Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 79 (2001)

Heft: 10

Artikel: Empowering the user to correctly assess security

Autor: Pope, Nick / Ross, John

DOI: https://doi.org/10.5169/seals-876585

IT-Security

Empowering the User to Correctly Assess Security

As with many other technologies, IT security is becoming more and more complex. In many instances the user is presented with questions that can only be answered by an IT security expert. The user is left uncertain of what to do next and whether he can carry on with confidence or whether real dangers exist.

This article will present a ground-breaking approach to interfacing security to users in a coherent and comprehensible manner. It describes how the complexities of security can be brought together in a way that enables the user to make an informed assessment of the security risks without having to be an expert.

NICK POPE AND JOHN ROSS

The Current Situation

Currently, information relating to security is provided to users in a patchwork manner, which is incomprehensible and in some cases misleading. It is generally presented in technical terms that cannot be interpreted without the aid of a security expert and often provides no help to the user in assessing the risks. Internet shopping and business-to-business e-commerce provide the potential for significant savings.

However, without the ability for the user to assess the effectiveness of security measures that are in place, it is impossible for him to use the Web and other applications with confidence, thereby it is limiting the potential of the Web and the Internet. Consider, for example, using the Web to access a site from which you have decided to purchase some goods. In making that purchase you will be providing sensitive information such as credit card details for payment.

How can you:

- be sure that these details are not going to be copied by a hacker snooping on the Internet?
- be certain who operates the web site that you are accessing ?
- be confident that the web site employs reasonable practices in handling your payment details or dealing with any complaints?

Presently, there is a security protocol widely available to protect the privacy of information passing over the Web called Secure Socket Layer (SSL). There are also more sophisticated mechanisms, such as SET, slowly entering the market. Web browsers commonly provide an indication of whether SSL protection is applied through a padlock or key icon. However, in many cases (e.g. where a page is made up of several frames) this padlock does not appear when SSL protection is being applied. Moreover, the strength of protection afforded by SSL depends on the size of the key being used, 128 bit being generally accepted as being very difficult to break, whereas 40 bit can be easily broken. An expert user may be able to find this information through particular features of the web browser and understand the implications, but the

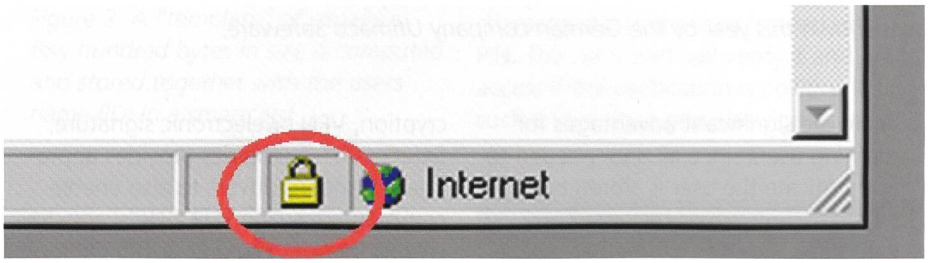

Figure 1. Microsoft Internet Explorer Padlock Icon.

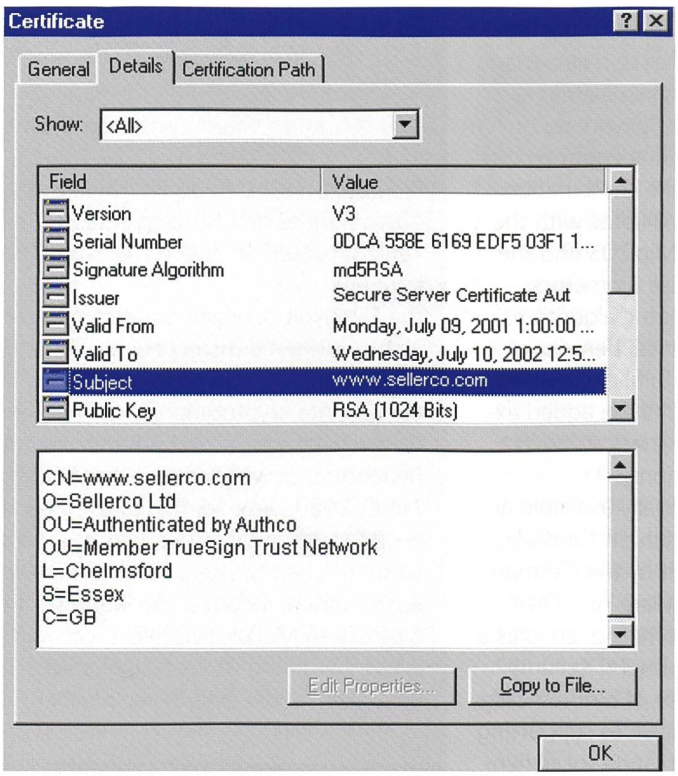

Figure 2. Certificate Information Display from Microsoft Internet Explorer.

general user is unlikely to be able to find the necessary information, let alone comprehend the implications (fig. 1).
As well as protecting the confidentiality of information, security protocols such as SSL authenticate the name of the web site being accessed, as well as the organisation responsible for operating that site. However, this information is only made available to the user in a way in which it is difficult for the ordinary user to be found, and can only be interpreted by an expert (fig. 2).
When situations occur that are potentially a security risk, for example when the data comes from a source different from that identified by the security protocol, a warning message is displayed by the user's web browser. However, the user is not generally aware of the potential implications of such a situation and commonly ignores the warning altogether, treating it as "just one of many warning windows that pop up from time to time".

WaryWolf™

"Security and Standards", with its WaryWolfTM software has made a major breakthrough in bringing security. It empowers everyday users of open network services, such as the World Wide Web, to make an informed decision on the security risks. Rather than the existing array of security relevant information that may be thrown at the current web user, WaryWolfTM provides a straightforward interface to the user. It provides all the information that the user needs through a single interface and in a way that is easily understood. The information is provided through a layered interface which starts with a simple traffic light indicator giving a basic indication of whether an access is secure, and is backed up by detailed information for situations where further investigation is necessary.
The starting point for the WaryWolf™ user is the traffic light indicator that shows (fig. 3):

- Green, to indicate that the current web access is secure according to the user's assessment criteria.
- Amber, to indicate that the security of current web access has factors which may require caution.
- Red, to indicate that the current web access is not secured or the security mechanisms being applied have a major weakness, for example site certificate is revoked.

Figure 3. Three states of WaryWolf™ Traffic Light Indicator.

The assessment criteria, which define exactly what constitutes a secure access, are controlled by the user and can be set to reflect the security policy of the user's organisation. Default assessment criteria are provided as initial settings for the user when he starts using WaryWolf™.

The user can obtain further information on the security of the current access by expanding the basic view to provide a display of the security factors which lead to the current rating (fig. 4). This expanded display shows the factors which effect the security of an access along with an indicator of the rating of that

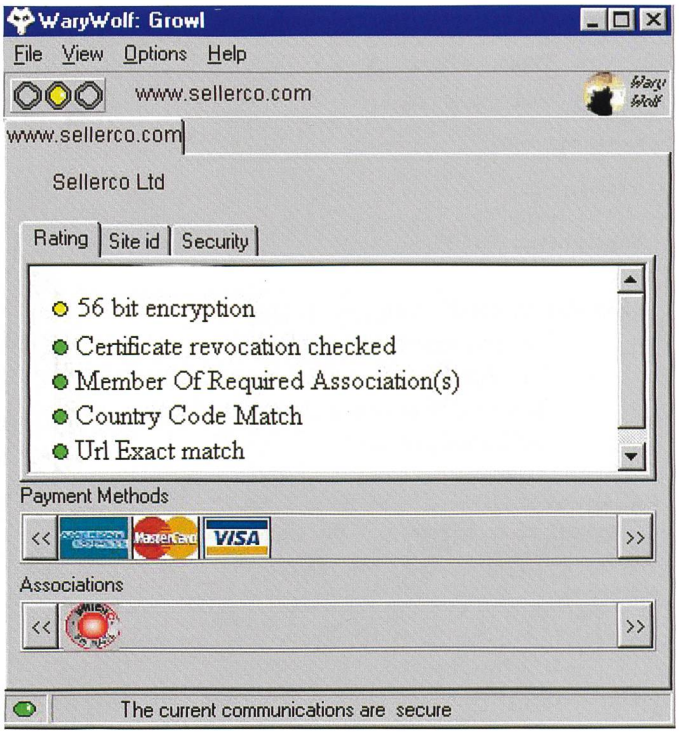

Figure 4. The WaryWolf™ display of Security Rating Factors.

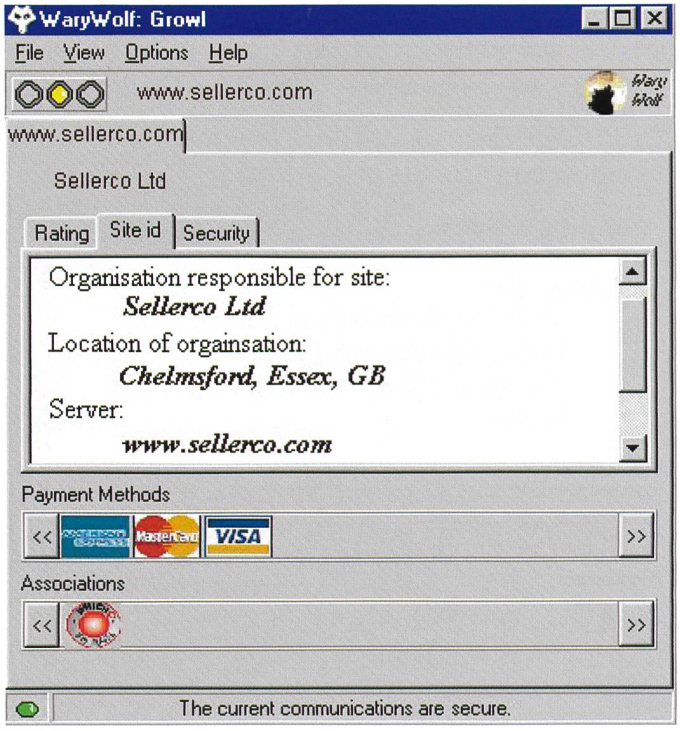

Figure 5. The WaryWolf™ display of Site Identity Information.

factor in accordance with the assessment criteria set by the user. Thus, in the example shown above, because the user's assessment criteria rule that 56 bit encryption should be treated with caution that factor of the access security is set to amber.
The overall rating for the site currently being accessed is based on the lowest rating factor. So, in the example illustrated above, because the security factor relating to key length is rated amber, the over rating is set to amber. If, for example, the certificate used to secure the access had been revoked, which would be rated as red (not secured), the overall rating would be red.
WaryWolf™ rating can take into account commercial factors as well as the technical security mechanisms being used. Where a web site is known to belong to an association which is important for assessing the trustworthiness of the site, this can be included in the rating. For example, where an independent body, such as a consumer association, recognises a site as following a code of practice and so providing a Trust Mark to that site, this can be displayed as part of the site assessment, and if necessary included as part of the overall rating for the site. Moreover, because membership of an association can be validated through the certified identity, the user is protected against a site masquerading association membership through placement of the appropriate icon on its site.
The user can find out further information about the site being accessed, derived from the security certificate but displayed in a generally understandable form, by clicking on the site tab as shown below (fig 5).
By clicking on the Security Tab information the user is provided with further details about the security being applied to the current secure access (fig. 6).
A further important feature of WaryWolf™ information display is that when a site is made of data provided by two separate web sites, the user is provided with information about all the sites accessed and so can be fully informed of the security implications (fig.7).

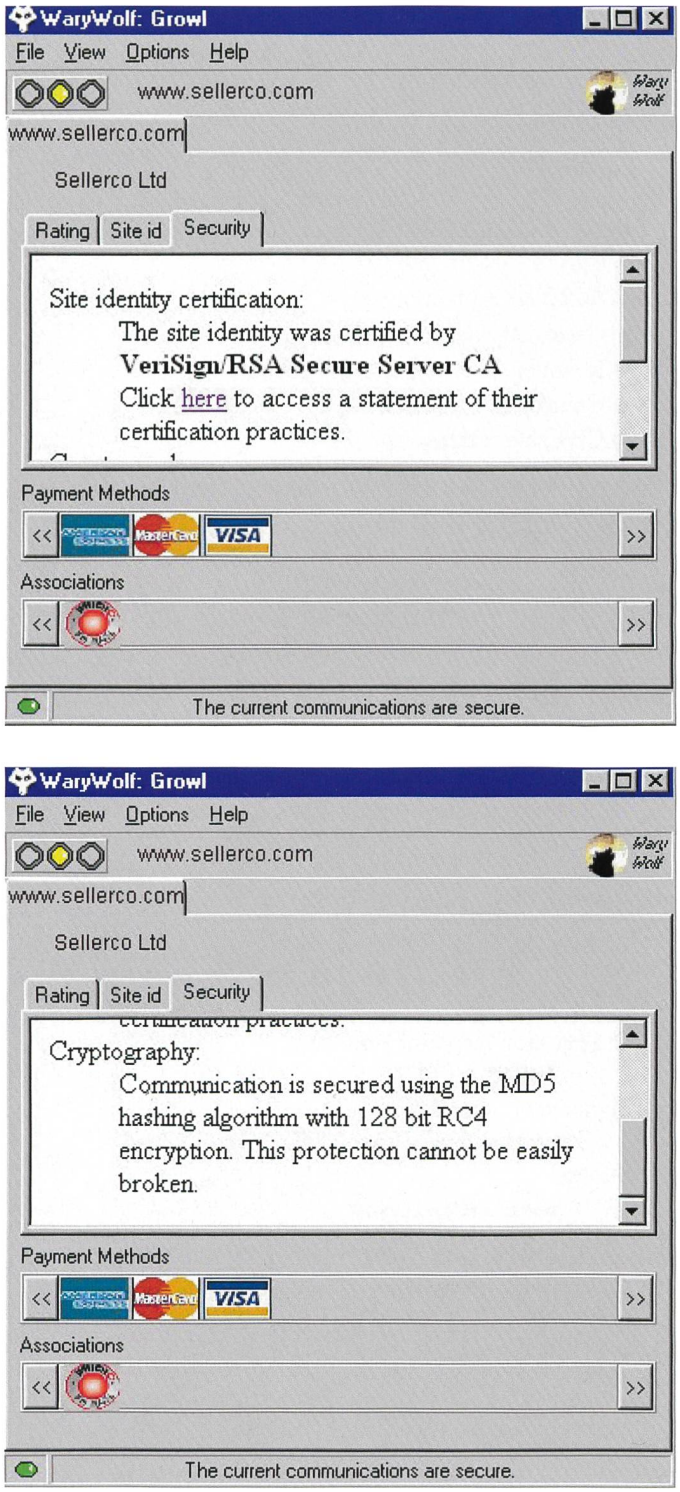

Figure 6. The WaryWolf™ display of Security Information.

Conclusions

As described above WaryWolf™ provides the normal every day Internet user with a simple indication of any potential security problems. This starts with the overall traffic light giving the user an immediate indication of whether the access to the site is safe or not. This is backed up by information on the status of all the important security factors, as well as other relevant information, provided through a single interface. Instead of leaving the user bemused with a patchwork of indicators, warnings and detailed technical information, WaryWolf™ provides the user with a single source of information. With the information provided by WaryWolf™ the user is able to make the important decision on whether he should proceed with a transaction in full knowledge of the security implications.
The "WaryWolf:GrowlTM" security rating software is only the first of the series of WaryWolf™ security software modules developed by Security and Standards Ltd. A range of packages is produced which bring the power of security to the general user. The next WaryWolf™ product will also enable users to securely record important web transactions. This "WaryWolf:BuyerTM" package provides

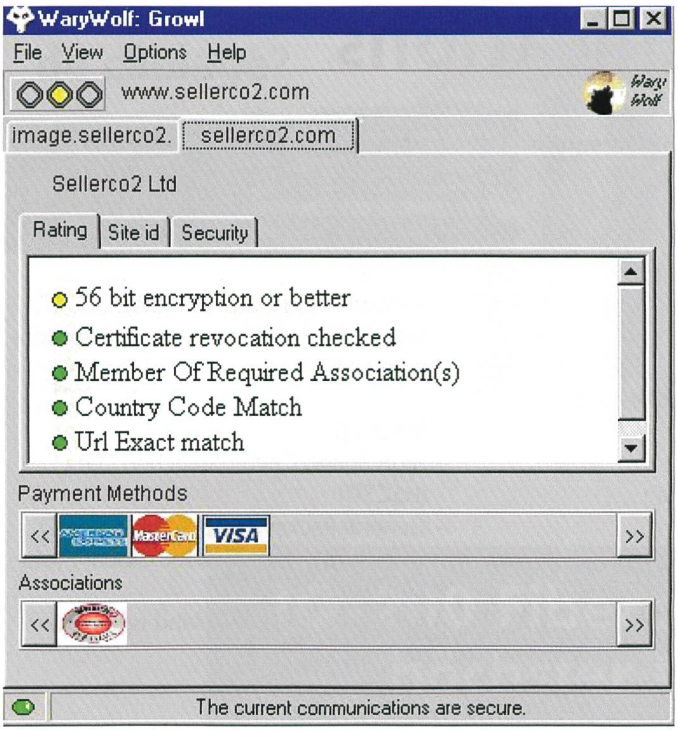

Figure 7. The WaryWolf™ display with Multiple Site Access.

vital evidence for e-commerce, using time-stamping to seal existing security data with application data as received and seen. As with other WaryWolf software, this package avoids the major overhead and expense of deploying an additional public key infrastructure by building on security mechanisms that are already widely employed. [4]

Nick Pope and John Ross, *Security & Standards Ltd., spoke on "Interfacing Security to Users" at ISSE 2001 – Information Security Solutions Europe – which has been held from 26-28 September 2001 at QEII Conference Centre, London.*

Zusammenfassung

Die Bedeutung der Beurteilung von Sicherheit

Wie die Sicherheit anderer Techniken wird auch die IT-Sicherheit immer komplexer. Oft stellt sich der Nutzer Fragen, die nur ein IT-Sicherheitsexperte beantworten kann. Doch wenn er die Wirksamkeit der Sicherheitsmassnahmen vor Ort nicht zu beurteilen vermag, kann er auch kein Vertrauen zum Web und den anderen Anwendungen fassen, und damit schöpft er dessen Möglichkeiten nicht aus. Er weiss nicht recht, was er tun soll, ob seine Bedenken berechtigt sind oder ob er sie fallenlassen kann. Dieser Artikel macht den Leser mit einem vollkommen neuen Ansatz, wie der Nutzer die Frage nach der Sicherheit angehen kann, bekannt. Er erfährt, wie man die einzelnen Sicherheitsaspekte so zur Deckung bringt, dass der Nutzer die Sicherheitsrisiken einschätzen kann, ohne ein Sicherheitsexperte zu sein.

Peter Pernards

Digitaltechnik 1
Grundlagen, Entwurf, Schaltungen. Hüthig Verlag, Heidelberg, 4. erweiterte Auflage, 2001. 256 S., kart., Fr. 70.50, DM 78.–, öS 569.–, ISBN 3-7785-2815-7.

Die Digitaltechnik hat sich in den letzten Jahren zu einer der wichtigsten Grundlagen der Elektronik entwickelt. Dementsprechend nimmt sie in der fachlichen Aus- und Fortbildung einen breiten Raum ein. Der Hüthig Verlag bietet mit den beiden Bänden Digitaltechnik 1 und 2 von Peter Pernards eine gründliche und umfassende Einführung in das gesamte Gebiet der Digitaltechnik und ihrer Anwendungsmöglichkeiten. Band 1 liegt nun in einer neu bearbeiteten und erweiterten Auflage vor. Das Buch wurde über die notwendigen Aktualisierungen hinaus um das wichtige Themenfeld des Rechner gestützten Entwurfs von Digitalschaltungen ergänzt. Erläutert wird auch die Hardwarebeschreibungssprache VHDL, die Lösungen standardisiert und damit vor allem komplexere Problemstellungen wesentlich effizienter und übersichtlicher in Programmierdaten umsetzt. Der Band behandelt Grundlagen, Funktionseinheiten und Logikbausteine der Digitaltechnik detailliert mit Hilfe von Beispielen, Grafiken und Übungsaufgaben.

Andreas Meier (Hrsg.)

Internet & Electronic Business
Herausforderung an das Management. Orell Füssli Verlag, Zürich, 2001. 304 S., geb., Fr./DM 49.–, öS 358.–, ISBN 3-280-02654-7.

Electronic Business ist eine der wichtigsten Innovationen der letzten Jahre. Das Internet kann für die Arbeit von grossen und kleinen Unternehmen völlig neue Perspektiven eröffnen. Anerkannte Fachleute äussern sich zum ganzen Spektrum der neuen Möglichkeiten: von den rechtlichen und organisatorischen Rahmenbedingungen über das Sicherheitsmanagement, die Waren- und Beschaffungsorganisation, die Auswirkungen für den Finanz- und Versicherungssektor, das Online-Marketing bis hin zu den Chancen, die das Internet für die Entwicklung der Gesellschaft eröffnet.

Mobile Data Communications

Modulares, interaktives Tagesseminar für Gruppen bis vierzehn Personen in deutscher Sprache:
- Technologien, Funktionen und Anwendungen
- GSM-Intro, GSM 2.5G (HSCSD, GPRS, EDGE) und UMTS
- WAP – Was ist das? Was macht man damit? Wer braucht WAP?
- Datendienste und WAP-Dienste, WAP-Portale
- Kundennutzen (Argumentarium)

Trainer:	Rüdiger Sellin, Dipl.-Ing., langjährige Beratungs- und Trainingserfahrung
Anfragen an:	E-Mail: ruediger.sellin@swisscom.com
Kurskosten:	nach Absprache, Preis pro Person und Kurstag (inkl. Unterlagen)
Termine:	auf Anfrage
Weitere Kursthemen:	xDSL, VoIP, High-Speed WANs

Ausgangslage
Die mobile Kommunikation boomt weiter. Weltweit gibt es heute über 350 Millionen Mobilkommunikationskunden, davon allein in Europa über 230 Mio. Experten rechnen damit, dass es anfangs 2002 weltweit eine halbe Milliarde sein werden. Noch vor Ende 2005 wird die Zahl der Mobiltelefonanschlüsse jene der Festnetzanschlüsse (heute rund 600 Mio.) bei weitem überflügelt haben. Ausserdem wird erwartet, dass danach mehr Kunden das Internet über mobile Endgeräte nutzen werden als über den Festnetzanschluss. Wegen der nahen Marktsättigung zeichnet sich ab, dass mobile Sprachdienste umsatzmässig an Bedeutung verlieren. Das Augenmerk der Netzbetreiber richtet sich auf neue Einnahmequellen rund um die mobile Datenkommunikation. Dazu gehört das Umfeld der Mehrwertdienste (Value Added Services), die von den so genannten Mobility-Portalen abgedeckt wird. Hier setzt das Seminar «Mobile Data Communications (Overview)» mit zahlreichen und interessanten Informationen an.

Zielsetzung
Das Seminar zeigt, wo die Entwicklung des mobilen Internets heute steht, was sich hinter den zahlreichen Abkürzungen verbirgt, wie die Netze auf diese Entwicklung vorbereitet werden und welche Dienste heute angeboten werden bzw. welche zu erwarten sind. Neben einfach dargelegter Technik wird Grundwissen über Funktionen der Netze und der Anwendungen der mobilen Nutzung der Datenkommunikation und des Internets vermittelt. Der Teilnehmer lernt dabei mit den richtigen Argumenten auf den Kunden zuzugehen und den Nutzen für den Kunden aufzeigen zu können. Ein Konkurrenzvergleich zu Mobility Portalen rundet das Seminar ab.

Kursinhalt
Networks
- Telecom- und Datacomnetze
- Mobilkommunikationsnetze, insbesondere GSM

GSM 2.5G
- High Speed Circuit Switched Data (HSCSD)
- General Packet Radio Service (GPRS)
- Enhanced Data Rates for Global Evolution (EDGE)
- Angebote in Deutschland und in der Schweiz

Mobile Services
- Wireless Application Protocol (WAP)
- Technik und Anwendungen
- WAP = Mobiles Internet?
- Formate: HTML, WML, XML
- Vergleich der wichtigsten Mobility-Portale

Endgeräte
- Einige Highlights der führenden Hersteller
- Weitere Entwicklungen

Mobile 3rd Generation
- Universal Mobile Telecommunications System (UMTS)
- Unterschiede zu GSM
- Neue Dienste: UMTS als Service Enabler

Bluetooth-Alternative zu Handynetzen

Der koreanische Spezialist für Internet-Telefonie, Clipcomm bringt mit seiner Bluetooth-Zugangslösung eine billige Alternative zu Mobilfunknetzen auf den Markt. Der BlueStation-Accesspoint bietet nicht nur einen Zugang zum Internet, sondern unterstützt auch Voice over IP. Damit kann der Benutzer mit seinem Blue-tooth-fähigen Handy oder PDA über das Internet telefonieren, selbst wenn das Gerät nicht für Internet-Telefonie vorbereitet ist. Die BlueStation erkennt selbstständig alle Bluetooth-Geräte im Sendebereich und stellt nach Angaben von Clipcomm eine sichere Verbindung her. Ein integrierter Netzserver sorgt für die Verbindung ins Internet. Der Internet-Zugang erfolgt über eine 10-Base-T-Ethernet-Schnittstelle. Die BlueStation ist zu verschiedenen Protokollen wie TCP/IP, PPP oder DHCP kompatibel. Für Voice over IP werden die Sprachsignale von einem eigenen Digital Signal Processor in der Station codiert und decodiert. Die maximale Reichweite der BlueStation beträgt in Gebäuden 20 m und im Freien bis zu 100 m. Verlässt der Benutzer den Sendebereich der Basisstation, bricht allerdings der Kontakt ab. Ein Überwechseln zwischen verschiedenen Basisstationen wie bei Handynetzen ist nicht möglich. Nach Ansicht von Clipcomm kann die BlueStation nicht nur für Kommunikationsanwendungen, sondern auch für den Kartenverkauf, Hotel-Check-in oder für Zahlungszwecke eingesetzt werden.

Homepage: www.clipcomm.co.kr