Below the Salt

The Dangers of Unfulfilled Physical Media Assumptions

Matt Blaze[1] and Patrick McDaniel[2]

[1] Computer Science Department, University of Pennsylvania
mab@crypto.com
[2] Systems and Internet Infrastructure Security Laboratory,
Department of Computer Science and Engineering, Pennsylvania State University
mcdaniel@cse.psu.edu

1 Introduction

The physical access media communication traverses is increasing in diversity. Users now access data and services from wired computers, wireless laptops, PDAs, cell phones, and any number of embedded devices. All of these devices now share the same network — the Internet. Of course the Internet itself consists of many media including traditional long haul, ISP, home, and telecommunication networks. Uncertainty introduced by the media diversity has historically led to insecurity simply because the threat models upon which a protocol or security technique may depend, make false or unfulfilled assumptions about the attacker. This has direct consequences on security protocol requirements.

Consider for a moment a simple but ubiquitous case: the move to personal wireless networks. Only a few years ago it was the norm to access the Internet via modem and later cable modem physically connected to a personal computer. The security needed at the physical location was limited to host-level protections, e.g., virus scanners, access controls, etc. When commodity wireless networks were introduced, unknowing users did not anticipate any increased threats. However, the nature of the media completely changed the security profile of the home. Things got even worse when the poor security was added, e.g., WEP [1, 2]. Adversaries could sit up to several hundred meters outside a home while accessing its network and traffic. Thus, users who once freely accessed web, email, and other content could not longer trust the media in their home. This led to massive war-driving[1]. To this day, anyone with a wireless card (and absent ethics) can obtain access to the Internet in any moderately populated location within minutes.

The failure here is not one of security; it was a problem of a moving target. Because the user assumed that the communication was physically secured between the wall socket and his computer, she need not provide any security. As the access moved from the cable to radio frequencies, all of those assumptions

[1] War-driving is the act of scanning a geographic area for "open" networks. This has become a kind of sport where websites like http://www.wardriving.com/ list open networks.

B. Christianson et al. (Eds.): Security Protocols 2009, LNCS 7028, pp. 24–27, 2013.

were no longer valid. In this paper, we argue that a consequence of this reality is that protocol designers should assume the adversary has total control of the media in all circumstances. The media that any protocol will be used on in all possible futures is unknowable. Therefore, one must assume the worst case or accept your fate.

Vulnerabilities introduced by new media can be substantially more subtle in other media, networks, and applications. We argue this case at length in the following sections by exploring the use of telecommunications networks as universal vehicles for data and services. We begin in the next section by exploring the transition of these networks to open systems.

2 Telecommunications Networks

The ongoing transition from closed, proprietary telecommunications networks to open services, open-source mobile phone systems, and diverse applications and content has radically changed traffic patterns and end-point behavior. The provider community views this change with both excitement and unease — while the new revenue streams and business models afforded by open networks will re-invigorate the industry, it is un-clear how the infrastructure will respond to the malicious behavior that is sure to follow.

Even more so than in IP, the misbehavior of a client (mobile phone or tethered lap-top) can negatively affect the health of a telecommunications network. In prior work we studied the effects of open interfaces and abusable protocols in telecommunications networks [3, 4, 5, 6, 7]. We found that the subtle manipulation of traffic violates the underlying "voice-only" design of these systems [3]. A consequence of these violations is vulnerability; we have shown that very low rate attacks can incapacitate voice, text messaging, and data services in large areas (such as Manhattan, see below). Such vulnerabilities not only exist in legacy networks, but also in next generation wireless data networks. These realities strongly suggest that such vulnerabilities are going to become more damaging and prevalent as networks expose open interfaces. Moreover, the move to open mobile phone platforms will increase adversaries' ability to compromise and control large numbers of end-points in the network — thus increasing the networks' and users' vulnerability to abuse. As a consequence, telecommunications networks are likely to increasingly find themselves in an Internet-style morass of unstable services, compromised endpoints, and widespread malicious behavior. Telecommunications networks are fundamentally unprepared for such environments.

3 Attacks on the Telecommunications Network

A central observation we draw from our past experience is that security of the network is not a consequence of one entity enforcing security policy, but it is the collaborative behavior of providers, phone manufacturers, mobile phone operating system and application developers, and ultimately, end users. This leads to

diverse requirements and sometimes complex interactions between the phones, the media, and applications.

Instant messaging is tool for providing synchronous communication between endpoints on the Internet. In an effort to boost highly profitable text messaging revenues, cellular providers introduced network interfaces through standard IM clients, browsers, etc. They provided generalized gateways open to the public that would translate these missives into SMS messages (text messages) that were delivered to the phones. Tension between the applications assumed access to high-speed packet switched networks (IP) and the relatively constrained cellular network led to substantial new vulnerability [5].

To illustrate, a cellular network must perform multiple tasks before delivering a text-message. The network first conducts a series of lookups to determine the location of the destination device. The device must then be awoken from an energy-saving sleep state and authenticated. A connection can then be established and the incoming text message delivered. Critical to this process is the Standalone Dedicated Control Channel (SDCCH), which is responsible for the authentication and content delivery phases of text messaging. With a bandwidth of 762bps [8], this constrained channel is shared by the setup phases of both text messaging and voice calls. Consequently, by keeping the SDCCH saturated with text messages, incoming legitimate voice and text messages cannot be delivered by the network. Understanding this, an adversary attempting to exploit this system can use web-scraping and feedback from provider websites to create hit-lists of targeted devices. By sending traffic to these targeted devices at a rate of approximately 580Kbps, the adversary would be able to deny service to all of Manhattan.

Conversely, note that a protocol can also have a negative effect on the underlying media. In prior work [3], we showed one such circumstance that introduces a vulnerability. To simplify, GPRS/EDGE (cellular data access protocols) use allocated voice channels to transfer data. Each such channel is reserved when the first packet of data is sent from a phone, and held until a period of no use is reached. Because the channels are finite and the bandwidth is fixed, this can lead to severe under-utilization of the network. Moreover, attackers who control groups of cell phones can seize entire cells simply by sending infrequent ping packets. Here the upper layer protocol can abuse the access media because of protocols that assume packet switching but are accessed by circuit switching (channels).

4 Conclusions

Returning to the home network example in the introduction, posit an alternate reality in which the host operating system developer and ISP made no assumptions about the access within the user's home. The two would create a secure tunnel between the host and the ISP access point, e.g., via IPsec [9]. In this case, the adversary would be severely restricted in the kinds of attacks that could be mounted (see below). In addition to providing for the integrity and confidentiality of communication content, the adversary could not access to the Internet

through the invaded network — the ISP would simply filter out all traffic not emerging from the secured tunnel as a matter of policy.

Note further that there are attacks that are specific to the media. Jamming and traffic analysis would still be possible, but other more direct attacks. We observe that addressing these attacks within the protocol, rather than within the access layer is problematic for two reasons. First, any protocol that attempts to address the threats of every possible media type is a practical impossibility. Second, even if such a protocol were possible, the overheads of its execution would enormous and possibly prohibitive.

Of course, the challenge here is to figure out which threats are specific to (and best solved by) the access media, and those that are fundamental to the target protocol. In the case of the home wireless network, the access protocol requires the communication from the paying customer's computer to be confidential and integrity-checked. The use of IPsec is sufficient in this case. The potential for jamming and traffic analysis is an artifact of the media, and thus are best dealt with at that layer. When implemented with the access layer, techniques like frequency hopping and nulling could effectively mitigate these attacks.

References

[1] Stubblefield, A., Ioannidis, J., Rubin, A.: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In: Proceedings of the Networking and Distributed Systems Security (NDSS) Symposium (2002)

[2] Bittau, A., Handley, M., Lackey, J.: The Final Nail in WEP's Coffin. In: Proceedings of the IEEE Symposium on Security and Privacy, S&P, Oakland, CA, USA (May 2006)

[3] Traynor, P., McDaniel, P., Porta, T.L.: On Attack Causality in Internet-Connected Cellular Networks. In: Proceedings of the 16th USENIX Security Symposium, Boston, MA (August 2007)

[4] Traynor, P., Enck, W., McDaniel, P., Porta, T.L.: Mitigating attacks on open functionality in SMS-capable cellular networks. In: Proceedings of the Twelfth Annual International Conference on Mobile Computing and Networking, MobiCom, Los Angeles, CA, pp. 182–193 (September 2006)

[5] Enck, W., Traynor, P., McDaniel, P., Porta, T.L.: Exploiting Open Functionality in SMS-Capable Cellular Networks. In: Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS, Alexandria, VA, pp. 393–404 (November 2005)

[6] Traynor, P., Enck, W., McDaniel, P., Porta, T.L.: Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. IEEE/ACM Transactions on Networking, TON 17(1), 40–53 (2009)

[7] Traynor, P., Enck, W., McDaniel, P., Porta, T.L.: Exploiting Open Functionality in SMS-Capable Cellular Networks. Journal of Computer Security 16(6), 713–742 (2008)

[8] 3rd Generation Partnership Project: Technical realization of the Short Message Service (SMS). Technical Report 3GPP TS 03.40 v7.5.0

[9] Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol. Internet Engineering Task Force, RFC 2401 (November 1998)