Cybercriminalité dans les réseaux Télécom

Mots clés :
- Directeur de thèse : aurelien FRANCILLON
- Co-encadrant(s) :
- Unité de recherche : Laboratoire de recherche d'EURECOM
- École doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

Today telecom networks are pervasive and we rely on them for our daily activities. So it is for cybercrime, for example, telecom fraud has been reported to cost $40 billion globally[5]. This fraud takes very diverse forms, such as Nigerian scams [6, 7, 8, 4], abuse of compromised PXB, routing phone calls on "gray" networks or security agencies breaking into telecom operators [1]. In general telecom networks are an attractive target for criminals because operations are always linked to billing (e.g., cashback phone numbers, termination costs, premium text messages, bulk SMS spam or denial of phone service). Therefore, there are many ways that are used to manipulate networks and especially to extract revenue from those networks. While some commercial products exist that attempt to mitigate such abuses, this field was left mostly aside by the research community. This is, in part, because the lack of access to equipment or to the telecom networks themselves. The goal of this PhD thesis will be to investigate the different classes of cybercrime and fraud on telecom networks, develop experimental tools for improving the state of the art detection or prevention methods and to improve the understanding of those cybercrime ecosystems. Examples of techniques that may be experimented with are SIP and/or POTS (Plain Old Telephone Service) based PBX honeypots, wardialing [2, 3] detection, etc. The student will start by performing a significant state of the art phase which will help in identifying interesting directions. Finally, projects to pursue will be defined depending on resources available either in the Center or that could be provided by MC (e.g., a range of phone numbers, SIP trunking, traffic logs, SS7 access...).

Résumé du projet de recherche (Langue 2)

Today telecom networks are pervasive and we rely on them for our daily activities. So it is for cybercrime, for example, telecom fraud has been reported to cost $40 billion globally[5]. This fraud takes very diverse forms, such as Nigerian scams [6, 7, 8, 4], abuse of compromised PXB, routing phone calls on "gray" networks or security agencies breaking into telecom operators [1]. In general telecom networks are an attractive target for criminals because operations are always linked to billing (e.g., cashback phone numbers, termination costs, premium text messages, bulk SMS spam or denial of phone service). Therefore, there are many ways that are used to manipulate networks and especially to extract revenue from those networks. While some commercial products exist that attempt to mitigate such abuses, this field was left mostly aside by the research community. This is, in part, because the lack of access to equipment or to the telecom networks themselves. The goal of this PhD thesis will be to investigate the different classes of cybercrime and fraud on telecom networks, develop experimental tools for improving the state of the art detection or prevention methods and to improve the understanding of those cybercrime ecosystems. Examples of techniques that may be experimented with are SIP and/or POTS (Plain Old Telephone Service) based PBX honeypots, wardialing [2, 3] detection, etc. The student will start by performing a significant state of the art phase which will help in identifying interesting directions. Finally, projects to pursue will be defined depending on resources available either in the Center or that could be provided by MC (e.g., a range of phone numbers, SIP trunking, traffic logs, SS7 access...).