IP Interception, Collection and Analysis: A new approach required

Erik de Bueger 2008

Lawful Interception is like:

SS8™

The Architects of Intercept

PAYING TAX

TAX IN THE NETHERLANDS

- 52% income tax
- 19% sales tax
- Property Tax, Taxation on cars, …….

BACK TO LAWFUL INTERCEPTION:

Building the business case

- Security
- Brand protection
- Liability
- Cost control
- Future proof investment

THREE PILLARS

Economic

Procedural

Technical

CHALLENGE - RESPONSE

- No secret recipe
- Consultative approach
- Applying product in a project fashion
- Offering options and choice

THE REAL DIFFERENTIATOR

Focus

- On Lawful Interception

Scale

- People, partnerships, programs

Stamina

- IOT: version after version
- IP equipment vendor after equipment vendor
- Service

IP

SO NOW IP DATA CAN BE INTERCEPTED

- Automated
- In one format or another
- Organized on a per-case basis
- Potentially in high volume
- What to do with it?

WHAT IS NEW?

CHANGE

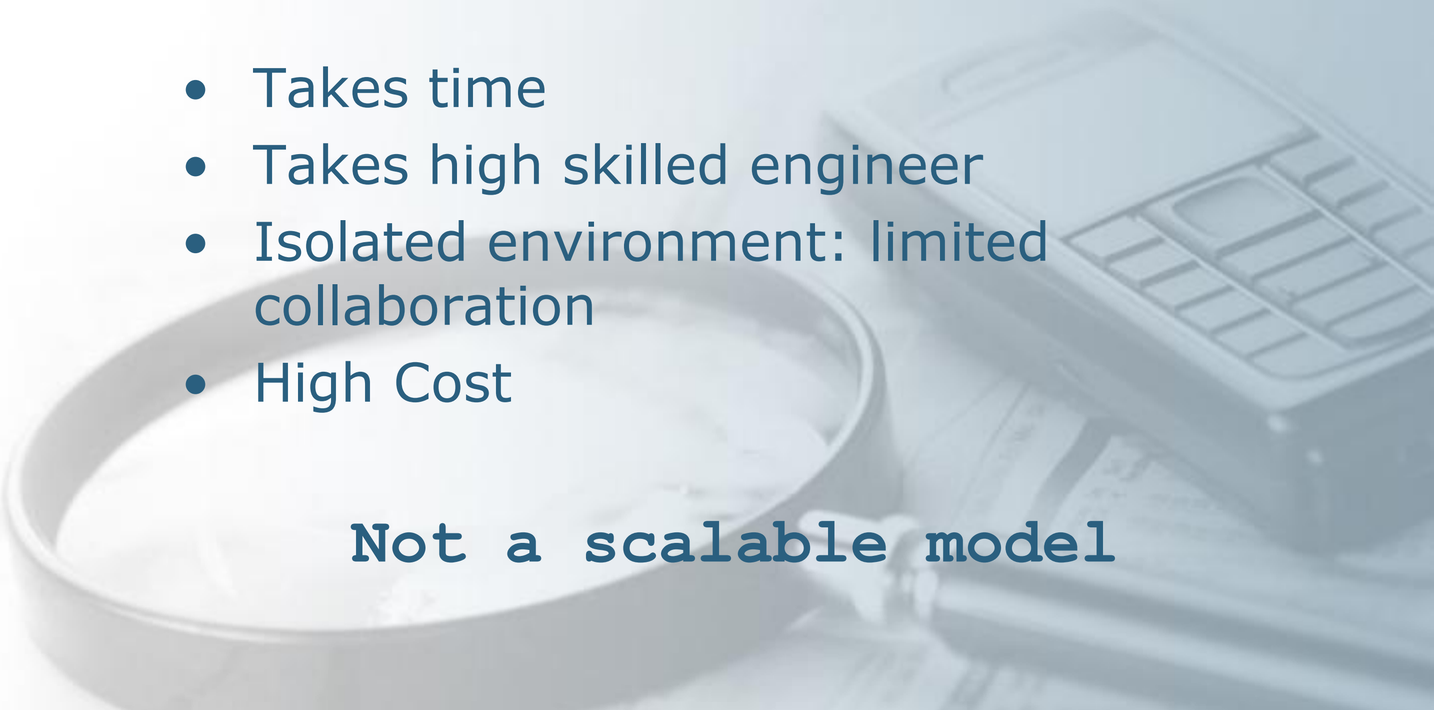
- IP not ‘recordable’: not intended for ‘replay’
- To and From are fluid
- Single Communication – Multi media

LOW VOLUME IP ANALYSIS

- Specialist Job
- Specialist tools
- Hexdumps

- Takes time
- Takes high skilled engineer
- Isolated environment: limited collaboration
- High Cost

Not a scalable model



SCALING UP

Requires a new approach

- Ease of Use
- Record and Replay approach
- Eliminate the required technical skill
- Control – who gets to work on what
- Zoom in – capability to look into detail
- Ability to spot triggers
- Control Cost

HOW?

- Applying a ‘flow’ paradigm
  - There is no beginning and there is no end
  - The Batch approach is outdated
- Reflecting the layered and recursive nature of the Internet and its protocols
- Abolishing the ‘monolithical’ approach
  - Open Architecture based on networked agents
- Reflecting the dynamic nature of the Internet
  - Adding protocols and services without upgrade or even re-compile
- Using a ‘re-use’ approach
  - Use existing viewers and clients as much as possible to visualize content

CONCLUSION

- IP Can be intercepted
  - On a large scale
- IP can be monitored and analysed
  - On a large scale
- REQUIRES A NEW MINDSET

LET'S GET ON WITH IT!