

# Perspectives on Wireless Security

Thomas Woo  
Bell Labs

# Vendor Perspectives

- Closing security holes require money
  - Like features, business driven
  - Cost of the security hole vs resource to close the hole
  - E.g., blue box => out of band signaling
- Vendors have control over only certain things
  - Layer 1 and 2 often out of our hands
- Regulation vs explicit mechanisms
  - E.g., encryption on calls
- Certified closed vs open device
  - Protocol violation not common
  - E.g., MobileIP in firmware
- Most effort on:
  - Upfront standards work
  - Development practice – static code analysis
  - Best security practice/system hardening – close ports, remove programs, passwords
  - Overload control

# Vendor Perspectives (cont'd)

Revenue impacting (theft of service)

>

Differentiation (blackberry)

>

User experience

- Revenue impacting
  - Infrastructure attacks are serious
  - Attacks on mobiles are less of an issue
    - Need to demonstrate widespread nature – difficult to know
    - Similar to non-mobile case
- Differentiation
  - Application layer features
  - E.g., Anti-virus, URL filtering, etc
  - Cloud-based services

# Cellular Wireless System Features

- Mobiles are not always connected
  - Detached mobiles
  - Idle mode buffering
  - Paging/tracking
  - Channel setup
- Variable channel state
- Mobility
  - Cannot enforce physical control
  - Accept foreign mobiles
  - Handoffs
    - Make and break
    - Context transfer
  - Location
- Limited resources
  - Battery
  - Processing/memory
  - Air link and processing at mobile device are expensive
    - cloud-based services
- Emerging features
  - UMA
    - Dual-mode handset for seamless service
  - Femto cell
    - Base station at home
    - Signaling into a previously closed network
    - Secure kernel

# Overload Control

- Overload control mechanisms are widely implemented in modern cellular networks
  - Crash of modern cellular network due to security attacks was never reported
- Overload mechanism design
  - Detailed traffic model providing design parameters
  - Add margin
  - Do coarse-grained proportional control (policing, pacing) to achieve graceful degradation
- Does not identify attacks and explicitly remove source of attacks
- Immune to false positives

# False Positives

- Do you stop proceeding when browser certificate is invalid?
- An IPS can generate thousands of alerts per hour
- Most systems are not used because it generate too much information to be useful
- Root cause analysis, correlation are more important as detection

# Current Issues

- Mobiles will behave more like data end points
  - CS domain is gone in all 4G
  - 4G is a more promising area
- Most pressing security issues
  - Are not wireless specific, but simply have much higher impact in wireless
  - Are not academically interesting
  - Examples:
    - System hardening
      - Configuration auditing
    - Mobile compromise
      - Quarantine
      - Recovery
    - Network control
      - P2P
      - Streaming
    - Secure and flexible charging/billing
    - Scalable security gateway
- Positives
  - Wireless bandwidth is still small, can afford to do packet level analysis
  - Tracking of all sessions is possible
- Negatives
  - Most service providers are conservative and reactive

# ALU Non-stop Laptop Guardian

- Problem: allow enterprises to overcome the "mobile blind spot" by managing their laptops anywhere, any time, even when the laptop is turned off
- Solution: utilizes a unique Mobile Broadband connection card that serves as a two-factor authentication device. The card itself is an ignition key; the user must insert the card into the laptop to gain access to his/her laptop. The same card can be controlled by an enterprise IT administrator to remotely revoke authentication privileges always rendering control over the laptop and, more importantly, the corporate data on the laptop.
- Awards:
  - Internet Telephony - 2007 Product of the Year Award
  - Info Security Products Guide - 2008 Outstanding Products Awards Best Wireless/Mobile Product Customer Trust Award
  - Information Security(TM) magazine and SearchSecurity.com 2008 Readers' Choice Awards
- Sprint is a big customer

# ALU 9900 Wireless Guardian

- Problem: enhanced carrier visibility in third-generation (3G) and emerging 4G networks
- Solution: Tracks the impact of individual subscribers and their applications on the performance of the network. Forensics allow administrators to track and analyze the root cause of any specific event. The device is located at the core and uses network protocols such as Radius and MIP to obtain the performance data it needs. It looks at every packet from within the core and relate that in real time to the radio access network
- Awards:
  - winner of CTIA WIRELESS 2008 Wireless Emerging Technologies Awards as best product in two separate categories
    - 4G - Service Management
    - Network Infrastructure for Wide Area Networks
- Tian Bu, Samphel Norden, Thomas Woo: “Defending against novel DoS attacks in 3G Wireless Networks” (withdrawn)