Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2008 Proceedings

European Conference on Information Systems (ECIS)

2008

Providing Spontaneous WLAN Guest Access as a Mobile Value Added Service

Stefan Stein
Institute for IS Research, University of Koblenz-Landau, stein@uni-koblenz.de

J. Felix Hampe
Institute for IS Research University of Koblenz-Landau, hampe@uni-koblenz.de

Providing Spontaneous WLAN Guest Access as a Mobile Value Added Service

Stefan Stein and J. Felix Hampe
University of Koblenz-Landau, Institute for IS Research,
56070 Koblenz, Germany
{stein, hampe}@uni-koblenz.de
WWW home page:
http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGHampe

Abstract. In this paper we describe the design and realization of a system that allows guests to connect to a company's internet-access channel via wireless local area network (WLAN). The core of the corporate infrastructure stays protected against unauthorized access. Although a growing number of companies provide WLAN access for their employees, guest access is rarely granted due to security concerns and substantial maintenance hurdles. Even if a network administrator might be willing to provide such access, it often would be done manually with substantial time delay. The solution we propose to solve this problem and to simplify the whole procedure is based on establishing a chain of trust. An authorized corporate user assumes the role of a host who invites and trusts his guests, thus he issues access codes together with the invitations. The system we propose is composed of two scenarios. The first scenario is called the „consultant scenario" and uses a Spontaneous WLAN Guest Access Server (SpoGA Server). In the second scenario, the so called „congress scenario", we describe how to support a great number of guests. Here we propose an „Extended Invitation Management System" (E–IMS) for ease of use. This system can help organizers of events not only to provide participants with wireless network access but also to support other related tasks in the preparation of larger events. The current results as described in the paper pave the way for field testing and broad enrollment. In addition some considerations on further developments are provided.

1. Introduction

In recent years, internet access has become a necessity for most people around the globe. Many companies provide a high speed network infrastructure for their employees and, increasingly, corporate-wide wireless network access for convenience and flexibility. External business partners, consultants or visitors often

need an internet connection as well. But as they belong to a different company, they frequently face the difficulty of easily and rather spontaneously gaining access to an existing network on the corporate campus they are visiting. The company's wireless network is normally protected from unauthorized use and therefore they would need special permission to gain access. Due to security policies it is common that such permissions can only be granted by the company's central network administration, which in many cases causes a lengthy administrative procedure. Sometimes applications might even be rejected because of remaining security concerns; and it is extra work for the administrators to follow that up and revoke permissions later. Clearly, if access would be granted without safety measures, there would be a security hole in the corporate network In general one might summarize that most administrators do not like to have guest accounts running on their networks. On the other hand, any public WLAN hotspot has mechanisms to provide guest access (e.g. any carrier-based WIFI-hotspot at airports or hotels). These networks, however, are totally separated from the corporate network, only available around dedicated locations and often are expensive to use. This last argument holds especially true for mobile internet connections via 2.5G or 3G.
The basic concept of the SpoGA project described in this paper is to combine existing security technologies used in WLAN hotspots with additional security precautions in order to realize a secure WLAN guest access via a company's network. This article first discusses a system that allows a host to give a guest a temporary wireless access to the part of the company's network providing internet connectivity. The central administrator still has the opportunity of controlling all activities but he does not have to manage any of these guests accounts. One of the additional advantages of this approach is that a guest receives only a time-limited access to a wireless network for which the inviting host is responsible in all ways (cost coverage, time-limit and revocation, point of contact in case of misuse). With the SpoGA (Spontaneous WLAN Guest Access) system a host can handle a small number of visitors. This scenario is therefore called the „consultant scenario". For larger groups, e.g. conferences, we extended the system by integrating the similar approach into an extended invitation management system (E-IMS).

2. Research Methodology

The research approach we follow is known as design research. Beside many others Takeda et al. [1] have analyzed the reasoning of the general design cycle (q.v. [2] and [3] for a synopsis - illustrated in Figure 1).

There are four stages:

- Awareness of Problem
- Suggestion
- Development
- Evaluation

Some of the stages are frequently performed iteratively, and we go back in the design circle when we notice that we could use our artifact for a greater scenario, too. Practical tests are still being carried out. Since development and evaluation are not finished, we regard our work as research in progress

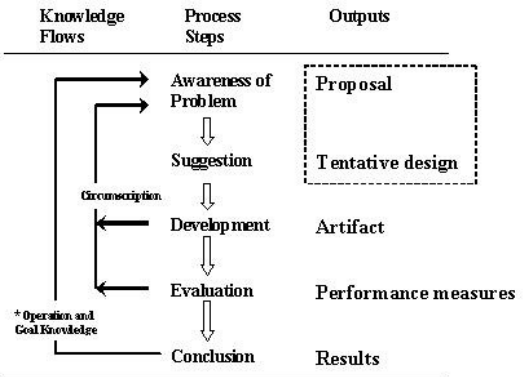

Figure 1 - "The design cycle and derived research methodology of Design Research" (taken from [2])

3. Design of the SpoGA-System

We developed the SpoGA Service (Spontaneous Guest Access) as a value-added service that provides wireless network access for any visitors not regularly connected to an available network infrastructure. The demand for such instantaneous or short time internet connectivity occurs very often in daily business, governmental and academic environments.
There are obviously some important criteria (these are the suggestions of the design research approach – see Figure 1) to fulfill:

- The security level from the corporate perspective has to be as high as that of administrator-controlled network access. The wireless network has to be protected from unauthorized access. The access to the internet should be limited in time. Thus, after a pre-defined time interval guest access codes expire.

- The guests have no direct connection to the company's critical infrastructure (their connections are bypassed through the demilitarized zone (DMZ). This can be done by pre-configuring dedicated VPN-tunnels, which connect SpoGA-Servers to an edge-router in the DMZ.)

- Guests do not need any special knowledge about network configuration and client-setup in order to use the SpoGA service. The SpoGA server

configures all parameters autonomously. It is not necessary to install additional software. The system works with all current devices and operating systems. (Nonetheless common measures of client-security as demanded in most corporate environments should be activated).

- Any user of the system must be identifiable by relating him/her to the host who initiated the invitation process. Thus the host is responsible for guest identification and trust relationship, cost coverage, etc.

- An invitation including an access code is sent to the personalized mobile device of a guest by using regular GSM mobile phone connectivity. (Here we could equally well allow for other communication channels, such as instant messaging (IM) or VoIP speech-messaging via GSM/UMTS).

Minor extensions to the common infrastructure of an existing corporate network are needed to realize this service. The SpoGA server running the service can be regarded as a special router (see Figure 2) with some additional functionality. It is connected to the wireless network and the internet by using two interfaces.

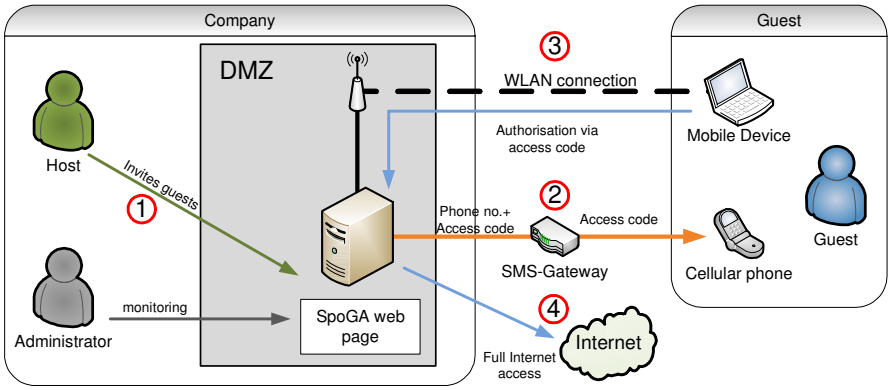

Figure 2 – The basic structure of the SpoGA-System

From the internal or external network the host (being a registered, fully authorized user) may access a different web-page allowing to setup SpoGA accounts (see ①). For any such account the system will send out the access code to the invitee (see ②) including basic explanations if necessary. By using the WLAN interface (see ③ in Figure 2) any WLAN-adapter of a guest device may connect to the SpoGA server, getting access to a web-page. For the latter communication either the Internet-gateway of the corporate network as essential component within the demilitarized zone (DMZ) is used (see ④) or dedicated channels are provided. In the case of sending out SpoGA codes by SMS, either a web-based SMS-gateway or an GSM-interface could be used. In principal the SpoGA server could be linked to the internet-gateway in the DMZ by a dedicated, secured connection based on either LAN or WLAN. In the case of a WLAN connection to another router within the

DMZ one would use a Wireless Distribution System (WDS) pre-configured link, as it is provided by most WLAN-routers today.
The integral part of the SpoGA server is the web server. It provides the GUI for all users (hosts, guests and administrator). The central network administrator can configure a list of people who are authorized to act as host. He can also check the status of the system and monitor guest activities.

In case a host wants to issue a SpoGA invitation, he will have to enter the for any guest the name, their cellular phone numbers and the permission period via the administrator web-page. The guests will receive their access codes via SMS with minimal delay. This procedure allows for spontaneously occurring demand, under certain assumptions (the host could be pre-registered for the service) even outside of office hours. We assume that a cellular phone is a personal private device that is only used by its owner. We effectively use the infrastructure of the cellular network as an overlay channel to transmit instantaneously the access code for the SpoGA server. Most mobile networks have the advantage that the transmission is encrypted, so the notification messages (SMS) may be used for such security relevant actions (this needs to be considered when using other channels such as IM- or VoIP messages, too).
Running a hosted SpoGA server and distributing security relevant messages may be regarded as a new mobile value-added service for either mobile network providers or traditional ISPs. In this case all WLAN access points at the corporate premises would have to be connected via a VPN link from the service provider.

It is clear that common media such as e-mail may be less appropriate for the distribution of access codes, since guests may print them out, lose or forget them and hence a third party may misuse the code (especially more likely if sent long in advance).

It is possible to invite many people in a short time using simple SMS. Guests get their access codes just before the meeting is scheduled. The cost such service including the message transmission is nearly negligible.

The SpoGA server needs some information about the user in order to provide authorized access to the WLAN-infrastructure. In our approach we assume that the users (guests, hosts) do not have special knowledge about computers and networks. So we implemented the system to detect the required information automatically.
This requires that the WIFI-mode of the guest device is switched on and the auto-connect mode is configured. But as the WLAN-interface of the SpoGA interface does not use encryption like WEP or WPA, no further system configuration or key-phrases are needed. All we request from the user is to open any web-browser which allows him to access the web page of the SpoGA system which pops up automatically. The user then enters the valid access code in order to get authorized access. The SpoGA system checks this code and any restrictions on the usage time. A positive check leads to immediate internet access after some firewall settings on the SpoGA system have been configured in the background. The IP- and MAC-

address of the guest's device are stored. The firewall rules granting the guest access will be revoked after the SpoGA code has expired.

With this SpoGA service it is very easy to enlarge the corporate network to enable guest access. Many users might know this type of configuration already from the typical carrier-based WLAN-hotspot services available in hotels, airports or other public places. But using those instead –if coverage is available– would be much more expensive.

4. Summary of Security Considerations for the SpoGA-System

The following security mechanisms and rules should be integrated in order to achieve a high level of security for all parties involved [4]:

- Communication via air interface of the wireless network is not encrypted and thus unsafe. This is only for convenience of setting up a connection. Guests are therefore informed that they should not use any services that need passwords and should not transfer security relevant information over this unencrypted air interface. The SpoGA system advises the guest to use an encrypted connection (e.g. VPN, IMAPS) from the moment they log in. This is in fact general knowledge and not in any way specific for the SpoGA-service.

- The wireless network is separated from the critical corporate network, because the radio interface of the wireless network is not encrypted. To access the critical business infrastructure the user need to connect via a VPN gateway, which implies that he is a fully authorized, registered corporate network user. In this case the traffic is protected.

- The administration of any guest access is conducted by the host. As the corporate network administrators still control the SpoGA server, they can monitor and detect problems and directly address the responsible hosts or any guests connected (e.g. for emergency shut down).

- The guest's permissions to access the internet are determined by a firewall rule. Only systems initiating a valid code can send data from the guest network to the demilitarized zone of the corporate network and get access to the internet in this way. These codes are short-time tokens.

- Guests cannot connect several mobile devices to the network at the same time. They have to log out via the SpoGA web page if they want to change a device, but can then use the access code again until the time period expires. If someone uses the logout function, or in case the period of access has expired, the SpoGA system changes the firewall settings. Only the web

page of the SpoGA system is now available. The connection to the internet is blocked. Guests may then request a new access code.

- If a guest stays for several days he does not get one access code for the whole period of time. The code is only valid for a maximum of one working day at a time. We introduced this restriction to avoid any overhead in case of lost or stolen devices. In principle, the maximum validity time interval for access codes can be globally set by the SpoGA system administrator.

5. Software Base of the SpoGA-System

The SpoGA server is a transportable "black-box" system with at least two network interfaces. It is possible to integrate this system quickly and easily into every existing network infrastructure (LAN or WLAN).
Integrating the SpoGA service features into any common business router is a future option. By doing so, a SpoGA service would be yet another selectable mode of operation.
The realisation can be done following a truly cost saving approach. In our prototype the SpoGA system uses open source components like the command iptables for the firewall and MySQL as database. As most stand-alone hardware routers use Linux as the operating system, so does our prototype. Any integration of a SpoGA server is simple and straightforward.
Presently we are porting our software to a small, inexpensive stand-alone embedded machine, resulting in a portable SpoGA server system that could be quickly setup at special events. This device has the size of a book, allowing for some degree of mobility [4].
The prototype has an SMS gateway called sms77.de [5] which has a web service interface to send short messages to cellular phones. So it is not necessary to set up an extra expensive SMS gateway to send the access codes to the guests.

6. The Invitation Management System Extension

The SpoGA server permits a host to grant WLAN-access to a limited number of visitors. In case there are many participants at a meeting (e.g. conferences), the procedure needs to be automated. We call this scenario the "congress scenario".
Here the SpoGA server is extended by adding a web service interface as well as other functionalities. In order to allow a single host to invite a large number of guests, an invitation management system was implemented as an additional system that uses this web service interface of the SpoGA server.

We called this system E-IMS (Extended Invitation Management System). [6]

The functionality is separated from the SpoGA server because most companies run only a small number of larger conferences, but many may never need such a service. The operating expenses of running an E-IMS server would be too high, the resulting system overloaded with features. Thus, we regard this type of conference management primarily as a field of activity for dedicated service providers. Any E-IMS service provider could than charge fees for the whole event or only for the period of usage. An internal E-IMS only makes sense if the company will run a sufficient number of events with many participants under their own conference management. The integration of the SpoGA and E-IMS servers is show in Figure 3.

The E-IMS administrator needs to be part of the extended trust-chain approach when using E-IMS & SpoGA. He thus could be either a service provider's employee or the company's administrator if the company runs its own E-IMS server.
After the installation of the E-IMS server, the E-IMS administrator creates accounts for the company's conference managers. He also enters the basic configuration which enables E-IMS to connect to the SpoGA server. He or the conference managers define all resources a guest could order (packages). This generic information needs to be entered only once.

From then on the host (any authorized conference manager) can initiate new events. To invite guests he needs the guests' names and e-mail addresses. These could be imported from any conference admin-software or PIM (e.g. Microsoft Outlook). Based on this data the E-IMS sends out emails to the invitees. The invitation contains a link to E-IMS web pages. Guests may use them to access the E-IMS server via the internet. They may log in and if they do not have an account they create one. Furthermore they are asked to enter all necessary information for the use of E-IMS and the SpoGA system in relation to the specific conference. If any data entity is missing, the E-IMS system could acquire it (e.g. a cellular phone number) at a guest's next login. For each registered guest the SpoGA service could then be ticked in his profile, specifying prices and time frames for usage.
The E-IMS service can provide many more service components. Registered users could get information about any event in the past as well as upcoming ones, or receive slides used for presentations. Speakers could book resources like rooms or special equipment for the current event they are involved [7].

The SpoGA service will start up shortly before the event based on automated scheduling schemes. Any usage data are logged and reported to the E-IMS server (this information is primarily needed for billing purposes).

With the E-IMS it should be possible to check how many guests will attend the meeting. So an organizer can estimate the appropriate number of rooms and consider their sizes but also extend the number of WLAN access points connected to the SpoGA server.

To realize a prototype of such E-IMS we decided to use an open groupware system with a modular assembly. We used eGroupware [8] for this project, but activated only those modules needed: calendar, user management and resource management.

We implemented some additional modules for the communication to the SpoGA server, called the SpoGA manager. This induced the need for modification of some of the existing modules found in eGroupware [7].

We regard the resulting E-IMS system to be user-friendly and clearly very cost-effective.

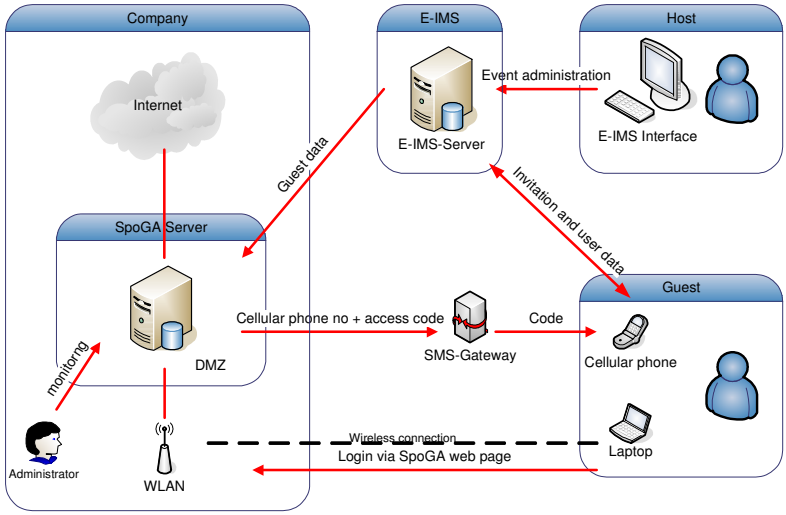

Figure 3 – Integration of SpoGA and E-IMS

7. Related Work

Some partially related work and products exist already in the literature and on the market, which consider internet guest access provision. But these approaches do lack the flexibility of the approach presented here. Obviously, the easiest way to provide an internet guest access would be by using a special router with a connection to a separated network. This approach is used by the special routers of Linksys [9] or Lancom [10]. These Routers are using an UMTS connection to the internet. Depending on the number of guests connected simultaneously this connection could be easily too slow. Another disadvantage could be insufficient UMTS coverage. This occurs frequently as a problem in some parts of a building or in rural areas and smaller cities. Depending on the pricing plan this connection type could also be comparably expensive.

Another approach is to integrate the functionalities into a corporate network [11]. This gives the guest a corporate wide access to the granted functionalities of the infrastructure. The disadvantage is that the guest must have direct access to an

existing network connection via cable or wireless LAN. Our SpoGA-E-IMS prototype has the advantage that it contains a wireless access point for the guest connections. So it gives the host also a special flexibility. The most significant feature is the possibility to host an event with a larget number of guests, too. The infrastructure of the SpoGA-E-IMS system supports the hosts to provide a guest access and to manage and bill the used services. It does so likewise for rooms and technical equipment.

8. Evaluation and Outlook

With the combination of E-IMS and SpoGA, it is possible to provide internet guest access via wireless networks for a small number of guests as well as for large groups in a cost-saving way for organizations of all types and sizes.

E-IMS offers the host many more possibilities than just the automation of different tasks, booking resources and invoicing. E-IMS can be used as a portal for a number of different events that could be arranged by different hosts. It even provides documentation repositories of current and past events.

Real life tests of the combined system setup of E-IMS and SpoGA have not yet been performed. But we evaluated this setup at the present stage of development under laboratory conditions. The prototype of the „consultant scenario“ running the SpoGA service only was tested first. This pre-test indicated high stability, ease of use and performance. Thus we considered it as overall successful. As a next step we combined the E-IMS and SpoGA services to allow for pre-testing the „congress scenario“. As “participants” we involved a larger number of students” who reported about their experiences. In summary, the combined prototype worked well, too. But because of the modifications and extensions added to eGroupware, some functions were difficult to find for the users. This caused a refinement cycle leading to an improvement and modification of the prototype. It is now due to conduct a field test of the system, which is planed for Q1/2008, as we are organizing an academic conference

As an interesting side-effect of the design cycle we received feedback from current users who suggested even different application scenarios and business models for the SpoGA service, ranging from customer self registration models to private neighborhood (“citizen”) networks. In separate research studies we now have to conceptualize, realize and evaluate these approaches in detail.

9. References

[1] H. Takeda, P. Veerkamp, T. Tomiyama, and H. Yoshikawam, "Modeling Design Processe," *AI Magazine,* vol. Winter, pp. 37-48, 1990.

[2] V. Vaishnavi and B. Kuechler, "Design Research in Information Systems," (March 27, 2007) ; http://www.isworld.org/Researchdesign/drisISworld.htm

[3] S. Purao, "Design Research in the Technology of Information Systems: Truth or Dare," 2002.

[4] M. Ehrenstein, "Spontaneous (WLAN) Guest Access ": Universität Koblenz-Landau, 2007.

[5] "SMS 77," (April 6, 2007) ; http://www.sms77.de

[6] M. Müller, "Spontaneous Guest Access (SpoGA) & Extended Invitation Management System (E-IMS) - Module "Veranstaltungsverwaltung" & "Abrechnung" ": Universität Koblenz-Landau, 2007.

[7] C. Speich, "Spontaneous Guest Access (SpoGA) & Extended Invitation Management System (E-IMS) - Modul SpoGA Manager und Erweiterung der Ressourcenverwaltung," Universität Koblenz-Landau, 2007.

[8] "eGroupware," (April 6, 2007) ; http://www.egroupware.org.

[9] Linksys, "WRT54G3G - Wireless-G Router for 3G/UMTS Broadband." (March 10, 2008) ; http://www.linksys.com

[10] News & Nachrichten, "Lancom 3850 UMTS: WLAN-UMTS-Route." (March 10, 2008) ; http:/www.lancom-systems.de /

[11] idEngines, "Secure Network Access for Contractors, Business Partners and Guests," (March 10, 2008) ; http://www.idengines.com/downloads/ IDE_Contractor_Guest_Access_wp.pdf