Satellite Communication without Privacy – Attacker's Paradise

—

appeared in *Sicherheit 2005*
Jahrestagung, Fachbereich Sicherheit der Gesellschaft für Informatik, April 5th 2005, Universität Regensburg, LNI Proceedings P-62, pp. 257-268

André Adelsbach and Ulrich Greveler
Horst Görtz Institute for IT Security
Ruhr University Bochum
Germany
e-mail: {andre.adelsbach, ulrich.greveler}@nds.rub.de

Abstract: In this paper we highlight the fact that a huge amount of information is sent unsecured via satellite broadcast data channels (here: encapsulated in DVB-s). By applying straightforward data analysis it is possible for any attacker equipped with a digital satellite dish and a DVB card PC to derive extensive confidential information on single users (e.g., legal name, banking details, monthly income facts, mail content etc.) as well as to hijack the user's web identities (e.g., online auction accounts). Many users do not seem to know or to care that broadcasted data can be easily intercepted; moreover even commercial users let high confidential customer related data (e.g. tender calculation details, negotiations with military customers) be sent unsecured via broadcast channels.

1 Introduction

A satellite is a specialised wireless transmitter placed in terrestrial orbit for diverse purposes such as weather forecasting, television broadcast, radio communications, Internet access and GPS positioning. Satellites can receive and re-transmit thousands of signals simultaneously, from simple digital data to television programmes. Especially, in low-infrastructure areas they provide an interesting alternative, e.g., for high-speed access to the Internet, because they provide high data rates and cover very large areas with comparably low efforts.

Satellite Internet access comes in two flavours:

- One-Way: This lower cost option sees the satellite handling only the data downstream with outbound data travelling through a telephone modem taking care of the low-bandwidth traffic from the user to the ISP. Most users only desire a high down-

load bandwidth while they would accept a rather small uplink capacity so this hybrid solution satisfies their needs. The service provides high-speed Internet downloads at bit rates exceeding those offered by DSL providers.

- Two-Way: The more expensive two-way option lets the user have a satellite transmitter entity at their site that enables two-way communication with high bandwidth for up-link and down-link.[1] This option is more suitable for companies connecting their remote branches to a data network.

Existing data communication enabled satellites are based on digital technology and often transmit TV signals with the same radio frequency (bandwidth is shared) or they dedicate Internet access to certain channels, providing high communication speed. The current bandwidth (applying the Digital Video Broadcasting (DVB) standards [DVB]) offers a maximum data transfer rate of 40 Mb/s on one transponder frequency being shared among several users for the downstream. However the provider often limits the downstream bandwidth per user to a certain value, e.g. 768 kB/s. In this paper we will focus on this one-way satellite communication as it is the more important use-case from the end-user's point-of-view.

1.1 Broadcast issue

The data packets in the downstream are broadcasted to each user which makes it easy to receive the data of all users, not only the data packets for a specific user. Every person or organisation owning a DVB-S card and a digital enabled satellite dish is able to intercept all the data packets sent by the satellite so confidentiality needs to be assured by other technical means (e.g., encryption of the data). This security characteristic of satellite data broadcast is well known for years in technical circles [Dis97] and there are publicly available tools to watch data stream information in human readable form [GNU]. Moreover, interception of unsecured satellite signals for intelligence purposes is on the public agenda since the nineties [Cam99].

One could imagine that data being broadcasted via satellite is either secured or it is not sensitive data at all so the user might consider the possibility that somebody else listens to the data stream as non-relevant if he uses an unsecured down-link.

As a matter of fact we have found various confidential and sensitive data in the unsecured data channel; a lot of users do not seem to care or to know about the public availability of satellite broadcast data; moreover there are commercial companies using the unsecured data channel to transmit highly confidential data such as customer bank account information (e.g., account + card number) or customer monthly income details. We also found company mail traffic that was received by employees via unsecured broadcast containing confidential information, e.g., bid details.

[1] Note, that the up-link bandwidth is commonly still smaller than the down-link bandwidth.

1.2 Outline

In the remainder of this paper we will first sketch how satellite based Internet access works and how the bandwidth and performance is optimised. We will then describe how network sniffing in DVB-s environments is done and what kind of data is collected this way; we will also give some statistical information about individual ratios of application protocols in the bulk data which will give us a first glimpse of the sensitivity of the collected data.

More details about the data content will follow and also some attackers' strategies to exploit the data is presented. Two samples of (anonymised) sniffed data will be presented that speak for themselves regarding the high confidentiality. We will also sketch the concept of user profiling by combining different data items and mapping them to a user hardware item ID (i.e., by means of the *MAC* address). Eventually we will draw some conclusions and give some advice to users and providers.

2 Satellite Internet Services

2.1 How it works

A user establishes a small bandwidth dial-up Internet connection, e.g., an ISDN line, to the ISP. In order to initiate a download a request is sent through the dial-up line to an ISP proxy server (Fig. 1, Step 1), which relays the request to the desired destination (Fig. 1, Step 2). The reply coming from the server (e.g., a WWW page) (Fig. 1, Step 3) is re-routed by the satellite ISP so that it will not come back to the user's PC through the dial-up line. Instead it will be encapsulated together with the user's specific IP address into a signal based on the DVB standard and the ISP ground station relays it to the satellite (Figure 1, Step 4). The satellite broadcasts it back to the user who is running a piece of software on his PC which completes the TCP communication transparently to the application or operating system (Fig. 1, Step 5).

2.2 Performance vs. Security

Security mechanisms operating on the lower levels of the network stack, such as IPSEC [KA98b, KA98a], have the general advantage that they provide security for all protocols and applications which operate on higher levels of the network stack. As those low-level security mechanisms are often hard to set up and maintain they are typically only used to protect the network infrastructure of companies, e.g., to connect subsidiaries to one secure virtual private network (VPN).

Apart from these general security protocols there is a large variety of application level security protocols that protect communication of a certain application only. Prominent examples are SSL for secure web access or SSH as a replacement for the Telnet protocol.

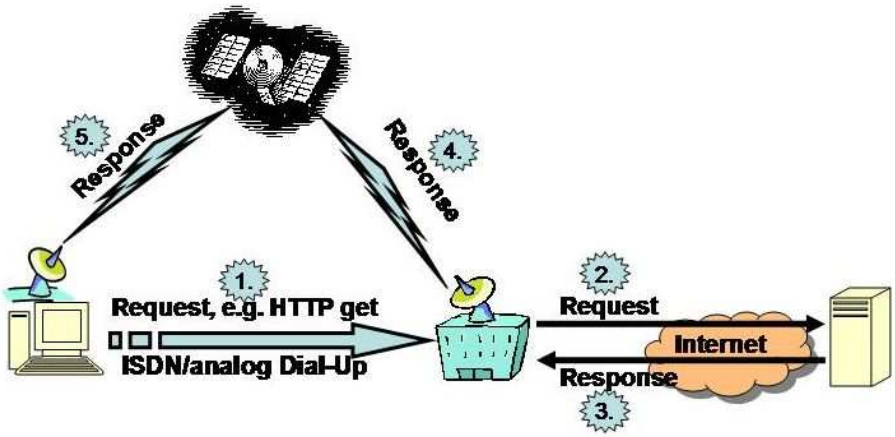

Figure 1: How a satellite Internet connection works.

Satellite communication links differ in several characteristics from terrestrial channels used for Internet communication [AGS99]: Firstly, satellite communication links have a relative large latency, due to the large altitude of satellites.[2]

This large latency also results in a long feedback loop between sending a TCP packet and receiving the corresponding acknowledgement. Another important characteristic is that satellite channels have a higher bit-error rate than wired terrestrial networks.

As these characteristics would result in a significant performance degradation of the TCP protocol [3], performance enhancing techniques have to be applied by the satellite ISP in order to achieve a satisfactory performance. Prominent examples for performance enhancing techniques are

- local TCP acknowledgements by the ISP's proxy (to speed up TCP slow start),
- local negative acknowledgements to improve error recovery,
- local TCP retransmissions from the satellite ISP to the client if a packet was lost on the satellite link (improve error recovery),

For details, we refer the interested reader to [ADG+00, AGS99, BKG+01].

Satellite ISPs use a combination of performance enhancing techniques along this line to improve the overall performance of their Internet access.[4] Unfortunately, these perfor-

[2] According to [ADG+00] many satellites are located at the Geostationary Orbit with an altitude of approx. 36.000 km. This results in a propagation delay of at least 279 ms for one hop (station-to-satellite-to-ground).

[3] As delayed feedbacks and transmission errors are interpreted as signals of network congestion, TCP would automatically reduce the transmission rate. For more details see [AGS99].

[4] Besides these transport layer measures, application layer improvements, such as prefetching the links contained in a HTML document requested by a user.

mance enhancements, implemented in *performance enhancing proxies (PEP)* and operated by satellite ISPs (or satellite carriers), are not compatible with standard low-level security measures such as IPSEC because PEP breaks the end-to-end semantics of a connection and the proxy interferes with the transport layer security measures, e.g., by sending pre-acknowledgements.

2.3 Two alternatives: VPN vs. Proxy Access

As performance enhancing proxies (PEP) interfere with IPSEC/VPN protocols some satellite ISPs (e.g. Deutsche Telekom) also offer direct, plain Internet access without using a PEP. This access – sometimes referred to as "VPN Access" – allows users to run arbitrary applications over this satellite Internet connection. However, in this case users have to accept a loss of performance *and have to care about security on their own* either by using application layer security measures or by setting up a secure VPN to protect their intranet communication. Users that use their Internet connection mainly for standard applications, such as web browsing and mail access, should usually prefer a proxy based satellite ISP as these proxies improve the performance and also provide security for standard applications by using encryption.

Our results show that users do not seem to be aware of this tradeoff and frequently make the wrong choice in favor of "VPN" access!

3 Sniffing in blue sky

In order to obtain experimental results we used standard off-the-shelf hardware (a standard PC with Pentium III processor, 512 MB RAM and a Hauppauge Win-TV-Nova DVB-S card) and open source software (Suse Linux 9.1, DVB drivers from linuxtv.org, and Ethereal V0.10.4). The satellite we listened to was the *Astra 1E* on 19.2^o East orbital position (visible from Central-Europe). The SAT-ISP services we focused on were those from *Netsystem*, *Deutsche Telekom* and *Megasys*.

3.1 Sniffing Statistics

Table 2 shows the data that was received on a satellite ISP frequency (Deutsche Telekom) during a period of 24 hours. First note that only one part of the TCP/IP communication can be received via satellite dish: the down-link to the user. A typical user will use the *POP3*-protocol for receiving mails via the downlink-channel from his e-mail-service provider and *SMTP* for sending e-mails via the telephone line to the outgoing mail service point; this gives an explanation why *POP3*-traffic outnumbers *SMTP*-traffic for example. Most of the data being sent is part of HTTP or FTP communication, only a small part of it being encrypted (here: SSL column). The reader can also observe traffic related to peer-to-peer

network communication (e.g., *edonkey* and *gnutella*) and personal messaging and relay chat communication (*aim*, *irc*).

time	http	ssl	pop	smtp	ftp	edonkey	gnutella	irc	aim
00:00	214.462	3.456	200	85	371.308	34	545	408	0
01:00	3.751	831	132	10	442.652	158	274	150	0
02:00	9.963	0	17	7	567.144	5	0	14	0
03:00	112	0	22	13	755.764	0	0	34	0
04:00	208	0	10	13	706.218	0	0	66	0
05:00	4.165	16.048	212	13	2.146.819	1.860	585	198	0
06:00	759	1.227	482	3	1.438.289	733	732	229	2
07:00	17.464	3.725	147	1	815.764	8	698	197	0
08:00	55.243	888	825	3	427.134	6	630	157	20
09:00	30.372	822	811	2	195.199	11	263	79	3
10:00	47.483	1.806	630	0	215.283	37	525	127	2
11:00	93.684	650	413	1	284.218	70	561	145	5
12:00	330.150	578	501	5	472.500	15.501	788	490	12
13:00	353.153	2.733	450	5	413.903	17.407	1.421	323	27
14:00	222.709	1.889	505	3	366.795	10.311	1.034	63	28
15:00	84.390	837	1.445	5	295.121	9.437	1.065	68	21
16:00	102.919	662	957	5	217.433	25.821	1.216	66	17
17:00	47.753	1.428	3.463	4	212.505	20.198	1.360	149	9
18:00	141.242	3.195	764	2	157.425	4.594	1.155	35	1
19:00	62.632	7.646	2.072	0	112.292	12.277	1.349	32	11
20:00	185.238	16.039	872	0	118.666	21.799	2.966	15	13
21:00	391.110	10.459	1.783	1	138.115	21.686	4.449	42	3
22:00	217.748	35.591	489	0	154.314	26.173	859	10	5
23:00	244.254	13.158	468	2	316.526	15.366	1.122	13	50

Figure 2: Sniffing results (in kilobytes) for a period of 24 hours (Deutsche Telekom).

3.2 Possible Impact of sniffed data: the attacker's paradise

Due to the increasing acceptance of e-commerce much private information is being sent by e-mail and HTTP protocol, apparently unencrypted. Examples of broadcasted information are account information, orders, bills or bids in online auctions. Our analysis shows that a significant amount of private e-mails is broadcasted in plaintext all over Europe. Moreover, we could observe that also commercial companies make use of unsecured broadcast data channels to transmit highly confidential data. The data can be used for different attack scenarios that we will detail in the following sections.

3.2.1 Receiving company internal mail traffic via users fetching mail from their home office

Many employees use home office environments to be able to work at home while accessing company IT services (e.g., e-mail, intranet). By applying state-of-the-art VPN solutions this scenario does not jeopardise the confidentiality and integrity of company-owned data.

```
Protocol Hierarchy Statistics (1 minute of data)
Filter: frame

frame                          frames:82096 bytes:71296692
  eth                          frames:82096 bytes:71296692
    ip                         frames:82096 bytes:71296692
      tcp                      frames:80020 bytes:70762488
        http                   frames:54167 bytes:64081047
        data                   frames:4518 bytes:3395795
        msnms                  frames:1319 bytes:312187
        irc                    frames:178 bytes:82399
        ymsg                   frames:722 bytes:157358
        nntp                   frames:216 bytes:278939
        ssl                    frames:563 bytes:436954
        edonkey                frames:617 bytes:393671
        rtsp                   frames:172 bytes:203992
        gnutella               frames:236 bytes:150535
        pop                    frames:111 bytes:29189
        telnet                 frames:44 bytes:7731
        ftp                    frames:7 bytes:1130
        ldap                   frames:6 bytes:1168
(...)
```

Figure 3: Sniffing statistics for 1 minute on Netsystem.

However, we observed that there are a number of employees fetching their company mail account messages via *POP3* using an unsecured satellite ISP link. Thus we could intercept all the message without doing any data analysis at all. The stunning finding was that this company-related communication also contained highly sensitive information (quotation details, internal bid calculation, applicants' CVs, communication with customers) and that companies that acted in this irresponsible way were suppliers to the U.S. military (see Fig. 5).

3.2.2 Hijacking of web identities, e.g., online auction accounts

An attacker may connect to the auction service provider web site and pretend that a user forgot his password and ask the web service to send the password by e-mail just by providing his user ID. The e-mail can then be intercepted via the broadcast channel by the attacker.

Some web services may ask the user for some "personal" information before sending the password (or provide an individual weblink for changing the password) by e-mail. However, the "personal" information required is not secret anymore but can be easily collected from other sniffed e-mails (such as the zip code of the user's address, which can be collected from orders or past online auction bills sent via e-mail). By analysing the 24h sniffing data bulk we obtained enough information to be able to hijack several online auction accounts, i.e., it would have been possible to set a new password unknown to the user and use the account while the user is discontinued from the service at the same time. These kinds of attacks can even be automated as the password changing process follows a

```
Sample data from a user who accessed a webshop via SSL. The
data was forwarded via an insecure satellite broadcast. Some entries
were deleted by the authors for privacy reasons (----------).

(...)
Name: ----------, Familienstand: verheiratet
Passnummer: ----------, Ausstellerbehoerde: Stadt S----
AusstellungsdatumTag: 30, AusstellungsdatumMonat: 05
AusstellungsdatumJahr: 2001, unterhaltspflichtige Kinder: 0
Tel: ----------, eBay: ----------, E-Mail: ----------
Nachricht:=20, Karte: ec, Kartennummer: ----------
Kreditinstitut: Citi Bank W------
Taetig: Angestellter, Taetig als: Gastronomin
Seit wannTag: 01, Seit wannMonat: 07, Seit wannJahr: 19--
Arbeitgeber: ----------, Standtort: Barnstorf
Branche: Gastronomie, Schifffahrt, Nettoeinkommen: ----------
Bank: Citi Bank W------, Kto: ----------, BLZ: 3------0
Rate: 20, Rate2: 25, Abbuchung: abbuchung 1.
Handywunsch: Samsung SGH E800, Stueckzahl: 1
Erreichbar unter:  0170----------
(...)
```

Figure 4: Plaintext user data forwarded by a German webshop to the back-office.

simple scheme that could be performed by a short shell script (*a.* do the web request, *b.* enter zip code or other personal information obtained from older mail *c.* receive the link by e-mail, *d.* follow the link , *e.* enter new password).

3.2.3 Profiling Users

Every sniffed IP packet can easily be linked to the user that requested it, because every *DVB-S* card has a unique MAC address. This allows an attacker to create extensive user profiles by linking different information sources, such as sniffed e-mails, access to web-sites (e.g., search strings at *eBay*, *Amazon* or *Google*), file sharing requests, chat communication etc.

By focusing on a special MAC address (in the 24h data bulk) we were able to find out the following information about a chosen user:

- Personal *POP3*-traffic: the user's e-mail addresses/accounts, his communication partners' e-mail-addresses, content of the mails, his legal name, bank account number, the name of his company, his web-shop customers, his ZIP code.
- *HTTP* traffic: to get a quick overview about the user's web usage we filtered the sniffed data for `<title>`-tags that return all titles of web-pages the user requested with his browser. By analysing the details of the user's *HTTP* traffic we were able to find out that the user runs a so called *eBay Shop* and collects stock information about a certain public traded company.

```
From: ----------- R LtCol -- SFS/-- [mailto:------@------.af.mil]
Sent: Friday, November 12, 2004 4:06 AM
To: ----------; ------------- F TSgt -- SFS/SF---
Cc: ----------; ----------; ----------; ----------; ---------- LtCol
-- SFS/--; ---------- Capt 31 SFS/---; ---------- SMSgt 31 SFS/---
Subject: RE: ---------- System
   Mr.  ----------,
   We would greatly appreciate a sooner installation.  We have
   troops that need this training and can no longer afford to
   have our system sitting in a warehouse.  Let me know if
   there is anything I can do to help.
   Thank you.          Lt Col ----------
-----Original Message-----
From: ---------- [mailto:----------.co.uk]
Sent: Friday, November 12, 2004 10:02 AM
To: ---------- TSgt 31 SFS/SF---'
Cc: LtCol 31 SFS/CC'; ------ Capt 31 SFS/---'; ------ SMSgt 31 SFS/---'
Subject: RE: ---------- System
   TSgt ----------,
   I will contact the Installation and Training team at headquarters in
   Atlanta USA to see if they can get your system installed sooner.
   Regards        ----------
(...)
From: ---------- F TSgt 31 SFS/SF---
[mailto:----------@----------.af.mil]
Sent: 12 November 2004 08:43
To: ---------- Cc: ----------; ----------; ----------; ---------- LtCol
31 SFS/--; ---------- Capt 31 SFS/SFT; ---------- SMSgt 31 SFS/---
Subject: RE: ---------- System
   All:   We would really like to have the -------- set up before then,
   if you have the resources, please check and see what you can do
   for our unit.   If you can't do it then we would like it done
   on the first available date that you have. I will be awaiting
   your response.  Thanks for your help in advance.
   TSgt ----------       ---------- Training
```

Figure 5: Company — US military conversation exposed to broadcast (- - - used for privacy reasons).

- Cookies: An attacker could collect cookies sent to the user by several sites. By storing these cookies into the attacker's web browser a web server may give an attacker access to web-services used by the attacked user without knowing access credentials (e.g., ID and password) or allow the attacker to derive long-term information about the user.

The fact that a (commercial) user does not encrypt his satellite link traffic (as we observed, see Fig. 4) does not only have impact on his privacy, but also on the privacy of his customers. In the case we observed that the web site of the commercial user advertises the fact that all private customer information is SSL encrypted! This might even be the case but security is completely jeopardised because the detailed customer information is forwarded by unencrypted e-mail. This way sensitive information is publicly broadcasted, while customers feel safe after having used SSL for providing confidential information.

This real-world example shows that comprehensive information can be collected about users that use satellite ISPs in a naive way.

3.2.4 ISP broadcast misuse

Users may also exploit the fact that satellite ISPs do not enforce secure communication: in principle it allows any user to broadcast *public* data to a huge number of potential recipients. This fact may be used to establish a multicast communication scheme where a user sends data to himself via the downstream while a number of other persons are receiving the data stream. In case of copyrighted material it is not clear whether the service provider could be made liable for the broadcast while the user might argue that he does not communicate with anybody else thus not share any files.

By enabling public key encryption users may even set up private broadcast channels which offer anonymity for all receivers sharing a private key.

3.3 Advice for Users

Users must be aware that Internet over satellite requires an even more careful setup and configuration than cable-based Internet access regarding privacy issues.

Satellite carriers and ISPs are obviously aware of security and confidentiality issues of broadcasted data and also of the crucial role of a correct configuration at the users' end.

The main goal of this paper is to draw users' attention to these open security issues. Companies should enforce a policy regarding home office usage and mail access. The bulk of secret information that was intercepted via DVB would be secured if companies just prevented *POP3*-access to their e-mail-server. If employees were forced to use SSL for accessing mails outside the company premises then a satellite broadcast of this data would not cause any harm. This also holds for other public network services as public WLANs. By providing unsecured *POP3*-access to a mail server any company jeopardises the secrecy of e-mails as the content is delivered in plaintext over the network.

3.4 Advice for Satellite ISPs

Satellite ISPs shall be aware of the severe security and privacy issues that we showed in this paper. It is a rather simple task to scan for users in their customer base who are using the services in such an insecure way (e.g., running *POP3* via a broadcast channel) and to regularly send a warning message to these users.

ISP customers who set up their equipment in an insecure way would most probably appreciate to be informed about severe security holes that expose their confidential data to the outside world. In many cases these customers could face legal consequences if attackers make use of the exposed data.

4 Conclusion

In this paper we showed that sensitive information is sent unsecured via satellite broadcast data channels and that this data can be retrieved easily by anyone equipped with a digital satellite dish and a DVB card. The exposed users do not seem to be aware of the fact that broadcasted data can be easily intercepted. Even commercial users expose company-related data.

There is room for improvement regarding the knowledge about these issues in the user base. The ISPs are in a position to provide information to their customers to support them in securing their data connections. Satellite Internet access is in place for several years now; the enforcement of a security baseline for this kind of broadcast communication is more than overdue. Users may utilise application layer security protocols to achieve end-to-end security. Our analysis showed that for *HTTP* this is already the case to protect critical information such as home banking PINs and TANs or passwords[5], however, little *POP3* communication is encrypted.

Acknowledgements

We would like to thank Jörg Schwenk for calling our attention to satellite Internet services and Ravi Rathore for setting up our Linux-based DVB-S lab environment.

References

[ADG+00] M. Allman, S. Dawkins, D. Glover, J. Griner, D. Tran, T. Henderson, J. Heidemann, J. Touch, H. Kruse, S. Ostermann, K. Scott, and J. Semke. Ongoing TCP Research Related to Satellites. Internet Request for Comment RFC 2760, Internet Engineering Task Force, February 2000.

[AGS99] M. Allman, D. Glover, and L. Sanchez. Enhancing TCP Over Satellite Channels using Standard Mechanisms. Internet Request for Comment RFC 2488, Internet Engineering Task Force, January 1999.

[BKG+01] J. Border, M. Kojo, J. Griner, G. Montenegro, and Z. Shelby. Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations. Internet Request for Comment RFC 3135, Internet Engineering Task Force, June 2001.

[Cam99] Duncan Campbell. Interception Capabilities 2000. Report to the Director General for Research PE 168.184, European Parliament, April 1999.

[Dis97] Dr Dish. Digital data from the sky. magazine publication 10/97, TELE-satellite International Magazine, October 1997.

[5] Note that many e-commerce providers, e.g. online auction services, provide SSL access to their servers only for the user registration phase. After registration only unencrypted HTTP is available so the hijacking of the accounts via credential cookie interception cannot be prevented by the user with SSL in these cases.

[DVB] DVB Project. DVB Project Homepage. http://www.dvb.org.

[GNU] GNU General Public License. DVBSNOOP: a DVB / MPEG stream analyzer program. http://dvbsnoop.sourceforge.net.

[KA98a] Stephen Kent and Randall Atkinson. IP Encapsulating Security Payload (ESP). Internet Request for Comment RFC 2406, Internet Engineering Task Force, November 1998.

[KA98b] Stephen Kent and Randall Atkinson. Security Architecture for the Internet Protocol. Internet Request for Comment RFC 2401, Internet Engineering Task Force, November 1998.