A Taxonomy of Cyber Attacks on 3G Networks

Kameswari Kotapati, Peng Liu, Yan Sun, Thomas F. LaPorta

The Pennsylvania State University, University Park, PA 16802

Early first and second generation (1G and 2G, respectively) wireless telecommunication networks were *isolated* in the sense that their signaling and control infrastructure was not directly accessible to end subscribers. *The vision of the next generation 3G wireless telecommunication network is to use IP technologies for control and transport*. The introduction of IP technologies has opened up a new generation of IP-based services that must interwork with traditional 3G wireless telecommunication networks. *Cross Network Services* will use a combination of *Internet-based data* and *data from the wireless telecommunication network* to provide services to the wireless subscriber. They will be multi-vendor, multi-domain, and will cater to a wide variety of needs. An example of such a Cross Network Service is the *Email Based Call Forwarding Service (CFS)*, where the *status of the subscriber's email inbox* is used to *trigger call forwarding* in the wireless telecommunication network.

A security risk is introduced by providing Internet connectivity to the 3G networks in that certain *attacks* can be *easily enforced* on the *wireless telecommunication network indirectly from the IP networks*. These *Cross Infrastructure Cyber Attacks* are simple to execute and yet have serious effects. In this paper we present a *unique attack taxonomy* in which we consider the Cross Infrastructure Cyber attacks in addition to the standard Single Infrastructure attacks, some of which have already been studied. In presenting the taxonomy of attacks on the 3G Network, we classify the attacks into three dimensions summarized in Table 1.

Table 1. Summary of Attack Taxonomy

Dimension I: Physical access	**Dimension II**: Attack type	**Dimension III**: Attack Means
Level I: **Access to air interface with physical device**: Intruders have access to standard inexpensive 'off-the-shelf' equipment that could be used to impersonate parts of the network.	**Interception:** Passive attack- Intruder intercepts information but does not modify or delete them.	**Messages:** Signaling messages are compromised.
Level II: Access to Cables connecting 3G entities: Intruder may cause damage by disrupting normal transmission of signaling messages.	**Fabrication:** Intruder may insert spurious objects (data, messages and service logic) into the system.	
Level III: Access to 3G core network entities: Intruder can cause damage by editing the service logic or modifying subscriber data (profile, security and services) stored in the network entity.	**Modification of Resources:** The intruder causes damage by modifying system resources.	**Data:** The data stored in the system is compromised.
Level IV: Access to Links connecting the Internet based Cross Network Services and the 3G core network: This is a Cross Infrastructure Cyber Attack.	**Denial Of Service:** Intruder causes an overload or a disruption in the system.	**Service Logic:** The service logic running on the network is compromised.
Level V: Access to Internet Cross Network Servers: This is a Cross Infrastructure Cyber Attack. Intruder can cause damage by editing the service logic, modifying subscriber data (profile, security) stored in the Cross Network Servers.	**Interruption:** The intruder causes an Interruption by destroying resources	

To understand such attacks, we have developed a detailed abstract model of the 3G telecommunications network infrastructure. Each entity is modeled into atomic processing units (agents) and data stores (permanent and cached) as shown in Figure 1. We map attacks to these specific modules in each entity as discussed below.

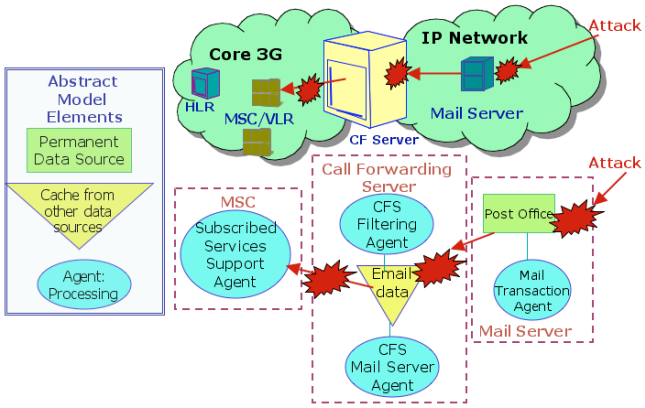

Fig. 1. Attack Propagation in CFS with simplified abstract model

The CFS forwards a call to a subscriber's voice mail if there is no email from the caller in its inbox of over a certain age; otherwise the call is forwarded to the subscriber's cellular phone. The *CFS Mail Server Agent* in the CFS periodically fetches email stored in the *Post Office* data source of the Mail Server. This data is stored in the *Email data* cache of the CFS. When there is an incoming call for the CF subscriber, the *Subscribed Services Support Agent* in the MSC will query the CF Server on how to forward the call. The *CFS Filtering Agent* will check its *Email data* cache, and if there is appropriate email from the caller, the call is forwarded to the subscriber's cellular phone.

The propagation of the attack from the Mail Server to the CFS, and finally the 3G-network entity, is illustrated in Fig 1. Using any well-known Mail Server vulnerabilities the attacker may compromise the Mail Server and corrupt the *Post Office data* source by deleting emails from certain people from whom the victim is expecting calls. The *CFS Mail Server Agent* queries the *Mail Transaction Agent* for emails from the *Post Office data* source and the *Mail Transaction Agent* will pass on the corrupted email data to the *CFS Mail Server Agent*. The *CFS Mail Server Agent* will cache the email data in its *Email data* cache. When the *Subscribed Services Support Agent* in the MSC entity of the 3G network sends out a 'How to forward the call?' query to the CF Server, the CF Server will check its corrupt *Email* data cache, find that there are no emails from the caller, and route the call incorrectly. Thus the effect of the attack on the Internet Mail Server has propagated to the 3G network. This is a classic example of a *Dimension: I-Level V Cross Infrastructure Cyber Attack*, where the attacker gains access to the *Cross Network Server* and attacks by modifying data in the data source of the *Cross Network Server*.

The full paper presents a model for 3G networks, a set of *Cross Network Services*, and a full attack taxonomy including *Cross Infrastructure Cyber attacks*.