european communications office

International Telecommunication Union

ITU Workshop on "Caller ID Spoofing"

(Geneva, Switzerland, 2 June 2014)

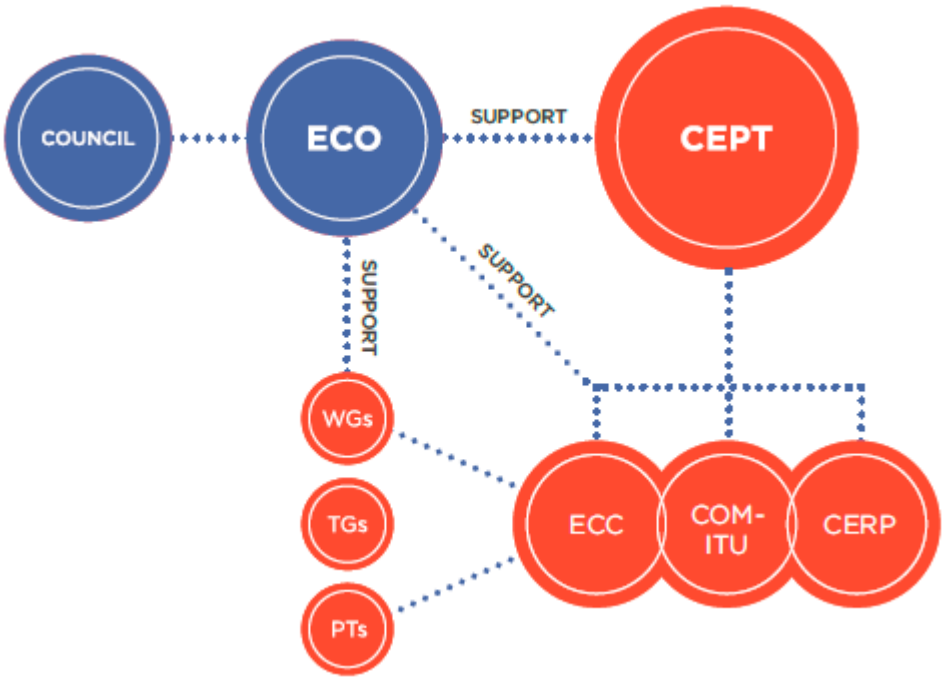
Caller ID Spoofing – Good and Bad

Freddie McBride
Numbering & Networks
European Communications Office
freddie.mcbride@eco.cept.org
Follow us on Twitter **@CEPT_ECC**

european communications office

About CEPT/ECC

CEPT ECC Electronic Communications Committee



SUPPORTING CEPT

The ECO provides a Secretariat for CEPT (including its Presidency) as an umbrella organisation for its three autonomous business committees.

Contents

- Definition of Caller ID spoofing
- History of CLI and erosion of trust in CLI
- Case Study: Experience from Ireland
- Lessons Learned
- Useful references
- Introduction of ongoing work stream within ECC/WG NaN on “Evolution in CLI – Decoupling of rights of use of numbers from service provision”

Caller ID Spoofing is bad!

- Wiki Definition:

"Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, a Caller ID display might display a phone number different from that of the telephone from which the call was placed……

……..The term is commonly used to describe situations in which the ***motivation is considered malicious****."*

- Important Policy Consideration

ITU Policy initiatives to tackle spoofing should be cognisant of the fact that scenarios exist where the motivation may not be malicious.

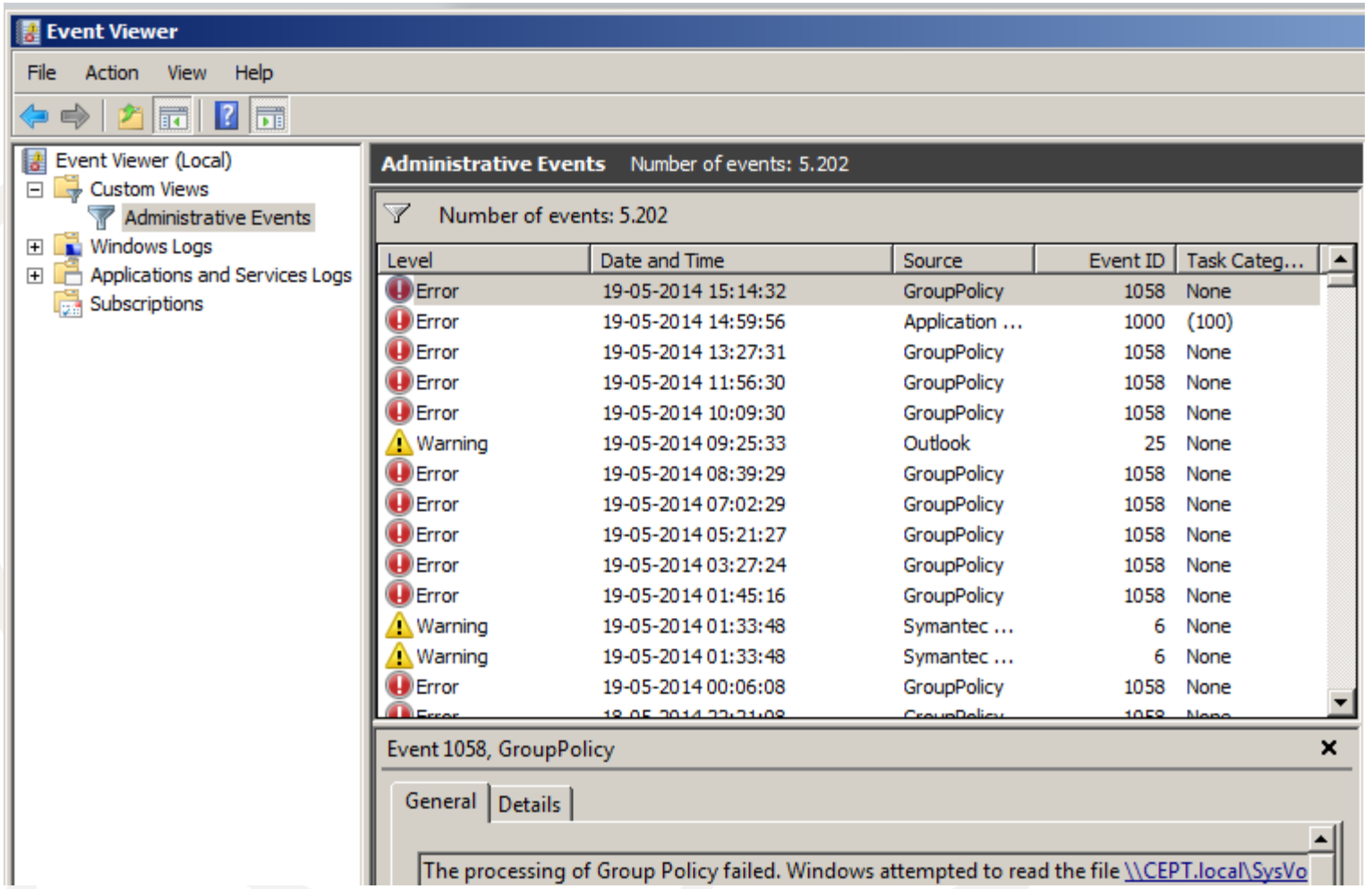
Some history

- CLI was historically an important and trusted identifier
- CLI set by originating operator and trusted by transit and terminating operators.
- As intelligence moved from the network to the terminal, user-generated CLI became possible and the trust in CLI began to decrease
- Use of Internet for VoIP services further eroded that trust

Experience from Ireland

- Online PC Doctor scam
  - Professionally organised scam
  - To make its offer seem more genuine, its website listed an Irish number which people can also call
  - Aim was to target unsuspecting, vulnerable groups
  - Irish numbers auto-dialled by call centre application. When call answered called party connected to call centre agent
  - Agent proceeded to tell called party that they have a virus on their PC. Called party asked to open up Event Viewer on PC

Event Viewer



Experience from Ireland-cont'd

- The agent used a free tool called Log-MeIn which gives remote access to the PC
- €149 - €249 quoted to "fix" problem (which was to clear the event viewer log!). User asked for credit card details
- No rogue antivirus, keyloggers or Trojan Horse programmes installed
- A very basic scam – essentially its just social engineering
- ….but the numbering played a crucial role. The victims trusted the Irish Geographic number presented as CLI
- How did the scammers get Irish geographic numbers?

Numbering Resources Used

- Major VoIP operator had a secondary allocation of Geographic Numbers from an Authorised Operator in Ireland
- To get such a number the Irish National Numbering Conventions require that a user have a registered address within the Minimum Numbering Area (MNA)
- When signing up the address given is not validated it is merely an ”assertion” by the user that they have an address in the MNA
- Online PC Doctor used this VoIP service to target its unsuspecting victims
- Crucially, when law enforcement authorities had difficulty in tracking down the perpetrators and bringing them to justice, the Numbering Conventions were sufficient to instruct the operators concerned to cease services on the numbers concerned. The VoIP operator and the Number Range assignee both co-operated without question
- However, it was then quite easy to start again with a new number and indeed valid addresses were provided for these new subscriptions in the Dublin area (usually commercial properties for sale)

Some Lessons Learned

- Outside of numbering, jurisdiction a huge problem in tackling these scams
- Awareness campaigns promoting customer vigilance most effective way of stopping scams
- Of course, there will always be some victims before awareness campaigns are effective
- Co-operation between national and international carriers is essential. The originating operator is the gatekeeper
- A harmonised international solution (i.e. ITU policy measure) could help
- Technical solutions required to validate originating numbers particularly for VoIP calls would also help
- ITU-T SG2 should take note of IETF STIR work in this regard

References (European Context)

- Some ECC deliverables which could also be useful inputs to inform any future policy initiative by the ITU
  - ECC REPORT 133 - Increasing Trust in Calling Line Identification and Originating Identification
  - ECC RECOMMENDATION 11/02 - Calling Line Identification and Originating Identification

Evolution in CLI Usage: Decoupling End User Rights to use Numbers from Service Provision

- Current work stream for Project Team Number Portability
- Focus on different scenarios where numbers used as CLI for services not directly associated with that number.
- Some examples – Seperate inbound and outbound services for call centres, ”SIM Stickers” for long distance calls.
- Many of these services are legitimate and usually have regulator consent on a case-by-case basis.
- Report at an early stage. Next meeting in June `14.
- The Report, when ready for consultation, can be sent to ITU-T SG2 for information

Thank You!

Freddie McBride,
Numbering & Networks
European Communications Office
freddie.mcbride@eco.cept.org
Follow us on Twitter **@CEPT_ECC**