Technology presentation

Verji SMS

Odd Helge Rosberg
CTO and Co-Founder

Rosberg System as

What is Verji SMS?

- A solution to protect Smart Devices from infections using SMS as an infection method
- An SMS cannot be dangerous, can it?
  - An SMS can contain code to infect your smart device, and is invisible to the user
  - They are used for:
    - Infecting your device invisibly, making it possible to see all activity and content
    - Seeing where you are at any given time
    - Destroying your phone, or leaving it offline
    - Military / Government surveillance
    - Industrial espionage
    - Financial fraud
    - And much more
- We have the ONLY solution on the market that protect you against all this.

SMARTPHONES

- **Smartphones have three different Processor units and OS's**
  - Operating system, where the GUI is, typically iOS, Android, Blackberry, Windows Phone
  - Modem, takes care of all communication, typically embedded Linux
  - SIM-card, controls the modem and can contain code like bank security signatures (BankID) functionality.
- All three levels can be infected using SMS
- Antivirus solutions can only monitor the OS, not the modem or the SIM card

SMS attacks

- Attacks using SMS as an attack vector has been known for a few years now. Until now the seriousness of these attacks have been perceived to be low to medium in range.
- This has changed now, at least the knowledge about serious attacks.
- Attack types using SMS:
  - Silent ping
  - Fuzzing
  - Remote cloning of SIM-cards
  - Provisioning service SMS’s
- Attacking weaknesses in the GSM AT command set
  - SIM card upgrades
  - Remote wipe
  - Remote location
  - Etc…

How can we stop this?

- There is a wide selection of threats using SMS, and though Telco's try to plug these holes, they are not able to stop everything
- Stopping these effectively will cause a lot of legitimate functions, especially in the m2m space.
- Many threats are invisible to the user and does not require any user interaction.
- Untraceable by anti virus systems
- The only way to stop these threats is to make sure the device does not receive any SMS's at all.

Our approach

- We communicate with the Telco’s SMS-C server, having the SMS’s delivered there and not to the smartphone.
- We clean the messages, searching for known threats and service SMS’s in general.
- We wrap the SMS’s into an encrypted package (256 bit AES) and send them over the Internet to the APP
- The APP completely replaces the standard SMS service on the phone
- In later versions we will also include femtocell protection and roaming services.
- For maximum protection the ideal solution is to combine our service with a cryptophone solution.

Verji SMS

Server:

- Linux Server platform.
- Low memory, disk, and processor requirements
- Easily scalable
- Requires a connection to a Telco, or a Telco partner.
- No modems required

Clients:

- Android
- iOS

BlackBerry (Android compatible), Native QNX version in v2.

- Windows Phone (v3)
- Installed app takes over the SMS functionality.
- AES 256 encrypted send/receive
- Enterprise managed App
- Branding optional

Functions:

- Send / receive as normal
- Communicates with the Telco's SMS-C
- Threaded view
- Detail view

Versions

V1

- Server
- Cleaning engine
- Encryption
- Android app
- iOS app
- RIM (Blackberry) app on Android compatible OS versions
- End to end encryption

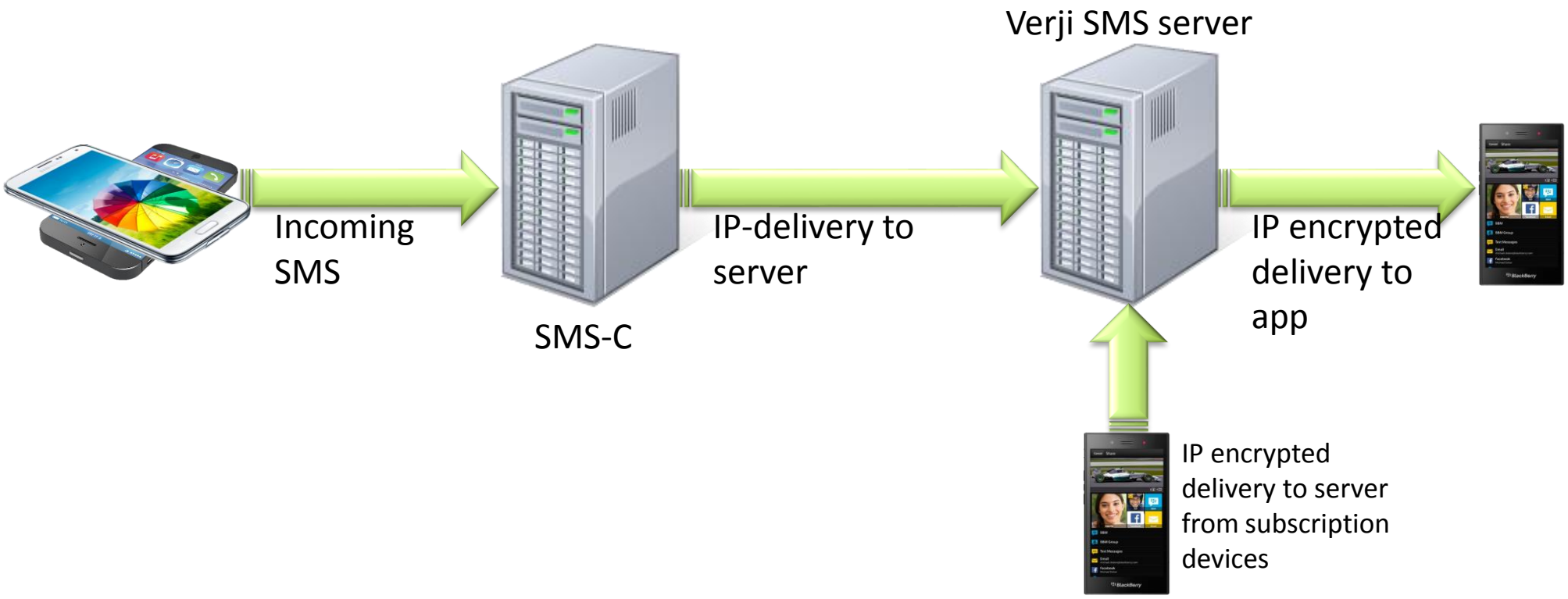
V2

- Native Blackberry QNX app
- Roaming encrypted SMS support

V3

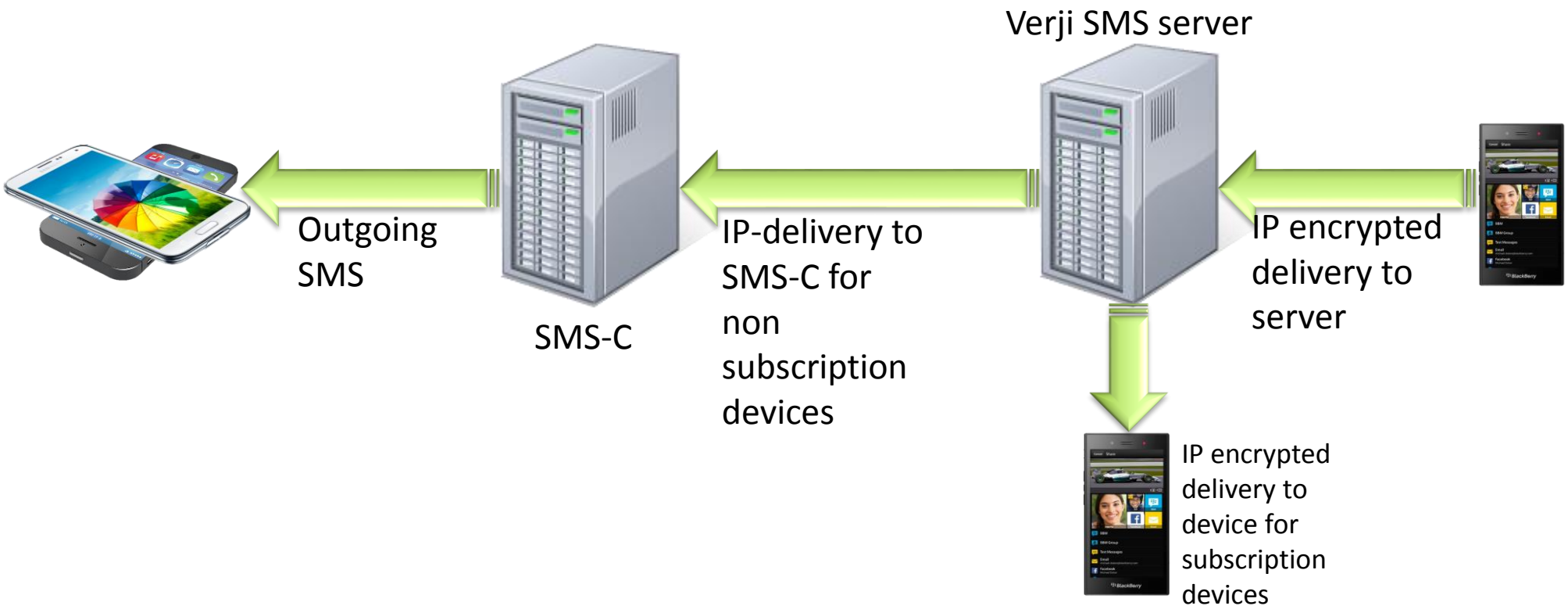
- Windows Phone app
- Femtocell, macrocell, microcell, picocell and IMSI catcher protection

Standard reception of SMS



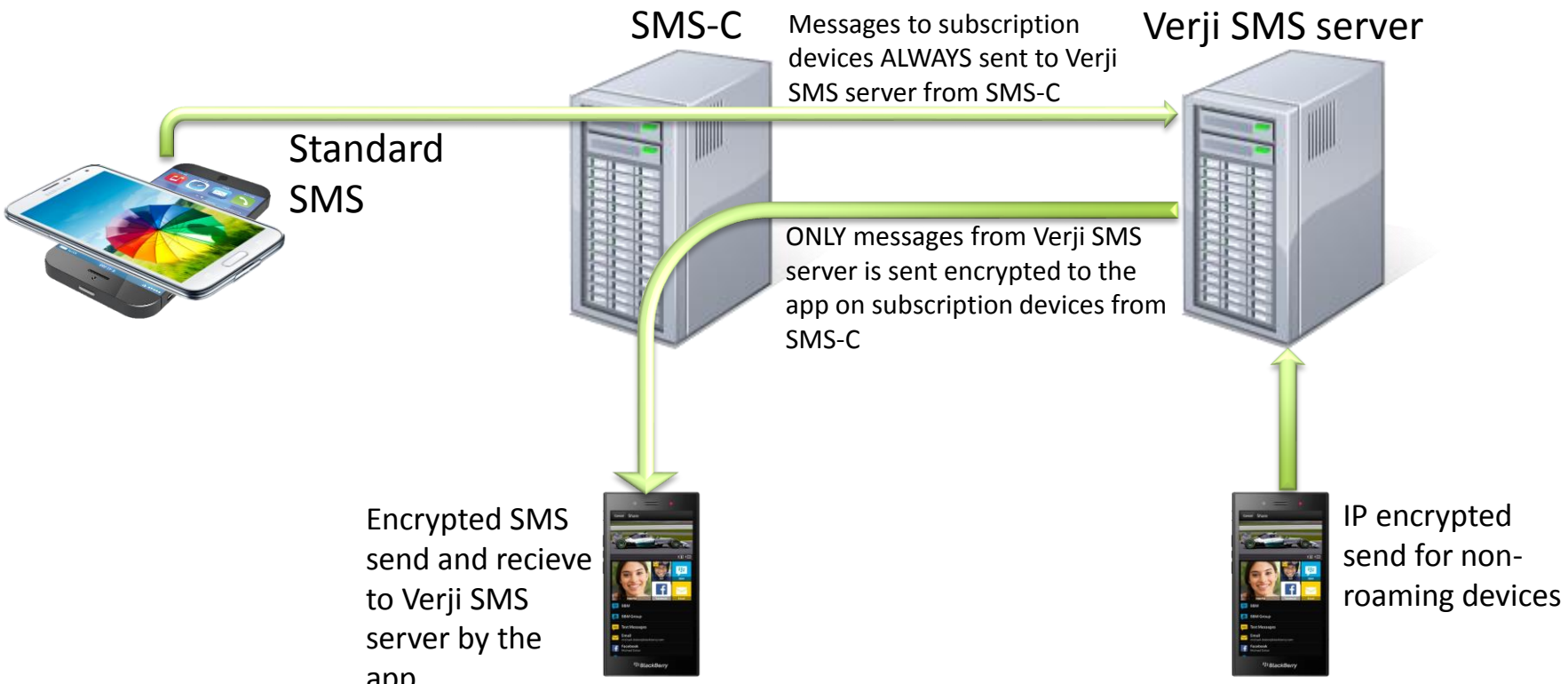
The SMS is delivered to the Telco's SMS-C system. The SMS-C will not deliver directly to the subscriber, but deliver the messages to your Verji SMS server for cleaning. After cleaning, the messages that has been cleaned will be encrypted and delivered to the handset using TCP/IP.

Standard sending of SMS



The SMS is delivered to the Verji SMS server where it is decrypted, checked, and then sent to the SMS-C if it is not a subscription device, but if it is it will be encrypted and sent securely to the app on the second Smartphone.

Roaming SMS



Here the SMS-C is set up to ONLY send what is received from the server to the handset. No other messages will be allowed. All messages to the roaming device are delivered to the server. All messages to the roaming device are encrypted and delivered to the app. The process is reversed for sending from the handset, the server is always in control.

Encryption options

- Encryption can be done in different ways in this system depending on the customer's needs:
- All traffic between the Smartphone app and the server is always encrypted.
  - Encryption, standard usage
    - All traffic is encrypted wtih 256 bit AES, all messages are logged on server, messages are re-encrypted before delivery to other Smartphone devices, sent as standard SMS's to other devices
  - Encryption , end to end
    - As long as a message is designed to go to another Smartphone device on the server, the connection is set directly between the two devices, nothing is logged on the server. To a non subscription device it is sent unencrypted.
  - Encryption, internal version.
    - As previous example, but here you can only send to other devices within the corporation, not to any external device.

Roles

- ***Rosberg offers:***
  - White label solution
  - Revenue share model
  - IP-license
  - Integration into existing systems
  - Software – third line of support
- ***Distributor provides:***
  - Sales / Marketing
  - Hosting
  - Customer support
  - Customer invoicing

Smart Simple Solid

Contact:
Odd Helge Rosberg
Phone: +47 9321 6630
E-mail: odd.helge@rosberg.com
E-mail: sales@rosberg.com
Skype: odd.helge.rosberg

Rosberg System as