

TAV 10 2 e

I. GEGEVENS AANVRAAG

Nummer aanvraag : 10 2 g

Datum aanvraag : 26-09-2012
Type aanvraag : Individueel, Globaal, Overig
Land eindbestemming : de wereld muv LvZ
Land van bestemming :

Datum voorlegging : 04-10-2012
Regime/subregime : W 000
S.G.-postnummer : 5A002a7
Land van oorsprong : Onbekend
Land van herkomst :
Goederenomschrijving: Apparatuur voor informatiebeveiliging
Hoeveelheid : 10 1 c, 10 2 g
Waarde + valuta :
Exporteur : Fox Crypto BV, Delft

Ontvanger :

Eindgebruiker :

Eindgebruik : Netwerkbeveiliging

Aard van transactie : verkoop

Contactpers. bedrijf: 10 2 e
Telefoonnummer :

II. BESLISSING IB/IMH

Beslissing : Toewijzen
Naam : 10 2 e
Datum : 12-10-2012
Opmerking aan CDIU : land eindbestemming moet zijn: de Wereld muv LvZ,
10 1 c, 10 2 g

Voorwaarden : + voorschrift 1d uit IB-instr.: 2 x per jaar
rapportage-verplichting aan CDIU

Voorgelegd AIVD : J[] / N[x] (dwz alleen mondeling)
Voorgelegd POSS : J[] / N[x]

Collegiale toets :
Akkoord :

III. PRE-ADVIES CDIU

Risk Report
Risk Report :
Europese Denial DB :
Eindgebruiker :

Land : Diverse Landen
Programma van zorg :
Int. Regime :

Vergunningenoverzicht: 102 g
Toewijzingen NL : zie boven
Afwijzingen NL : nee
Denial eindgebruiker : nee
Denial land van best.: nee
Nummer (EU)-Denial(s):

Naam behandelaar CDIU: 102 e

Collegiale toets : 102 e

Eerdere sondage : N[] J[]
Nummer sondage :
Advies CDIU : [x]Toewijzen/[]Afwijzen/[]Overig

Toelichting advies : Geen veranderingen tov de vorige vergunningsaanvraag
102 g

Overige informatie : Info per mail. Overigens is er geen gebruik gemaakt
van 102 g

10 2 e

From: 10 2 e
Sent: woensdag 30 januari 2013 13:49
To: 10 2 e
Subject: FW: vergunningsaanvraag fox-it

From: 10 2 e
Sent: woensdag 26 september 2012 12:08
To: 10 2 e
Subject: Re: vergunningsaanvraag fox-it

Beste 10 2 e

Uit Wenen kan ik je berichten dat een crypto formulier niet nodig zal zijn. Je krijgt nog bericht. Zaak zal er niet door worden opgehouden. Excuses voor ogenschijnlijke geharrewar.

Met vriendelijke groet,

10 2 e

Van: 10 2 e
Verzonden: Tuesday, September 25, 2012 10:24 AM
Aan: 10 2 e
Onderwerp: vergunningsaanvraag fox-it

Beste 10 2 e

Zoals zojuist telefonisch besproken.
Douane groningen vraagt om een cryptoformulier.
Kenmerk van de brief is 10 2 g

Ik heb begrepen dat jij even in de telefoon klimt.
ik hoor/lees graag hoe e.e.a. afloopt en of ik nog acties moet ondernemen.

hartelijk dank,
vriendelijke groeten,

10 2 e

Product Manager Crypto

Fox-IT ...for a more secure society
Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands
T: 10 2 e
M: 10 2 e
F +31 (0) 15 2847990
I www.fox-it.com
KvK Haaglanden 27301624

10 2 e

From: 10 2 e
Sent: woensdag 30 januari 2013 13:48
To: 10 2 e
Subject: FW: aanvraag globale vergunning op maatFoxIT

From: 10 2 e
Sent: maandag 17 september 2012 14:16
To: 10 2 e@fox-it.com
Subject: Re: aanvraag globale vergunning op maat Fox IT

Hallo 10 2 e,

Dank je, we houden het in de gaten en nemen contact op indien nodig.

Met vriendelijke groet,

10 2 e

Van: 10 2 e@fox-it.com]
Verzonden: Monday, September 17, 2012 08:44 AM
Aan: 10 2 e
Onderwerp: aanvraag globale vergunning op maat Fox IT

Beste 10 2 e,

Slechts ter informatie:
Bijgevoegd formulier heb ik zojuist op de post naar Groningen gedaan.
Op een gegeven moment zal deze jouw bureau passeren.

met vriendelijke groeten,

10 2 e

10 2 e

Product Manager Crypto

Fox-IT ...for a more secure society

Olof Palmestraat 6

P.O. box 638

2600 AP DELFT

The Netherlands

10 2 e

F +31 (0) 15 2847990

I www.fox-it.com

KvK Haaglanden 27301624

Van: [redacted]@fox-it.com]

Verzonden: woensdag 27 april 2011 16:20

Aan: [redacted]

Onderwerp: Vraag mbt levering buitenland

Hoi [redacted],

Zoals je misschien weet ben ik werkzaam voor Fox-IT. Naar aanleiding van de gesprekken die mijn collega's [redacted] onlangs met jullie hebben gehad, vroeg ik mij af of het mogelijk is een praktijksituatie waar wij momenteel voor staan aan jullie voor te leggen. Ik doe het stiekem alvast, de situatie is als volgt.

Onze partner [redacted] heeft gevraagd of wij FoxReplay Analyst kunnen leveren aan de [redacted]. Met behulp van FoxReplay Analyst kan onderschept Internet- en ander IP-verkeer op een eenvoudige wijze inzichtelijk en doorzoekbaar gemaakt worden. Vooral nog is niet bekend hoe de [redacted] de oplossing precies wil inzetten. Wel is gevraagd of we een demonstratie kunnen verzorgen in [redacted].

Dit hele traject staat nog volledig aan het beginstadium en we zijn momenteel intern in gesprek over hoe hier mee om te gaan. Denk je dat enig advies vanuit het ministerie in deze situatie mogelijk zou zijn?

Mvg, [redacted]

[redacted]
COO Fox Replay

10 2 e

From: 10 2 e @fox-it.com>
Sent: vrijdag 29 juni 2012 13:05
To: 10 2 e
Subject: afspraak onder voorbehoud EL&I - Fox Crypto

Beste 10 2 e,

In navolging van ons telefoongesprek van zojuist:
We hebben een conceptafspraken gemaakt op 17 juli, van 14.00 tot 15.00 bij jou ten kantore.

Onderwerp is processen rondom exportvergunningen voor de producten die Fox Crypto voert.

Vanuit Fox-IT neem ik de volgende mensen mee:

10 2 e de logistiek manager
10 2 e product manager van product "A"
10 2 e (ondergetekende): product manager van product "B"

Graag ontvang ik een definitieve bevestiging van je op het moment dat je die kunt geven, en een adres waar we verwacht worden.

met vriendelijke groeten,

10 2 e

Product Manager Crypto

Fox-IT ...for a more secure society
Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

10 2 e
F +31 (0) 15 2847990
I www.fox-it.com
KvK Haaglanden 27301624

10 2 e

From: 10 2 e @fox-it.com>
Sent: vrijdag 29 juni 2012 15:10
To: 10 2 e
Subject: Re: afspraak onder voorbehoud EL&I - Fox Crypto

Beste 10 2 e ,

Dank. Over cloud computing kunnen we denk ik wel een aantal zaken zeggen.
Tot dan op de Bezuidenhoutseweg nr 20.
Met vriendelijke groeten,

10 2 e

Product Manager Crypto

Fox-IT ...for a more secure society

Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

10 2 e

F +31 (0) 15 2847990
I www.fox-it.com
KvK Haaglanden 27301624

On Jun 29, 2012, at 14:00 , 10 2 e wrote:

Beste 10 2 e ,

Bij deze kan ik de afspraak van onze kant bevestigen. 10 2 e zal er van onze kant ook bij zijn. Tevens hebben wij de vraag of wij jullie ook wat vragen zouden kunnen stellen over cloud computing (in het algemeen), omdat we ons met dat onderwerp op dit moment bezig houden.

Met vriendelijke groet,

10 2 e

Beleidsmedewerker Strategische Goederen
Directie Internationale Marktordening en Handelspolitiek

.....
Directoraat-Generaal Internationale Betrekkingen
Ministerie van Economische Zaken, Landbouw en Innovatie
Bezuidenhoutseweg 20 | 2594 AV | Den Haag
.....

10 2 e

10 2 e @mineleni.nl
www.rijksoverheid.nl/exportcontrole

17-18

Van: [10 2 e]@fox-it.com]

Verzonden: woensdag 25 juli 2012 15:08

Aan: [10 2 e]

CC: [10 2 e]

Onderwerp: Opvolging exportvergunningen Fox Crypto.

Beste [10 2 e]

Om te beginnen onze hartelijke dank voor de ontvangst op 17 juli, waarbij we hebben kennisgemaakt, en veel hebben geleerd over de zaken die komen kijken bij het internationaal verkopen van de producten van Fox Crypto.

Bij deze stuur ik jullie de algemene insteek die we als Fox Crypto zouden kunnen gebruiken bij de vergunningsaanvraag.

Graag verneem ik jullie commentaar/visie.

De komende drie weken ben ik op vakantie, daarna pak ik e.e.a. weer op.

met hartelijke groeten,

[10 2 e]



Insteek vergunningsaanvragen Fox-IT
versie 25 juli 2012 [redacted]

Beste [redacted]

Bij deze stuur ik jullie de algemene insteek die we als Fox Crypto zouden kunnen gebruiken bij de vergunningsaanvraag.
Graag verneem ik jullie commentaar/visie.

mvg [redacted]

DataDiode

- De DataDiode is een betrekkelijk [redacted] hardware product, waarmee vitale infrastructuur beschermd kan worden tegen digitale aanvallen, en waarmee er een eenwegkoppeling tussen netwerken van verschillende rubricering kan worden gemaakt.
- Het product is gecertificeerd door de AIVD (NL), BSI (Duitsland), NATO, en CC EAL7+.
- De vergunning heeft betrekking op de hardware die de DataDiode functionaliteit implementeert, en niet op de middleware (software) die bij deze hardware wordt geleverd.
- Dit speelt per nu. We hebben onder de oude vergunning (nr NL [redacted] [redacted]) al geëxporteerd.
- Voor dit product wordt een "Globale vergunning op maat" aangevraagd.
- Wederverkopers:

○ [redacted]

○

○

○

for a more secure society



- Landenlijsten

- o 10 1 c, 10 2 g

- o

- o

- o

- We houden een sluitende administratie bij van uitgeleverde (en geretourneerde) exemplaren, zowel export buiten de EU, als leveringen binnen de EU en binnen 10 1
- Per kwartaal informeren we EL&I met een overzicht van uitgeleverde (en geretourneerde) exemplaren.

RedFox

- De RedFox is een hoogtechnologisch cryptografieplatform, een halffabriek dat veel verschillende mogelijke toepassingen kent.
- Dit speelt vanaf begin 2013
- Per project zal een individuele vergunning worden aangevraagd.
- De vergunningen worden vooraf doorgesproken met het 10 2 g.
- De verwachting is dat het advies van het 10 2 g leidend zal zijn.
- Er wordt een zeer nauwkeurige administratie bijgehouden zodat elk exemplaar gevolgd kan worden.

Van: [redacted]@fox-it.com]

Verzonden: vrijdag 5 oktober 2012 16:28

Aan: [redacted]

CC: [redacted]

Onderwerp: Fox IT, exportvraag over een ongebruikelijk land

Beste [redacted],

Fox Crypto is benaderd met de vraag of we één onze it-beveiligingsproducten (niet eerder met jullie besproken) zouden kunnen/willen leveren aan [redacted]

De toepassing van het product en het doelland zijn zodanig dat we graag even met jullie van gedachten zouden willen wisselen om te bepalen of daar bezwaren aan kleven, of dat we spoken zien waar ze niet zijn.

Concreet: wij zouden op 11 oktober 's middags of 12 oktober 's middags jullie kant op kunnen komen.

Geven jullie aan of je hiervoor beschikbaar bent en zo ja: welk moment jullie goed uitkomt?

dank, groeten,

[redacted]

nb. ik zou dan graag de product manager van Fox Crypto van het betreffende product mee willen nemen: [redacted]

[redacted]

Product Manager Crypto

Fox-IT ...for a more secure society
Olof Palmestraat 6

21

41

10 2 e

From: 10 2 e @fox-it.com>
Sent: maandag 8 oktober 2012 21:07
To: 10 2 e
Cc: 10 2 e
Subject: Re: Fox IT, exportvraag over een ongebruikelijk land

Beste 10 1 c, 10 2 g,

Dank! We zullen er zijn.
Tot donderdag,

10 2 e

10 2 e

Product Manager Crypto

fox-IT ...for a more secure society

Olof Palmestraat 6

P.O. box 638

2600 AP DELFT

The Netherlands

T 10 2 e

M

F +31 (0) 15 2847990

I www.fox-it.com

KvK Haaglanden 27301624

On Oct 8, 2012, at 11:42 , 10 2 e wrote:

Beste 10 2 e,

wij (ondergetekende 10 2 e) zouden jullie kunnen ontvangen op donderdag 11 oktober om 16.00
ur aan de Bezuidenhoutseweg 20 te Den Haag om over genoemde kwestie te spreken.
Schikt jullie dat tijdstip? In afwachting van jullie berichten,

Met vriendelijke groet,

10 2 e

Beleidsmedewerker Exportcontrole en Strategische Goederen

Email 10 2 e @mineleni.nl

tel. 10 2 e

10 2 e

From: 10 2 e @fox-it.com>
Sent: maandag 10 december 2012 13:32
To: 10 2 e
Subject: Re: Eerder overleg

Beste 10 2 e

Ik heb de klant gevraagd om adres-details van de eindgebruiker, die benodigd zijn voor de sondage, maar ik heb tot nu toe nog geen antwoord ontvangen. Tot die tijd gaan wij door met voorbereiden van de offerte.

m.vr.gr.

10

On Mon, 2012-12-10 at 12:23 +0000, 10 2 e wrote:

Beste 10 2 e

>
> Hoe is het ermee? Ik begrijp van de CDIU dat er tot op heden nog geen
> aanvraag voor de (gemodificeerde) Skytale is binnen is gekomen.
> Ik vraag het je, omdat we destijds hierover intensief gecommuniceerd
> hadden. Kan het inderdaad kloppen dat jullie nog niet aan de aanvraag
> toezijn, of zien we hier iets over het hoofd?

>
> Met vriendelijke groet,

> 10 2 e

>
>
>
>
>
>
>
>
>

> Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien

> u niet de
> geadresseerde bent of dit bericht abusievelijk aan u is toegezonden,
> wordt u
> verzocht dat aan de afzender te melden en het bericht te verwijderen.
> De Staat
> aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die
> verband
> houdt met risico's verbonden aan het elektronisch verzenden van
> berichten.

>
> This message may contain information that is not intended for you. If
> you are not
> the addressee or if this message was sent to you by mistake, you are
> requested to
> inform the sender and delete the message. The State accepts no
> liability for
> damage of any kind resulting from the risks inherent in the electronic
> transmission of messages.

10 2 e

From: 10 2 e
Sent: woensdag 30 januari 2013 13:56
To: 10 2 e
Subject: FW: SkyTale informatie

-----Original Message-----

From: 10 2 e
Sent: donderdag 8 november 2012 15:34
To: 10 2 e
Subject: RE: SkyTale informatie

Hallo 10 2 e,

ik weet niet of je nog overweegt de zaak formeel in te dienen om voor een vergunning in aanmerking te komen?
Als je het indient bij de CDIU, kan je mij eventueel een seintje geven. Ik ben dan in elk geval alert op de voortgang in de stukkenstroom.
Over de behandelingstermijn kan ik niets zeggen, vanwege de noodzakelijke checks zal dat zorgvuldig moeten. Maar momenteel kan ik niets ondernemen.

Met vriendelijke groet,

10 2 e

Beleidsmedewerker Exportcontrole en Strategische Goederen

.....
Ministerie van Economische Zaken, Landbouw en Innovatie
DG Internationale Betrekkingen
Postbus 20401 | 2500 EK | Den Haag

.....
T 10 2 e
V 10 2 e @mineleni.nl
W <http://www.rijksoverheid.nl/exportcontrole>
.....

10 2 e

From: 10 2 e
Sent: woensdag 30 januari 2013 13:56
To: 10 2 e
Subject: FW: SkyTale informatie

-----Original Message-----

From: 10 2 e
Sent: vrijdag 2 november 2012 12:19
To: 10 2 e
Cc: 10 2 e
Subject: RE: SkyTale informatie

Beste 10 2 e ,

normaal gesproken is er de volgende route open. Als niet helder is wat de productsindeling is (dual use, militair en welke SG post dan), dat de aanvrager dat uitzoekt. Komt die er na gedegen inspanning niet uit, kan er een zogenaamd indelingsverzoek worden gedaan. In dit geval denk ik dat dat de zaak te veel zou vertragen, ook omdat er dan niet per se aanvullende informatie boven tafel komt. Laten we die stap maar overslaan. Op basis van de huidige informatie die je overlegt neig ik er naar te concluderen dat het een dual use product betreft, 5A002a1 (crypto). Mogelijk is er ook een dual use 5A001 SG post (telecom) van toepassing, kijk daar even naar graag. Deze conclusie onder voorbehoud want ben afhankelijk van wat jij zegt uiteindelijk te gaan doen. Ik wil dus nog wel de optie hebben deze indelingsconclusie te toetsen, zoals ik ook op de eindgebruiker wil toetsen.

Ik raad je aan via onze site zsm een vergunningsverzoek of proefverzoek (sondage) te doen met SG code 5A002a1 en evt 5A001. Dan komt het proces tenminste echt in beweging.

Met vriendelijke groet,
10 2 e

10 2 e

From: [redacted]@fox-it.com>
Sent: woensdag 31 oktober 2012 13:56
To: [redacted]
Subject: RE: SkyTale informatie

Beste [redacted]

Het punt is: er is geen goed. [redacted]
[redacted] van het product. We kunnen maw, het product vormgeven
zoals we zelf willen; we kunnen kiezen.

[redacted] 10 1 c, 10 2 g
[redacted] Maar dat laatste hoeft allemaal niet
voor deze specifieke klant. Sterker nog, voor deze opdracht zat ik er
sterk aan te denken om gewoon een COTS stuk hardware uit de markt te
trekken, iets als dit:

[redacted] 10 1 c, 10 2 g
En daar gewoon mijn software op te draaien, in speciale, 'commerciële'
modus. Wat doe je in zo'n geval? Want ik weet het zeker niet.

m.vr.gr.

[redacted] 10 2 e
On Wed, 2012-10-31 at 09:29 +0000, [redacted] wrote:

> Beste [redacted],
>
> dank voor je antwoorden. Ik wil de volgende punten met je bespreken.
>
> I Classificatie van het goed

[redacted] 10 1 c, 10 2 g

>
> II Formele indiening
> Zoals ik aangaf, op een gegeven moment moet je toch schriftelijke aanvraag doen, anders kunnen wij weer niet
goed onze inlichtingen verkrijgen. Als we I vooraf kunnen vaststellen, is een indelingsverzoek niet nodig. Dan kan je
gelijk een verzoek of proefverzoek ('sodage') voor een uitvoervergunning doen via onze website. Als je me er op
wijst, kan ik bij de dienst die de binnenkomende verzoeken verwerkt, om alertheid verzoeken zodat het niet onnodig
blijft liggen. Maar het beste kan stap I opgehelderd worden.

>
> Hopelijk heb ik je hiermee voldoende geïnformeerd.

> Met vriendelijke groet,

[redacted] 10 2 e

>
>

10 2 e

From: 10 2 e @mineleni.nl>
Sent: vrijdag 19 oktober 2012 15:28
To: 10 2 e
Cc:
Subject: RE: SkyTale informatie

Beste 10 2 e

Voor wat betreft jullie wens om (een variant van) de skytale te vermarkten aan een specifieke afnemer, het volgende:

Het product is vergunningplichtig. Vervolgens is er de vraag onder welke lijst of artikel. Iets kan voldoen aan de militaire controle lijst, of aan de dual use lijst (zie ook onze website voor meer informatie). Afhankelijk daarvan, dient een ander toetsingskader bij de beoordeling van de aanvraag bij ons zich aan. Het is daarom wel van belang de zogenaamde indeling goed te hebben.

Jullie gaven daarover aan dat 10 1 c, 10 2 g

We hebben op dit moment dus te weinig informatie om die inschatting te kunnen maken of het militair dan wel civiel product betreft dat zou worden uitgevoerd. Graag dus nadere informatie op dat punt.

Om eea ook wat beter administratief in te bedden, zouden jullie eigenlijk een indelingsverzoek moeten doen (via onze website). Omwille van de voortgang zouden jullie ook gelijk kunnen overstappen op een vergunningaanvraag, als we tenminste voor die tijd uitsluitsel over de productaard kunnen krijgen. Meer informatie is nodig op dat punt. Het zou ook behulpzaam zijn als jullie meer kunnen achterhalen over de identiteit van de eindgebruiker.

Met vriendelijke groet,

10 2 e

Beleidsmedewerker Exportcontrole en Strategische Goederen

Ministerie van Economische Zaken, Landbouw en Innovatie
DG Internationale Betrekkingen
Postbus 20401 | 2500 EK | Den Haag

T 10 2 e
M
e @mineleni.nl
W <http://www.rijksoverheid.nl/exportcontrole>

-----Oorspronkelijk bericht-----

Van: [REDACTED]@fox-it.com]

Verzonden: maandag 15 oktober 2012 16:36

Aan: [REDACTED]

Onderwerp: SkyTale informatie

Heren,

Bij deze nog de beloofde product-marketing informatie.

m.vr.gr.

[REDACTED] Fox-IT



Secure Networking in the Field

by Kees Jan Hermans

Technical Project Lead, Crypto Unit, Fox-IT, Delft, Netherlands
hermans@fox-it.com



Abstract

As it is with all aspects of modernity encroaching on our lives, in many professional, mobile situations the need for computer networking is growing. Mobile ('smart') telephones already provide rich network experiences to consumers, and many people working in army command-and-control, first-response or other field-situations wonder why they can't have these possibilities at their disposal in the line of duty.

Emergency circumstances typically encounter the following problems: unplanned network topologies, limited radio coverage and roaming restrictions, low (or no) bandwidth, overloaded networks, high latency, high cost, application constraints, differentiation between voice- and data- handling and no control over security.

In this paper we outline a solution to mitigate the combination of these issues, and we propose a new security model. By joining mobile ad-hoc networking (MANET) capabilities of modern routing platforms, and a single, robust security solution tailored to the dynamism of MANET, we can counter most if not all of these issues, and thereby provide professionals on the move with modern, networked information systems that they need in the field.

Our security solution 'payload encryption' has been successfully demonstrated, during its proof-of-concept phase, enabling voice- and data over multiple wireless and wired transmission means, including broadband and message based satellite communication systems. As a follow up, the Dutch armed forces will use the payload encryption security solution as one of the basic building blocks to deploy an all IP, all encrypted network following the principles outlined in the NC3A Protected Core Networking concept.

Table of Contents

| | |
|---|----|
| Secure Networking in the Field..... | 1 |
| Abstract..... | 1 |
| 1 Introduction..... | 3 |
| 2 Problem Definition..... | 4 |
| 3 High Level Solution..... | 5 |
| 4 Solution Details..... | 6 |
| 4.1 Operating Environment..... | 6 |
| 4.1.1 Modular Architecture..... | 6 |
| 4.1.2 IP Networks..... | 6 |
| 4.1.3 MANETS and Self-healing Radio Meshes..... | 7 |
| 4.1.4 Alternative Operating Environments..... | 7 |
| 4.2 Payload Encryption..... | 8 |
| 4.2.1 Statelessness..... | 9 |
| 4.2.2 Comparison to IPsec..... | 9 |
| 4.2.3 Security and Accreditation..... | 10 |
| 4.2.4 Challenges..... | 10 |
| 4.2.5 Security Risks..... | 11 |
| 4.2.5.1 Header Leaks..... | 11 |
| 4.2.5.2 Packet Length Leaks..... | 12 |
| 4.2.5.3 Reduced Crypto Parameters..... | 12 |
| 4.2.5.4 Replay..... | 12 |
| 4.2.5.5 Adequate and Timely Wiping (Zeroisation)..... | 13 |
| 4.2.5.6 Group-key Discovery..... | 13 |
| 4.2.6 Multi-factor Authentication..... | 13 |
| 4.2.7 Management..... | 13 |
| 4.2.7.1 Security Management..... | 13 |
| 4.2.7.2 Other Management Protocols..... | 14 |
| 5 Business Benefits..... | 14 |
| 6 Future (and Alternative) Directions..... | 14 |
| 6.1 A Family of Payload Encryptors..... | 14 |
| 6.2 Using L2 Radio Meshes..... | 15 |
| 6.3 Deployment in Protected Core Networks..... | 15 |
| 7 Summary..... | 15 |
| 8 Acknowledgement..... | 15 |
| 9 References..... | 16 |

1 Introduction

Today, existing army vehicular communications infrastructure still consists mostly of radios. These provide voice transmission over impressive distances, but they have their own particular brand of problems. Skip distances, available electric power and line-of-sight prohibit certain ranges and require multiple kinds of radios, the intricacies of day- and night-rhythms and solar variations require specialists on the ground and submission to unpredictable natural forces. Bandwidth is low. Obviously, the use of modern command-and-control computer applications is difficult.

In 2008, the Dutch army initiated an experiment to address this challenge. The problem was set out thus: to build a rugged, global communications system for inside vehicles to carry both voice and data, with acceptable bandwidths and latencies, capable of using all available means of communication at a given site, be able to roam without disconnections, and be appropriately secure (at least NATO mission-confidential level). This paper addresses the cryptographic network tunneling solution that was born from this concept.

The architecture that was originally proposed and that outlined the situation to its fullest extent was specified as follows: a modular chain of Internet Protocol (IP)-enabled devices, each with their own solution domain. There would be four elements to this chain: 1) the IP-based application-terminals, creating a trusted or 'red' cloud, 2) a device for creating secure, transparent IP-tunnels (the 'black', or untrusted side) from this traffic - the Payload Encryptor, 3) a Mobile (MANET) Routing platform and 4) the various means of transmission, land-based or aerial, such as satellite-, mobile-telephone-, radio- or WiFi- transceivers.

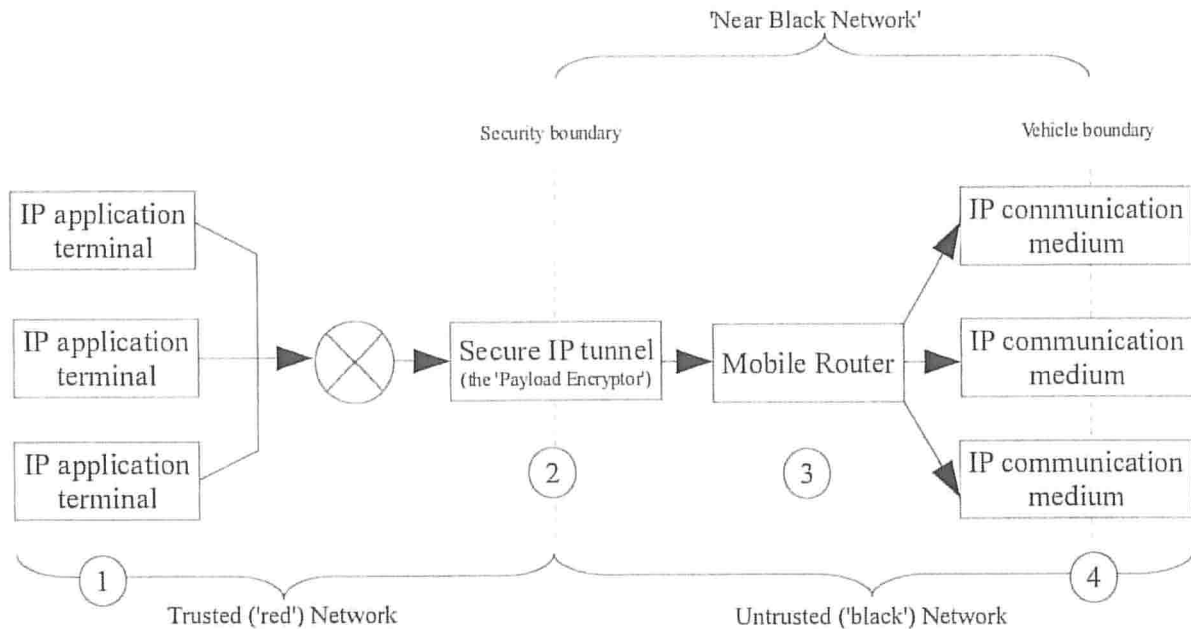


Figure 1: High level network solution diagram

Some further clarification from this illustration:

The 'IP application terminal' on the far left side can be anything from a (VoIP-)phone to a database service, a GPS message to a mapping stream; just so long as they're all Internet Protocol-aware. Secondly, on the far right, it must be noted that although they are denoted 'IP communication medium', there is no specification of as to how it must transport this. Certain radios, for example, can greatly improve on bandwidth-usage by stripping off IP-headers when using multicast.

Secondly, there are two 'boundaries', and two 'black' networks to consider: the most outlying boundary is the vehicle-boundary. This is a physical boundary and defines what is 'ours' in a real-world sense and what it not, and it is seductive to see this boundary as our security perimeter but it is not: that role befalls to the security device. This creates a schizophrenic situation of sorts: we own and operate machinery that we do not (really) trust (the 'near black network'). Plus: this machine may create network traffic of its own, that we do not really control (although under certain circumstances, we do control the *black core* [6.3]).

If we take two such set-ups and make them communicate with each other, we get something like this:

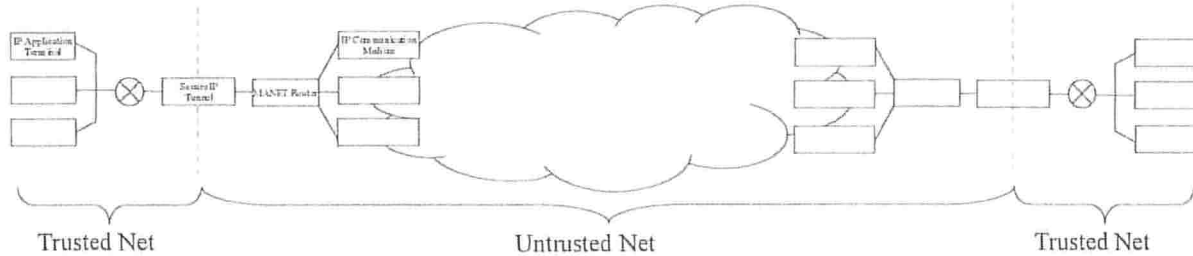


Figure 2: Set-up of our secure MANET chain within two vehicles.

The figure above shows our MANET-chain twice to illustrate a working red-to-red network setup; people working the network-terminals at both the left- and right extremes of this schema can communicate with each other, while attackers, tapping data in the untrusted middle, will get nothing but noise.

The advantages of this approach are obvious. Modularization may require an initial investment in multiple pieces of equipment (which can be costly, both in real terms, and in terms of use of power and space), but it provides many advantages, such as doing away with multiple radios for multiple distance ranges, their individual cryptos and their respective administration-, power- and space-requirements. It also tackles power requirements through delegation - namely when using cellular networks. It provides one-size-fits-all cryptography, which is easy to evaluate. It allows for plug-in applications and -transmission media. And it's easy to modernize and keep up-to-date.

And so, given the perimeters of this set-up, in 2008 we were tasked with developing a proof-of-concept of a custom cryptographic network tunneling device, which we gave the working title: 'Payload Encryptor'.

2 Problem Definition

To create a modular, bump-in-the-wire IP-network crypto device that serves the needs of applications and networks with the following characteristics:

Unstable links. Aerial networks are naturally unstable. They fade with distance, suffer from earth intrinsic physical oddities, skip distances, and natural and man-made objects in the line of sight.

Multiple routes. When using MANETs, not all packets are always routed along the same paths. Not all paths are as reliable as one another, or take equal amounts of time to traverse.

Low and fluctuating bandwidths. From a client-node perspective, the two characteristics described above translate into one problem: low and fluctuating bandwidth. To build network-tunneling mechanisms that supply both confidentiality and authentication, typically encounter non-trivial challenges in the areas of reliability, overhead and replay-detection.

Single addressing scheme. In ad-hoc networks, it is very difficult to maintain red/black mapping of addresses when using encapsulation. In multicast, it is almost an impossibility.

Usable in unilaterally separated networks. Because the Payload Encryptor requires no security association and can be configured with pre-shared keys, it can be used through one-way separations between differently classified networks (data diodes) [fig.3].

Supporting QoS and multicast. Networks that suffer from such low and fluctuating bandwidths can benefit from a well thought-out quality-of-service scheme that is supported throughout the network. Also, in certain areas of applications (VoIP, position-data) using multicast can ease the burden of carrying packets on a network tremendously. It is therefore important that our solution supports both mechanisms transparently.

IPv6. With more and more networks and network-equipments moving on from IPv4, and given its superior support for flexible addressing and roaming, it should be a given that our network crypto supports IPv6.

NATO mission-confidential level or higher. The Payload Encryptor is envisioned for usage in military vehicles, carrying network information of tactical or strategic quality. With that should come an appropriate security-level. We believe that mission-confidential level is achievable for our software version, and mission-secret level for the Payload Encryptor with HSM [6.1].

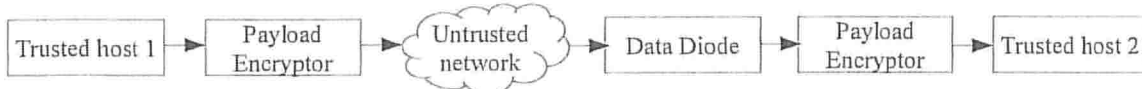


Figure 3: Using the Payload Encryptor to cross untrusted networks to behind a data diode.

3 High Level Solution

The Payload Encryptor is a bump-in-the-wire IP-network tunneling device. It is placed between a trusted ('red') and a usually larger, untrusted ('black') network, and connected to both. It provides the following network functionality to its network interfaces:

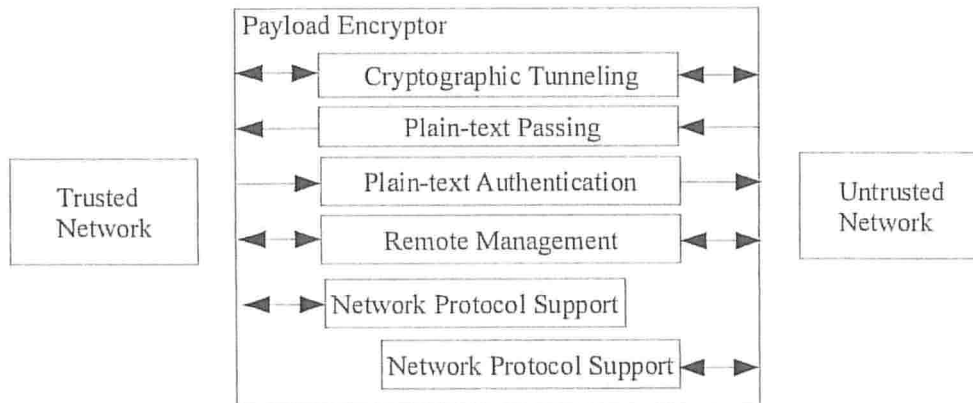


Figure 4: High level breakdown of the functionality of the Payload Encryptor

Network Protocol Support. On both network interfaces, the Payload Encryptor maintains a proxy for the network on the other side, so as to appear 'transparent' to it. These proxies are kept logically separate from each other as much as possible. They provide essential network-services to their respective network-peers such as ARP and IGMP (for IPv4), NDP and MLD (for IPv6), ICMP (in general), and even more complex 'maintenance' protocols such as DHCP.

Remote Management. The Payload Encryptor can be managed remotely using (asymmetrically) encrypted and authenticated management messages. This can be done (and turned off) on both sides. Messages that are accepted (i.e. they are intrinsically correct and also come from a peer that is recognized as 'master') change configuration and behavior of the Payload Encryptor. In reverse, Payload Encryptors can also be 'configuring masters' to other Payload Encryptors.

Cryptographic tunneling. This is the 'core business' of the Payload Encryptor. Packets are checked, and have their payload timestamped, encrypted and authenticated, and are then sent through. And vice versa. Multiple key-schedules may exist next to one another, and three different tunnel protocols exist to choose from. Keys, and lengths of the cryptographic parameters used can be configured differently among 128 possible channels.

Plain-text passing and plain-text authentication. Something that must be avoided at all cost, but is inevitable at times: machines in the 'nearby' black network sometimes need maintenance, or need to be able to send their (logging) data through. For this purpose it is possible to pass data plain-text through the Payload Encryptor from black to red. And in the presence of an authentication header, from red to black.

4 Solution Details

4.1 Operating Environment

In this chapter, we give an overview of the elements surrounding the Payload Encryptor, and the design choices that were made. This is done to illustrate the motivations surrounding the design of the whole communication-chain which, in turn, is necessary to understand the concept of the Payload Encryptor.

4.1.1 Modular Architecture

Our operating environment is modular, that is – it is composed of multiple, interchangeable parts that each perform a closely defined function. The advantages of this approach are:

Plug-in IP applications. Although the list of applications generally used on systems like these (position information, voice, video, chat, files, management) is predictable and short, we do not claim to know what the future will bring. Leaving one end of our set-up free to plug in any IP-application, makes the system robust and future-proof.

One-size-fits-all cryptography. Our security device brings any network traffic, created by the trusted network, up to level 'confidential'. There is no confusion, or need to implement or use embedded cryptography in either the applications or the communications-media.

Easier accreditation. Not only is there the advantage of having a modular crypto unit instead of multiple cryptos, having it physically separate from the applications and the router, also allows for easy evaluation of the unit. Parties who have algorithms or crypto devices of their own, can just plug them in. Foreign parties who wish to perform evaluations on our Payload Encryptor, can do so without having to dis-entangle logic that shouldn't have been entangled in the first place.

Plug-in communications-media. Just like the other side of the chain - what's true for plug-in applications also applies here: clients must be able to set up their aerials tuned to their needs and according to their possibilities.

4.1.2 IP Networks

The operating environment the Internet Protocol (IP) is the general carrier of all communications - both voice and data. There were several benefits to this decision:

Technologies support it. Modern operating systems (OS-es) and applications 'speak it natively', as it were. In many cases, it's the *only* thing they 'speak', even. In a similar vain, many COTS (commercial, off-the-shelf) devices exist for handling IP, and many communications-media provide support for it.

Developers know it. In a related manner, a lot of expertise surrounding IP, for development resources, can be had relatively easily. There are many existing applications that can either serve as themselves, or as prime examples for development. In other words, IP is cost-effective.

MANET maturity. MANETs, a research topic since the 1970's, had in the early 2000's developed into several mature technologies and specifications, as well as several commercial offerings [ref.10].

4.1.3 MANETS and Self-healing Radio Meshes

The original operating environment assumes a self-healing multiple-medium radio mesh network at the black, or untrusted, side of the Payload Encryptor. This can be achieved using MANET-technology (at IP-level, using MANET protocols such as OLSR [ref.2] or OSPF [ref.3]) or ethernet-level radio meshes, combined with multiple means of transmission. Such MANET set-ups and their equivalents provide:

Stability against changing topologies. When meta-data constantly provides updates on how the network is currently structured, and the difference between routers and endpoints is purposely blurred, you can protect yourself more adequately from changing topologies that are intrinsic to being on the move. To put it simply: MANETs keep networks efficient, even when everybody on it is 'roaming'.

Stability against changing bandwidths. Bandwidths on radio-based networks can drop quickly and unexpectedly. However, losing all coverage on all available means of transmission is rare. Being able to select and combine among those, allows you to keep your network up, longer.

The advantages of using such networks, are:

Ubiquitous connectivity. In the world of radio, one trades in reach for bandwidth. But when one is enabled to use all means of transmission, or at least make a clever selection of them (based on availability, cost, bandwidth), one can create the idea of an 'always-on' network.

Cost reduction. In the end, being able to make an intelligent and adequate decision when it comes to using means of transmission, should always bring about, statistically, a reduction of associated cost.

4.1.4 Alternative Operating Environments

The original operating environment assumes a self-healing multiple-medium radio mesh network at the black, or untrusted, side of the Payload Encryptor. This, however, is not set in stone; other set-ups have been implemented using the Payload Encryptor.

Directly onto a transmission medium (router mode).

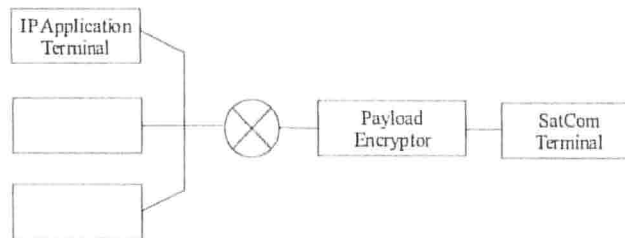


Figure 5: An operating environment without the MANET-technology.

A single vehicle in the dessert will not require WiFi or UMTS connectivity; it can do with its application terminals, a Payload Encryptor, and a position beakoning terminal. This way, a simple, rugged solution for sole operatives can be set up, which can still use the needed applications, and which is still appropriately secure.

Directly onto a LAN (or a layer-2 transmission medium). This could go all the way from multiple vehicle LANs that disguise as one in the air (a diagram much like the one we've already seen) to a more 'office-like' individual workstation protection device, as below:

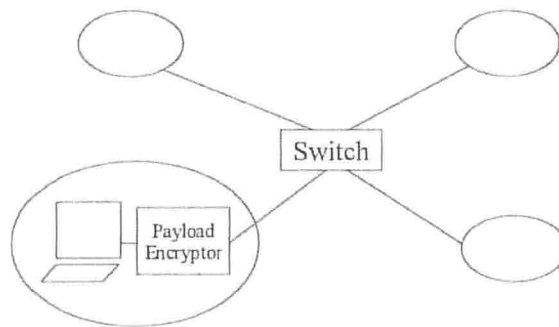


Figure 6: Using the Payload Encryptor as a 'personal' workstation protection device.

NB. The switch in the figure above can also be 'dark fiber' - a network that isn't under one's own control. As a tunnel-process on a wireless device (a tablet computer). Specially configured hand-held devices can, over WiFi back to the vehicle, enlarge the mobile ad-hoc network to the professional in the field.

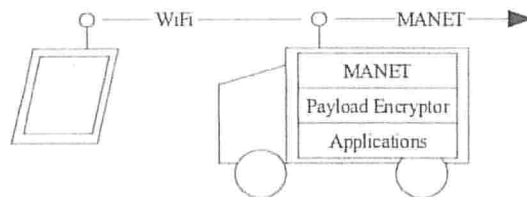


Figure 7: Extending the network from the vehicle to the person.

NB. This set-up would require an extension in the form of a module or a process in or added to a standard tablet, or a custom-built tablet.

4.2 Payload Encryption

IP networks are conduits for streams of data, split up into so called 'datagrams', or packets. IP packets, in turn, consist of a header (in the IPv4 protocol, usually 20 bytes), and the payload (on IPv4-over-ethernet, usually maximized at 1480 bytes, that is: 1500 minus 20). In IP payload encryption, as opposed to other tunnel solutions (e.g. IPsec), we only encrypt the payload; the header, on the other hand, is not encapsulated or copied - it is left largely untouched.



Figure 8: Transformation of a packet by payload encryption.

Payload encryption is unusual in the world of network cryptography, where we like to hide as much information as we can; the Payload Encryptor considers addresses to be non-confidential - it is most closely comparable to IPsec in transport mode with authentication and encryption. Payload encryption has serious advantages pertaining to our specific (MANET) set-up, namely:

Routability. Our encrypted packets remain completely routable by any network-node in between. There is no need for extra support from normal network hardware.

Preservation of essential information. Since our packet header also contains information that is used by other mechanisms than routing *per se*, these mechanisms continue to be usable. Packets denote Quality-of-Service (QoS), for example, by which MANET routers can determine which packets deserve preference over others.

Less overhead. We keep our cryptographic overhead lower by not encrypting (and therefore incorporating into the payload) the IP-header, therefore we are more suitable for use on our (generally) low-bandwidth communication media. Below is an overview of the amount of overhead incurred by the Payload Encryptor, and a comparison to other types of cryptographic tunneling methods.

| Tunnel-type | Overhead | Lossy | Intended Application / Comment |
|----------------------------------|----------|-------|---|
| Standard | 20-53 | No | All types |
| High speed | 28-61 | No | All types |
| (Standard & high speed) fragment | plus 4 | n/a | Both standard & high speed protocols support fragmentation |
| (Standard & high speed) UDP mode | plus 8 | n/a | Traffic that has to be transported through a NAT gateway, or pass a firewall (header compression can diminish this overhead). |
| Voice optimized | 8 | Yes | Voice data |

Figure 9: Packet-overhead of the Payload Encryptor, per tunnel-type.

4.2.1 Statelessness

Statelessness is another characteristic of the Payload Encryptor. It refers to the fact that it keeps minimal, or no, information about its peers – it can encrypt packets without this knowledge – it uses the same keys as its peers; they are, in fact, group-keys. In this way, there need not be any handshakes or key negotiation, and any network hick-ups – and we expect many – will not compromise our tunnel. The fact that this implies the use of group-keys is, in our minds, an acceptable trade-off vis-a-vis security. Being stateless, we gain:

Small memory footprint. We don't have to have large dynamic memory buffers to contain security associations with a potentially very large list of peers. Our software can be more simple and therefore faster and less error-prone.

Smooth service. When a network hick-ups down the line, the hiatus will not propagate into higher layers that also depend on connection feed-back (for example, TCP).

Radio-like functionality. Our use of group-keys has the advantage that it resembles radio: one sender, multiple receivers. This is, of course, an often-used way in army- and emergency-services scenarios and will benefit many relevant applications. It also allows us to support multicast unhindered.

4.2.2 Comparison to IPsec

There exist many different methods of creating secure tunnels over IP networks. TCP-based VPNs (e.g. OpenVPN) and SSL all operate at high levels that make them rather incomparable to payload encryption, but IPsec comes close: it too encrypts packets mostly as-they-are, and it has the option to leave original headers intact, allowing for routing as intended. While it is probably desirable to keep IPsec as an option in wired (back-bone) settings, leaving payload encryption as a preferred solution for secure networking in the field, we would still like to note these differences:

IPsec requires a 'security association'. It isn't stateless: a handshake, using ISAKMP [ref.15], determines all sorts of cryptographic parameters, such as authentication lengths, keys used, etcetera. The Payload Encryptor considers this undesirable, as missing information might jeopardize the ability to decipher a packet, and information might easily go missing in unstable networks.

Multicast is difficult. Not only are our networks unreliable - since security associations are particular to tunnels between individual peers, it is difficult to use IPsec in anything but unicast scenarios. The Payload Encryptor supports multicast, and therefore does its encryption with group-keys. Negotiation is unnecessary - keys are always 'pre-shared'.

Headers (in transport mode) aren't scrubbed. We feel that there is a substantial difference between simply passing a header, and being intelligent about it. The Payload Encryptor allows users to configure, and change, in great detail how the individual bits of each IP-header are to be treated before being passed on to the other side.

Overhead is still larger. In spite of carrying more cryptographic parameters, a Payload Encryptor packet is still smaller, on average, than an IPsec packet. Something that is of great value when it comes to encrypting many small packets over low-bandwidth links.

| Mechanism | Packet increase (bytes) | Percent increase | Percent increase to UDP/IP |
|---------------------------------|-------------------------|------------------|----------------------------|
| VoIP payload *) | 20 | baseline | - |
| IPv4 header | 20 | 100% | - |
| UDP header | 8 | 140% | baseline |
| Payload Encryption (voice) **) | 8 | 180% | 16% |
| Payload Encryption (standard) | 30 | 290% | 62% |
| Payload Encryption (high speed) | 38 | 330% | 79% |
| IPsec ***) | 70 | 490% | 145% |

Figure 10: Overhead of network- and encryption-layers for VoIP packets

*) Based on G 729 / 20ms [ref 6].

**) Average

***) Average, based on comparable IPsec in transport mode using 12-byte authentication and 16-byte blocks for confidentiality [ref 7]

4.2.3 Security and Accreditation

The Payload Encryptor has been developed for 'mission-confidential' level. With that in mind, it uses the following cryptographic methods and associated bit-strengths:

| Requirement | Cryptographic Device | Remarks |
|---------------------------------|----------------------|---|
| Network/storage confidentiality | AES-256 | |
| Management authenticity | RSA-4096 | In line with future NATO standards, elliptic curve support is currently in development |
| Network integrity | SHA2-256 HMAC | The length of the integrity reference can be configured. Because of the extremely brief period for which integrity must be safeguarded in tactical applications, the risk of a shorter reference is small |

Figure 11: Cryptographic parametrization as used in a standard Payload Encryptor.

4.2.4 Challenges

One of the functions of the Payload Encryptor is to stop 'leakage'. With that is meant that no plain-text data that resides on the red networks, should ever make it to the black network in unacceptable amounts and/or frequencies. Such acceptability will have to include the leaking of some IP-header information, though, as that is the very principle the Payload Encryptor is based on. Therefore, we employ:

Header scrubbing. We have to scrub the header to the best of our abilities, given the circumstances. That is, all header data that we're surely not going to use, must be either set to zero, or to some unpredictable, but deterministic value.

Field circumscription. Dynamic configuration can make a Payload Encryptor narrow down even further on what could be wrong or has to be changed about an IP header.

Network-emulation. The Payload Encryptor can, when configured as such, hide the source of traffic coming from multiple hosts behind one IP-address, both at level-2 (opaque ethernet) and at level-3 (NAT).

Secondly - since in our set-up we placed the crypto device between the red network and its router, this also poses some challenges: the red network needs to communicate with that router. Scenarios include:

Network-to-router meta-data. For example: red hosts, when sending out data to the black network, must query the ethernet address of the router by sending out ARP requests (or NDP messages in IPv6). These messages must travel in plain-text to the router. However, they must not contain any data that can be construed as a plain-text channel by an adversary.

User/application-level access to the router. There are times when we must configure or read information from the 'near-black' network. That is the network that sits between our security device and the vehicle border; essentially the MANET router and the communications antennae.

Thirdly – the Payload Encryptor must also 'play well' with the other elements in our communication-chain. Therefore we must be:

Minimizing overhead. Since we're specializing in the field of arial communications, bandwidth is a luxury, and we want to maximally reduce our cryptographic overhead (obviously at the price of lowering the expected strength of our security parameters, who need size to be effective). The way in which this is done, is tunable: not only do we offer three separate tunnel-modes, a user can specify different values for all sizes of cryptographic parameters being used.

Sensitive to traffic requirements. QoS-fields must be promulgated when necessary, replaced with zero-bits when not. In this way, we can secure leakage to the best of our abilities, yet be cooperative when we should be. For this purpose, our security device can be configured with dynamic rules, that determine how specific traffic is handled.

IPv6 ready. Many networks are switching over to IPv6. In the situations we deal with, this makes sense: IPv6 'rooms' much better than IPv4. Many devices however, still only support IPv4. For this reason, we also support transitioning between the two protocols.

4.2.5 Security Risks

4.2.5.1 Header Leaks

In payload encryption, the potential to leak exists only in the IP header; all the rest is encrypted chaos to an attacker, looking to see what's going on on the trusted side. Fields within the header are subdivided in the following characteristics with respect to their sensitivity to leaking:

Not sensitive at all. The first byte of an IPv4 header (containing IP-version and IHL), the ID- and fragmentation-fields, as well as the IP-protocol and checksum-fields, are not sensitive at all to leaking. They are either absorbed and replaced with whitespace or unpredictable but deterministic values, or non-sensical when used as a channel for leaking.

Intrinsically limited. The packet- or payload-length field is intrinsically limited by two phenomena: the fact that it cannot possibly exceed the Maximum Transfer Unit or MTU (or be any smaller than twenty, in the case of IPv4), and the fact that it has to match the underlying (ethernet) length. Also, that it must correlate (when using TCP or UDP) with the further given packet lengths and checksums in higher-level protocols.

Properly limitable by circumscription. The QoS-bits and source-address fields can be narrowly defined in the crypto unit's rule-engine. Using these rules, the damage that tweaking these fields could cause, can be greatly diminished. It's quite likely that the amount of hosts on the trusted side of the Payload Encryptor is below ten or not far above it. It's also quite likely that the amount of permutations of the QoS-field's bits is somewhere around the same number (most methods leave room for about sixteen permutations [Ref.13]). With regards to source-address leaking, also bear in mind that the Payload Encryptor supports NAT, a method by which one can hide multiple source-addresses behind one source-address.

Degrading with distance. Finally, the IP destination-address field, as well as the TTL- or hop-limit-field, are the biggest potential leaks. The former because even though a packet's destination can be circumscribed, its circumscription will probably have to be 'roomy', the latter because any value (except zero and one) is good. However, in both cases, their value as a channel for an attacker degrades with distance: the destination-address field because packets will start to elude him with more routers in the way, the TTL- (or hop-limit-)field because an attacker will have no way to predict the amount of hops between him and the original host. *Especially* in multiple- and dynamic-routing set-ups such as MANETs.

In conclusion, we propose that given our set-up, a certain amount of leakage potential is inevitable, but that it can be reasonably protected against by 1) *closely defining the networks on both sides in rule-sets*. Also that generally, for the most sensitive fields, 2) *leaking potential decreases rapidly with distance*; packets either become unroutable and therefore never reach an attacker, or change unrecognizably and become useless to an attacker.

4.2.5.2 Packet Length Leaks

There have been some remarkable attacks on network-systems in the last few years, that focus on packet length. For example, it turned out that spoken phrases could be deduced from encrypted, low-latency VoIP packets, purely by examining their packet lengths [ref.14]. To address this issue, we would like to state:

The Payload Encryptor provides padding. However, this is padding necessitated by the cryptographic method used in only one of the three tunnel-modes ('high speed'), and only provides padding of up to fifteen bytes (which, in the example of VoIP packets, would be quite effective). But it wasn't intended as a security-measure, and it could generally only be used poorly as such.

This issue must be resolved at the client. Our goal is overhead-reduction. While it could be possible to introduce random padding as part of the tunnel protocols, or perhaps become VoIP-protocol aware, dis- and re-assemble packets on the fly, we feel that this method is neither productive or future-proof. If clients wish to protect themselves from such risks, they should pad their own packets (or, in the example of VoIP packets, accept higher latencies).

4.2.5.3 Reduced Crypto Parameters

Reduced crypto parameters imply two types of attacks: the ones that allow an attacker to decipher data from an intercepted stream. And those that enable him to inject newly fabricated packets into the stream that will be authenticated correctly. You need the first to 'read' data, the second to 'write' it. Theoretically, because we allow for the shortening of our cryptographic parameters to gain a decrease of packet overhead, we should be more vulnerable to those types of attacks.

But even given the (relatively short) size of our crypto parameters, we do not believe that brute force attacks are feasible, especially when one considers the tactical use of our equipment, the advanced cryptography, the rapid changing key-schedules and an extremely short validity of the data.

4.2.5.4 Replay

'Replay' means an attack to a system, by re-running a previously intercepted message by it again. Past impressions of a certain state can be passed off, to the observer, as new, thus creating confusion. Imagine for example, that position-data of a certain vehicle is passed off to another vehicle as current while it is not – a perfect diversion. To protect against replay, systems must not allow previously processed messages to be processed again. Replay detection, given the statelessness of our security device and the fact that many messages will arrive late or out of order, cannot be implemented using a counter, as many implementations rely on. Instead, the Payload Encryptor relies on time. It is vital that it knows the exact time, and for this we employ many mechanisms, including hardware clocks, NTP and proprietary protocols.

4.2.5.5 Adequate and Timely Wiping (Zeroisation)

The Payload Encryptor can be 'rendered harmless' (that is, be unusable to an attacker to a degree) in many ways; remotely – through a management interface at another site or close by (within the vehicle), or through the use of buttons of the casing. We underestimate two 'stages' of zeroisation:

Key material wiping. This can be done even when the Payload Encryptor is 'cold' (not connected to any power source). A dedicated piece of memory containing the key material to unlock the solid state will have its gold-cap-powered power-circuit interrupted.

Total wiping. This requires an active wipe, and therefore can only be done when the Payload Encryptor is 'hot' (connected to a power source and booted). In this case, all solid state files will be erased from the device.

4.2.5.6 Group-key Discovery

Because group-keys are used by everyone in a network, they are used a lot. A lot more than individual, single-connection-based keys would be, and therefore they are more vulnerable to discovery. To mitigate this, one would probably write a doctrine that obligated quicker cycling of such keys, but there are also a few down-to-earth measures that one can take in the physical world:

IV's are never re-used. This is enforced network-wide, and across power-cycles of the device. IV's are kept relatively short in standard payload encryption, for efficiency reasons. However, based on calculations that assume a network speed of 100Mbps and 21-byte (168 bit) packets (IPv4 header + 1 byte payload), it shows that these relatively short IV's still have a large life-span. Much larger anyway, than most doctrines would proscribe the use of their associated, symmetric keys.

Remote exclusion and on-the-air re-keying. Using the management system of the Payload Encryptor, which can communicate with all of them out in the field over an especially, and personally encrypted channel using messages, one can 'remote control' our security device: one can zeroise it to level 'un-initialized' or even make it lose all of its solid-state data, plus – one can provide all other units with a new key schedule. Rigorous methods all in all, to ensure that a vehicle which is over-run, can never again speak to, or listen-in on the others.

4.2.6 Multi-factor Authentication

The Payload Encryptor contains an encrypted solid-state that it needs to function, for which it does not hold the key itself. This is part of its security model; without this key, and in a 'cold' state, the Payload Encryptor is useless. The key must be provided to it by a trusted party from the outside. Usually, it comes by such a key in the form of smart-card memory, an entry on a key-pad, or both. This is called multi-factor authentication: its (valid) user must provide more than one token to make it work properly, and a thief shall have to steal more than one item in order to do the same.

The Payload Encryptor can be entrusted with a (USB-based) reader of such devices on the casing itself however, it is in our minds a much more elegant solution to leave this to central, vehicle on-board computers. Such a device would receive the smart-card, unlock it using a PIN and, using the management protocol, then forwards a pre-signed and -encrypted message on it, to the Payload Encryptor. Such messages could also be used by the same on-board computers to issue a central zeroisation command, for example.

4.2.7 Management

4.2.7.1 Security Management

The Payload Encryptor comes with a remote management protocol. This protocol can be addressed by machines from inside the vehicle, but also by dedicated management systems, set up in fixed locations. The management protocol, and therefore management devices, can interact with the Payload Encryptor in the following way:

Cause zeroisation. From a security standpoint, this is obviously extremely important; vehicles that have been 'overrun' without time for proper procedure, can still be disabled this way.

On-the-air re-keying and configuration. Key-schedules, as well as running configuration are all stored inside a configuration database. Exactly what data can be configured, and by whom, is part of an extensive, detailed access control scheme.

4.2.7.2 Other Management Protocols

The Payload Encryptor supports syslog and SNMPv1, which can be configured to send their messages both to their own trusted segment (on-board computers), as well as another trusted segment, through a 'black' tunnel (central management machines).

5 Business Benefits

To professional users of networks in the field, we offer a high-level security device optimized for use in vehicle set-ups that enable everything that consumers of commercial solutions these days enjoy and more:

Integration with all IP-based applications. Transparency and support for all IP-based protocols end-to-end ensure that you can connect to whomever you want, whenever you want to.

A security device that doesn't interfere with traffic. Meta-data overhead is kept to a minimum. Addressing is left untouched. Quality-of-Service is guaranteed.

A security level that professionals require. A single device that immediately creates confidentiality at 'NATO confidential' level for all your applications, for all your means of communication.

Availability. The connection stands when the path is there - no need for cryptographic sessions. Low overhead implies less congestion.

A network that is future-proof. Using state-of-the-art crypto and IPv6 support throughout.

A solution that is cost-effective. Modular design and clever use of available networks drive costs down. A single addressing scheme means that network-management does not befall to the crypto managers.

6 Future (and Alternative) Directions

6.1 A Family of Payload Encryptors

We envisage a product-family of Payload Encryption installations, that allow communications from vehicle-based networks through to other, bordering, non-vehicle-based networks. 'Family-members' would not necessarily have the same hardware- or security-requirements as they would not serve the same purpose. However, we feel that the following additional set-ups would greatly enhance the usability of our communication-chain:

A Payload Encryptor for level mission-secret. Our software version is likely to be evaluated at level NATO mission-confidential. This is enough for tactical data. For strategic and for feedback-data, mission-secret is usually required. We are currently looking into the developing a Payload Encryptor with a hardware security module, or HSM, which will allow it to be evaluated at secret level.

Land-based networks. Indispensable for operational control - the Payload Encryptor management station is in effect already such a device. Other such devices would allow operators in army bases to manage operations by monitoring positions, for example. Land-based set-ups are usually less constrained than those in vehicles, and would probably not require much in the way of conversion, save for a 19-inch rack-mount.

Mobile devices for the dismounted soldier. Mobile devices usually have even less battery-power than vehicles. A software-only version of the Payload Encryptor, installed on a modern, open, COTS, mobile device, could extend the vehicle network even further out, and create a second-tier mesh: dismounted soldiers communicate with their vehicles - their vehicles communicate with each other and their home base.

6.2 Using L2 Radio Meshes.

In the commercial self-healing L2-radio-mesh market, there are several excellent off-the-shelf offerings [ref.8] [ref.9]. While our initial operating environment concentrated on L3 MANETs with its inherent support for multicast and QoS, it makes sense to examine this path, especially as it is already deployed in certain areas of emergency response.

6.3 Deployment in Protected Core Networks

Since availability (in our case: saving overhead and transparent QoS-handling) and security are founding principles of the Payload Encryptor, *and* of Protected Core Networks (PCN) as envisioned by its NC3A workgroup [Ref.12], we are currently in the initial stages of setting up combined experiments with the workgroup's Dutch representative (TNO) to include Payload Encryptors in their testing environment.

7 Summary

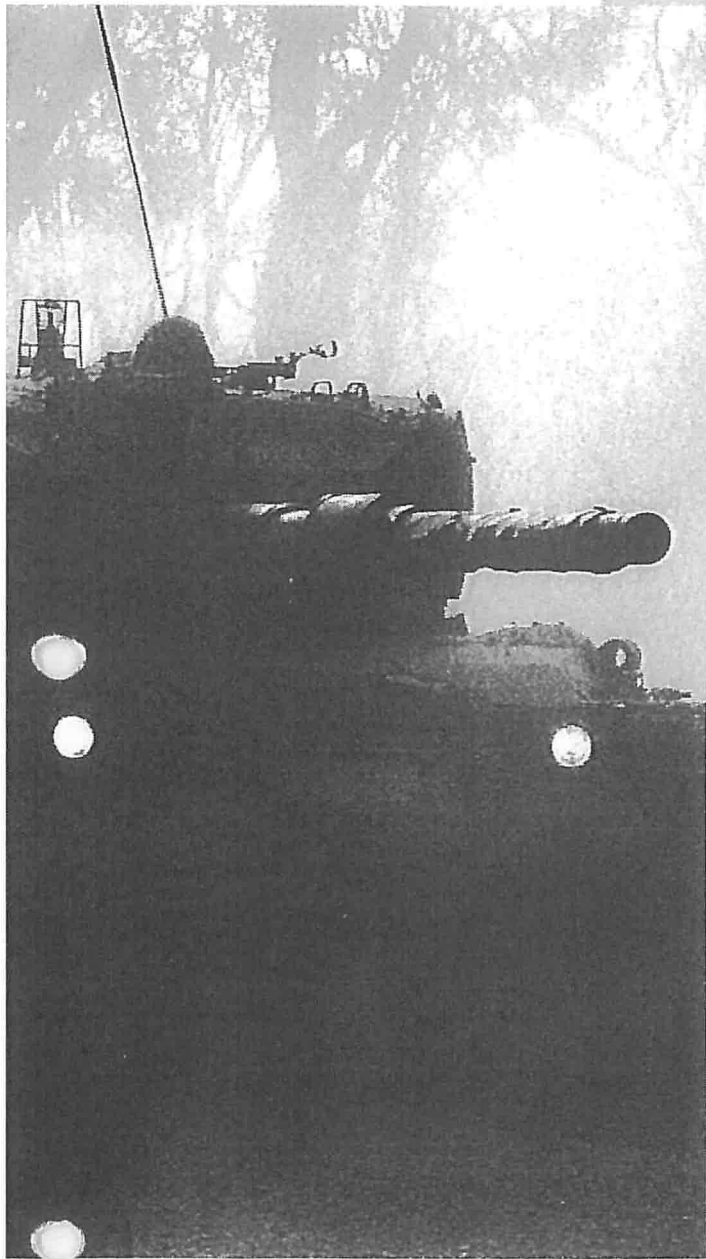
In this paper, we propose the idea of a modular IP network cryptographic tunneling device, to be placed in a potentially polymorph, modular chain of devices, together to be used to achieve more ubiquitous network connectivity for vehicles in the field. It can be implemented in any such set-up that uses IP. We think that the Payload Encryptor, combining transparency, statelessness, low overhead and future-readiness is a good alternative to many communications set-ups in vehicles today. More generally, we think that the surrounding concept of pluggable applications and MANETs provides an excellent solution to a problem that many armies and first responders deal with nowadays: how to achieve cost-effective, ubiquitous, acceptable networking conditions in the field, so that essential applications can be operated, and their service-level can be aligned with today's needs.

8 Acknowledgement

I would like to thank Teco Boot, of the NL C2SC, for his overall sympathy and the reviewing of this paper. Then I would like to thank Frank Brouwer of TI-WMC for his help in the area of LAN and L2-radio support. Thirdly, I would like to thank Jos Moens, Paul Fry and Steve Mills of Stratos for their help on SatCom terminal support. And lastly, I would like to thank Jozef Roeleveld of Arcobel BV, and Elbert Spaans of Gannexion BV, for knowing what it means to produce milspec hardware, and their willingness to share that knowledge.

9 References

- [1] Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing, by Jun-Zhao Sun, University of Oulu, Finland.
- [2] RFC 3626.
- [3] RFC 2328.
- [4] <http://hipercom.inria.fr/olsr/draft-ietf-manet-olsr-molsr.txt>
- [5] <http://sourceforge.net/projects/olsr-bmf/>
- [6] Study on Appropriate Voice Data Length of IP Packets for VoIP Network Adjustment, by Hiroyuki Oouchi, Tsuyoshi Takenaga, Hajime Sugawara and Masao Masugi, NTT Network Service Systems Laboratories.
- [7] A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms, by Christos Xenakis, Nikolaos Laoutaris, Lazaros Merakos, Ioannis Stavrakakis, university of Athens 2005.
- [8] <http://www.ti-wmc.nl>
- [9] <http://www.rajant.com/products/breadcrumb-lx-series-wireless-network-node>
- [10] http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/MobileIP.html
- [11] <http://datatracker.ietf.org/wg/manet/charter/>
- [12] G.Hallingstad & S.Oudkerk - Protected core networking: an architectural approach to secure and flexible communications (IEEE Communications Magazine, November 2008)
- [13] 'QOS in Packet Networks' by Kun Il Park, 2005, Springer.
- [14] 'Uncovering Spoken Phrases in Encrypted Voice over IP Conversations', Charles Wright et al. Jan. 2010
- [15] RFC 2408.



Network encryption in the field

Fox SkyTale

The Fox SkyTale is a ruggedised hardware VPN solution, developed for the military mobile domain. The Fox SkyTale combines an optimised network protocol with very low overhead and support for multicast, with high network performance of up to 100 Mbps. At the network level it is transparent for IP traffic (IPv4 and IPv6), so that existing network equipment in vehicles can be used virtually without reconfiguration. Partly as a result of this transparency, the Fox SkyTale is extremely easy to use. The Fox SkyTale uses state-of-the-art strong cryptography and is designed to be suitable for use at NATO and national Confidential levels.

The issue

To avoid dependence on radios, which provide bandwidth too limited for modern applications, many military organisations are moving towards communication solutions based on Mobile Ad hoc Networking (MANET). In a MANET, each participating vehicle potentially occupies a key position in the network, and all vehicles cooperate to ensure maximum availability of the network: for each transmission, the best route is chosen from the available communications resources (SatCom, WiFi, Wired networks, radios). Limited resources are combined into a constantly changing, but always available, network. Vehicles in a MANET typically contain a chain of devices to support the ad-hoc network functions, such as routing and up-links. A key function in this chain is security of the communications.

Requirements and properties

The Fox SkyTale r is specifically designed to provide the cryptographic security required in the dynamic and flexible environment of a MANET. As part of the MANET chain, the Fox SkyTale ensures the security of communications, regardless of the channel over which information is sent or received. The most important requirements and properties of the Fox SkyTale in the MANET chain are:

- Simple and user-friendly for the end-user and operational maintenance; the Fox SkyTale can be operated via the network (onboard computers).
- Suitable for use at NATO and national Confidential levels.
- Transparent for IP and usable in a Mobile Ad hoc Network (MANET) to offer the flexibility to dynamically support various communications media.
- Extremely low overhead in cryptographic protocols, to allow use of very low bandwidth channels; an overhead of 8 bytes per packet is possible.
- Support for multicast, to enable group communication.
- Future-proof, with strong cryptography, IPv6 support, and planned support for higher classification levels and protocols like HAIPE and/or SCIP.

Management and integration

The Fox SkyTale is provided with a management system for administration and configuration. This system is designed for flexibility and can be used both in off-line scenarios (settings and key material are transferred to the device on physical carriers, e.g. secure USB sticks), and in on-line scenarios. The Fox SkyTale supports re-keying over the network (over-the-air-rekeying, or OTAR) and it can be deactivated remotely (zeroisation). In addition to the management system, Fox-IT offers a standard integration and programming interface to control the Fox SkyTale, for example from an onboard computer on a vehicle's internal network. A fine-grained permission model allows precise control over authorisations, for example controlling who is permitted to enable communications over the device. Strong encryption of all management messages allows administration over untrusted communication channels.



Characteristics of the Fox SkyTale:

- Easy to configure and operate
- Suitable for use at NATO and national CONFIDENTIAL levels
- High throughput of up to 100MBit/s
- Minimal, configurable packet overhead
- Transparent for IP communications
- Multicast support
- IPv6 ready
- State-of-the-art encryption technology
- Off-line and on-line management using a standard management system
- Flexible integration with existing systems
- Future-proof roadmap

Fox-IT

Fox-IT specializes in cyber defense, IT Security, lawful interception and digital forensics solutions, providing completely secure, easy-to-use and automated products for data transport, interpretation and archiving to dozens of government defense and intelligence agencies, systems integrators and commercial organizations worldwide. Fox-IT solutions maintain the security of government systems up to "state secret level" sensitivity, critical infrastructure and process control networks and other highly confidential data. The company also provides services including IT security audits, digital forensic investigations, training programs and managed security services. Established in 1999, Fox-IT is based in the Netherlands and works with trusted partners in more than 20 countries.

contact

Fox-IT
Olof Palmestraat 6 P.O. Box 638
2616 LM Delft 2600 AP Delft
The Netherlands

t +31 (0)15 284 79 99
f +31 (0)15 284 79 90
e fox@fox-it.com

102 e

Van: [redacted]@fox-it.com]
Verzonden: dinsdag 19 april 2011 9:29
Aan: [redacted]
Onderwerp: RE: Ter afstemming: nieuwsbericht

Dit dekt de lading goed, dank voor je inzet [redacted]! zo geeft het de situatie goed weer.

Ik vond het des te actueler omdat ik op de fiets naar de meeting nog door [redacted] gebeld werd en die had afgepoeierd ;-)

[redacted]

-----Oorspronkelijk bericht-----

Van: [redacted]@minez.nl]
Verzonden: dinsdag 19 april 2011 9:27
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Ter afstemming: nieuwsbericht

Allen,

Dank voor jullie opmerkingen. Hopelijk kunnen we met bijgaande nieuwe versie jullie zorgen wegnemen. Is het voor jullie zo akkoord?

Dank,
Groet,

[redacted]

[redacted]

BEB/HPG

tst: [redacted]

Sent: Tuesday, April 19, 2011 9:04 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Ter afstemming: nieuwsbericht

Heren,

Wij herkennen ons nog steeds niet voldoende in dit bericht, terwijl onze naam wel genoemd wordt.

Graag overleg voor publicatie, mogelijk kunnen jullie onze zorgen nog wegnemen met een gerichte aanpassing.

Groeten,

[REDACTED]
Fox-IT

[REDACTED]

Van: [REDACTED]@minez.nl
Verzonden: dinsdag 19 april 2011 8:53
Aan: [REDACTED]
CC: [REDACTED]
Onderwerp: RE: Ter afstemming: nieuwsbericht

Beste [REDACTED]

Dank voor je reactie. Het lijkt me inderdaad niet goed de indruk te wekken dat jullie tot afgelopen week niet over deze thematiek nadachten. We hebben geprobeerd zoveel als mogelijk je opmerking in het bericht te verwerken. De minister heeft het ook nog gezien en dat heeft bijgaande versie opgeleverd. Later vanmorgen zal het online gezet worden.

Vriendelijke groet,

[REDACTED]

Directie Handelspolitiek & Globalisering
.....
Directoraat voor de Buitenlandse Economische Betrekkingen Ministerie van Economische Zaken, Landbouw en Innovatie Bezuidenhoutseweg 20 | 2594 AV | Den Haag

.....
T + 31 [REDACTED]
M + 31 [REDACTED]

[REDACTED]@minez.nl <mailto:[REDACTED]@minez.nl>

35-36

10 2 e

Van: 10 2 e [redacted]@fox-it.com]
Verzonden: maandag 18 april 2011 11:27
Aan: 10 2 e [redacted]
CC: 10 2 e [redacted]
Onderwerp: RE: Ter afstemming: nieuwsbericht
Opvolgingsmarkering: Opvolgen
Markeringsstatus: Voltooid
 Hallo allemaal,

Van onze kant moet ik toch wat moeilijk kijkende gezichten melden. Hoewel het een daadkrachtig bericht is schetst het de indruk dat onze bedrijven voorafgaande aan het gesprek nog niet zo kritisch waren over leveringen in landen met moeilijke situaties.

Dit beeld kwam ook al bij de oorspronkelijke beantwoording van de Kamervragen naar boven en wij (Fox-IT) herkennen ons daar niet in.

Wij zouden een alinea zoals de volgende daarom waarderen:

Tijdens de bijeenkomst kon geconstateerd worden dat voornoemde bedrijven zich reeds zeer bewust waren van het potentieel tot misbruik en een leveringsbeleid voerden om dit te zo veel mogelijk te voorkomen.

Voor het overige blijven wij het gevoel hebben dat een zalvende verklaring als nu voorgesteld mogelijk juist meer zorgen genereert dan minder, maar ik kan me goed voorstellen dat de wens bestaat iets uit te doen gaan.

Ik hoop van jullie te horen!

Groeten,

10 2 e

Van: 10 2 e [redacted]@minez.nl]
Verzonden: vrijdag 15 april 2011 13:50
Aan: 10 2 e [redacted]
CC: 10 2 e [redacted]
Onderwerp: Ter afstemming: nieuwsbericht

Beste heren,

Nogmaals veel dank voor uw bereidheid om gisteren met ons te spreken over gebruik en misbruik van uw technologie. Zoals besproken vindt u bijgaand een concept nieuwsbericht, dat wij naar aanleiding van de bijeenkomst hebben opgesteld. Graag zouden wij dat de komende dagen willen publiceren, uiteraard na uw instemming.

Ik verneem graag of u akkoord bent met dit bericht. Alvast veel dank voor uw spoedige reactie.

Met vriendelijke groet,

10 2 e

Directie Handelspolitiek & Globalisering

22-1-2013

37-38
43-44

69

10 2 e

Van: [redacted] (Fox-IT) [redacted]@fox-it.com]
Verzonden: maandag 11 april 2011 10:19
Aan: [redacted]
CC: [redacted]
Onderwerp: internet filters bij foute regimes
Opvolgingsmarkering: Opvolgen
Markeringsstatus: Voltooid
Beste Maarten,

Ik kan zo snel de brief van de minister hierover niet vinden online. Kan jij hem doorsturen?

Voorts suggereert hij nu dat er bedrijven in NL zijn die filter software/hardware exporteren. Ik denk dat dat niet juist is. Tappen wel, maar censureren gebeurt niet.

Groetjes,

[redacted]

FOX-IT

EXPERTS IN IT SECURITY for a more secure society

[redacted]@fox-it.com | m +31 [redacted] [LinkedIn](#) | [Twitter](#) | [Skype](#) [redacted]
Olof Palmestraat 6, 2616 LM Delft, the Netherlands

22-1-2013

70

39
4K

10 2 e

Van: [redacted]@fox-it.com]

Verzonden: vrijdag 25 november 2011 16:26

Aan: [redacted]

Onderwerp: RE: Brief aan TK: Beantwoording Kamervragen over de export van internetfilters en aftaptechnologie

Geen bezwaar. Voor zover dat bericht niet al binnen was gekomen ☺

10 2 e

From: [redacted]@minez.nl]

Sent: maandag 21 november 2011 12:49

To: [redacted]

[redacted]

Cc: [redacted]

Subject: Brief aan TK: Beantwoording Kamervragen over de export van internetfilters en aftaptechnologie

Importance: High

Geachte heren,

Zoals beloofd stuur ik u de conceptantwoorden op de Kamervragen over de export van internettechnologie.

I

k wil u vragen om te bevestigen dat u akkoord kunt gaan met de vermelding van uw antwoorden zoals verwoord in antwoord 3. Ik heb de vrijheid genomen hier en daar een klein beetje te redigeren, maar heb getracht uw antwoorden zoveel mogelijk intact te laten.

Zou u mij voor morgen **22 november 17:00** uur uw instemming of eventueel commentaar willen melden?

Mocht ik voor die tijd niets van u horen, ga ik ervan uit dat u met deze verwoording in kunt stemmen.

Met vriendelijke groet,

[redacted]

Ministerie van Economische Zaken, Landbouw en Innovatie
Internationale Betrekkingen; Exportcontrole & Strategische Goederen

[redacted]

A Postbus 20101, 2500 EC Den Haag

T 070 - [redacted]

M 06 [redacted]

F 070 - 379 7392

E [redacted]@minez.nl

W www.rijksoverheid.nl/exportcontrole

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic

22-1-2013

71

40-41
46-47

10 2 e

Van: 10 2 e [redacted]@fox-it.com]
 Verzonden: donderdag 27 oktober 2011 14:59
 Aan: 10 2 e [redacted]
 Onderwerp: RE: Kamervragen over internetvrijheid
 Tot 1530 uur dan.

10 2 e

From: 10 2 e [redacted] (Fox-IT)
 Sent: woensdag 26 oktober 2011 19:51
 To: 10 2 e [redacted]
 Cc: [redacted]
 Subject: RE: Kamervragen over internetvrijheid

10 2 e

Ik ben donderdag weer in het land, en zal u dan graag telefonisch te woord staan. Fox-IT zelf is niet meer actief in de wereld van Lawful Interception dus ik vermoed dat de beantwoording zeer beperkt kan blijven.

Daar waar het gaat om de rol van NetScout verwijs ik u terug naar 10 2 e [redacted] aangezien hij nu werkt voor FoxReplay BV dat in eigendom is van NetScout.

10 2 e

From: 10 2 e [redacted]@minez.nl
 Sent: vrijdag 21 oktober 2011 13:59
 To: 10 2 e [redacted] (Fox-IT)
 Cc: 10 2 e [redacted]
 Subject: FW: Kamervragen over internetvrijheid

Geachte heer 10 2 e [redacted],

Zojuist sprak ik vrij uitgebreid met uw voormalig collega, dhr. [redacted] die mij uitlegde dat de betreffende afdeling van Fox-IT inmiddels is overgenomen door het Amerikaanse bedrijf NetScout, waardoor hij niet meer voor Fox-IT kon spreken.

Ik begreep dat hij u zelf ook gesproken had, dus kan ik deze introducerende mail waarschijnlijk vrij kort houden.

Ik hoop dat Fox-IT ook medewerking wil verlenen bij het beantwoorden van deze Kamervragen (zie bijlage). Indien u daar prijs op stelt, kunnen we elkaar misschien ook telefonisch even spreken..

Met vriendelijke groet,

10 2 e

22-1-2013

72

42
43 sc
44

Ministerie van Economische Zaken, Landbouw en Innovatie
Internationale Betrekkingen; Exportcontrole & Strategische Goederen

10 2 e
A Postbus 20101, 2500 EC Den Haag
T 10 2 e
M
F 070 - 379 7392
E 10 2 e @minez.nl
W www.rijksoverheid.nl/exportcontrole

Van: 10 2 e
Verzonden: dinsdag 18 oktober 2011 17:44
Aan: 10 2 e
CC: 10 2 e
Onderwerp: Kamervragen over internetvrijheid

Geachte heren 10 2 e

Eerder dit jaar sprak u met mijn collegas 10 2 e over het risico dat bepaalde technologie gebruikt wordt voor het beperken van internetvrijheid. De heer 10 2 e heeft ons ministerie inmiddels verlaten voor een baan bij de VN, vandaar dat ik even contact met u zoek.

Zoals u weet is de Tweede Kamer erg geïnteresseerd in dit onderwerp, wat blijkt uit het feit dat er onlangs een aantal vragen zijn gesteld door Groen Links. (zie bijlage)

Ik zou graag van u horen of er initiatieven zijn die u heeft genomen sinds het gesprek op het ministerie van ELI, die we zouden kunnen gebruiken bij het beantwoorden van deze vragen?

Alvast bedankt voor uw medewerking,

Vriendelijke groet,

10 2 e

Ministerie van Economische Zaken, Landbouw en Innovatie
Internationale Betrekkingen; Exportcontrole & Strategische Goederen

10 2 e
A Postbus 20101, 2500 EC Den Haag
E 10 2 e @minez.nl
W www.rijksoverheid.nl/exportcontrole

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

=====

Bezoekt u het kerndepartement van het Ministerie van Economische Zaken, Landbouw en Innovatie?

Houd er dan rekening mee dat u een geldig identiteitsbewijs (paspoort, ID-kaart of rijbewijs) dient te tonen. Indien u bij de receptie geen geldig identiteitsbewijs kunt tonen, wordt u geen toegang verleend. Legitimatiebewijzen en toegangspassen van andere organisaties worden niet geaccepteerd.

=====

22-1-2013

73

45

From: [REDACTED]
Subject: FW: SkyTale informatie
Date: donderdag 13 juni 2013 14:17:21

-----Oorspronkelijk bericht-----

Van: [REDACTED]@fox-it.com]
Verzonden: donderdag 25 oktober 2012 17:10
Aan: [REDACTED]
CC: [REDACTED]
Onderwerp: RE: SkyTale informatie

On Fri, 2012-10-19 at 13:27 +0000, [REDACTED] wrote:

> Beste [REDACTED],

>

> Voor wat betreft jullie wens om (een variant van) de skytale te vermarkten aan een specifieke afnemer, het volgende:

>

> Het product is vergunningplichtig. Vervolgens is er de vraag onder welke lijst of artikel. Iets kan voldoen aan de militaire controle lijst, of aan de dual use lijst (zie ook onze website voor meer informatie). Afhankelijk daarvan, dient een ander toetsingskader bij de beoordeling van de aanvraag bij ons zich aan. Het is daarom wel van belang de zogenaamde indeling goed te hebben.

>

> Jullie gaven daarover aan dat [REDACTED]

[REDACTED]

We hebben op dit moment dus te weinig informatie om die inschatting te kunnen maken of het militair dan wel civiel product betreft dat zou worden uitgevoerd. Graag dus nadere informatie op dat punt.

>

1) Wij ontwikkelen een [REDACTED].

2) [REDACTED] Het verschil tussen deze en [REDACTED] doet nauwelijks ter zake.

> Om eea ook wat beter administratief in te bedden, zouden jullie eigenlijk een indelingsverzoek moeten doen (via onze website). Omwille van de voortgang zouden jullie ook gelijk kunnen overstappen op een vergunningaanvraag, als we tenminste voor die tijd uitsluitel over de productaard kunnen krijgen. Meer informatie is nodig op dat punt. Het zou ook behulpzaam zijn als jullie meer kunnen achterhalen over de identiteit van de eindgebruiker.

3) Ik zal eens kijken of ik zo'n indelings-verzoek kan vinden, al zou het wel helpen om te weten of wat ik daar moet invullen, wordt beïnvloed door wat gegeven is bij 1) en 2).

4) [REDACTED] hebben we inmiddels vernomen.

m.vr.gr.

[REDACTED]

>

> Met vriendelijke groet,

[REDACTED]
[REDACTED]

>

> Beleidsmedewerker Exportcontrole en Strategische Goederen

>

>