System Threat Analysis Case Study for Software Based Communications

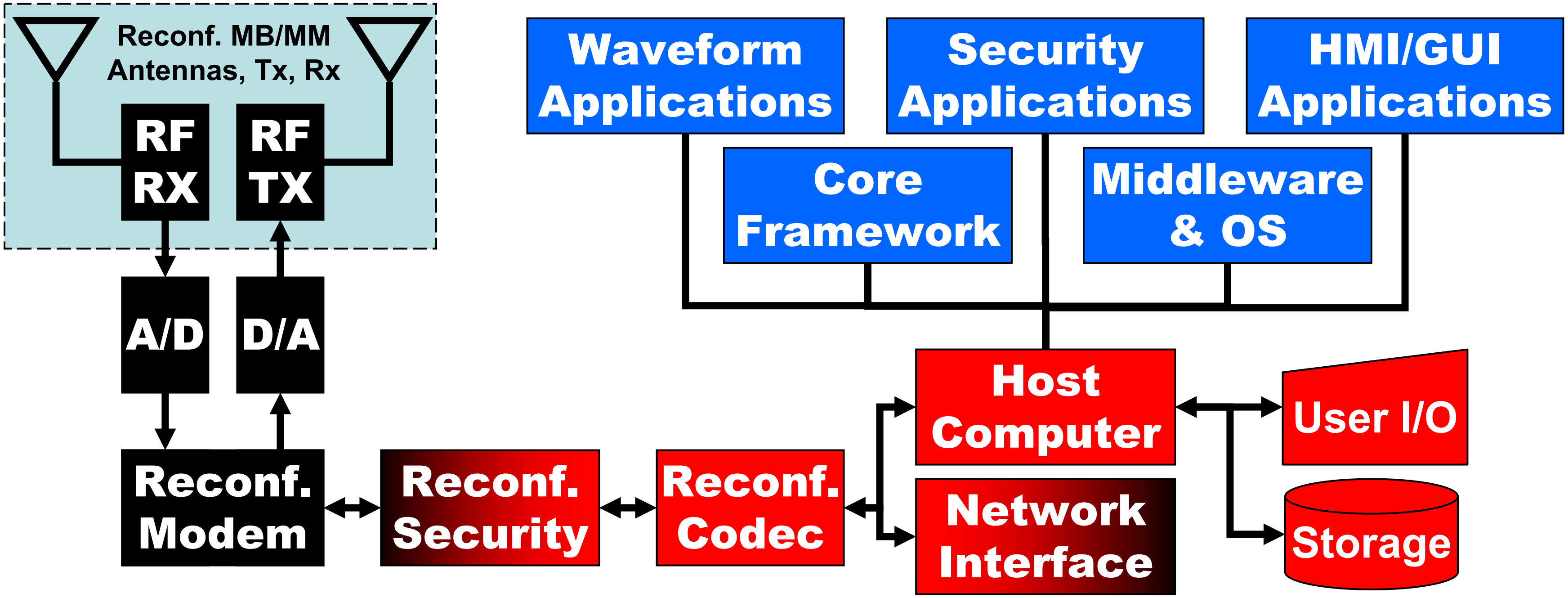
David K. Murotake, Ph.D.
dmurotak@scatechnica.com

Mobile: (603) 321-6536
www.scatechnica.com

Introduction

- Software based communications (SBC)
  - Becoming mainstream technology
  - Commercial, civil and military mobile terminals and access points.
- IEEE 802.11 Wireless Fidelity (WIFI) provides a useful case study
  - Weak security design open to blended attacks
    - Radio and computer interfaces
    - Wireless and traditional Internet “hacking” exploits
  - Highlight potential dangers posed by hackers against networks of SBC’s.

What is a *Software Radio*?



- *A software defined radio (SDR) can switch between waveforms (such as AM, FM, SINCGARS, Have Quick, DAMA, JTIDS) without hardware changes by downloading software and firmware to reconfigurable modems, codecs and security chipsets.*
- *Software radios are expected to be “mainstream” in commercial and consumer wireless devices within five years. Leading-edge users are already adopting SDR.*
- *The US Government is procuring over $6 billion worth of Joint Tactical Radio System (JTRS) SDR’s complying with the Software Communications Architecture (SCA) within the next five years.*

SDR Radio System Components

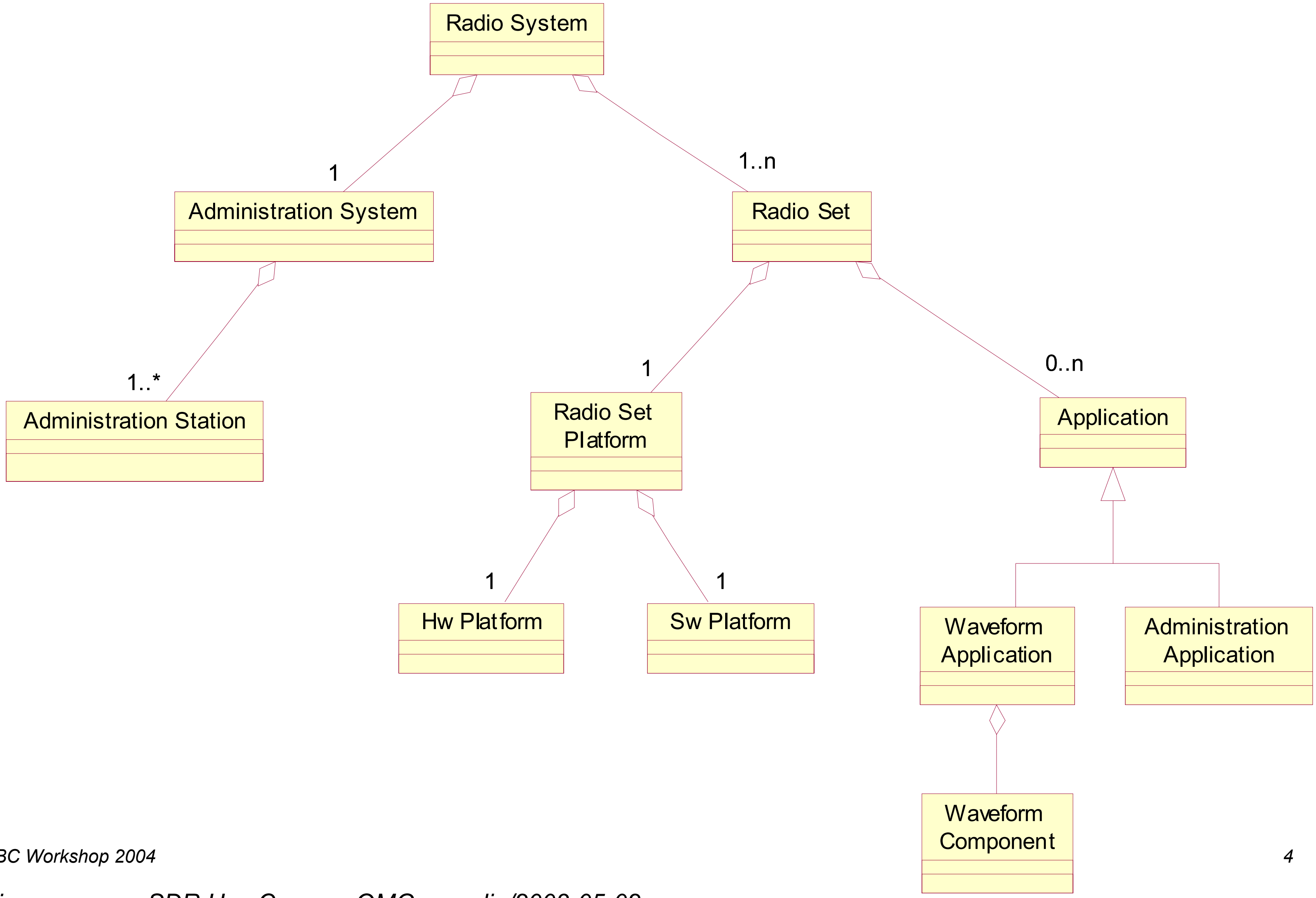
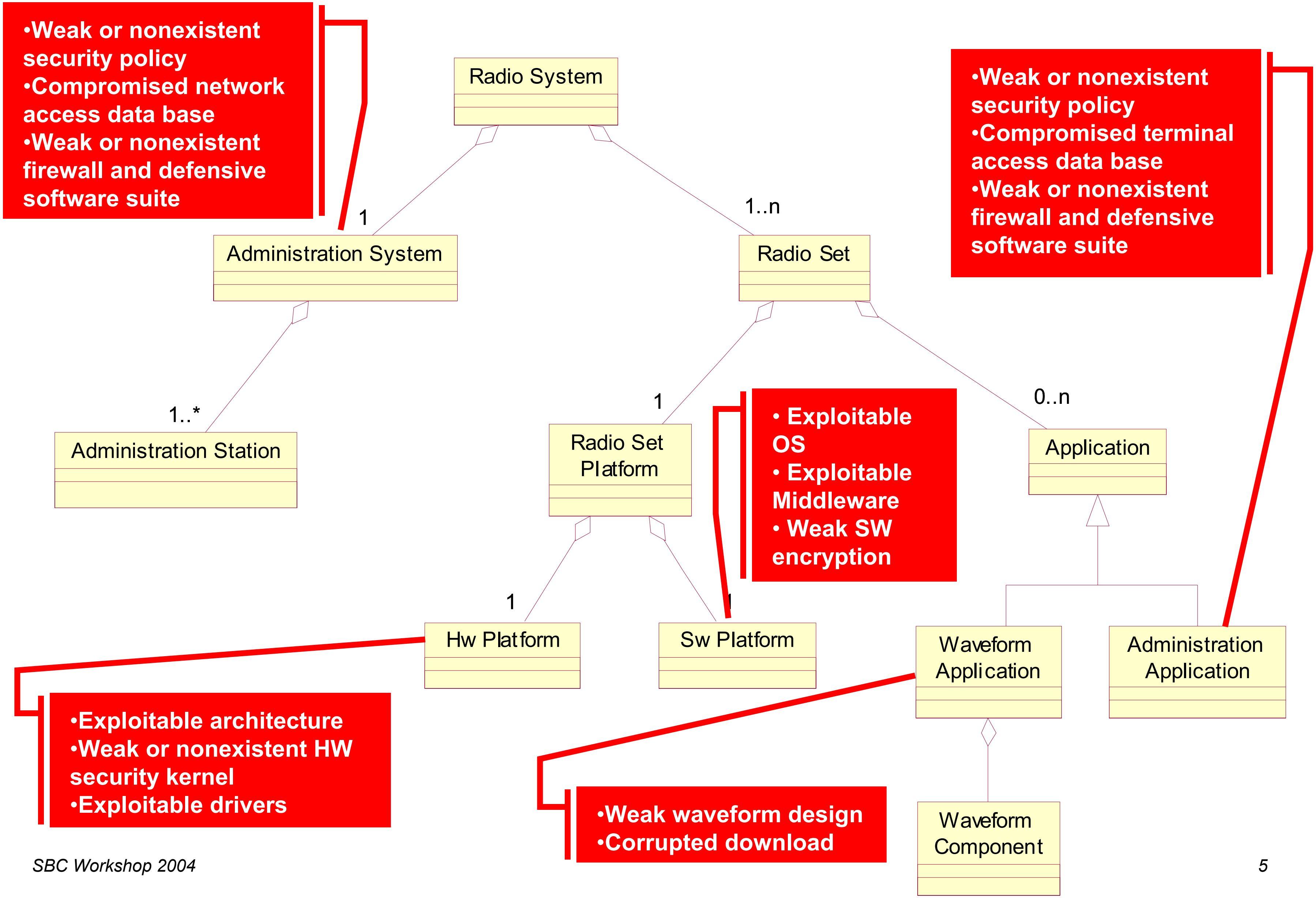


Figure source: SDR Use Cases – OMG swradio/2003-05-02

SDR Radio System Vulnerabilities



- •Weak or nonexistent security policy
- •Compromised network access data base
- •Weak or nonexistent firewall and defensive software suite

- •Weak or nonexistent security policy
- •Compromised terminal access data base
- •Weak or nonexistent firewall and defensive software suite

- • Exploitable OS
- • Exploitable Middleware
- • Weak SW encryption

- •Exploitable architecture
- •Weak or nonexistent HW security kernel
- •Exploitable drivers

- •Weak waveform design
- •Corrupted download

Figure source: SDR Use Cases – OMG swradio/2003-05-02, with modifications by SCA Technica, Inc.

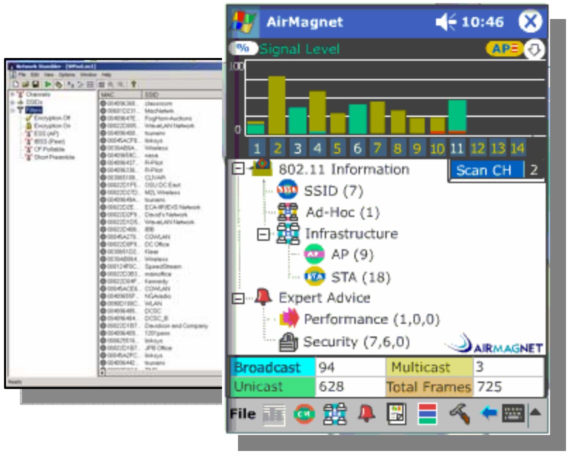
The System Threat: WIFI Case Study

Hackers & Willing Victims

- Hackers
  - Not just college kids with too much time on their hands
  - “Rogue” radio reconnaissance operators from “displaced” intelligence agencies
  - “Rogue” mathematicians and computer scientists
  - Industrial espionage
  - Terrorists
  - Intelligence agencies
- Willing victims
  - “Rogue” WLAN’s are those operating despite corporate regulations banning WLAN (because of security threat)
  - Over 30% of corporations and government agencies have “rogue” nodes operating
  - Over 80% of WIFI access points are unencrypted
  - Most users having any difficulty with encryption turn it off and operate in the clear
  - Most users will do ANYTHING for an internet connection NOW

WIFI Threat: Hacker Tools

- Software Tools
  - Downloadable from internet (most are Linux based)
  - Stumblers allow wireless hackers to explore the network characteristics of wireless access points (base stations) and mobile terminals
  - Sniffers intercept, display, and store data being transmitted over the network
  - Crackers break encryption codes, such as Wired Equivalent Protection (WEP)
  - Enterprise level tools available (e.g. AirMagnet)
  - Malicious software (e.g. keystroke repeaters)



Broadcast	94	Multicast	3
Unicast	628	Total Frames	725

- Hardware Tools
  - Modified wireless cards, access points, and software drivers
  - High gain antennas (used with hacker mobile terminals or access points)
  - Power amplifiers (used with hacker terminals or access points; often illegal)
  - Enterprise level (professional grade) tools available including hand-held products; can be used by both IT managers and hackers

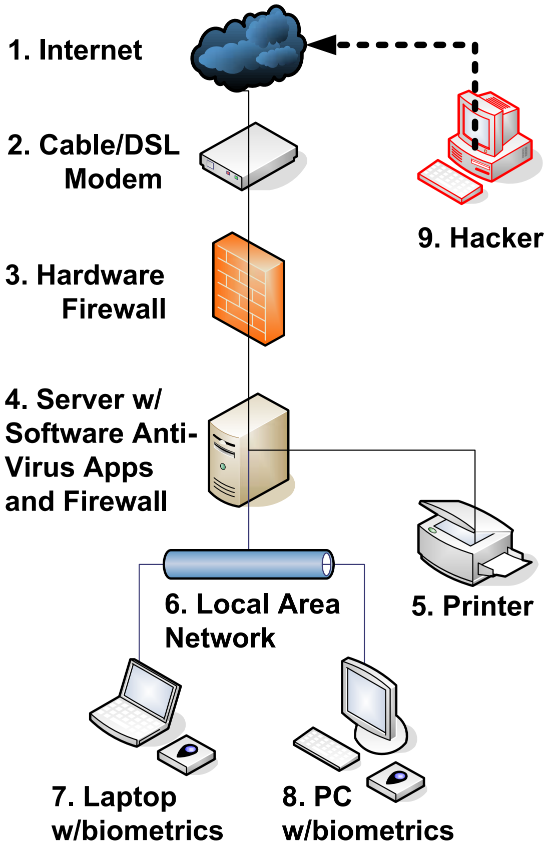
SDR's may be the "ultimate" hacking tool in the wrong hands

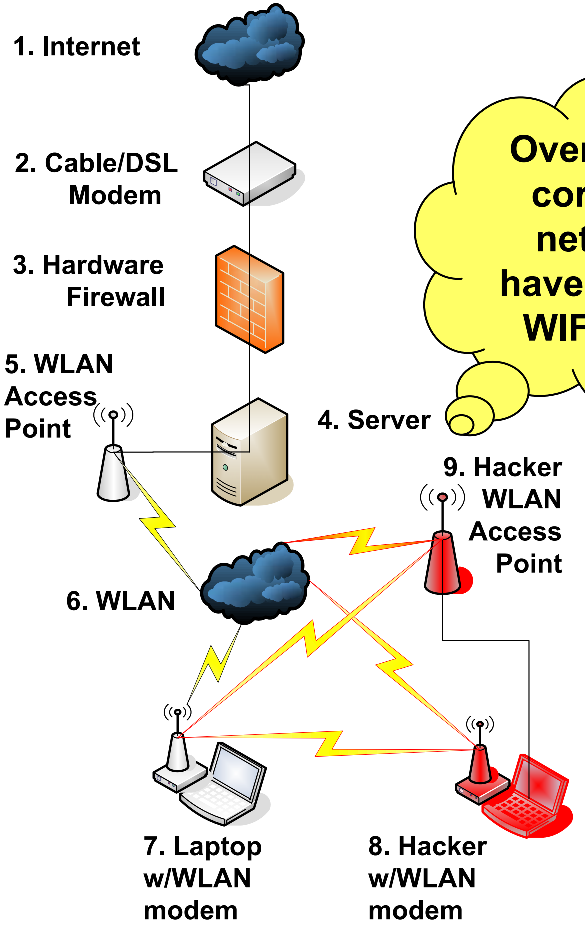
Wireless Attack Methods

Threat Category	Attacks on Radio Interface	Attacks on Other Parts of System
Unauthorized access to data	Example: Use of “stumbler” SW to detect WIFI hot spots, identify wireless access point (WAP) characteristics. Use of “sniffer” SW to intercept data.	Intruders may eavesdrop signaling data or control data on any system interface, whether wired or wireless. This may be used to conduct other attacks on system.
Threats to integrity	Hacking encryption codes using SW e.g. WEPCRACK. Planting malicious SW in radio component.	Intruders may modify, insert, replay or delete signaling or control data on any system interface, whether wired or wireless. Planting malicious software on computer.
Denial of service	Intruders may prevent user traffic, signaling data and control data from being transmitted on the radio interface, e.g. jamming.	Intruders may attempt to prevent user traffic by a coordinated transmission of large numbers of packets by means of a virus infection of a network..
Unauthorized access to services	The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication.	Intruders may impersonate a user to utilize services authorized for that user.
Repudiation	Repudiation of user traffic origin: A user could deny that he entered the network (no access logs).	Repudiation of user traffic origin: A user could deny that he sent user traffic.

“Security Threats and Requirements; 3GPP TS 21.133 V4.1.0 (2001-12); 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects”.

The WIFI Hacking Scenario





Over 30% of corporate networks have "rogue" WIFI users

The blended attack allows hackers to penetrate the wireless layer and gain full access to the mobile computer

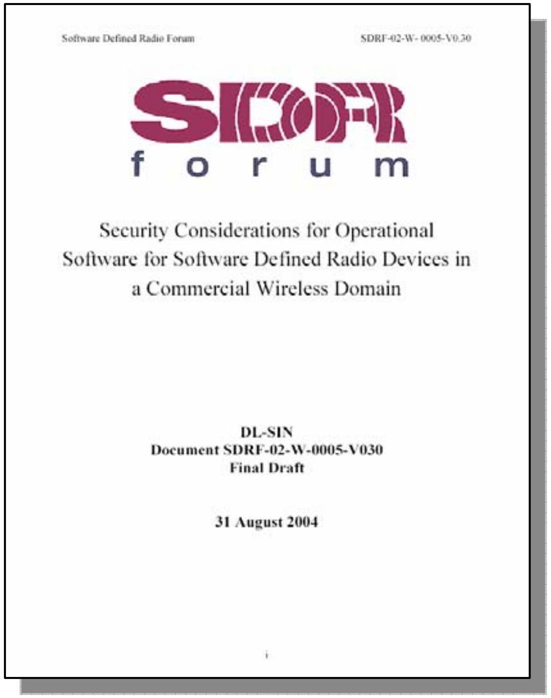
Blended Attacks against WIFI

- Attack vs unencrypted WIFI infrastructure
  - Use “stumbler” SW to detect wireless network, obtain wireless access point (WAP) control information
  - Enter network and use “sniffer” SW to obtain unauthorized access to data
  - Install malicious software (malware) on PC to obtain unauthorized access to computer information
- Attack vs WEP encrypted WIFI
  - Use stumbler SW to detect WAP control information
  - Method 1: Use hacking software, e.g. WEPCRACK, to break WEP encryption code. Enter network and use “sniffer” to obtain unauthorized access to data
  - Method 2: Use Denial Of Service (jamming) attack on target WAP. Force users to turn off encryption. Users automatically switch to Hacker’s WAP on another channel.
  - Install malicious software (malware) on PC to obtain unauthorized access to computer information
- Attack vs WPA encrypted WIFI
  - Use stumbler SW to detect WAP control information
  - Use Denial Of Service (jamming) attack on target WAP. Force users to turn off encryption. Users automatically switch to Hacker’s WAP on another channel
  - Install malicious software (malware) on PC to obtain unauthorized access to computer information

System Threat Analysis Conclusions

- Wireless computers are vulnerable to blended attacks
  - WIFI has a weak security design
  - Hackers have access to sophisticated, enterprise grade tools
  - Coordinated attacks against the radio and computer interfaces
  - Coordinated attacks against mobile terminal and access point
- Wireless computers must protect against blended attacks
  - Holy Grail #1: Protect mobile terminals without requiring changes to existing (weak) standards or access points
  - Holy Grail #2: Protect access points (and corporate networks) without requiring changes to existing (weak) standards or upgrades to mobile terminals
  - Be able to leverage improved WIFI standards (e.g. 802.11 g)
- Protecting the data using encryption is not enough
  - Must protect the integrity of the underlying computer system against malicious software e.g. keystroke repeaters

Software Radio Security Architecture



Software Defined Radio Forum SDRF-02-W- 0005-V0.30

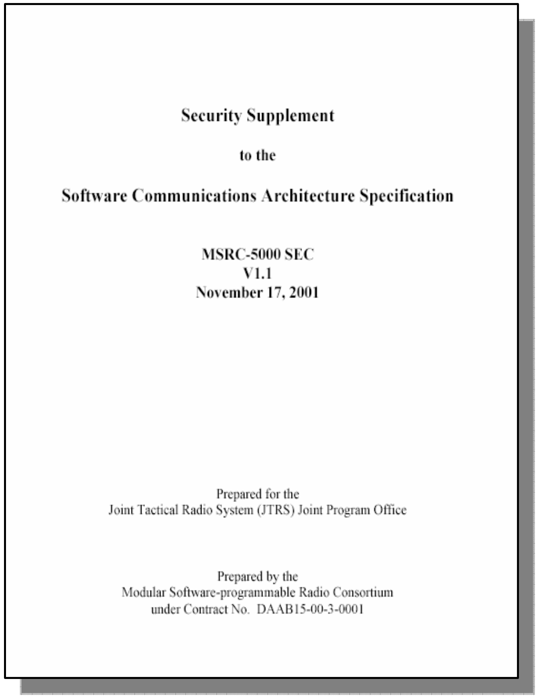
SDR forum

Security Considerations for Operational Software for Software Defined Radio Devices in a Commercial Wireless Domain

DL-SIN
Document SDRF-02-W-0005-V030
Final Draft

31 August 2004

i



Security Supplement

to the

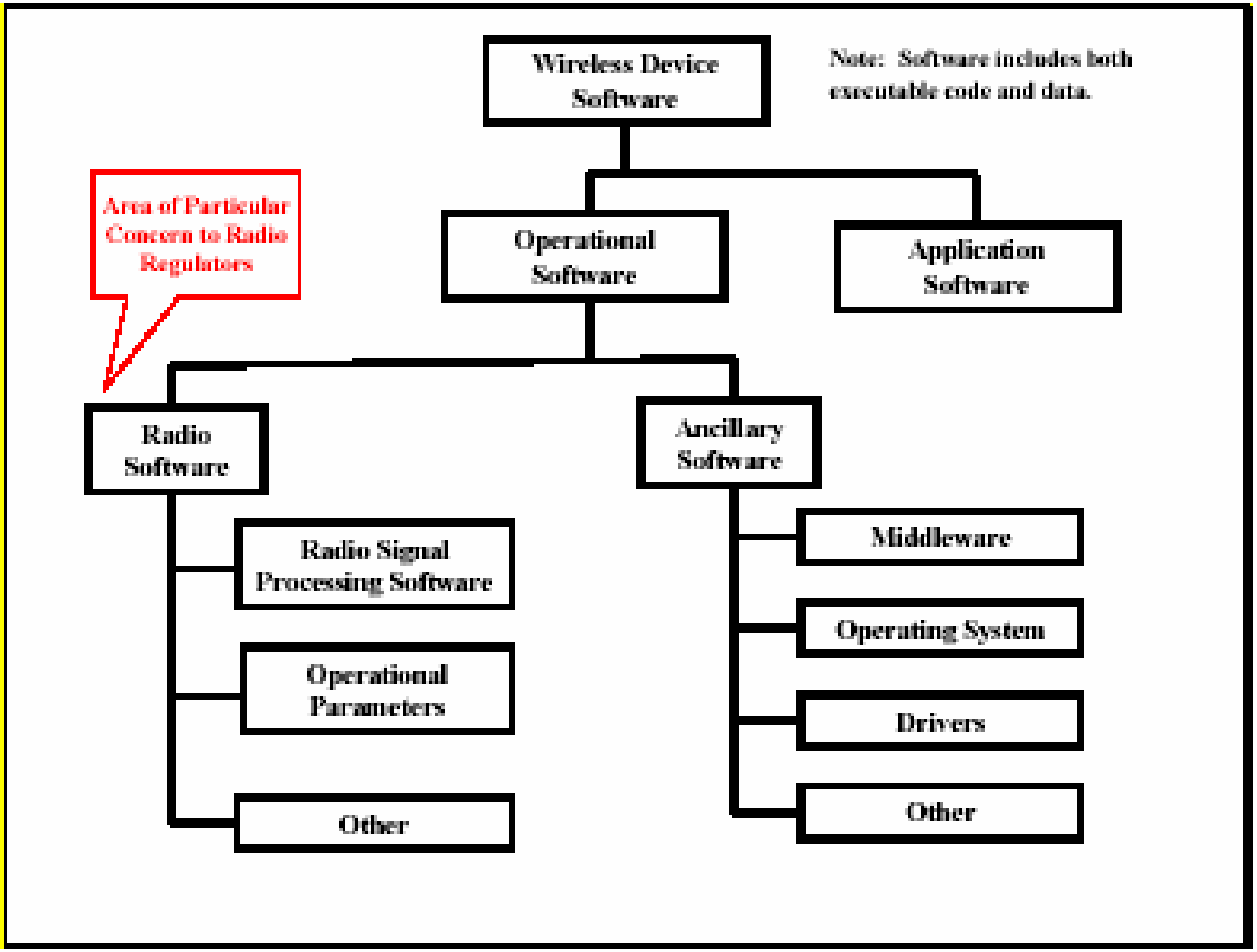
Software Communications Architecture Specification

MSRC-5000 SEC
V1.1
November 17, 2001

Prepared for the
Joint Tactical Radio System (JTRS) Joint Program Office

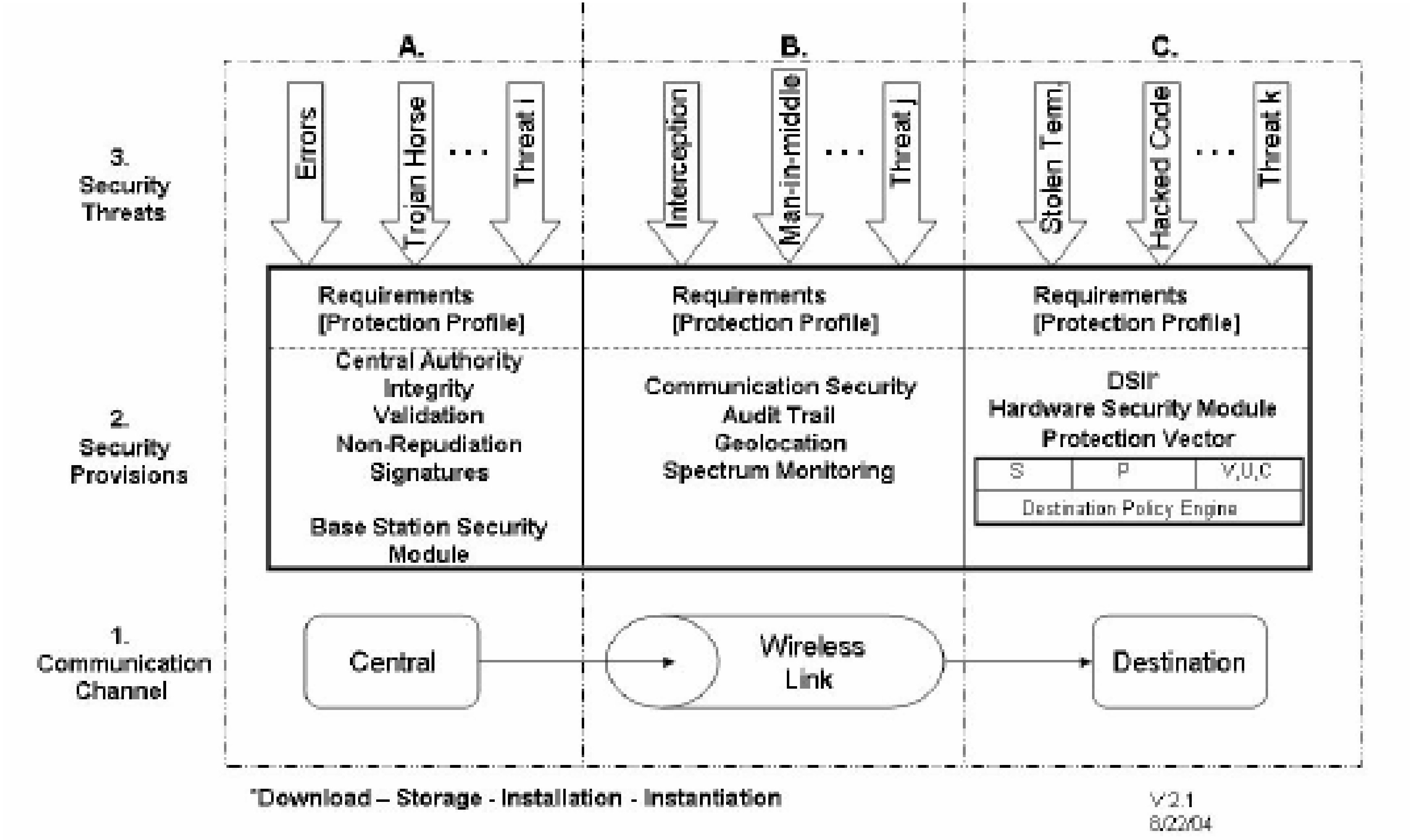
Prepared by the
Modular Software-programmable Radio Consortium
under Contract No. DAAB15-00-3-0001

Software/firmware categories for commercial wireless devices



Source: Document DL-SIN, Final Draft, SDRF-02-W- 0005-V0.30, 31 August 2004

SDR Forum Security Reference Model (Draft)



Source: Document DL-SIN, Final Draft, SDRF-02-W- 0005-V0.30, 31 August 2004

SCA Technica, Inc.

Security Framework (Gallery 2003)

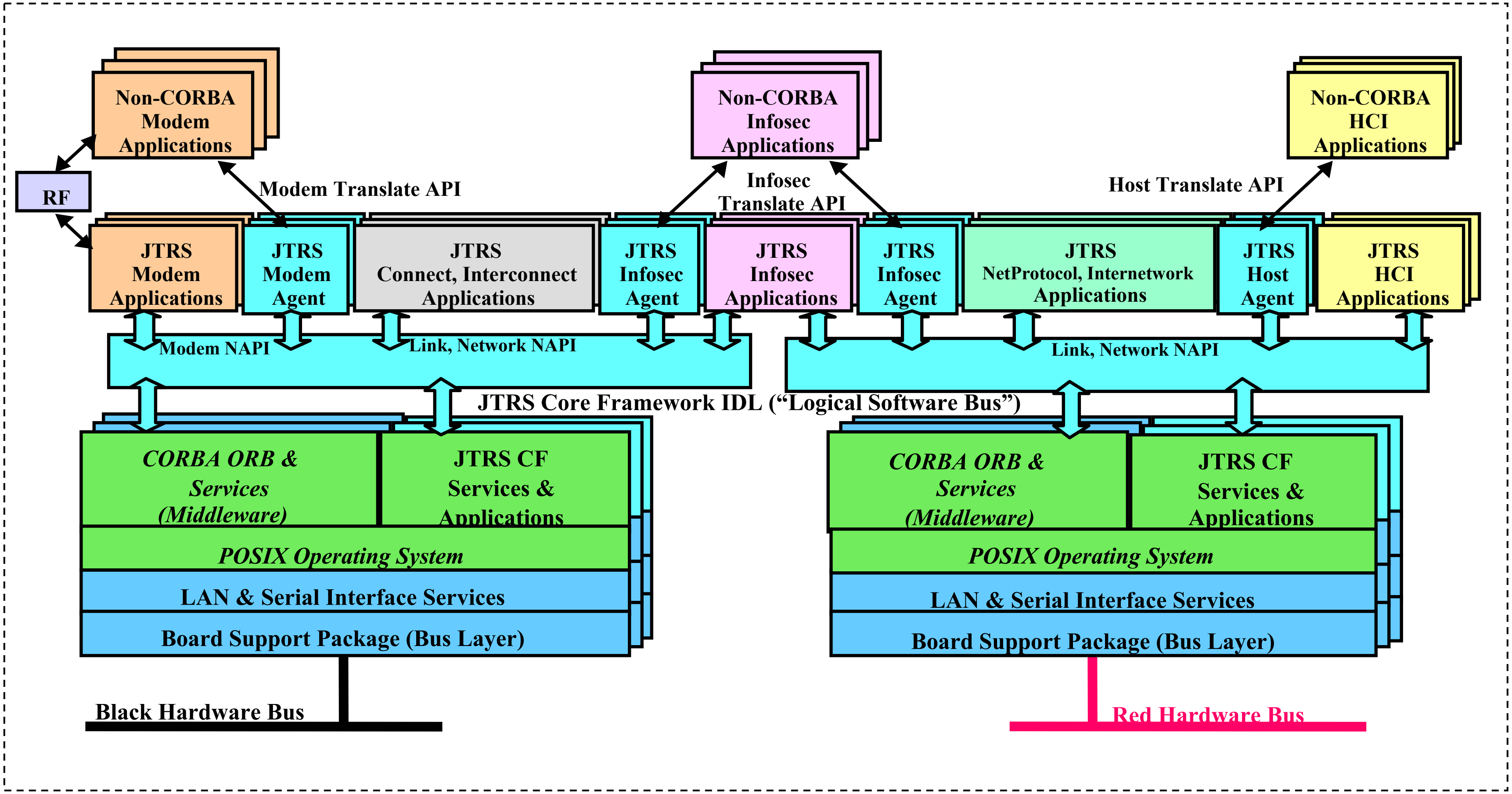
- Entity Roles and Responsibilities
- Digital Signatures
- Public Key Infrastructure (PKI)
- Virus Scanning
- Trust Relationships
- Proof Carrying Code (PCC)
- Path Histories

Source: Gallery, E. (2003). A Policy-Based Framework for the Authorisation of Software Downloads in a Mobile Environment. 2003 Software Defined Radio Technical Conference, Session SY-2.

Recommended Security Features (Defense-in-depth)

1. Security Policy Enforcement and Management
2. Information Integrity
3. Authentication and Non-repudiation
4. Access Control
5. Encryption and Decryption Services
6. Key and Certificate Management
7. Standardized Installation Mechanisms
8. Auditing and Alarms
9. Configuration Management
10. Memory Management
11. Emissions Management
12. Computer Security, including virus scanning and firewalls

JTRS "Red/Black" Security (SCA 2.2) Example of "Layered" Defense In Depth


Non-CORBA Modem Applications
Non-CORBA Infosec Applications
Non-CORBA HCI Applications
RF
Modem Translate API
Infosec Translate API
Host Translate API
JTRS Modem Applications
JTRS Modem Agent
JTRS Connect, Interconnect Applications
JTRS Infosec Agent
JTRS Infosec Applications
JTRS Infosec Agent
JTRS NetProtocol, Internetwork Applications
JTRS Host Agent
JTRS HCI Applications
Modem NAPI
Link, Network NAPI
Link, Network NAPI
JTRS Core Framework IDL ("Logical Software Bus")
CORBA ORB & Services (Middleware)
JTRS CF Services & Applications
POSIX Operating System
LAN & Serial Interface Services
Board Support Package (Bus Layer)
CORBA ORB & Services (Middleware)
JTRS CF Services & Applications
POSIX Operating System
LAN & Serial Interface Services
Board Support Package (Bus Layer)
Black Hardware Bus
Red Hardware Bus

Source: JTRS JPO, Joint Program Status Update, 30 June 2003

JTRS and/or Legacy Applications
JTRS Core Framework (JCF)
Commercial Off-the-Shelf (COTS)

Biometric Sensor Model

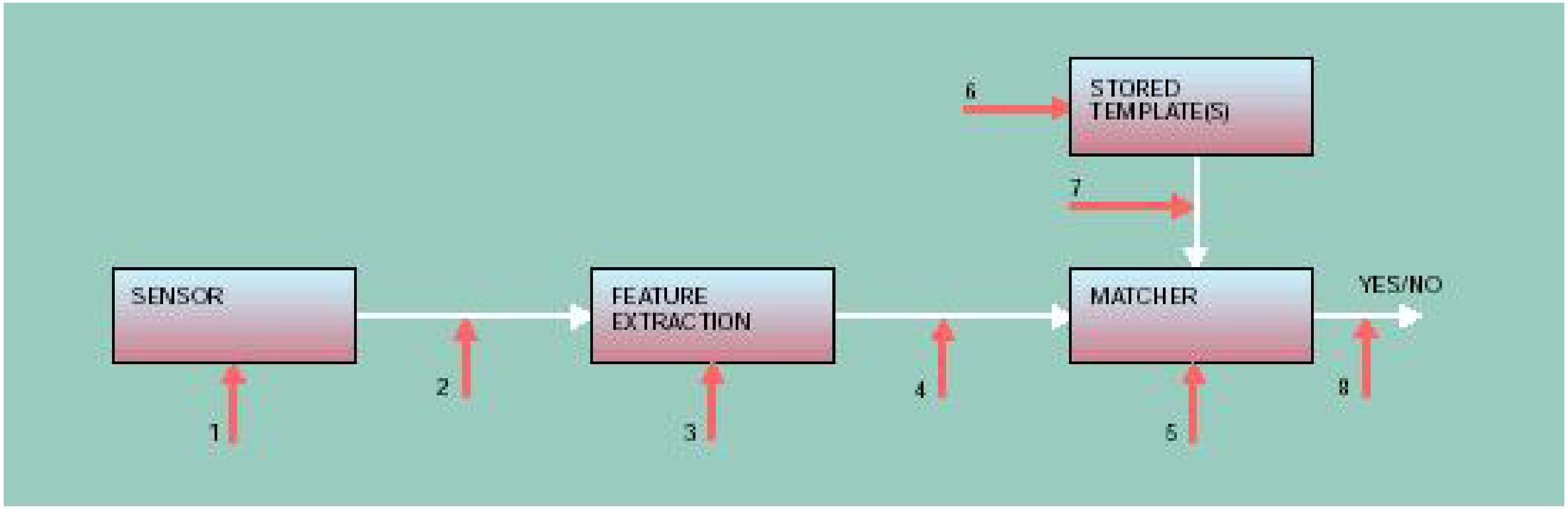


Figure: Ratha et al, "Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40:3, 2001

- Model can be generalized to include:
  - Password entry
  - Fingerprint scanner
  - Speaker verification
  - Retinal scanning
  - Face/body recognition
  - RF watermarks
  - Radio fingerprinting
- Synergistic with software radio

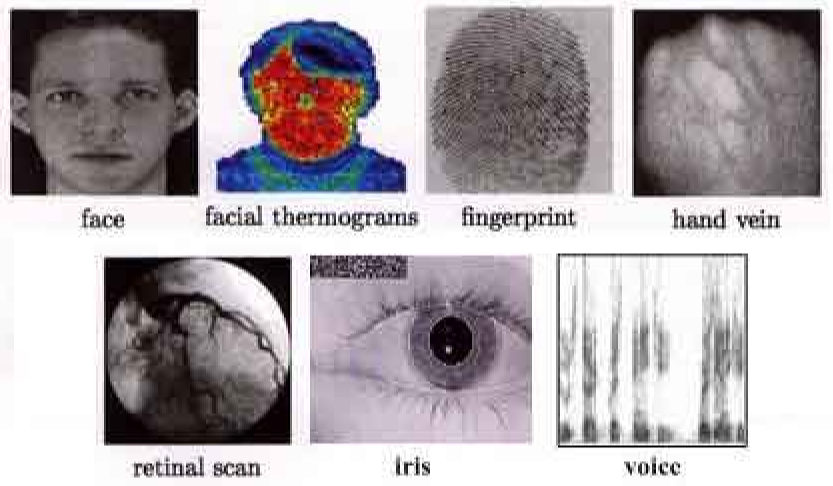


Figure source: Sonetech Corporation

SDR Security Architecture Conclusions

- SDR security is a *system level* problem
- Must understand the system threat and requirements
  - Blended attacks against radio and computer layers
- Must protect…
  - Both the mobile clients and servers
    - Mobile radio, mobile host
    - Server radio, server host
  - Integrity of software applications and downloads
    - SDR Forum Download Security, Installation and Instantiation (DSII)
  - Integrity of the reconfigurable platform
    - Defeat blended attacks
    - Employ 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
- Employ…
  - Security oriented architecture with defensive layer to defeat blended attacks
  - High assurance components e.g. MLS orb and OS to enhance platform integrity
  - Integrated, multi-mode biometrics etc. for improved end to end assurance