

WAP AND VIRUSES – CAN YOUR MOBILE PHONE GET INFECTED?

Mikko Hyppönen

F-Secure Corporation, Pyyntitie 7, 02231 Espoo, Finland

Tel +358 9 8599 0513 • Fax +358 9 8599 0713 • Email mikko.hypponen@f-secure.com

ABSTRACT

The use of WAP-enabled mobile phones is booming. Cellular phones with support for WAP (Wireless Application Protocol) allow users to access a wide variety of services. WAP enables users to do on-line banking, monitor stock markets, use email, access the Internet – all from their mobile phones. Future WAP services with positioning support will enable even more advanced services – for example, you could ask your phone to find the closest restaurant in a strange city and your phone would answer back with map and directions.

However, this functionality does not come free. Current WAP terminals cannot be infected with traditional viruses as there simply isn't enough functionality yet. However, new versions of the WAP standards will make the possibility of WAP viruses a reality as soon as 2001.

This paper will discuss the threats with current WAP protocol and how changes in the protocol will enable real viruses. Future threat scenarios are presented along with suggestions to avoid these problems.

INTRODUCTION

'Okay, dudez but for now – let's go to work . We are starting Cell Phone Virus Challenge. Any contribution welcomed (the more funny solution, the better). Deadline has not been set'

Statement from an underground Web news service directed to virus writers, June 2000.



Figure 1: Example of a simple WAP service – real-time currency converter

WHERE'S THE PROBLEM?

When it comes to WAP security, why worry? From the outset, vendors of mobile phones and WAP servers have ensured that much consideration was given to confidentiality and privacy issues for WAP data, as well as to user authentication. Add this to the fact that data integrity checking has been taken into account, and you could be forgiven for thinking that the WAP infrastructure is already secure enough.

However, we believe that there are still a number of security issues to be resolved. Firstly, there is no content security for the WAP infrastructure, and yet this is where one of the biggest threats typically lies. As we have already seen in the desktop-PC world, content-related security is the single biggest security issue for home and corporate users alike. Even now, we receive an average of seven new PC virus samples every day, with actions that range from benign to potentially catastrophic. In the telecommunications world, content has traditionally been *speech* – with no security risks involved. Now the content is *code*, and the whole picture changes.

The WAP infrastructure has not taken executable mobile content – such as downloadable programs – into account from a content-security point of view. The WAP content requested by the mobile device and returned by the origin server can, for example, contain WML cards, which may display text or pictures, working similarly to HTML pages on the Web. The pages can also contain script written with WMLScript language – which is a close relative to the *JavaScript* scripting language. As a sidenote, several PC viruses written with *JavaScript* were discovered during 1999 and 2000.

A simple WAP virus could damage user data such as phonebooks, text messages, calendars or other settings. Corruption of data in the form of Trojan horses trying to steal user information, worms or automatic email chain-letters could also appear. The latter methods are far more dangerous as they threaten not only locally-stored content, but also other network connections, such as links to corporate LANs.

MOTIVES

Viruses are written for a variety of reasons, such as curiosity, a challenge, or to gain wider attention. Some virus writer groups are known to target any new platform, just to be able to say they were the first to write a virus for this platform. At the time of writing, the WAP infrastructure is still emerging and the uptake of WAP devices is still increasing. Currently therefore, WAP devices do not present a big enough target and so no WAP-specific viruses have yet been seen. However, a growing threat is coming in from the horizon as the power of WAP devices is set to increase dramatically with future WAP protocol versions.

As WML also increases in sophistication, so do the opportunities for creating more advanced, malicious code. When the first WAP virus hits, it could spread as fast or faster than similar PC viruses. The implications for the WAP infrastructure as a whole are ominous if this were to occur. For example, public confidence for an activity such as wireless banking would deteriorate if the threat of WAP viruses loomed large.

VIRUS ACTIONS

The only way to deal with these threats is to secure all remaining gaps in WAP security, *before* such attacks are mounted. The industry is in a unique position to benefit from past experience and proactively prevent the type of weaknesses in infrastructure that caught us unaware with past computer incidents. There are no viruses on WAP yet – we still have time to react.

Before we consider the key security issues, and solutions that will help identify and meet WAP content security risks, it is best to understand how a basic WAP network is composed. There are three logical components: the WAP client (or mobile terminal), the WAP gateway and the origin server. This is illustrated schematically in Figure 2. The origin server is located in the traditional Internet domain and functions like an ordinary Web server by providing storage for WAP content. The WAP gateway interconnects the Internet domain with the mobile network domain by providing the mobile terminal with Internet access. The mobile terminal roams in the mobile network and sends encoded content requests to the origin server via the WAP gateway.

WAP needs more functionality in order to be useful and for it to really take off the ground. Unfortunately, more functionality means more risks. The power of WAP devices is set to increase dramatically with future functions set to be included in the WAP specification in the near future. Such functions include making phone calls, accessing and modifying phone book data, and sending Short Messaging Service (SMS) messages.

With such functionality available to WML scripts, it is not difficult to imagine a virus which would spread by accessing your phone book and sending a link to itself in SMS text messages to

all the phone numbers found within. Subsequently, the virus could do damage by either deleting or modifying your phone book, or by starting to make phone calls to pay-per-minute numbers – in the middle of the night. With such a feature, virus writers could easily make money with their viruses – thus providing an obvious motivation. As WML increases in sophistication, so do the opportunities for creating more sophisticated, malicious code.

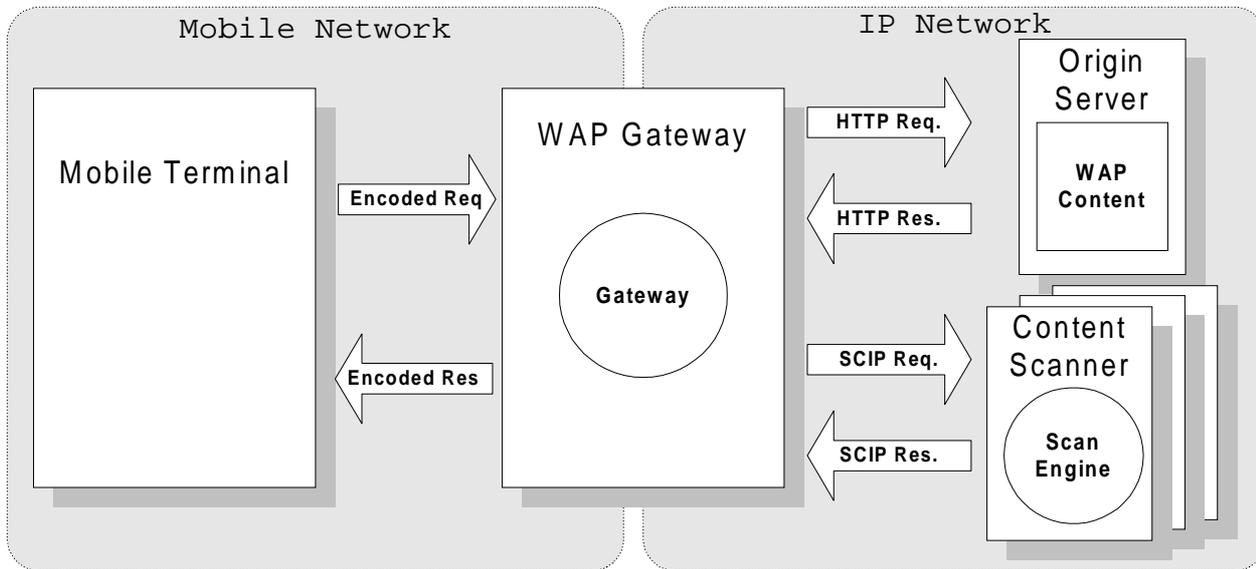


Figure 2: Schematic illustration of the basic WAP infrastructure

CURRENT THREATS

Although WAP viruses are not yet possible, it's possible to launch other kinds of attacks; denial of service or social engineering. Figure 3 shows a demonstration of a simple social engineering attack which is possible with today's WAP technology.

SHUTTING THE STABLE DOOR

The first, and biggest, step in delivering content security into the WAP world is a gateway-level solution for protecting the WAP infrastructure. A WML script scanner is integrated with the WAP gateway, which detects and removes malicious code before it is passed to users' devices.

Gateway protection will also ensure that when a new virus is found, counter-measures to provide protection can be developed quickly and distributed over the Internet-based framework to WAP servers worldwide.

This type of solution has the advantage for the current WAP infrastructure (see Figure 2) of requiring no client software and leaving no 'footprint' on the client device, making it suitable for the current generation of WAP phones, for example. The WAP subscriber simply receives virus-free content in a way that's transparent to them, and the solution is centrally-managed by the content provider to ensure optimum control of content.

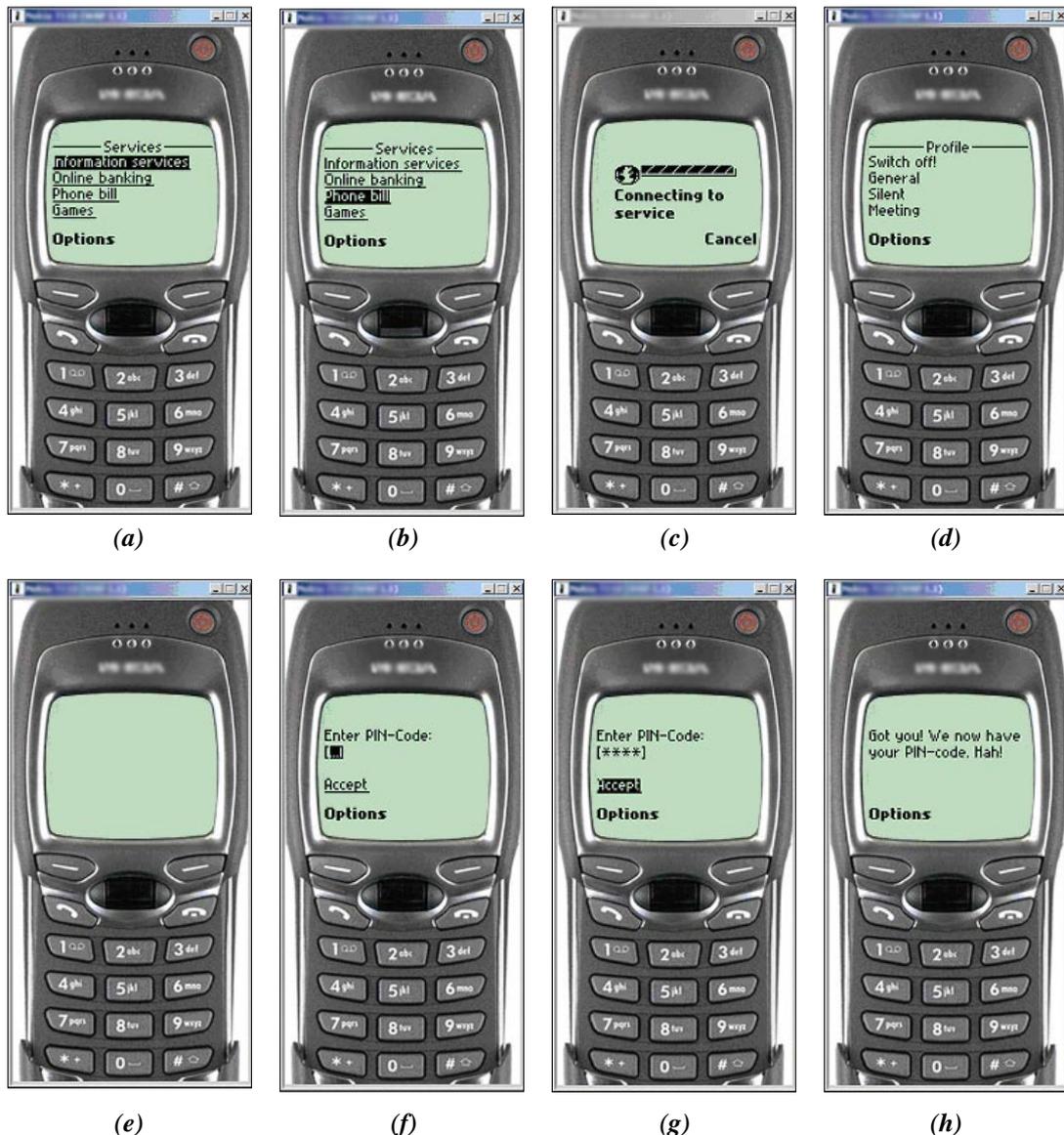


Figure 3: Demonstration of a simple WAP social engineering attack

- (a) User enters a WAP portal with a variety of services.
- (b) User chooses one of them.
- (c) Service is being downloaded, please wait.
- (d) Bummer – suddenly the phone hangs and reboots.
- (e) New WAP phones often do this. Oh, well.
- (f) After rebooting, user enters his secret PIN-code, as usual.
- (g) Everything *looks* normal.
- (h) Except the connection was never broken, and the reboot was fake. The attacker now has the secret PIN-code.

THE MANAGEMENT APPROACH

If just one of the WAP gateways is out of date with regard to virus definitions, the entire network can be compromised. Therefore, a highly scalable policy management framework can be used, particularly ideal for companies that have tens of thousands of employees using WAP phones.

The idea is that as soon as a new malicious WAP program is located, it can be analysed and antidotes can be developed for it. With central management, this update can be sent and deployed automatically to all WAP gateways around the globe – well before the malicious program has time to spread widely.

BE PREPARED

What is clear is that although there are no content security issues as yet, they will most likely appear when WAP takes off. Vendors can't afford for WAP to lose its credibility. Therefore, it is in everyone's best interest to ensure that the infrastructure is in place before the first WAP virus is found.

ENDNOTES

- *Nokia WAP Toolkit 2.0 documentation files.*
- Presentation 'Security of Wireless Application Protocol', Antonius Bekker, *Sonera Corporation.*
- Presentation 'Security of New Mobile Phone Techniques', Valteri Niemi, *Nokia Corporation.*
- Thanks to Craig Coward, Pasi Lahti, Ari Hyppönen and Seppo Salorinne.