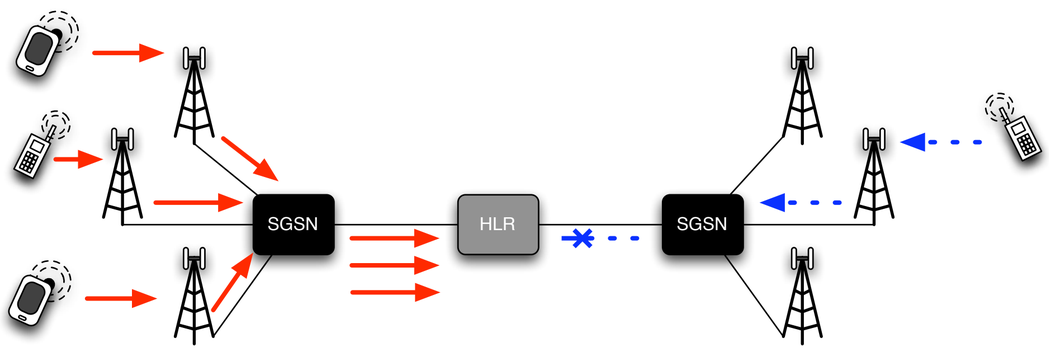
On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core

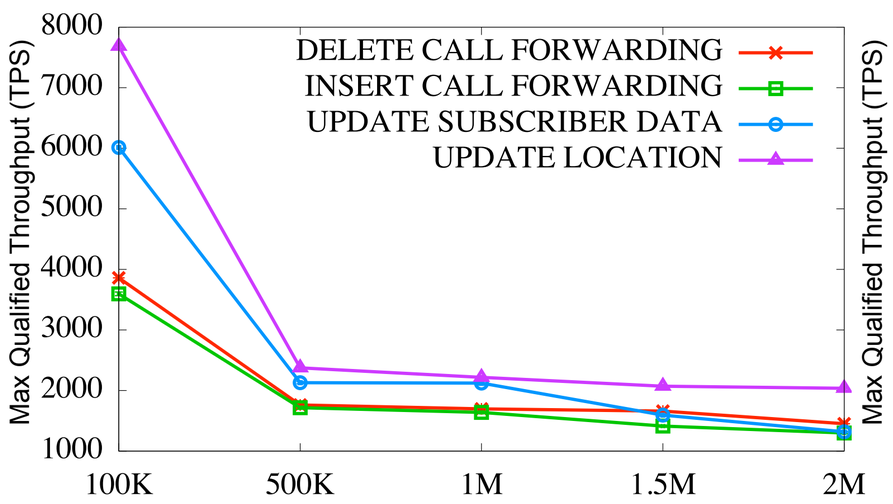
Patrick Traynor†, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger,
Patrick McDaniel, Thomas La Porta
†College of Computing, Georgia Tech

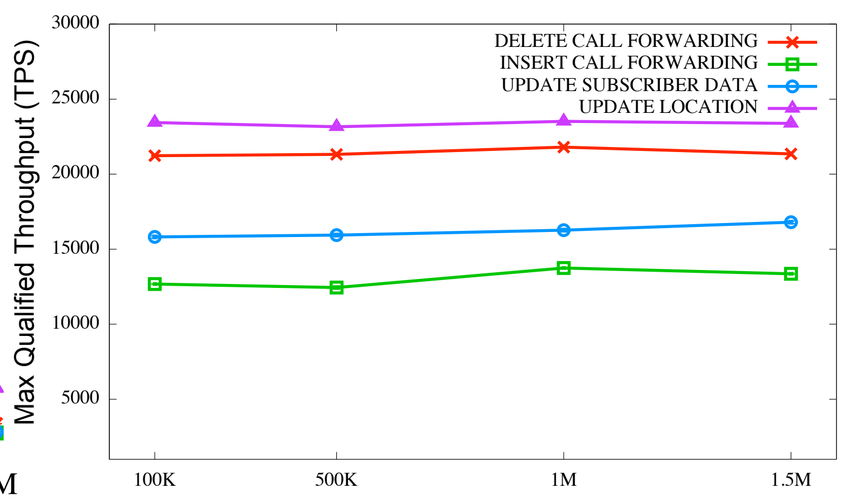
The expansion of interconnectivity with the Internet and the evolution of highly capable, but insecure, mobile devices threatens cellular networks. We characterize the impact of the large scale compromise and coordination of mobile phones in attacks against the core of these networks. A botnet composed of as few as 11,750 compromised mobile phones can degrade service to area-code sized regions by 93%. As such attacks are accomplished through the execution of network service requests and not a constant stream of phone calls, users are unlikely to be aware of their occurrence. We investigate a number of significant network bottlenecks, their impact on the density of compromised nodes and how they can be avoided.

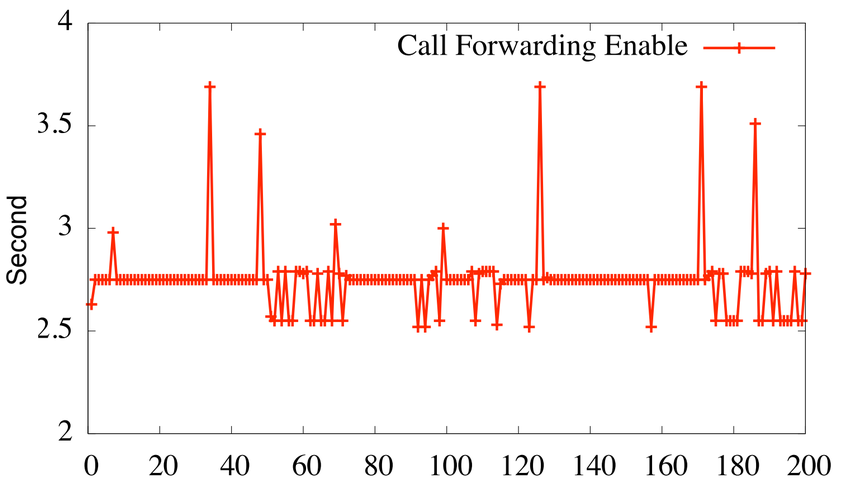


Characterize HLR Performance & Profile Network Behavior

- HLRs are massive databases that act as central repositories for all subscriber data in cellular networks.
- To prevent legitimate users from using the network, attack HLR
- Need to quantify performance impact caused by the invocation of the range of services provided by an HLR.
- Used TM1, a telecom industry-standard database performance benchmark, to characterize the performance of both MySQL HLR and SolidDB HLR under normal operating conditions.
- Found that overall HLR performance depends greatly on the transactions being processed and the number of subscribers.



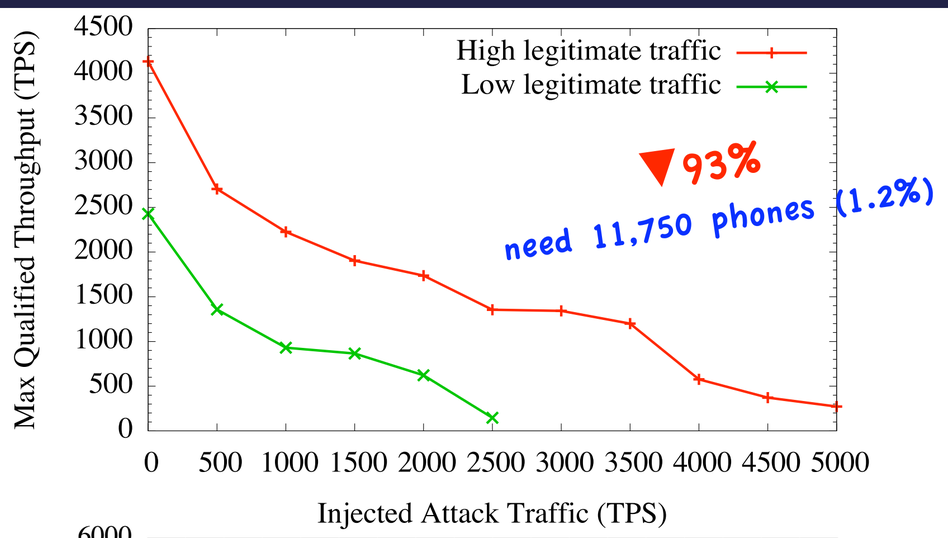


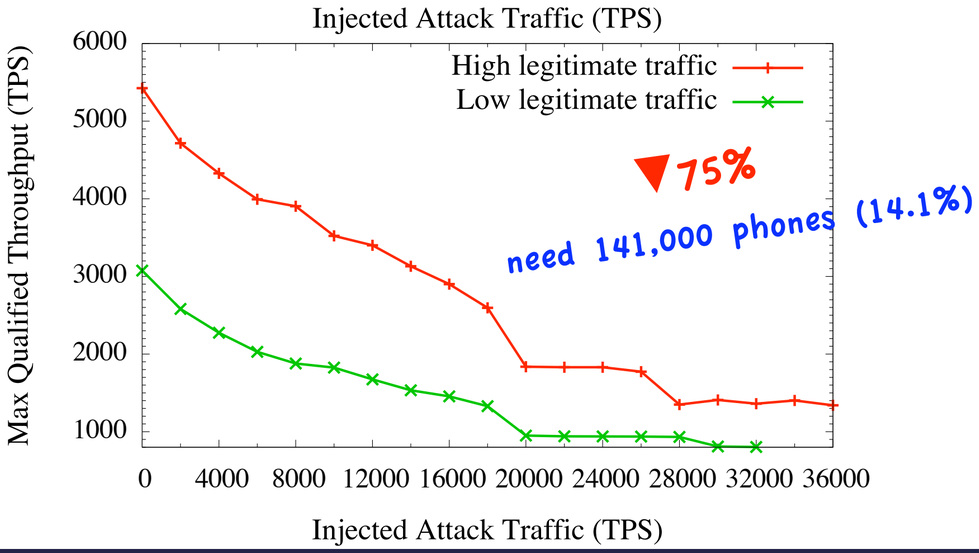


- We injected and measured service requests representing each of the four write-based meta-command on a live cellular network
- AT commands are meta-commands used as a standard means of communication between the phone and the network.
- Correlation between TM1 transaction types and AT commands.
- Tested AT command response time performance on real cellular network

From the experiments with both TM1 and AT commands, we chose *call forwarding enable* to be the command used in our attack

Attack Characterization





Other Considerations

- Consider RACH capacity and SDCCH limitations, we need dispersed compromised phones to avoid contention, e.g. distributed over 375 base station for MySQL HLR and 2,252 base station for SolidDB HLR.
- Command & control channels for coordinating the actions, e.g. internet coordination, local wireless coordination, and indirect local coordination.

Attack Mitigation

- Filtering -- can be tuned work but still with concerns on false negative. Filtering at the core network may be too late to prevent users from experiencing significant congestion.
- Call gapping -- investigate shedding rules that mitigate specific attacks and not simply benign elevated traffic conditions
- It is still challenging for network providers to address a more dynamic attacks especially to separate attacks from other traffic.

Supported by the NSF