

ANI / CPN SPOOFING

Pierre-Guy Lavoie

Marek Roy

Définition Téléphonique

ANI - Automatic Number Identification

ALI - Automatic Location Identification

ANAC - Automated Number Announcement Circuit

BTN - Billing Telephone Number

CPN - Calling Party Number

CID - Caller ID

CNAM - Caller ID NAME

NPA - Number Plan Area / "Area Code"

NXX - 3 digit prefix / "Exchange"

-- <http://www.clipx.net/npanxx.php> --

Vulnérabilité Générale

Pourquoi sommes-nous concerné?

- Rend l'afficheur téléphonique inefficace
- Camoufle l'identité de l'appelant
- Permet à un imposteur de se faire passer pour quelqu'un d'autre
- Déjoue l'authentification basée sur le numéro de téléphone

CPN SPOOFING

Quel est la méthode la plus utilisée?

- Serveur Linux (Gentoo)
- Application PBX (Asterisk)
- Carte ISDN/E1 (Digium)
- Telephone IP (Snom)



Situation numéro 1

Vérification du numéro de téléphone spoofé.

- MCI 1-800-444-4444 / Vérification CPN Seulement
- Utilisation du script `cidspoof.agi`



Situation numéro 2

Simuler la communication entre 2 individus.

- A reçoit un appel avec le # de téléphone B
- B reçoit un appel avec le # de téléphone A
- Enregistrement de la conversation



Situation numéro 3

Déjouer l'authentification CPN.

- Vérification du système sans spoofer le numéro
- Utilisation du numéro valide
- Établir la communication
- Utilisation des services



ANI Spoofing

Méthode utilisée

- Utiliser Asterisk afin de spoofer le CPN
- Appeler un service de carte d'appel vulnérable
- Appeler la victime avec le nouveau ANI

ANI 1-418-688-1234

1-418-688-1234

1-800-333-6666

CPN 1-418-688-1234

1-800-333-6666

1-800-333-6666



Remarque

Les conséquences de cette vulnérabilité

- Les SCAMS téléphonique seront à la hausse
- Des systèmes basés sur le CPN seront accédés illégalement
- Retracer l'origine d'appelle deviendra un vrai casse-tête

Solution = Présentement Aucune

Brève période de questions

MERCI

[HTTP://WWW.SEKCORE.COM](http://www.sekcore.com)

pglavoie@sekcore.com

mroy@sekcore.com