

Network Security

Collaboration with

- Frank Akujobi
- Michel Barbeau
- Joaquin Garcia-Alfaro
- Jyanthi Hall
- John Lambadaris
- Paul Vanorschoot
- Tao Wan
- David Whyte

Outline

The Network is a complex dynamical system whose security requires the interaction of multiple techniques.

- DNS (Domain Name Server)
- BGP (Border Gateway Protocol)
- NEM (Network Exposure Maps)
- Endpoint-Driven Intrusion Detection
- RFF (Radio Frequency Fingerprinting)
- RFID (Radio Frequency ID)
- Sensor Networks

DNS

Problem

- Scanning worm propagation can occur extremely fast
 - Recall Slammer infected 90 % of vulnerable Internet hosts in less than 10 mins.
- Automated countermeasures are required for worm containment and suppression
- Current worm propagation detection methods are limited by:
 - Speed of detection
 - Inability to detect zero-day worms
 - Inability to detect slow scanning worms
 - High false positive rate

Characteristics

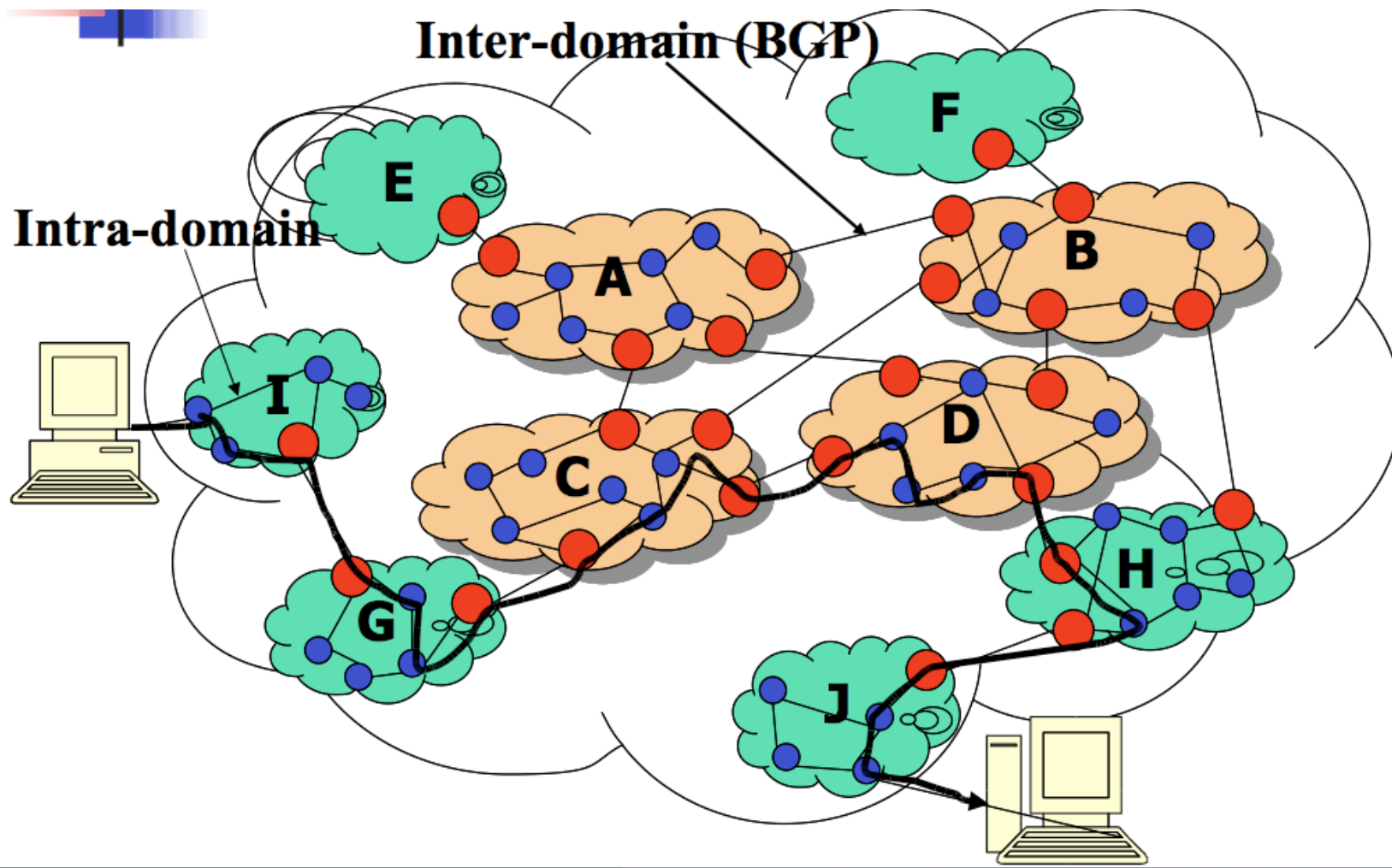
- Scanning worms can employ a variety of strategies to infect systems
 - Topological scanning
 - Slow scanning
 - Fast scanning
- So far, all make use of a pseudo random generated 32-bit numbers to determine their targets
- The use of numeric IP addresses does not require a DNS lookup
- Violation of typical network behavior (i.e. DNS)

Detection Approach

- Most legitimate traffic uses the alphanumeric equivalent of an IP address and thus requires a DNS lookup
- Hosts within a domain use their respective DNS servers for IP translations
- As the network traffic leaves the network boundary it can easily be determined if a DNS request was involved
- If no DNS query is detected for a con-attempt it is considered anomalous

BGP

Routing on the Internet



Common BGP Security Goals

- Data Origin Authentication
 - BGP Speaker Authentication
 - AS Number Authentication
- Data Integrity (of control messages)
- Message Truthfulness
 - Prefix Ownership Verification
 - AS-PATH Verification

Proposals for BGP Security

- **Problem:** for $r := [prefix, AS - path]$ how do we secure the operation

$$f(rt_t, r) = rt_{t+1}?$$

- **S-BGP**
- **soBGP**
- **psBGP** (pretty secure BGP)
 - A Centralized Trust Model for AS# Authentication
 - A Decentralized Trust Model for Prefix Ownership Verification

NEM

Attribution-based Scanning Detection

- Variety of scanning detection techniques
 - Observing connection failures
 - Abnormal network behavior
 - Connections to darkspace
 - Increased connection attempts
- Majority of these rely on correlating scanning activity based on the perceived last-hop
- Focus of detection is who is scanning instead of what is being scanned

Attribution is not practical!

- Attribution is not practical for an increasing number of sophisticated scanning techniques
- Focus on attribution overlooks critical components of any observed scanning campaign:
 - What are my adversaries looking for?
 - Has the network behavior changed as a result of being scanned?
- Exemplar technique: Darkports and Exposure Maps

Exposure Maps and Darkports (Intended Capabilities)

- Scanning detection
Sophisticated and simple
- Active Response
Network awareness allows for fine grained response
- Network Discovery and Asset Classification
Exposure Profiles
- Network Change Detection
Trans-darkports and changes in exposure profile

HEM (Host Exposure Map)

- Associated with a fixed IP address (host), is the set of ports observed responding to external connection attempts within a predefined period.
- For each active host i in the network, HEM_i is a set of elements each of which begins with the IP address of i , followed by a port number j ; there is such an element for each $port_j$ that has responded to a connection attempt within a predefined period.
- In symbols, we can abbreviate this as
$$HEM_i = \{IP_i : port_j \mid port_j \text{ was observed responding}\}.$$

Endpoint Driven Intrusion Detection

Intrusion Detection Techniques

- Signature-based
 - Host anti-virus signature
 - Network traffic profiling
- Anomaly-based
 - Host anomalous behavior
 - Network traffic anomalies

Requirement for effective detection and containment

- Verifiable detection of malicious intrusions
- Collaborative network-based containment
- Automated rapid response

Proposed detection technique

Detector agent (DA) running on detector endpoints (DEs)

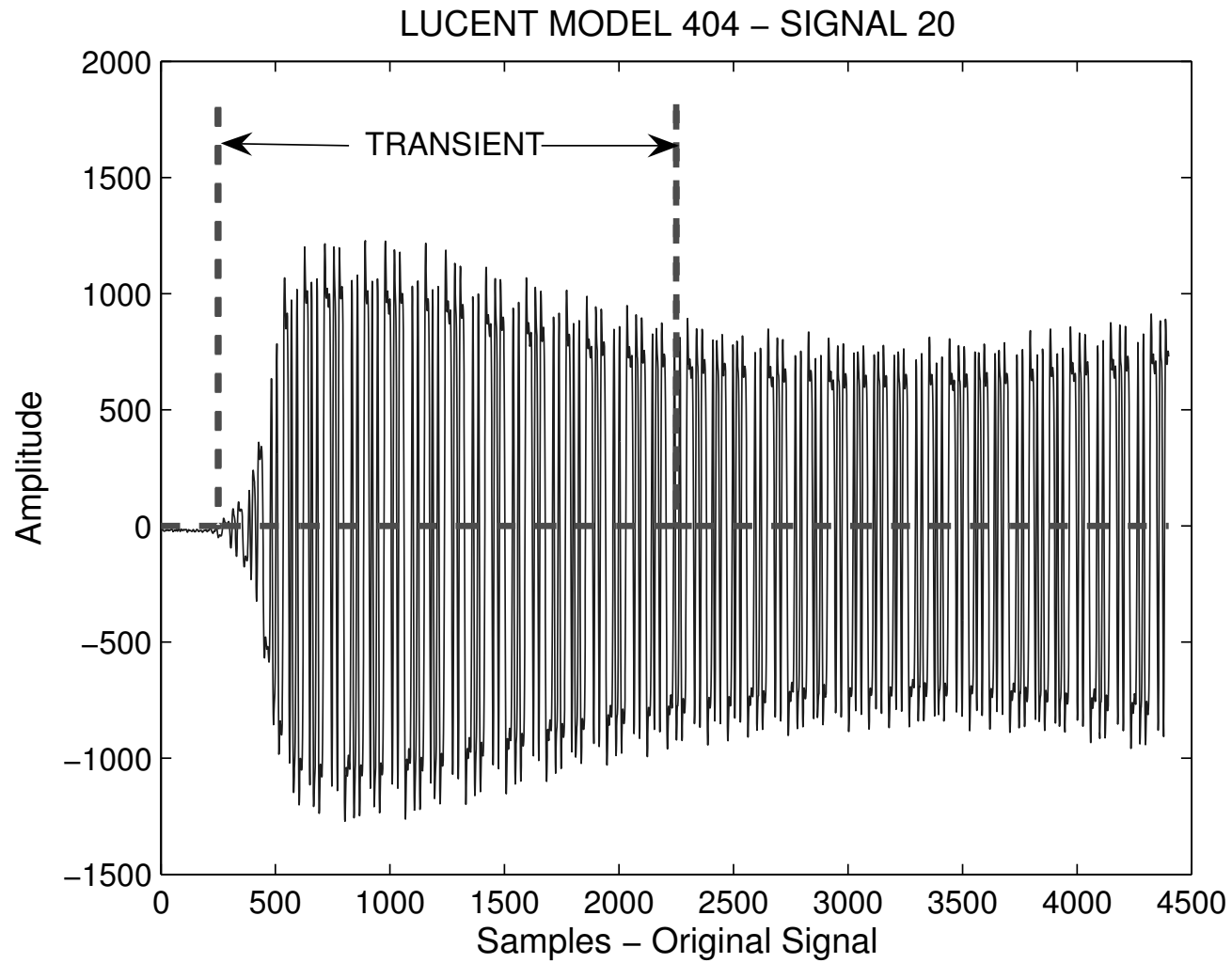
- DEs located in distributed subnets or cells
- DA responds to anomalous host behavior
- DA sends alert to gateway router (GR)
- DA performs real-time recording of intrusion traffic profiles.
 - srcIP, dstport, proto
 - More flow characteristics can be recorded with deep packet inspection
- DA sends traffic profile records to GR

Radio Frequency Fingerprinting (RFF)

Radio Frequency Fingerprint

- Pioneered by the military to track movement of enemy troops.
- Designed to capture unique characteristics of the transceiver's radio frequency energy, for identifying cell phones and other devices.
- Has been implemented, as an authentication mechanism, by cellular carriers (e.g. Bell Nynex), to combat cloning fraud.

Signal from a 802.11b Transceiver



RFF Transceiverprints

- Transceiverprints cannot be easily forged unless the entire circuitry of a transceiver can be replicated.
- After extracting the transient its instantaneous amplitude, phase and frequency are obtained.
- Using these components, one or more features are extracted. This set of features represents a fingerprint of the transceiver, or in other words *transceiverprint*.
- The transceiverprint is, in turn, classified as belonging to one of the profiled transceivers.

Intrusion Detection Framework (Two Phases)

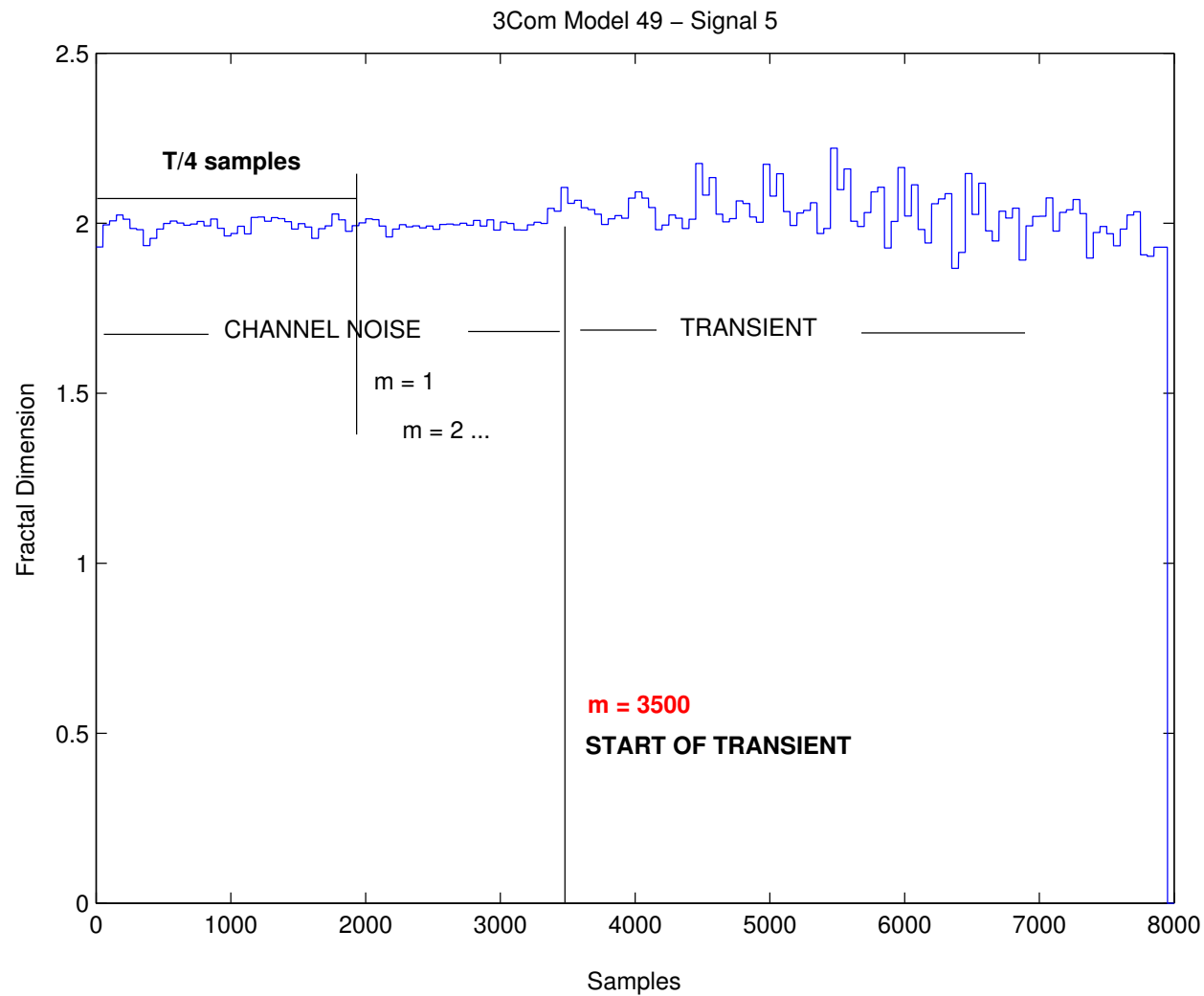
1. Profiling

- (a) Transient-, Component-, and Feature-Extractor
- (b) Profile Definition and Update

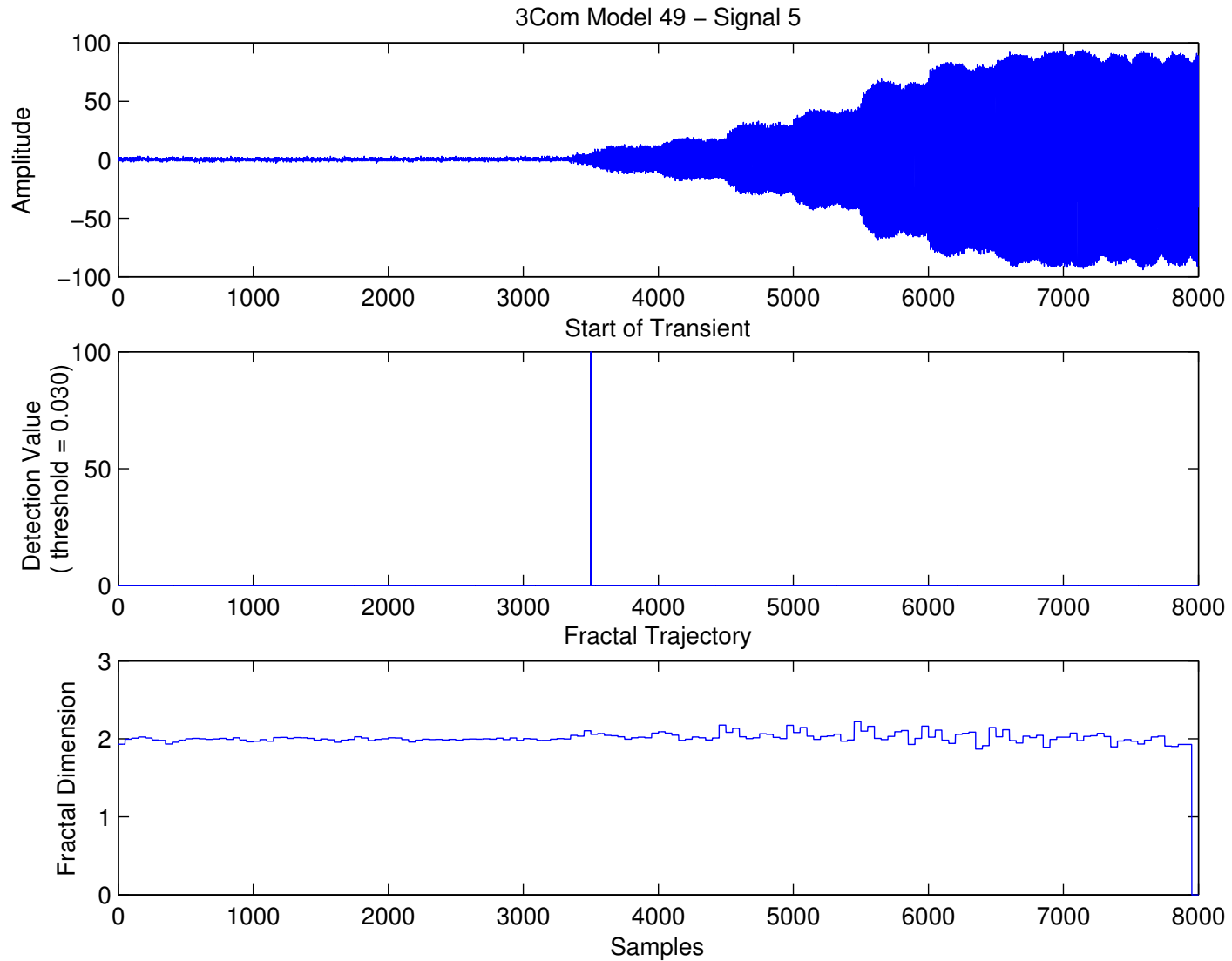
2. Classification

- (a) Identification of Transceivers
- (b) Validation (Statistical Classifier, Decision Filter)

Transient Detection using Threshold (3Com Model 49)

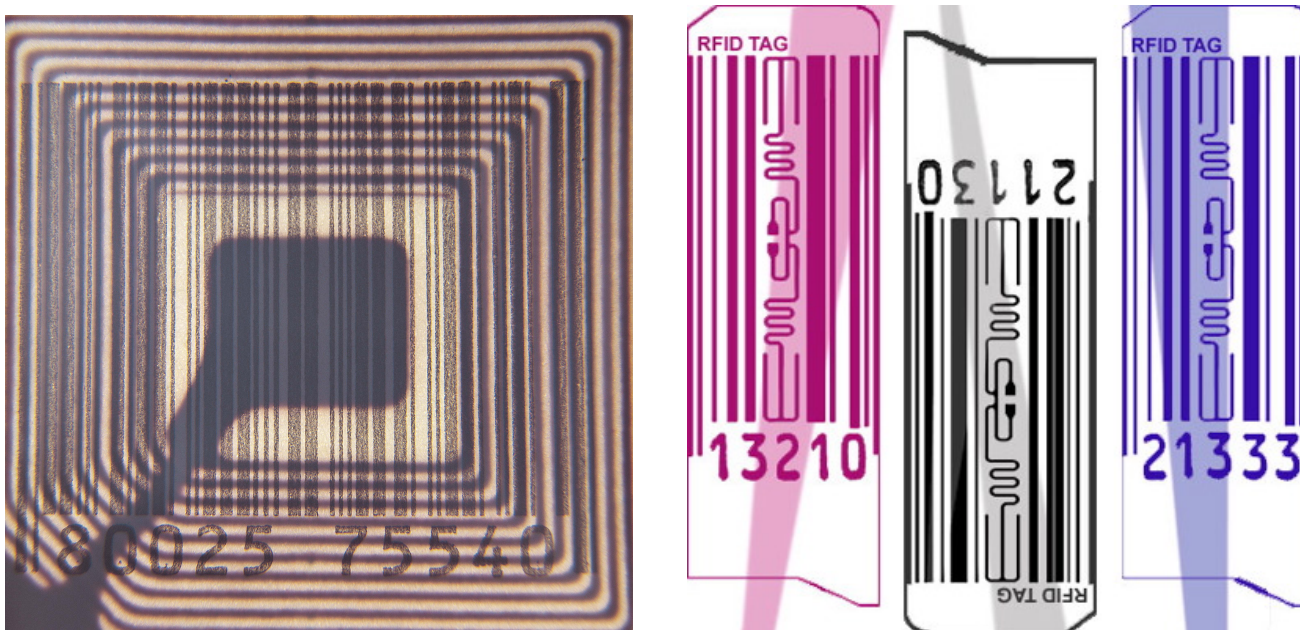


Test Case for Threshold Detection



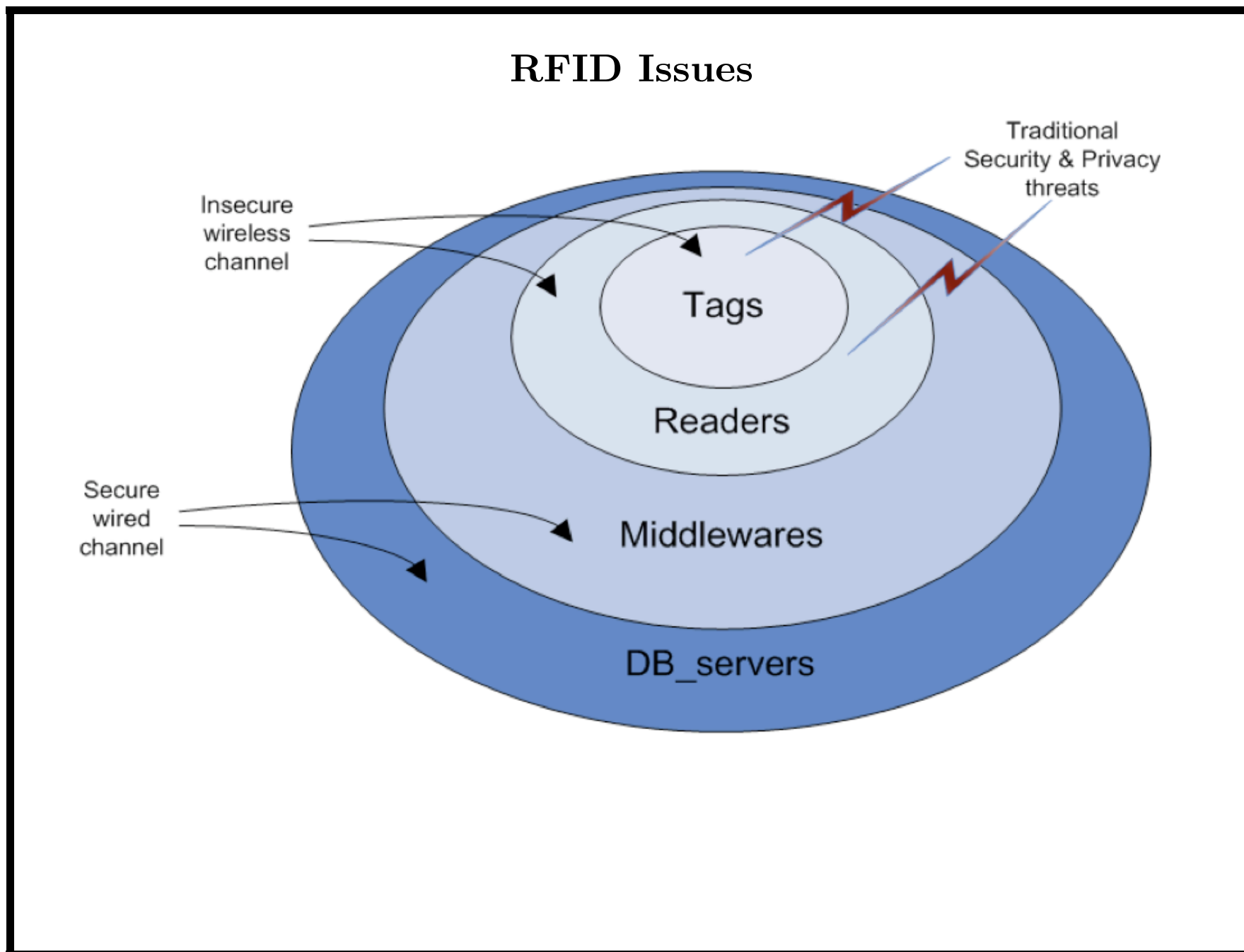
Radio Frequency Identification (RFID)

RFIDs to replace Barcodes



RFID Tags

- Radio frequency devices that transmit information (e.g., serial numbers) to compliant readers in a contactless manner
- Classified in the literature as:
 - Passive: transmission power is derived from reader
 - Active: energy comes from on-board battery
 - Semi-passive: battery to power microchips, but transmission power from reader
- Electronic Product Code (EPC) tags
 - Main kind of tags spread on today's RFID supply chain applications
 - Passive UHF RFID tags
 - EPCglobal inc: Main organization controlling development



Open Problems

1. Threats to and by front-end components (i.e., tags and readers)
2. Attacks against the back-end components (i.e., middleware and database systems)
3. Vulnerabilities of the ONS (Object Name Service) discovery service
 - Heritage of well-known threats against DNS protocols
4. Privacy and security concerns during the receiving of information
 - Availability, confidentiality, and integrity limitations
 - Moreover, necessity of a fine grained access control for the interaction of principals

Sensor Networks

Problems

- Given a layout of sensors produce predictable security parameters in order to protect
 - a given area
 - a given border