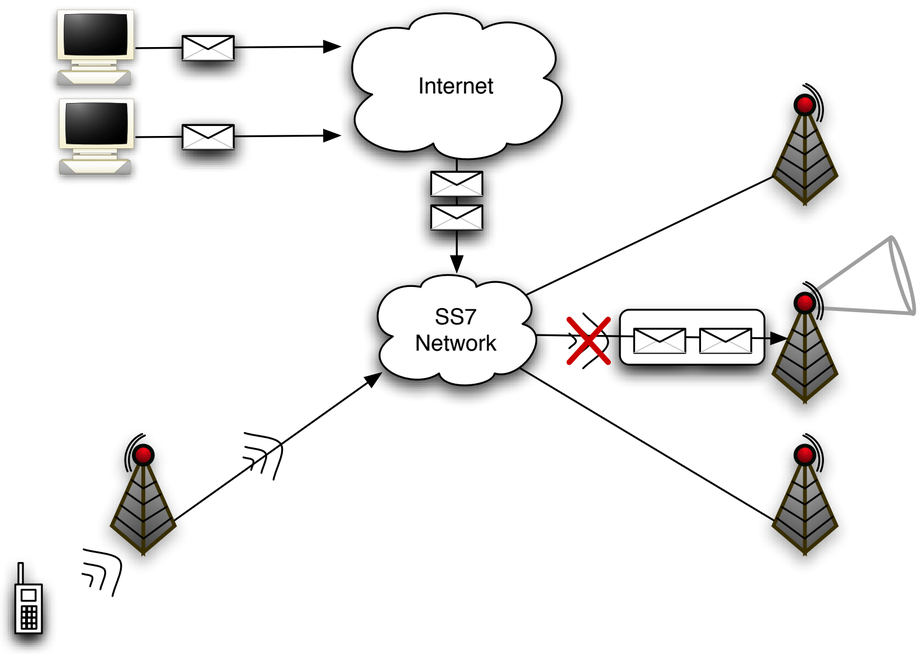
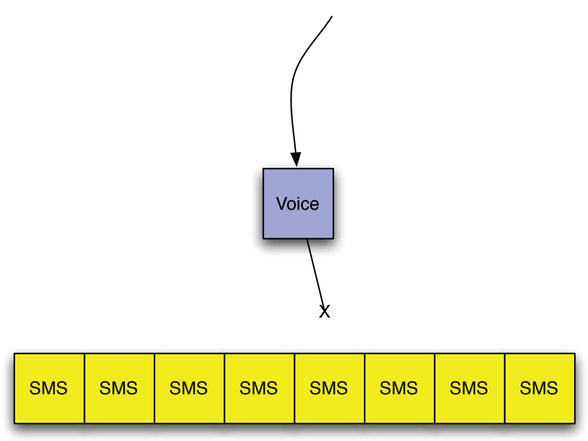
Exploiting Open Functionality in SMS-Capable Cellular Networks

Patrick Traynor, William Enck, Patrick McDaniel, Thomas La Porta

Cellular networks are a critical component of the economic and social infrastructures in which we live. In addition to voice services, these networks deliver alphanumeric text messages to the vast majority of wireless subscribers. To encourage the expansion of this new service, telecommunications companies offer connections between their networks and the Internet. The ramifications of such connections, however, have not been fully recognized. We evaluate the security impact of the SMS interface on the availability of the cellular phone network. Specifically, we demonstrate the ability to deny voice service to cities the size of Washington D.C. and Manhattan with little more than a cable modem. Moreover, attacks targeting the entire United States are feasible with resources available to medium-sized zombie networks.

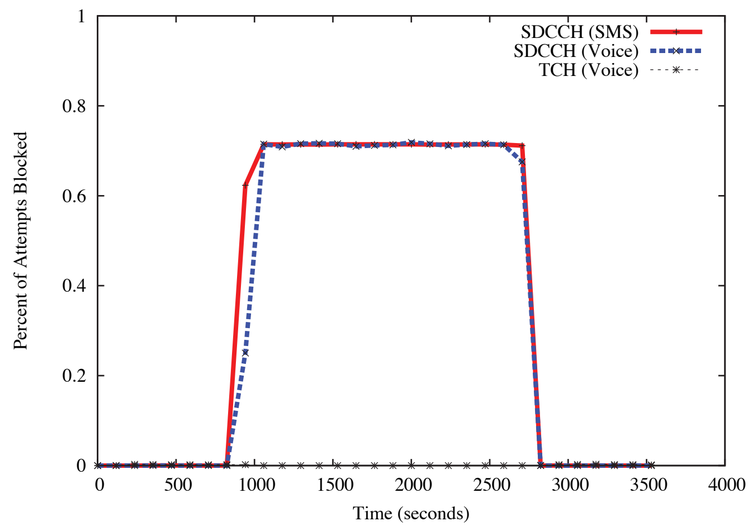


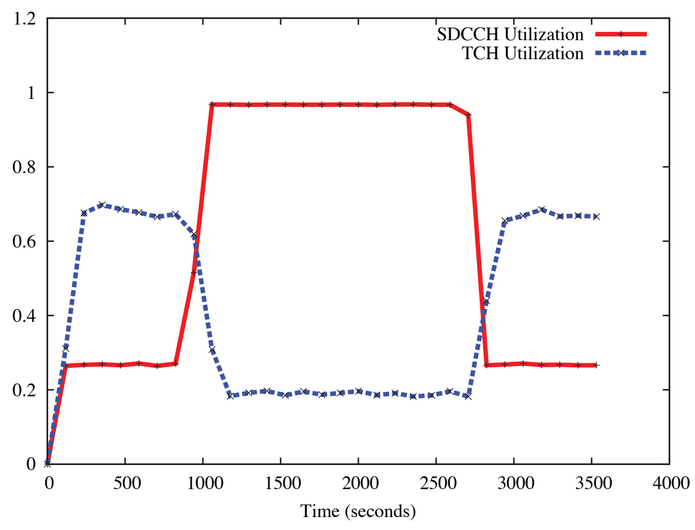
Shared Channels



- Voice Calls and Text Messages share a number of common channels.
- The *Standalone Dedicated Control Channel* (SDCCH) is a low bandwidth bottleneck used for call setup and message delivery.
- By filling this channel with superfluous messages, an attacker can prevent legitimate calls and messages from being delivered.

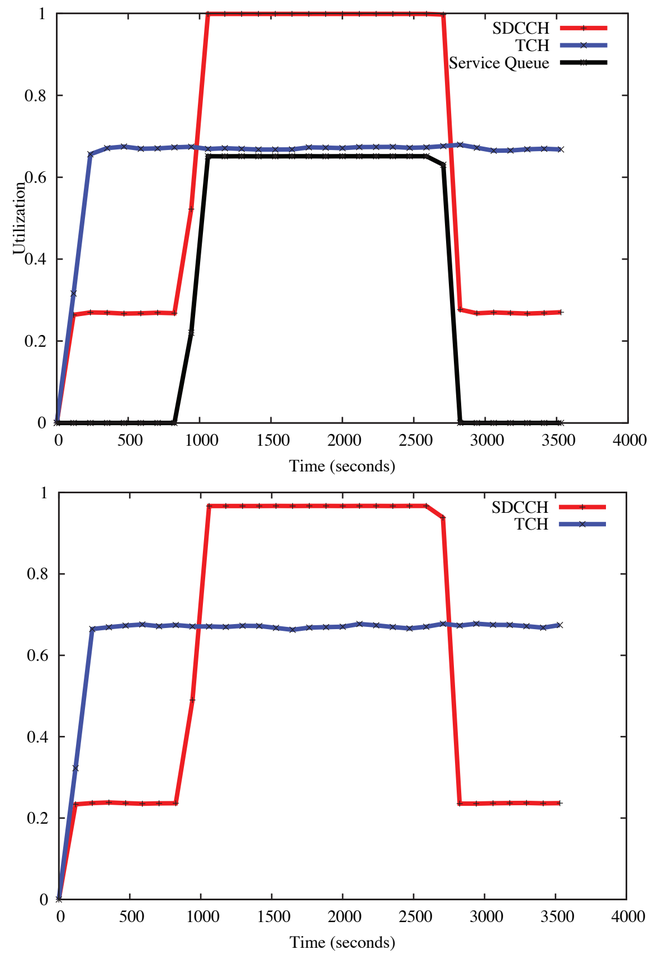
Characterizing Attacks

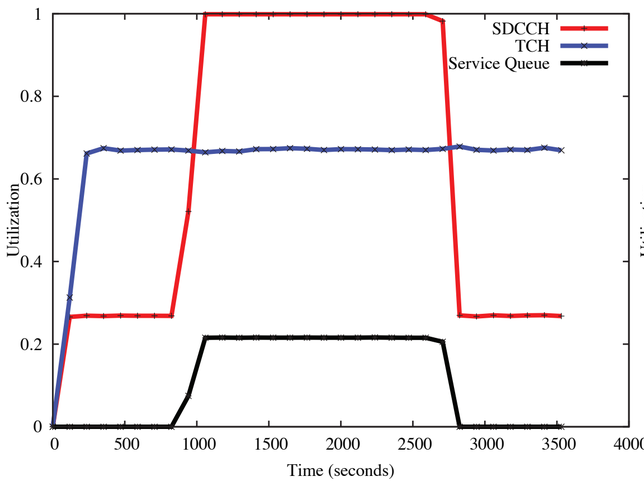


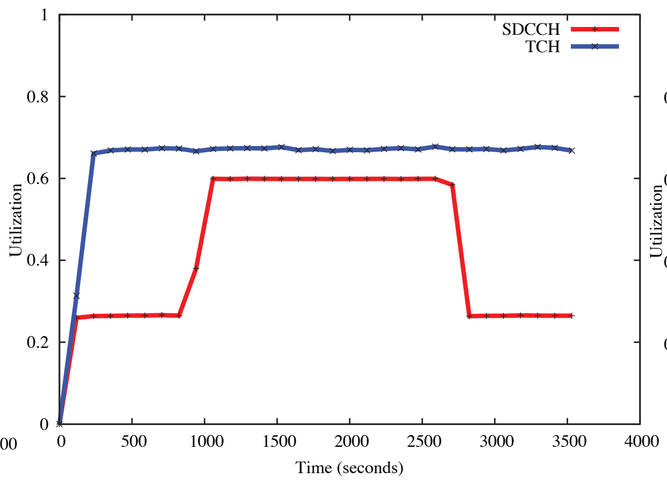


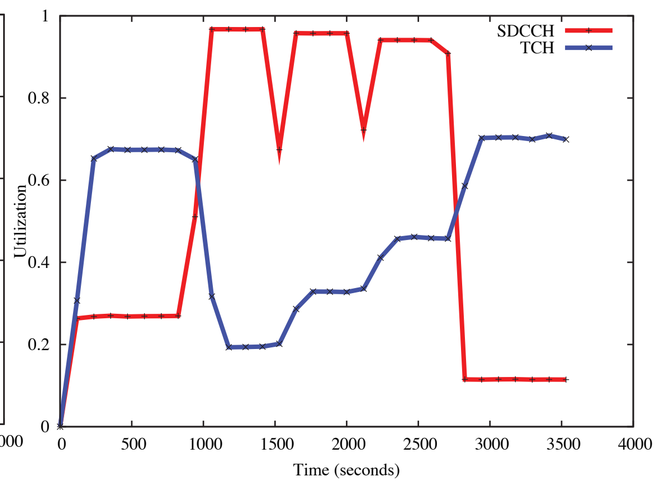
- We have developed a simulator that allows us to characterize and visualize targeted SMS attacks.
- Our simulator is designed according to publically available specifications (e.g. 3GPP) and parameters (e.g. NCS, US Census)
- On the left, a blocking rate of over 71% for all incoming SMS and voice calls is observed for a rate of 9 messages/sector/second.
- On the right, the effects of the attack over time can be observed. Notice that *traffic channel* (TCH) utilization drops significantly during the attack.

Developing Countermeasures









- We develop five strategies to prevent such attacks from occurring: *Weighted Fair Queueing* (WFQ), *Weighted Random Early Discard* (WRED), *Strict Resource Provisioning* (SRP), *Dynamic Resource Provisioning* (DRP) and *Direct Channel Allocation* (DCA). (left to right)
- Each strategy experiences varying tradeoffs in attempting to provide high fidelity for both SMS and voice services.

Publications

P. Traynor, W. Enck, P. McDaniel and T. La Porta, **Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks**, Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom), September 2006.

W. Enck, P. Traynor, P. McDaniel and T. La Porta, **Exploiting Open Functionality in SMS-Capable Cellular Networks**, Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS), November 2005.

Future Work Sponsored by Raytheon