The Threat of Mobile Worms

Marc Fouquet[1], Elnaz Eghbali Afshar[2], and Georg Carle[1]

[1] Technical University of Munich
[2] University of Tübingen

Abstract. Mobile devices, such as cellular phones, are becoming more and more powerful. The latest devices assume permanent data connectivity to the Internet and provide the user with a rich set of 3^{rd} party applications. These developments also increase the risk of malware on mobile phones. In this work we first investigate one way of worm propagation on mobile devices. Then we explore the possible harm a mobile worm can do, including a discussion of regional denial of service attacks.

1 Introduction

Mobile phones are becoming more and more intelligent. With fast processors, the ability to install and run a huge amount of client applications and permanent Internet connectivity, today's smartphones have become powerful platforms for work and gaming.

Many mobile phones have some form of short-range communications besides the actual cell phone functionality. This is usually Bluetooth, but WLAN is also not uncommon. For the future, Near Field Communication is planned, mainly to support mobile payment applications.

There have been a number of worms for mobile devices, spreading by Bluetooth like Cabir or MMS like Beselo.A, however no serious outbreak has been observed until today. There is hope that the problem of mobile worms will not become as bad as PC worms, since mobile phones are a relatively closed platform. However phones based on Symbian, Android or Windows Mobile allow the installation of software which has not been tested by the operator. Further it is not unlikely that worms can spread via security holes, as mobile phones are patched rarely.

Cell phones are an interesting target for worms, possible goals of an attacker could be payment systems or spying on the user's location, calls and stored private data.

In this work we provide two main contributions. A study of worm propagation via shot-range communication is presented in Section 3. In Section 4 we will describe, what possible harm a mobile worm can do and what defences look like.

2 Related Work

There have been a number of publications on epidemic spreading of viruses for biological diseases but also for computer worms. In the latter case, the authors either use simulations [1] or mathematical models of epidemic spreading [2]. Yan et. al. [3] observed that the mobility model plays an important role for worm propagation. Su et. al. [4] did experiments and simulations, showing that large-scale infections with Bluetooth worms are in fact possible.

Today, worms on PCs form highly organized botnets [5]. These networks of drones are used by criminals to send spam, to host phishing sites and to launch denial-of-service (DoS) attacks. This kind of organization has not yet been observed with mobile worms.

Security research regarding cellular networks mostly focuses on encryption and authentication issues, but also DoS attack scenarios have been investigated in the past [6].

3 Worm Propagation

In this section we describe our own worm propagation simulations using the PS-Model framework [7] for OMNeT++. PS-Model provides a radio propagation model with attenuation by walls, and a “strategy-based” mobility model, which allows users to select destinations by mood, i.e. a restaurant when they are hungry. Further, the users prefer to walk in groups rather than independently.

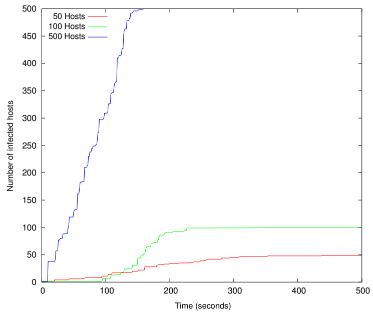

Fig. 1. Influence of the Population Size.

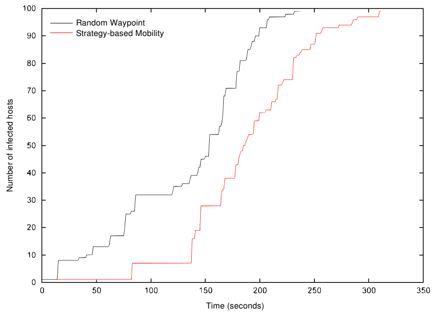

Fig. 2. Group Mobility vs. Random Waypoint.

Figure 1 shows a simple setting, different numbers of users are moving on an open 500 m×500 m playfield according to a random waypoint model. The users are carrying simulated Bluetooth class 1 devices with 100 mW transmission power, which results in a communication range of approximately 100 meters. We assume that the reception of one broadcast (i.e. Bluetooth Inquiry) message is sufficient to infect a new device. Such a message is sent by each infected device in intervals of 10 seconds. Initially only a single device is infected.

One can see that with a low density of only 50 users, it takes more than 400 seconds to infect the whole population. With a higher number of users, the time for spreading the worm decreases. With 500 users, the whole population is already infected after 150 seconds. A higher density of users means that more potential victims are in range of infected devices and also reduces the need to rely on user movement to bring the worm to new areas.

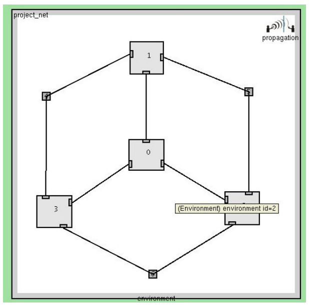

Fig. 3. Map for the Group Mobility Experiment

For Figure 2 we changed the setup to make it more realistic. The map for this experiment is shown in Figure 3. Four rectangular areas (houses) were placed, the walls of these houses attenuate the radio signal. Users can decide to move around inside each of the houses, or they can walk out on roads to move to a different house. The movement model was changed to "strategy-based" mobility as described above.

The result shows that worm propagation is slowed down under these more realistic conditions. All 100 hosts are infected after 325 seconds, while this only takes 240 seconds with the simple random-waypoint scenario. The main reasons for this are radio attenuation and the group mobility, which causes the users to form isolated clusters and therefore reduces the opportunities of spreading the worm.

On the other hand it should be noted that, even though the map has the same size as before, it is not fully occupied by the users as they stay in the houses or on the roads between them. Therefore the general user density can be considered higher in this simulation run.

4 Threat Analysis

Until now we only have considered worms that spread from one device to the next via short-range communications. However there are numerous other possibilities to infect mobile devices: SMS/MMS, drive-by infection on websites or even shipping malware as a trojan in some seemingly useful software. In this section we will explore possible dangers by mobile malware, therefore we will not restrict ourselves to a single method of infection.

4.1 Direct Threats for the User

As already mentioned in the introduction, there are a number of reasons for an attacker to write malware for cell phones:

- Users increasingly use their cell phones for email and processing other documents. Malware can have the goal of harvesting passwords and other user-specific information.
- Mobile phones are used for payment services. Especially banks are sending one-time passwords for PC-based online-banking to cellular phones. Tampering with payment systems could bring a direct financial benefit for the author of the malware.

- If desired, mobile phones allow new ways of spying on people. Not only is it possible to get audio and video from the phone, also tracking the location of the user is possible.
- Mobile malware could call expensive service numbers or use other paid services.

Further a mobile phone could also be made unusable by malware, i.e. by changing connection settings (which would cut the phone off from the network) or by automatically launching an application on startup which immediately crashes the phone. Such a destructive behaviour was common to viruses in the past, however it is rarely observed today as it limits spreading and does not give the attacker a benefit.

Defence against such malware is possible by controling the applications on the device. This would not necessarily mean a complete walled-garden philosophy, the network operator could just force the users to run a virus-scanner.

4.2 DoS Attacks on the Infrastructure

A number of denial-of-service scenarios against the network operator's core network and Voice-over-IP infrastructure in general have already been discussed in the past [6]. In this section we focus on possible flooding DoS attacks against individual cells of the radio access network.

Of course an attacker could perform any kind of jamming attack if he had direct access to the radio interface. In this section we will make the more realistic assumption that any user-installed software on a mobile phone is bound to the implemented MAC protocols for the cellular as well as the short-range interfaces.

Generally cellular networks are subject to admission control and apply QoS mechanisms, so they are more robust against DoS attacks than an unmanaged Ethernet or WLAN. A single device is unable to flood a cell, as its share of the medium would be limited by air-interface scheduling.

When multiple infected devices are present in the same cell, an attack is possible. Again air interface scheduling of the operator strongly determines the effectiveness of such attacks. The authors of [8] investigated the capacity of cells in different operator networks and their reaction to high-load conditions. Their results suggest that 20-80 voice calls are required to deplete the resources of an UMTS cell. They also found out that there is an operator-specific guaranteed minimum bandwidth for each data call and that not all operators prioritise voice higher than data. Highly-loaded cells tend to show strange behaviour, including the possibility that all active connections are dropped. Some network operators also offer video calls which are given a relatively high priority while using 3-4 times more bandwidth than voice calls. These results suggest that it is generally possible to DoS an UMTS cell with less than 30 terminals when choosing a combined attack pattern of voice, data and possibly video.

Such an attack requires coordination between the participating devices which could be achieved in one of the following ways:

- **Decentralized Coordination**: When multiple infected devices are close together, they form a (possibly meshed) network, which has the main purpose of counting the number of nearby infected devices. As soon as this number crosses a threshold which allows the devices to DoS the local cell of the mobile network, the devices launch their attack. This method has the advantage that no communication via the cellular network is necessary for the coordination of the attack. Disadvantages are the lack of control by the malware author and that the fact of enough devices being in the cell may not be detected as they are not close enough to form a common ad-hoc network.
- **Central Coordination**: The malware contacts some central coordination point on the Internet (possibly via some proxy to disguise the communication) and transmits its location information. Location data is available in many mobile phones today; even without GPS, the location of a mobile phone can be estimated by GSM or UMTS. The central botmaster can see the distribution of mobile phones and chose to attack cells with enough infected devices.
- **Hybrid Coordination**: To reduce the amount of detectable traffic via the cellular networks, bots can coordinate themselves via an ad-hoc network, but still contact a central point of control when a threshold regarding the network-size has been crossed. This would still allow central control with only minimal exposure.

We see several options to detect and mitigate this threat:

- Looking at the communication to the Internet-based botmaster, if existent. However this is difficult, as already today bots can disguise their traffic, i.e. as normal HTTP communications.
- Detecting short-range coordination traffic, i.e. by placing probes at crowded places. This has already been suggested in [4] to detect worm propagation.
- Scheduling attack traffic to use no or only very limited bandwidth during an attack. This requires the possibility to distinguish the attack traffic from legitimate traffic, which will again be difficult. In any case voice calls should be given highest priority.
- If the attack started on all devices simultaneously, the operator could use this fact to identify the attacking devices. However this can be disguised by the attacker by using individual start times for each device.
- If the attack is coordinated locally using an ad-hoc network, the operator could detect the participating hosts by looking at the locations of the nodes in the cell. The attacking nodes are expected to be relatively close together. This might allow blocking the attackers, however it may also cause some legitimate sessions to be dropped.
- Detecting devices that issue large numbers of localisation requests. However there might also be legitimate applications that behave similarly.

Users might also become suspicious when noticing fast battery depletion of devices with active bots, as close-range communications, GPS and also cellular localisation consume a lot of energy.

5 Conclusion

In this paper we presented our own investigations regarding mobile worm propagation. We also discussed threats by mobile worms, including a possible DoS attack on cellular networks.

One open question is, whether we really have to expect such attacks. Most of today's worms are used by criminals to earn money. It is unlikely that money can be made from extortion of network operators. However this attack can also be seen as targeting a geographical region rather than a specific operator, so for example public events could be potential victims. Even if this attack is hypothetical now, the possibility should be considered when designing cellular networks.

6 Acknowledgements

The authors would like to thank Andreas Klenk for fruitful discussions and Andreas Monger and Marcel Kronfeld for their help with PS-Model.

References

1. Vogt, T.: Simulating and optimising worm propagation algorithms. (2003)
2. Bulygin, Y.: Epidemics of mobile worms. Performance, Computing, and Communications Conference, 2002. 21st IEEE International (2007) 475–478
3. Yan, G., Flores, H.D., Cuellar, L., Hengartner, N., Eidenbenz, S., Vu, V.: Bluetooth worm propagation: Mobility pattern matters! In: ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security, New York, NY, USA, ACM (2007) 32–44
4. Su, J., Chan, K.K., Miklas, A.G., Po, K., Akhavan, A., Saroiu, S., Lara, E.D., Goel, A.: A preliminary investigation of worm infections in a bluetooth environment. In: Proceedings of the ACM Workshop on Rapid Malcode (WORM), Alexandria, VA, USA (2006)
5. Holz, T., Steiner, M., Dahl, F., Biersack, E.W., Freiling, F.: Measurements and mitigation of peer-to-peer-based botnets: a case study on storm wor. In: LEET'08: 1st USENIX Workshop on Large-Scale Exploits and Emergent Threats, April 15, 2008, San Francisco, USA. (Apr 2008)
6. Zhao, B., Chi, C., Gao, W., Thu, S., Cao, G.: A chain reaction dos attack on 3G networks: Analysis and defenses. In: IEEE INFOCOM 2009. (2009)
7. Petrak, L., Landsiedel, O., Wehrle, K.: Towards realistic strategy-based mobility models for ad hoc communication. In: Proceedings of the 2005 Conference on Software for Communication Systems and Computer Networks. (2005)
8. Tan, W.L., Lam, F., Lau, W.C.: An empirical study on the capacity and performance of 3G networks. IEEE Transactions on Mobile Computing **7**(6) (2008) 737–750