Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 2. February, 2004

First Bluejacking, Now Bluesnarfing

The latest sign that Bluetooth has finally become a mainstream technology is the emergence of Bluesnarfing, where a hacker silently accesses information stored on a device, such as the calendar and phone book. Typically, the only way the user learns of a Bluesnarf attack is if the hacker modifies the information accessed, such as by deleting or changing contact list entries.

Bluesnarfing comes on the heels of Bluejacking, where the goal is to amuse, irritate or surprise the recipient with an unsolicited message that pops up seemingly out of nowhere (for more information on Bluejacking, see the **November 2003** issue of *Wireless Security Perspectives*). Both hacks exploit a Bluetooth device's ability to discover other nearby devices. They also exploit naïveté: Most users do not know about Bluetooth's security risks, and if they did, they probably would not know how to disable it to thwart attacks, or knowing how, would not want to bother.

The Bluestumbler website claims this attack could obtain the IMEI (International Mobile Equipment Identity) of an attacked GSM cellular phone. They imply that this could be used in cloning attacks, but this is simply not true. Cloning requires access to the IMSI (which is easy, because this is openly transmitted) and the internal secret keys for the authentication algorithm. The IMEI, a hardware identifier, is not used in authentication, and its major role is to track stolen phones, not to validate a subscription. A bad IMEI may deny you service, but a good IMEI will not get you service.

Although these techniques have been known since at least November 2003, Bluesnarfing attracted little attention until early February 2004, when several news outlets picked up the story. Most cited the work of AL Digital, a U.K. firm that claims to have uncovered the flaw and then brought it to the Bluetooth SIG's attention.

Although Bluetooth-equipped laptops also are vulnerable to Bluesnarfing, phones apparently are most commonly targeted – they are less complex. According to AL Digital's Bluestumbler web site, nearly a dozen models of Ericsson, Nokia and Sony Ericsson phones are vulnerable to Bluesnarfing attacks. An attack against some of these can only succeed if Bluetooth is set to "discoverable" or "visible" mode, while an attack against others can circumvent those settings.

AL Digital reports that it has developed several utilities to help thwart or track Bluetooth-related attacks. So far, it will not release them publicly, but the company is willing to work with manufacturers of Bluetooth devices.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $350 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$400 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpsales@cnp-wireless.com

Next Issue Due…

March 29th, 2004.

Future Topics

Light-weight Wireless Security for UWB • Personal Area Network Security • Radius for Wireless • 4G Security • Zigbee Security • PKE-enabled Wireless

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published **11** times a year by Cellular Networking Perspectives Ltd, 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $350 for delivery in the USA or Canada, US$400 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to **10** copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.

Article Sourcing: Tim Kridel.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Securely Enabling Intermediary-Based Services, Part II

Sneha Kasera, Semyon Mizikovsky, Ganapathy S. Sundaram and Thomas Woo

Encapsulating Security Variable Payload (ESVP)

Our approach to exposing partial end-to-end packet information to a trusted intermediary involves a new IPsec option called ESVP that extends IPsec ESP by leaving certain portions of the payload in the clear (unencrypted). The exposed text must be a contiguous block at the head or tail of the payload. As shown in **Figure 1,** the ESVP packet header fields that are not present in ESP are:

- **A**: A one-bit field. When set to 0, the clear text is authenticated end-to-end, and therefore, each intermediary has permission only to inspect the clear text of the packet rather than modify it.
- **T**: A one-bit field that indicates whether the head or tail of the payload is encrypted. When the tail of the payload is encrypted, the T-bit is set to zero to indicate that the clear text is placed before the SPI field. When the head of the payload is encrypted, the T-bit is set to 1, and the clear-text follows the Authentication Data field. The T-bit helps prevent multiple encryptions of the same data.
- **Proto**: This 1-octet field indicates the next protocol.
- **Clear text Length**: This field contains the clear text's length in octets. This field is two octets long and therefore allows lengths up to 65,536 octets to be defined.
- **Clear text**: This part of the payload is received from the upper layers and is not encrypted.

Definitions of the remaining ESP fields can be found in RFC 2401 [1].

ESVP must be supported in both transport and tunnel mode. **Figure 2** shows ESVP in the tunnel mode for a typical IPv4 packet. In both the transport and the tunnel mode, the Proto field of the outer IP header should have a new value indicating that the next protocol is ESVP.

ESVP Security

ESVP relies on ESP for handling the encrypted portion of the payload and on the Internet Key Exchange (IKE) [2] for setting up and managing the keys required to perform encryption and authentication. Therefore, the security properties of ESVP with respect to the encrypted portion of the payload should derive directly from the properties of IKE and ESP.

Are You the Arcanist?

Last's month's question was:

What is next in the series: 212, 312, 213, 214 ... ? And why?

There were no winners of last month's Arcanist contest. The series is the list of valid North American area codes in order of the number of decadic pulses required to transmit them. Note that the digit 1 was the fastest to dial (1 pulse) and 0 the slowest (10 pulses). Some potential area codes, such as 211 or 011, were unavailable because they had special meanings or because of restrictions on the values of certain digits (e.g., the second digit could only be 0 or 1).

In the days of rotary dial phones, the listed series of area codes were the quickest to dial, and therefore the most desirable. The areas they represent are Manhattan, Chicago, Los Angeles and Dallas. Following these would be 313 (Detroit, also 7 pulses) and then the 8-pulse area codes 215 (Philadelphia), 314 (St. Louis), 413 (Massachusetts) and 512 (Austin, Texas).

The question for this month: If you have this list: 17, 24, 1, 8, 15, 23, 5, 7, 14, 16, 4, 6, 13, 20, 22, 10, 12, 19, 21, 3.

What are the next five numbers?!

Submit your answer to wsp@cnp-wireless.com

Additional mechanisms are required to secure the portion of the packets that ESVP leaves unencrypted (the clear text). For example, when ESVP is used to secure the unencrypted portion of the packets between the end points and a trusted intermediary, as with the TCP/IP headers in the example application described on the next page, the security properties of ESP will also apply to the TCP/IP headers, allowing a trusted intermediary to have access to them. In this case, no end-to-end security property applies to the unencrypted portion of the packets.

With ESVP the end points have complete control over the portion of the packets, if any, that is not encrypted or authenticated. Security policies, therefore, can be implemented by system administrators who can decide, even on a per-packet basis, to what extent ESVP should be applied, depending on the trust relationship they have established with their service providers, as well as on the additional security mechanisms available to protect the unencrypted portions of the packets.

ESVP at Other Layers

ESVP is designed as an IPsec option to offer a generic capability at the IP layer that can be used by higher layers. ESVP could also be implemented at other layers by appending the first four bytes of ESVP packet format at any layer. For example, if ESVP were implemented at the secure socket layer (SSL), the first four bytes of ESVP packet format would be appended to the partially encrypted application data, where the cleartext length of ESVP would refer to any contiguous unencrypted application data. By implementing ESVP at the socket layer, it is possible to enable intermediary-based overlay services.

Impact of Mobility

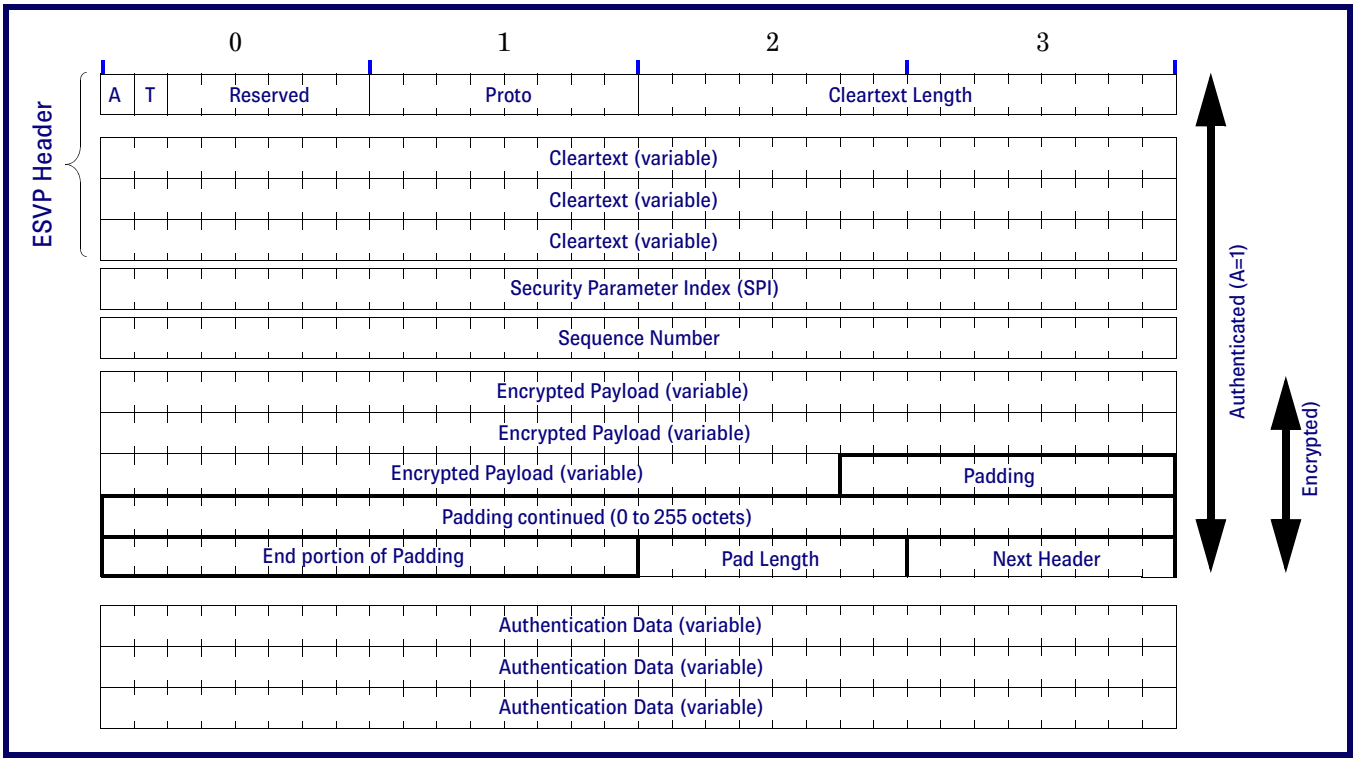
Two important issues highlight the impact of user mobility on intermediary-based services. For simplicity, we assume that a single intermediary provides services to a session between a wireless user and an enterprise gateway. The following discussion applies to more general scenarios, including those involving multiple intermediaries.

Issue #1: Intermediary Communication

The basic communication protocol for enabling intermediary-based services was outlined in **last month's** *Wireless Security Perspectives* on page 4, under the section heading: "Communication between End-points and Intermediary." However, when a client moves from one network to another, the handoff procedures may result in a new intermediary. This applies to both idle roaming as well as handoff (with an active packet data session).

The advertisement and registration procedures must be repeated during handoff. Registration involves mutual authentication between the intermediary and the end-points to confirm each others' identity after which the intermediary receives an authorization to provide services. This involves communicating with the home network.

Figure 1: ESVP Packet Format with Tail Encrypted (T=0)



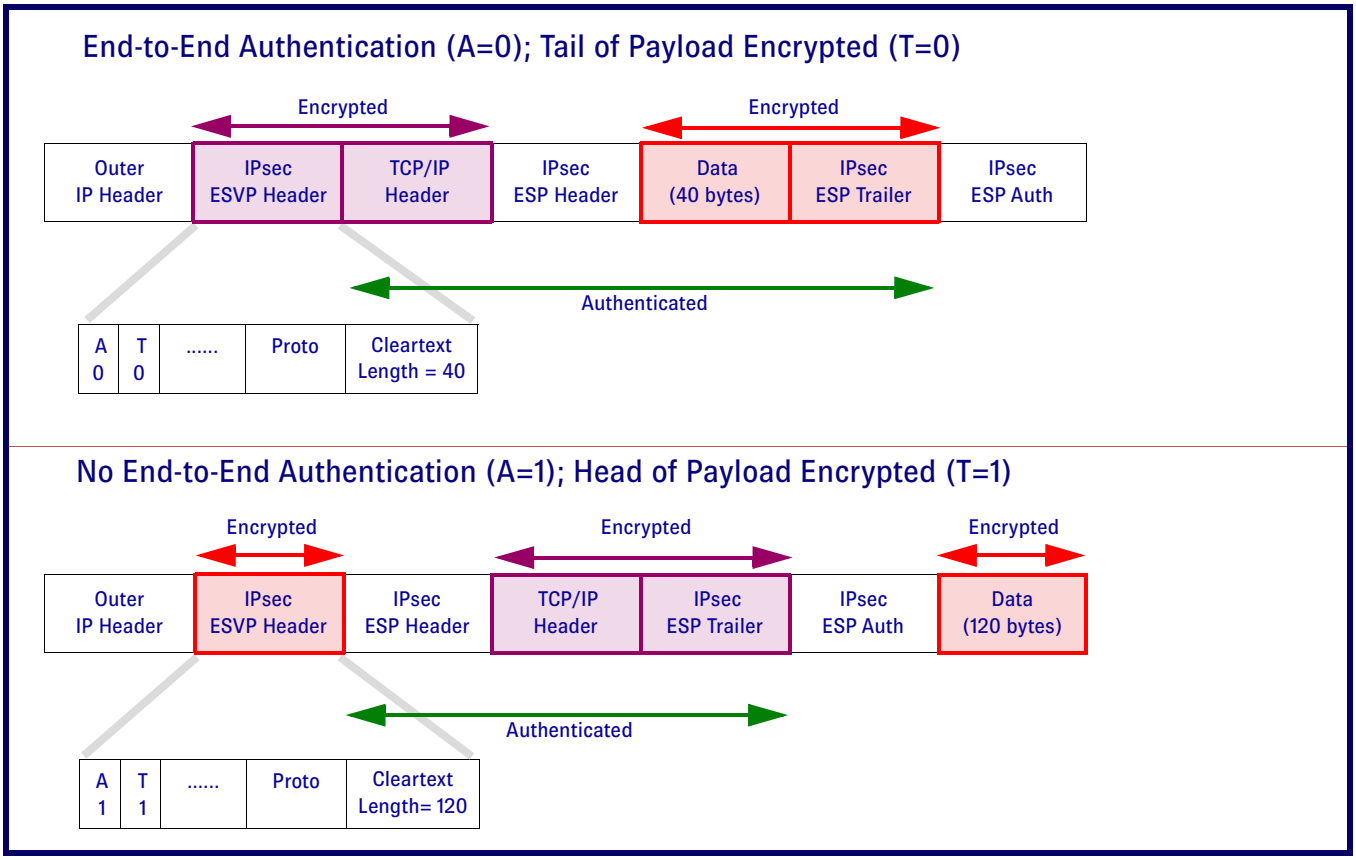
Issue #2: Key Management

Management of the keys shared with the intermediary is important during active handoff, where the security association between the end points should not be affected. Two choices exist:

1. Transfer of the secure session key between the old and the new intermediary; or
2. Form new security associations (requiring new keys) with the new intermediary.

If the home network is involved in the registration process, it may be efficient to securely transfer the keys used in the old security association from the old intermediary to the new one. In particular, this will be applicable to the case of link layer handoff where existing wireless standards already address this issue [3]. However, a transfer of keys, buffered data and any cryptographic counter information (in order to prevent replay attacks) between the intermediaries will require a secure path.

Figure 2: ESVP in Tunnel Mode



To secure that path, a new security association can be created between the new intermediary and the other end point. If this is an enterprise gateway, it makes sense to multiplex multiple sessions in one security association between the intermediary and the gateway. However, if this is done, transfer of the keys for the old security association between the intermediary and the enterprise gateway to the new intermediary may result in compromising the security of all the other sessions that are multiplexed on the old security association. It is safer to establish a new security association between the new intermediary and the enterprise server.

Example Application

Figure 3 shows a wireless enterprise user communicating with an enterprise gateway. First, the user goes through the registration, authentication and authorization processes with the wireless provider (or the Internet service provider or both), the enterprise gateway, and if the user is in a foreign domain, the home domain.

The mobile user learns about the intermediary-based services (e.g., TCP PEP service) from advertisements from the intermediary (e.g., a Packet Data Serving Node). The mobile user, the enterprise gateway and the intermediary then agree on the services required for the session.

Next, the mobile user establishes an ESVP security association with the enterprise gateway. It uses the secret key exchanged with the enterprise gateway to encrypt TCP payload, but leaves the TCP/IP header unencrypted. To secure the TCP/IP header from the rest of the network, the user establishes another ESVP security association with the intermediary, and the intermediary establishes a third ESVP security association with the enterprise gateway.

As illustrated in Figure 2, in the first ESVP operation at the mobile user, the TCP/IP headers are left open and the T-bit is set to 0 because the tail of the TCP/IP packet is encrypted. In the second ESVP operation, the inner TCP/IP headers are encrypted and the T-bit is now set to 1. There is no need to re-encrypt the TCP payload. IPsec ESP security associations could also be used between the end points and the intermediary, but the use of T-bit saves an additional encryption step. On receiving the encrypted packet from the mobile user, the intermediary decrypts the outer ESVP packet and hence the TCP/IP header. The intermediary performs the TCP PEP service, applies another ESVP operation to secure the TCP/IP header, and sends the encrypted packet to the enterprise gateway, using the security association established with it.

The enterprise gateway receives the encrypted packet and applies two ESVP operations to obtain the payload and the protocol headers. Note that the outer ESVP tunnel between the mobile and the intermediary could be replaced by a secure wireless link layer when available. This approach would save the overhead of the second ESVP operation.

Figure 3: Mobile Wireless Enterprise User benefiting from Intermediary-based Services

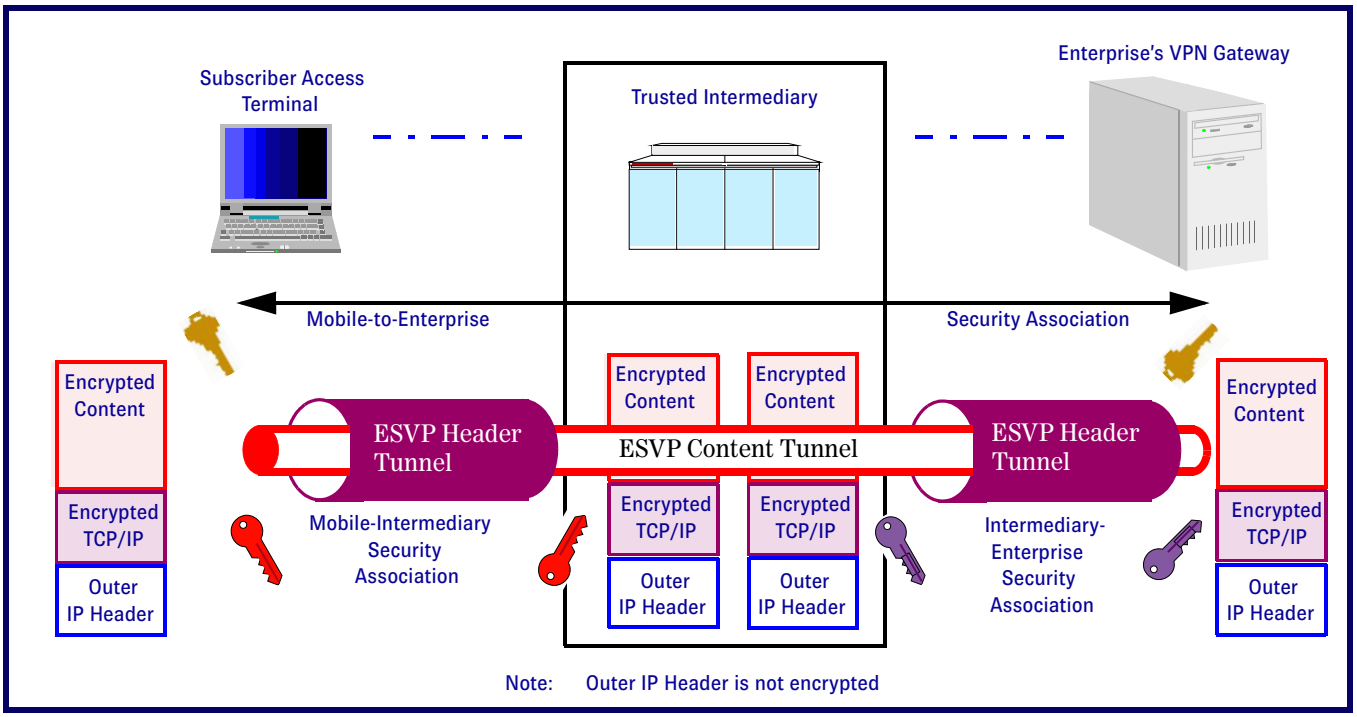
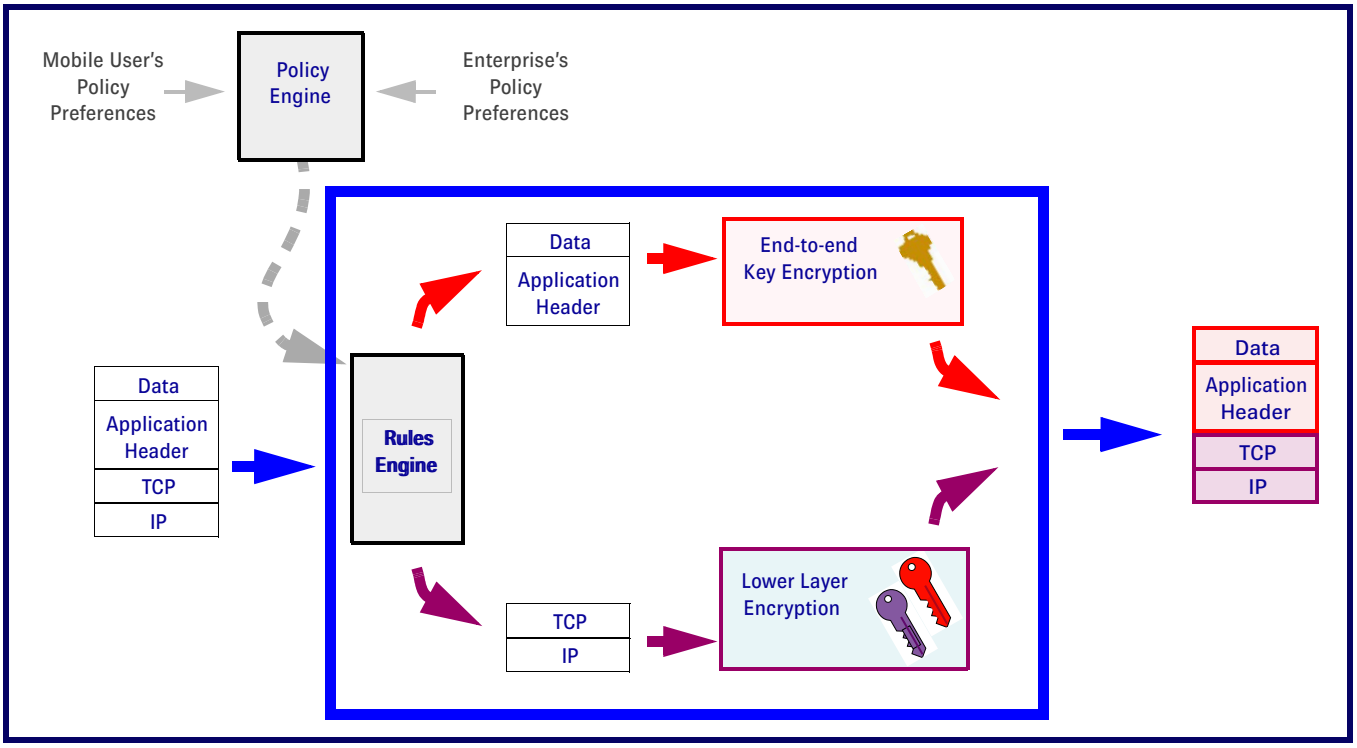


Figure 4: ESVP Packet Generation



In this example, an application header accompanies the application data payload. For the sake of simplicity, these are depicted as "Data" in Figure 2. The blue box in Figure 4 shows these parts treated separately as they proceed through their two tunnels.

Figure 3 illustrates the red tunnel delivering the "Data," while the two purple tunnels deliver the TCP/IP Header.

In Figure 4, the ESVP operations are shown along with the policy and rules engine. If the mobile user roams

into a foreign domain during an ongoing session, then the handoff procedure will involve either a session key transfer or a new session key setup. However, the end-to-end ESVP security association that exists between the mobile user and the enterprise gateway will remain intact. The mobile user must receive new service advertisements from the intermediary in the foreign domain and agree on the services required.

Upon session completion, the security associations between the mobile user, the intermediary and the enterprise gateway are terminated.

One-to-Many vs. One-to-One

In our architecture, all security associations involving the end-points and the intermediary are *one-to-one*. That is, only two nodes (end-point or intermediary) are part of any security association.

It is possible to have composite security associations or *one-to-many* security associations that involve more than two nodes, such as both the end-points and the intermediary[4]. Each approach has advantages and disadvantages. For example, suppose that multiple intermediaries are involved in providing services to two end points.

- A one-to-one security association between two intermediaries (if any), or between an intermediary and a gateway or server end-point, allows multiplexing of several sessions into one security association, whereas the one-to-many approach will require as many security associations as the number of users.
- In the case of the one-to-one approach, user mobility involving only its first intermediary will not affect the security associations among the other intermediaries and the security associations between the intermediaries and the other end point. With the one-to-many approach, every change of an intermediary will affect all the nodes.
- A potential advantage of one-to-many security associations is that because the same key is used across all the nodes involved in the security association, an intermediary need not decrypt and encrypt every packet. In the case of one-to-one security associations, each has a separate key. Therefore, an intermediary must decrypt using one key and encrypt using another key for every packet transmitted end-to-end.
- A one-to-many security association allows more generality in making different parts of the packet accessible to a different subset of intermediaries. The one-to-one approach requires a large number of security associations to achieve this.

We chose one-to-one security associations because they are simpler, use well-established one-to-one key exchange mechanisms and are more efficient in the presence of user mobility. They address most of the intermediary-based services that can be envisioned.

ESVP Compared

Several other intermediary-based services have been proposed and studied extensively (e.g., [5, 6, 7] for TCP performance enhancements over wireless, [8, 9] for active networks, OPES [10], and MIDCOM [11]). None of these address how packet level information can be made available to an intermediary when a security solution such as IPsec is used. We address two of the most important – TF-ESP and ML-IPsec:

1. At IETF-44, Bellovin proposed a variant of ESP called Transport-Friendly ESP (TF-ESP) [12]which left certain portions of the payload unencrypted. He also suggested that the clear text be integrity protected with the rest of the ESP header. The problem with this approach is that when the ESP header is integrity protected with keys known only to end points, the intermediaries cannot verify that the information is correct. Also, end-to-end integrity protection does not allow an intermediary to enable services or performance enhancements that require modification of the clear text.

   In ESVP, the A-bit allows an end-point to grant the trusted intermediary write access to the clear text. The clear text can be verified (regardless of whether it is authenticated end-to-end) at the trusted intermediary by using another ESVP tunnel between the end-point and the trusted intermediary.

   ESVP also allows the flexibility of having the head or tail of the payload in the clear, which prevents double encryption for certain applications, as illustrated by the example application described, beginning on **page 4**. Another situation where the T-bit could prevent additional encryption of encrypted data is when Secure Socket Layer (SSL) is used over ESVP. Bellovin proposed another variant of ESP, called a "Disclosure" Header, where all fields of interest are copied from the payload into an unencrypted portion of the ESP header [12]. Although cleaner,

this approach requires pre-defined header formats to be known to the trusted intermediaries and end-points, making it less flexible. The trusted intermediaries also need to be informed about which "disclosure" header format is being used. This approach also increases the length of the packet, which might be prohibitive for bandwidth-limited wireless scenarios.

2. Zhang *et al* have proposed a generic approach called Multi-Layer IPsec (ML-IPsec), which divides the payload into multiple zones, with each encrypted using a different key[4]. Composite security associations involving intermediaries are established, and intermediaries with the keys to encrypt/decrypt certain zones are given access to those zones. The fine-granular control provided by this approach makes it complex. ML-IPsec changes the nature of the security associations from one-to-one to one-to-many. We retain the security association as one-to- one.

   SSL secures only the application payload, leaving the transport and network layer headers as clear text. Therefore, SSL over IPsec could be used to obtain some intermediary-based services, such as TCP PEP. Our approach proposes a simple framework that does not restrict the services to being based only on exposure of TCP/IP headers. Our framework could be applied at the IP layer or above for a variety of services, including those that expose application headers.

Last, but very important from a wireless perspective: Unlike ESVP, neither TF-ESP nor ML-IPsec address mobility or dynamic invocation and revocation of intermediary-based services.

References

[1] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*. RFC 2401, Nov. 1998.

[2] D. Harkins and D. Carrel. *The Internet Key Exchange Services*. (IKE). RFC 2409, Nov. 1998.

[3] *Guide to 3rd Generation Security.* TR 33.900, Third Generation Partnership Program 2 (3GPP2).

[4] Y. Zhang and B. Singh. *A Multi-layer IPsec Protocol.* In Proc. 9th Usenix Security Symposium, Aug. 2000.
www.wins.hrl.com/people/ygz/papers/usenix00/index.html

[5] H. Balakrishnan, S. Seshan, and R. Katz. *Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks.* ACM Wireless Networks, Dec. 1995.

[6] J. Border, et al. *Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations.* RFC 3135, June 2001.

[7] M. Chan and R. Ramjee. *TCP/IP Performance over 3g Wireless Links with Rate and Delay Variations.* In Proc. of ACM Mobicom, Sep. 2002.

[8] S. Kasera, S. Bhattacharyya, M. Keaton, D. Kiwior, J. Kurose, D. Towsley, and S. Zabele. *Scalable Fair Reliable Multicast using Active Services.* IEEE Networks, Jan. 2000.

[9] R. Keller, et al. *An Active Router Architecture for Multicast Video Distribution.* In Proc. of IEEE Infocom, Mar. 2000.

[10] A. Barbir, et al. *An Architecture for Open Pluggable Edge Services (OPES)*. Internet Draft, Dec. 2002.
www.ietf.org/proceedings/03mar/I-D/draft-ietf-opes-architecture-04.txt

[11] P. Srisuresh, et al. *Middlebox Communication Architecture and Framework*. RFC 3303, Aug. 2002.

[12] S. Bellovin. *Transport-friendly ESP (or layer violation for fun and profit)*. IETF-44 TF-ESP BOF, Mar. 1999.

About the Authors

Dr. Sneha Kumar Kasera is an assistant professor in the School of Computing at the University of Utah in Salt Lake City. From 1999-2003, he was a member of technical staff in the mobile networking research department of Bell Laboratories. He has a Ph.D. in Computer Science from the University of Massachusetts, Amherst, and a Master's degree in electrical communication engineering from the Indian Institute of Science, Bangalore. Dr. Kasera's research interests include: computer networks, and systems encompassing mobile and pervasive computing; wireless networks, network security and reliability, overload and congestion control; multicast communication; Internet pricing, Internet measurements and inferencing.

Dr. Thomas Woo is a Director in the Networking Research Lab at Bell Laboratories. He currently heads two departments, where he leads research and development efforts in mobile computing, wireless security and in Voice over IP, respectively. Dr. Woo has more than 15 years experience in the field of IP networking, network security and wireless data. He has published numerous original research papers and has received more than 10 US patents. He is an editor for the IEEE Wireless Communications. He has a B.Sc. degree (First Class Honor) from the University of Hong Kong and M.S. and Ph.D. degrees in Computer Science from the University of Texas at Austin.

Semyon (Simon) Mizikovsky joined Lucent Technologies, Inc in 1994, and has been leading the standardization efforts of wireless signaling, protocols, wireless security and fraud detection and prevention technologies. He heads up an internal team of security experts dedicated to developing and deploying authentication and encryption technologies for wireless industry. He has 29 years of professional experience in the telecommunications and wireless industry such as authentication, information privacy, telecommunications and data communications signaling protocols, commercial and consumer TV products, and satellite communications.

Dr. Ganapathy S. Sundaram is a distinguished member of technical staff in the wireless secure communications group at Lucent Technologies in Whippany, New Jersey. He holds a Ph.D in mathematics specializing in algebra, arithmetic, and geometry from Purdue University, West Lafayette, Indiana. Dr. Sundaram's research areas include algebraic geometry, number theory, algebraic coding theory, cryptology and data security, data networking algorithms over wireless, and wireless algorithms in general.

Upcoming Wireless Security and Fraud Conferences & Events

The following are upcoming wireless, wireless security and general security conferences and events that may be of interest to our wireless security and network security practitioners.

NWACC Workshop 2004 – Wireless Security
1st March 2004
OHSU West Campus
Portland, OR
www.nwacc.org/conferences/wirelesswkshp.html

Australian Wireless Summit 2004
3rd- 4th March 2004
Cockle Bay Wharf – Darling Park
Sydney, Australia
www.acevents.com.au/wireless2004

12th Annual Wireless Systems Design Conference & Expo
8th- 10th March 2004
San Diego Convention Center
San Diego, CA
www.wsdexpo.com

Gartner Wireless & Mobile Summit
8th- 10th March 2004
Chicago Marriott Downtown
Chicago, IL
www3.gartner.com/2_events/conferences/ra7.jsp

Wireless Future Conference
12th- 16th March 2004
Austin Convention Center
Austin, TX
www.wirelessfuture.org

PerCom 2004 (2nd IEEE International Conference on Pervasive Computing and Communications)
14th- 17th March 2004
Holiday Inn
International Drive Resort
Orlando, FL
www.percom.org

ACM Symposium on Applied Computing
14th- 17th March 2004
Hilton Park Hotel
Nicosia, Cyprus
www.ing.unipi.it/sac04

Wireless LAN and 802.11 Security Workshop
16th March 2004
Doubletree Hotel
Tysons Corner, VA
www.itvshop.com

WiFi Planet Conference & Expo
16th- 18th March 2004
Sheraton Centre Hotel
Toronto, Canada
www.jupiterevents.com/wifi/canada04/index.html

CTIA Wireless 2004
22nd- 24th March 2004
Georgia World Congress
Atlanta, GA
www.ctiawireless2004.com

[Note: Co-located with IEEE WCNC 2004]

WCNC 2004 (IEEE Wireless Communications and Networking Conference)
21st- 25th March 2004
Georgia World Congress
Atlanta, GA
www.wcnc.org

[Note: Co-located with CTIA Wireless 2004]

Infosec World Conference & Expo 2004
22nd- 24th March 2004
Rosen Centre Hotel
Orlando, FL
www.misti.com

NSDI '04 (1st Symposium on Networked Systems Design)
29th- 31st March 2004
Grand Hyatt
San Francisco, CA
www.usenix.org/events/nsdi04/index.html

RFID Journal Live! – Where RFID is Happening
29th- 31st March 2004
Hilton Chicago
Chicago, IL
www.rfidjournallive.com

Fraud and Security Patent News

US Patent: 6,697,944

Digital content distribution, transmission and protection system and method, and portable device for use therewith

A digital content file distribution, transmission, and protection system comprising a digital content provider having stored therein a digital content file such as an audio file, video file, literature, program file, etc. The digital content provider includes an authentication interface and a USB port from which the digital content file may be downloaded. The system also contemplates a portable device to which the digital content file will be transferred. This portable device includes an authentication interface and a USB port, and conforms to the USB storage device class. The portable device communicates with the digital content provider via the USB interface and, pending the establishment of a trusted relationship, downloads the digital content file therefrom. The establishment of the trusted relationship with the portable device is accomplished through communications between the authentication interfaces over the USB. If the level of the trusted relationship is high, the digital content provider may transmit unencrypted digital content to the portable device without fear of violation of the DRM associated with this content. A medium level requires some form of encryption, and a low level only allows downloading of digital content with a low level requirement for DRM. The digital content provider may be a PC, a kiosk, a server, etc.

Issued: February 24, 2004

Inventors: Thomas Jones and Bill Brackenridge

Assignee: Microsoft Corporation (Redmond, WA)

Notable References:

[1] *Digital Rights Management*: www.intertrust.com/main/overview/drm.html

[2] *Elliptic Curve Cryptography Question & Answers*; Brochure; Certicom Corp; 1997-1998.

US Patent: 6,697,839

End-to-end mobile commerce modules

A system providing the capability by which mobile applications can provide improved usability in the areas of information input to the mobile application, such as to online forms, storage and management of information used with mobile applications, and support for mobile application content created using various different formats. The system utilizes a server-side approach, in which online applications for a mobile device are invoked on a server through a server-side proxy/cache. The proxy scans the content that is generated by the application for transmission to the mobile device to find forms that may be embedded in the content. When a form is encountered, fields of the form are filled with stored information based on automatically generated mapping information. The information is stored in a secure, extensible wallet used to store information for automated entry into forms transmitted from online applications to mobile devices. The proxy also translates the content that is generated by the application from an initial format to a format that is supported by the mobile device.

February 24, 2004

Inventors: Jean Sini and Jacob Christfort

Assignee: Oracle International Corporation (Redwood Shores, CA)

US Patent: 6,697,829

Method of and apparatus for generating random numbers

A random number generator that has a random event source, a random event detector, and a counter for counting the number of pulses generated by the detector for a predetermined length of time. Two memories are provided, in which are stored successive sets of counts, and a controller compares the sets to determine whether one or both of the sets counted one or more events. Where both sets have one or more events, no output is generated, and where both sets have no events, no output is generated. However, where one set has one or more events and the other set has no events, then a binary number is output in dependence on which of the two sets recorded events. This random number generator has the advantage that the probability of counting no events does not have to be exactly equal to the probability of counting one or more events while still ensuring truly random results.

Issued: February 24, 2004

Inventor: Mark Shilton

Assignee: AEA Technology plc (Didcot, Great Britain)

Notable References:

[1] J. Von Neumann (summary by G. Forsythe). *Various Techniques Used in Connection with Random Digits*. Von Neumann's Collected Works, vol. 5, pp. 768-770, 1963 (XP002103231), reprinted from J. Res. Nat. Bur. Stand., Applied Math. Series 3: 36-38 (1951).

US Patent: 6,697,490

Automatic resynchronization of crypto-sync information

An apparatus and method for transmitting and receiving cryptographic information which provide a mechanism for resynchronization between a transmitter and receiver of the cryptographic information. A cryptographic synchronization counter at the transmitter generates a transmitter signature tag. A corresponding cryptographic synchronization counter at the receiver generates a receiver signature tag. Information is ciphered and the transmitter signature tag is appended to the ciphered information. The ciphered information is received. The transmitter signature tag is compared to the receiver signature tag and the cipher text is decipher into plain text if the tags are equal. If the tags are not equal, the receiver crypto-sync counter is incremented and a new

receiver signature tag is calculated to determine if the receiver is resynchronized (i.e., tags are equal) to the transmitter. If after a certain number of increments, resynchronization does not occur, a resynchronization procedure is initiated.

Issued: February 24, 2004

Inventors: Semyon Mizikovsky and Milton Soler
Assignee: Lucent Technologies Inc. (Murray Hill, NJ)

US Patent: 6,697,355

Method and apparatus for communication using a mobile internet in a mobile communication network

A mobile internet system and method in a mobile communication network, in which a mobile host given an Internet Protocol (IP) address uses an existing Code Division Multiple Access (CDMA) type mobile network and an Home Location Register and an Inter-Working Unit in a personal communication system network to establish communications without restricting a mobile host to a particular network. The mobile internet system and method includes a plurality of mobile hosts, a plurality of mobile access points, a mobile router, and a plurality of gateway routers.

Issued: February 24, 2004

Inventor: Byung Lim
Assignee: LG Information & Communications, Ltd. (Seoul, Korea)

US Patent: 6,697,354

Method and system for distributed network address translation for mobile network devices

A method and system for distributed network address translation for mobile network devices. A mobile network device requests one or more locally-unique ports with a Port Allocation Protocol from a second network device on a first network to identify the first network device on the first network if the mobile first network device roams to a second external network. One or more default or ephemeral ports on the mobile network device are replaced with one or more locally-unique ports obtained with the Port Allocation Protocol. The one or more locally-unique ports allow distributed network address translation to be used with the mobile network device. A combination network address is created for the mobile network device with a locally unique port and an external network address for the first network to identify the mobile first network device if the mobile first network device roams to a second external network.

Issued: February 24, 2004

Inventor: Michael Borella, *et al*
Assignee: 3Com Corporation (Santa Clara, CA)

About WSP Patent Listings

The US Patent and Trademark Office (USPTO) frequently grants fraud and security patents that will be of interest to some of our wireless security practitioners. Each patent includes the invention title – linked to the corresponding USPTO web page. We brief ly describe it and provide, at minimum, its inventor(s) and assignee (owner).

With the listing of patents provided each month, one can see *who* is doing *what* in the world of wireless inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

If the wording in these is difficult to understand, recognize that the patent abstracts are generally provided in their raw legal-jargon form, straight from an attorney's word-processor. Sometimes we edit the abstracts for readability when the legalese is too impenetrable.

Notable References:

[1] Kent, Stephen, *Evaluating Certification Authority Security,* Aerospace Conference, 1998 IEEE, Online, vol. 4, pp. 319-327 (Mar. 21-23, 1998).

[2] Thayer, Rodney. *Bulletproof IP With Authentication and Encryption IPSec Adds a Layer of Armor to IP*. Data Communications, vol. 26, No. 16, pp. 55-58, 60 (Nov. 21, 1997).

[3] Afifi, H. , et al. *Method for IPv4-IPv6 Transition.* Proceedings IEEE International Symposium on Computers and Communications, Jul. 6-8, 1999, pp. 478-484.

US Patent: 6,695,214

Device with integrated circuit made secure by attenuation of electric signatures

An integrated circuit device designed to be incorporated in a portable object with memory, in particular of card format. The integrated circuit device comprises at least a capacitor for attenuating the amplitude of current peaks (Idd) consumed by the integrated circuit device. The attenuation of such current peaks is particularly useful for attenuating electric signatures in smart cards.

Issued: February 20, 2004

Inventor: Robert Leydier, *et al*
Assignee: Schlumberger, Systemes (Montrouge, France)

US Patent: 6,694,431

Piggy-backed key exchange protocol for providing secure, low-overhead browser connections when a server will not use a message encoding scheme proposed by a client

A method, system, and computer program product for establishing security parameters that are used to exchange data on a secure connection. A piggy-backed key exchange protocol is defined, with which these security parameters are advantageously exchanged. By piggy-backing the key exchange onto other already-required messages (such as a client's HTTP GET request, or the server's response thereto), the overhead associated with setting up a secure browser-to-server connection is minimized. This technique is defined for a number of different scenarios, where the client and server may or may not share an encoding scheme, and is designed to maintain the integrity of application layer communication protocols. In one scenario, a client proposes a message encoding scheme, but the server will not use this proposed scheme. The server proposes a different scheme, after which the client re-issues its request for secure content.

Issued: February 17, 2004

Inventor: Carl Binding, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,694,430

Data encryption integrated circuit with on-board dual-use memory

An interface chip for a peripheral module connectable to and for use with a host computer. It uses a static Random access memory (SRAM) within the interface chip for both encryption of data packets and temporary storage of Card Information Structure (CIS) information. The CIS information is stored in the SRAM only during the power-up phase of operation, when encryption of data packets is not necessary and thus the memory is not being utilized for that purpose. This precludes the need for a separate SRAM IC, thus saving space on the card.

Issued: February 17, 2004

Inventors: Chris Zegelin and Sarosh Vesuna

Assignee: Symbol Technologies, Inc. (Holtsville, NY)

Further Patent Information

To obtain a complete copy of these patents, contact the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

800-786-9199 or 703-308-4357