# In The Air Tonight: Operational Security Challenges for Wireless Network Operators

**Roland Dobbins**
<rdobbins@arbor.net>
*Senior ASERT Analyst*
+66-83-266-6344 BKK mobile
+65-8396-3230 SIN mobile
*Arbor Public*

## Wireless Security Capsule History

- Early systems like Carterfone subject to RF-based jamming, FCC involved in USA, some high-profile prosecutions in the late 1960s/early 1970s.
- Toll-fraud made the move from payphones (remember those?) to early AMPS systems in the early 1980s.
- 1980s the ‘Golden Age’ of mobile phone abuse, offshoot of phone-phreaking of phone switches, PBXes.
- Kevin Mitnick hacked mobile phone switches to listen in on the mobile phone conversations of Secret Service agents hunting him.

## This Was Your Father's (or Grandfather's) Mobile Phone . . .

## Free Kevin Mitnick!

## Wireless Security Capsule History (cont.)

- Long-haul microwave relay towers shot up by drunken hunters, good ol' boys - gradual signal degradation, multi-million-dollar-a-year problem into the late 1990s.
- Mobile phone cloning popular in mid-1980s - mid-1990s.
- Use of frequency analyzers and scanners to illegally wiretap mobile phone conversations routine until widespread adoption of GSM, CDMA in late 1990s.
- Early GSM & CDMA data services largely disrupted via accidental RF interference.

## In the New Millennium . . .

- Inadvertent battery-draining attacks caused by botted laptops with GPRS/EDGE dongles in 2002 - host-scanning/port-scanning wakes up phones, drains batteries.
- Inadvertent RAN/GGSN/SGSN DDoS caused by botted laptops - host-scanning/port-scanning causes fragile TCP/IP stacks to fall over.
- Inadvertent firewall DDoS caused by botted laptops - host-scanning/port-scanning causes fragile/ useless stateful firewalls to fall over.
- Inadvertent stateful firewall DDoS caused by botted laptops launching outbound/crossbound DDoS.

## Recently . . .

- DNS, Web portals, other ancillary services DDoSed by botted laptops with dongles, generally inadvertently.
- Botted subscribers increasingly deliberately targeted - mainly criminal-on-criminal activity directed at the bots, also mobile gamers talking smack.
- Many wireless operators don’t have highly skilled TCP/IP personnel, poorly-designed networks with loads of state, no visibility, no control, no engagement with the larger operational community.

## Recently (cont) . . .

- Smartphone PoC botnet code showed up in the wild in 2009.
- First botted smartphones showed up at the end of 2010 - Android phones in China, compromised via poisoned apps in app store (Android isn't curated like iDevices). Committing toll-fraud, online click-fraud, et. al.
- Double-byte encoding issues with SMS messages allow buffer overflows on many types of smartphones, including iDevices (Apple patched).
- First smartphone worm for jailbroken iPhones in 2009.

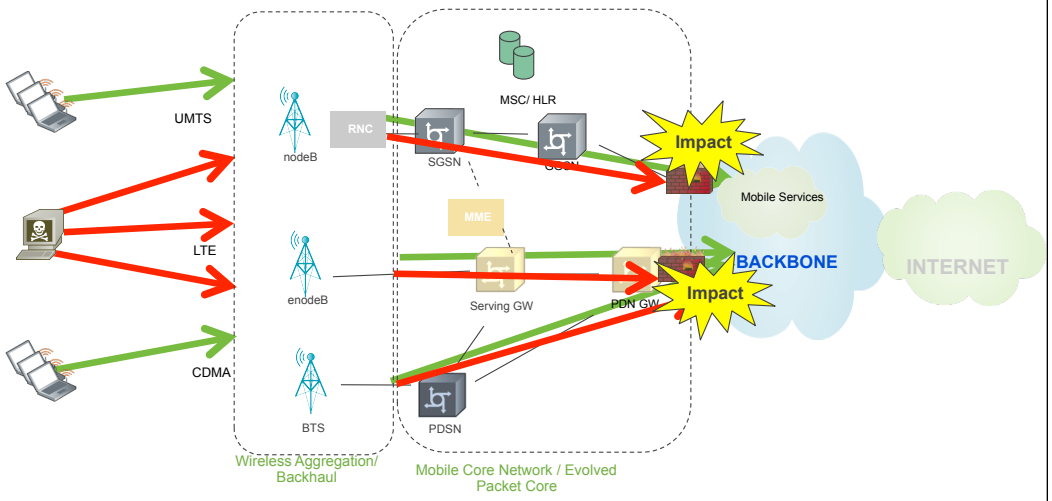
## Recently (cont) . . .

- Bluetooth hacking for fun & profit!
- WiFi attack surface.
- NFC, ZigBee, USB 3.0, WiFi Direct under development.
- More and more side-channels!

# This isn’t speculation . . .


**“The risk has arrived.”**
**-- Ted Seely, SprintLink**

# 4AM Call - “Help! Our *entire* 3G network is down!”



## Today . . .

- ~2.9M **compromised** iPhones worldwide.
- ~560,000 **compromised** iPads worldwide.

***WHAT?!***

## Do the Jailbreak Rock!

- How are iPhones/iPads/iPod Touches jailbroken?
- Via security vulnerabilities!
- No end in sight, every new version has exploitable vulnerabilities!
- And this is in the most tightly-controlled, curated platform family on the market . . .

## 2010 WISR Wireless Summary

- Wireless operators have little visibility into their traffic.
- Wireless operators have little control over their traffic.
- Few wireless operators institute TCP/IP BCPs.
- Wireless operators continue to avoid participating in the global opsec community.
- Wireless operators will be instantiating even more state in their networks via 6-to-4 and CGNs.
- The most popular, rapidly-expanding ISPs on the planet - and they're the least-prepared!

## 2011 WISR Wireless Summary

- Wireless operators reported much greater visibility into their traffic.
- It turns out that this was an artifact of how questions were worded - most survey respondents still do not have operationally useful visibility into their network traffic.
- More CAPEX and OPEX expenditures on infrastructure security and network visibility, greater awareness of the problem.
- 9% had deployed IPv6 for subscriber addressing, 50% planned on implementing IPv6 for subscriber addressing within the next year.  IPv4/IPv6 security feature parity a major concern.

# And don’t forget about RF . . .

## Wireless – Same as Wireline, Plus More

- Wireless operators have all the same concerns as wireline operators.
- Wireless operators have additional concerns beyond those facing wireline operators.
- Fixed wireless and mobile wireless share most of the same wireless-specific concerns, though there are some differences in architecture.
- Biggest differences between fixed wireless and mobile wireless today are battery life in mobile devices, more-or-less 1:1 mapping of user:device in mobile, mobile focus on voice (changing), mobile prevalence (though fixed is growing fast).

## Opsec Priorities for Wireless Operators

- RF spectrum preservation
- Backhaul capacity preservation
- Transit capacity preservation
- Detection/classification/traceback of undesirable traffic
- Subscriber awareness
- Subscriber quarantine
- Wireless/wireline infrastructure protection.
- State-table exhaustion for firewalls/NATs (deliberate & inadvertent)
- SMS flood mitigation
- DNS server protection
- Ringtone/video/music/content/portal server protection
- Battery-exhaustion attacks (deliberate & inadvertent)
- Inbound DDoS against customers
- Outbound/crossbound DDoS/spam/scanning from botted customers

## RF Spectrum Preservation

- RF spectrum is the single most precious, expensive, and scare asset of wireless operators.
- Current industry BCPs are helpful – when we influence TCP/IP traffic via DDoS mitigation, S/RTBH, flowspec, subscriber control, we indirectly influence RF spectrum consumption.
- Integration with wireless vendor control/ management planes necessary to do more.

## Backhaul Capacity Preservation

- Backhaul capacity from wireless PoPs to backbone a major priority.
- Current industry network visibility & bandwidth control capabilities address these concerns.

## Transit Capacity Preservation

- Transit capacity ingressing/egressing mobile core a major concern as users download/upload more videos & music, do teleconferencing, play games, etc.
- Current industry network traffic visibility, traffic engineering, & bandwidth control functionality address these concerns.

## Detection/Classification/Traceback of Undesirable Traffic

- Many/most mobile operators don't have adequate visibility into their network traffic, subscriber/node behavior.
- Current detection/classification/traceback functionality addresses these concerns on the TCP/IP portion of the network.

## Subscriber Awareness

- Subscriber/device identity is key for mobile billing, for identifying compromised/abusive users/hosts, offering tiered services, etc.  Must be correlated with TCP/IP.
- The industry currently has **no standardized capabilities** in this area.
- Requires integration with management/control planes, AAA of wireless vendors & customized operator subscriber systems.

## Subscriber Quarantine

- The ability to quarantine based upon subscriber/ device identity is of great interest to mobile providers – they can already do this on the voice side, they need to be able to do it at a TCP/IP level based upon behavior.
- The industry currently has **no standardized capability** in this area.
- Requires integration with management/control planes, AAA of wireless vendors & customized operator subscriber systems.

## Wireless/Wireline Infrastructure Protection

- Wireless infrastructure is often very fragile; networks often suboptimally-designed.
- Current industry **basic** capabilities are helpful – we can perform detection/classification/traceback and block individual IPs via S/RTBH and/or flowspec.
- Wireless-specific equipment needs self-protection capabilities analogous to those on wireline equipment (e.g. iACLs, CoPP, etc.).
- BCP implementation a huge deficit, must be prioritized.

## State-Table Exhaustion for Firewalls/NATs

- Many mobile operators have installed stateful firewalls in their access networks (should be using stateless ACLs in router hardware, TCP established rules). These firewalls often perform NAT, as well.
- Compromised/abusive hosts can easily take down firewalls/NATs due to state-table exhaustion.
- Current industry **basic** capabilities are helpful – detection/classification/traceback and block individual IPs via S/RTBH and/or flowspec.
- Must do everything possible to protect firewalls/ NATs from state-table exhaustion.

## SMS Flood Mitigation

- SMS infrastructure capacity often overwhelmed by spammers, can also be a deliberate attack vector.
- Currently **no standardized capability** in this regard – can be done on an ad-hoc basis, but slow reaction times militate against this.

## DNS Server Protection

- If DNS is down, ‘the Internet’ is down for subscribers. DNS can be an attack vector and a target.
- Wireless operator DNS infrastructure often poorly-designed, non-scalable, natively indefensible.
- Current industry DNS architectural principles and DDoS mitigation capabilities can address these concerns.
- Again, architectural and operational BCP implementation is a serious challenge.

## Ringtone/Video/Music/Content/Portal Server Protection

- Revenue-generating content is becoming increasingly important to wireless operators.
- Servers/apps/services/delivery architecture often poorly-designed, non-scalable, natively indefensible.
- Customer portals for billing and for content purchases/subscriptions key in the revenue chain – poorly-designed, non-scalable, natively indefensible.
- Current industry DDoS mitigation tools (S/RTBH, flowspec, IDMS, etc.) can address these concerns.

## Battery-Exhaustion Attacks

- Host-scanning/port-scanning by botted hosts can wake up the batteries in data-capable handsets, exhaust the handset batteries rapidly due to constant invoked TCP/IP responses.
- Basic S/RTBH and/or flowspec capabilities help; subscriber-aware quarantine is needed.
- Requires integration with management/control planes, AAA of wireless vendors & customized operator subscriber systems.

## Inbound DDoS Against Customers

- Botted/abusive users/hosts tend to attract DDoS attacks – miscreants vs. miscreants
- Current industry DDoS mitigation capabilities via S/RTBH and flowspec can address these concerns.

## Outbound/Crossbound DDoS/Spam/Scanning from Botted Customers

- Outbound DDoS from abusive/botted hosts can be just as disruptive as inbound DDoS, large-scale collateral damage, infrastructure outages, DNS issues, firewall/NAT state-table exhaustion, etc.
- Current industry S/RTBH and/or flowspec capabilities are useful in this regard.
- Subscriber/RF quarantine capabilities are needed to fully meet this requirement.
- Requires integration with management/control planes, AAA of wireless vendors & customized operator subscriber systems.

## Opsec Priorities for Wireless Operators

- RF spectrum preservation
- Backhaul capacity preservation
- Transit capacity preservation
- Detection/classification/traceback of undesirable traffic
- Subscriber awareness
- Subscriber quarantine
- Wireless/wireline infrastructure protection.
- State-table exhaustion for firewalls/NATs (deliberate & inadvertent)
- SMS flood mitigation
- DNS server protection
- Ringtone/video/music/content/portal server protection
- Battery-exhaustion attacks (deliberate & inadvertent)
- Inbound DDoS against customers
- Outbound/crossbound DDoS/spam/scanning from botted customers

# Opsec Priorities for Wireless Operators – Current Industry Capabilities

- RF spectrum preservation
- Backhaul capacity preservation
- Transit capacity preservation
- Detection/classification/traceback of undesirable traffic
- Subscriber awareness
- Subscriber-based quarantine
- Wireless/wireline infrastructure protection.
- State-table exhaustion for firewalls/NATs (deliberate & inadvertent)
- SMS flood mitigation
- DNS server protection
- Ringtone/video/music/content/portal server protection
- Battery-exhaustion attacks (deliberate & inadvertent)
- Inbound DDoS against customers
- Outbound/crossbound DDoS/spam/scanning from botted customers

# Operational Security Priorities of an APAC Wireless Mobile Operator

- National operator
- ~10M subscribers, ~5M 3G users.
- 3G growing logarithmically, LTE on the horizon.
- 10 GGSNs throughout the country.
- GGSNs connected to MPLS VPN backbone owned/operated by parent company ISP.
- Multiple brands/models of firewalls, management issue.

# Opsec Priorities for Wireless Operators – Current Industry Capabilities

- RF spectrum preservation
- Backhaul capacity preservation
- Transit capacity preservation
- Detection/classification/traceback of undesirable traffic
- Subscriber awareness
- Subscriber-based quarantine
- Wireless/wireline infrastructure protection.
- State-table exhaustion for firewalls/NATs (deliberate & inadvertent)
- SMS flood mitigation
- DNS server protection
- Ringtone/video/music/content/portal server protection
- Battery-exhaustion attacks (deliberate & inadvertent)
- Inbound DDoS against customers
- Outbound/crossbound DDoS/spam/scanning from botted customers

# Self-Identified Initial Opsec Priorities for APAC Mobile Wireless Operator

- ✓ **RF spectrum preservation**
- ✓ **Backhaul capacity preservation**
- Transit capacity preservation
- ✓ **Detection/classification/traceback of undesirable traffic**
- ✓ **Subscriber awareness**
- ✓ **Subscriber-based quarantine**
- Wireless/wireline infrastructure protection.
- State-table exhaustion for firewalls/NATs (deliberate & inadvertent)
- SMS flood mitigation
- ✓ **DNS server protection**
- Ringtone/video/music/content/portal server protection
- Battery-exhaustion attacks (deliberate & inadvertent)
- Inbound DDoS against customers
- ✓ **Outbound/crossbound DDoS/spam/scanning from botted customers**

# Updated Opsec Priorities for Mobile Wireless Operator Based Upon Comprehensive Analysis

- ✓ **RF spectrum preservation**
- ✓ **Backhaul capacity preservation**
- • Transit capacity preservation
- ✓ **Detection/classification/traceback of undesirable traffic**
- ✓ **Subscriber awareness**
- ✓ **Subscriber-based quarantine**
- ➢ Wireless/wireline infrastructure protection.
- ➢ State-table exhaustion for firewalls/NATs (deliberate & inadvertent)
- ➢ SMS flood mitigation
- ✓ **DNS server protection**
- ➢ Ringtone/video/music/content/portal server protection
- ➢ Battery-exhaustion attacks (deliberate & inadvertent)
- • Inbound DDoS against customers
- ✓ **Outbound/crossbound DDoS/spam/scanning from botted customers**

## But What About Wireless-Specific Attack Vectors?

- Other than concerns about RF jamming and spectrum consumption due to attack traffic, wireless-specific attacks were not deemed to represent a significant real-world threat to most operators we interviewed.
- While they acknowledged attacks against encryption, user-tracking concerns, the dangers of rogue base stations, compromises of endpoint devices (i.e., handsets), and targeted wireless DoS against subscribers (IMSI Detach, etc.), these weren't top-of-mind.
- Well-known abuses of so-called 'Lawful Intercept' subsystems come up in conversations from time to time.
- Employees of a major mobile carrier decided to DoS the network of a rival carrier, so they filled a van with ~300 mobile phones, drove to a tower in the busiest section of town during rush hour, and hit the 'Send' button on the phones as simultaneously as possible, thus creating a control-channel flood on the BSS.
- There is lots of low-hanging fruit with regards to pure TCP/IP and the junction of TCP/IP and 3GPP to interest attackers. More exotic techniques may well be utilized at some point, but not common today.

# Internet 2022

## What Will the Internet Look Like in Ten Years?

- Largely wireless/mobile, ubiquitous and pervasive.
- The cloud is in your hand/pocket/picture frame - distributed apps/ data/services/content means everything runs/resides everywhere.
- Dynamic arbitrage of compute/memory/storage/network resources amongst fixed & mobile wireless iDevices.
- DNS ++, follow-the-X.
- Locator/EID separation - LISP++
- Everyone gets his own /48 (or equivalent) for life.
- Near-complete consumerization of IT.
- The End of Phone Numbers is Nigh.
- Ubiquitous mobile telepresence, augmented reality - holopresence on the way.
- Video increasingly synthetic, locally-generated. Less bandwidth/ session, but more sessions means overall growth.
- **Continuously, pervasively hostile** security environment.

# Conclusions

- Wireless and wireline operators **share** many opsec priorities/concerns.
- Wireless = wireline plus **wireless-specific** issues.
- Implementing BCPs brings **large benefits to wireless operators today**.
- Future integration w/wireless vendor management & control planes, AAA are a must. **RF & subscriber gaps** are critical.
- The Internet in 10 years will be largely wireless - we must understand the implications and start preparing **now**!

# Thank You!

**Roland Dobbins**
<rdobbins@arbor.net>
*Senior ASERT Analyst*
+66-83-266-6344 BKK mobile
+65-8396-3230 SIN mobile
*Arbor Public*