Research Challenges in Cellular and Mobile Network Security

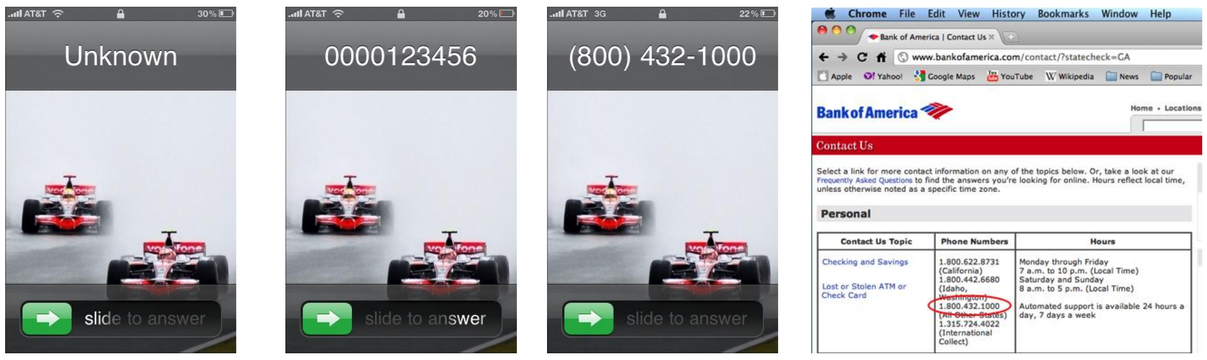
Assistant Professor Patrick Traynor

Georgia Tech Information Security Center (GTISC)

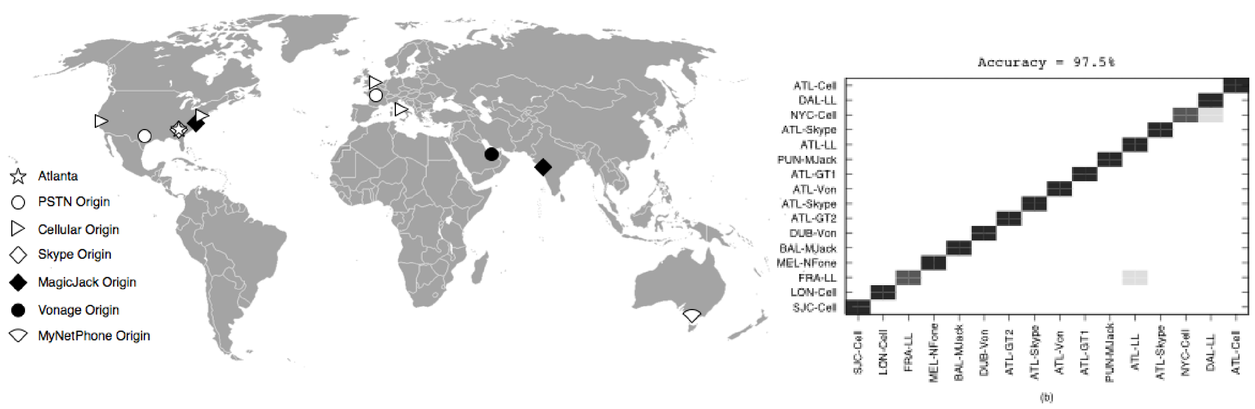
The security of cellular systems has long relied on their closed nature and trust in the honest behavior of users. However, because of their recent integration with the Internet and introduction of highly capable mobile phones, these assumptions no longer hold true. Given that these systems provide connectivity to well *over five billion subscribers* around the globe and represent the only reliable critical infrastructure available to the majority of those people, the need to protect these systems is an absolute imperative. This poster offers highlights of our work in this space.

Authenticating Callers

•Caller ID informs a receiver of the source of an incoming phone call.
•Unfortunately, such data is *asserted* and *not authenticated*, making it easy for an attacker to trick potential victims into believing their false identity.



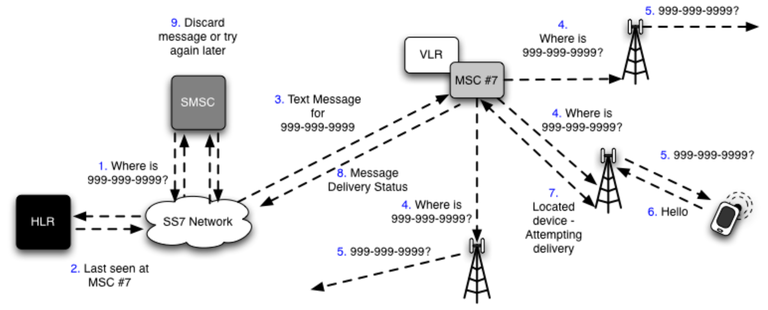
•Instead of Caller ID, we instead identify the source of a call by its provenance, or the path it took between sender and receiver.
•We do this by detecting and quantifying audio artifacts (e.g., spectral clarity, packet loss) at the receiver end.
•Performed a world-wide study to determine if such information could distinguish between phones.



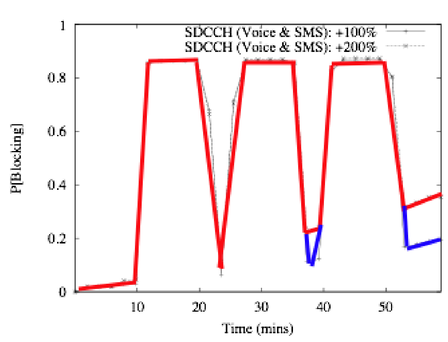
•With three training messages from each phone, we could identify the call source with greater than 97% accuracy.
•Our techniques are not caller specific – instead, they characterize the path!

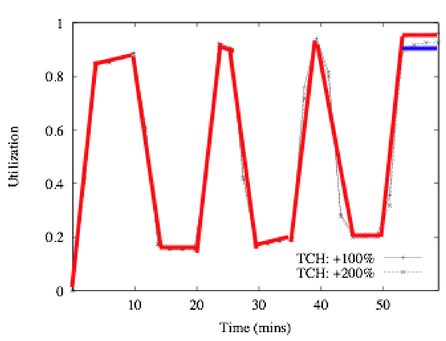
Emergency Management

•Text messaging has become the dominant means of communication
  ○ 3 billion calls vs 4.2 billion SMS in 2009!
•Because of availability during previous disasters (e.g., 9/11/2001, Hurricane Katrina), many vendors have started selling systems to send alerts via text message during emergencies.
•Messages are (ideally) delivered as shown below:



•Unfortunately, cellular networks were never built to provide high volume service across highly-localized users.
•Introducing this large number of messages into the network causes overload, which results in *blocking rates of greater than 80%*.
  •These networks generally have less than 1% blocking rates.
• These “alert” messages actually make it *much more difficult* for people in trouble to make calls/send messages!





•Priority messages will not solve this problem – the issue is that we are using a point-to-point technology to perform broadcast communications.
•Continuing efforts: Working with providers to develop and deploy efficient broadcast SMS for use in these scenarios.

Securing Mobile Browsers

•The majority of users will access the Internet through their mobile phones in the near future.
•Given the dramatic differences between the desktop and mobile phone displays (e.g., space, interaction methods, etc), *what are the security differences between mobile and desktop browsers?*
•Given that mobile browsers often share the same names and rendering engines, *should we expect there to be any differences?*

•The differences are dramatic:
  ○Most mobile browsers fail to implement strong display security policies found in desktop systems.
  ○Usability clashes with other implemented policies, making other attacks easier.
•Demonstrated attacks include phishing (left), click-jacking and login CSRF.
•Many other problems likely exist!