A Secure Image Transfer Application for the NHSnet

Kerry Jean kjean@ee.ucl.ac.uk, Walter Eaves weaves@ee.ucl.ac.uk, John Lam jolam@ee.ucl.ac.uk, Alex Galis agalis@ee.ucl.ac.uk,
Department of Electronic Engineering, University College London

Abstract: *This paper outlines the application of some of the security technologies investigated in the HARP (Harmonisation for the security of web technologies and aPplications) project to the NHSnet. It proposes the use of dynamic secure VPN's, web applications and trusted third parties to enable mobile health care practitioners to securely transfer images into the NHS network while working in the field. It describes a testbed developed at the University College London and presents results of the testing of the application. An evaluation of the effects of the different security protocols used in the application is presented along with some possible improvements.*

In a modern health service the exchange of medical information is crucial for the diagnosis and treatment of patients as well as in the research into better health care and drugs. However, the medical information exchanges can be very sensitive, so communication and co-operation require appropriate security services to be instigated according to the implemented policy [1]. The HARP (HArmonisation for the secuRity of web technologies and aPplications) project developed TTP (Trusted Third Party) services, and technologies for the integration of Web oriented security systems in the telemedicine environment [2]. Due to the open environment of web-based applications, their exploitation in telemedicine introduces many security concerns. Through the use of secure servers called HARP servers, certificates and secure VPN's (Virtual Private Networks), the HARP project has shown how harmonised security of web applications for the telemedicine sector can be implemented. This paper describes briefly one such system developed at the University College London using secure VPN's and TTP's (Trusted Third Parties), a proposal for secure image transfer in the NHSNet (NHS Network). It then goes on to describe the testbed developed, its testing and evaluation.

The HARP Secure Image Transfer (SIT) provides a viable solution for the secure transfer of medical images into the NHSnet of the UK by mobile medical practitioners outside of it. This is especially useful for a district nurse, who performs house visits and wants to immediately send a photograph, of perhaps a skin ailment, to a GP for referral.

HARP ECE Proposal

The HARP proposal is to create small networks in the Regional Health Authorities for the sole purpose of hosting a HARP server. The Regional HA's were used to ensure manageability and robustness of the system. The HARP server will serve as a bastion host to enable mobile medical practitioners to remotely connect to the NHS Network. The HARP servers would be connected to the NHSnet via the Internet. Security, would not be compromised as the mobile network users would only be able to access the HARP server through encrypted tunnelling protocols (PPTP) and persons within the NHS Net would only access the HARP server through SSL (Secure Sockets Layer).

Secure Image Transfer (SIT)

Secure access into the NHSnet is achieved by forming a secure VPN by tunnelling into the NHSnet. The scenario, in which a nurse visiting a patient at home wants to show a GP in his surgery some photographs just taken of a patient's skin ailment, is detailed in **figure 1** overleaf.

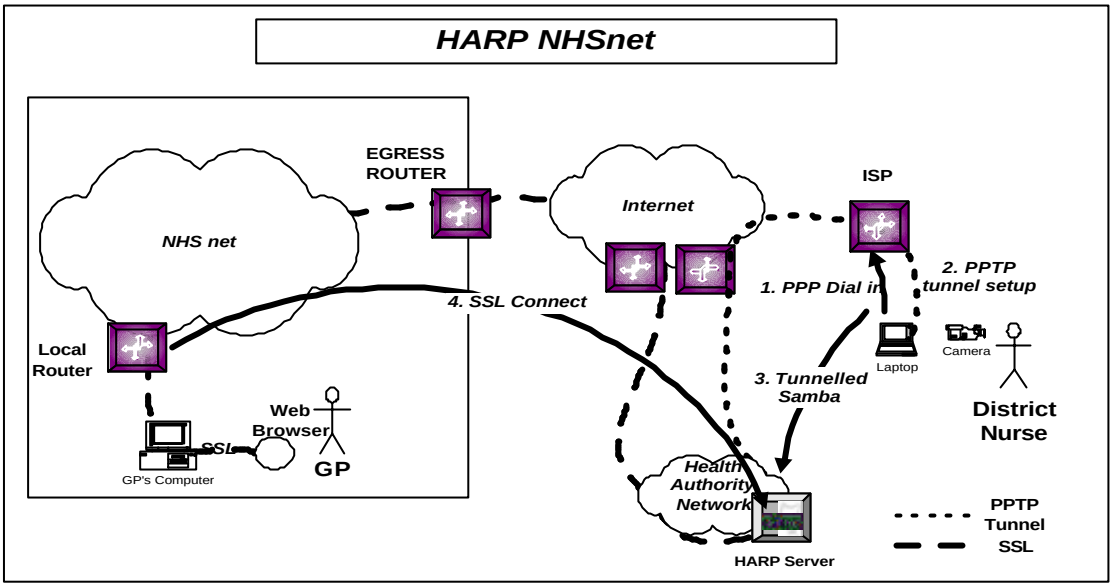

Figure 1: HARP solution for the NHSnet allowing a nurse on a house call to send photographs of a patient to a GP in his surgery using a PPTP tunnel and a bastion server.

Digital photographs of the patient are stored on the nurse's laptop. A dial in PPP session to an ISP is made from the laptop. Then a PPTP tunnel is made from the laptop into the HARP server and a directory from the HARP server mounted onto the laptop using Samba and the photographs transferred there. An out of band control signal is sent to the GP informing him that the pictures are there. The GP, through his web browser accesses the photographs that the nurse has obtained by visiting a URL. Security is not compromised as SSL is used to get out of the NHSnet and into the HARP server. Mutual authentication of the client and server occurs. An encrypted layer two tunnelling protocol, PPTP(Point to Point Tunnelling Protocol) is used to get into the HARP server, a TTP (Trusted Third Party), from outside the NHSnet forming a Virtual Private Network. The above system has been implemented on a test-bed at UCL as shown in **figure 2** below.

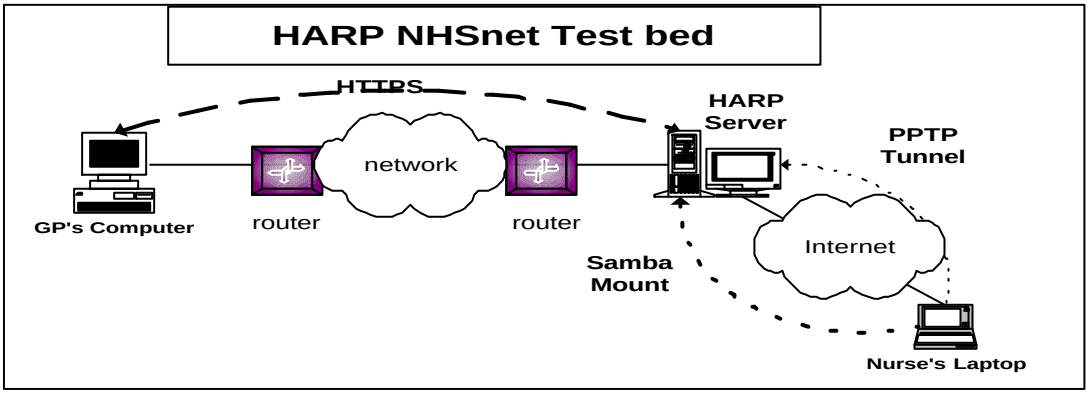

Figure 2: HARP test-bed implementation of the SIT scenario.

The HARP Secure Image Transfer testbed was implemented using the following three machines.
HARP server: It acts as a bastion host allowing the PC to securely access images from the laptop. It is a PPTP server and allows the laptop to tunnel into it forming a secure VPN. An Apache-SSL web server provides secure HTTPS access while Samba allows the mounting of directories.
Nurse's laptop: The laptop dials onto the Internet using PPP and creates a PPTP connection with the HARP server to form a secure VPN. It contains a web cam, which enables the taking of digital photographs, which are transmitted over a network. The laptop is a Samba server.
GP's PC: This machine is used to access and view photographs mounted on the HARP server from the laptop. The only requirement for this machine is an SSL enabled browser.

Testing and Results

The performance metric used was the time taken for the clients to access the servers and for data transfer to occur. The connections among the test machines were varied from insecure ones to very secure ones while the number of clients (laptops) was increased from one to ten and the access times measured. Four replicates were done where the link between the GP's computer and the HARP server and that between the HARP server and the Nurse's laptop were changed as shown below:

	Between GP's computer and HARP server	HARP server and Nurse's Laptop
1.	IP	HTTP
2.	IP	HTTPS
3.	PPTP	HTTP
4.	PPTP	HTTP

Figure 3 below shows the comparison between the times for all the systems. It clearly indicates that as security increases there is an increase in the access and transmission times. Furthermore, there is a greater increase when the HTTPS protocol is used instead of a PPTP tunnel. This suggests that there is a greater time penalty with HTTPS than with PPTP.

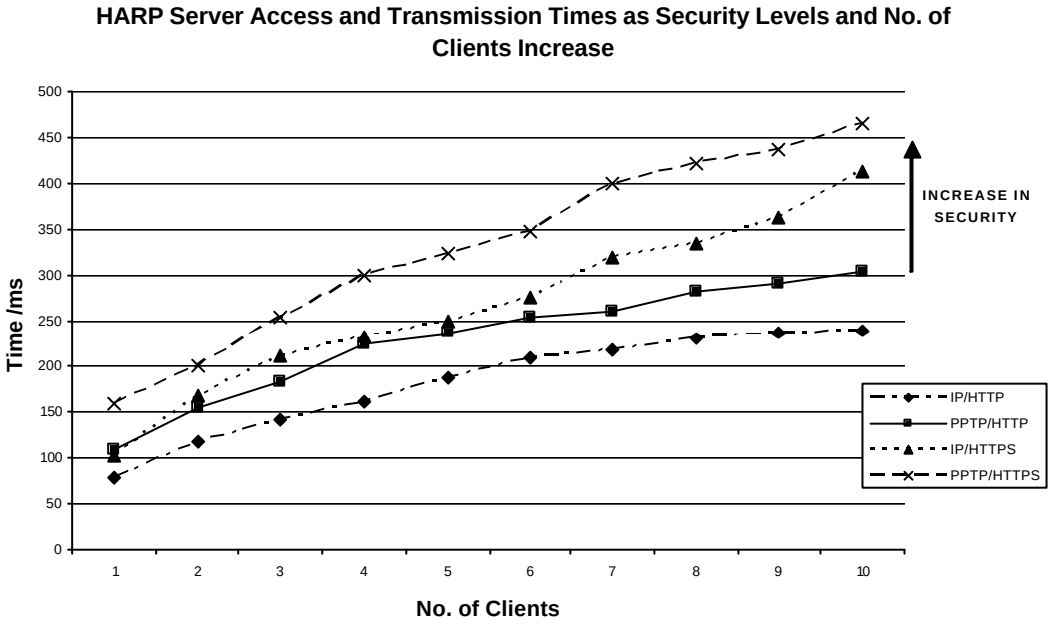

Figure 3: Graph showing the access and transmission times from the laptop to the GP's computer, with an increase in the number of clients for the different levels of security in the HARP SIT system.

Discussion

The results have clearly stated that there is a great increase in the response times for accessing an image via a web server as the security used in the system increases. However, the major finding in our results was that HTTPS introduced the greatest increase in response time in the HARP SIT system. Hence while HTTPS makes image transfers very secure it introduces a high response time penalty for that security. The response time of the server, measured in milliseconds (ms), is the time a user waits between requesting and receiving the image. The performance of any web server depends on three basic resources: the network, backend services, and the computer. Here we are interested in cases where the server is compute bound (also called "processor bound"), the most common for secure servers. HTTPS uses SSL which uses the RSA cipher suite with 1024 bits while PPTP uses MD5. HTTPS web servers are commonly CPU bound due to the overhead of public key cryptography. It is common for 80% or more of the CPU time to be spent performing public key cryptography in servers running Apache-SSL. The 1024 private bit operation for RSA requires millions of CPU instructions to perform. This is because of the fact that the mathematics behind RSA is modular exponential of a set of 1024 bit long integers. Breaking down x^y mod z (where x, y and z are over a thousand bits long each) into small enough steps for a 32 bit processor is not efficient. The time required to compute an RSA private key operation is a function of the length of the key, commonly referred to as the key length. As key length increases, security increases but performance decreases. 1024 bit RSA keys are

used for server authentication but the optimal operation of a RSA 1024 bit private key takes almost 50ms with a Pentium 166 MHZ computer. In our implementation of PPTP, MD5 was used as the cipher suite so we will compare it to RSA with 1024 bits. An average 32 bit processor can easily handle the necessary RC4 and MD5 at only a few percent loading. They are fast enough to run on a general purpose processor since they are designed to run efficiently on 32 bit general processors. It is because of this that the use of HTTPS results in a greater response time than the use of a PPTP tunnel. As more clients log in, there is a faster increase in the response time for HTTPS as system resources are being used up.

Improvements

While the security in the HARP SIT application can be described as adequate in terms of the confidentiality of the information transmitted and the cost benefit analysis, it can be improved tremendously. The area where security can be improved most is the between the Nurse's laptop and the HARP server. Machine certificates for the laptop and HARP server to authenticate themselves for PPTP VPN will improve security even more. Such a machine certificate is used to validate a sender or receiver at a system level. Through the use of smart card login, the HARP server can more reliably authenticate the nurse than just secure passwords or machine certificates. Smart Card for client authentication and authorisation is ideal for field workers as in the case of the District Nurse. However, smart cards require extra hardware and software and if the smart card is lost then the nurse cannot connect to the HARP server.

Internet Protocol Security (IPSec) can be implemented between the laptop and the HARP server. However, IPSec is a new technology and is only implemented on Windows 2000 and the laptops would be limited to that operating system. Also when this system is implemented on the NHSnet, the Nurse's laptop connecting to the Internet using the 56K modems or mobile phones would have too low a data transfer rate as IPSec introduces much data overhead. Most of today's IPSec implementations support public key certificates and can generate stronger encryption keys than mechanisms based on shared passwords.

The Layer Two Tunnelling Protocol (L2TP) can also be implemented between the laptop and the HARP server. When L2TP tunnels appear as IP packets, they take advantage of standard IPSec security using IPSec transport mode for strong integrity, replay, authenticity, and privacy protection. L2TP was specifically designed for client connections to network access servers, as well as for gateway-to-gateway connections. L2TP has many advantages over PPTP such as header compression, support for multiple tunnels between end points and also tunnel authentication which PPTP does not support. L2TP can be combined with IPSec to give L2TP/IPSec. This provides well-defined and interoperable tunnelling, with the strong and interoperable security of IPSec. It is a good solution for secure remote access and secure gateway-to-gateway connections. Lacking a better pure IPSec standards solution, this is probably the best standards based solution for multi-vendor, interoperable client-to-gateway VPN scenarios.

Conclusion

It has been showed that the HARP SIT application is a viable proposal for the secure transfer of images into the NHSnet. However, the security of the HARP SIT application can be improved vastly by the use of better security techniques, but they would usually add an extra cost or will slow done response time. The best alternative would be to implement L2TP instead of PPTP between the laptop and the HARP server.

Acknowledgements

The work presented was done as part of an IST (Information Society Technology) project, HARP partly funded by the European Commission.

References

[1] Blobel B, Katsikas S. K., (1998) Patient data and the Internet – security issues, Chairpersons introduction, International Journal of Medical Informatics 49, pp S5-S8

[2] Deliverable D4.1, First Prototype of a Harmonising Cross-Security Platform, HARP – IST 1999 – 10923, July 19th, 2001