Alcatel·Lucent

STRATEGIC WHITE PAPER

Top Threats to Mobile Networks – and What to Do About Them

Mobile network operators are experiencing increased traffic as laptops become more portable and cell phones and other wireless devices add power, features and functions. The downside is that the growing population of mobile users taking advantage of voice, video and data services are drawing the attention of hackers, eavesdroppers, and other malefactors.

By understanding the growing number of threats to their networks and what countermeasures to take to minimize security risks, mobile operators can protect their customers and their networks against many of the attacks that inevitably will take place. This white paper describes the most common attacks on mobile networks and what to do about them.

Table of Contents

Introduction

Cellular networks continue to adopt new technologies to provide subscribers with faster, more flexible access to a broad spectrum of cellular based services. Security has been a constant driver throughout this process, prompting the evolution of the solutions that use a self-healing approach.

When early cellular networks were being deployed worldwide, individuals using frequency scanners were able to listen to phone calls. Understandably, the public confidence in the confidentiality of their calls was quite low. The solution came in the form of legal changes and modifications to the technology itself. For example, in the US, new laws were passed making it illegal to monitor cellular communications, radio scanners were manufactured with additional restrictions in the 800 MHz band, and cellular equipment manufacturers added encryption support to protect communications.

Today we are living a new chapter in the history of cellular network security–increasing numbers of operators are offering data services to their customers, and more importantly, the cost of these services continues to drop. In some countries, mobile data services are starting to compete with broadband services offered by DSL and cable service providers. Subscribers are able to purchase a relatively inexpensive USB wireless modem and pay for the service on demand (pay as you go or prepaid).

With this new flexibility, users have relatively inexpensive access to the technology, and, without a monthly contract, also have the advantage of anonymous access. Low cost access attracts a higher number of new users, while anonymity clearly affects security. Since the introduction of Internet dial up, every user has been linked with a physical medium such as a telephone line, DSL, or cable connection. Even semi-public access sites, such as universities and libraries, have the potential of recording the specific source of communications over the Internet.

WiFi, and now mobile networks, allow users to connect from a relatively wide coverage radius. In the case of mobile networks, the user is able to connect from any point where there is cellular coverage. Finding the exact location of a specific user requires special equipment, and a very rapid response when searching for them.

Mobile operators offering data services to their subscribers face a number of threats from anonymous users who intend to abuse the service and its network. There are a number of typical threats to third parties such as spam, hacking of third party sites, copyright infringement, and illegal communications. Mobile operators are not accustomed to dealing with these threats. However, solutions have been developed by Internet service providers (ISPs) that are relatively simple to deploy into the mobile environment.

New challenges continue to appear related to the mobile network environment. DSL and cable ISPs use relatively high available bandwidth. As a result, it is difficult to crash or otherwise impact the normal operation of the network. On the other hand, compared to DSL and cable networks, mobile networks have reduced bandwidth and are more vulnerable to infrastructure related attacks. As with any new network or mobile connectivity service, operators must pay special attention to the initial customer experience – customers can easily compare the mobile network's operation against their experience with other services, such as wired and WiFi. In order to gain market share and maintain a low churn rate, the operator must ensure a high quality of service and consistent customer experience at all times.

Initial CDPD offerings by 1G operators, and subsequent rollouts of GPRS, EDGE, CDMA, and 3G services such as CDMA EV-DO and UMTS/HSDPA,[1] create an all IP-based environment that makes it easier to attack the infrastructure. Attackers have readily available tools to assault these networks, and with the availability of USB modems for 3G access, they have a simple path to threaten any mobile network. Data flows are difficult to analyze and even valid connections can pose a threat – for example, when too many requests are sent legitimately.

There is an additional threat to external networks that are now allowed to connect with systems within the mobile network. Previously, these networks were closed to data connections from the outside. These new connections have to be verified – stateful inspection is required to prevent unauthorized packets from flowing into the network.

Different Kinds of Attacks

Threats to mobile networks include, but are not limited to, information confidentiality, data integrity, and service availability. Below are various types of attacks.

TRADITIONAL IP NETWORK VULNERABILITIES IN A FLAT ENVIRONMENT

Known vulnerabilities and attacks are migrated from the Internet and TCP/IP LANs to the TCP/IP mobile networks. Because all network equipment is exposed to unauthorized access attempts, it is critical that operating systems and platforms undertake a hardening process before being deployed into production environments. Mobile devices will also be targeted by attackers and vulnerable ports can be exploited by intruders.

Mobile networks present a flat environment without segregation. An attacker on the mobile network can target mobile devices and the mobile network infrastructure.

FLORA AND FAUNA

Computer worms, viruses, and spyware threaten the mobile network and can cause significant damage if internal systems are infected. If mobile devices are infected with malware, they can send packets in an attempt to infect other devices on the network. This traffic can cause a service outage and a general degradation of service. Large scale infections on email systems (“love you virus”), web servers (“red worm,” “Chinese worm”), and databases (“Slammer”) have proven that a simple attack aimed at systems with a common vulnerability can reach hundreds of thousands of victims in a matter of hours.

Attackers do not need deep knowledge of how mobile networks operate in order to cause significant damage. TCP/IP-based worms with simple payloads can dramatically affect the availability of service.

[1] CDPD (cellular digital packet data)
GPRS (general packet radio service)
EDGE (enhanced data rates for GSM evolution)
CDMA (code division multiplex access
CDMA EV-DO (CDMA evolution-data optimized
UMTS/HSDPA (universal mobile telecommunications systems/high-speed downlink packet access

FLOOD THE GATES

The TCP/IP protocol and stack implementations have a number of vulnerabilities that can be exploited by attackers. A simple example is the "SYN flood attack," where large number of packets sent by a single mobile device can crash connected systems. Other attacks use spoofed IP addresses to cause response floods from multiple mobile devices to a central server. Additionally, many TCP/IP stacks contain vulnerabilities that can be exploited to crash vulnerable elements on the network and dramatically increase bandwidth consumption.

TCP/IP attacks can be started from the Internet or from within the mobile environment from anywhere in the world. This makes it even harder to stop attackers who are outside the reach of local law enforcement.

MAN-IN-THE-MIDDLE

TCP/IP communications, and even some implementations of SSL, include vulnerabilities that allow attackers to compromise private communications by capturing the initial handshake between communicating parties and applying a man-in-the-middle attack. The attacker can eavesdrop on the communicating parties conversation, capture all information exchanged, or relay false messages between the parties.

DENIAL OF SERVICE

Denials of service (DoS) and distributed denial of service (DDoS) attacks usually involve overwhelming the target site with external communications requests that consume all its resources. DoS attacks can have a particularly serious impact on mobile networks that are part of the critical infrastructure in developed countries. Individuals and businesses that rely on mobile networks for their day-to-day functioning are severely impacted by any widespread blackouts. And these attacks, if successful, have a direct impact on the image and revenue of the target victim's service providers.

AIR TIME

The radio spectrum is a scarce resource. Simple attacks aimed at overloading the available spectrum can have a high impact on service and can result in a denial of service attack. Carefully prepared traffic originated from the Internet can be targeted at a number of base stations, ultimately depleting the available wireless spectrum and affecting service levels.

Mobile networks are based on the concept of shared access to wireless channels and air resources (RF bandwidth). This principle allows mobile devices and radio network controllers to become dormant until required. With dormant connections, numerous mobile devices are able to share available resources, minimizing the power consumption and extending the device's battery life.

Attackers sending frequent packets with intervals shorter than the dormancy timeout can cause mobile devices receiving these arbitrary packets to initiate new connections, consuming air resources from the radio network controller. If enough mobile devices are made to maintain active sessions, air resources will be depleted and valid subscribers will be unable to connect.

JOINING FORCES

Another variety of DOS attack that applies to the mobile environment involves flood attacks aimed at the base transceiver station. Attackers can start low volume attacks, tuned to increase the number of channels consumed by open connections and cause valid subscribers to lose access to the service. Attacks can be launched from inside the mobile network, or from the Internet, with a frequency just below the dormancy threshold defined by the mobile operator. Connections are then kept alive by the base transceiver station.

A variation of this attack includes port scans of mobile devices, computer worms scanning for other vulnerable systems, and in some cases misconfigured settings for VPN keep-alive-traffic and heartbeats.

KEEPS ON GOING

Attackers can easily attack mobile environments by sending frequent arbitrary packets to high numbers of mobile devices. This ensures that these packets arrive at a specific interval within the dormancy timeout thereby forcing the mobile device to maintain a high power consumption until its battery power is drained. By increasing user power consumption, attackers can keep hundreds of subscribers from being able to use their phones.

BILLING FRAUD

In addition to pure technical attacks, intruders can take a profit-oriented approach. Attackers can hijack active subscriber IP addresses and spoof them in order to use fee-based services. Another potential threat is the dissemination of worms or viruses that target handsets and infect the system by sending SMS to high rate numbers that can be mixed between legitimate companies and fraudulent ones.

Countermeasures

To reduce the impact of attacks on the mobile environment, some of the following countermeasures can be implemented:

INCREASED VISIBILITY

Until recently, mobile operators transmitted only voice traffic across their networks. New data services had some initial effect on the volume of voice minutes being used by subscribers, and some mobile operators included clauses in their data contract banning the use of the data service to transfer voice.

Mobile operators need to look inside the data traffic and analyze the information flowing across the network. They need to understand the type of applications and content being used by subscribers, and over time determine what types of service packages should be offered to the subscriber base. This analysis also helps to increase the security of the network by facilitating the detection of dangerous traffic and attacks to the infrastructure.

BANDWIDTH ALLOCATION

Subscribers have different access requirements at specific times during the day, forcing mobile operators to provide guaranteed bandwidth allocation in alignment with specific subscriber profiles. Bandwidth allocation ensures that the customer experience is consistent with the access purchased by the subscriber.

With bandwidth allocation the mobile infrastructure can be protected by blocking excessive connection requests and ensuring that at all times the infrastructure is within expected and designed bandwidth usage limits.

USER QUOTAS

Always on connections have the potential of disrupting service quality to other subscribers. Usage quotas can be deployed within the mobile network to ensure users are following acceptable use policy. This approach avoids the possibility of an always on connection consuming all or part of the available resources.

Peer-to-peer networks are another demand on the mobile network. These networks account for high bandwidth consumption and impact the experience of other subscribers. By limiting overall data consumption for each user, the amount of consumption is managed against needs and service agreements.

The data usage quota protects against long-term service degradation. For example, a subscriber may decide to use his allocated quota in a short period of time, for example, early in the month. Assuming a normal distribution of others subscribers doing the same thing, resources are freed up for use later in the month. This allows the operator to better balance all subscriber usage.

APPLICATION MANAGEMENT

Filters can be deployed to enhance or reduce the bandwidth available to specific applications. Mobile operators can deploy specific filters to ensure that IPTV and in-house services have the maximum bandwidth available. At the same time, other applications, such as peer-to-peer and VoIP services, can be controlled to limit their bandwidth availability to predetermined values – again balancing overall use of network resources.

Known viruses and worms can be filtered by blocking connection requests to known vulnerable applications. Specific packet payloads targeted to vulnerable applications can be blocked.

Conclusion

The growing power of handheld devices, faster Internet connections, and the increasing deployment of wireless networks are bringing a new range of services to mobile phone users. But at the same time, this enhanced mobility brings with it numerous security risks. If these vulnerabilities are not addressed, operators may experience having their networks compromised, customer relations damaged, and the possibility of increased churn and decreased revenues.

By understanding the risks associated with mobile networks, operators can put in place a variety of countermeasures that are both simple and effective. This knowledge also allows operators to take appropriate steps to counter the new threats that are bound to emerge in the future.

About the Author

David Ramirez
Senior Manager
Alcatel-Lucent
Services Business Group

David Ramirez has been involved with information security for the past twelve years. He began his career as a networking specialist and then joined a consulting company managing information risk management practice implementation where he was involved in risk assessments for more than 80 companies. His next move was to a risk management company in the U.K as part of their new information security division. In that role, Ramirez was responsible for developing the methodologies for the practice, including penetration testing, ISO 17799 compliance, and disaster recovery. He was involved in security projects for banks and other financial institutions around the world. The projects focused on security awareness, disaster recovery and business continuity, security policies, security architecture, managed security services, and compliance with international standards.

Ramirez is a member of Alcatel-Lucent's Security consulting practice. His responsibilities include supporting the EMEA and CALA regions with responsibility for innovation and technology, thought leadership, and knowledge sharing

www.alcatel-lucent.com

Alcatel·Lucent