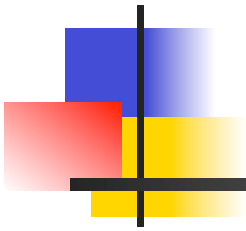


Biotelemetry and Computer Security



Alf Weaver (CS)
Ben Calhoun (ECE)
Travis Blalock (ECE)



Alf Weaver

- CS faculty since 1977
- Research in networks, communications protocols, e-commerce, CS education, telemedicine, computer security
- PI or co-PI on 125 sponsored research projects
- Supervisor for 65 MS, MCS, and PhD students



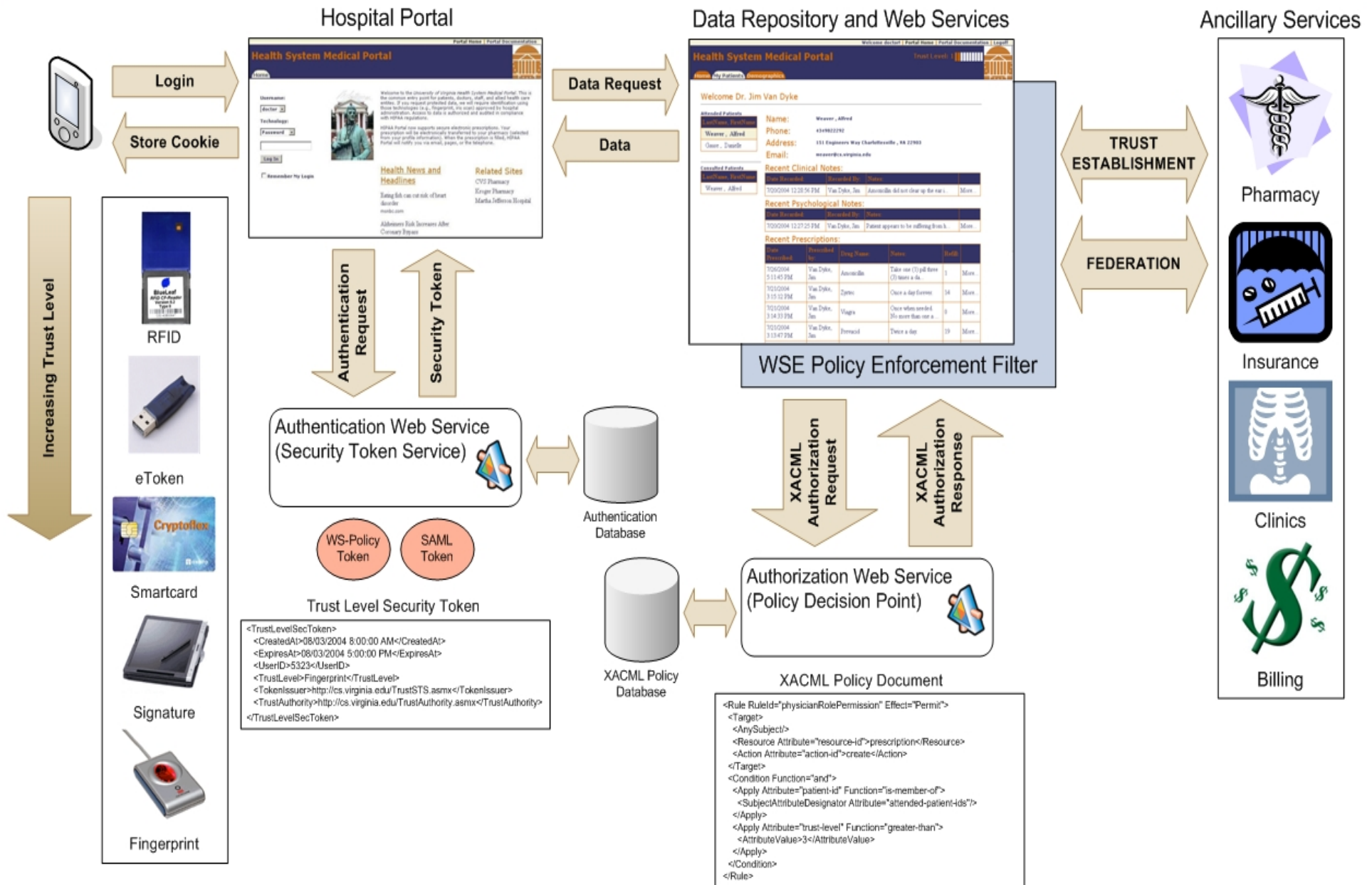
Previous Work in Medicine

- Quantitative medical decision aids
- Compression of digital ultrasound images
- NSF Research Experience for Undergrads during 2005-07 on “Computer Applications for Medicine”
- Using web services to protect healthcare information

SECURITY ARCHITECTURE

Advancing Cyber Security with .NET

Alfred C. Weaver, Brian Garback, James Van Dyke,
Joseph Calandrino, Paul Bui, Ryan Kurtz, Zhengping Wu
Department of Computer Science, University of Virginia





One Project, Three Goals

- Mobile device security—device useful only in proximity to its user
- Biotelemetry—view physiological data at a distance
- Data analysis—ECG characterization and (ultimately) assistance with disease diagnosis



Biotelemetry and Computer Security

- Problem: mobile devices (PDA, laptop, cell phone) can represent a security leak if either user or device is compromised
- Goal is to secure devices by:
 - require initial strong personal authentication
 - continue operation only in the presence of an acceptable physiological signal
 - revert to a *locked state* (all user files encrypted) or *safe state* (all user files erased) if user or device is compromised

Uses



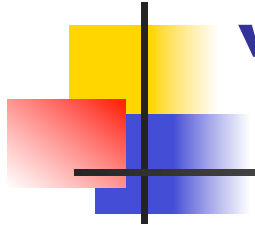
Soldiers



Physicians



Emergency Medical Services

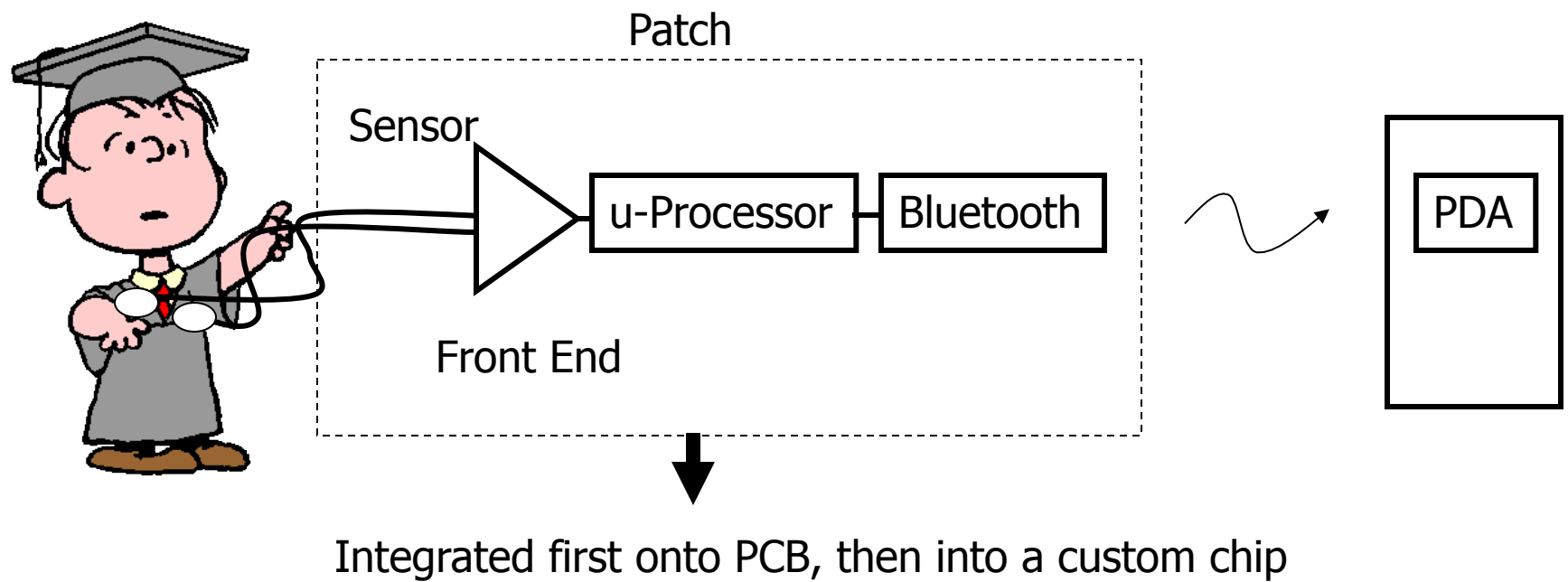


“The Patch”

- Low-power IC with sensor, microcontroller, and radio
- Designed using sub-threshold logic
- Form factor like a Band-Aid
- Collects physiological data, performs some local processing, and transmits over a wireless channel
- Initially: heart rate sensor, Bluetooth
- Intermediate: additional sensors such as respiration, pulse oximetry, temperature, motion, environmental
- Ultimately: energy-scavenging from body
- Innovations: sub-threshold logic to reduce power; local signal processing; view data at a distance; control patch remotely

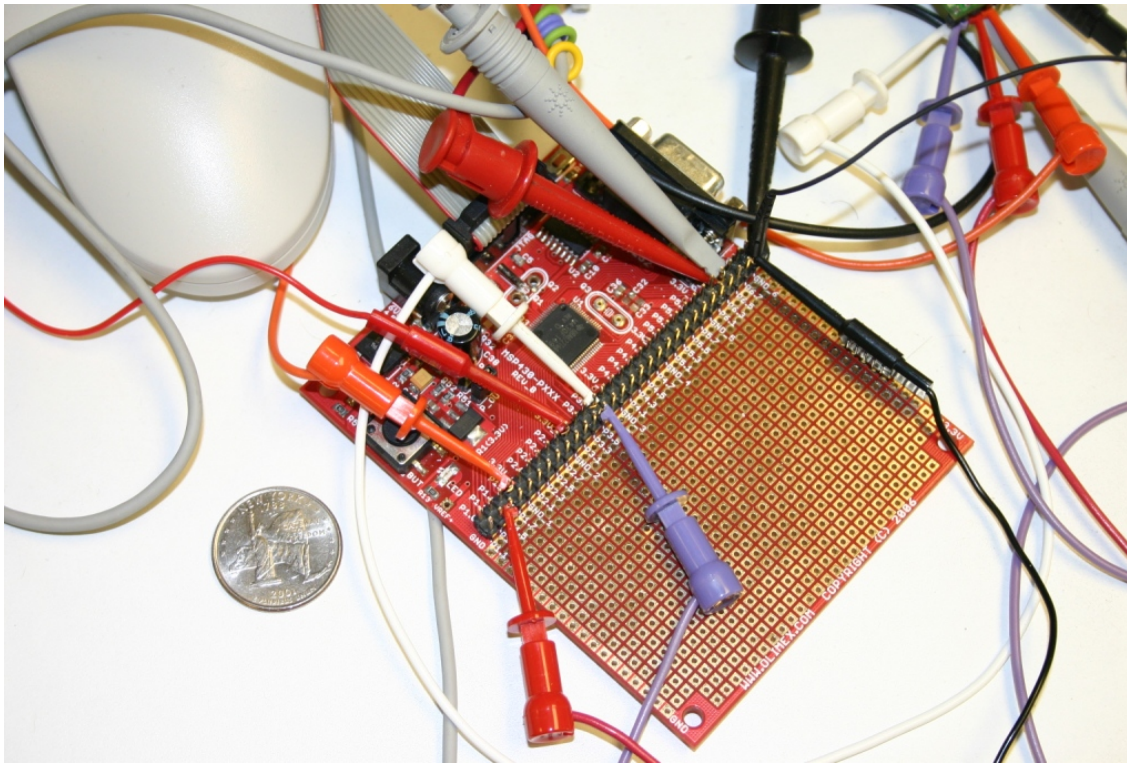
PCB Prototype – Data Flow

- Full ECG data flow working on PCB



Patch Prototype

- Sensor, microcontroller, radio



PCB Prototype





PDA policy setting

- PDA monitors heart rate to determine if the data should be *locked* (inaccessible until re-authentication) or *erased* (safe state)
- Potential triggers:
 - no heart beat detected
 - low heart rate for some period of time
 - PDA out of range
 - tampering with the patch
 - many more possible with more/different sensors

Setting Policies



Secure Mobile Computing 2007

Please Log In to Authenticate

User Name:

Password:

Attempts left: 5

123 1 2 3 4 5 6 7 8 9 0 - = <

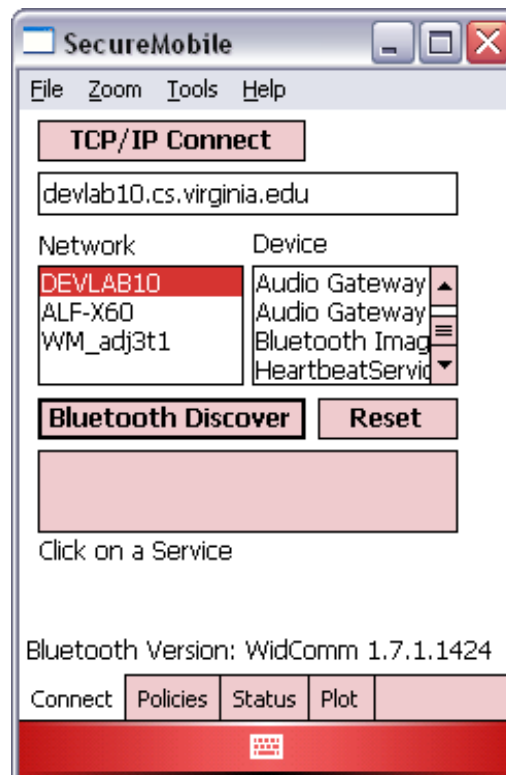
Tab q w e r t y u i o p []

CAP a s d f g h j k l ; ' CAP

Shift z x c v b n m , . / <

Ctl á ü ` \ | _ < > <

Initial Authentication

SecureMobile

File Zoom Tools Help

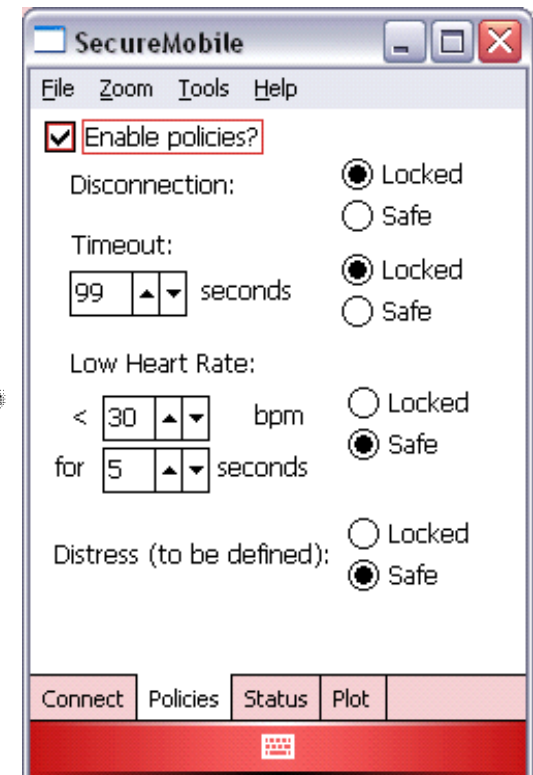
TCP/IP Connect

Network	Device
DEVLAB10	Audio Gateway
ALF-X60	Audio Gateway
WM_adj3t1	Bluetooth Imag
	HeartbeatServic

Bluetooth Version: WidComm 1.7.1.1424

Connect Policies Status Plot

Connect to Patch Simulator

SecureMobile

File Zoom Tools Help

☒ **Enable policies?**

Disconnection: ☒ Locked ☐ Safe

Timeout: seconds ☒ Locked ☐ Safe

Low Heart Rate: ☐ Locked ☒ Safe

< bpm

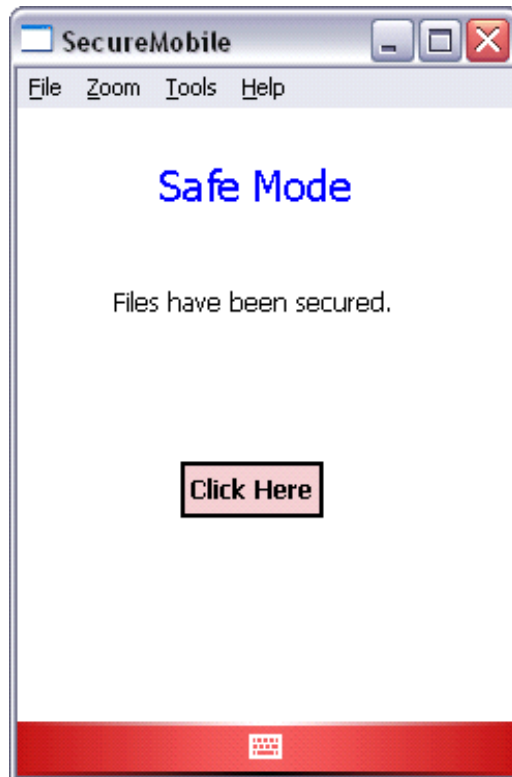
for seconds

Distress (to be defined): ☐ Locked ☒ Safe

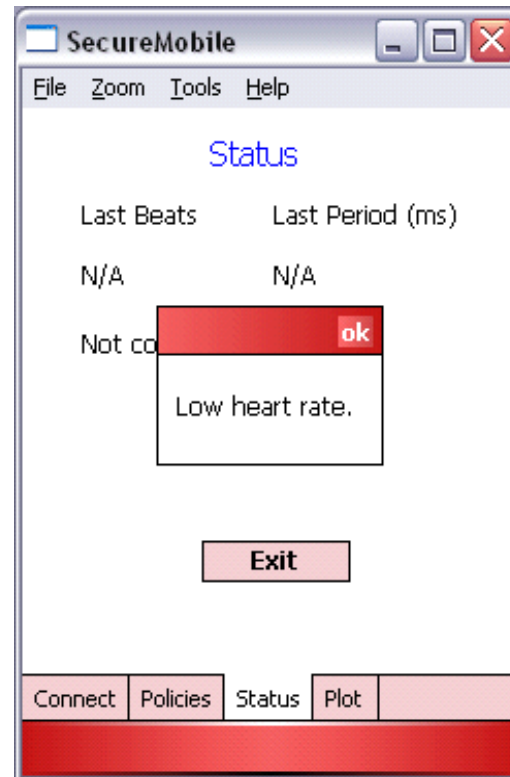
Connect Policies Status Plot

Policy Control Engine

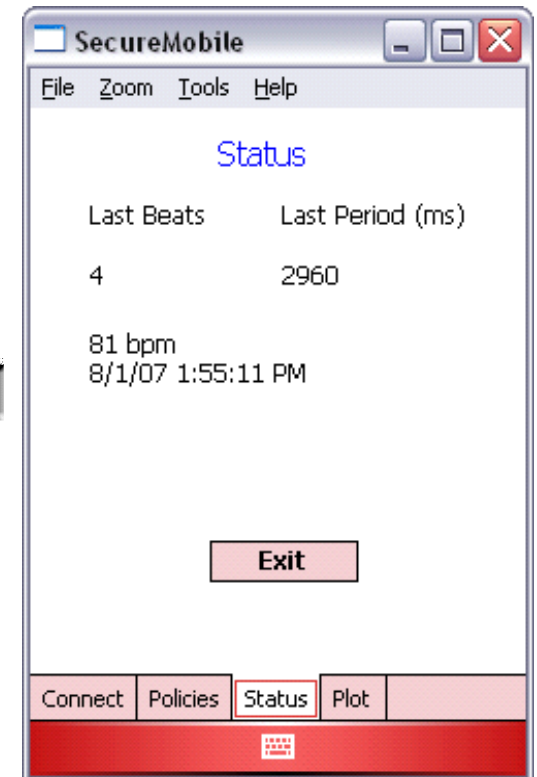
Monitoring the Signal



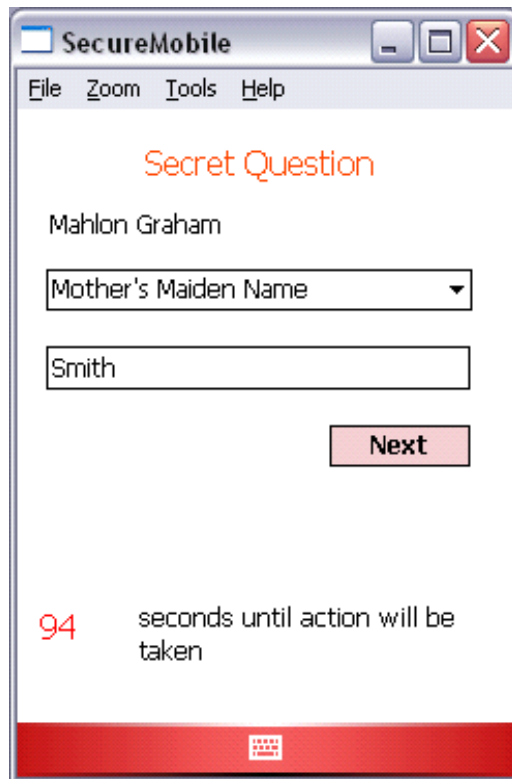
Safe Mode Entered



Low Heart Rate Event



Re-authentication



SecureMobile

File Zoom Tools Help

Secret Question

Mahlon Graham

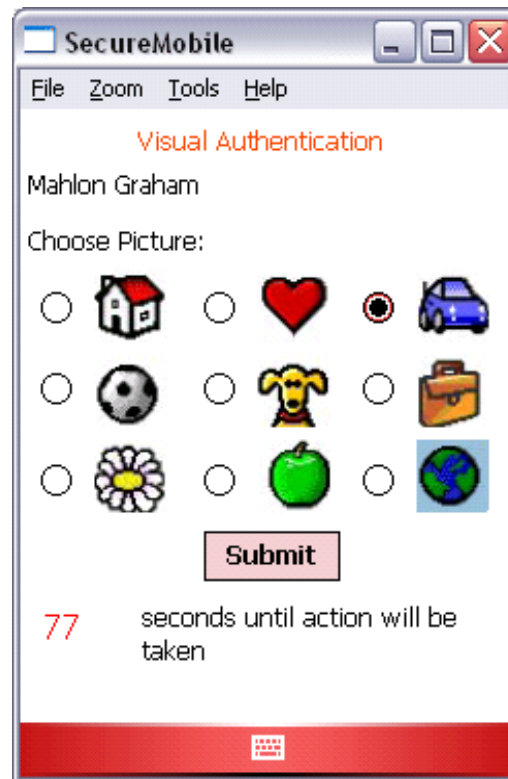
Mother's Maiden Name

Smith

Next

94 seconds until action will be taken

Re-authenticate 1












SecureMobile

File Zoom Tools Help

Visual Authentication

Mahlon Graham

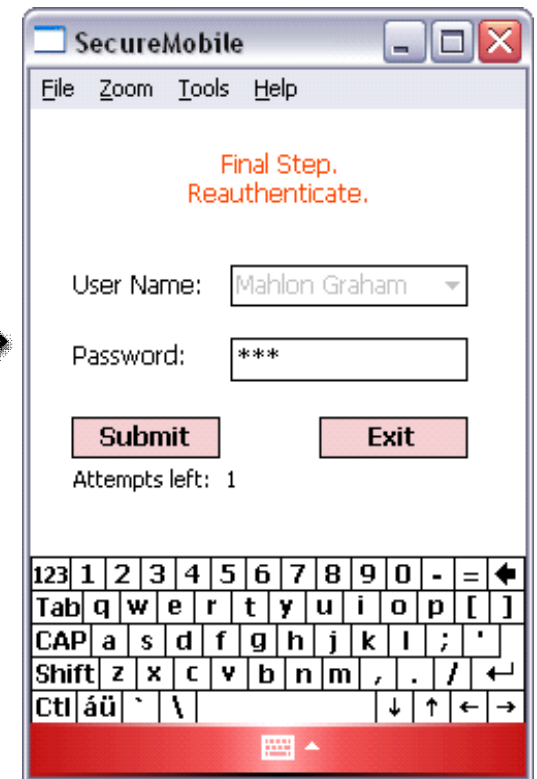
Choose Picture:

<input type="radio"/>		<input type="radio"/>		<input type="radio"/>	
<input type="radio"/>		<input type="radio"/>		<input type="radio"/>	
<input type="radio"/>		<input type="radio"/>		<input type="radio"/>	

Submit

77 seconds until action will be taken

Re-authenticate 2



SecureMobile

File Zoom Tools Help

Final Step.
Reauthenticate.

User Name: Mahlon Graham

Password: ****

Submit Exit

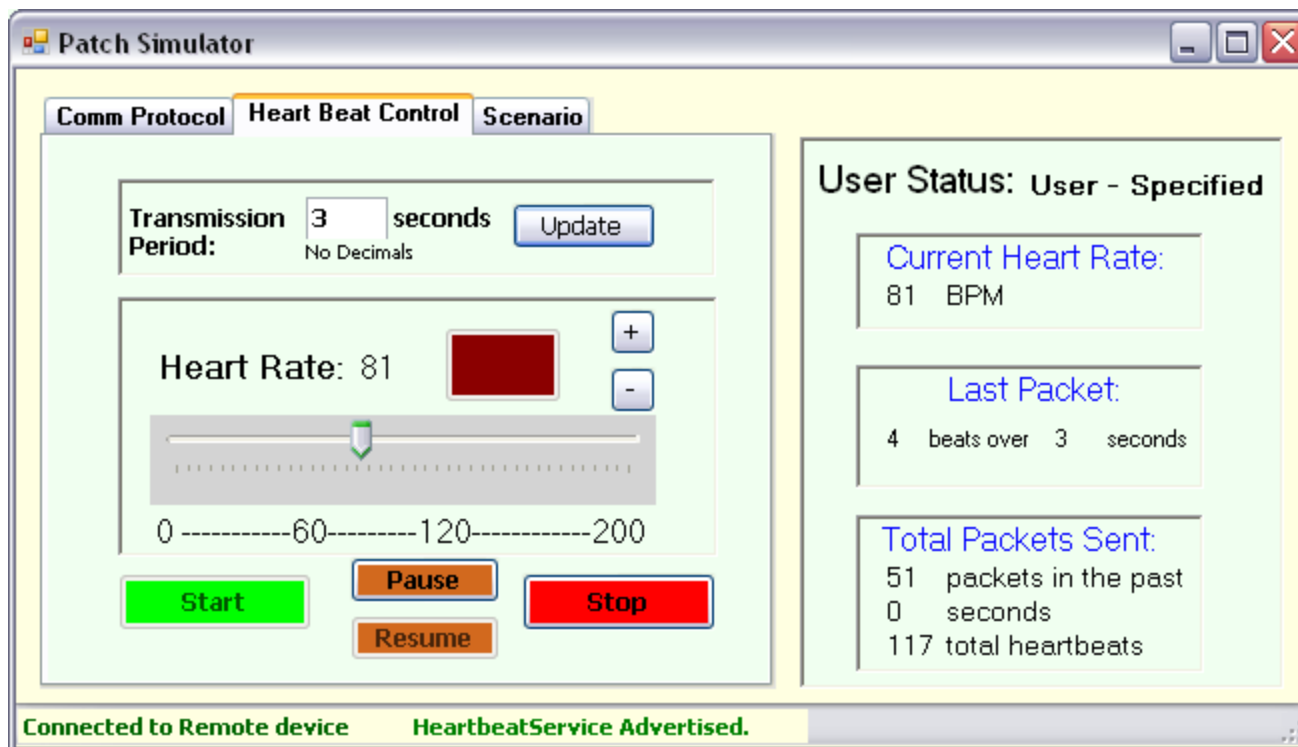
Attempts left: 1

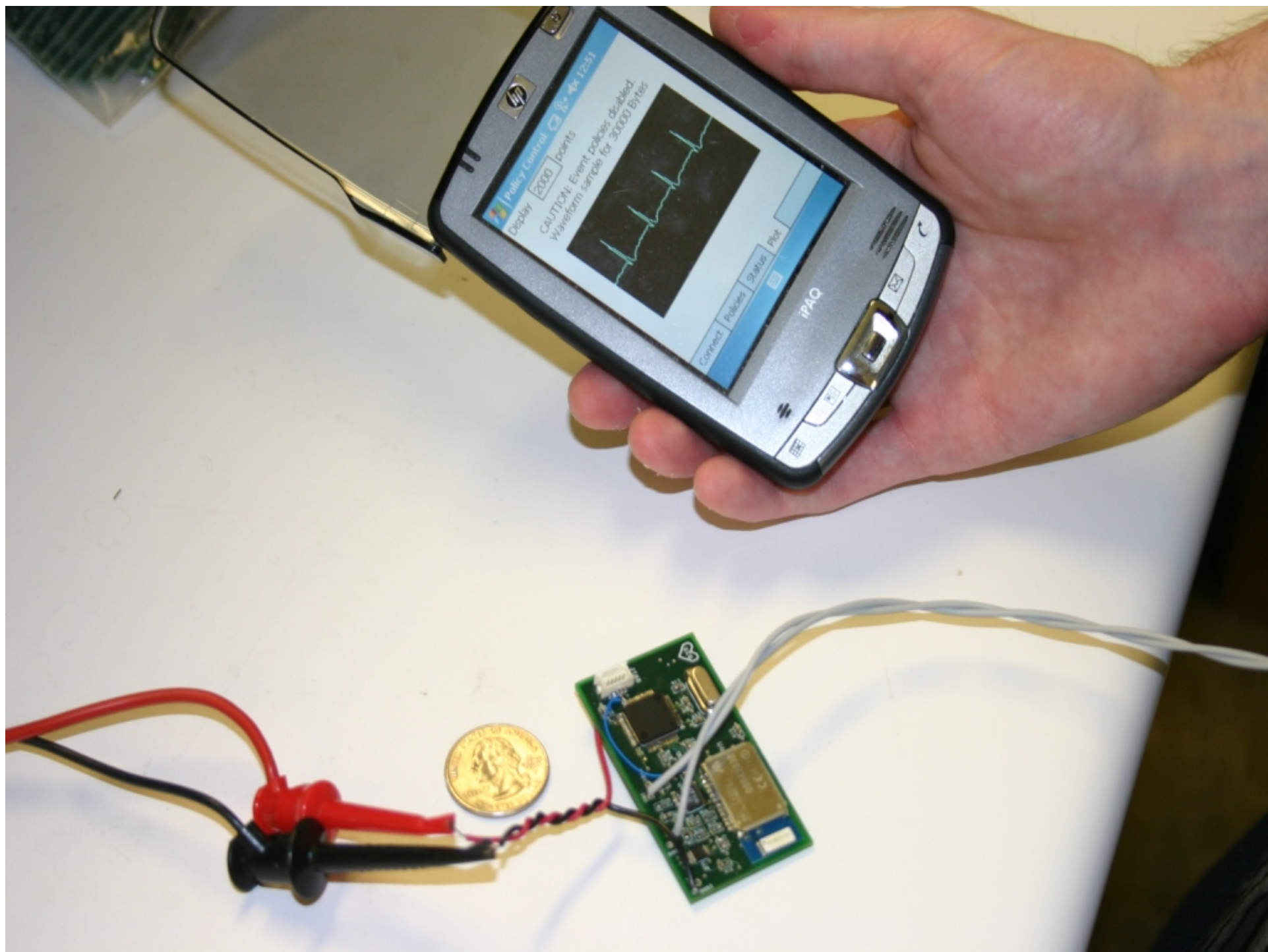
123	1	2	3	4	5	6	7	8	9	0	-	=	↩
Tab	q	w	e	r	t	y	u	i	o	p	[]	
CAP	a	s	d	f	g	h	j	k	l	;	'		
Shift	z	x	c	v	b	n	m	,	.	/		↵	
Ctl	á	ü	`	\							↓	↑	↔

Re-authenticate 3

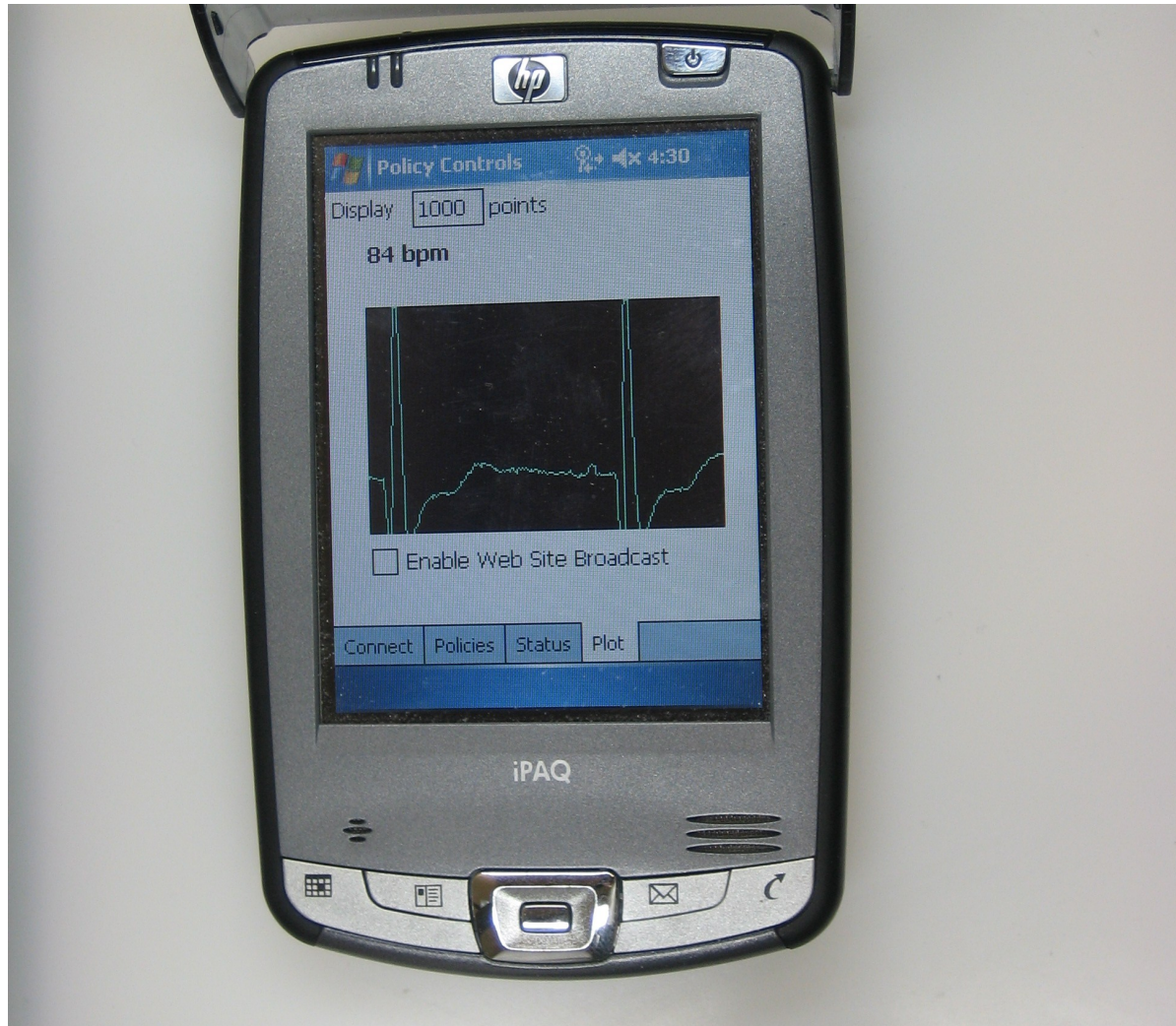
Patch Simulator

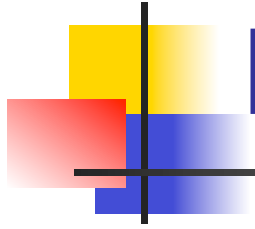
- Simulates the heart beat data in a repeatable way for development and debugging





PDA or Laptop Display

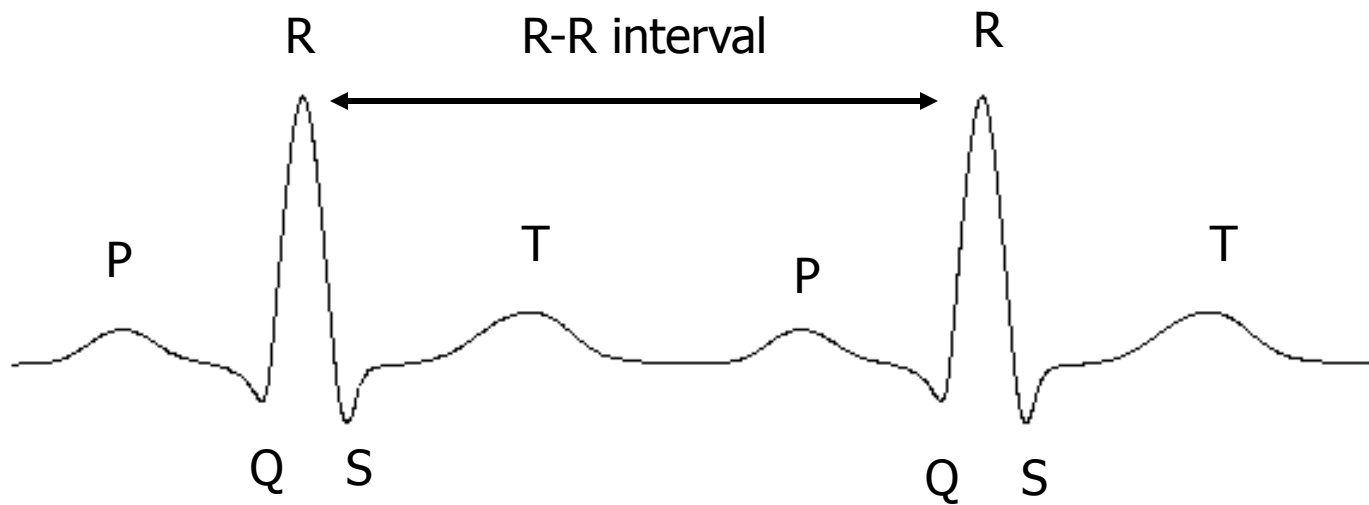


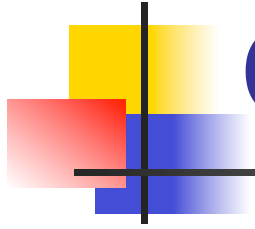


ECG Characterization

- Heart rate paced by the sino-atrial node
- Blood from body -> right atrium -> right ventricle -> lungs -> left atrium -> left ventricle -> body
- P wave represents atrial depolarization
- QRS complex represents ventricular depolarization
- T wave represents ventricular repolarization
- Rest period between beats

ECG Characterization





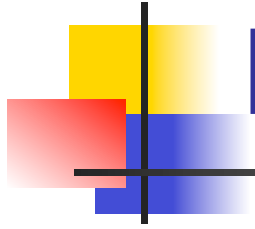
Can We Detect Heartbeats?

- From the raw data (voltages), use software to detect the QRS complex
- From the QRS complex, extract the R-R interval
- This is a challenge in the face of analog-to-digital converters, sampling error, noise, sensor placement, differences among people, body motion, heart acceleration...

Movie

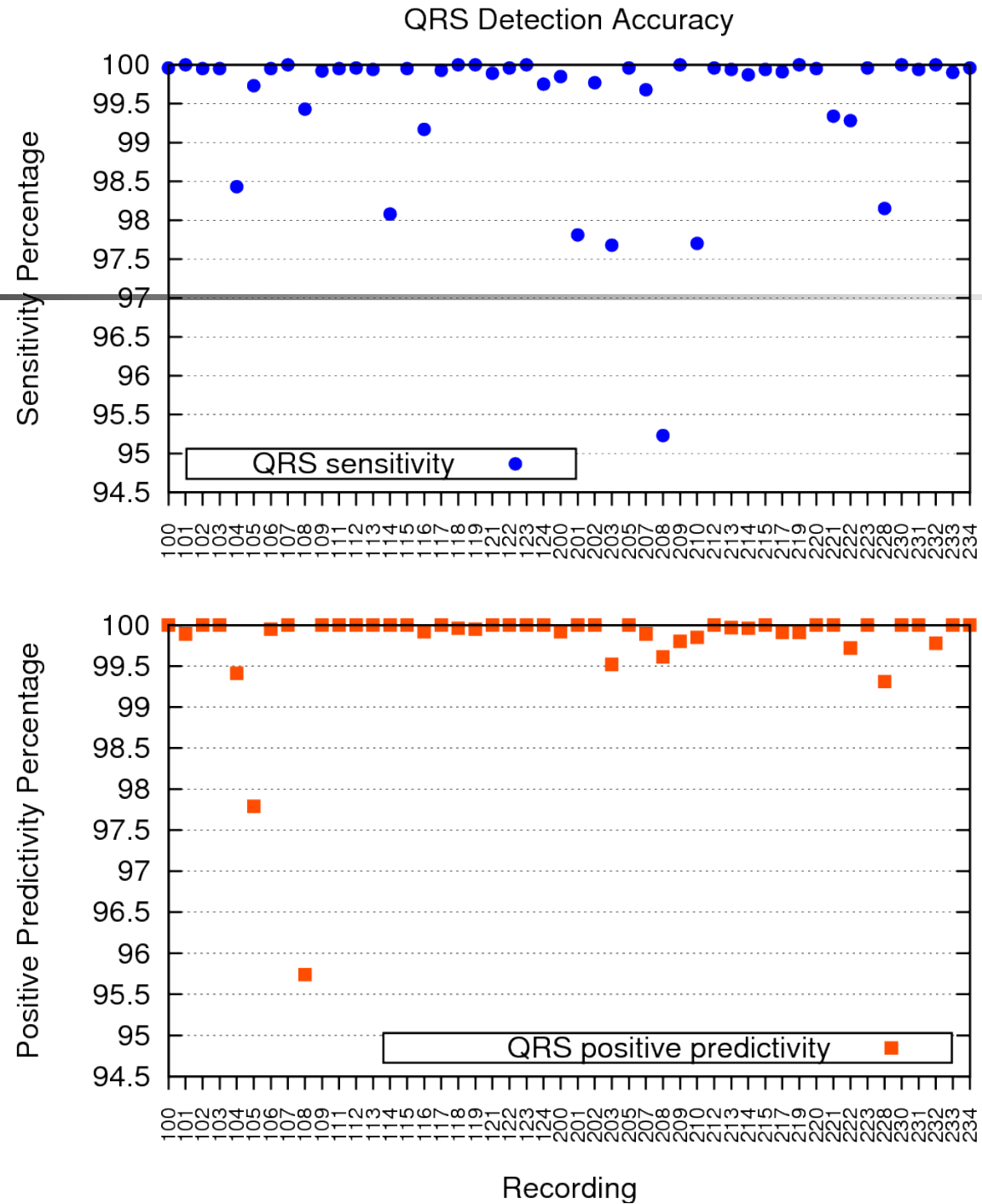
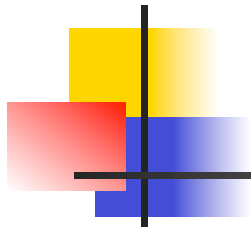
The image shows two overlapping windows from a software application. The background window is titled "Patch Simulator" and features a "Bluetooth" dropdown menu with a value of "0". Below this, the "Service Name" is set to "HeartbeatService0". A red button labeled "De-advertise Service" is visible. A status message at the bottom left says "Service is available." To the right, a "Current Data: ###" section contains a horizontal slider ranging from 0 to 200, with a "Transmission Period" of 1 seconds. At the bottom of this section are "Load File" and "Start" buttons. A yellow "Add Sensor" button is located to the right of the "Current Data" section.

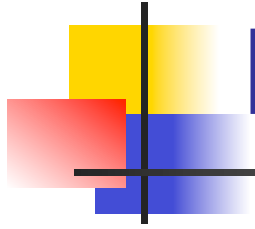
The foreground window is titled "WM_adj3t1" and has a menu bar with "File", "Zoom", "Tools", and "Help". It also features a "Bluetooth" dropdown menu with a value of "0". Below this is a table with two columns: "Device" and "Service". The "Device" column lists "weaver-0", "ALF-X60", and "GOLD". The "Service" column is empty. Below the table are "Discover" and "Reset" buttons. A status message reads "Device discovery complete: click on a device." At the bottom, there are two checkboxes: "Enable Web Site Broadcast" and "Enable Waveform Logging", both of which are unchecked. The window has a blue title bar and a standard Windows-style interface.



ECG Characterization

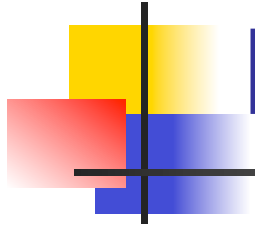
- Evaluated software against an annotated database of 48 half-hour recordings in the MIT-BIH Arrhythmia Database
- Sensitivity (percentage of QRS complexes correctly identified) $> 99.5\%$
- Positive predictability (probability that a QRS detection is correct) $> 99.7\%$





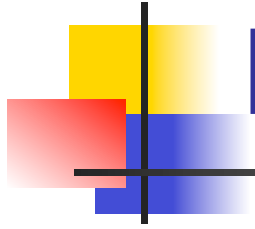
Research Issues

- Sub-threshold logic design
- Additional sensors (temperature, respiration, accelerometer)
- Tradeoffs between continuous vs. periodic communication
- Handling foreseeable events (battery change, out of range)



Research Issues

- Expanding the types of mobile devices (laptops, cell phone, special gear)
- Signal processing on the mobile device
- Exporting the signal (raw or processed) to the Internet for remote monitoring
- Does ECG signal contain enough information for personal authentication?



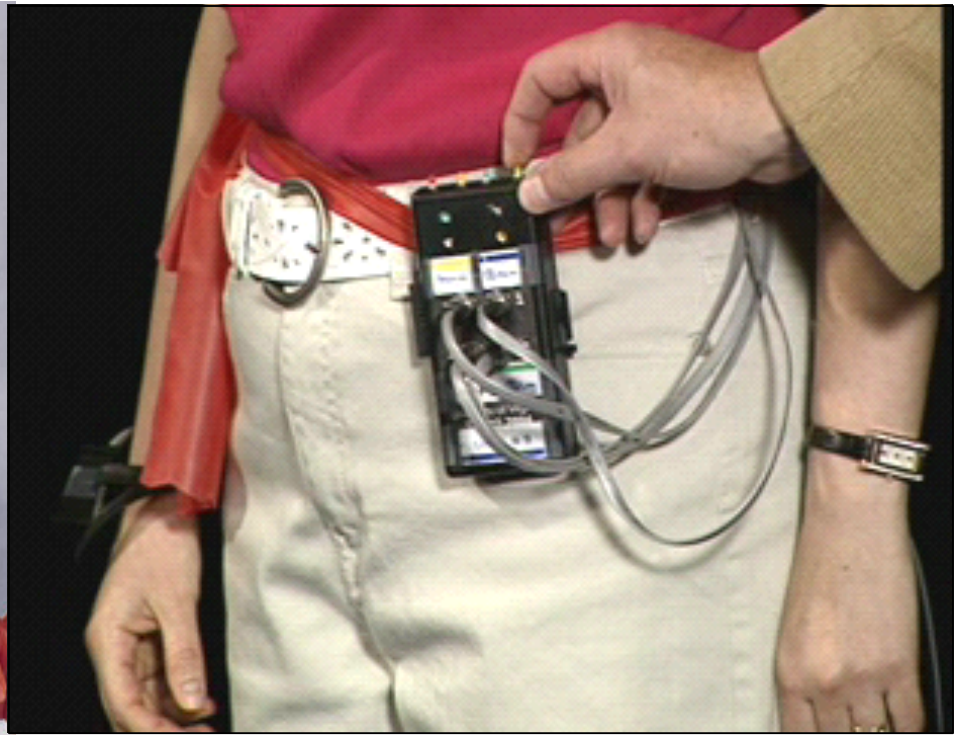
Research Issues

- Multiple sensors per person, multiple people being monitored simultaneously
- Energy scavenging
- Algorithms for QRS and R-R detection
- “Eye-in-the-sky” view of individuals and groups
- Signal exfiltration

Signal Exfiltration



Infant monitoring



Gait Analysis