CallerID Spoofing

Andrew White
VP for Technology and Standards
ATIS

April 23, 2015

Background

- The issue with caller ID spoofing is growing with the implementation of SIP traffic.
- SIP is more prone to spoofing because it is an end-to-end signaling protocol while allows customer systems and devices to more easily originate fraudulent traffic.
- By contrast, the legacy SS7 system was intended to be used within a trusted system of communication service and database providers.
- Today, SS7 also has challenges with spoofing because of SIP-originated traffic that transits onto the legacy network.

Fraudulent Call Types

	Description	Example
Robocalling	Large-volume, automated solicitations	The FTC has brought over 100 lawsuits against over 600 companies and individuals.
Vishing	Calls impersonating specific companies, banks, or government agencies for fraudulent purposes	Call purporting to be from Microsoft for the purpose of gaining computer access and gaining false payment
SWATing	Calls designed to elicit a potentially significant emergency services response	False calls to 911 reporting “a suicidal gunman holding two hostages”

Call Verification Activities

- ATIS PTSC: IP NGN eCNAM
  - Draft document is in development to provide extended caller ID information
  - CNAM Plus: Extended Name (mandatory)
  - CNAM Plus: Additional Caller Information (optional)
    - May included address, business, and other information
- IETF STIR: Secure Telephone Identity Revisited (STIR)
  - The STIR Working Group (WG) is developing a solution to ensure that the calling party is authorized to use the presented phone number.