3GPP TSG SA WG3 Security ó SA3#35 **S3-040873**

October 5-8, 2004

St Paul's Bay, Malta

Title: **Selective Disabling of UE Capabilities; updated S3-040737 based on the comments in SA3#35 meeting**

Source: **Nokia**

Document for: **Discussion**

Agenda Item: **6.23**

Work Item:

1 Introduction

The new WID ìSelective Disabling of UE Capabilities was approved in SA#24î. The main responsibility is in SA1 but the WI also includes a feasibility study in which SA3 in involved. The Feasibility Study should analyze both the threats that could be mitigated by this type of mechanisms and the threats created by introduction of such a mechanism. The text below provides input for this feasibility study. It has to be noted that the study from SA3 has focused on the specific part aiming to disabling in order to quarantine terminals infected by viruses/worms. The study does not consider the aspects related to other parties wanting to disable terminals. The characteristics and implications of such scenario may differ. The goal was to prevent the propagation of virus/worms in mobile networks, and to protect the operator's infrastructure. The best solution is definitely prevention. However some viruses/worms still being able to get to the terminals (e.g. not through the cellular network), solutions have been discussed for the post-infection case to minimize damages to the network.

In the recent past, attacks have proliferated on the Internet. Attacks like worms and viruses not only perform malicious actions such as using up the terminal's resources, modifying the configuration of the terminal, preventing applications from running, or shutting the system down but these programs typically also propagate and infect other terminals.

In a short period of time, these viruses and worms can quickly spread, affecting a considerable number of users and affecting the network resources because of the traffic generated. Some of these worms include DoS attacks (e.g. SYN floods, HTTP floods) that actually worsen the impact on the network by the large amount of traffic created.

Detecting infected terminals and quarantining them can help reducing these threats. By quarantining the terminal, the network will place restrictions to the ability of the terminal to establish IP connection. This prevents these attacks from propagating and infecting other terminals, as well as protecting the network resources.

Once a terminal has been identified as infected, its services should not be completely cut, but depending on the gravity of the viruses/worms, its services may be restricted. Emergency services should remain available to the users in all situations. Also, based on the operator configuration/requirements, other connectivity services may remain accessible. The network will provide with some means to clean the terminal and make sure the attack cannot be propagated, e.g. connectivity to network servers that allow the terminal to download anti-virus software.

This document is a preliminary analysis that identifies some of the threats that can be prevented, some of the threats that cannot be prevented, and consider other methods that can be adopted to address the attacks. Further study is required to identify further threats and scenarios.

2 Discussion

2.1 Which threats could be mitigated with this kind of approach

Having the required infrastructure and defining the required procedures can alleviate several threats. These e.g. include:

- Preventing the propagation of worms: A worm is a program or algorithm that replicates itself over a network and usually performs malicious actions, such as using up the terminal's resources and possibly shutting the system down.

  Worms may also attempt Denial of Service attacks on some pre-determined servers by e.g. flooding the target with TCP SYN (SYN Flood) or generating a high volume of traffic towards the target. Considering worms propagate and therefore many terminals will launch the attacks, the damages can be disastrous.

  Worms typically propagate in a network by using specific ports (e.g. TCP 135 for MSBlast, TCP 445 for W32.Korgo.P): the program e.g. generates IP address according to a specific algorithm and then send data on selected ports in order to infect other terminals.

  Having the network entities to scan the outgoing traffic and identifying the infected terminals can prevent the worms from infecting other devices, and affecting the network resources.

- Cleaning infected terminals from worms and viruses: due to the threats mentioned above, identifying infected terminals and cleaning them from the viruses/worms allows subscribers to re-use their terminal. Usersí irritation and frustration can significantly increase when the userís terminal has been infected by a virus/worm and the subscriber cannot use the terminal.

  Providing a mechanism to detect and quickly clean infected terminals can increase the userís experience.

- Stopping Trojan Horses: As viruses and worms, Trojan Horses can be downloaded to a device through a connectivity that is not controlled by the network operator (e.g. public WLAN, Bluetooth or Infrared).

  Trojan Horses can not only steal information (passwords, bank information) from the victim but also let malicious node take control of the infected terminal.

  These programs typically listen on specific ports for remote instructions, and send data (e.g. stolen information or notification) to a predetermined address.

  By scanning the outgoing traffic and scanning the listening ports (e.g. by sending a TCP SYN), a network can detect terminals infected by Trojan Horses and provide methods to clean them.

- Detecting spywares: A spyware is software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

  Spyware also steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

  Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author.

  As with viruses, worms, and Trojan horses, scanning the outgoing traffic and scanning the listening ports (e.g. by sending a TCP SYN) can help a network to detect terminals infected by spywares and provide methods to clean it.

2.2 Which related threats are not mitigated

- Assistance from the terminal can help detecting viruses, worms and other malicious programs. However legacy terminals may not have the required functionality implemented. Also viruses/worms may prevent the terminal from performing the expected operations.

  As an example, many malicious programs modify the registry when infecting a terminal. The terminal could scan the registry or simply notify the network when suspecting that it has been infected by a virus. This latter one may however prevent the sending of the notification message.

The network can thus not always rely on the terminal.

In such case, the network can only detect malicious programs that generate or listen to specific traffic.

- Also such approach would not prevent terminals from being infected since viruses/worms can be downloaded to a device through a connectivity that is not controlled by the network operator (e.g. public WLAN, Bluetooth or Infrared). This is likely to become the most common route for infection in the future so any GSM/3Gnetwork based solution will have to be combined with other terminal based solutions

    1. It may be useful to review the specifications from MExE which were intended to control download using terminal based security methods as well as the potential new R7 work item on ìTrust Requirements for open Platformsî (S3-040480).

    2. A useful source of requirements and mechanisms for network based selective enabling and disabling of features are the TETRA security specifications from the TETRA Security and Fraud Prevention Group (SFPG) in ETSI.

- Finally, it has to be noted that some malicious programs may be designed not only to affect the terminalís behavior but may also prevent the terminal from connecting to e.g. any server/service set up by the network to clean the terminal. In such case, the network cannot help cleaning the infected terminal from the virus through IP connectivity and therefore protect the terminal from a DoS attack.

2.3 What can be done by existing mechanisms

Firewalls can prevent propagation of viruses and worms if all traffic passes through the firewalls and if the firewalls blocks unsolicited packets.

NOTE: Firewalls may however present other issues (e.g. how to open required pinholes for the required applications).

Firewalls can:

1. Prevent the propagation of viruses and worms.

2. Protect the network from viruses and worms: A firewall located at the Gi interface would drop the malicious packets and prevent them from further affecting the network.

Firewalls however cannot:

1. Detect Trojan Horses and Spyware. Trojan Horses and Spywares however do not propagate. It will therefore more be for the benefits of the users to know that it had been infected.

2. Provide a fast mean to clean the infected terminals. When infected, users might not know how to clean the device from the malicious programs.

These features cannot be provided by FW but could be by the considered approach. It also has to be noted that firewalls cannot stop traffic generated on the radio by viruses/worms

2.4 What are the potential problems introduced by this type of mechanisms

- If the terminal is disconnected from the required services after being detected as infected, this may not be acceptable by the user. The user may not care too much about the virusís impact but may need to make a call. If he is disconnected from that service (e.g. because the network wants to protect its resources), this may be a problem.

- Such situation could be addressed by still allowing the user to access the required services and only restricting the ones affected by the viruses/worms.

- When a virus spreads (not between terminals in the operator network, but e.g. from Internet to the terminals), there will be many terminals that need cleaning all at the same time. This may create a huge bottleneck for the connectivity towards the îrepair centerî.

- Once the terminal is infected, can we guarantee that by connecting to the repair center it can actually be clean?

- It should be made sure that the introduced procedures do not introduce potential DoS attacks to 3GPP subscribers. In other terms, a malicious node should not be able to use the proposed procedures to prevent users from accessing services. For example, an attacker may be able to abuse the proposed procedures to deny service to uninfected terminals. Another example is that a virus may infect a terminal and prevent it from connecting to the network to get rid of the virus. The terminal may thus not only be infected but also unable to connect to the desired network services until the terminal is cleaned from the virus by other means.

- There are problems to correctly "target" the infected device. Is it the ME connected to the network, or is it the Computer currently connected to it? It makes no sense to disable the ME, when the Computer can be connected to a different ME. Furthermore, binding the quarantine to the ME or the subscription (UICC) may not be suitable, as both may be exchanged.

- A simple quarantine mechanism (possible caused by an infected Computer) will also shut the subscriber off from using other IP-based services with her ME, like MMS, WAP etc.

- If quarantining should be done thoroughly, shutting an infected ME off select IP-based services might not be sufficient. The ME could be infected by a "dialer", and consequently the ME must also be denied to initiate "expensive" CS calls

- Adding security software to the terminal requires a privilege concept in the terminal, where the device owner (and the applications run by her) has a lower privilege level than the security software. Otherwise the device owner (or any attacks on vulnerable software run by her) can disable the security software. This spoon-feeding of users might be accepted in professional environments, but it is hardly possible for all users. Very few existing terminals support such privilege concepts yet.

- Furthermore, managing and updating security software requires a secure means for remote device management and software push. Even in a homogeneous client environment with several thousand clients this management causes tremendous costs. In a heterogeneous ME environment with many million devices it is surely impossible.

3 Conclusions

- The limitation of the virus/worm propagation and the protection of the operator's resources can already be achieved transparently.

    - For the propagation of the virus, many viruses and worms propagate by sending IP packets over specific ports. The 3GPP network can deploy firewalls at the Gi interface to identify those malicious packets and stop them preventing the propagation of viruses and worms. The packets can be silently dropped

    - For the protection of the operator's resources, many viruses/worms include malicious programs that e.g. launch DoS against specific entities. With all the devices infected, the Distributed DoS may bring down the target (e.g. by having all the infected terminals sending TCP SYN packets to a specified target) and one of the goals of the proposed work was to protect the operator infrastructure. However, it has to be noted that this can also be achieved by deploying firewalls to protect the relevant resources (servers). Current firewall technology include methods to address TCP SYN flood, and other well know DoS.

- Disabling the infected terminals may present an opportunity for malicious programs to have a greater impact on the victims by blocking them out of the network.

- The network can detect that a terminal is infected and could provide methods to disinfect it, but this requires device management means (knowledge of the operating system, etc.)

- Blocking the terminal may not seem recommendable in most environments.

- The best solution is definitely prevention.