Telenor mobil – security case study essay sample

1. Introduction

Telenor Mobil is currently deploying Public Wireless Internet Zones. Telenor Mobil is one of the two largest Mobile providers in Norway. The company is represented in Eastern Europe and Asia, but this installation is so far a test for Norway.

Telenor Mobile is represented in the countries marked in red.

Telenor Mobile is part of Telenor that had a monopoly on the fixed telephone network in Norway until 2000. It is now possible for any company to compete on the Norwegian market. The mobile telephone market has been open for competition from the beginning, but the years of monopoly that Telenor had gives Telenor Mobile a lot of resources that their competitors do not have. All mobile telephone providers must cover entire Norway to be able to get licensed.

In 2002 Telenor Mobile worked expensively to make it possible to pay using your mobile telephone. You can now pay for services like parking you car, log on to the internet, use your phone as your wallet, integrated to you debit, credit card and SmartCash.

This makes it possible for any user with a WLan (Wireless local area network) card to log on to the internet. The intention is to offer Wireless access to existing and non existing customers. Wireless zones have been installed in public places and companies that want to provide that service for visitors or their own company

The purpose of the Public Wireless Internet Zones is that someone comes to a place covered by the IP zones and starts the browser and can then browse web pages the provider makes available. This can be the local shop, part of the intranet and so on. If the person tries to browse outside the intended web pages available, a start page will bee pushed on the browser and that home page can have links to more free pages or just a logon page.

If the user then wants to log in, they fill in their telephone number which is then sent to the radius server. The radius generates a password and sends a SMS to the user mobile telephone. The user fills in the password given and can start browsing the internet.

The charge for browsing is invoiced on the user’s mobile telephone bill. In certain cases companies are using this as identification and not to make revenue.

As the IP address has to be issued to all possible users, hackers could take advantage of this. Therefore, system security has been an issue that is needed to be addressed.

The solution proposed is “ a world-class wireless access solution” based on world-leading products and services from mentioned partners. The joint efforts of the leading expertise team, enables Telenor Mobile to extend its market leading position also into the Wireless LAN market place, and in turn to provide a strong combined service offering based on GSM/GPRS and WLAN access technologies.

The IP Zone will provide internet access, and use of payable and non payable services as shown in the picture.

1. 1. The Partners

This system design represents a joint effort between Birdstep Technology, Hewlett Packard and Cisco Systems, headed and lead by Eterra as the system integrator.

The solution proposed is “ a world-class wireless access solution” based on world-leading products and services from mentioned partners. The joint efforts of our leading expertise team, enables Telenor Mobile to extend its market leading position also into the Wireless LAN market place, and in turn to provide a strong combined service offering based on GSM/GPRS and WLAN access technologies.

The solution is based on solutions from our “ best-of-breed” products and solutions. The following criteria’s has been our guidance and priorities for the proposed solution:

* Open standards

* Scalability

* Flexibility

* Simplicity

* Security

* Ease of management

* Turnkey solution

Taking the best from all team members, Telenor Mobile will achieve great business benefit in providing secure and cost effective services to the Telenor Mobile wireless LAN customers. The partners of this proposal represent the following value-add to Telenor Mobile:

Eterra

* Broad and widely experienced in delivering complex roll-outs as a value add system integrator in the Nordic market scene

* Benefiting from long term relationship with Telenor

* Covers Norway and the Nordic region with 2200 skilled and dedicated employees

Birdstep Technology

* Development strategy in Birdstep aligned with Telenor Mobile wireless access strategies

* Birdstep Wireless Access solution features a “ Close to 100% compliant” Access Control Device solution for Telenor Mobile

* A solution extendable, through Birdstep Mobile IP client software, to deploy roaming services between various access technologies such as Wireless LAN, GSM/GPRS, ADSL, Bluetooth and IrDA.

Cisco Systems

* Market leader communication product portfolio

* A non-debatable competence-profile

* Enjoys a substantial and comprehensive legacy of exciting Cisco-base within Telenor since `94

Hewlett Packard

* Market leader ICT-product portfolio

* Industry-leading performance with multi-technology based on scalability, availability and manageability

* HP OpenView is key for this case’s operation and maintenance solution

1. 2. Aim of report

In this report the main focus will be on security issues within areas of the project

1. 3. Limitations

We will not have the possibility to go through all details of the project as we have been limited by the maximum word count for this assignment.

2. The big picture

To give an overview of the complexity of the system, we have illustrated the installation as it looks with the DMZ (demilitarized zone). There is one firewall Titanic1 standing in front of this zone and one in the back Titanic2 stopping all communication coming from outside Titanic1. It is thought

impossible to get any communication from the outside and into the network without a server expecting and processing the data.

This is in correlation with the theory given in this course; Turban Page 567, the reason why a DMZ is used, ‘ the idea behind the screened subnet is that there is no way for outside traffic to gain access to any other hosts on the internal network’

The servers and program used for the IP zone configuration is from Birdstep run on Linux servers.

2. 1. The ACD

This is the first server giving the functionality.

When the user wants to access the internet he will have to go through the ACD (Access Controlling Device). This is a Linux RedHat 7. 2 server.

* The purpose of this server

* Give IP addresses to the users

* Provide the users with the https:// page that they will be using to log on

* Block all communication that is not explicitly set up to bypass, this will be certain pages that the providers want the user to have access to.

* Open all communication when you have successfully logged on.

The access controlling function is integrated in the ACD, the IP zone Controller. This server, however, communicates with the Back end IP zone

server. The Back end IP zone server takes care of interface to Telenor Mobil RADIUS server, and stores information about prepaid subscribers. Prepaid is handled either through Telenor Mobil RADIUS server, or by the Scratch Card/Voucher generator function in the Back end IP zone server.

The IP zone Billing Gateway is responsible for interface to SMS Billing (CPA, CIMD or UCP), Credit Card billing (through Credit Card broker), and future payment options such as SmartPay.

The access controlling functions is divided between the IP zone controller, the Back End IP zone server and the IP zone Billing Gateway, and the Nomadic Portal can also be used for the access control function by generating the login pages. The IP zone Controller constitutes the firewall and generates accounting information. SSL-based login page is generated from the IP zone Nomadic Portal.

For password based login, the login request is directed from the IP zone Back end server to the Telenor Mobile Radius server – A RADIUS request is issued towards Telenor Mobil Radius Server (Funk), and if the login is authorized the IP zone Back end server will instruct the IP zone Controller (ACD) to open the firewall.

For Voucher/prepaid card. The operator may generate a username/password series using the IP zone Billing Gateway, print these on vouchers and sell them to subscribers. The subscribers use the username/password printed on the voucher to gain access for a specified time limit or volume of data. Alternatively, the prepaid login solution is realized using the Telenor Radius server. The latter is the chosen solution in the Telenor Mobile WLAN project.

The IP zone Billing Gateway authorizes the login according to one of the following authentication options:

* SMS login – The customer enters his/her GSM phone number in the logon page. The logon page is normally generated from the Nomadic Portal, but can also be generated from the IP zone server. The request is sent to the IP zone Billing Gateway, which identify which operator the subscriber use through a call to a third party GSM number catalogue service. After the correct operator is identified, an SMS message with a one-time password is sent to the GSM phone of the customer through CPA (Telenor) or CIMD (Netcom), or UCP (generic) depending on which operator owns the GSM subscriber. The customer enters the password received on SMS into the login page of the Internet Zone and is granted access for the time that the operator has specified in the IP zone Billing Gateway.

* Credit Card login. When the customer enters the Internet Zone, and start a web browser, the user may chose to purchase internet access for a specified time using his/her credit card. Credit Card details are inserted in the web page, and a request is sent to the IP zone Billing Gateway. After authorizing the Credit Card charge through a broker (we currently interface Visa Paynet, but other credit card brokers can easily be added to the IP zone Billing Gateway).

* SmartPay (Telenor Mobile) and Toll number charging is under development and may be offered as alternative billing options in the future.

This means it is not possible to communicate going through this server before it is told to let your session get through. When logging on to the

server the user has to access using a secure page https://. The user sends his phone number and gets a password for this session on SMS. When login on the user will get all privileges and for a company, this will mean giving him access to use VPN in to the inner part of the company’s data.

2. 2. The Nomadic Portal and XML

This is the second server giving that functionality. Run on RedHat Linux.

The work of the Nomadic portal is to find out what device size you have and what you can retrieve thereby translating what you want. The server is programmed so that there should not be any difference in service if you are using a Mobil telephone, PDA or lap top.

To do this, Birdstep has designed all requested internet pages to be translated into XML (Extensible Markup Language). This is a ‘ standardized way of representing structured data as text files’ and is being used for ‘ content intended for people, for content intended for computers, and as an underlying interchange format for communications’ (Treese and Stewart page 185/6). For people, XML supports screen calibration, which means that all pages given are reconfigured to fit the size of the client screen. This is important as a lot of portable devices have different screen sizes.

XML also support giving information on where the client is situated, this gives the possibility to be more exact giving information. In the future we hope to see more creative use of this. For example, if an IP Zone is installed in a shopping mall you can, by knowing what AP is the strongest, know where in the mall the client is, and therefore be able to provide “ local”

information on this spot. Knowing what direction the client is moving you can give information like, “ The next shop has a sale on shoes”.

2. 2. 1. Unique features

* Local Services

Birdstep IP zone Nomadic Portal supports two types of services; Automat Interaction and Information Services. Automat Interaction supports user interaction with local commodities such as printers, faxes, beverage automats, music jukeboxes etc. An automat is also a usable metaphor for on-line services, such as ticket ordering, menu selection/ordering, taxi orders etc. Information services support multiple views into a possibly large information space represented in the IP zone Nomadic Portal.

* Transcoding framework

The only requirement for using the Nomadic Portal is a device with a HTML browser. The IP Zone also requires SSL and cookie support in the browsers. Information from the Nomadic portal is transcoded to match the capabilities of the terminal. The nomadic portal development framework utilizes XSLT to ensure that the markup language sent to the wireless terminal takes account of the color and resolution capabilities of the platform. Currently, WML, simplified HTML, HTML and XML are supported. Cascading Style Sheets (CSS) are also used to ensure correct presentation where the terminal supports this.

* Personalization framework

The nomadic portal user may store preference information, indicating what kinds of information they prefer. Using this information and the tags in the XML documents, the Nomadic Portal personalizes content for delivery to the user terminal. This personalization functionality is provided in addition to any subscription- based personal information services offered by the IP zone server. User-specific information allows the nomadic portal to provide targeted and personalized IP zone information services, and the same portal can provide information to a large variety of nomadic users. The personalization and transcoding functionality is part of the same framework, thus providing resource-efficient information extraction and terminal adaptation in the same operation, combining the power of advanced XSLT operations, XML searches using XPATH and WML/HTML/XML, and CSS technologies.

3. Security

Addressing the security issue has been a major part of this project. Looking at all that can happen, and what resources the hackers are using, has been a concern.

Importantly the focus of the project is to provide internet for the users and not to interfere with what the user is using the internet for. This means as soon as the user has paid he will be open to the internet with no restriction. The user has to be responsible themselves making the workstation secure (firewall, VPN). The only restriction given in the IP Zone is that the customers can not use SNMP.

3. 1. Why security

Telenor has addressed the issue of security in many ways, which will be discussed further in the parts below. In this section, we will explain what security issues affect the internet in general and with wireless internet.

A survey carried out in 2000 by the Computer Security Institute and Federal Bureau of Investigation, based on the responses of 643 practitioners, showed the following:

* ‘ Cyber attacks are on the increase’

* ‘ Internet connections are increasingly a point of attack’

* The varieties of the attacks are on the rise’

(Turban, page 543)

Security breaches are costly for businesses and individuals. It is up to the service providers to ensure that their systems are as secure as possible against attack, however, this is a progressive issue that these companies need to address as the ‘ hackers’ and ‘ attackers’ are constantly training new ways to penetrate systems. Service providers’ reputations will be at stake if these companies have not taken enough measures to protect end users.

Telenor has ensured the following in their system set-up:

* Authentication and authorization for

o Users – through passwords being sent to the user’s mobile phone by means of SMS. However, in certain circumstances, the security issue can be

challenged and damaging for the ‘ real’ user. I. e. stolen mobile phones that have not yet been deactivated.

o And businesses, this being the use of Https secure pages with 128 bit private encryption.

* Integrity for access to the company’s private data

* Availability

We have not been able to determine whether or not Telenor has a risk management team/process for the security issues. It can be assumed that they do as the consequences of not addressing these issues on an ongoing basis would be detrimental.

3. 2. Assumptions taken

The assumption taken by Telenor Mobil is that if the phone is stolen, the owner will report this. Thereby deactivating the mobile telephone for all usage, including the net, but if the customer does not report the phone stolen or lost, then it could be possible that someone else will be using this mobile telephone to call or even browse the internet, but still serving the bill to the original owner. In this case, service providers will assume that nothing suspect is going on, as this mobile telephone is still operable.

The phone only gives internet access and no other access; it is not a certification logging on any services like mail or bank. It is therefore recommended that additional security is solved by using VPN (virtual private network) to get in to the company server park. A VPN ‘ uses the public

internet to carry information but remains private by using a combination of encryption to scramble the communications, authentication to ensure that the information has not been tampered with and comes from a legitimate source, and access control to verify the identity of anyone using the network'. (Turban, page 568).

3. 3. IP Zone Software and Server

The IP zone software provides firewall capabilities so that the network operator may allow only authenticated users to access network services.

The firewall provides security protection in the following areas:

* Protects wirelessly connected users from attacks from the Internet.

* Any installer-defined custom firewall rules. (Based on source address and/or destination address and/or port and/or protocol)

The IP zone server supports a very flexible firewall. Any client terminal or server can be opened by bypassing the normal authentication system. Using this feature, certain servers (such as external, public information servers) can be allowed anonymous access while general internet access is not opened. Thus, the user does not need to go through an authentication procedure to reach these servers. The white-list feature in the Birdstep IP zone server can also be used to allow seamless handover by means of Mobile IP so that the Mobile IP client can avoid specific authentication to reach Mobile IP home agents.

3. 4. Security step by step

Moving from the customer and in to the backbone, we have:

First, the AP (access point). Http (https) is turned on as a configuration tool but restricted to calls coming from the Ethernet interface. This will limit the access to this device from the IP zone. The Ethernet interface is attached to the ACD. SNMP is filtered so that this protocol can not be used in the zones at all.

All management using Telnet is turned off so the protocol is not accepted by the AP.

This means that to configure the AP you have to be able to browse the AP using Https from the ACD server.

Second ACD servers are set up to be controlled by using SSH and https. SNMP is used to monitor and send error messages. To limit the possibility to access the ACD, management can only be done from the GIPS (Physical network of Telenor).

In this way, Telenor have stopped the possibility of getting to the ACD from the IP Zone. All configuration of this server is managed from the back of the net.

The next step back is Cisco routers in Telenor’s backbone. These are set up to be passing on all information received and are not configurable from the internet. This is only part of the infrastructure and will not add any security.

The next step is a firewall called Titanic (UNIX server). For the purpose of this assignment, we will not discuss this in detail, as this could be a chapter by

itself. In general, it is stopping anything suspect as well as any communication not coming from defined servers. This server is the front end of the DMZ (Demilitarized zone) in Telenor Mobil.

By stopping all communication from the internet not coming from a defined device it will be hard to get to the servers on the inside of the DMZ.

Inside the DMZ we have the Nomadic Portal that is supplying the content to the ACD. This server is converting everything to XML making the content fit the screen of the appliance used such as computer, mobile telephones, PDA or other handheld devices.

It loads the internet page, reshapes it to fit the device, and sends it out to the client. Because of the excessive use of internet for this server it has its one leg on the firewall; this means that it is one physical line out that is configured different than the other physical lines.

If you look at a firewall as an octopus every physical line / cable is configured so that only defined communication can go from one to the other. This is the difference between a router and a firewall the router tries to send everything it receives to the next layer translating by rules. The firewall will try to stop everything it receives if not told other vice.

We will also have a billing server inside this DMZ monitoring how much the customer is using the system and thereby adding the cost to the telephone bill. The customer is billed from log in on to the last IP packed sent to the device. In this way Telenor Mobil dos not have to be confronted by customers that did not manage to log out.

You have the radius servers making up the password for the customer and confirming the password when it is used. It is important that this server only sends out the password back from the DMZ and out on the telephone network as an SMS. In this way, in order to hack the system for free use of internet, the hacker must attempt to hack the telephone network, which is much more work. The customer uses the password given by SMS in an Https secure page with 128 bit private encryption. The radius server accepts it and gives an OK to the other servers.

SNMP

This protocol is used for the gathering of all information from the server as well as some hardware configurations and is therefore a sensitive protocol. Therefore, you have one leg on the firewall where there is a SNMP proxy. This leg is configured with communication to the internet, it validated that the SNMP coming in or going out is valid and not some one trying to hack. This proxy server is communication to an other leg on the firewall that can not directly communicate with the internet. This makes it secure. The reason for not putting it back of firewall 2 is that this would make a possible hole inside the DMZ. It is now secured as much as possible, making it impossible to get through the DMZ using this protocol.

3. 5. Summing up security

Security has been a focus and it is made as impossible as known to stop hacker from hacking into the system. Communication that can change configuration in the system is efficiently stopped from the customer end. Configuration communication is only accepted if is sent from the server /

switch closer to the “ office” the next level. This makes it difficult for someone to be able to communicate with the servers at interest.

To hack the system the hacker will have to know the “ end of the line”. Hack into the network of Telenor Mobil and then move back to the access point to change the configuration of this switch.

The authentication provided by the Birdstep IP zone server is independent of WEP (Wired Equivalent Privacy) -based encryption for IEEE 802. 11b (the standard that specifies the WEP technique)-based Wireless Access Points. WEP may be enabled or disabled at the choice of the Network Operator. Normally, Telenor Mobile recommends disabling WEP for simplicity and relies on SSL (Secure Sockets Layer) to protect IP zone passwords. Business users should rely on VPN clients on their user terminals, or application-level encryption such as for example HTTPS, S/MIME or PGP to protect sensitive traffic.

4. The next step

Now that the IP Zones are in place the success of the installation will depend on what it can give the customer that the customer is willing to pay for? Some technologies are considered added in the near future.

The IP zones can use many forms of mobile technology. In this first step WLan is the one used. We have been looking at Bluetooth, the phone protocols, GSM, GPRS and 3G. All this technologies will be able to carry IP traffic to a PDA or PC making Internet available for the user and making the Nomadic portal a use full server.

4. 1. Mobil IP

To add on to the product line giving more value to the Zones it is considered include Mobile IP as a service the customer can subscribe to. Mobile IP is a technology that makes it possible to change platforms used and at the same time not lose the connection to your host. This is important if a VPN session is to be kept open while moving around, switching from a WLan to G3.

It has been possible for some time to move from one hot spot to another but to change the carrier completely moving from one IP Zone using the phone with GPRS and Blue Tooth going to a new IP Zone and never loosing connection.

Giving a constructed example on how this works:

You are working late, awaiting an important file that someone is intended to send to you. The file is 500mb. You take your PDA and you go to a nearby restaurant to eat. While on the way to the restaurant, you see that the file is being transmitted and you accept, but you have 40k bandwidth. Sitting down in the restaurant, there is an IP Zone and you log on the session changes to 10mb connection. After dinner, you go back it is still downloading but at 40k. At the office, you dock the PDA and download the rest at 34MB.

4. 2. Multi media

It is also possible to play video in the Zones. You could let companies make their commercials available make money if someone is looking at them, trailers for movies. Let people see a movie, paying for the movie one the

phone bill. This can be of interest for hotels, larger airports and other places where the customer might be saying for a longer time.

4. 3. Games

Combining Mobile IP with WLan will give way for a more continues play with the online games. We think that the future will give way for more of this type of games.

5. Conclusion

The system has been configured with as few holes as we have been able to. The security risk in this setup is for users losing there mobile telephone and not reporting it. It should be difficult to get through the system especially as all information is traveling one way and not both. The customer sends the request, the answer is coming back on a different media, and then the customer is sending his new request this time verifying that this is him and the server is opening up for traffic.

The billing system is interesting in this project as Telenor Mobile has integrated themselves to the bank systems. Debit and credit cards, as well as the new internet wallets give a lot of choices when invoicing the customer. For there one customer’s they can put it strait on the phone bill and for international travelers that do not have any of the Norwegian pay methods at hand they can ask the customer to pay with a card.

The system is in a start face and no revenue of importance is made yet. The problem now is to find places and services that can generate revenue in the future. The trend of WLan are relatively new but spreading fast, at the same

time the question is if it is spread out to the critical mass needed for this to be profitable, are the WLan customers willing to pay for using WLan when outside the office?

The expectations of the future and the services that will bee available on this system is wary much dependent on if Telenor Mobile is successful getting subscribers and at what age the subscribers will bee. There have been some research don showing business users but at the same time the young people of today have PDA’s and other devices that are made for using WLan. This can be giving way for revenue on multimedia and games.