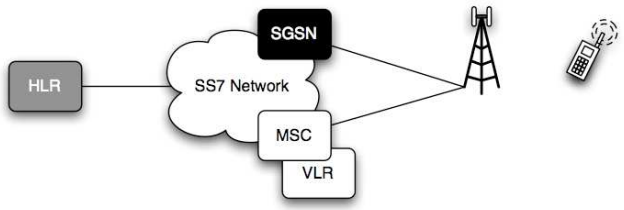
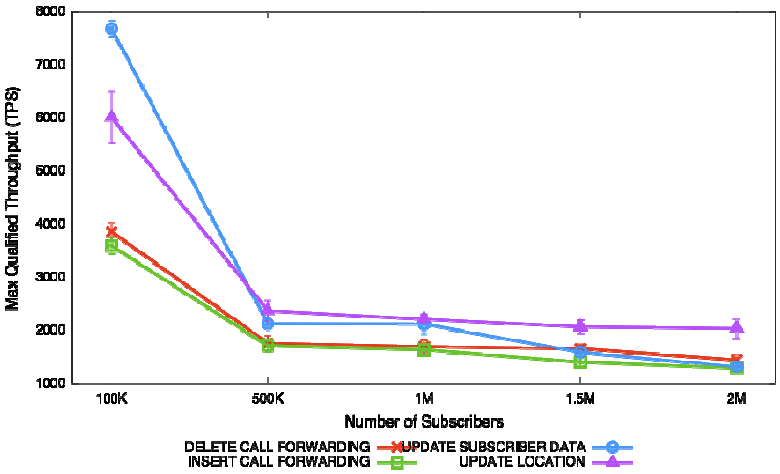
# Bringing Down the HLR

Patrick Traynor†, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, Thomas La Porta
†College of Computing, Georgia Tech

Cellular core networks are a vital part of our national infrastructure. A successful attack on a service provider's HLR (Home Location Register) could interrupt cellular service for the entire nation. Core networks are protected through separation; public access to the HLR is only possible through the cellular network, where devices have traditionally been limited in both capacity and design. Recent advances in handset technology have opened the doors to the possibility of large-scale attacks from handsets. This work explores the potential impact a handset-originated attack could have on the HLR. We use simulation and real world testing to construct an attack that can potentially reduce transaction processing at the HLR by 80%.

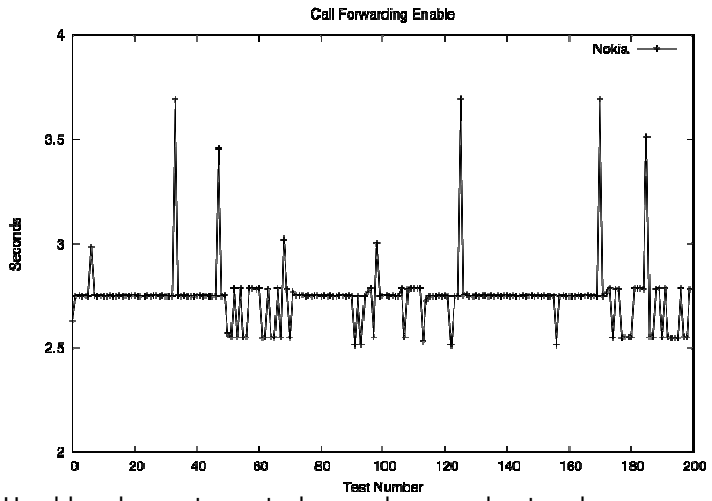



## TM1 Simulation




- HLRs are massive databases that act as central repositories for all subscriber data in cellular networks.
- High transaction performance is essential to maintaining a usable network.
- Needed baseline HLR performance benchmark to determine effectiveness of our attack.
- Used TM1, a telecom industry-standard database performance benchmark, to characterize the performance of an HLR under normal operating conditions.
- Found that overall HLR performance depends greatly on the transactions being processed and the number of subscribers.

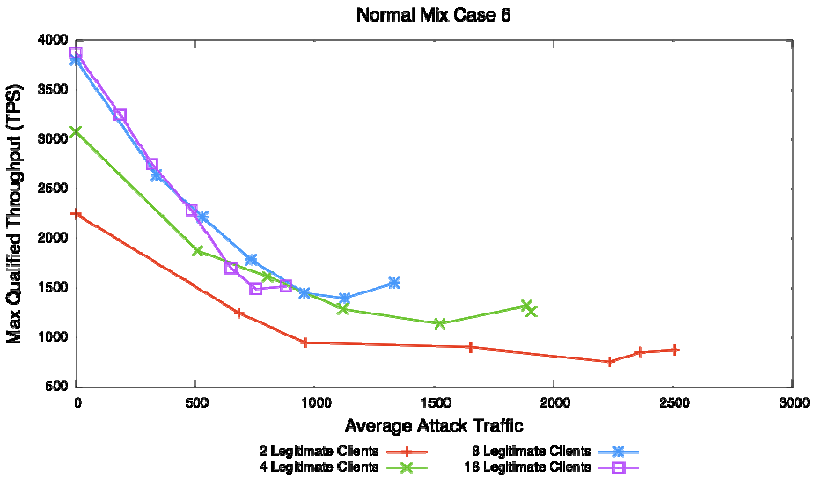
## AT Commands




- Used by phones to control core phone and network functionality.
- Provide a standard means of communication between the phone and the network.
- Correlation between TM1 transaction types and AT commands.
- Tested AT command response time performance on real cellular network
- Chose AT commands based on TM1 transactions and expected response time
- Based on our tests with TM1 and AT commands, we chose *call forwarding enable* to be the command used in our attack

## Formulating an Attack

- Attack is based on thousands of compromised phones spread over a wide geographic area
- Phones use AT commands to send specific requests to the HLR, in this case *call forwarding enable*
- The cumulative effect of such a large number of high-cost requests hitting the HLR will cripple its performance
- Simulated attack using TM1
- Ran a baseline transaction mix on the HLR then injected massive amounts of attack traffic
- HLR performance dropped sharply as attack traffic increased
- Performance plateaued, then rose again due to attack traffic contention
- Affected performance by 80% in the worst case
- Ongoing work with the in-memory database SolidDB




Supported by Sprint