M3AAWG
MESSAGING MALWARE MOBILE

Mobile SPAM in India

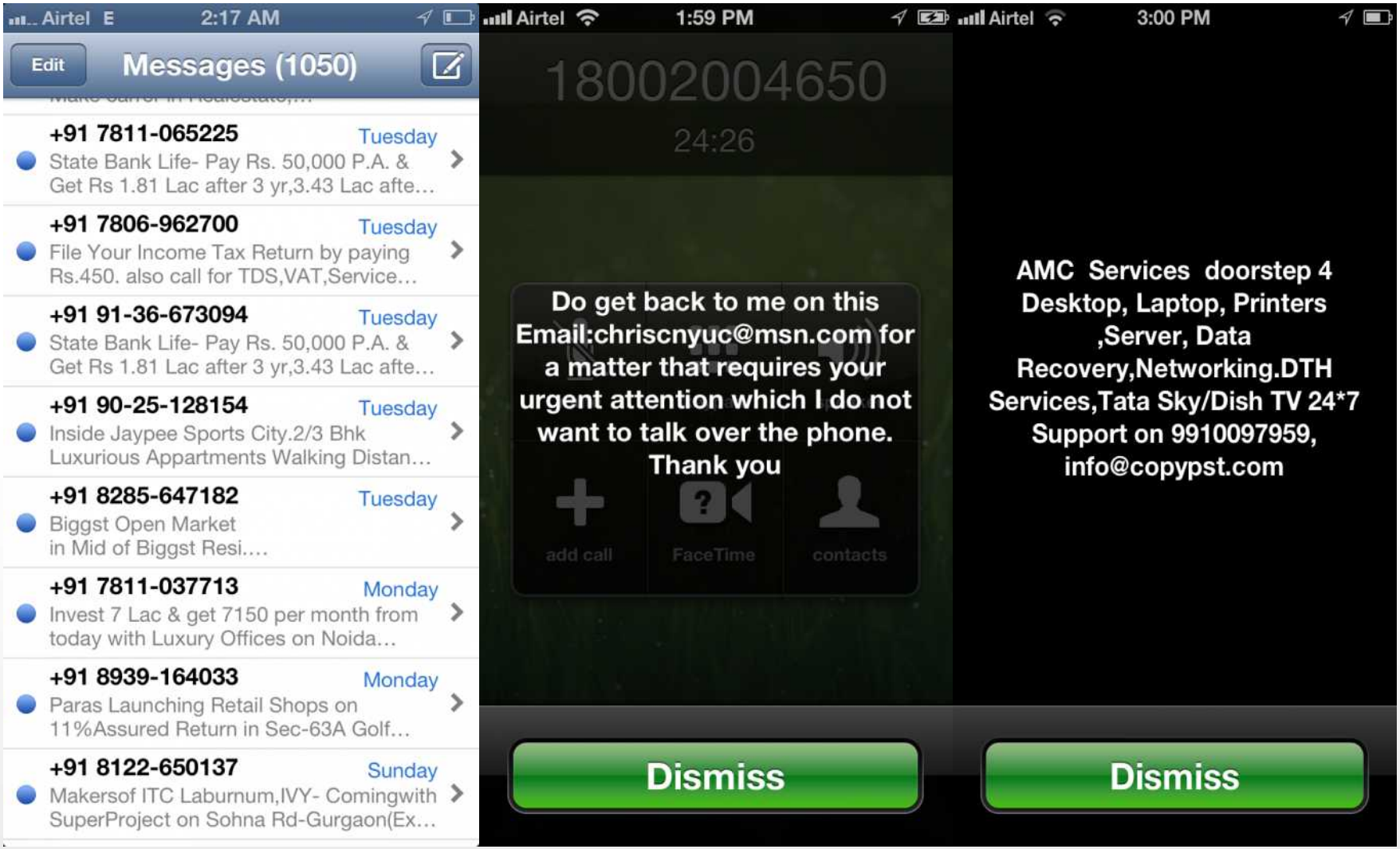
Animesh Bansriyar

4th August

Mumbai

ILLUSTRATION FOR TIME BY TOMASZ WALENTA

How do our Phones look these days?



Mobile Messaging Trends

Mobile Messaging is Target of Choice for Attackers

1. DMA/IAB Mobile Messaging study, 2011

Favorable Economics

- Unlimited messaging plans reduce per-message costs
- Pre-existing billing relationship to exploit and monetize

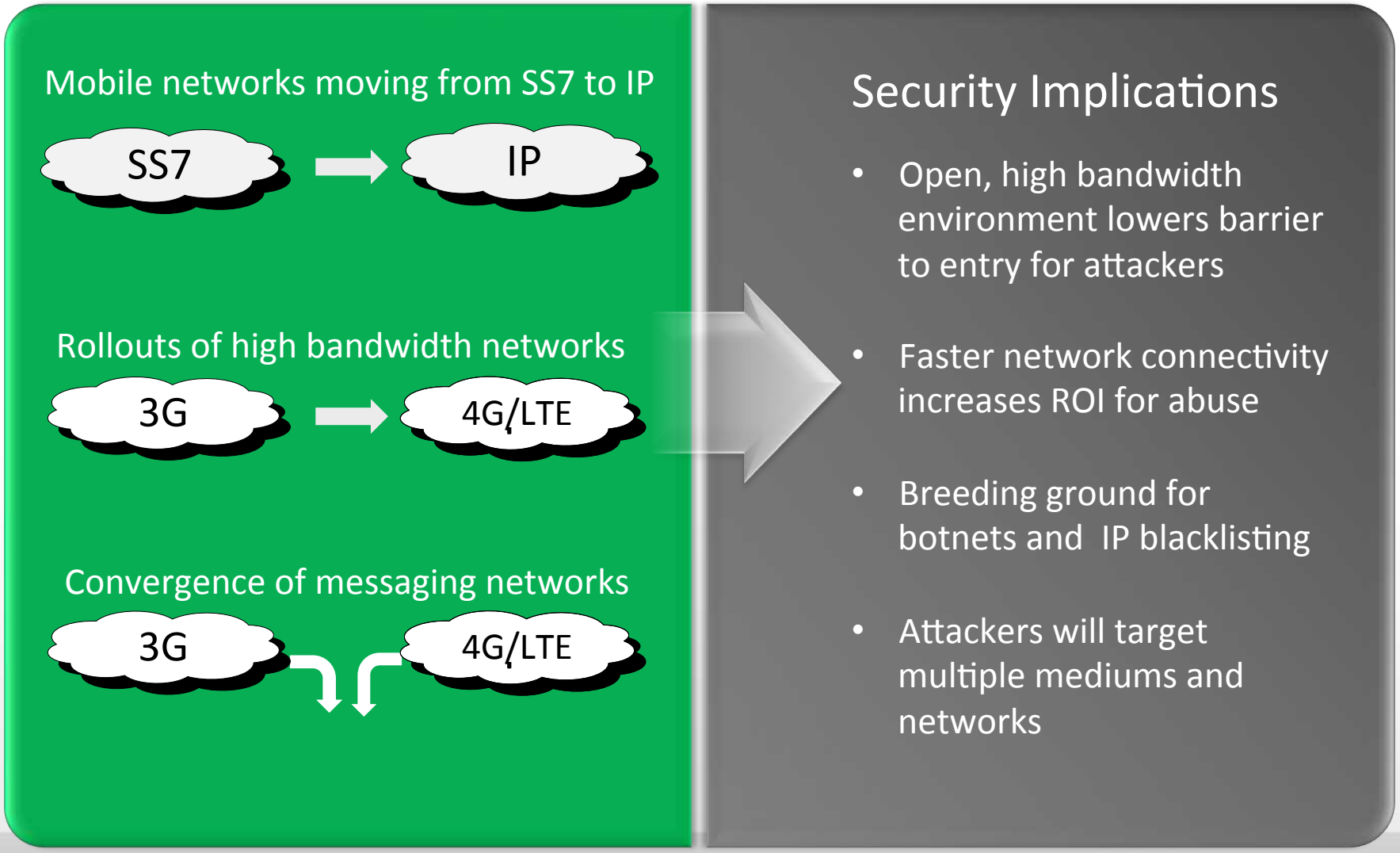
Subscriber adoption and trust in mobile operator

- SMS has 2.5 times more reach than email
- Used for news alerts, billing payments, business updates
- 98% open rate compared to 20% for email [1]

Lack of security impediments

- Most messaging environments and devices vulnerable
- Standard defenses (keyword filtering, volumetrics, anti-spoofing) easily defeated

Networks are Evolving and Converging



Threat Environment is Evolving

Malware moving to new, open systems

- Targets popular platforms such as Android
- Proliferates via applications in app stores
- Increasingly sophisticated and polymorphic

Background calling and texting apps

Trojans send premium rate SMS messages

Keyloggers that steal personal/ financial info

CBR Computer Business Review

Yahoo News 12.12.12

Researchers discover new Android phone spam botnet

"…changes the economics of SMS spam as the spammer no longer has to pay for the messages"

Subscribers are Evolving

Increasingly mobile…

10 Billion

devices by 2020[1]

1. IBM Research, 2012

and want more security

92% Of British adults who text say it is at least somewhat important that their carrier have a mechanism for reporting mobile spam.

64% U.S. adults who text say it is important or very important that their carrier have a mechanism in place to report ‘’mobile spam’’. [2]

What is Mobile SPAM

Definition of SPAM in Mobile Messaging

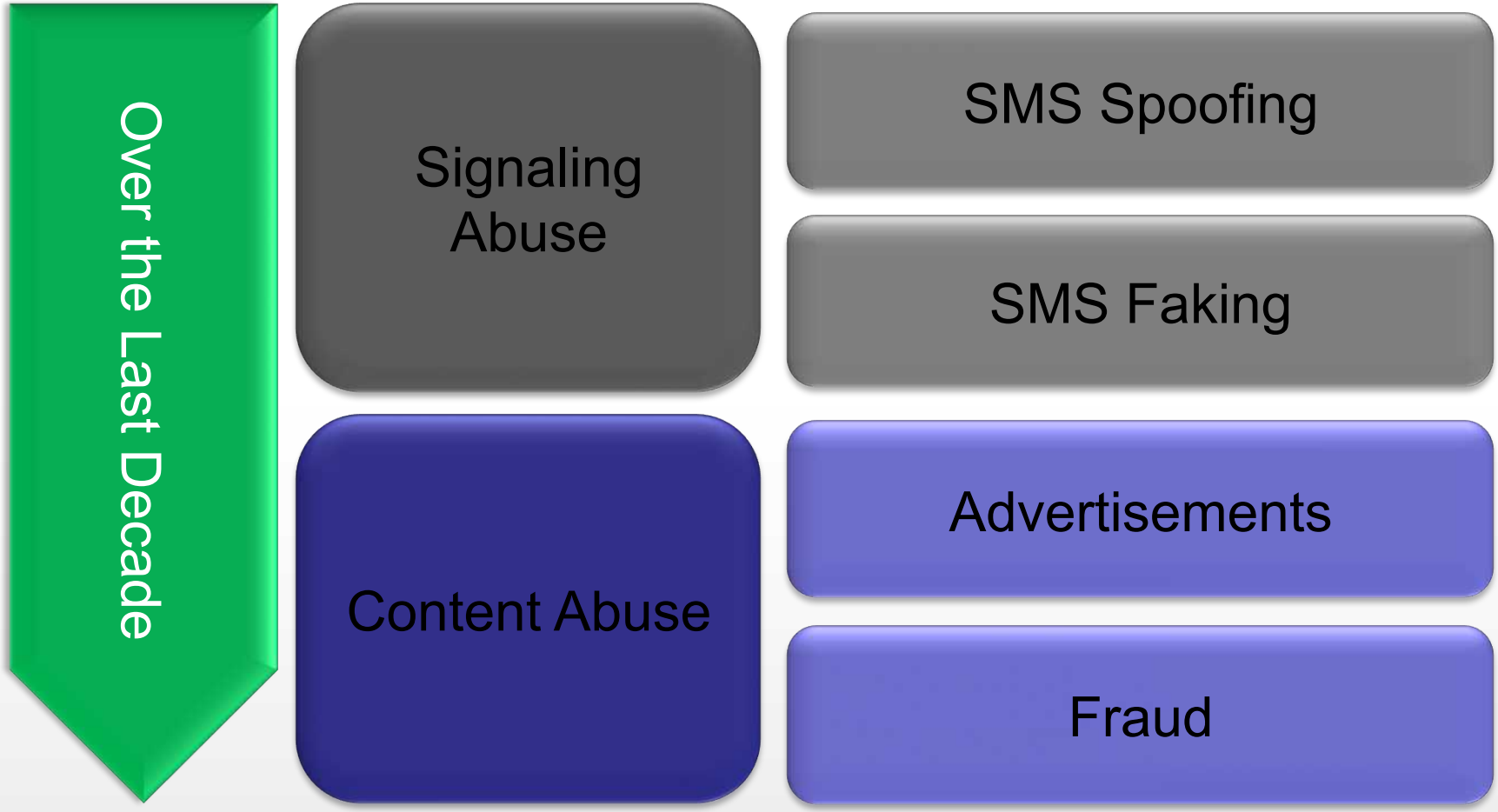
Traditional Understanding of SPAM

messages sent / received via illegal routes, over spoofing or faking, etc

True definition of SPAM

- Unsolicited Commercial Communication using any route
- Any communication not-opted in

Progression of Mobile Messaging Abuse

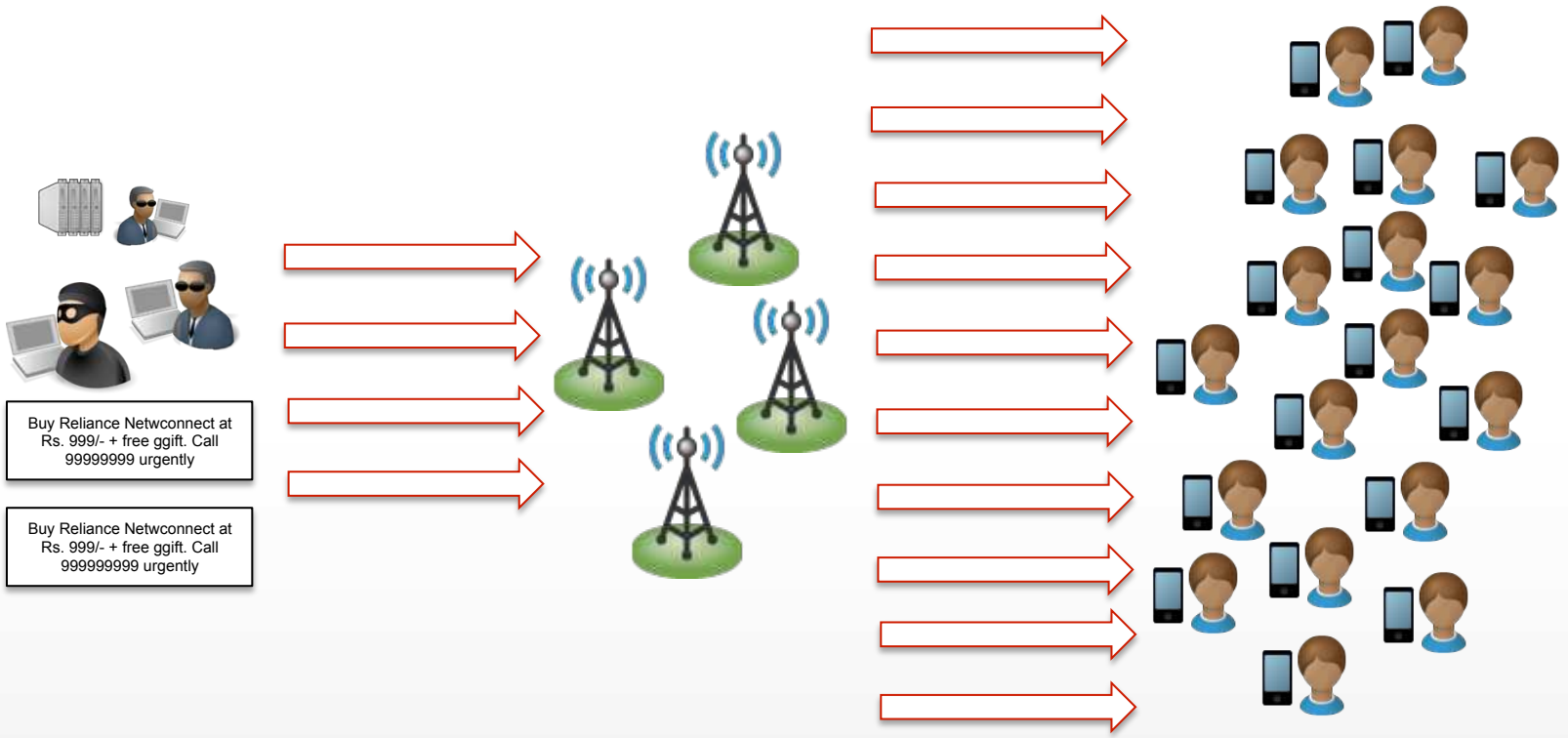


Mobile SPAM vs Email SPAM

- ✓ There is no SPAM Folder for SMS
- ✓ People trust their Phones more than their Email Accounts
- ✓ Cost of sending Mobile SPAM zeroing down towards the cost of sending Email SPAM.
- ✓ Its easier to block Originating Mobile SPAM than Incoming Mobile SPAM

Content Abuse

Typical Attacks



SPAM Attack #1

DLF Launching soon! The Ultima-Luxury Apartments -3/4 Bhk Appts. \nSec-81.Gurgaon.Limited Inventory on First Come First Basis.Call-8287330898 for Priority Booking

Call to Action	• 2 different Numbers
Number of Messages	• 12453
Sending Numbers	• Multiple Sending Numbers > 80
Timeline of Attack	• Attack Spread over 2 hours

SPAM Attack #2

Invest 36 LACS Get Rs.36000 pm, lease guarantee, fully furnished office at World Trade Center of New York @ New Gurgaon! Limited availability. Call 7836862292

Call to Action	• one
Number of Messages	• 4295
Sending Numbers	• Multiple Sending Numbers > 50
Timeline of Attack	• Attack completed within 5 minutes

Messaging Terms

- Traditional Messaging:
  - MO / MT
    - P2P
    - A2P
    - P2A
- Newer Mobile Messaging Vectors
  - IP Messaging
  - RCS

Fight against Mobile SPAM in India

What has DOT / TRAI been doing to stop Abuse before 2012

- Telemarketers had to register themselves
- DND Service
- Commissioning of 1909 for Spam Complaints
- Originating P2P messages restricted to 200 per day
- Originating P2P messages beyond 100 per day to be charged additionally

New Regulation since 2012

- Most important regulation to combat SPAM
- Focusing on Message Origination (MO) rather than Message Termination (MT)
- Says *"More than 200 messages with the same signature should not be allowed from the same source or number "*
- Reasons:
  - Use of sophisticated Equipment
  - Multiple A-party Numbers used for the attacks
  - Typical Attacks sent too quickly (a few minutes) or too slowly (a few hours), etc
  - Changes in Content to bypass typical volumetric controls on a per-MSISDN basis
- Risks:
  - Chances of transactional messages getting caught in these filters.

What have MNOs been doing till now?

Traffic Type	Previous Status	Current Status
CDMA - MO	Unfiltered	In the process
CDMA – AO	Semi-filtered	Strict Licensing
CDMA - Domestic MT	Unfiltered	Easy to be done
CDMA – International MT	Semi–filtered	50 - 50
GSM – MO	Unfiltered	In the process
GSM – AO	Semi-filtered	Strict Licensing
GSM – Domestic MT	Unfiltered	$$$
GSM – International MT	Semi-filtered	50 - 50

Impact of Mobile Messaging Abuse for MNOs

- Increased Volume of Messages
- Increased Spam Complaints
- Brand Damage
- Revenue Loss and / or Possible Customer Churn
- Increased Operational Costs

Recommendations for Indian MNOs

- ✓ Apply Signalling Firewall for Anti-Spoofing and Anti-Faking
- ✓ Implement latest TRAI regulation and other volumetric filters
- ✓ Implement simbox detection
- ✓ Implement aggressive Blacklists
- ✓ Disconnect spammers from their Network if found to be spamming
- ✓ Listen to your consumers - Implement Spam Reporting System
- ✓ Implement a no-abuse clause in the User Contracts

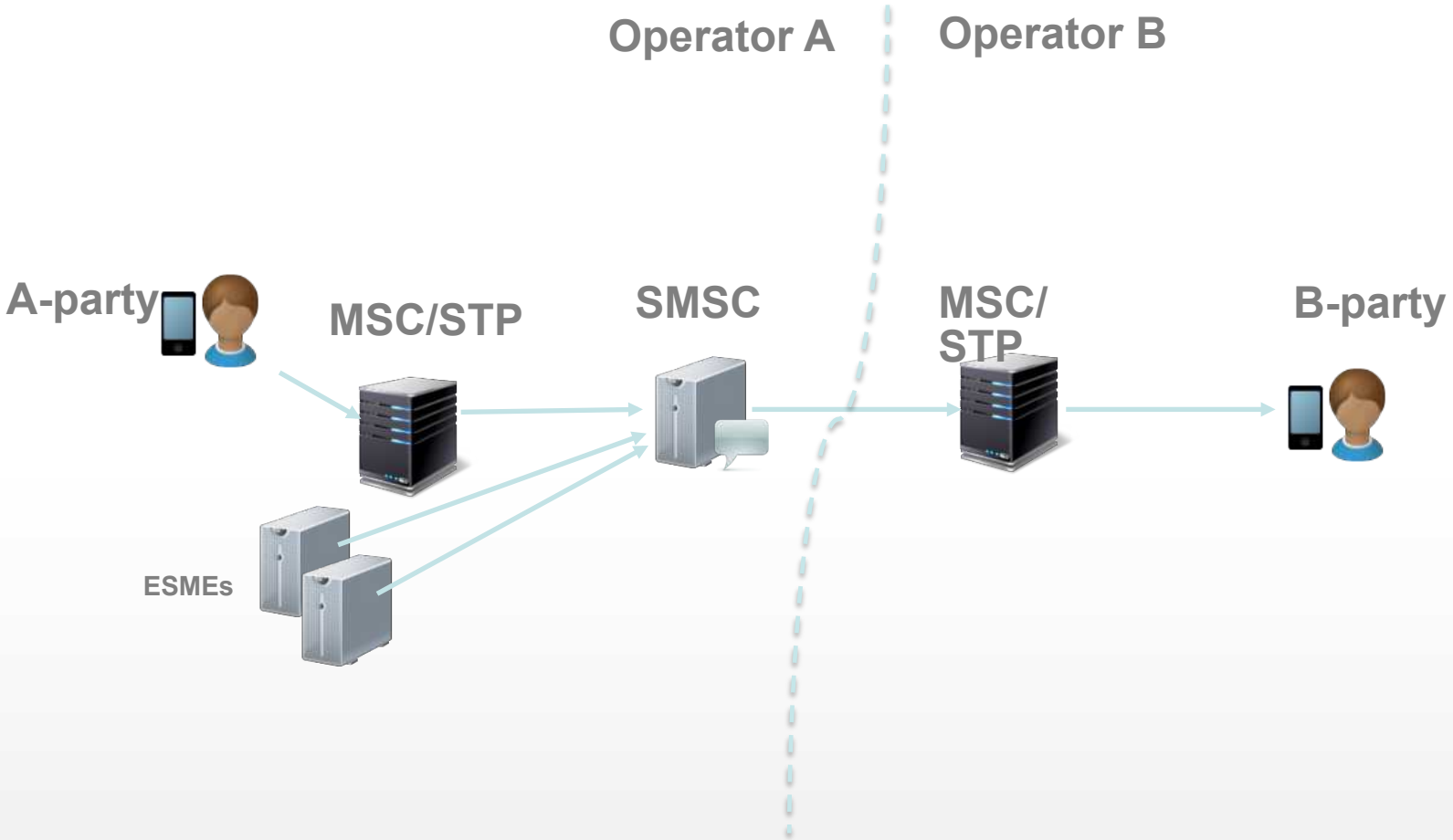
TRAI Spam Reporting Service

- Send a text to 1909 with the correct format
- Operator Call center at 1909

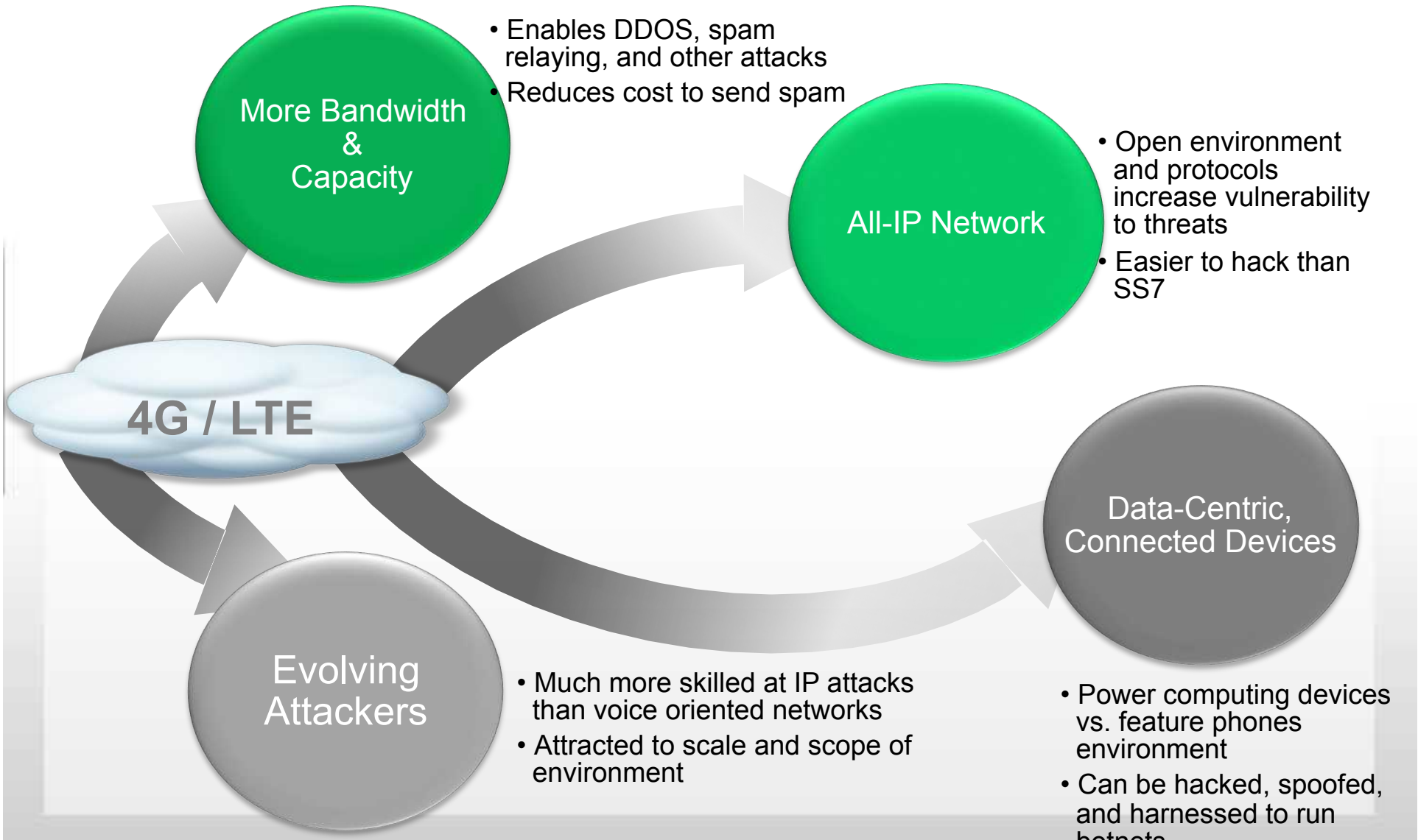
Challenges for Indian MNOs

- ✓ Dearth of Anti-SPAM Experts (Messaging Teams typically Signaling Experts)
- ✓ Complicated / Distributed Messaging Architecture
- ✓ MO Spam Easier but MT Spam trickier and Expensive to Implement
- ✓ No point-and-click Solution Available for Anti-Spam
- ✓ Large SIs / MS providers don't have necessary Expertise
- ✓ Investment in CAPEX and Operations / MS.
- ✓ Potential loss of Messaging revenue
- ✓ Possible Litigation
- ✓ False positives

High Level Messaging Architecture



The future: LTE and challenges



Q AND A