Enabling a Secure Mobile Environment for the State of Illinois

GOVERNMENT PUSHING THE MOBILE FRONTIER

SPACE PROGRAM

LAW ENFORCEMENT

LAW ENFORCEMENT

MILITARY

FUTURE CAPABILITIES

FUTURE CAPABILITIES

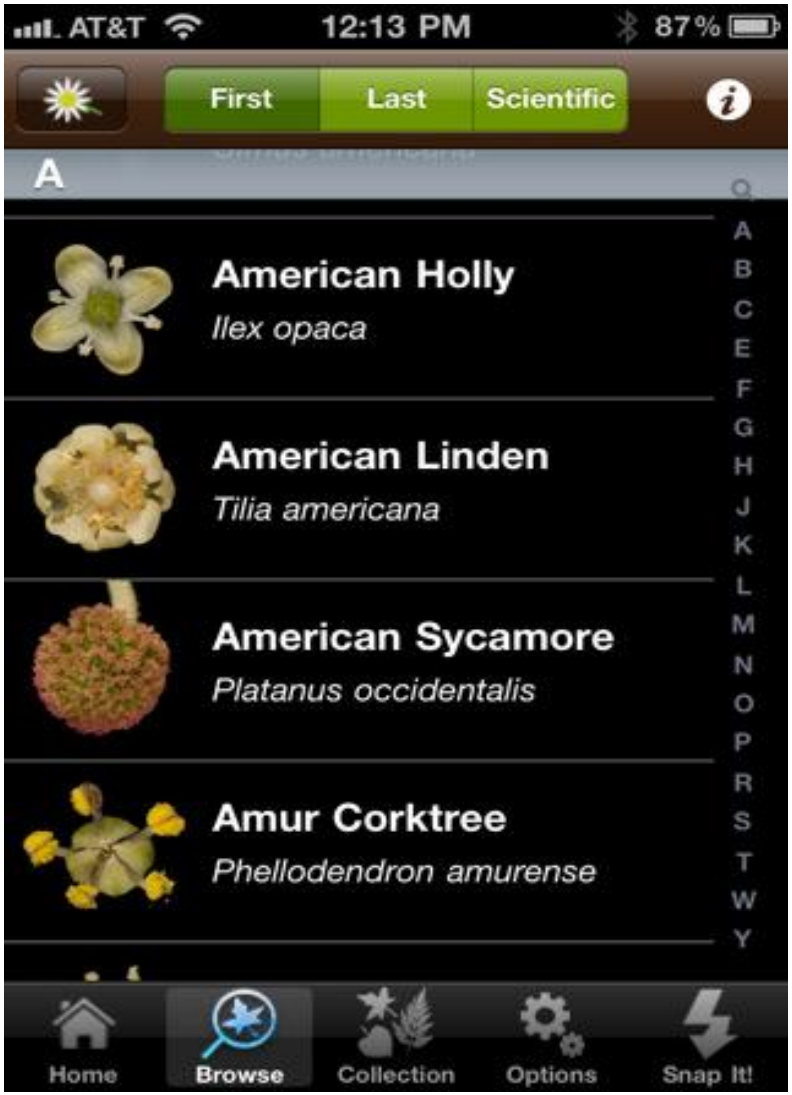
FUTURE CAPABILITIES

MOBILE APPLICATIONS

MOBILE APPLICATIONS

MOBILE APPLICATIONS

MOBILE APPLICATIONS

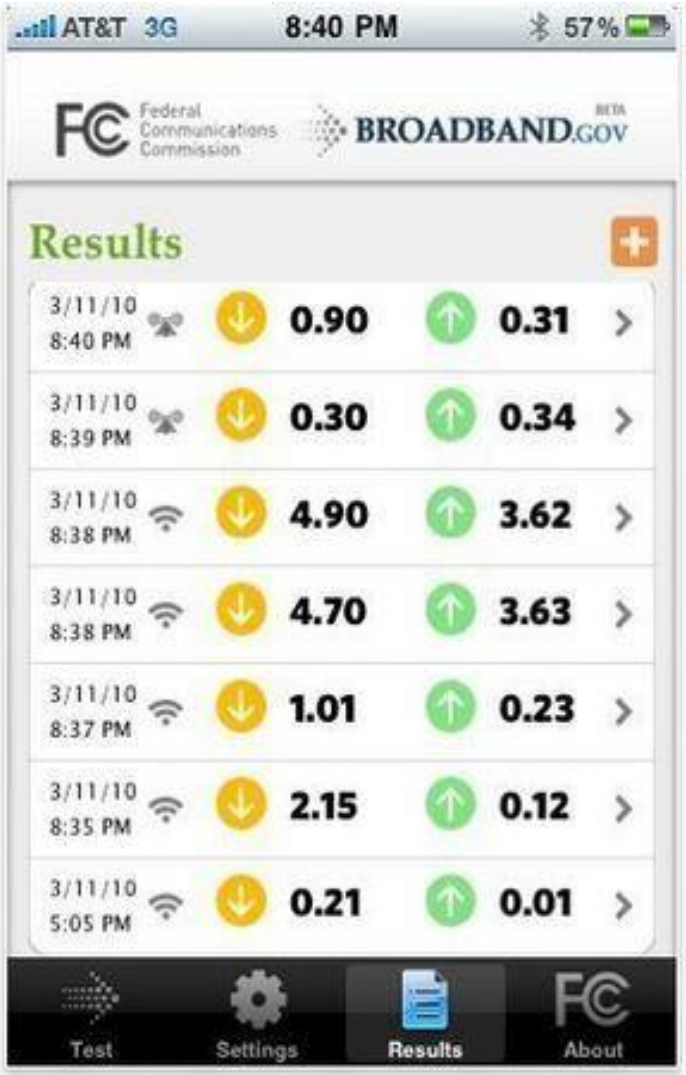


MOBILE APPLICATIONS

MOBILE APPLICATIONS

MOBILE APPLICATIONS

MOBILE APPLICATIONS



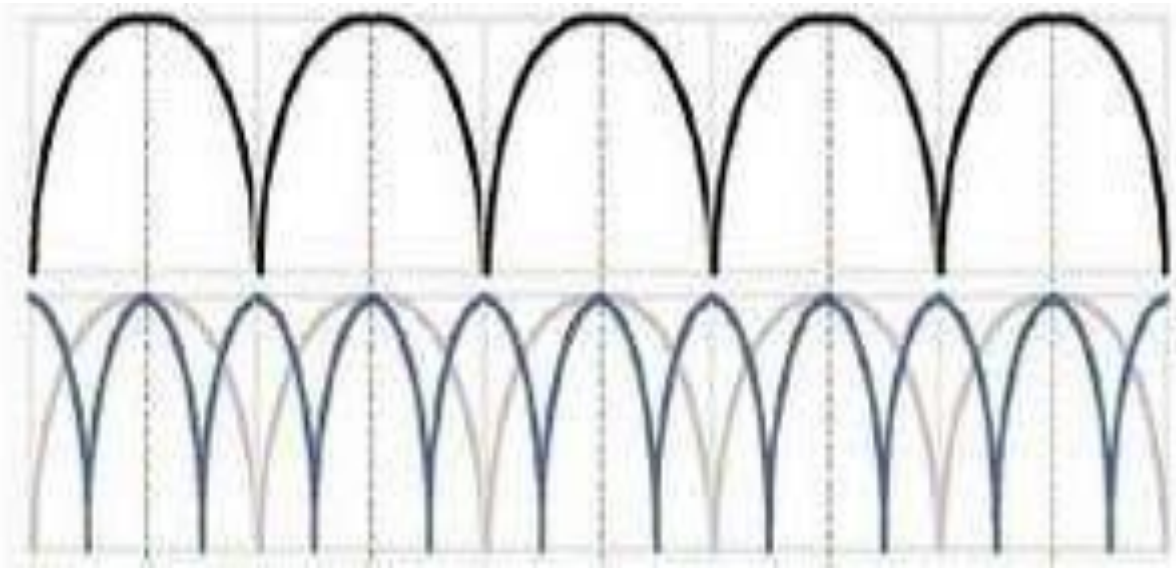
ILLINOIS – MOBILE FRONTIER

ILLINOIS – MOBILE FRONTIER

Illinois Terrorism Task Force

ILLINOIS – MOBILE FRONTIER

ILLINOIS – MOBILE FRONTIER



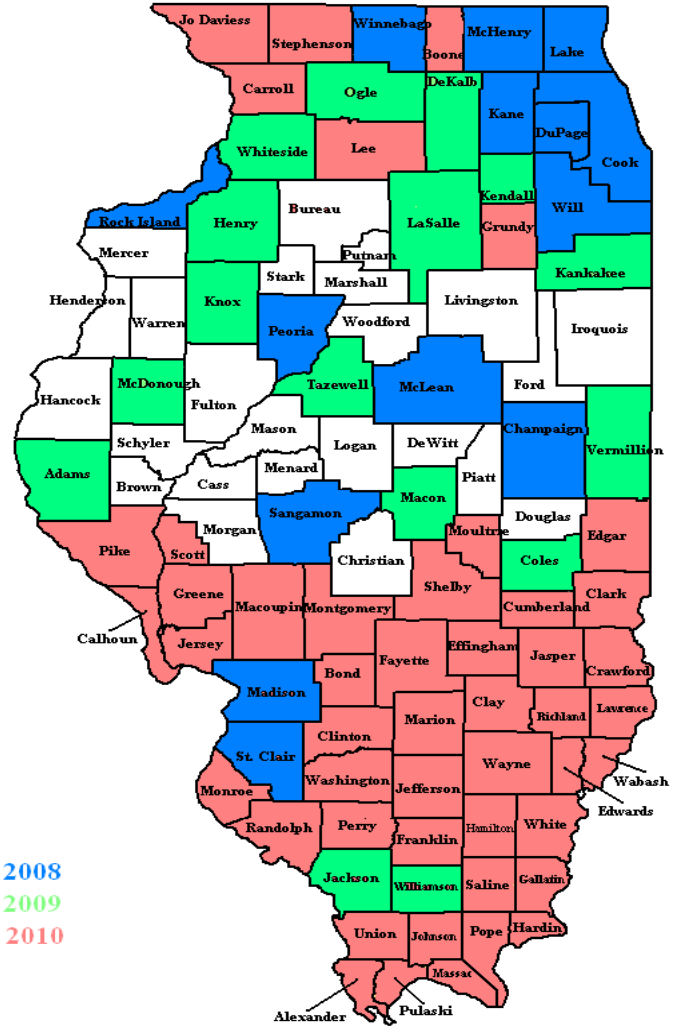
Legacy 25KHz Channels

Narrowband 12.5KHz Channels Phase1

All 25 KHz systems MUST be 12.5 KHz systems by Jan 1st, 2013

ILLINOIS – MOBILE FRONTIER

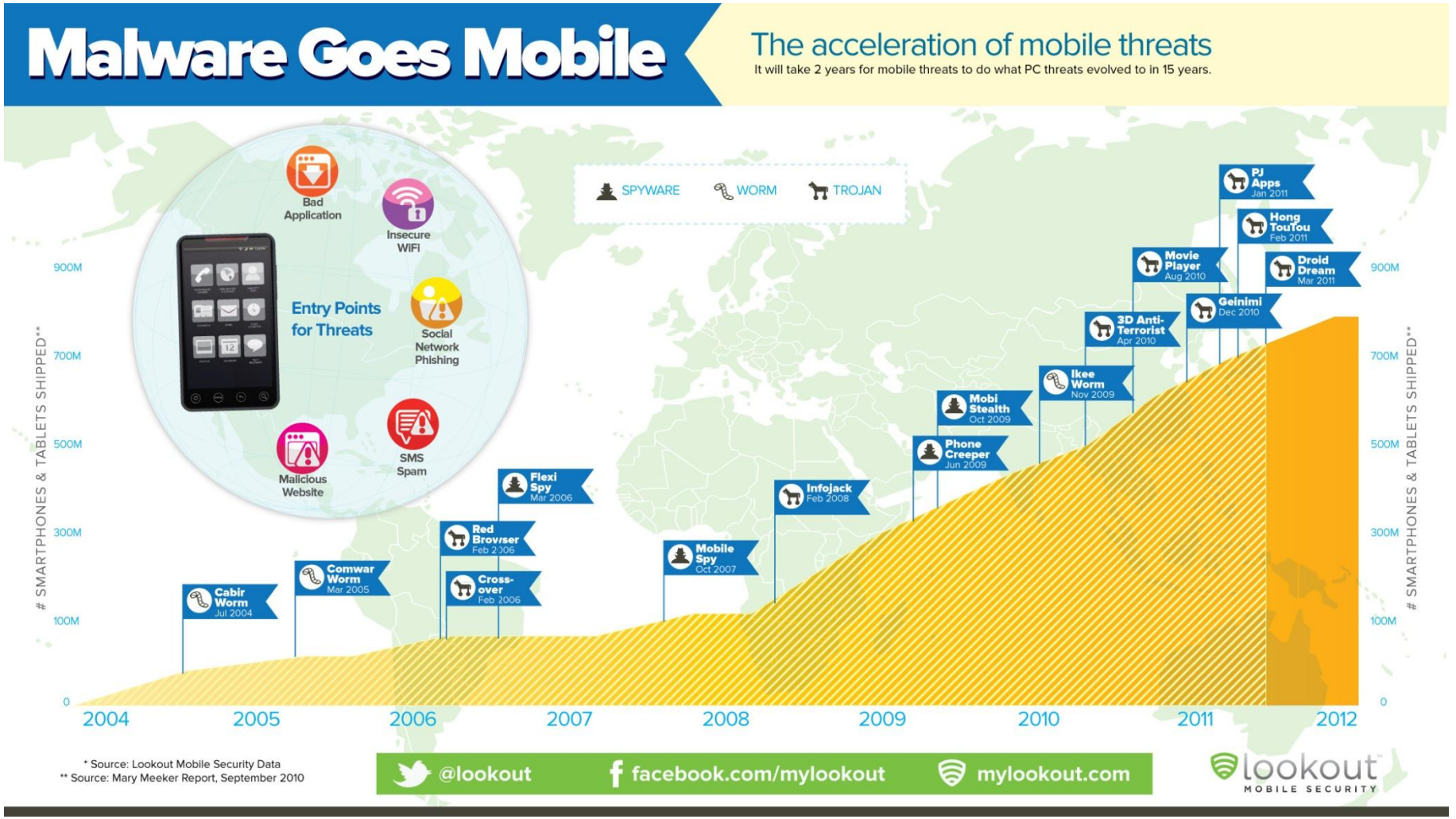
ILLINOIS – MOBILE FRONTIER



MOBILE SECURITY IS DATA SECURITY

DATA IS EVERYWHERE

MOBILE MALWARE



A NEW MODEL FOR MOBILE RESILIENCY

MOBILE SECURITY CONCERNS

- Lost/stolen devices
- Penetration of our corporate Wi-Fi networks
- Mobile malware on applications from public app stores
- Users forwarding corporate information to cloud-based storage services
- Security at public hotspots
- Users forwarding email to personal accounts
- Interception of over-the-air transmissions
- Malware exploiting vulnerabilities on internally developed mobile apps
- Devices jailbroken or rooted by end users
- Penetration of users' home Wi-Fi networks

MOBILE POLICIES

- 62% organizations allow personal devices at work,
- IT's juggling laptop policies and Wi-Fi policies and BYOD policies
- 80%, require only passwords for mobile devices that access enterprise data/networks
- 14% require hardware encryption
- 40% of organizations limit the range of devices supported and require that users connect them with an MDM system.

SECURING DATA IN TRANSIT

- VPN secure tunnel
- Secure HTTP
- BlackBerry secure email
- Virtual desktop (e.g., VMware, Citrix)
- Other secure email
- MDM technology

AUTHENTICATION MECHANISMS

- User name/password
- Power-on device password
- On-device certificates
- Secure token
- Image or pattern
- Biometrics
- Cellular call-back verification (e.g., PhoneFactor)
- Facial recognition
- Grid card (e.g., Entrust IdentityGuard)

AUTHENTICATION MECHANISMS

- Securing the data residing on mobile devices
- Securing data in transit from the network to mobile devices
- Securing the network perimeter
- Securing devices themselves using antivirus/anti-malware, MDM client software, etc.
- Preventing phone/SMS fraud

MOBILE SECURITY AWARENESS

PREPAREDNESS

MOBILE PREPAREDNESS ASSESSMENT

- Business and technical requirements analysis
- Review of your existing wireless LAN architecture
- Review of your existing RF design
- Wireless LAN configuration review
- Gap analysis and recommendations

WIRELESS CONFIGURATION REVIEW

- Wireless LAN security
- Quality of service
- Wireless multicast
- RF planning
- Client mobility
- High availability

MOBILE SECURITY “ART OF WAR”