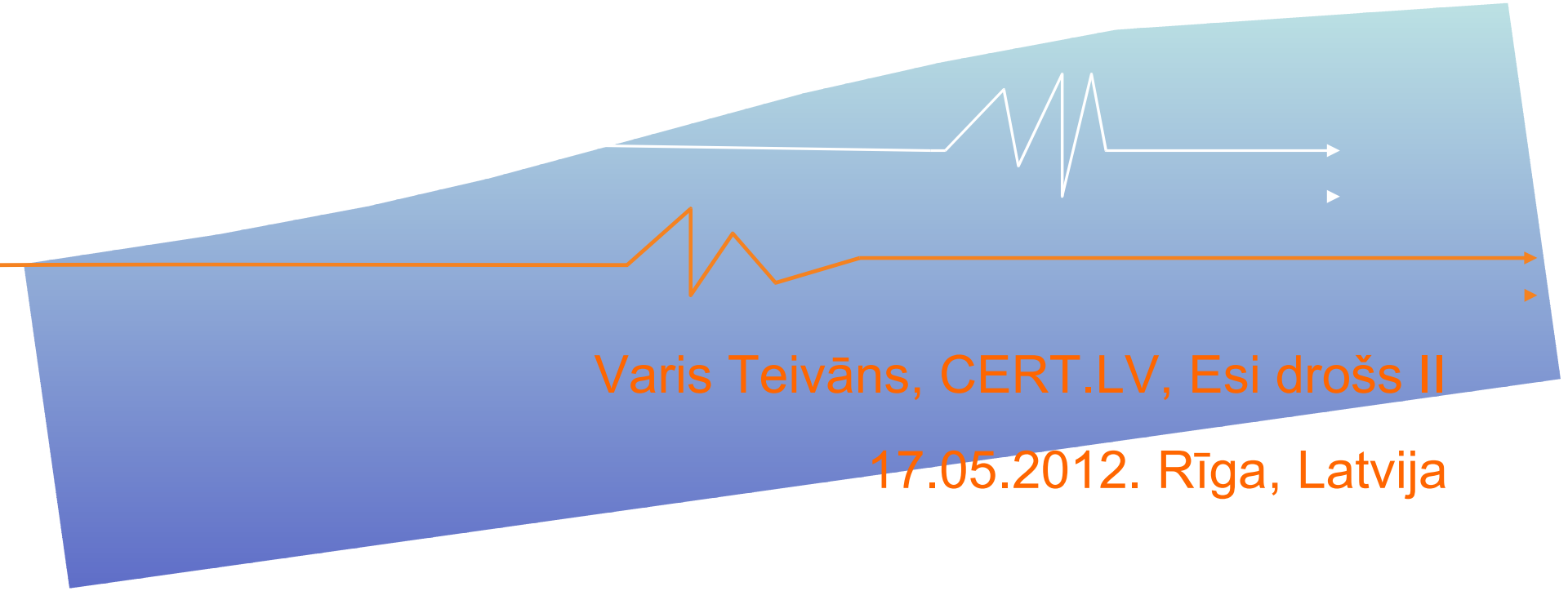
Bezvadu tīklu drošība



Varis Teivāns, CERT.LV, Esi drošs II

17.05.2012. Rīga, Latvija

CERT.LV

- Kas būtu jāņem vērā veidojot bezvadu tīklu
- Ko bez vadiem lietojam ikdienā
- Bezvadu ierīces un uzbrukumi

Kas būtu jāņem vērā veidojot bezvadu WiFi tīklu

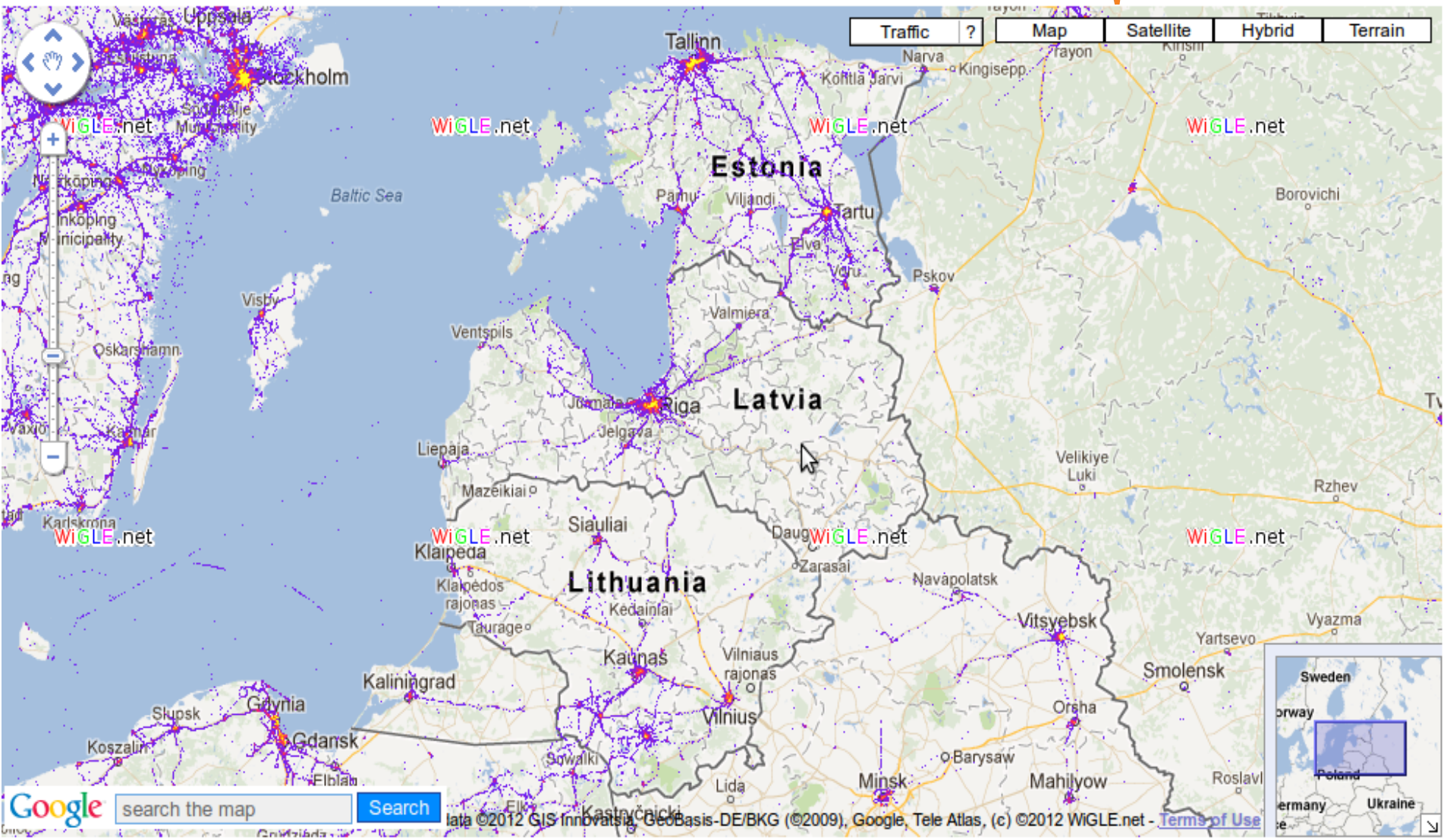
- Jāizvērtē bezvadu tīkla nepieciešamība un riski
- Bezvadu tīkls jānodala atsevišķā infrastruktūrā
- Lietošanas noteikumi
- Lietotāju autentifikācija / piekļuves kontrole
- Drošības un izmaksu samērība

Kas būtu jāņem vērā veidojot bezvadu WiFi tīklu

- Datu kanāla šifrēšana
- Bezvadu tīkla novērošana
- Žurnālfailu uzturēšana
- Lietotāja iekārtu konfigurācija
- Paroļu izvēle
- Apraides diapazons
- Funkcionalitātes apzināšanās

Datu kanāla šifrēšana

- “Neviens” vairs nelieto WEP un neatstāj “atvērtus” piekļuves punktus (Access Points)?
- Vai 802.11i WPA2 + AES atrisina visas problēmas?
- Vai piekļuves kontrole realizēta ar reģistrēšanos tīmekļa lapā ir tiešām kontrole?


Traffic
?
Map
Satellite
Hybrid
Terrain
Tallinn
Narva
Kohtla Järvi
Kingisepp
Estonia
Baltic Sea
Pärnu
Viljandi
Tartu
Pskov
Borovichi
Visby
Valmiera
Ventspils
Riga
Latvia
Jelgava
Liepaja
Mazeikiai
Velikiye Luki
Rzhev
Siauliai
Klaipeda
Klaipėdos rajonas
Lithuania
Kedainiai
Taurage
Kaunas
Vilniaus rajonas
Vilnius
Zarasai
Navapolatsk
Vitsyebsk
Yartsevo
Vyazma
Smolensk
Kaliningrad
Gdynia
Slupsk
Gdansk
Koszalin
Elblag
Suwalki
Orsha
Barysaw
Minsk
Lida
Mahilyow
Roslavl
Sweden
Poland
Ukraine
WiGLE.net
Google
search the map
Search
Data ©2012 GIS Innovatsia, GeoBasis-DE/BKG (©2009), Google, Tele Atlas, (c) ©2012 WiGLE.net - Terms of Use

WEP un “atvērti” piekļuves punkti

majas 12	A Y 001	83	0.0.0.0	0B
bobiks	A Y 011	1	0.0.0.0	0B
ASUS	A N 011	1	0.0.0.0	0B
BORGORE	A Y 006	1	0.0.0.0	0B
McDonald's Daugava	A Y 006	11	0.0.0.0	62B
lapsa	A Y 011	1	0.0.0.0	0B
Alex	A Y 006	1	0.0.0.0	0B
TP-LINK_10D01A	A Y 011	2	0.0.0.0	0B
eplink	A Y 011	1	0.0.0.0	0B
asus	A Y 001	1	0.0.0.0	0B
Igor 72 Network	A Y 005	1	0.0.0.0	0B
Pixie	A Y 006	48	0.0.0.0	60B
Vanesa	A Y 007	1	0.0.0.0	0B
dlink	A Y 006	41	0.0.0.0	790B
Sanda	A Y 013	1	0.0.0.0	0B
AVATAR	A Y 011	1	0.0.0.0	0B
TP-LINK_4DF372	A Y 001	1	0.0.0.0	0B

- **Kopā ~60 AP ar WEP un ~30 atvērti**
- **Pabraucot 10 minūtes prom no centra**
- **Centrā situācija būs vēl raibāka**

Vai 802.11i WPA2 + AES atrisina visas problēmas?

Nē

- WPS (WiFi Protected Setup)
- Vājas paroles
- PSK izgūšana no nozaudētām iekārtām
- Ad-Hoc tīkli

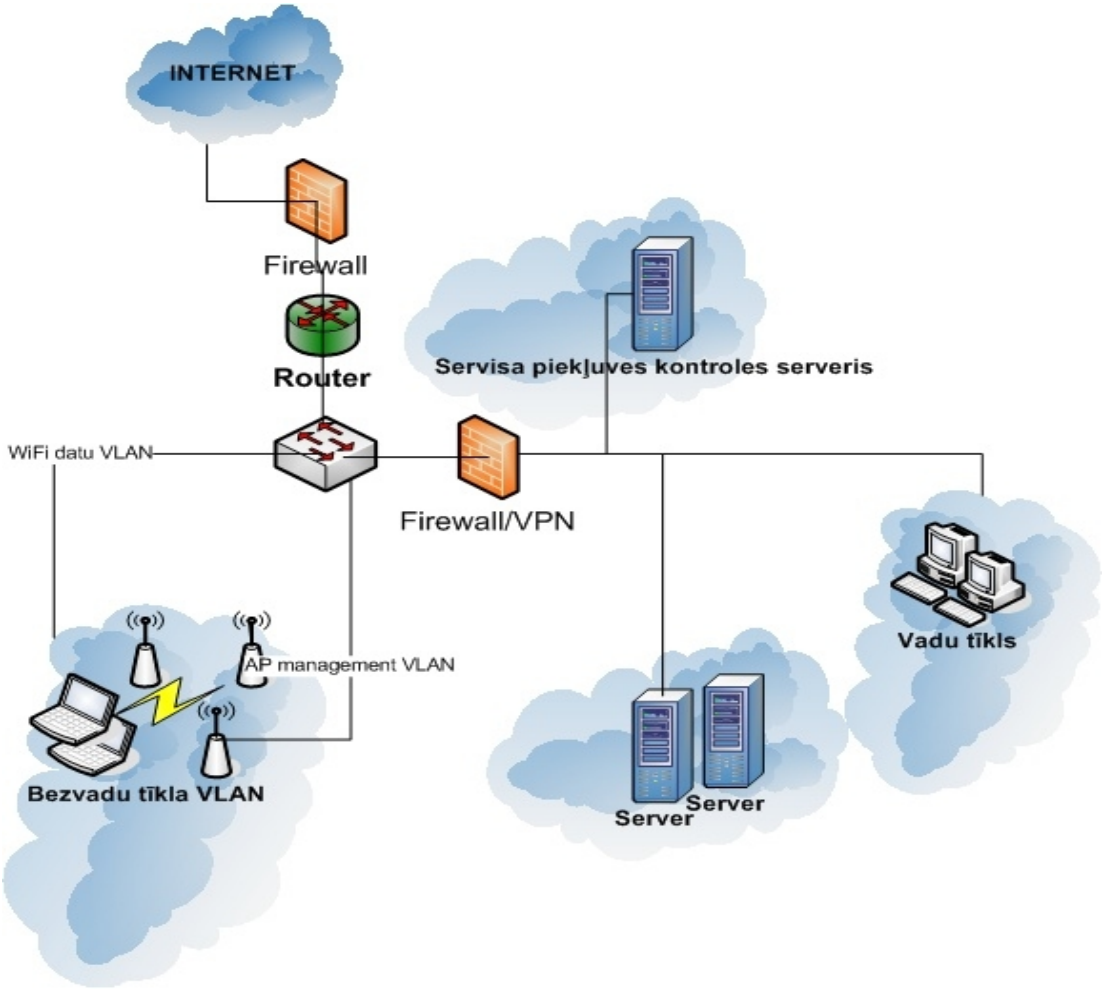
Federatīvi WiFi risinājumi

Strādajošs piemērs - eduroam

WPA2 + AES + PEAP/TTLS, EAP/TLS

- RADIUS piekļuves kontroles serveris
- Lietotājs var pieslēgties jebkurā federatīvajā apgabalā
- Sertifikāti katram lietotājam
    - Klientam jāpārbauda sertifikāts pie izvēlēta autoritātes servera
    - Android visi sertifikāti ir pieņemami pēc noklusējuma

Federatīvi WiFi risinājumi



Ko mēs lietojam bez vadiem?

- WiFi 802.11 un ne tikai
- Bluetooth
- RFID
- GPRS
- ...

Ko mēs lietojam bez vadiem?

RFID

- RFID – Radio Frekvences Identifikācija
- Passive
- Battary assisted
- Active

Ko mēs lietojam bez vadiem?

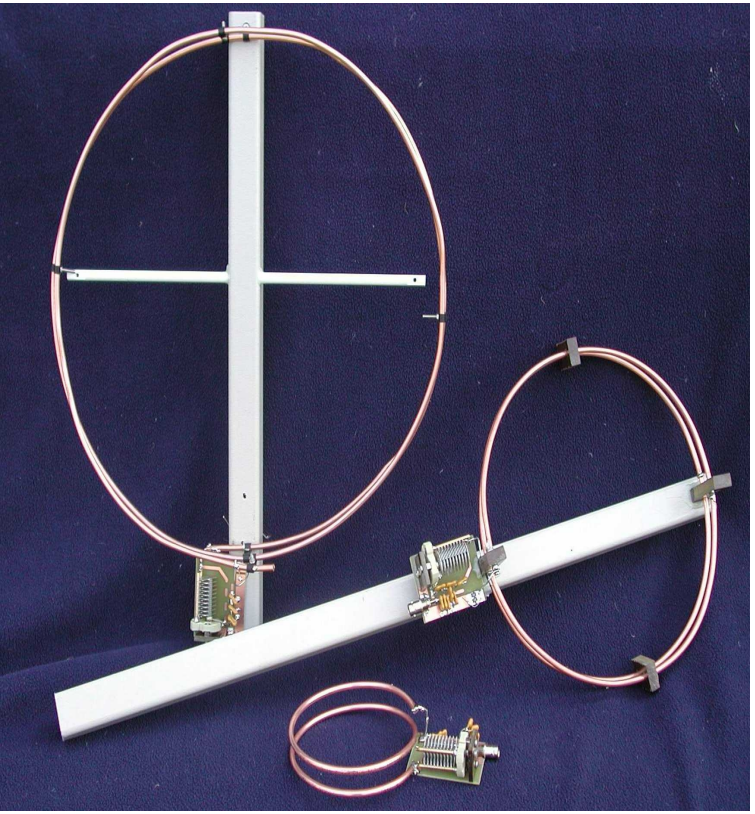
Nepieciešams kontakts, lai nolasītu

RFID

- Liela daļa neizmanto šifrēšanu
- Tie kas tomēr lieto šifrēšanu – tā nereti ir vāji implementēta
- RFID nolasāms pietiekoši lielā distancē
- RFID tiek lietots ļoti izplatīti kā identifikācijas un piekļuves kontroles mehānisms
- Dažādi standarti, dažādas darbības frekvences, bet iekārtas ir ar vien pieejamākas

RFID var nolasīt tik brutāli

RFID var nolasīt tik eleganti



DEMO – RFID klonēšana

GPRS

- Iespējams realizēt MITM uzbrukumus
- Ne vienmēr un visur izdosies
- Salīdzinot ar WiFi ir dārgāk

Secinājumi

- Veidojot WiFi tīklu ir jāizvērtē riski
- Jāievēro samērība drošības risinājumu ieviešanā
- Valsts iestādēs nebūtu vēlams WiFi ar vienu PSK uz visiem lietotājiem
- Atsevišķs WiFi mobilām ierīcēm nav slikta doma
- Tīkla novērošana ir nepieciešama

Secinājumi

- Uzmanīgi ar RFID

Paldies par uzmanību!

http://ww.cert.lv/
cert@cert.lv
varis.teivans@cert.lv