Global Information Assurance Certification Paper

Biometrics
and their use as authentication mechanisms for remote access

Christian Nørager-Nielsen

GCFW Practical
Version 4.1

Date: Mar. 20, 05

Table of Contents

List of Figures

List of Tables

Assignment 1: Future State of Security Technology

Abstract

In the industry there is an ever growing need to be able to securely access internal network resources from somewhere on the internet: people working at home, regional or even international offices, partners and customers.
We already have the possibility to encrypt data travelling from one place to another over the internet. What is also needed is a mechanism with which it is possible to verify the identity of the person at the other end of the line. There is also a need to tell whether the user's environment is safe, i.e. can the user, the computer and the network be trusted?

I'll try to shed some light on the user part by looking into biometrics as a means for authentication of remote employees.

Background / introduction

Authentication is the act of verifying that an individual is who he claims to be. Today we're using usernames and passwords, but passwords are weak in that many people write them down, or forget them. Passwords may be captured by spyware or Trojan horses on an infected computer and they are 'easy' to guess. The ease of guessing depends on the password strength, which is up to the user to define.
This is mitigated by the use of security tokens and servers such as RSA's SecurID and Authentication Manager[1] thereby creating a two-factor user authentication system – something the users know and something they own. Of course the token can be lost or stolen, leaving the user without a means of login.

Another two-factor approach is biometrics, which is a way of authentication through something your body is or can do, rather than something you know (a password). It comes in all sorts of flavours - fingerprint, iris scan, hand geometry, face recognition, voice recognition, handwriting and typing dynamics - most of these have different variants.

All biometric authentications consist of a reference data set that will be compared to the measured data. This means, that a person will have to enrol before they can start using the biometry. The comparison will return a probability, that the users are who they claim to be. To make sure that a legal user is not denied access a certain error margin is allowed. If the margin is too big, there is a chance the system would allow another person. Often the expressions False Reject Rate (FRR) and False Accept Rate (FAR) are stated for a given system. Of course both values should be minimized, but as they are

interrelated, this is rather difficult.[2],[3],[4]

One problem with biometrics is that we cannot use it as the only means of authentication. Some users might not be in possession of the biometric trait we're using or might lose the trait (if only temporarily).
For instance: the ferries going from Copenhagen to Bornholm gave their customers the option of using fingerprint for paying the fares (like a credit card), but found that people working with ceramics did not have fingerprints that could be read (Bornholm has a big ceramics industry). The same thing could probably happen with other manual labours (gardening) that might wear off the fingerprints or change them. In fact 7% of their customers were unable to use the scanners for one reason or another.[5]

Another problem is the actual communication lines.
Data must be transferred from the biometric reader to the system authenticating the user.
Most devices are connected to a computer via USB or serial cable which might make it possible for someone to insert a device in series with it and thus be able to record the data stream, possibly even replaying it at will[6]. This of course requires physical access to the computer used, but I've heard that about 70% of authentication abuse comes from within the company. Then information about the authenticity must travel on the internet. Whether the data travelling are the actual biometric data or some kind of checksum value, they are prone to wire tapping.

How can we trust an external system? It is usually difficult enough to trust an internal system, but to trust an external system is something different. Is there really a biometric reader at the other end? Maybe a clever software program can mimic the behaviour of the reader? Are the communication channels between the reader and the computer safe (encrypted)? Can we be certain they have not been tampered with?

Is it possible to fake a biometric?
In general terms, yes. This is why the biometric industry is hard at work finding an aliveness detection that works. I'll discuss individual problems when I address each biometric method.

Problem Domain

So why has biometry not become the standard for authentication long ago? There are several reasons for this. The methods may be well suited within a company, but may not be as easily implemented for internet users as they must install extra hardware.

There are at least as many different approaches to reading biometrics as there are biometrics to read.[7],[8],[9],[10] and [11],
It seems that most implementations have pros and cons. I'll try to discuss most

of them here but I'll focus on fingerprinting, iris scanning and face recognition, as these are currently the most realistic biometrics available.

Typing dynamics

This is a way of telling people apart from the way they type at a keyboard
Pros: cheap (most computers have a keyboard)
Cons: FAR rates too high

Fingerprint

A fingerprint is the pattern of ridges on the finger tips[12]. This is probably the most widespread biometric in use. The reason is price, size and ease of use.

There are several methods of acquiring fingerprints today, namely:

- Optical sensors
- Ultrasonic sensors
- Solid state electric field sensors
- Solid state capacitive sensors
- Solid state temperature sensors
- Piezo electric sensors

Several manufacturers of keyboards and mice have included fingerprint sensors in some of their products. This includes Microsoft[13] and Siemens[14]

Microsoft themselves say, that these products are fine for private use, but

> *The Fingerprint Reader should not be used for protecting sensitive data such as financial information or for accessing corporate networks. We continue to recommend that you use a strong password for these types of activities.*[15]

It would seem that they themselves don't trust the security it provides.

There is a good reason for this. We know that we leave our fingerprints everywhere and that it is possible to read these fingerprints later – the police do it all the time. Experiments show (Matsumoto[16] and c't [6]) that it is possible to lift these fingerprints and create a fake fingertip, that can be used to fool many of today's fingerprint scanners. It is neither expensive (less than 10€) nor very complicated.

The problem that needs to be solved is how do we know that the scanned fingerprint is actually affixed to the right person? Some scanners try to overcome this problem by sensing pulse or by deep scanning the finger (the second layer of skin has the same fingerprint as the top layer) but some of these methods can still be fooled.[17]

With over 90 companies developing fingerprint scanners these problems will certainly be overcome in the foreseeable future.

Pros: cheap
Cons: Some systems can be fooled, by 'gummy fingers'

Hand geometry

"Unlike fingerprints, the human hand isn't unique. One can use finger length, thickness, and curvature for the purposes of verification but not for identification" – quote Arun Ross and Anil Jain[18]

Pros: fast, relatively cheap
Cons: the human hand isn't unique

Facial recognition

Facial recognition in its simplest form consists of a camera that takes a picture of the users face. This picture is then analyzed by finding different numbers like distance between eyes, length of nose etc.
To get a good picture, the user must be directly in front of the camera at a distance of about 40-50 cm. This distance matches the distance the user is positioned from the computer monitor. A camera put on top of the monitor is perfectly positioned for this.

One way of fooling a facial recognition could be to hold up a photograph in front of the camera or wear a latex mask.This has been overcome by asking the user to smile or blink, thus seeing, that the face is attached to a person.
Another solution has been to take pictures in the infrared spectrum (see vascular patterns).
Another problem with facial recognition is today's trends of "extreme makeovers", where plastic surgery alters an individual's facial appearance by changing the chin, nose, cheekbones and lips. The problem isn't that great, because it just means the user must make a new enrolment. This system cannot be used if the face is covered (women in burka's or similar clothing).[19]

Pros: cheap
Cons: Some systems can be fooled by photographs or masks

Iris scan

Iris scanning works much like facial recognition but focuses on the eyes and specifically the irises.
It is therefore obvious that this method can be fooled in the same ways as facial recognition. More so, a contact lens can be made to resemble the real iris.

In an interview with Dr. John Daugman[20] he refers to the fact that Professor Tsutomo Matsumoto has shown how two commercial iris readers could be

fooled 100% of the time and a third was fooled 50% of the time by holding a photograph of an individual's irises in front of the iris scanner. He then says that other systems have been proven to resist this kind of fraud for example by checking aliveness of the eye by checking pupil dilation in changing light.

c't's experiences with Panasonic's bm-et100 show the same. With a photo of an iris (with a hole cut for the pupil) held up in front of a real eye, they were authenticated by the system. Panasonic, at the time, said they would change their product prior to release on the German market. Today I still see the same iris scanner at Panasonic's home page[21] with manuals dating back to 2001.
I have not been able to find any information about problems with eye corrective surgery, but this might change the way the iris looks.

Pros: low FAR and FFR
Cons: Some systems can be fooled by photographs

Retinal Scan

This is an optical system that uses an image of the blood vessels (vascular patterns) in the retina (at the back of the eye). It is a fairly intrusive detection in that the user must remove any glasses, be very close to the device (3-5 cm) and focus on a certain point for 10 to 15 seconds. Because the retina is situated at the back of the eye, this is probably the safest biometric currently available. [22]

Pros: Very low FAR and FFR, probably the safest system, as it is very difficult to fool.
Cons: Intrusive and expensive

Vascular Patterns

Vascular patterns are the patterns of the blood vessels in or close to the skin. They can be read using infrared camera technology. Vascular patterns can be obtained from the face (which makes it a lot like facial recognition in the infrared spectre) or from the hand.

Pros: better than facerecognition
Cons: more expensive. An emerging technology

Voice recognition

Voice recognition requires the user to speak into a microphone. The sample taken is then spectrum analyzed and a match is found. Unfortunately it is easy to capture speech from a distance too, so it is fairly prone to replication.
Voice recognition can be improved by adding speech recognition, so that the user is asked to say a particular sentence, thereby making sure it is a live sample rather than a recording.

Pros: Cheap – many computers have a microphone input.

Cons: Easy to record

Handwriting

This method utilises a digitizer or tablet, where the users sign their name. Then the dynamics of the signature are captured – pressure, speed and velocity. So even if someone learns to duplicate a signature, the dynamics are probably not the same. There is an enrolment problem though, as writing on a tablet or digitizer doesn't feel like writing with a pen. People will get used to it after a while, but as enrolment is the first thing they have to do, the signatures produced may not be natural to them (even if it looks the same).

Pros: fairly cheap
Cons: Signatures change over time, so enrolment must take place at regular intervals, maybe once a year.

Addressing the Problem Domain

Perhaps one way to remedy this could be for the biometric device to send data via another channel to the authenticating mechanism. I'm thinking along the lines of:

A user sitting at a computer wishes to establish contact to a remote server. Connected to the computer is a biometric device.

1. Computer establishes VPN tunnel to server.
2. Server asks for authentication, giving a unique key.
3. Computer establishes VPN tunnel to biometric device.
4. Computer sends key to biometric device.
5. User gets scanned by device.
6. Device sends data encrypted by key to server by another channel (maybe a cell phone?).
7. Server validates user and authorizes the user.

Impact on Perimeter Security

We're already seeing biometric devices built-in in common computer equipment, such as mice (Siemens ID Mouse), Keyboards and USB keys to name some.
The question is – are they good enough? Do they give us the security we're so interested in? They're probably good at protecting a single computer, where there are typically just a few users, but in a large company or even on the internet we need to make sure, that no one is authenticated as someone else. One way of doing this might be by combining different ways of authentication. If for instance fingerprint authentication is combined with either a username or better yet a smart-card or a token.

I'm sure we'll see many implementations of biometric authentication in the near future. Especially fingerprinting and iris scanning seem go be advancing in the right direction as are others.
The big question is: will it completely replace passwords as the authentication method? I don't think so. Passwords are easy to manage and can be changed if there is reason to suspect its integrity.
I think username/passwords will exist for many years to come.

Assignment 2: Security Architecture

GIAC is a small company selling fortunes on the internet. I have been give the task to design the internet related security architecture needed for the company to work in a given number of ways. The company has already installed Windows 2003 on their internal servers and deployed an Active Directory. I have chosen to use the Microsoft windows 2003 platform where possible as the system administrators are already familiar with this operating system. The same goes for some equipment I have used which they already had (Cisco 2611 Router and Cisco 3005 VPN concentrator).

Access Requirements

For GIAC to sell fortunes via the internet they need a web server. They also need to be able to communicate via e-mail so a mail relay is deployed.
As regional offices and teleworkers need access to the internal network, a VPN solution has been chosen, involving a Cisco 3005 VPN Concentrator.

General Public

The general public has access to the web server (TCP port 80) for general information about the company and what we're selling.
They must also have access to a secure online registration as customers via HTTPS (TCP port 445).
E-mail to GIAC will go through a mail relay, where e-mail will be scanned for viruses before being delivered to the internal mail-server.

Customers

In addition to the general public's access, our customers must login to the secure web store via HTTPS (TCP port 445), where they can order new batches of fortunes for download and change address information, password etc.

Suppliers

Our suppliers make new fortune sayings and must supply GIAC with them over the internet. They also login to the secure web store via HTTPS (TCP port 445) where they can upload new fortunes, change address information, password etc.
Additionally they have the same access requirements as the general public.

Partners

Our partners can download fortunes for reselling or for translation. They can also upload translated fortunes.
To do this, they must login via HTTPS (TCP port 445).
This, again, is in addition to the general public's requirements.

Employees

The regional offices are connected to the headquarter via a VPN tunnel. This gives us the possibility to ease the administrative burden a little, as all employees access the internet through the same firewall.
The employees are subdivided into several classes:

Adminitrators : users with administrative roles and physical access to the servers.

Database Users: users who are allowed to change the contents of the database (i.e. add/delete/modify fortunes, addresses etc.)

Employees have normal access to the internet (TCP port 80 and 445) and are able to send and receive e-mail via the internal mail server (internal mail server to/from mail relay allowed on TCP port 25).
All internal workstations have anti-virus software installed, in this case Sophos Antivirus.

Sales/Teleworkers

Out-of-office employees, like sales people or teleworkers need a way to access the systems as if they are in the office. This can be accomplished by using a VPN tunnel like the regional offices, but created by software at the client side of the connection.
Their computers must have an active firewall installed and anti-virus.

Internal servers

All employees connect to a local Microsoft Exchange server for mail access. This server in turn communicates with the mail relay on the DMZ which is responsible for the further delivery of e-mail.
To be able to correlate events on different servers it is of essence that they all share the same time. In a Windows environment the PDC automatically serves time for computers in the Active Directory.Thus the PDC must be configured as an NTP peer that can access at least two reliable time-sources on the internet (unless of course it had its own atomic clock).

Data Flows

Source	Destination	Port(s)/Protocol	Description
General Public	Web Server	80/TCP (HTTP)	General access to the public web server, for information about the company, and how to become a customer.
General Public	Web Server	445/TCP (HTTPS)	Secure access to registration page.
General Public Customers Suppliers Partners	Public Mail Relay	25/TCP (SMTP)	Everybody should be able to send e-mail to GIAC
Public Mail Relay	General public Customers Suppliers Partners	25/TCP (SMTP)	And Receive e-mail from GIAC

Customers Suppliers Partners	Web server	445/TCP (SSL)	Access to the web store
Web Server	Database server	1433/TCP (SQL)	
Internal mail server	Public Mail Relay	25/TCP (SMTP)	All employees should be able to send e-mail to recipients on the internet.
Public Mail Relay	Internal Mail Server	25/TCP (SMTP)	Everybody should be able to send e-mail to GIAC
Employees	Internet	80/TCP (HTTP)	All employees need access to HTTP on the internet
Employees	Internet	445 /TCP (HTTPS)	All employees need access to HTTPS on the internet
Employees	Database server	1433 /TCP (SQL)	All employees need access to the database.
Regional Office Routers Sales Force Teleworkers	VPN Concentrator	500 /UDP (IKE)	IKE Permits key negotiation for establishment of the VPN.
Regional Office Routers Sales Force Teleworkers	VPN Concentrator	10000 /UDP	VPN Access for GIAC employees
VPN Concentrator	Regional Offices Routers Sales Force Teleworkers	500/UDP (IKE)	IKE Permits key negotiation for establishment of the VPN.
VPN Concentrator	Regional Offices Routers Sales Force Teleworkers	10000 /UDP	VPN data protocol

Table 1, Data flows

Architecture Components

Filtering Router(s)

I have used a Cisco 2611 as the filtering router at the headquarter

Cisco 2611 with software revision 12.3(13)

Note : GIAC already had this box when I was assigned this job. It ought to be replaced by a newer model (e.g. the 2611XM) as it has been “end-of-lifed” by Cisco. It is a stabile model though and running a current IOS, So my recommendation is to keep it for the time being and upgrade when bandwidth or a newer software demands it.

Firewall(s)

For the firewall I have chosen a Firewall-1 NG Express running on Windows 2003. As far as I can tell, this is actually cheaper (per throughput) than running an appliance. It also has the additional bonus that it is more flexible. It would be easy to add extra nework interfaces if needed plus I get a chance to back up the system.

VPN(s)

I have used following VPN components:

Headquarters: Cisco 3005 VPN Concentrator with software rev. 4.1.7.D

I have chosen to use a VPN Concentrator instead of the firewall’s built-in VPN capabilities to ease the burden on the firewall. This could make it a

lot easier to upgrade the VPN-bandwidth at a later date.

Regional offices: Cisco 831 with software revision 12.3(2)XC2

These seem to be well fitted for the task at hand. I briefly considered the Cisco PIX 501 firewall appliance, but chose the router as I think it has more features and running IOS, which makes it more configurable and upgradable. It also seems to have a higher performance, encryption wise, than the PIX.

Sales Force: Cisco VPN Client version 4.6

Network based IDS sensor(s)

Snort running on a Linux PC
I have chosen only one PC for the four taps installed as the total expected bandwidth is limited by the internet connection speed, and even a modest PC should be well equipped to handle 10 Mbps.
This is a standalone server, so the security manager should check the logfiles daily to see what abnormal traffic has been seen and configure the filters to sort out traffic, that is normal. This is an ongoing process, as attack patterns change rapidly.

Additional Components

E-mail relay: A Windows 2003 Server running eSafe Mail.

Database server : A Windows 2003 Server running Microsoft SQL Server 2000 with Service Pack 3.

Network Diagram

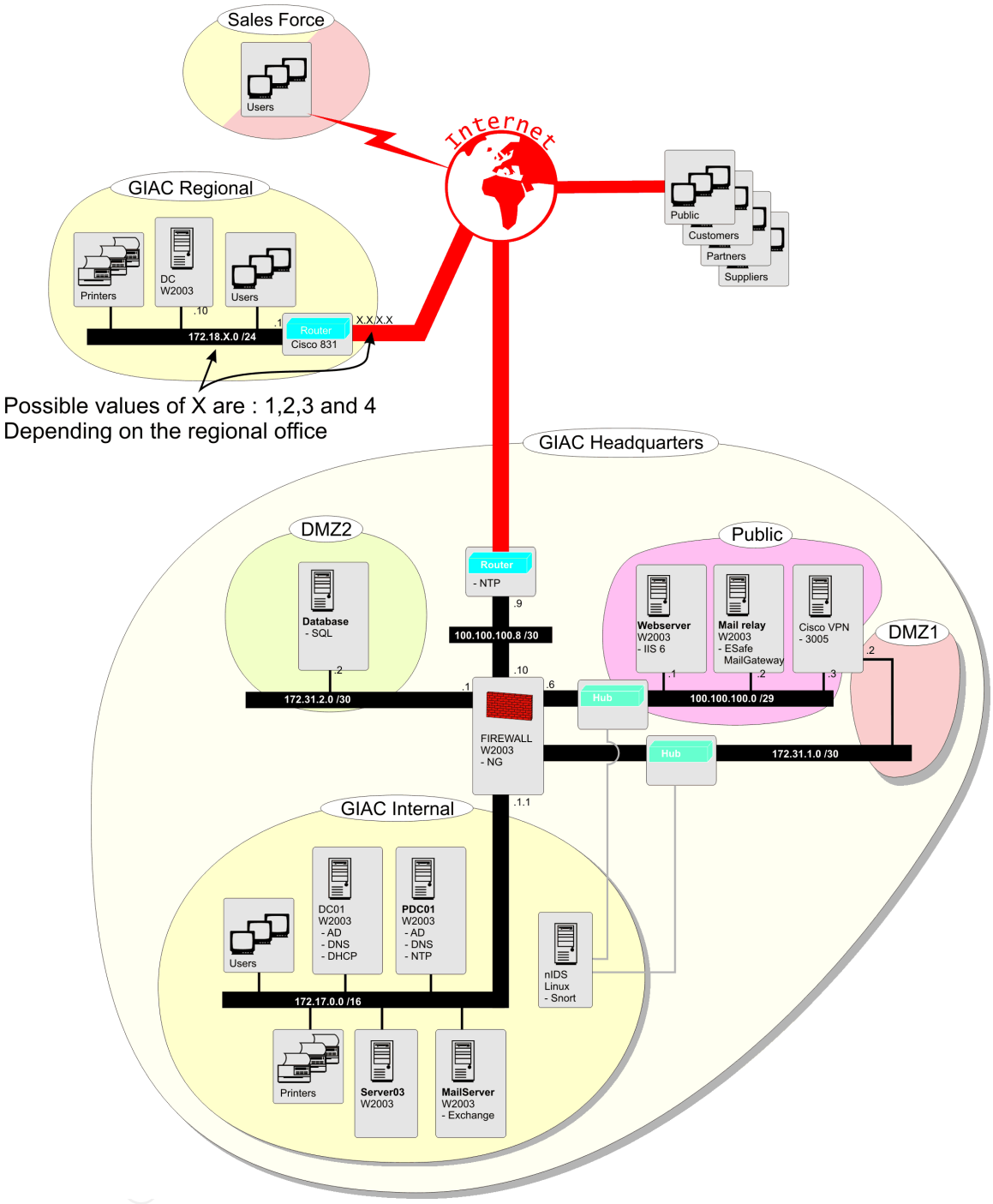

Figure 1, Network diagram

IP addressing scheme

There are quite a lot of different network segments at play here. We have no control over the IP-addresses of our teleworkers/sales force, customers, suppliers or partners, except the knowledge that they all have public IP

addresses and they are likely to change without our knowledge.

The following public IP-addresses are all fictional. Any resemblance to real-world addresses is purely coincidental. Their only purpose is to demonstrate how GIAC's network would look like with real IP-addresses.

The border router has the following external IP address of
Border router-external: 111.111.111.111

The Headquarter has been assigned a subnet with 16 IP addresses 100.100.100.0/28 (fictional). I have subdivided this into two networks
Public zone (100.100.100.0/29)
Web server: 100.100.100.1
Mail relay: 100.100.100.2
VPN Concentrator: 100.100.100.3
Firewall – public zone interface : 100.100.100.6
Border zone (100.100.100.8/30)
Border router – internal interface: 100.100.100.9
Firewall – external interface: 100.100.100.10

The regional routers have following external addresses:
Region 1: 1.1.1.1
Region 2: 2.2.2.2
Region 3: 3.3.3.3
Region 4: 4.4.4.4

I have assigned following internal private IP-addresses
- Headquarters, internal: 172.17.0.0 /16 (plenty of head room)
- Headquarters, DMZ1: 172.31.1.0 /30 (firewall and VPN internal)
- Headquarters, DMZ2: 172.31.2.0 /30 (firewall and database server)
- Office in region 1, internal: 172.18.1.0 /24
- Office in region 2, internal: 172.18.2.0 /24
- Office in region 3, internal: 172.18.3.0 /24
- Office in region 4, internal: 172.18.4.0 /24
- Teleworkers (NAT on VPN concentrator) , internal: 172.19.1.0 /24

Implementing Defense in Depth

Several layers

The hole point of defense in depth is to add several layers of security to the network and applications, not unlike an onion. Thus an intruder must peel off several different layers before he gets through. The border router and firewall is one example where the router protects the firewall which in turn fortifies the

defenses laid down by the router.

Web application

GIAC's main sales channel is the web; therefore a web application (the "web store") has been designed that sits between the user and the database holding the fortunes. It presents the user with secure web pages via SSL according to the group the user belongs to. The application is also responsible for validating user input. It checks conformation to the expected data types and values. For instance it will intercept a user trying to buy a negative amount of fortunes or a user trying to pass script or SQL statements in the data
Example
The user supplies the following name:

Susan" or "A"="A

If not checked this might result in a SQL statement as follows

Select * from bought_fourtunes where name="Susan" or "A"="A"

which will return all rows in bought_fortunes as "A" is always equal to "A".

In general, the application never uses a user supplied value directly, as this might result in disaster (overflows, executed code or improper SQL statements fired to the database)

E-mail

I have installed "Esafe Mail" on the mail relay. This enables us to scan e-mail for viruses and spam before they are allowed through. It also checks, that the syntax of the e-mail is valid.

Hardening

The firewall, web server, mail relay and database have all been configured with the Microsoft security policy called "Bastion host" which is an extension of the "Secure server" Security policy.
Each server is configured to only use TCP/IP (NetBios disabled) and have internal firewall rules that disable everything that is not required. This means, that:
The web server allows inbound traffic on TCP ports 80 and 445 (HTTP and HTTPS)
The e-mail relay allows inbound traffic on TCP port 25 (SMTP)
The database server allows only incoming traffic on TCP port 1433 (MS SQL) from the internal network or the web server.

Updates

Internally a WUS (Window Update Service) server has been deployed. Thought was given to letting the public servers access this server for "windows updates" – that is hot-fixes and service packs for automatic installation. The advantage of doing this is that the administrator can choose which hot-fixes and service packs

should be installed as he has to acknowledge them before they are deployed. This is very well for the internal systems, but I chose not to trust the automatic installation for the public servers which is why it doesn't show up anywhere but on the network diagram.

Physical security

All servers and network equipment are of course placed in locked rooms, with sufficient cooling and uninterruptible power supplies (UPS').

Assignment 3: Router and Firewall Policies

General Security Stance

The role of the border router and the firewall is “to protect and to serve”. This means that they must first of all protect our network and secondly allow legitimate traffic.
We have two different border routers in play namely the border router at the headquarters and routers at the regional offices.
The border router keeps the load on the firewall down by filtering away traffic that is either inappropriate for our network or traffic that is not destined for our network.
The firewall has more logic built-in and can better determine if traffic is in response to some other traffic.

I have chosen not to deploy firewalls at the regional offices as the router function as VPN terminators allowing only VPN traffic to and from the VPN concentrator.

Border Router(s) Security Policy

The border router has two sets of ACL’s configured: one for ingress traffic (from the internet to our network) and one for egress traffic (from our network to the internet). The order of the rules in the ACL’s is very important. The router processes them from the top and down and stops processing once it matches a rule. Thus one rule could potentially block the execution of other rules. As GIAC offers a very limited number of services, I have chosen to implement a positive list (allow some, deny anything else) rather than a negative list (deny some, allow everything else).

Ingress considerations for the router at the Headquarters:

Private IP-addresses are not supposed to be routed over the internet, but as this is not under our control we should deny them entrance to our network.
According to the IANA document “Special-Use IPv4 Addresses” (http://www.rfc-editor.org/rfc/rfc3330.txt) (which extends upon RFC1918) these are the IP addresses we should not expect on the internet:

0.0.0.0/8	"This" Network	[RFC1700, page 4]
10.0.0.0/8	Private-Use Networks	[RFC1918]
127.0.0.0/8	Loopback	[RFC1700, page 5]
169.254.0.0/16	Link Local	--
172.16.0.0/12	Private-Use Networks	[RFC1918]
192.0.2.0/24	Test-Net	
192.168.0.0/16	Private-Use Networks	[RFC1918]
224.0.0.0/4	Multicast	[RFC3171]
240.0.0.0/4	Reserved for Future Use	[RFC1700, page 4]

We must also block the IP-addresses we own, as we know them to be on the other side of the router.
To allow regional offices and teleworkers access through VPN we must allow everyone to connect to the VPN concentrator on UDP 500 (ISAKMP) and UDP 10000 (IPSEC).
Everyone should have access to the web server on TCP 80 (HTTP) and TCP 443 (HTTPS)
To allow for e-mail, everyone must be able to connect to the mail relay on TCP 25
Finally we should block anything else.

The ingress filter would thus look like this:

Action	Protocol (/port)	Source /mask	Destination/mask
Deny	IP	0.0.0.0 /8	Any
Deny	IP	10.0.0.0 /8	Any
Deny	IP	127.0.0.0 /8	Any
Deny	IP	169.254.0.0 /16	Any
Deny	IP	172.16.0.0 /12	Any
Deny	IP	192.0.2.0 /24	Any
Deny	IP	192.168.0.0 /16	Any
Deny	IP	224.0.0.0 /4	Any
Deny	IP	240.0.0.0 /4	Any
Deny	IP	100.100.100.0/29	Any
Allow	UDP /500	any	100.100.100.3
Allow	UDP /10000	any	100.100.100.3
Allow	TCP /80	any	100.100.100.1
Allow	TCP /443	any	100.100.100.1
Allow	TCP /25	any	100.100.100.2
Deny	IP	any	Any

Table 2 - Ingress filter (HQ)

Egress filter considerations at the headquarters.

This is simpler than the ingress filter, as only the public IP addresses should be allowed unto the internet. It doesn't pose as great a risk as it may seem, letting all public GIAC addresses use all TCP, UDP and ICMP services because they must all go through the firewall which restricts access further. To be good netizens private IP addresses will be denied access.

The egress filter then looks like this

Action	Protocol (/port)	Source /mask	Destination/mask
Deny	IP	any	0.0.0.0 /8

Deny	IP	any	10.0.0.0 /8
Deny	IP	any	127.0.0.0 /8
Deny	IP	any	169.254.0.0 /16
Deny	IP	any	172.16.0.0 /12
Deny	IP	any	192.0.2.0 /24
Deny	IP	any	192.168.0.0 /16
Deny	IP	any	224.0.0.0 /4
Deny	IP	any	240.0.0.0 /4
Permit	TCP	100.100.100.0 /29	Any
Permit	UDP	100.100.100.0 /29	Any
Permit	ICMP	100.100.100.0 /29	Any
Deny	IP	any	Any

Table 3, Egress filter (HQ)

Primary Firewall(s) Security Policy

The firewall adds network address translation (NAT) to our setup, thereby enabling internal computers to access the internet even if they have private IP-addresses. The firewall is connection and application aware and can match replies to requests.
NAT is only applied to the following networks for traffic directed towards the internet:

- Headquarters, internal: 172.17.0.0/16
- Office in region 1, internal: 172.18.1.0/24
- Office in region 2, internal: 172.18.2.0 /24
- Office in region 3, internal: 172.18.3.0 /24
- Office in region 4, internal: 172.18.4.0 /24
- Teleworkers, internal: 172.19.1.0 /24

Reverse NAT is performed the other way and is handled by the firewall.

The firewall has 5 interfaces configured:

Name	IP address	mask	Description
Fw-border	100.100.100.10	255.255.255.252	facing the border router
Fw-public	100.100.100.6	255.255.255.248	facing the public servers
Fw-vpn	172.31.1.1	255.255.255.252	facing the internal interface of the VPN concentrator
Fw-db	172.31.2.1	255.255.255.252	facing the database server
Fw-internal	172.17.1.1	255.255.0.0	facing the internal network

Table 4, Firewall interfaces

In the firewall rule set I have used several groups. These groups are

Name	Networks / groups
GIAC_HQ	172.17.0.0/16
GIAC_Regions	172.18.1.0 /24 172.18.2.0 /24 172.18.3.0 /24 172.18.4.0 /24
GIAC_Telework	172.19.1.0 /24
GIAC_Internal	GIAC_HQ GIAC_Regions GIAC_Telework
GIAC_Public	100.100.100.0 /28
GIAC_Public_Servers	100.100.100.1 (Web server) 100.100.100.2 (Mail relay) 100.100.100.3 (VPN concentrator)
GIAC_NTP	PDC01 (the primary domain controller)
GIAC_DNS	PDC01 (Primary domain controller) DC01 (Backup domain controller)
IANA_Private	0.0.0.0 /8 10.0.0.0 /8 127.0.0.0 /8 169.254.0.0 /16 172.16.0.0 /12 192.0.2.0 /24 192.168.0.0 /16 224.0.0.0 /4 240.0.0.0 /4
Internal_networks	IANA_Private GIAC_Public
External_networks	All except Internal_networks

Table 5, Firewall groups

I will start by showing the firewall rules that apply, and then continue to explain them.

Rule	Source	Destination	Service	Action
1	any	Fw-border Fw-public FW-vpn	any	drop
2	GIAC_DNS	External networks	TCP 53 (DNS) UDP 53 (DNS)	Accept
3	any	Web server	TCP 80 (HTTP) TCP 443 (HTTPS)	Accept
4	Mail relay	GIAC_DNS	UDP 53 (DNS)	Accept
5	External_networks	Mail relay	TCP 25 (SMTP) + SMTP incoming	Accept

6	Internal mail server	Mail relay	TCP 25 (SMTP)	Accept
7	Mail relay	Internal mail server External_networks	TCP 25 (SMTP)	Accept
8	Mail relay	Esafe.com	TCP 80 (HTTP) TCP 443 (HTTPS)	Accept
9	External_networks	VPN concentrator	UDP 500 (IKE) UDP 10000 (IPSEC)	Accept
10	VPN concentrator	External_networks	UDP 500 (IKE) UDP 10000 (IPSEC)	Accept
11	GIAC_Regions GIAC_Teleworkers	GIAC_HQ	any	Accept
12	GIAC_HQ	GIAC_Regions GIAC_Teleworkers	any	Accept
13	Web server GIAC_internal	Database server	TCP 1433 (MS SQL) UDP 1433 (MS SQL)	Accept
14	GIAC_NTP	Any	NTP	Accept
15	GIAC_Public_Servers	GIAC_NTP	NTP	Accept
16	GIAC_Internal	External networks	TCP 80 (HTTP) TCP 443 (HTTPS)	Accept
17	GIAC_Internal	External networks	TCP 21 (FTP) + FTP passive	Accept
18	any	Any	NBT	Drop
19	any	Any	Any	Drop

All rules are set to LOG activity except rule 18

Rule 1 This rule drops all connection attempts to the firewall, which will make it virtually invisible.

Rule 2 The internal DNS servers are allowed to make lookups on external DNS servers.

Rule 3 HTTP and HTTPS traffic to the web server is allowed

Rule 4 The mail relay needs to make DNS lookups both for the e-mail service and the integrated function that updates the software (see rule 8).

Rule 5 E-mail is allowed to traverse the firewall. Additionally I have defined an SMTP resource “SMTP Incoming”, that checks that the “rcpt to” is addressed to *@giac.com.

Rule 6 The internal mail server must be able to forward mail to the mail relay

Rule 7 The mail relay is allowed to deliver mail both to the internal mail server and all external mail servers.

Rule 8 eSafe Mail is configured to auto-update virus and spam signatures and must therefore be able to acces esafe.com

Rule 9 Our Teleworkers and sales force as well as the regional offices use a VPN connection to the VPN concentrator and must be able to connect to it.

Rule 10 And the VPN Concentrator must be able to connect the other way.

Rule 11	The regional offices and teleworkers are allowed through to the headquarters internal network from the internal interface of the VPN concentrator.
Rule 12	And the other way around
Rule 13	Employees and the web server can access the database
Rule 14	The internal time server is allowed to get the time from external NTP servers.
Rule 15	The web server, mail relay and VPN concentrator gets their time from the internal time server
Rule 16	The Internal networks are allowed to use HTTP and HTTPS
Rule 17	They are also allowed FTP, but with an added resource that is configured to only allow “Passive FTP”, which means, that external FTP servers should not make connections to internal computers.
Rule 18	Drops Netbios traffic. This rule was added to remove pollution of the log-file.
Rule 19	Anything else gets dropped.

References

[1] RSA Security - RSA SecurID Authenticators. RSA.
<http://www.rsasecurity.com/node.asp?id=1157>
[2] Uludag, Umut and Pankanti, Sharath and Prabhakar, Salil and Jain, Anil K. Biometric Cryptosystems: Issues and Challenges.MSU.
<http://biometrics.cse.msu.edu/Uludagetal_Cryptosystems_ProcIEEE04.pdf>
[3] Putting an End to Account-Hijacking Identity Theft, Pages 30-37. Federal Deposit Insurance Corporation, December 14, 2004.
<http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf>
[4] Jain, Anil K. et al.Biometrics: A Grand Challenge. Cambridge, UK, Aug. 2004.
<http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf>
[5] Lisbjerg, Jakob Vedel. Fingeraftryk på færgen. Danmarks Radio.
<http://www.dr.dk/Videnskab/Emner/Teknik/biometri/fingeraftryk.htm>
[6] Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler. c't 11-2002, page 114 – Biometrie, c't.
<http://www.heise.de/ct/english/02/11/114/>
[7] BIOMETRICS COMPARISON CHART. Court Technology Laboratory.
http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html
[8] COMPARISON OF BIOMETRIC TECHNIQUES. <http://www.bio-tech-inc.com/bio.htm>
[9] Biometric Software Products Overview.
<http://www.biometricsdirect.com/Products/SW/SWOverview.htm>
[10] Biometrics Resource <http://www.findbiometrics.com/>
[11] Mainguet , Jean-François. Biometrics: types. 2004.
<http://perso.wanadoo.fr/fingerchip/biometrics/types.htm>
[12] Prabhakar, Salil and Jain, Anil. Biometrics Fingerprint MSU.
<http://biometrics.cse.msu.edu/fingerprint.html>
[13] Mouse and keyboard products. Microsoft.
<http://www.microsoft.com/hardware/mouseandkeyboard/features/fingerprint.mspx>
[14] Siemens ID Mouse. Siemens. <http://www.siemensidmouse.com/>
[15] Fingerprint reader products. Microsoft.
<http://www.microsoft.com/hardware/mouseandkeyboard/productlist.aspx?fprint=yes>
[16] Jelly babies dupe fingerprint security ZDNet Australia News Security
<http://www.zdnet.com.au/news/security/0,2000061744,20265318,00.htm>
[17] van der Putte, Ton and Keuning, Jeroen. Biometrical fingerprint recognition:don't get your fingers burned Ton van der Putte and Jeroen Keuning (september 21st 2000).
<http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf>
[18] Ross, Arun and Jain, Anil Hand geometry MSU.
<http://biometrics.cse.msu.edu/hand_geometry.html>
[19] Individual Biometrics - Facial Recognition. Court Technology Laboratory.
<http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html>
[20] Interview with Dr. John Daugman, Cambridge University December 2004
<http://www.findbiometrics.com/Pages/feature_daugman_camuk.htm>
[21] BM-ET100US Authenticam Iris Recognition Camera. Panasonic.
<http://www.panasonic.com/business/security/biometrics_access.asp>
[22] RETINAL SCAN. National Center for State Courts. E-court conference 2002.
<http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html>