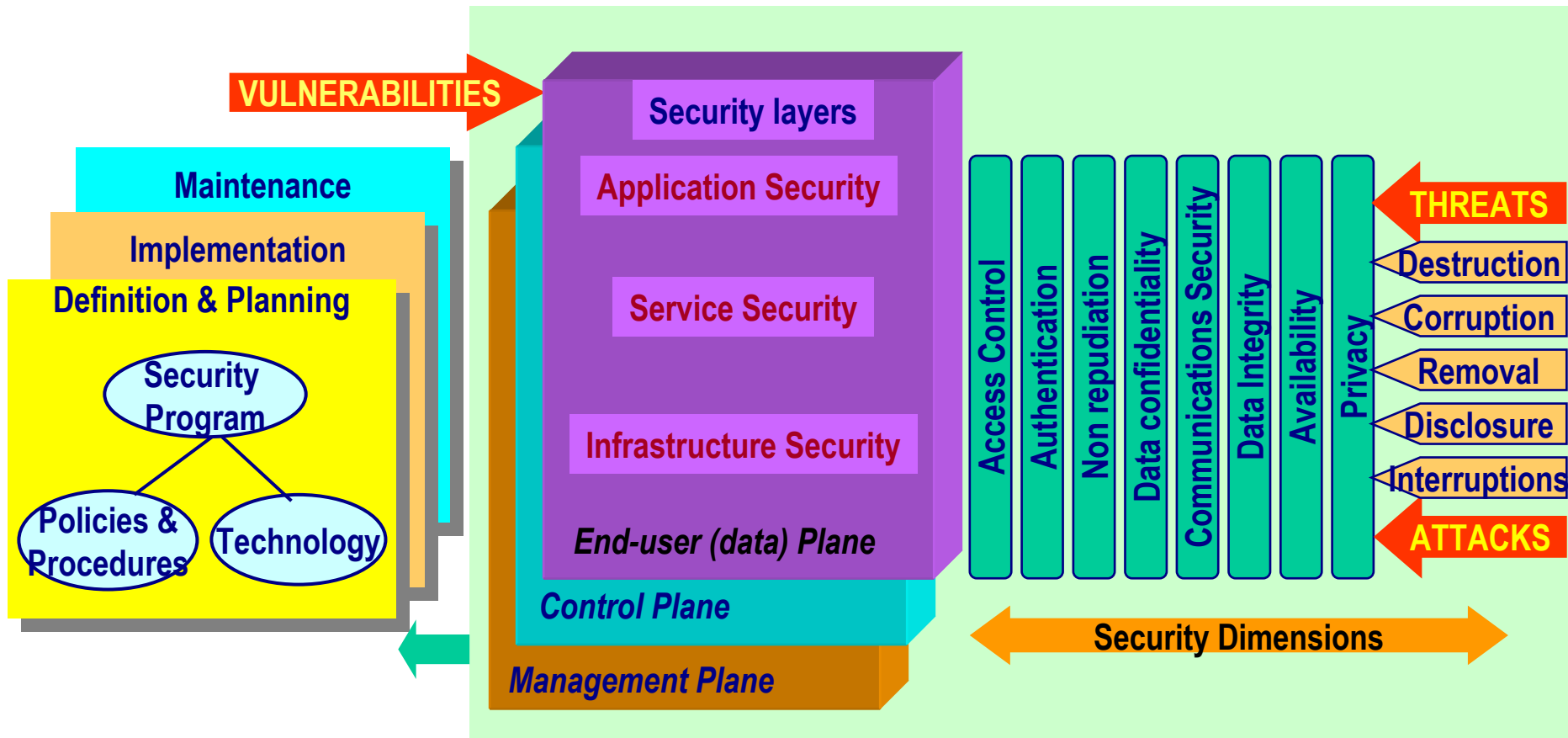
- **Recommendations: Objectives achieved by application of security dimensions to security layers**
- **We suggest that**
  - **Demand response systems have an associated security program that consists of policies and procedures in addition to technology, and that progresses through three phases over the course of its lifetime:**
    - **the Definition and Planning phase;**
    - **the Implementation phase; and**
    - **the Maintenance phase.**
- **The security architecture can be applied to security policies and procedures, as well as technology,**
  - **...across all three phases of a security program.**



# Security Architecture Framework: How is it used?

- The security architecture can guide
  - the development of comprehensive security policy definitions,
  - incident response and recovery plans, and
  - technology architectures
- ... by taking into account each security dimension at each security layer and plane during the definition and planning phase.
- The security architecture can also be used as the basis of a security assessment that would examine how the implementation of the security program addresses the security dimensions, layers and planes as policies and procedures are rolled out and technology is deployed.
- Once a security program has been deployed, it must be maintained in order to keep current in the constantly evolving security environment.
- The security architecture can assist in the management of security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the security program address each security dimension at each security layer and plane.

# Security Architecture Framework: Lifecycle Role





# Summary

# Summary

- **Goals: ... to foster an increased awareness and deeper understanding of the security and privacy issues in demand response networks & systems employing advanced metering and wireless/sensor networks**
  - among technologists who build the infrastructure/components; &
  - among the regulators & legislators who oversee or drive that process.
- **Results**
  - We have developed
    - ◆ A short/intermediate/long term framework capturing
      - likely demand-response functionality, architecture;
      - attendant security & privacy issues.
- **Research focus in 4 key dimensions**
  - ◆ Sensor Network Security & Privacy
  - ◆ Security Issues in Agile/Software Defined Radios
  - ◆ Network Security Framework
  - ◆ Legal and Public Policy Issues

# Potential Benefits to California Stakeholders

- We anticipate that this report will be useful to the energy industry,
  - ...help identify areas where security and privacy issues may be important
    - ◆ for both commercial and consumer protection.
- Potential Benefits for California Stakeholders
  - Utilities: their networks are strengthened against attack, and their customers retain confidence in the companies' handling of their personal information.
  - Consumers: protection of their California Constitutional rights to privacy, and in the safety of their personal information from exploitation or theft.
  - Regulators & Lawmakers: We hope this report may also provide information that is useful for enact new rules to enforce sound privacy and security choices.
- Recommendations provide a starting point
  - A lot of room for further work





**Open Discussion**  
**[psubra@ieee.org](mailto:psubra@ieee.org)**

