Endpoint Security for Mobile Devices

2012 NIST/OCR HIPAA Security Rule Conference
June 6, 2012

David Shepherd, CISSP
www.LMI.org
dshepherd@lmi.org

LMI

Disclaimer

- *"The information contained in this presentation is neither an endorsement of any product nor criticism. Nor does it constitute legal advice. The information provided is the result of independent research funded by the Office of the National Coordinator for Health Information Technology. Users of this information are encouraged to seek the advice of legal counsel in order to comply with various laws and regulations."*

Agenda

- Introduction – Project Description
- Establishment of Test Bed
  - HITEST lab description
  - Devices
- Testing
  - Requirements matrix
  - Test scripts
  - Findings
- Anomalies
- Sample Lockdown Procedures

Introduction – Project Description

- Initiative from HIT Cyber Working Group
  - Examine practical methods for improving security of health IT
  - Reduce security burden on end user
- Providers and patients must be confident that the electronic health IT products and systems they use are secure
- Several barriers to successful adoption of end user security measures
  - Lack of usability
  - High complexity
  - Misinformation
  - User awareness

Introduction – Project Description

- Project Goal
  - Develop and pilot test one or more methods of end to end automated security in healthcare settings
    - Identify and test practical steps to improve the security of PHI
    - Increase Electronic Health Record (EHR) adoption
    - Remove a significant barrier to the success of EHR

Introduction – Project Objectives

- ONC project objectives
  - Remove security as a barrier to EHR adoption
  - Identify methods to improve security of EHR products
  - Examine the impact of diverse configurations in the HIT ecosystem
  - Ensure that securing PHI is transparent to end users
  - Gather information about how EHR products can improve security
  - Leverage the investment in EHR security research across agencies and departments

Introduction - Stakeholders

- Primary stakeholders
  - HHS Office of the Chief Privacy Officer
  - HHS Office of Civil Rights
  - Health Information Technology Research Center
  - National Institute of Standards and Technology
  - EHR Vendors

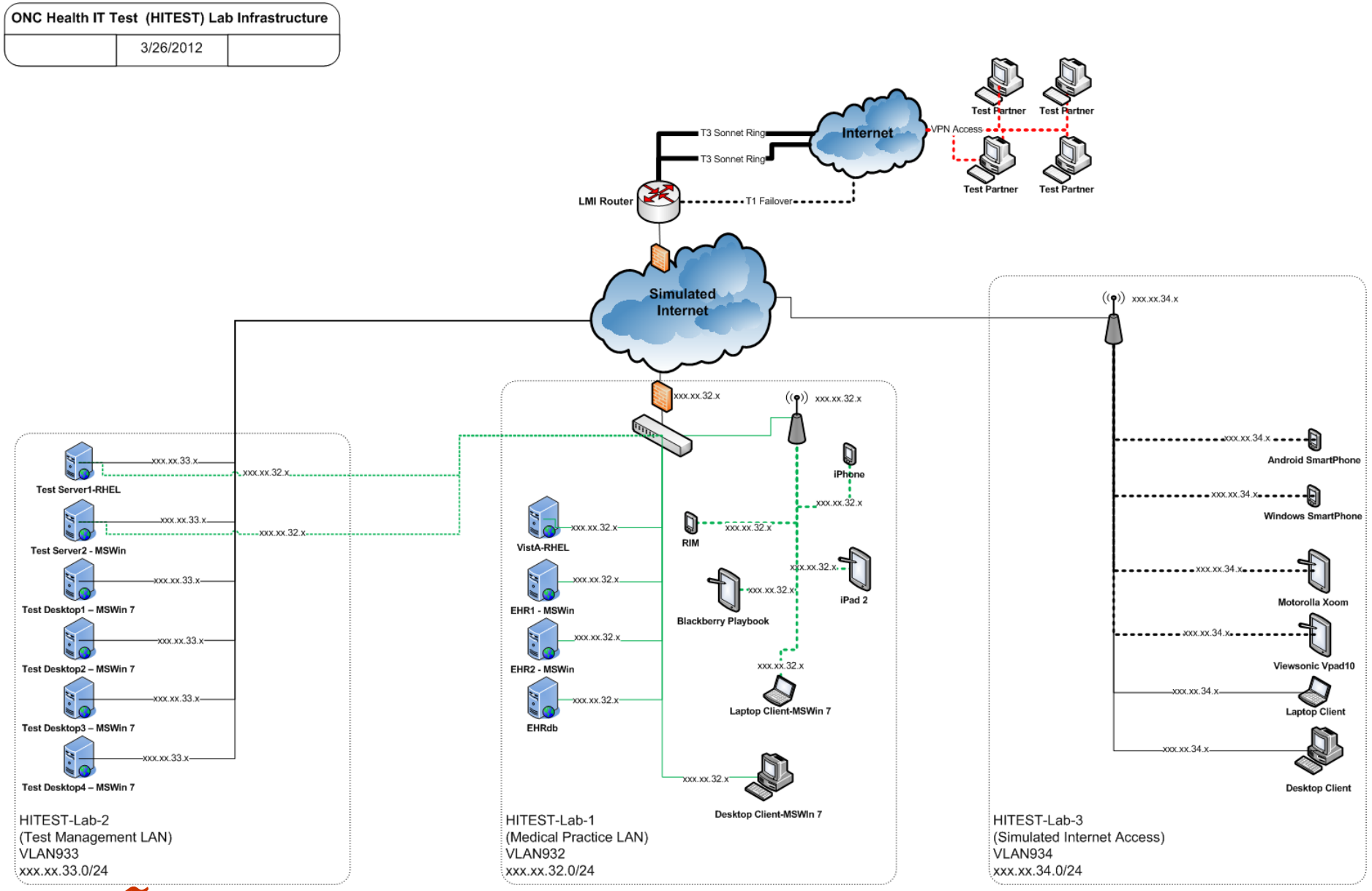
Phased Approach to Project

- Phase 1: Research and Establish Test Bed
- Phase 2: Test and Evaluation
- Phase 3: Reporting

HITEST Lab Design

- Provide maximum flexibility
  - Test software and technologies for effective security functionality in an isolated and scalable HIT ecosystem that simulates various EHR environments
  - Realistically model the chain of HIT events and simulate multiple real-world operating environments, including
    - Physician offices
    - Hospital nursing stations
    - Emergency departments
  - Contains all the elements necessary to manage and execute tests of information security at the endpoints of HIT systems
  - Enables accurate and efficient results reporting

HITEST Lab Build



HITEST Lab Devices

SmartPhones

Worldwide Mobile Communications Device (Phones) Sales to End Users by OS (Market Share)				
OS	**2010**	**2011**	**2012**	**2015**
Symbian	37.6	19.2	5.2	0.1
Android - Various Phones	22.7	38.5	49.2	48.8
RIM - Blackberry	16	13.4	12.6	11.1
iOS - Apple iPhone	15.7	19.4	18.9	17.2
Microsoft - Windows Phone	4.2	5.6	10.8	19.5
Other Operating Systems	3.8	3.9	3.4	3.3
Source: Gartner (April 2011)				

Gartner. (2011, April 7). *Gartner Says Android to Command Nearly Half of Worldwide Smartphone Operating System Market by Year-End 2012*. Retrieved November 2011, from www.gartner.com: http://www.gartner.com/it/page.jsp?id=1622614

HITEST Lab Devices

Smartphone devices:

Device	Operating System	Version
Apple iPhone 4	iOS	4.3.5 & 5.0.1
HTC Vivid	Android 2.3.4	HTC Sense 3.0
Blackberry Curve	OS 6.0 Bundle 2949	6.0.0.668
HTC T9295 Windows Phone	Windows Phone 7.5 OS	7.10.7720.68

LMI

HITEST Lab Devices

Tablets

Worldwide Sales of Media Tablets to End Users by OS (Market Share)				
OS	**2010**	**2011**	**2012**	**2015**
iOS - Apple iPad	83.9	68.7	63.5	47.1
Android - Various tablets	14.2	19.9	24.4	38.6
WebOS - HP TouchPad	0	4	3.9	3
QNX - RIM PlayBook	0	5.6	6.6	10
Other Operating Systems	1.3	0.6	0.5	0.2
Source: Gartner (April 2011)				

Gartner. (2011, April 11). *Gartner Says Apple iOS to Dominate the Media Tablet Market Through 2015, Owning More Than Half of It for the Next Three Years*. Retrieved November 2011, from www.gartner.com: http://www.gartner.com/it/page.jsp?id=1626414

HITEST Lab Devices

Tablet devices:

Device	Operating System	Version
iPad 2	iOS	4.3.5 & 5.0.1
Motorola XOOM	Android Honeycomb	3.2.1
Viewsonic Viewpad	Microsoft OS	Windows 7 Professional
Viewsonic Viewpad	Android 2.2	1.4
Blackberry Playbook	QNX Software	1.0.8.6067
HP Touchpad	HP webOS	3.0.5
Samsung Galaxy Tab	Android OS	2.2






LMI

HITEST Lab Devices

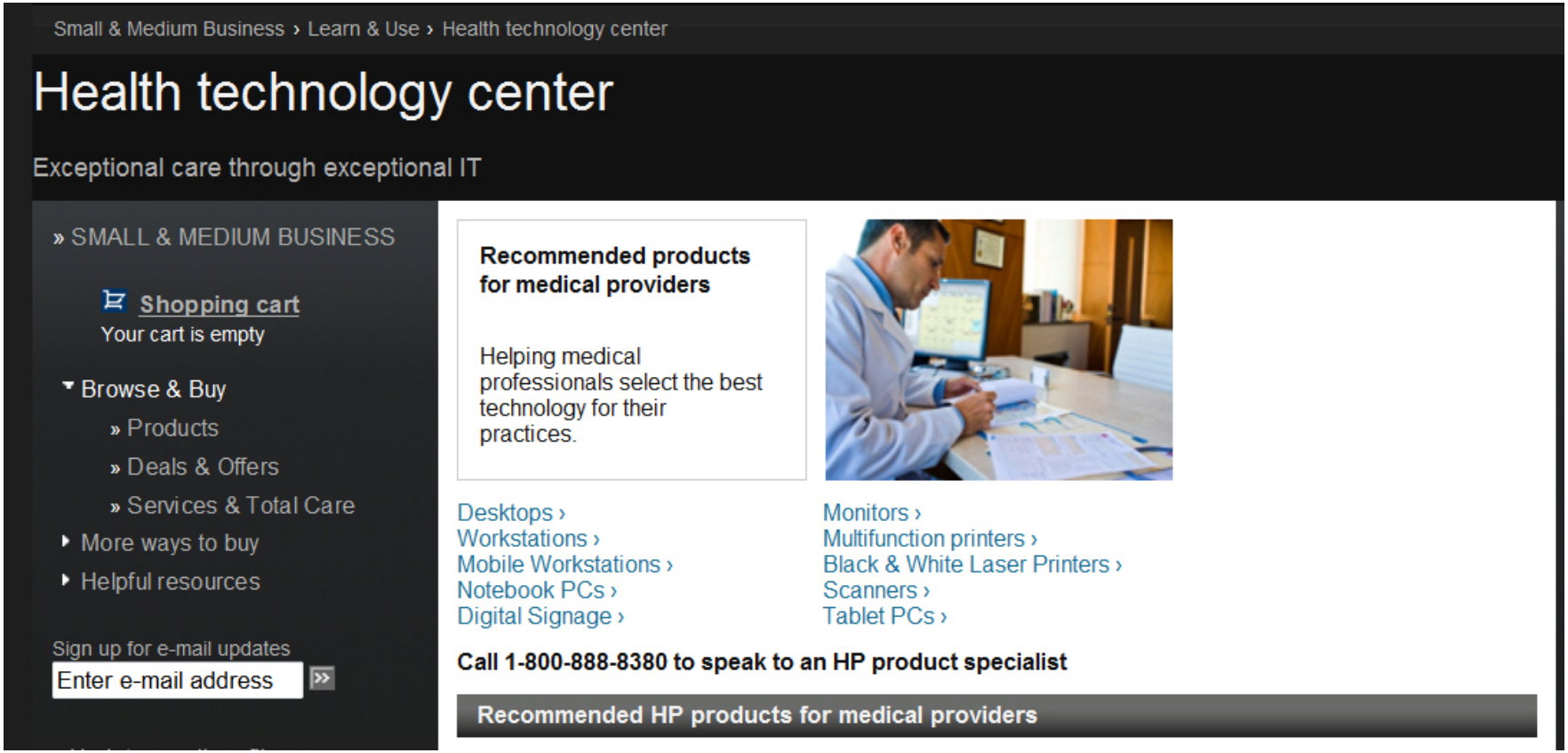
PC/Laptops

United States PC Vendor Unit Shipment Estimates for 2Q11 (Units)				
Company	**2Q11 Shipments**	**2Q11 Market Share (%)**	**2Q10 Shipments**	**2Q10 Market Share (%)**
HP	4,552,777	26.9	4,608,280	25.7
Dell	3,821,759	22.6	4,236,303	23.6
Apple	1,814,000	10.7	1,671,500	9.3
Toshiba	1,616,400	9.6	1,565,000	8.7
Acer	1,570,257	9.3	2,028,284	11.3
Others	3,539,666	20.9	3,803,974	21.2
Total	**16,914,859**	**100**	**17,913,341**	**100**
Source: Gartner (July 2011)				

Gartner. (2011, July 13). *Gartner Says Worldwide PC Shipments Increased 2.3 Percent in Second Quarter of 2011* . Retrieved November 2011, from www.gartner.com: http://www.gartner.com/it/page.jsp?id=1744216

HITEST Lab Devices

PC/Laptops recommended by HP's Technology Center



http://www.hp.com/sbso/solutions/healthcare/bestsellers.html

LMI

HITEST Lab Devices

Other endpoint devices:

Device	Operating System
HP Probook 6565b Laptop	Windows 7 Professional (64bit)
HP 505b MicroTower Desktop	Windows 7 Professional (32bit)

LMI

Testing – RTM Development

- Security Requirements Traceability Matrix (RTM)
- Basis of the RTM
  - HIPAA Security Rule (Technical Safeguards)
  - NIST Special Pub 800-53 Revision 3
    - Recommended Security Controls for Federal Information Systems and Organizations
  - NIST Special Pub 800-66 Revision 1
    - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
  - Center for Internet Security (CIS) security configuration benchmark guides

RTM Categories

Category	Subcategory
Access Control (§ 164.312 (a))	Password Policy and Authentication
	Connectivity (VPN, Network)
	Session Security
	Endpoint Protection
Audit Controls (§ 164.312 (b))	Auditing
	Maintenance, Patching, and Administration
Integrity (§ 164.312 (c))	Maintenance, Patching, and Administration
	Endpoint Protection
Person or Entity Authentication (§ 164.312 (d))	Password Policy and Authentication
Transmission Security (§ 164.312 (e))	Connectivity (VPN, Network)

RTM Example

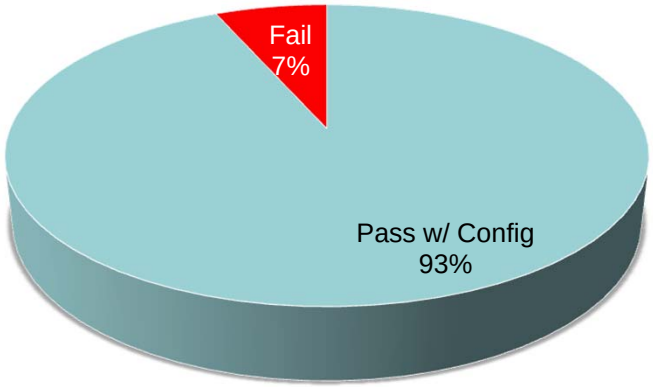
Requirement no.	Requirement description	Standards mappings	Expected test results
Password Policy and Authentication			
AC-1	Secure PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g. password access) when not in use.	HIPAA §164.312(a) NIST SP800-53 AC-11	When not in use (i.e. the device is locked), the device requires the user to authenticate to unlock.
AC-2	Limit the number of unsuccessful log-on attempts allowed to six (6) attempts	HIPAA §164.312(a)	The device limits the number of unsuccessful log-on attempts to six (6)
AC-3	Force a time delay of 30 minutes before further log-on attempts are allowed or rejecting any further attempts without specific authorization	HIPAA §164.312(a)	After six (6) unsuccessful log-on attempts, the device forces a time delay of 30 minutes before further log-on attempts are allowed.
Connectivity			
AC-4	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	HIPAA §164.312(a) NIST 800-53 AC-18	The device is configurable to disable Wi-Fi networking. This can be achieved through a Airport mode (disabling all wireless networking) or a Wi-Fi disable setting.
Session Security			
AC-5	A time-out system (e.g. a screen saver) shall pause the session screen after 2 minutes of inactivity	HIPAA §164.312(a)	The device automatically locks after 2 minutes of inactivity

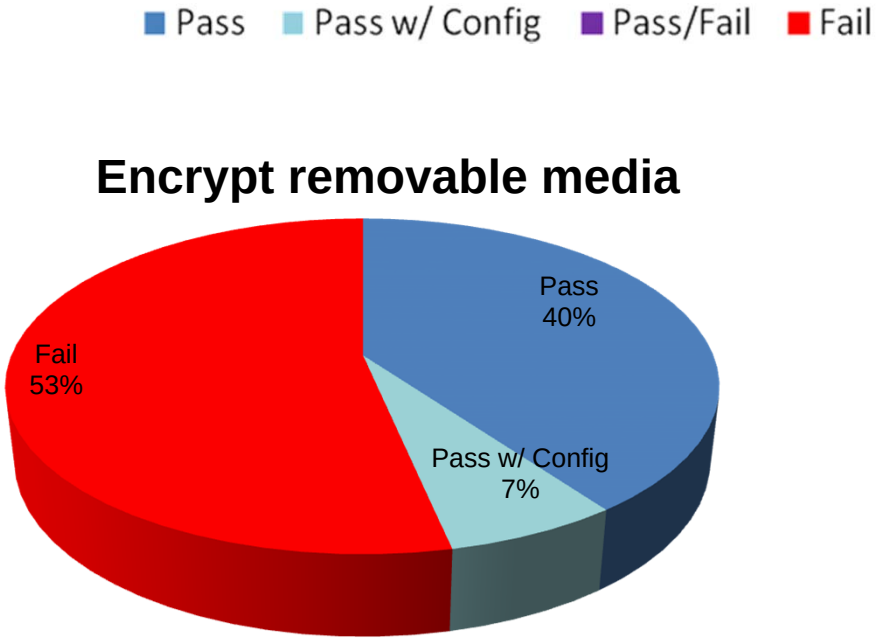
LMI

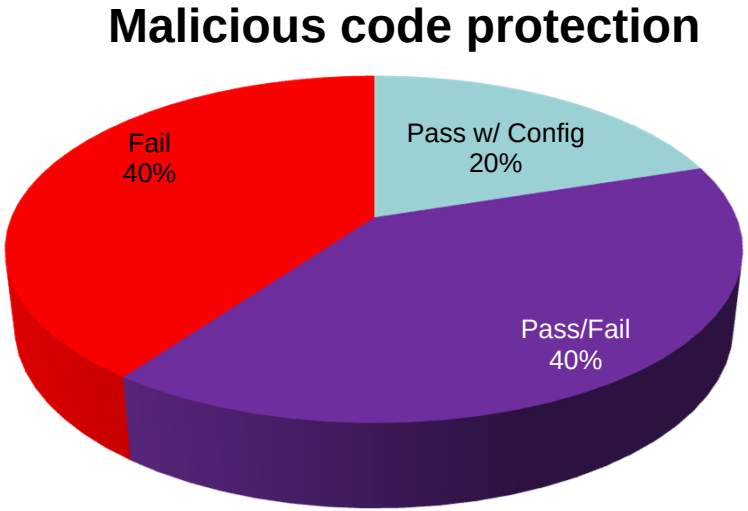
Testing

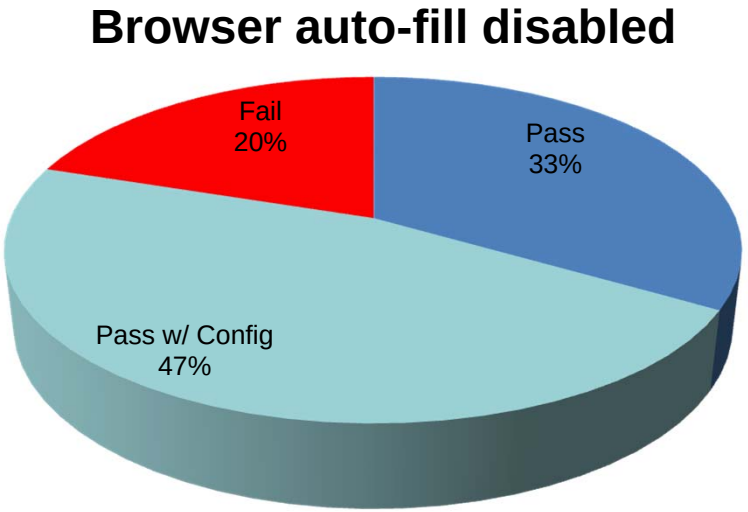
- Development of Test Scripts
- Application of Test Scripts to devices
- Refinement of RTM and Results categories based on actual testing

Findings – Highlights





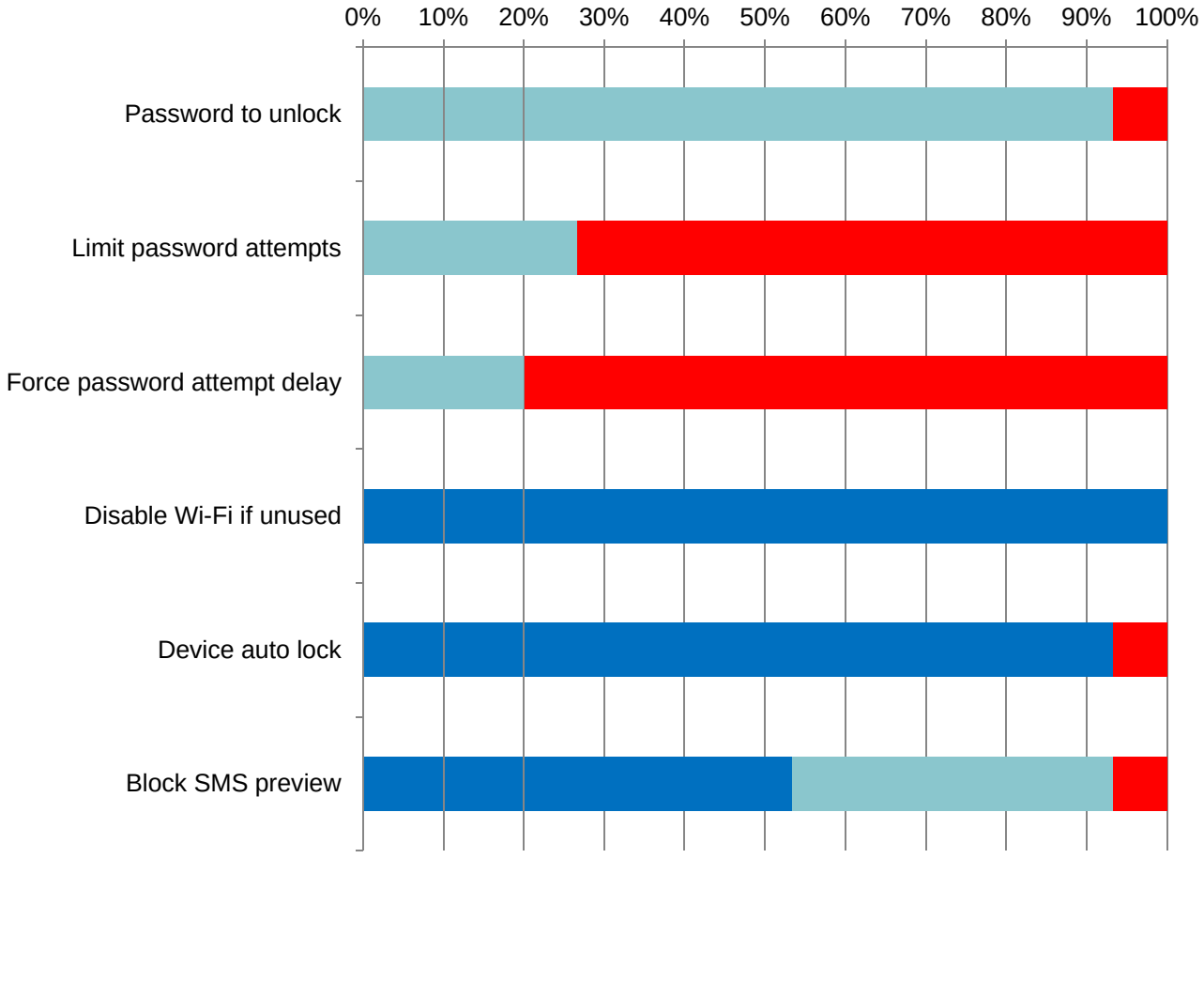




LMI

Findings

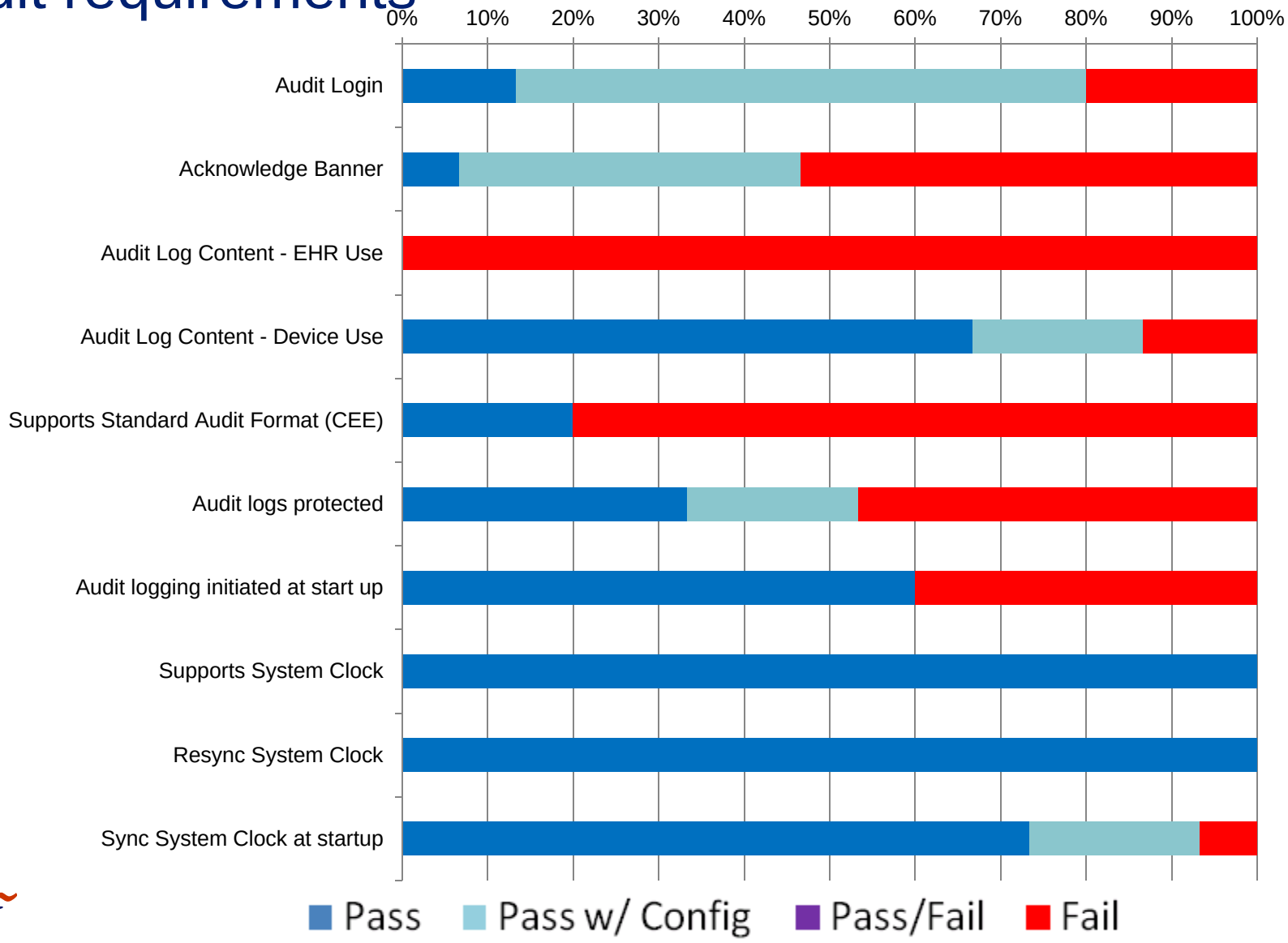
- Access requirements



LMI

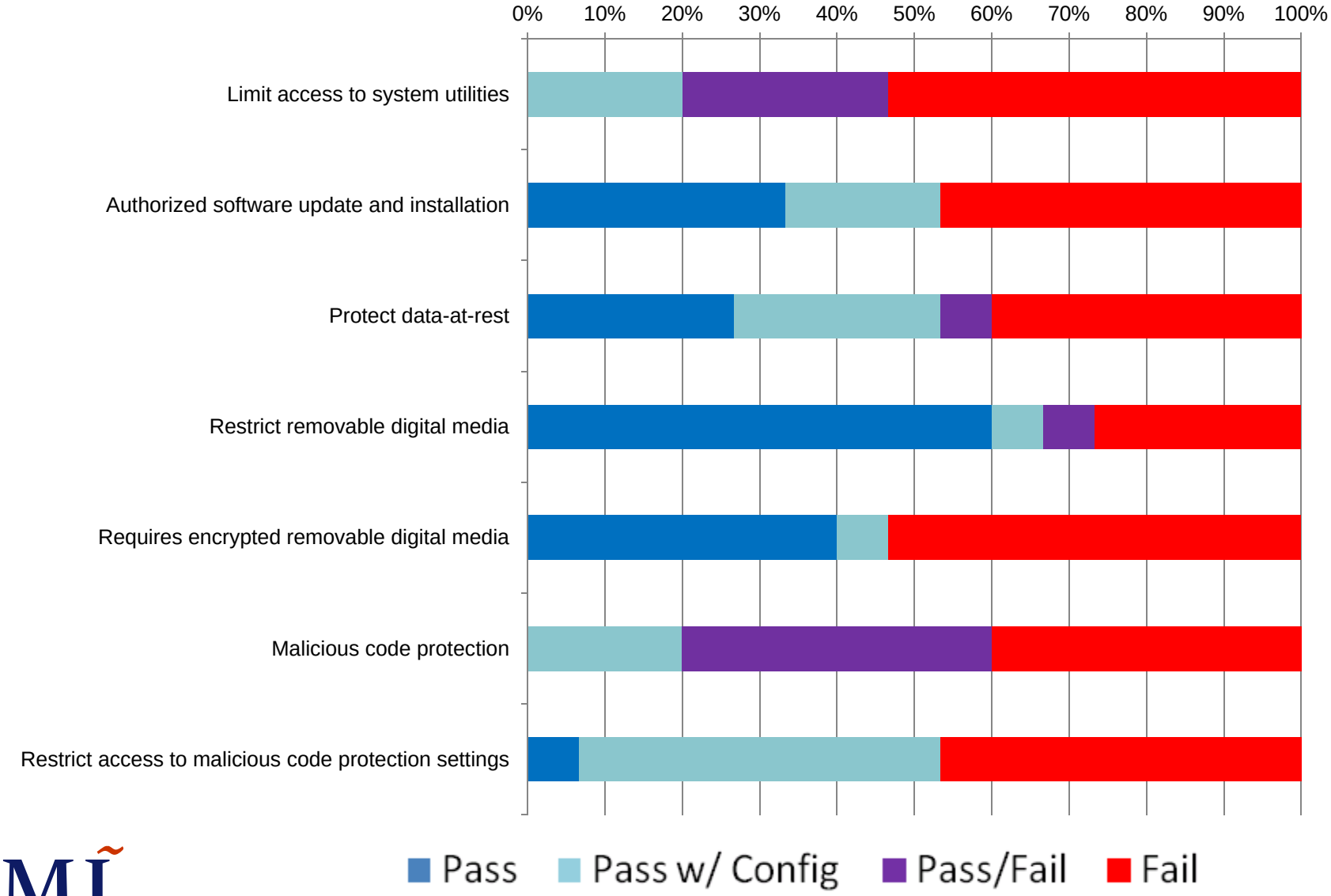
Findings

- Audit requirements



Findings

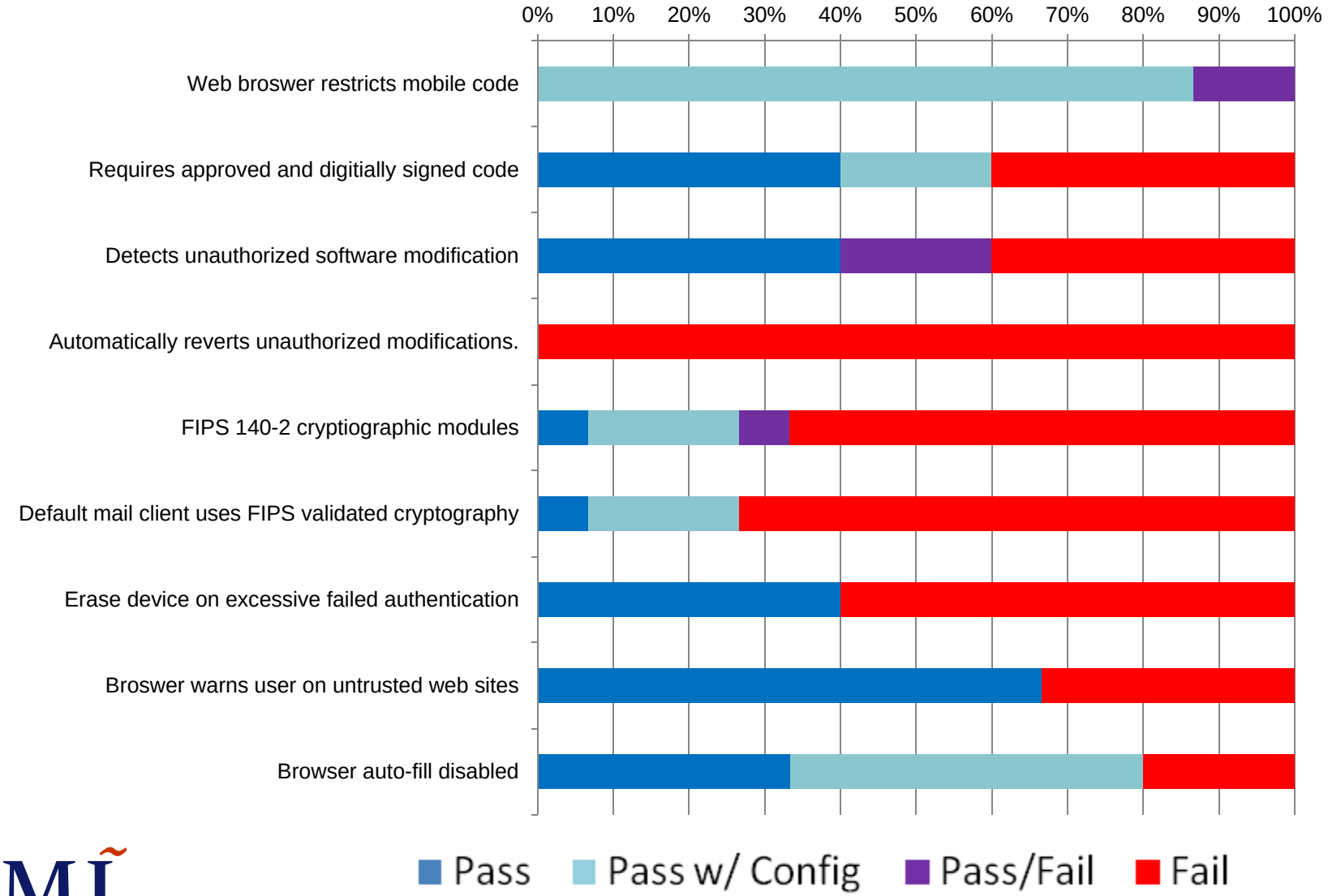
- Integrity requirements – Part 1



LMI

Findings

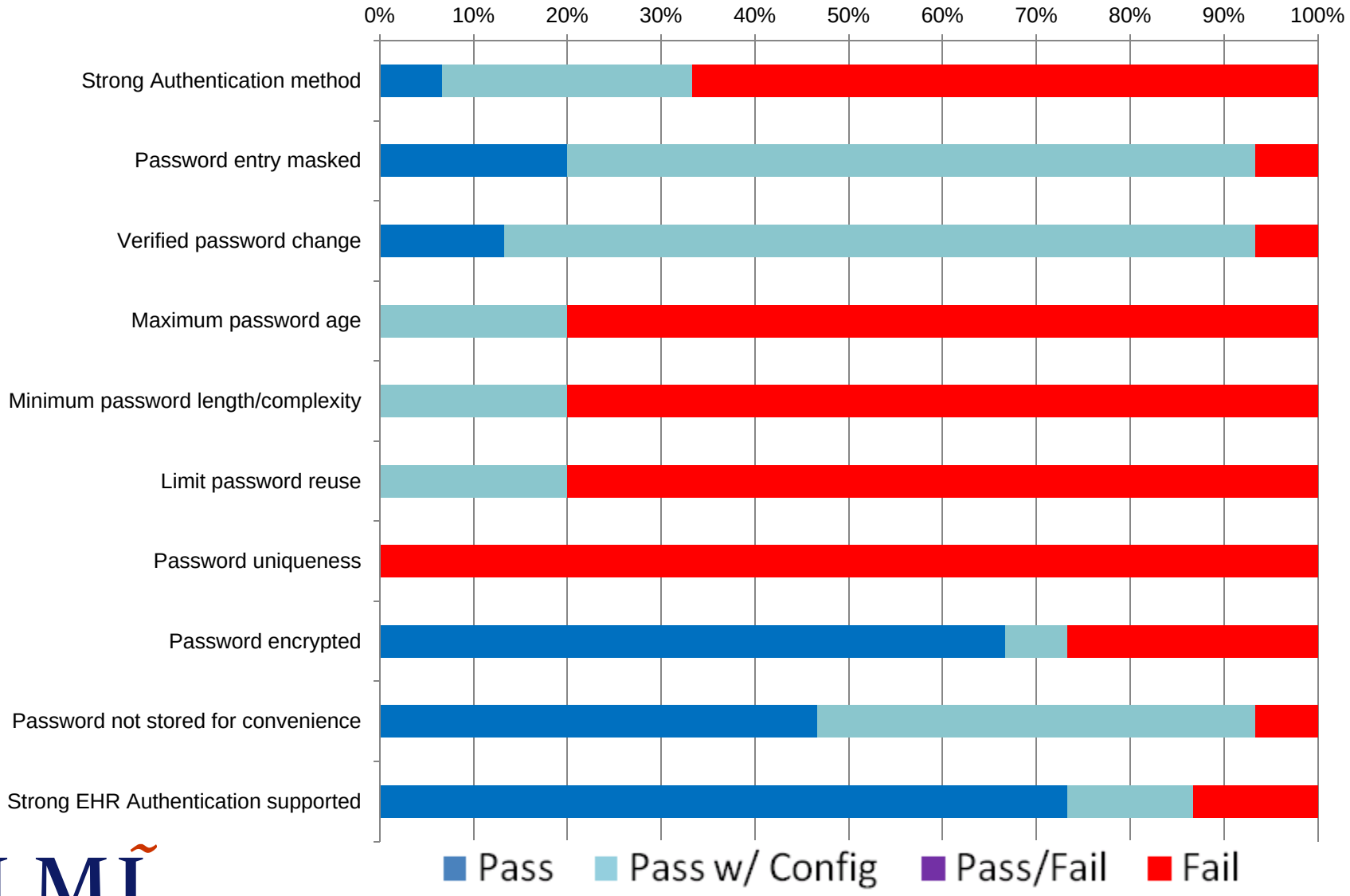
- Integrity requirements – Part 2



LMI

Findings

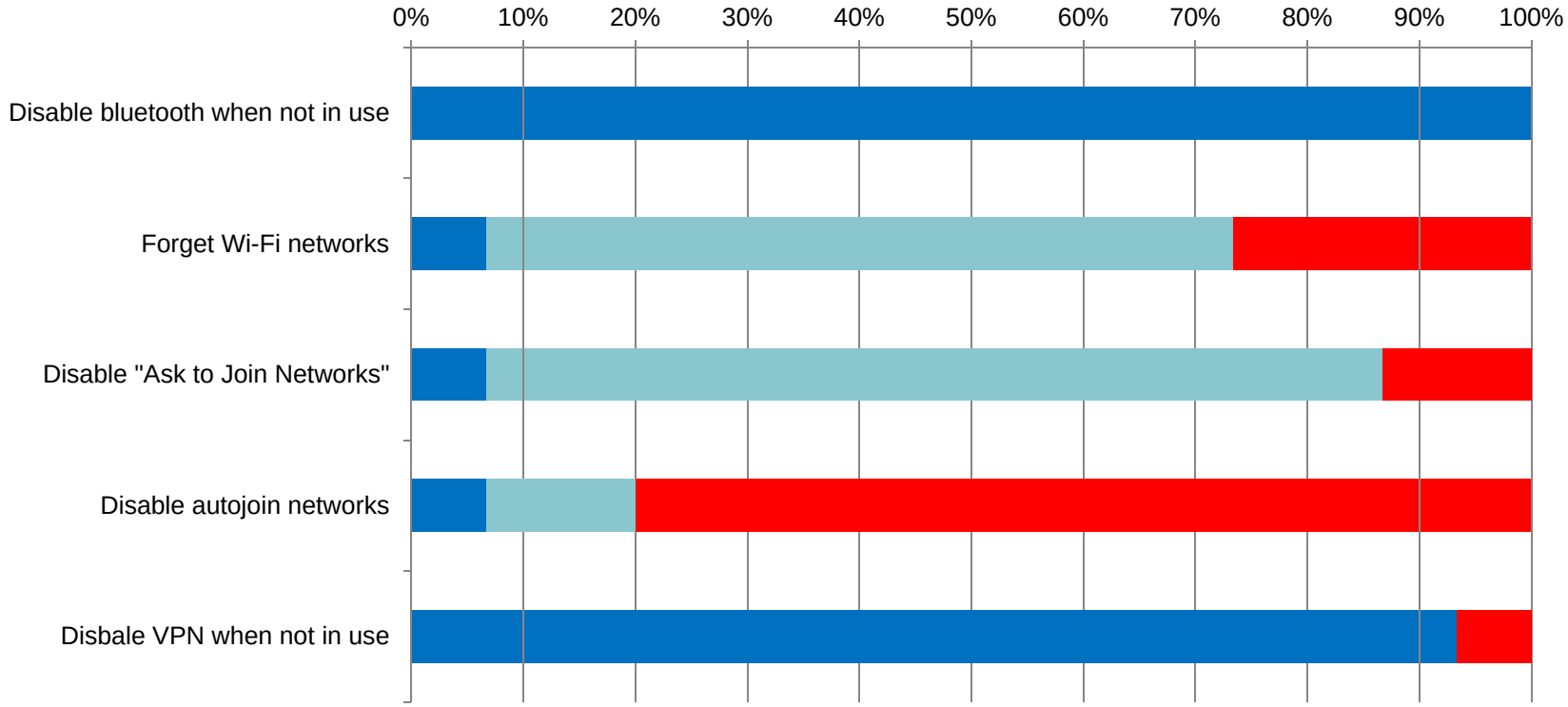
- Authentication Controls



LMI

Findings

- Transmission requirements



Heat Map Method

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail	Fail	Pass
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass	Fail	Fail
Pass	Fail	Pass	Fail	Pass
Pass w/ Config	Pass	Pass/Fail	Fail	
	Fail	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass	Pass	
	Pass	Pass	Pass	
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

21
9
2
15

LMI

Access Results

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config				
Fail				
Fail				
Pass				
Pass				
Pass w/ Config				

2
2
0
2

Access	
Pass w/ Config	Password to unlock
Fail	Limit password attempts
Fail	Force password attempt delay
Pass	Disable Wi-Fi if unused
Pass	Device auto lock
Pass w/ Config	Block SMS preview

LMI

Audit Results

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config			
Fail	Fail			
Fail	Fail			
Pass	Pass			
Pass	Fail			
Pass w/ Config	Pass			
	Fail			
	Pass			
	Pass			
	Pass			

7
3
0
6

Audit	
Pass w/ Config	Audit Login
Fail	Acknowledge Banner
Fail	Audit Log Content - EHR Use
Pass	Audit Log Content - Device Use
Fail	Supports Standard Audit Format (CEE)
Pass	Audit logs protected
Fail	Audit logging initiated at start up
Pass	Supports System Clock
Pass	Resync System Clock
Pass	Sync System Clock at startup

LMI

Integrity Results

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail		
Fail	Fail	Pass		
Fail	Fail	Pass		
Pass	Pass	Pass		
Pass	Fail	Pass		
Pass w/ Config	Pass	Pass/Fail		
	Fail	Pass w/ Config		
	Pass	Pass w/ Config		
	Pass	Pass		
	Pass	Pass		
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

16
5
2
5

Integrity	
Pass/Fail	Limit access to system utilities
Pass	Authorized software update and installation
Pass	Protect data-at-rest
Pass	Restrict removable digital media
Pass	Requires encrypted removable digital media
Pass/Fail	Malicious code protection
Pass w/ Config	Restrict access to malicious code protection settings
Pass w/ Config	Web broswer restricts mobile code
Pass	Requires approved and digitially signed code
Pass	Detects unauthorized software modification
Fail	Automatically reverts unauthorized modifications.
Fail	FIPS 140-2 cryptiographic modules
Fail	Default mail client uses FIPS validated cryptography
Pass	Erase device on excessive failed authentication
Pass	Broswer warns user on untrusted web sites
Pass	Browser auto-fill disabled

LMI

Authentication Results

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail	Fail	
Fail	Fail	Pass	Pass w/ Config	
Fail	Fail	Pass	Pass w/ Config	
Pass	Pass	Pass	Fail	
Pass	Fail	Pass	Fail	
Pass w/ Config	Pass	Pass/Fail	Fail	
	Fail	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass	Pass	
	Pass	Pass	Pass	
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

19
7
2
14

Authentication	
Fail	Strong Authentication method
Pass w/ Config	Password entry masked
Pass w/ Config	Verified password change
Fail	Maximum password age
Fail	Minimum password length/complexity
Fail	Limit password reuse
Fail	Password uniqueness
Pass	Password encrypted
Pass	Password not stored for convenience
Pass	Strong EHR Authentication supported

LMI

Transmission Results

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail	Fail	Pass
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass	Fail	Fail
Pass	Fail	Pass	Fail	Pass
Pass w/ Config	Pass	Pass/Fail	Fail	
	Fail	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass	Pass	
	Pass	Pass	Pass	
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

21
9
2
15

Transmission	
Pass	Disable bluetooth when not in use
Pass w/ Config	Forget Wi-Fi networks
Pass w/ Config	Disable "Ask to Join Networks"
Fail	Disable autojoin networks
Pass	Disbale VPN when not in use

LMI

Consolidated View

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail	Fail	Pass
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass	Fail	Fail
Pass	Fail	Pass	Fail	Pass
Pass w/ Config	Pass	Pass/Fail	Fail	
	Fail	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass	Pass	
	Pass	Pass	Pass	
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

21
9
2
15

LMI

Heat Maps – Phones – Default Configuration

Apple iPhone iOS 5				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail	Fail	Pass
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass	Fail	Fail
Pass	Fail	Pass	Fail	Pass
Pass w/ Config	Pass	Pass/Fail	Fail	
	Fail	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass	Pass	
	Pass	Pass	Pass	
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

21	
9	
2	
15	

HTC Vivid Android				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass	Fail	Fail	Pass
Fail	Pass w/ Config	Fail	Pass w/ Config	Pass w/ Config
Fail	Fail	Fail	Pass w/ Config	Pass w/ Config
Pass	Pass	Fail	Fail	Fail
Pass	Fail	Fail	Fail	Pass
Pass w/ Config	Fail	Fail	Fail	
	Pass	Fail	Fail	
	Pass	Pass w/ Config	Fail	
	Pass	Fail	Pass w/ Config	
	Pass	Fail	Pass	
		Fail		
		Fail		
		Fail		
		Fail		
		Pass		
		Pass w/ Config		

12	
10	
0	
25	

Blackberry Curve 9300				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass	Fail	Pass	Pass
Pass w/ Config	Pass	Fail	Pass w/ Config	Fail
Fail	Fail	Pass w/ Config	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass w/ Config	Fail	Fail
Pass	Fail	Pass w/ Config	Fail	Pass
Pass w/ Config	Fail	Fail	Fail	
	Pass	Fail	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Fail	Pass	
	Pass	Fail	Pass w/ Config	
		Fail		
		Pass w/ Config		
		Fail		
		Pass		
		Fail		
		Pass		

16	
12	
0	
19	

Windows Phone				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Fail	Fail	Fail	Pass
Fail	Pass w/ Config	Fail	Pass w/ Config	Fail
Fail	Fail	Fail	Pass w/ Config	Fail
Pass	Fail	Pass/Fail	Fail	Fail
Pass	Fail	Pass	Fail	Fail
Fail	Fail	Pass/Fail	Fail	
	Fail	Pass	Fail	
	Pass	Pass/Fail	Pass	
	Pass	Pass	Fail	
	Pass	Pass	Fail	
		Fail		
		Fail		
		Fail		
		Fail		
		Fail		
		Fail		

11	
4	
3	
29	

LMI

Pass Pass w/ Config Pass/Fail Fail

Heat Maps – Phones – After Configuration

Apple iPhone iOS 5

Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass/Fail	Fail	Pass
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Fail	Fail	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass	Fail	Fail
Pass	Fail	Pass	Fail	Pass
Pass w/ Config	Pass	Pass/Fail	Fail	
	Fail	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass	Pass	
	Pass	Pass	Pass	
		Fail		
		Fail		
		Fail		
		Pass		
		Pass		
		Pass		

21	
9	
2	
15	

HTC Vivid Android

Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass	Fail	Fail	Pass
Fail	Pass w/ Config	Fail	Pass w/ Config	Pass w/ Config
Fail	Fail	Fail	Pass w/ Config	Pass w/ Config
Pass	Pass	Fail	Fail	Fail
Pass	Fail	Fail	Fail	Pass
Pass w/ Config	Fail	Fail	Fail	
	Pass	Fail	Fail	
	Pass	Pass w/ Config	Fail	
	Pass	Fail	Pass w/ Config	
	Pass	Fail	Pass	
		Fail		
		Fail		
		Fail		
		Fail		
		Pass		
		Pass w/ Config		

12	
10	
0	
25	

Blackberry Curve 9300

Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass	Fail	Pass	Pass
Pass w/ Config	Pass	Fail	Pass w/ Config	Fail
Fail	Fail	Pass w/ Config	Pass w/ Config	Pass w/ Config
Pass	Pass	Pass w/ Config	Fail	Fail
Pass	Fail	Pass w/ Config	Fail	Pass
Pass w/ Config	Fail	Fail	Fail	
	Pass	Fail	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Fail	Pass	
	Pass	Fail	Pass w/ Config	
		Fail		
		Pass w/ Config		
		Fail		
		Pass		
		Fail		
		Pass		

16	
12	
0	
19	

Windows Phone

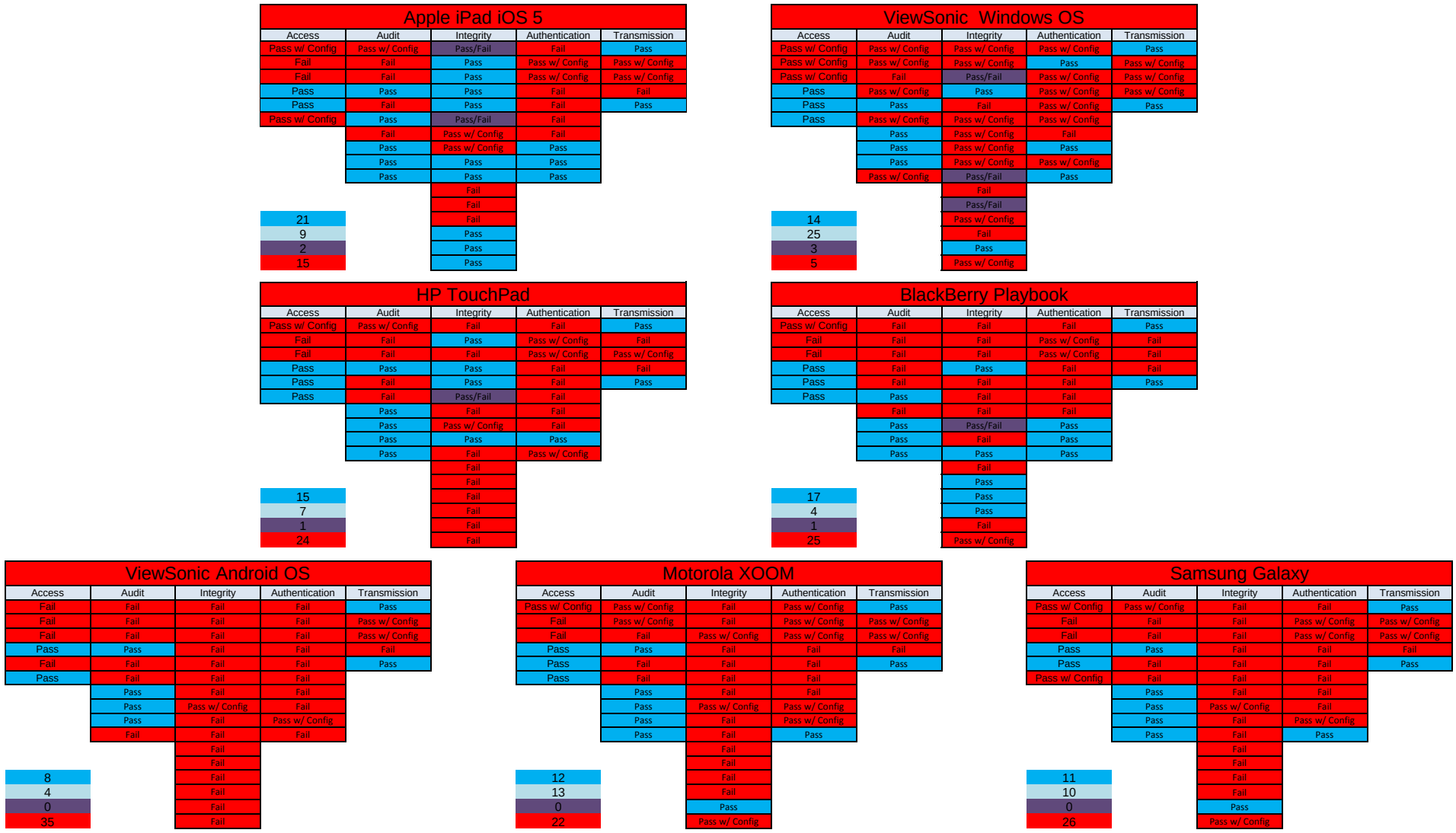
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Fail	Fail	Fail	Pass
Fail	Pass w/ Config	Fail	Pass w/ Config	Fail
Fail	Fail	Fail	Pass w/ Config	Fail
Pass	Fail	Pass/Fail	Fail	Fail
Pass	Fail	Pass	Fail	Fail
Fail	Fail	Pass/Fail	Fail	
	Fail	Pass	Fail	
	Pass	Pass/Fail	Pass	
	Pass	Pass	Fail	
	Pass	Pass	Fail	
		Fail		
		Fail		
		Fail		
		Fail		
		Fail		
		Fail		

11	
4	
3	
29	

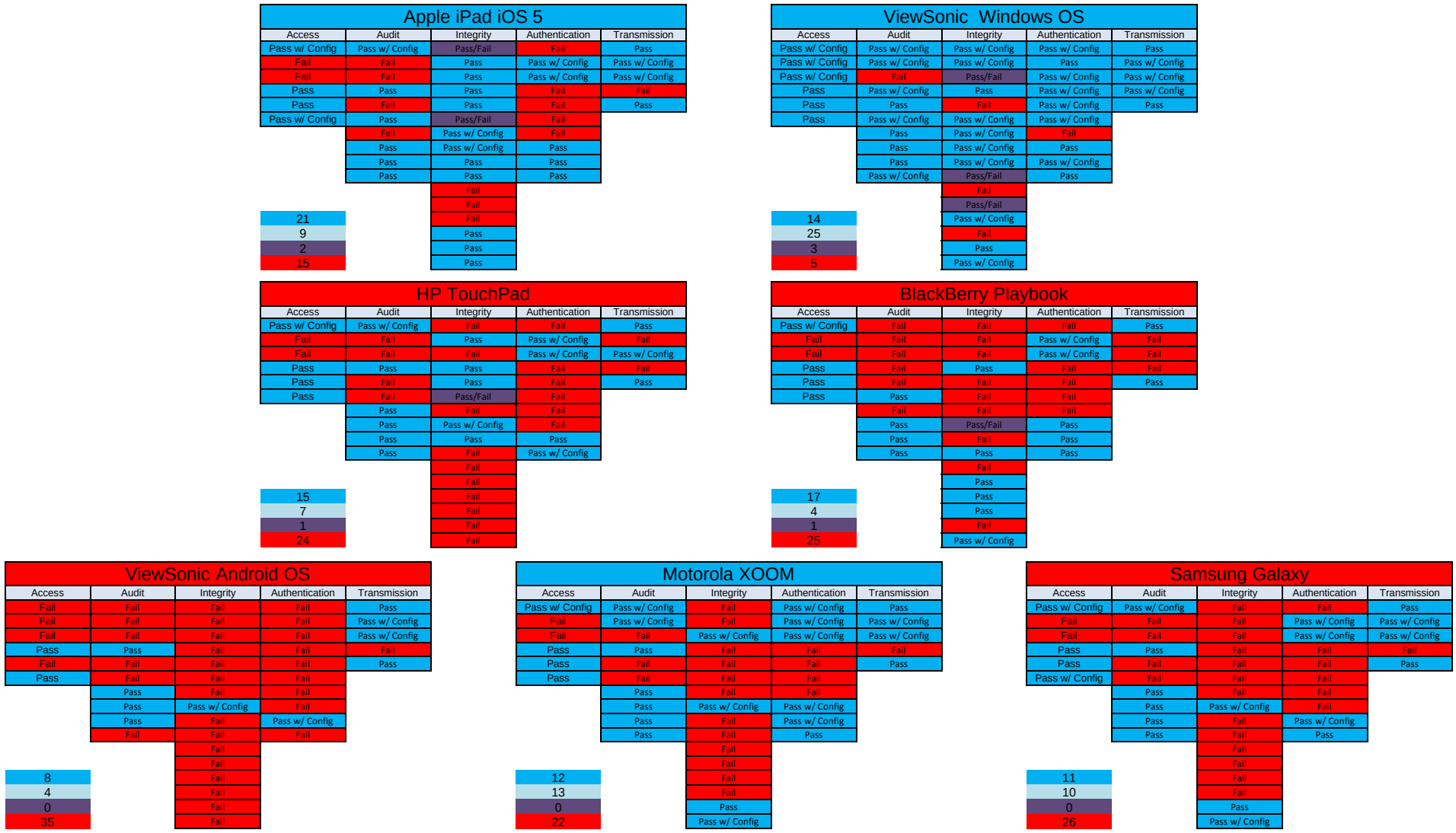
LMI

Pass Pass w/ Config Pass/Fail Fail

Heat Maps - Tablets – Default Configuration



Heat Maps - Tablets – After Configuration



Heat Maps - PCs – Default Configuration

HP ProBook Windows 7				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass	Pass w/ Config
Pass w/ Config	Fail	Pass w/ Config	Pass	Pass w/ Config
Pass	Pass w/ Config	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Fail	Pass w/ Config	Pass
Pass	Pass w/ Config	Pass w/ Config	Pass w/ Config	
	Pass	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass w/ Config	Pass w/ Config	
	Pass w/ Config	Pass/Fail	Pass	
		Fail		
		Pass w/ Config		
		Pass w/ Config		
		Fail		
		Pass		
		Pass w/ Config		

15
26
1
5

HP Microtower Windows 7				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass	Pass
Pass w/ Config	Fail	Pass w/ Config	Pass	Pass
Pass	Pass w/ Config	Pass	Pass w/ Config	Pass
Pass	Pass	Fail	Pass w/ Config	Pass
Pass	Pass w/ Config	Pass w/ Config	Pass w/ Config	
	Pass	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass w/ Config	Pass w/ Config	
	Pass w/ Config	Pass/Fail	Pass	
		Fail		
		Pass w/ Config		
		Pass w/ Config		
		Fail		
		Pass		
		Pass w/ Config		

18
23
1
5

LMI

Pass Pass w/ Config Pass/Fail Fail

Heat Maps - PCs – After Configuration

HP ProBook Windows 7				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass	Pass w/ Config
Pass w/ Config	Fail	Pass w/ Config	Pass	Pass w/ Config
Pass	Pass w/ Config	Pass	Pass w/ Config	Pass w/ Config
Pass	Pass	Fail	Pass w/ Config	Pass
Pass	Pass w/ Config	Pass w/ Config	Pass w/ Config	
	Pass	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass w/ Config	Pass w/ Config	
	Pass w/ Config	Pass/Fail	Pass	
		Fail		
		Pass w/ Config		
		Pass w/ Config		
		Fail		
		Pass		
		Pass w/ Config		

15
26
1
5

HP Microtower Windows 7				
Access	Audit	Integrity	Authentication	Transmission
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass
Pass w/ Config	Pass w/ Config	Pass w/ Config	Pass	Pass
Pass w/ Config	Fail	Pass w/ Config	Pass	Pass
Pass	Pass w/ Config	Pass	Pass w/ Config	Pass
Pass	Pass	Fail	Pass w/ Config	Pass
Pass	Pass w/ Config	Pass w/ Config	Pass w/ Config	
	Pass	Pass w/ Config	Fail	
	Pass	Pass w/ Config	Pass	
	Pass	Pass w/ Config	Pass w/ Config	
	Pass w/ Config	Pass/Fail	Pass	
		Fail		
		Pass w/ Config		
		Pass w/ Config		
		Fail		
		Pass		
		Pass w/ Config		

18
23
1
5

LMI

Pass Pass w/ Config Pass/Fail Fail

Configuration is Key

- Our tests show the importance of configuration
- Without configuration, none of the tested devices could achieve more than 50% of the security requirements
- With ‘on-device’ configuration, 9 of the devices were able to meet more than 50% of the security requirements
- With ‘on-device’ configuration, 87% was the highest score achieved among the devices

Unexpected Findings

- Devices without passwords/unlocked allow access to files via USB
- Android security varies greatly between vendors
- Blackberry PlayBook tablet runs a web server by default
  - Creates potential vulnerabilities
- ViewSonic ViewPad 10 runs a capable Windows 7
  - Same hardware runs Android with missing security features
- HP TouchPad moving toward Android applications
  - Security implications are varied
- Enterprise mobile device management tools could make devices more secure
  - Require additional, scarce resources

Sample Lockdown Procedures

- Based on the Security Requirements Traceability Matrix (RTM)
- Explains:
  - What to do – which items need configuration
  - How to do it – with text and graphics
- Address all results that are “Pass w/Config”
- Step by step directions to “Pass”
- Note:
  - Some of these procedures are available elsewhere, but are not specific to use in the medical ecosystem
  - Sources and quality vary greatly

Sample Lockdown Procedures: Password Protection

- Apple iPhone

  The first line of defense for protecting the privacy of your data on a mobile device is to enable a password.

LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - On the **Home Screen**, select the **Settings** Icon.

LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - Navigate through the Settings display and select **General**.

LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - Navigate through the Settings display and select **General**.

LMI

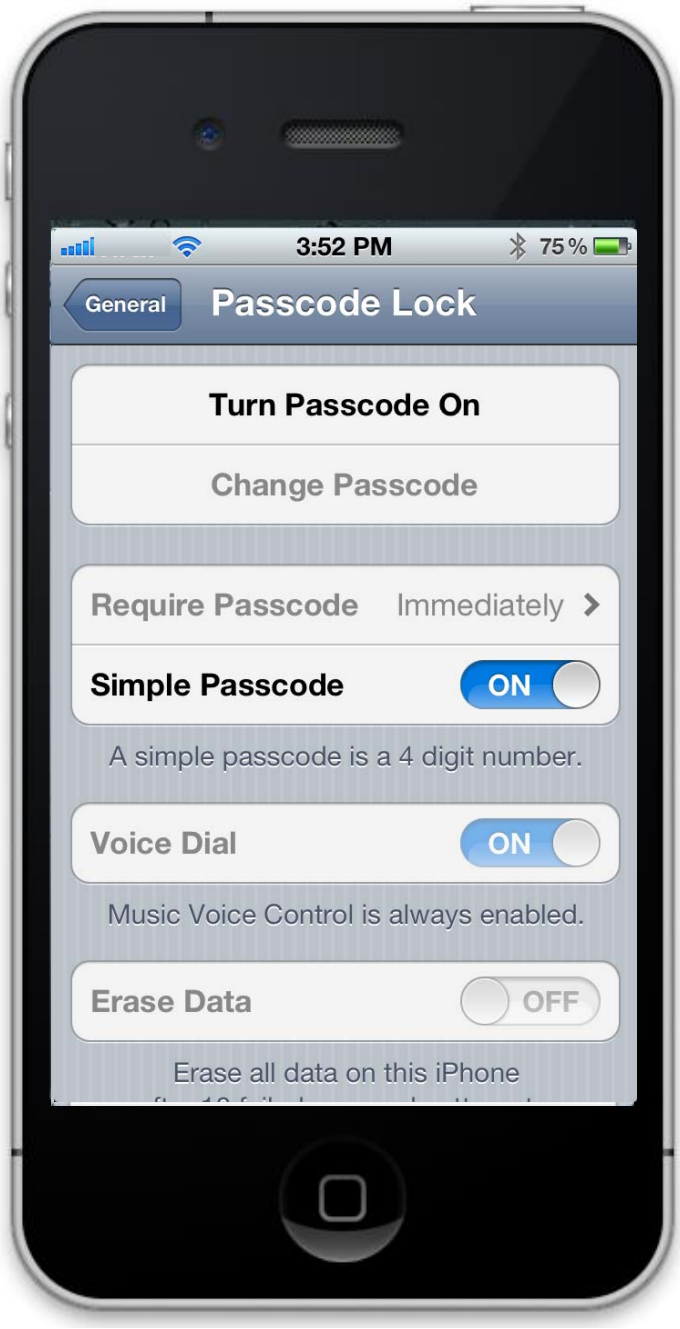
Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - In the General section, locate **Passcode Lock** and then select.

LMI

Sample Lockdown Procedures: Password Protection

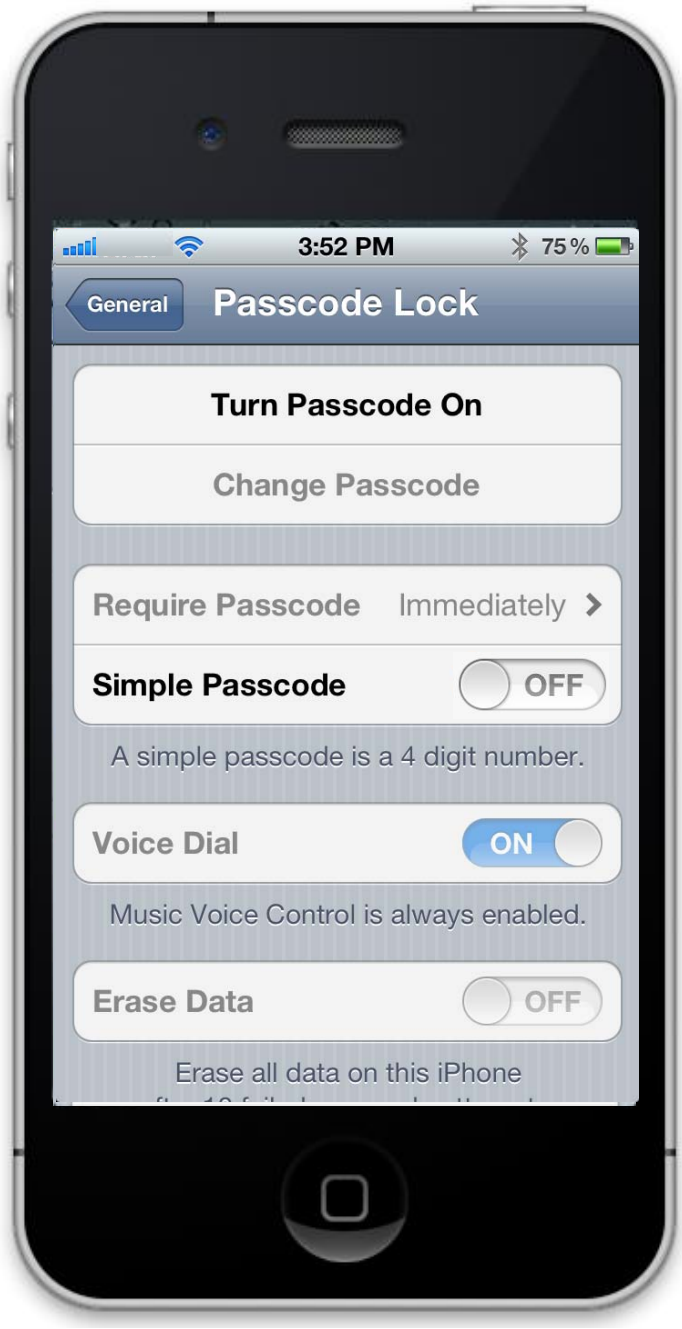
- Apple iPhone
  - If the **Simple Passcode** is in the ON position, *Slide* to the **OFF** position.



LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - If the **Simple Passcode** is in the ON position, slide it to the **OFF** position.

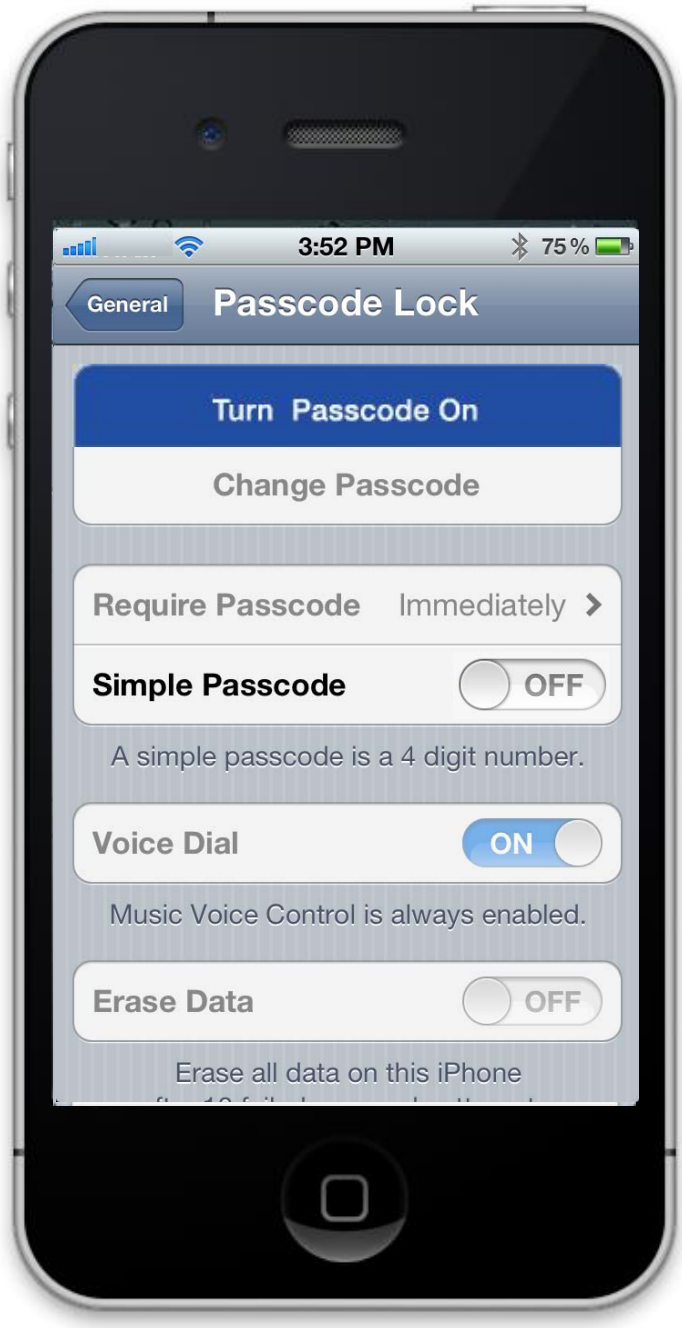


LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - If the **Simple Passcode** is in the ON position, slide it to the **OFF** position.

Next select **Turn Passcode On**



LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone

  By disabling Simple Passcode, you now can create a **Complex Password**.

  1. Create a password/passcode at least eight (8) characters in length.
  2. Use a combination of alphabetic, upper and lower case characters, numbers, and special characters.

LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone
  - Re-enter your complex password

LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone

  With password protection in place, you will now be challenged to enter your password the next time the iPhone's *Auto-Lock* screen appears.

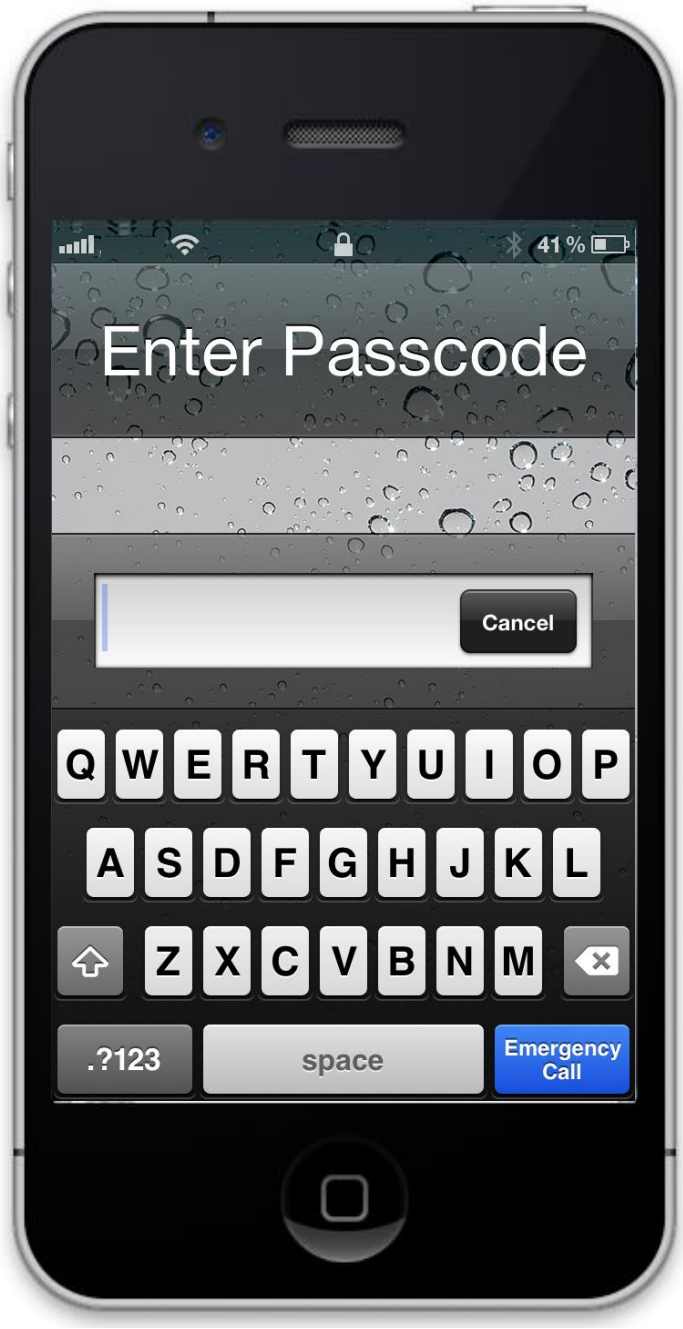
- The *Auto-Lock* timer should not be set to greater than 3 mins.

LMI

Sample Lockdown Procedures: Password Protection

- Apple iPhone

  Your iPhone is now secured with password protection after 3 minutes of inactivity.

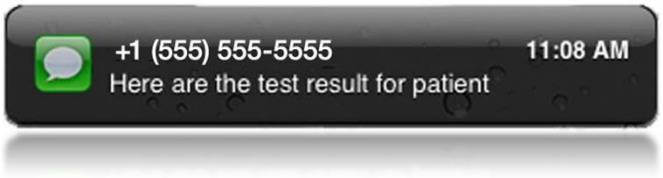


LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad

  It is important that sensitive data is only viewed by the intended audience.



LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad
  - To secure SMS messages, first *Tap* on the **Settings** icon.

LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad
  - Review the options under the **Settings** panel and locate **Notifications**

LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad
  - Next select the **Messages** icon near the center on the panel to the right.

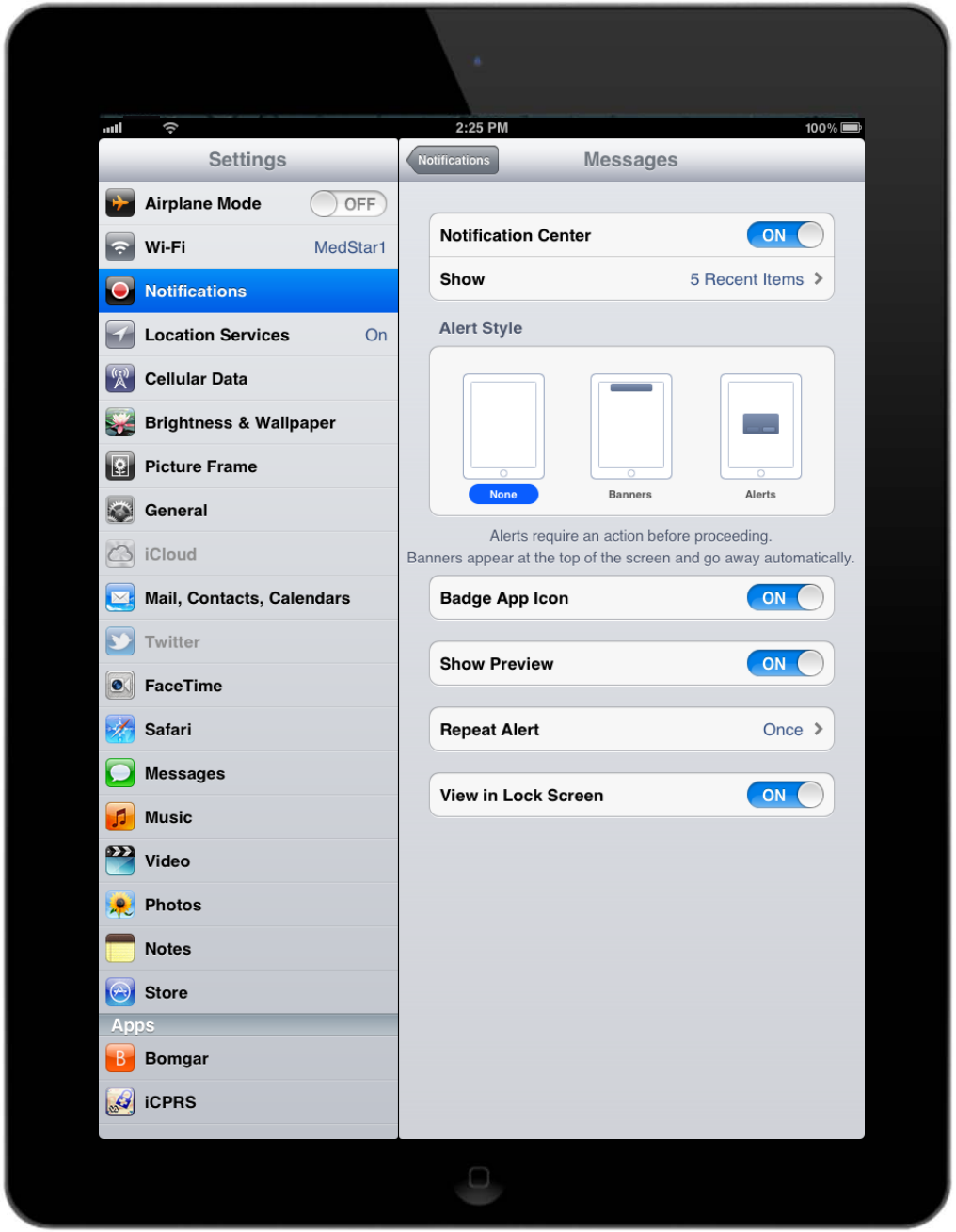
LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad

  The next view shows a variety of selections.

  1. Under **Alert Style,** select **None**



LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad

  The next view shows a variety of selections.

  1. Under **Alert Style,** select **None**
  2. Slide the **Show Preview** selection to **OFF**

LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad

  The next view shows a variety of selections.

  1. Under **Alert Style,** select **None**
  2. Slide the **Show Preview** selection to **OFF**.
  3. Slide the **View in Lock Screen** selection to **OFF**.

LMI

Sample Lockdown Procedures: SMS Messages

- Apple iPad

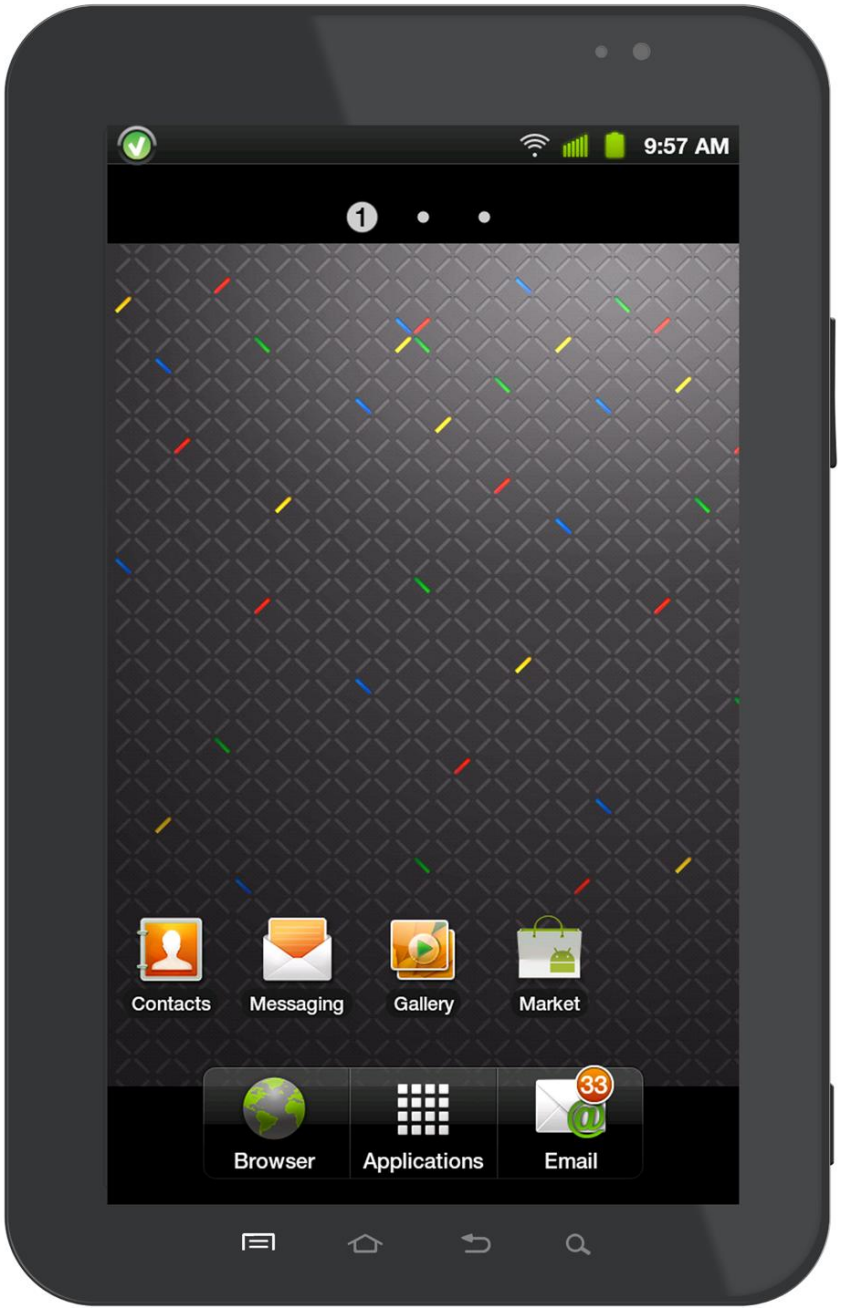
  With the new settings in place, the owner of the iPad will still be alerted of new SMS messages, but phone numbers and content will not be displayed.

LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

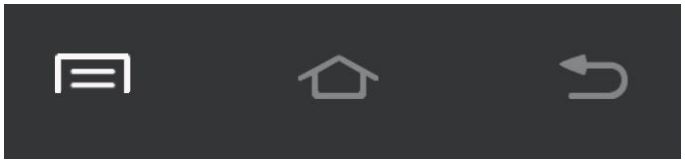
  To ensure privacy, it is important that personal data and passwords are not retained by the web browser of the mobile device.

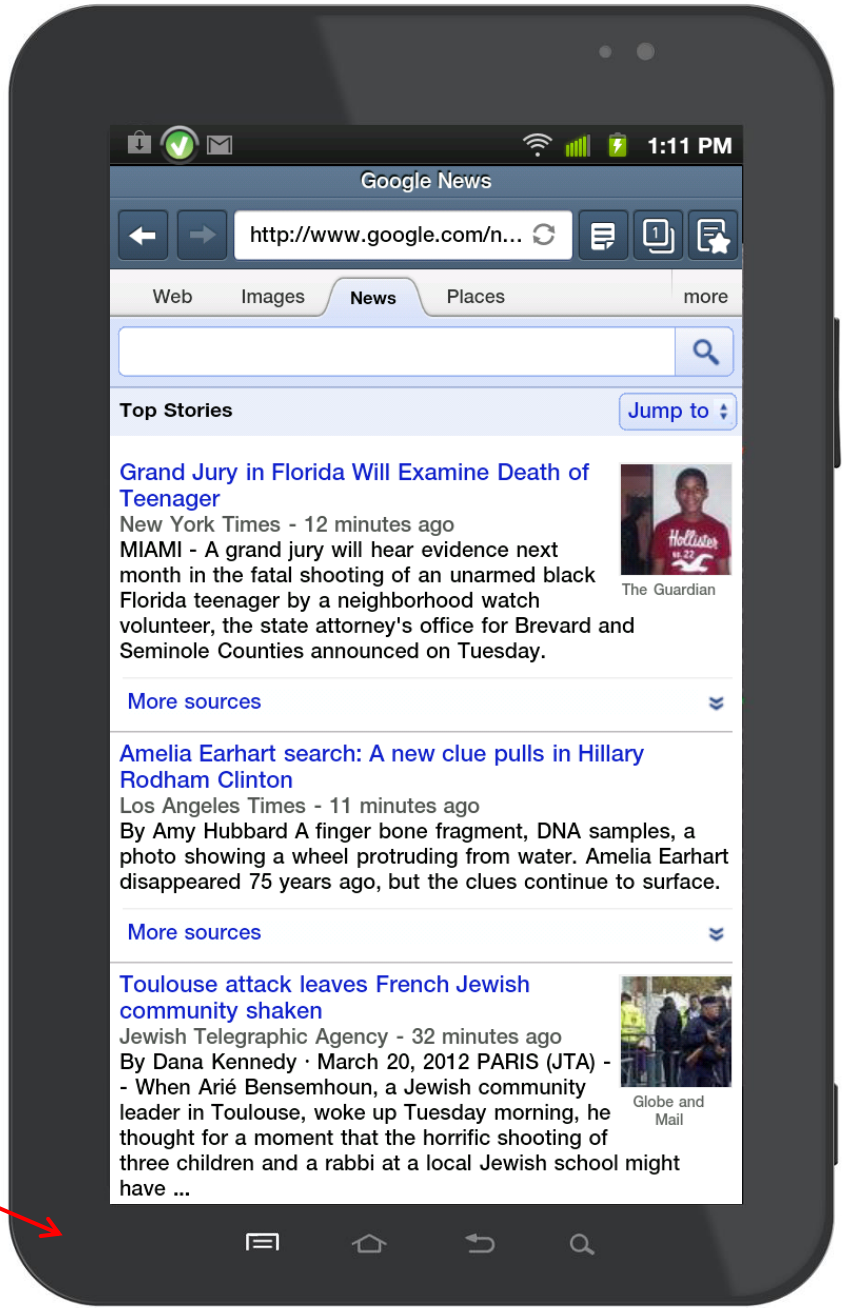


LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab
  - Launch the internet **Browser** from the home screen.
  - Select the **Menu Key** icon located near the base of the unit.

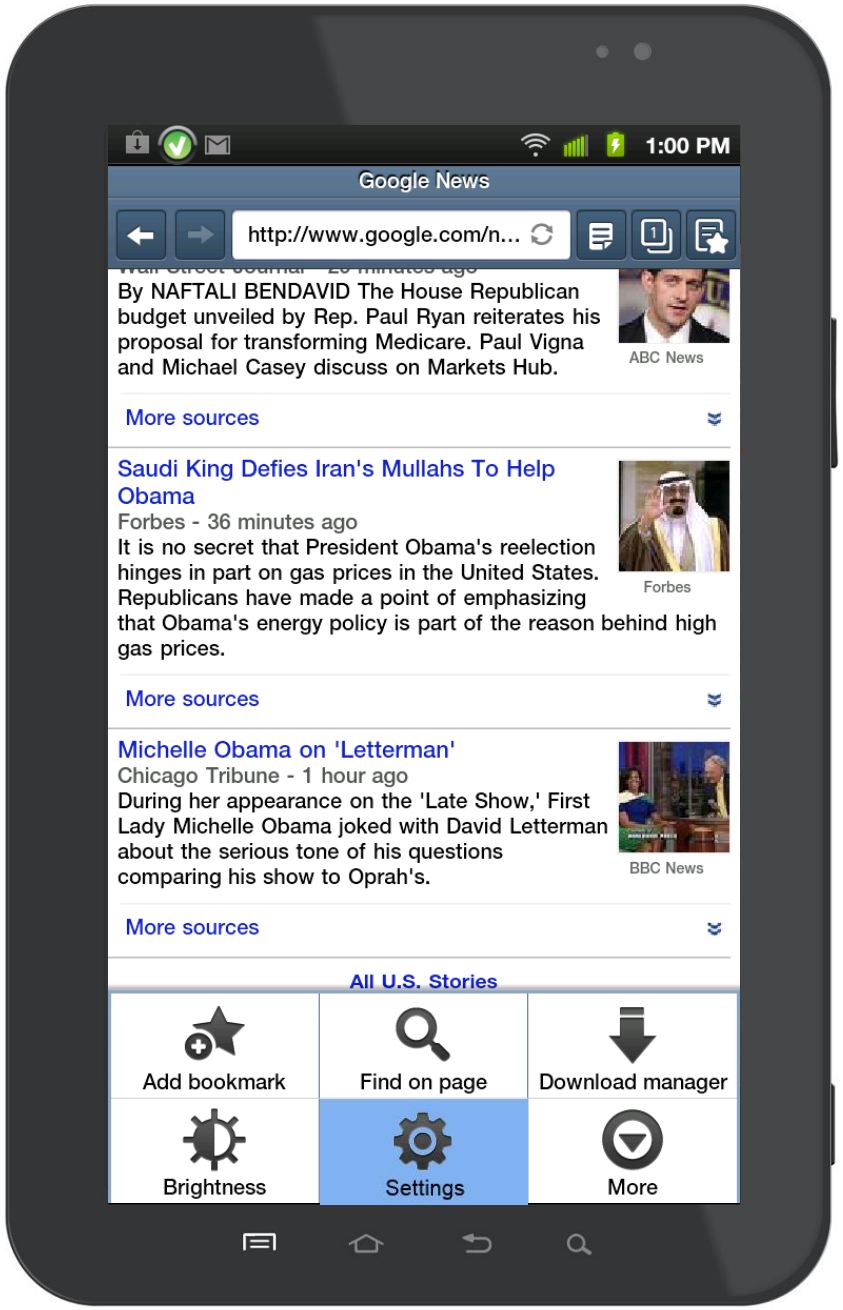




LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab
  - This will bring up the ***Browser Menu*** with a variety of options.
  - *Tap* on the **Settings** icon.

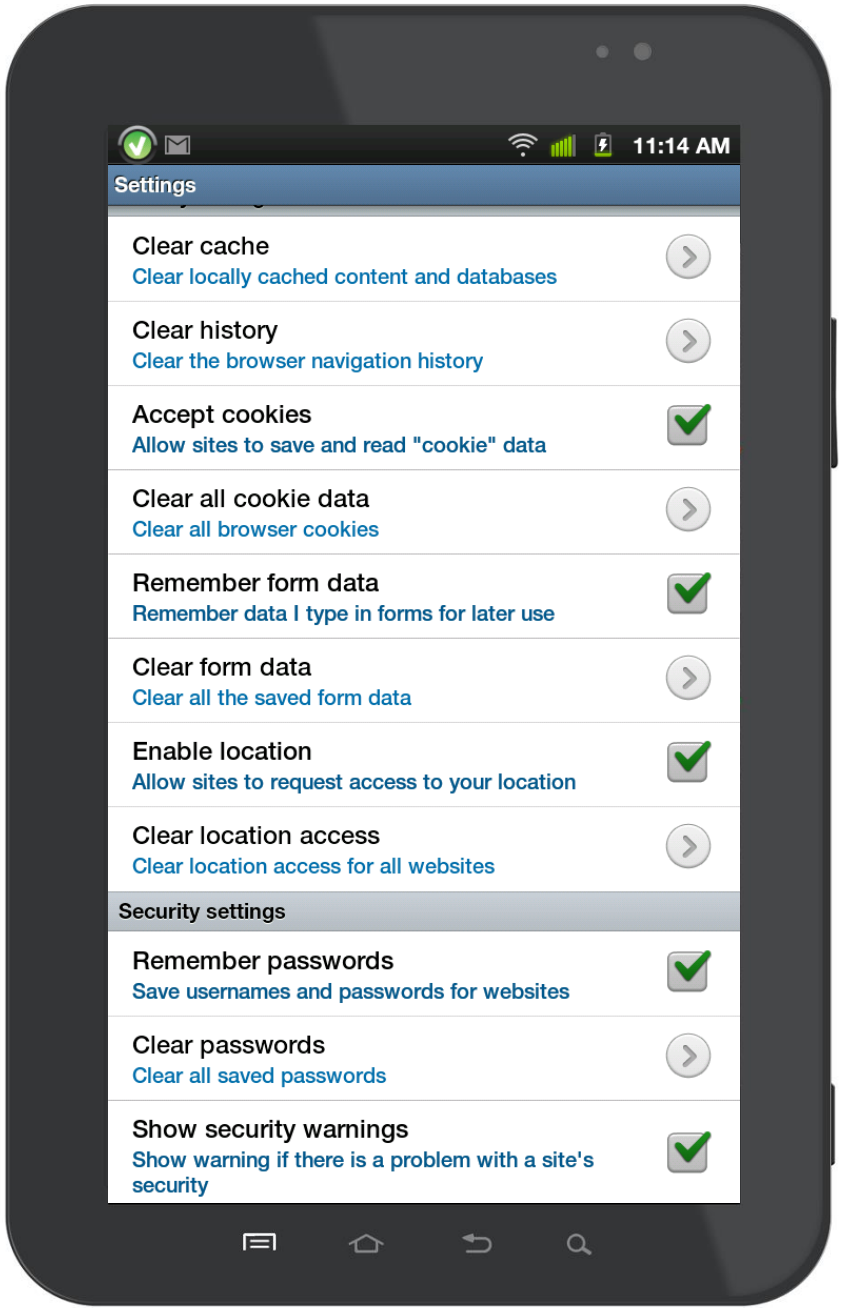


LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

  The **Adjusting Browser Page Settings** is now in view.



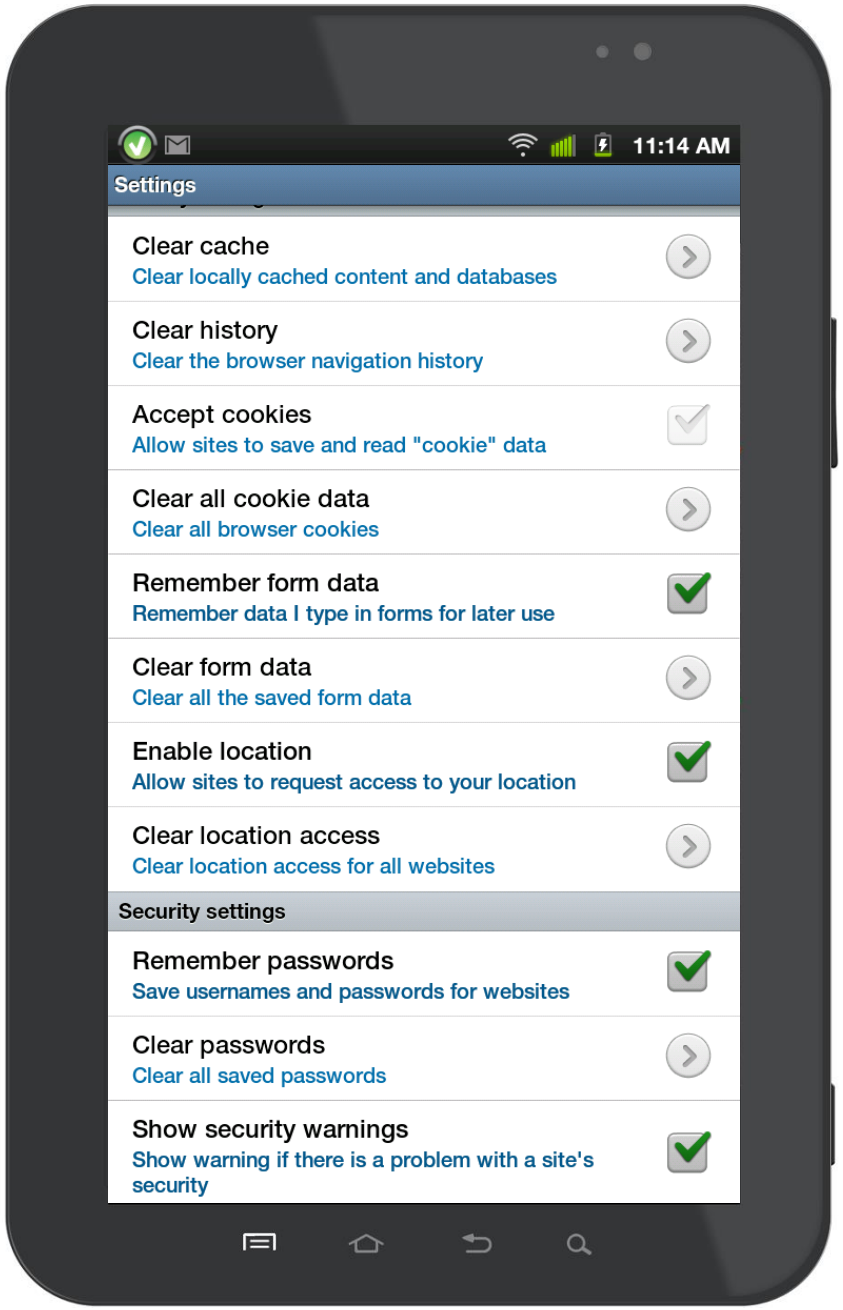
LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

  Uncheck the following:

  1. Accept cookies



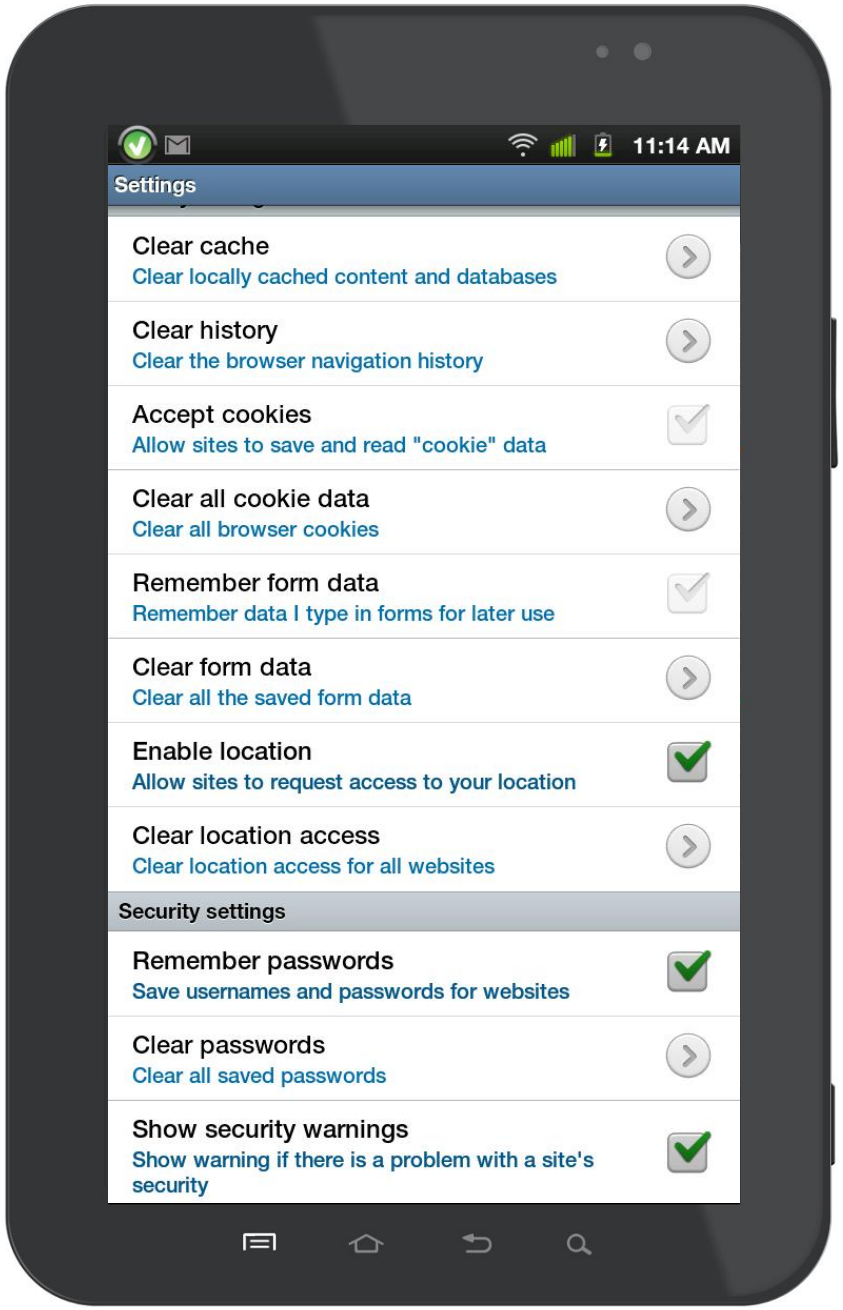
LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

  Uncheck the following:

  1. Accept cookies
  2. Remember form data



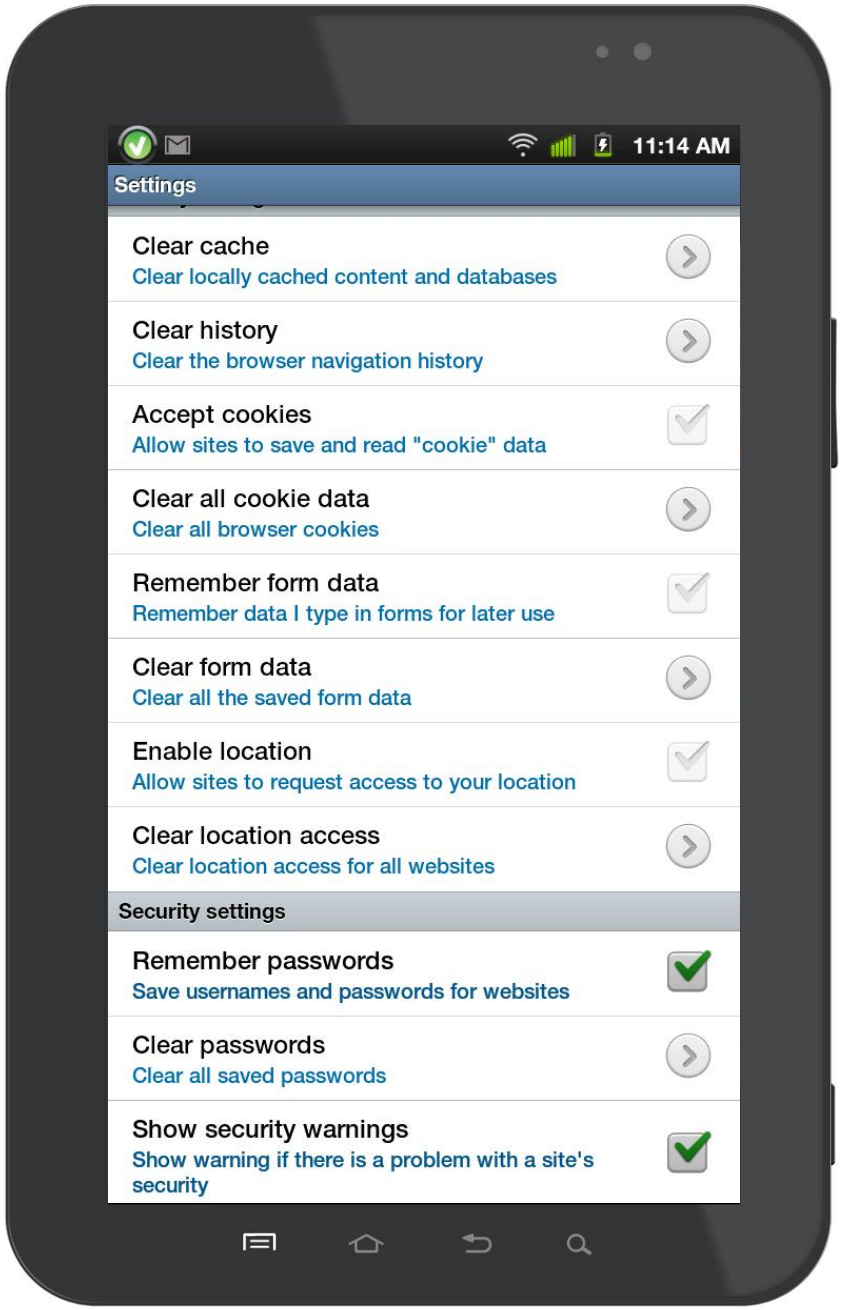
LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

  Uncheck the following:

  1. Accept cookies
  2. Remember form data
  3. Enable location



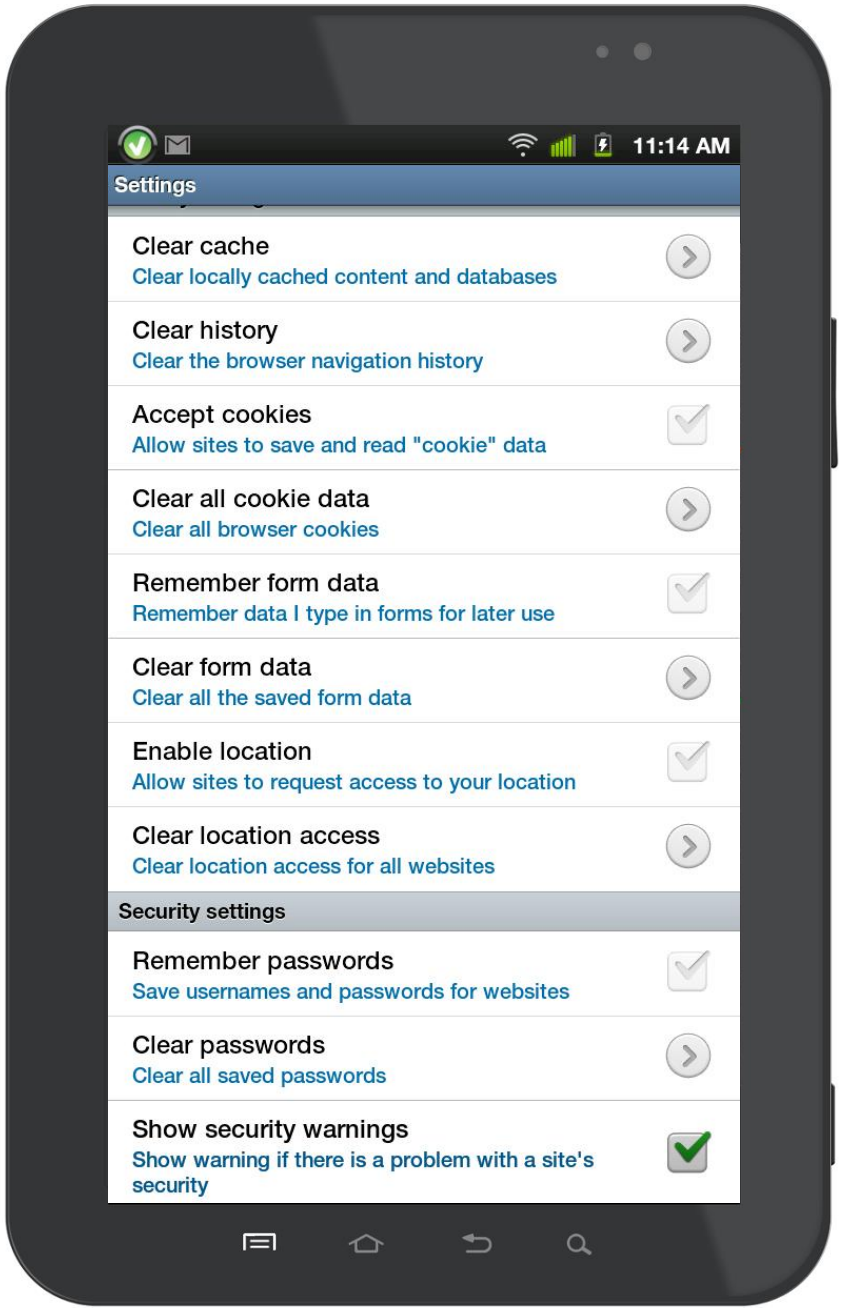
LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

  Uncheck the following:

  1. Accept cookies
  2. Remember form data
  3. Enable location
  4. Remember passwords

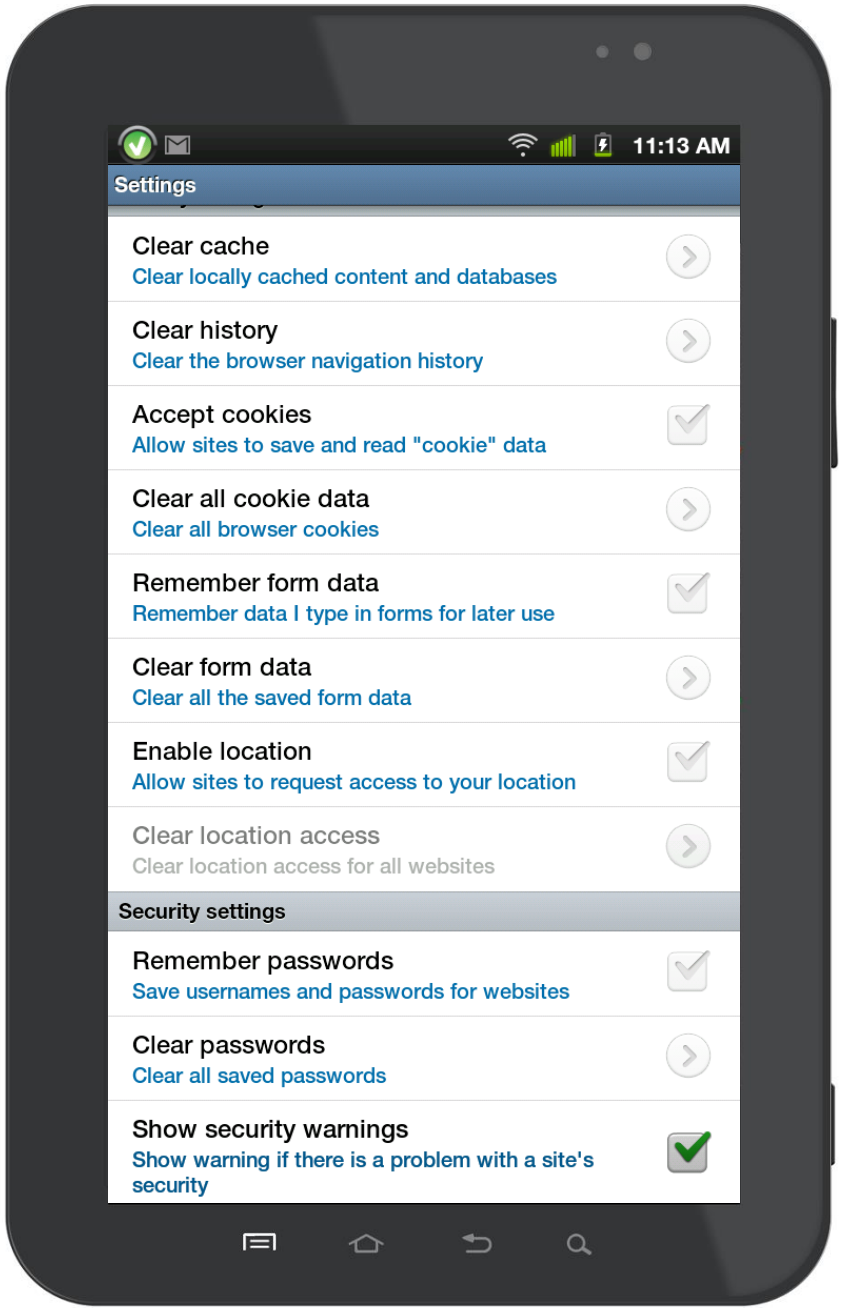


LMI

Sample Lockdown Procedures: Form Data

- Galaxy Tab

  All options should now be grey and inactive, except for **Show security warnings** which should remain selected with a checkmark.



LMI

Sample Lockdown Procedures: Security Code

- Windows Phone

  Windows mobile has a password protection feature but does not currently support **Complex Passwords**.

  The following steps will instruct an owner of a Windows mobile Smartphone to enable a numeric **Security Code**.

LMI

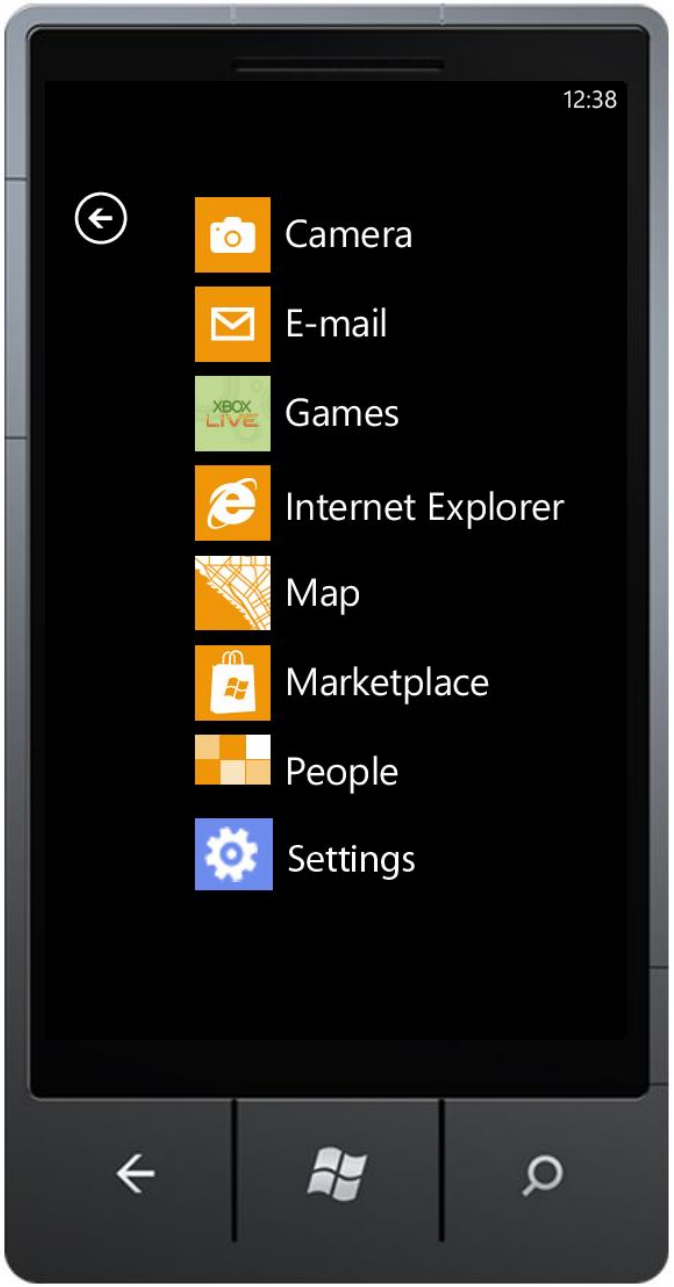
Sample Lockdown Procedures: Security Code

- Windows Phone
  - From the Start screen, *Tap* the **Arrow** icon.

LMI

Sample Lockdown Procedures: Security Code

- Windows Phone
  - In the **App Menu Screen**, *Slide* down the options till you reach the **Settings** icon and then select.



LMI

Sample Lockdown Procedures: Security Code

- Windows Phone
  - *Scroll* down to and *Tap* **lock + wallpaper**.

LMI

Sample Lockdown Procedures: Security Code

- Windows Phone
  - *Scroll* down to and *Tap* **lock + wallpaper**.

LMI

Sample Lockdown Procedures

- Windows Phone
  - *Slide* the **Password** toggle to enable the **Security Code**.

LMI

Sample Lockdown Procedures

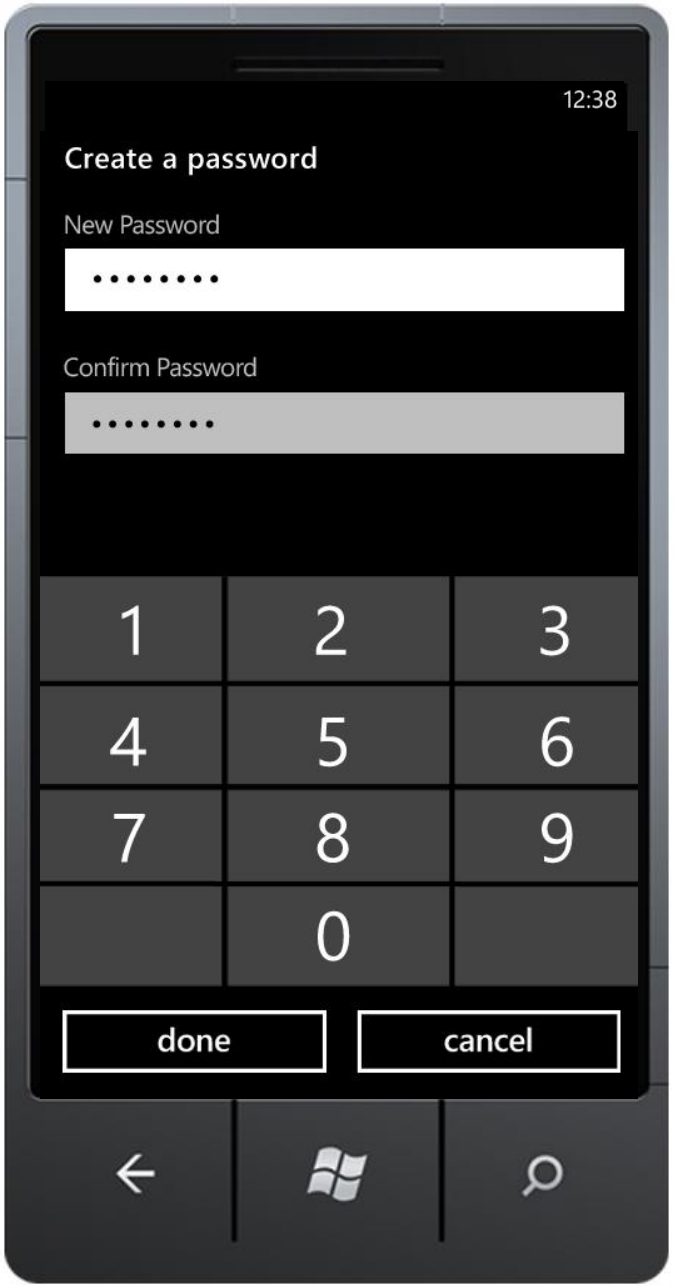
- Windows Phone
  - *Slide* the **Password** toggle to enable the **Security Code**

    When activated, the Password toggle is highlighted **Blue**.

LMI

Sample Lockdown Procedures

- Windows Phone
  - **Enable password**: Enter and re-enter numeric codes and then tap **Done.**
  - Security guidelines recommend a minimum of 8 digits be used.



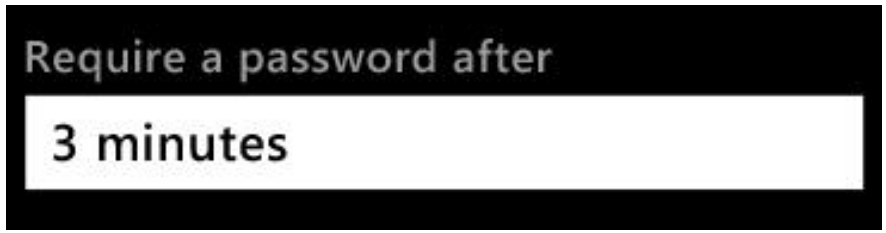
LMI

Sample Lockdown Procedures

- Windows Phone

  With Passcode protection in place, you will now be required to enter it when the *Lock Screen* appears after inactivity.

- The *Lock Screen* feature should not be set to greater than 3 mins



LMI