Editors: Patrick McDaniel, mcdaniel@cse.psu.edu
Sean W. Smith, sws@cs.dartmouth.edu

Securing Cellular Infrastructure

Challenges and Opportunities

PATRICK TRAYNOR
Georgia Institute of Technology

Cellular networks are undergoing their most radical transformation since their initial deployment in the early 1980s. Long characterized by their physical separation from other networks and well-defined but limited functionality, providers are now offering an array of data services, including high-speed mobile Internet access.

Such services' expansion is pivotal. Whereas the Internet boasts just over one billion users globally, roughly four billion people rely on cellular networks every day. Accordingly, these networks represent the only digital systems the vast majority of humanity will ever use. As both mobile devices and the communications infrastructure become increasingly capable of supporting a wide range of applications, the next great Internet expansion will be unlikely to come through any other interface.

Although deploying increasingly capable cellular networks can offer enormous positive technical and social benefits, it also raises several security and privacy issues. From mobile phones that more closely resemble general-purpose computing platforms than the dumb terminals of the past to the transition from the Signaling System No. 7 (SS7) to the IP Multimedia Subsystem (IMS), these new systems are vulnerable to a wide range of new attacks. I look at several of the issues resulting from this increasingly critical infrastructure and the challenges in addressing them. (For details on current cellular network architectures, see G. Bertrand, "The IP Multimedia Subsystem in Next Generation Networks," www.rennes.enst-bretagne.fr/~gbertran/files/IMS_an_overiew.pdf.)

Evolving Infrastructure

To support the vast expansion of services available to cellular customers, service providers are in the process of deploying an entirely new network core. The IMS is based on IP networking standards, and the shift from a largely circuit-switched architecture to an IP-based one not only simplifies fixed-mobile convergence (that is, integration with the larger Internet) but also significantly reduces the costs of building and maintaining such systems. All traffic in these networks, whether voice (via the Session Initiation Protocol [SIP]), signaling, or data, flows over the same links. Many large providers have already replaced portions of their core with this new technology, but no clear timetable exists as to when all operators will have converted entirely to IMS. Consequently, providers must currently manage a hodgepodge of technologies, from IMS and traditional SS7 to SS7 over IP.

One of the biggest challenges these networks face is the loss of separate signaling and data channels. Thus, adversaries—whether attached to the network via cellular connect cards or an infected phone—are more likely to be able to disrupt normal operations. For instance, the ability to transmit arbitrary (that is, malicious) messages to any *call session control functions* (CSCFs), which are responsible for handling most signaling requests, might let an attacker arbitrarily eavesdrop or redirect much of the network traffic.

These threats become more critical in the context of provider trust models. The SS7 network, for instance, was designed under the assumption of a closed environment in which the provider maintained total control. Because the risk of an external adversary or a malicious neighboring provider injecting control messages into the core was so low, cryptographically authenticating core signaling messages wasn't believed to be necessary. Although standards now exist for authenticating control messages between core nodes, experiments within our lab at the Georgia Institute of Technology found that, similar to commercial SS7 systems, carrier-grade IMS systems aren't configured to use

such authentication by default. Therefore, an adversary might be able to launch significant attacks on the signaling infrastructure that can affect communications' integrity, confidentiality, and authenticity. Such attacks might be possible without necessarily compromising a CSCF or applications server within the network.

Although we've yet to see the widespread outbreak of malware targeting mobile phones, the traffic such an event would generate could unintentionally knock out service to an area before it ever achieves its ultimate goal.

Device Challenges

The development of highly capable mobile phones also introduces a range of security issues for providers. Malware that targets phones has received the most attention to this point, although we've yet to see a true large-scale outbreak. However, the mechanisms these networks require to support such devices might make applications programmers a significant threat to normal operations.

This issue is best illustrated by the recent release of a Skype voice-over-IP (VoIP) client for the iPhone. Many bloggers were openly critical of this application because it supported VoIP calls only over Wi-Fi—and not via the provider's 3G network. Cries of conspiracy to force customers to purchase additional airtime quickly littered message boards and chatrooms. However, the real cause lies within the design of the scheduling algorithms for the wireless portion of the network.

Engineered with battery life in mind, these algorithms are built to deliver rapid bursts of data followed by long periods of silence, letting mobile devices quickly return to a state in which the cellular radio is inactive. Although Web browsing and email certainly fit these characteristics, applications with interactive requirements, such as video conferencing, generally don't. Accordingly, not only would the communications' quality for the device's user suffer, but so too would the experience of other users in the same cell.

Providers are observing the effects such applications have on their networks. Laptop users connecting to P2P networks such as eDonkey have significantly degraded entire cells, accidentally making data service virtually unavailable to other users. Other providers have noted similar problems from laptops infected with spyware. Although we've yet to see the widespread outbreak of malware targeting mobile phones, the traffic such an event would generate could unintentionally knock out service to an area before it ever achieves its ultimate goal if the author fails to understand how such networks operate. Antivirus services could offer some relief, but their waning success against increasingly sophisticated malware in the desktop environment, coupled with the challenges of battery limitations, make such solutions incomplete.

Wireless issues aside, the need to support mobility also creates significant challenges for the core network infrastructure. Imagine the increased load on Domain Name System root servers if domain-level resolvers couldn't cache their results. Consider how firewall rulesets might need to be dynamic based on which devices are currently located within a specific subdomain. From a corporate asset protection perspective, it also isn't clear how individual mobile phones will be firewalled so as to match the policies required by a given company.

Privacy Expectations

The expectation of privacy in the telecommunications world has always been high. Legal interception, whether eavesdropping on a conversation or simply obtaining a record of incoming and outgoing calls, has traditionally required a judge's permission. However, network and user devices have evolved, challenging our understanding and expectations of privacy in this environment.

One important change is in how voice is transported through the network core. As much of the network is converted to IP-based links, voice traffic will frequently traverse the same channels as data. Because we can consider packetized voice as merely a type of data traffic, some law enforcement agencies have argued that the stringent requirements for legal interception no longer apply. The implications of such logic are enormous. Cellular phones are posed to pass the desktop as the platform of choice for personal computing, yet governments might afford privacy to almost no action in these networks.

Phones themselves are likely to become a source of sensitive information leaks. The International Mobile Equipment Identity (IMEI), a unique identifier for every mobile device, represents one such threat. Similar to the controversy surrounding the Intel Pentium III's processor serial number, IMEI use would let those observing it track individual users across all applications and transactions—think of it as the ultimate unerasable cookie. Although Apple was incorrectly accused of sending such information from the iPhone in 2007, it's not impossible to believe that other applications will try to use such an identifier to manage users in the future.

Whereas owning wiretapping

equipment targeting traditional wired telephony systems is illegal for private citizens, several companies now legally sell smartphone eavesdropping software. Such software can record voice calls and location, text messages, visited Web pages, and received email messages without any user approval. Absent legal intervention, there's no reason to believe that socially motivated wiretapping won't become a more regular threat.

The legal battles surrounding all these points are looming—we'll no doubt begin hearing about them in the near future.

The Future of Communication

A colleague of mine recently visited India and planned a side trip to see the Taj Mahal. On his drive south from New Delhi, he observed numerous local farmers moving tremendous mounds of straw from their fields to the market. Dressed in traditional clothing and riding atop mule-drawn carts, these hard-working individuals were doing their jobs the same way their families had done for many centuries, with one important difference—they were all carrying cell phones. As his driver explained, farmers used to take their goods to the market only to find an overabundance of the product they were trying to sell. Worse still, customers at many other markets were unable to get these same products, leading to significant hardships. Cell phones now help prevent such incidents—not only can farmers learn where they can get the best price for their goods by knowing exactly where they're needed, but consumers can purchase those goods with increased regularity. This phenomenon is by no means limited to India.

New efforts from any one community won't solve the challenges facing cellular networks. Significantly improving security in this space will require government assistance and strong partnerships between academia and industry. Particularly critical are efforts to allocate spectrum for radical experimental research, reinforce the right to privacy, develop mobile phone operating systems aware of wireless network characteristics (so as to prevent malicious or poorly designed applications from causing outages), and create independent testbeds in which we can evaluate security threats and countermeasures.

When Africa truly comes online, cellular data networks will be the conduit. As markets in Southeast Asia become directly reachable for Western businesses, mobile phones will be the platform by which people will conduct their transactions. Even in industrialized countries, where wide swathes of the population are already abandoning traditional landlines in favor of cellular-only communications, the need for the security community to address these systems grows daily. How we respond to these challenges will greatly influence how well you can hear me now and in the future. □

Patrick Traynor *is an assistant professor in the School of Computer Science at the Georgia Institute of Technology. His research interests include network and systems security, telecommunications, and applied cryptography. Traynor has a PhD in computer science and engineering from the Pennsylvania State University. He's a member of the ACM, the IEEE, and Usenix. Contact him at traynor@cc.gatech.edu.*

Interested in writing for this department? Please contact editors Patrick McDaniel (mcdaniel@cse.psu.edu) and Sean W. Smith (sws@cs.dartmouth.edu).