R2, "Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks"

1) Target system and service

- applicable to all handsets running vulnerable protocol stacks, but mainly focused on smartphones which has a application processor and a baseband processor
- Apple iPhone 4 (using a Comneon stack on an Intel chip) and the HTC Dream (using a Qualcomm stack and chip)

2) Vulnerability

- the primary criterion for network reception is signal strength
- GSM does not provide mutual authentication
- memory corruption vulnerabilities (mostly stack buffer overflows)
- insufficient verification of input parameters transmitted over the air interface can lead to remotely exploitable memory corruptions in the baseband stack
- Insufficient length checks usually resulted in data on the heap or on the stack being overwritten, which can be leveraged by an attacker to gain control over the execution flow
- Object/structure lifecycle issues such as use-after-free bugs or uninitialized variables
- other vulnerabilities like integer overflows/underflows and memory information leaks

3) Exploitation

- The attacker operate a rogue Base Transceiver Station (BTS) in vicinity to the targeted Mobile Station (MS)
- the BTS sends out system information messages announcing the availability of a network that the targeted mobile station is willing to connect to.
- The MS will connect to attacker's BTS if transmits a stronger signal than the legitimate base station
- Once the attacker has control over the baseband. he may operate microphone, camera, place calls, send SMS, etc.

4) Evaluation and experimental method

- reverse-engineered smartphones to extract firmware images and baseband software
- used a modified Ettus Research USRPv1 together with 2 RFX-900 daughterboards
- The USRP is connected to a Thinkpad X60 with a Core Duo CPU @1.6GHz that runs OpenBTS 2.6
- test target operation: turning on auto-answer
- HTC Dream: exploited AUTN stack buffer overflow that overwrites the program counter and the register R0 -> result: auto-answer enabled without the user being able to notice anything
- Apple iPhone 4: A LOCATION UPDATING REQUEST is sent by the phone as soon as it connects to fake network to which OpenBTS will send the malformed LOCATION UPDATING ACCEPT -> result: auto-answer was enabled and the phone briefly lost connectivity to the network

5) Defense

- confirm length check
- require mutual authentication (always check to which network the phone is connecting every time it builds connection)

- disable execution of remote application or notice the user using sound or display
- some overflow issue should be patched by phone and chip vendors
- block reverse engineering of baseband to hide existing bugs or overflows

6) Future work

- vendors should fix the overflows (for example, the TMSI overflow was fixed in the baseband firmware shipped with Apple's iOS 4.2 and AUTN overflow has been patched in Qualcomm's tree)
- 3G stacks may be vulnerable to similar memory corruption problems even though they require mutual authentication
- baseband operating stacks should undergo a systematic and continuous code audit and use hardening options
- privilege-separation is needed for establishing well-defined boundaries between the different portions of a baseband stack