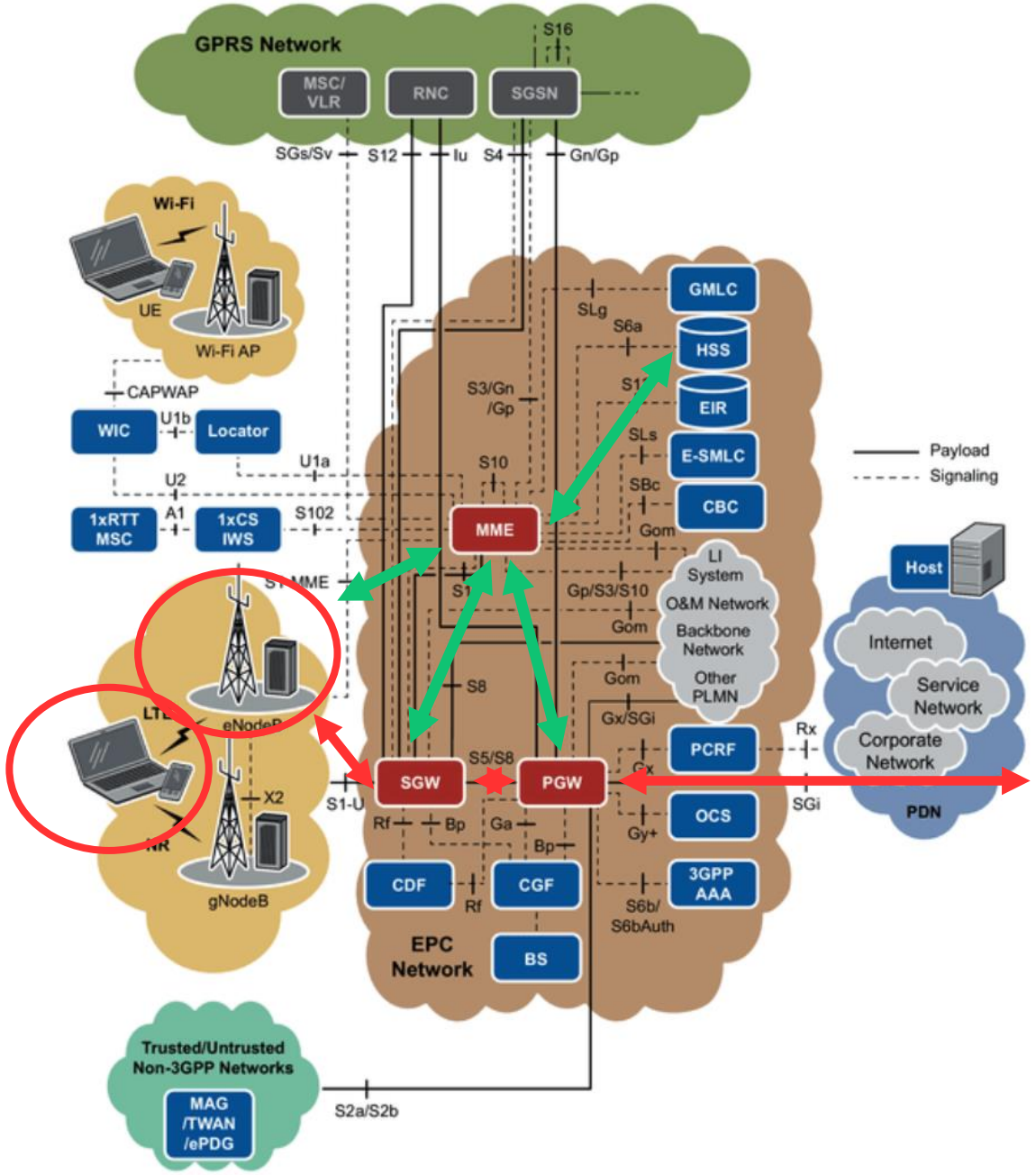
Telecom security challenges

Mathias Weibull, Senior Security Specialist Ericsson AB 2019-10-14

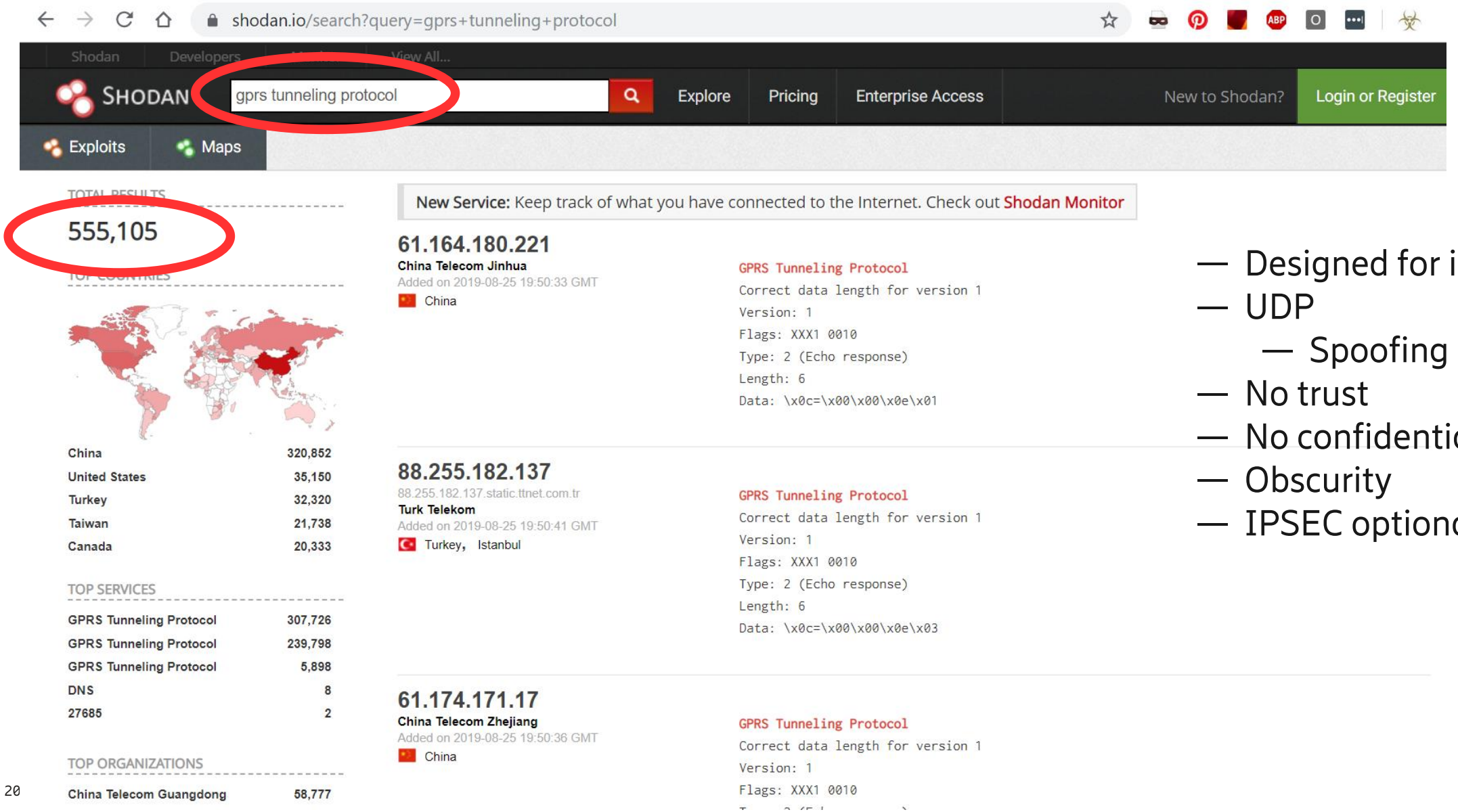
Ericsson

- Telecom systems
  - Base stations
  - Charging
  - User databases
  - Analytics
  - Management
- ~100 000 employees
- 5G

Packet Core


GPRS Network
S16
MSC/ VLR
RNC
SGSN
SGs/Sv
S12
Iu
S4
Gn/Gp
Wi-Fi
UE
Wi-Fi AP
CAPWAP
WIC
U1b
Locator
U1a
U2
1xRTT MSC
A1
1xCS IWS
S102
S1-MME
eNodeB
LTE
NR
X2
gNodeB
S1-U
SGW
S5/S8
PGW
MME
S10
S3/Gn /Gp
SLg
S6a
S1
SLs
SBc
Gom
Gp/S3/S10
S8
Gx/SGi
Gx
Rx
SGi
Rf
Bp
Ga
Gy+
CDF
CGF
S6b/ S6bAuth
BS
EPC Network
GMLC
HSS
EIR
E-SMLC
CBC
LI System
O&M Network
Backbone Network
Other PLMN
PCRF
OCS
3GPP AAA
Host
Internet
Service Network
Corporate Network
PDN
Payload
Signaling
Trusted/Untrusted Non-3GPP Networks
MAG /TWAN /ePDG
S2a/S2b

GPRS Tunneling Protocol @ shodan.io



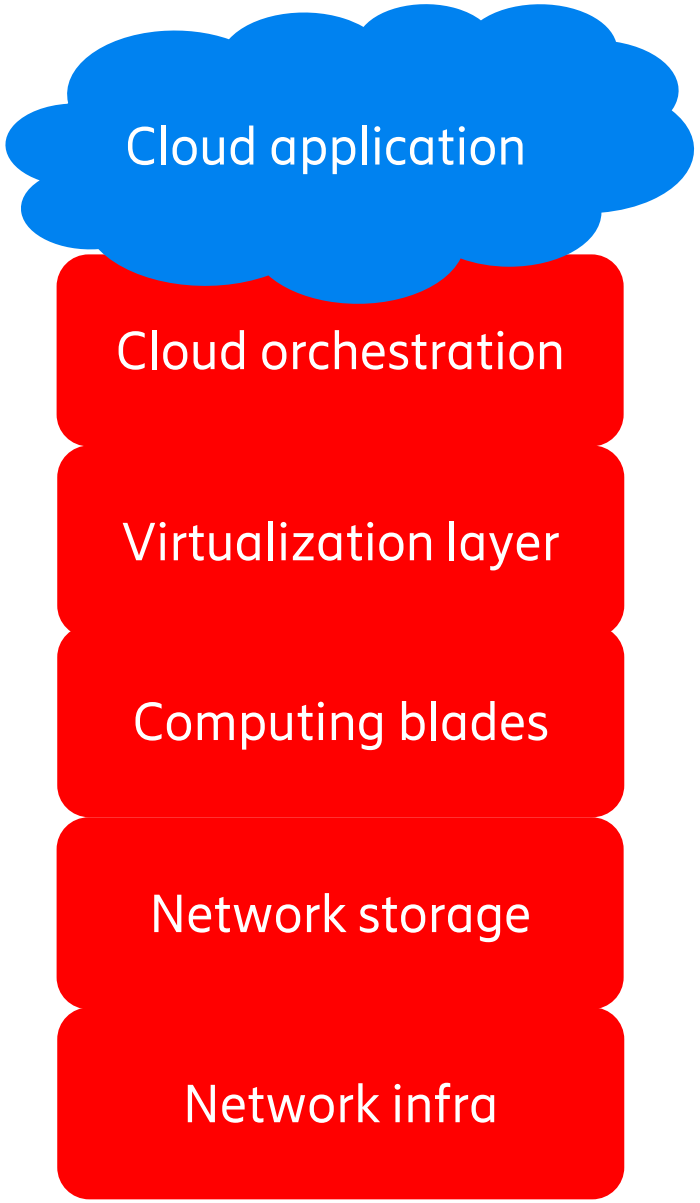
- Designed for intranets
- UDP
  - Spoofing
- No trust
- No confidentiality
- Obscurity
- IPSEC optional

Trends

- Native to virtualization to containers
  - Cut costs
  - Conservative business
- Multitenant – multiple virtualized applications sharing cloud infrastructure
  - Same hardware and infrastructure
- Replacing fixed networks - transport media for
  - Sensitive information, for example bank transactions
  - Safety critical systems, controlling power distribution systems
  - Public Safecty (112, FirstNet)
- Mobile networks seen as part of the (critical) infrastructure
- Privacy

From dedicated hardware to cloud

- Physical interfaces
- Internal storage
- Closed backplane



Microservices and security (telecom perspective)

- Advantages
  - CI/CD
  - Fast patching for vulnerabilities
  - Automation of 3PP monitoring/patching
  - IT Industry standard

- Challenges
  - Sidecars / analytics
  - Dependency to host (shared kernel)
  - Container – container traffic is visible
  - Network separation

- Solutions
  - TLS – Mutual authentication and encryption
  - Secure enclaves
  - Network separation

Hackers – new landscape

- Old school
  - For fun
  - For knowledge, honor
  - Low-end fraud
  - Low-end destruction/disruption
  - Expose security issues

- Today
  - Paid
  - Government
  - Information and vulnerabilities are assets
  - Purpose
    - Political
    - Commercial
    - Impact society
    - Information gathering

Assets

- Privacy related information
  - Calls
  - Payload
  - Location
  - Three reasons
    - Privacy/security regulations
    - Money
    - Statistics
- High availability
- Trust

Threats

- Illegal tracing
  - Specific enduser
  - Geographic area (rogue base stations)
  - Calls/payload/location
- Setting critical systems out of service
  - Emergency calls
  - Other infrastructure
- Fraud
- Information gathering

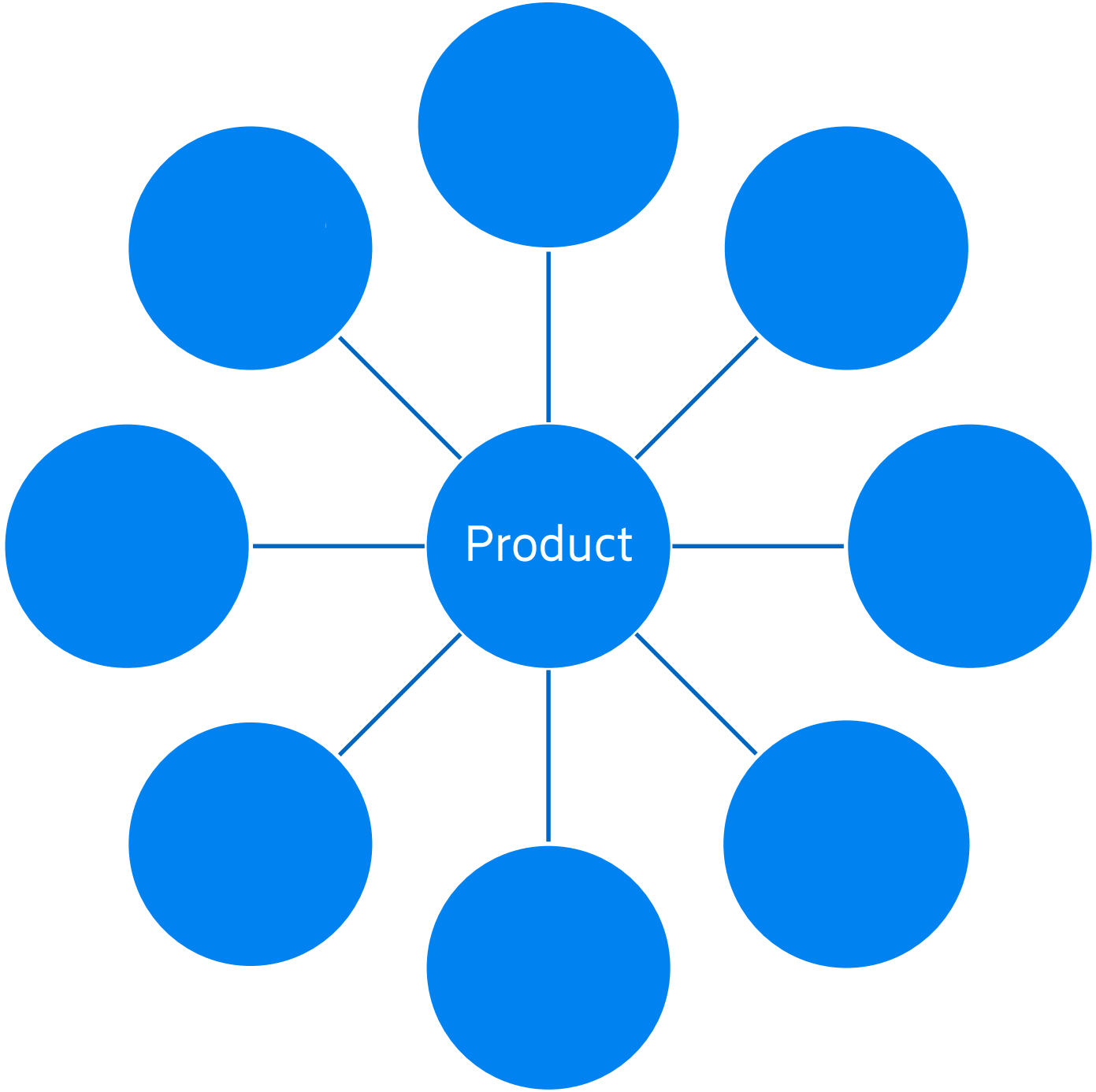
5G

- Security in focus
  - Encryption
  - Authentication
  - Privacy
- New markets
- Implementation reqirements
- Simplify information collection and business – analytics...
- Multiple radio standards
  - 5G radio
  - NB-IOT
  - WiFi

Third party products

- Open, semi-open or closed source
- gcc, MySQL, Apache, Openssh, Openssl, Linux...
- Pros
  - Fasttrack to standard well-known protocols/databases/webservers
  - Not core product parts for Ericsson
  - Security
- Cons
  - Integration
  - GPL/Apache/"free for non-commercial use"

What makes a secure product?



Ericsson in security

- 5G security
- Secure development (design, test, delivery, tracability,...)
- Analytics – privacy
- Telecom grade security
- Business ethics

Key takeaways

- More advanced attackers
  - States/companies
- Increased complexity
  - Virtualization/containers/5G
- Mobile telecom used in critical infrastructure

Q&A