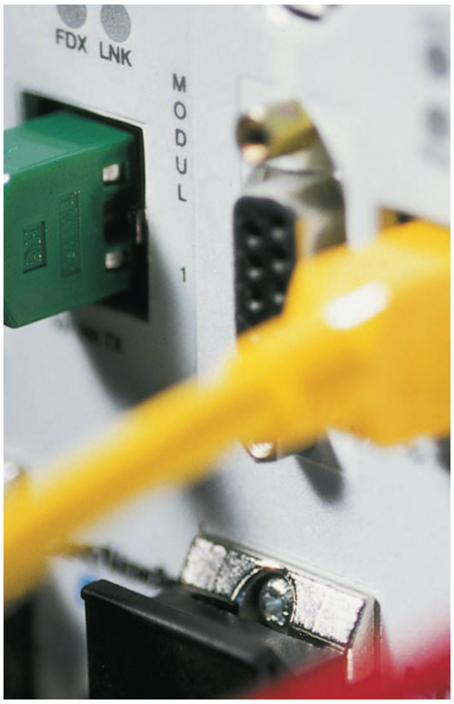
Secure architecture for embedded web servers



The integration of web servers into embedded systems offers a dividend at many levels. Operationally it can place industrial control, diagnostics and maintenance half a world away from the actual plant location – in fact anywhere with access to a reliable Internet connection. The ease and economy with which web-based architecture can integrate the activities of geographically diverse plant locations alone justifies use of the technology: The low cost and ubiquitous nature of Web Services components makes the case unassailable. Using public networks as a transmission layer for industrial architecture raises a legitimate concerns about security. But Virtual Private Networks can now deal effectively with the issue say Axel Sikora and Peter Brügger

Integration of web servers into embedded systems advantageously combines the use of the familiar TCP/IP and HTTP internet protocols in seamless integration with a graphical user interface displayed on a standard web browser for use both locally and remotely[1]. The concept works as well for legacy technology as it does with new installations, but in all cases the major driver to use embedded web servers is the huge potential to save cost.

The cost savings occur over the lifetime of a product but start with eased product development. The savings continue into the maintenance and production phase, simplifying integration along the way. Web server technology can then add flexibility in making changes to an existing product approaching the end of its production life. As a consequence, the number of applications where web servers are finding a use is rapidly increasing. Applications include home, building and industrial automation, as well as consumer and communication electronics.

Against these advantages, some serious challenges come into play when using embedded web servers. Security is a major issue. Many embedded web servers may give access not only to data but may allow the control of devices, machines and factories. The resulting potential security risk must be totally cleared at the lowest possible cost.

Scalability is another challenging issue. The devices themselves permit a high degree of scalability: computing performance may be increased from an 8-bit microcontroller to a 64-bit high end enterprise server without changing communication protocols or access mechanisms. But this ease of scalability does not apply nearly so well to the system itself. Imagine a remotely administered web-based HVAC system working across all the schools of a municipality (Fig. 1). The administration wants to reduce heating cost by lowering the building temperature on a public holiday. In a traditional approach, one would have to contact each and every web server for every location and click the appropriate menu buttons – not an efficient way of working!

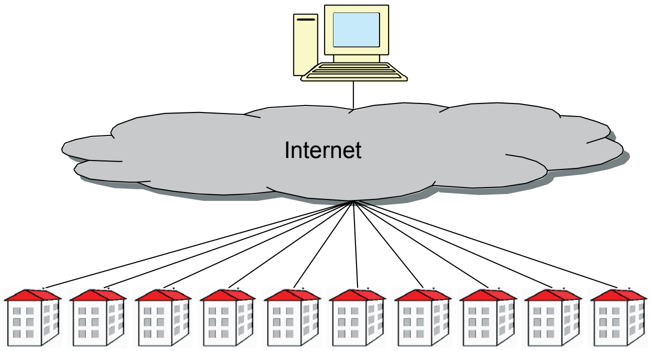


Fig. 1. Simple Internet-based architecture for teleservices

In many cases, embedded web servers are initially used due to their low investment – with severely restricted resources as a consequence. For instance, the storage of large documentation files or images may not be possible. Additionally, an update on locally held information may present its own difficulties.

Very real security issues are closely connected with scalability. In many systems employing embedded web servers, username and password are stored in the device. This makes implementation of password policies, administration and updates on access rights a significant task. This frequently leads to a situation where only one common password is used for all devices so presenting a severe security flaw.

Finally, connectivity may itself pose an additional challenge. Many embedded web servers are not permanently connected, linking instead to the Internet via dial-up modem. This can bring further incompatibility in reconciling V.34, V.90, V.92, ISDN, GSM/GPRS and other protocols, etc. ADSL modems offer high traffic volumes at low cost but are not inter-working. Additionally, modem connectivity implies the use of Point-to-Point-Protocol (PPP) with a multiplicity of options.

Multi-tier solution

These challenges may be addressed with a multi-tier architecture (Fig. 2) in which web servers are not accessed directly from the client, but via a Portal. This leads to an multi-tier architecture, the Virtual Private Infrastructure (VPI). Returning to the previous example of temperature reduction across all school buildings, these could be administered via a single website on the VPI Portal.

The VPI Portal is more than just a HTTP proxy as it provides a number of additional services: it becomes the central administration platform for the all target devices in the system.

- It holds a list pointing towards all target system links to which the administrator has rights of access – so centralising security accession to a single point. However, the Portal establishes a transparent HTTP connection to the target device once it has been selected by the administrator.
- A VPI Portal provides access security, as the user has to authenticate against a centralised user/password database.
- A VPI Portal can execute additional tasks such as handling larger documentation files and images, event-driven messaging or escalation

> “A Virtual Private Network can be described as the ability to tunnel through the Internet or other public network in a manner that provides the same security and other features formerly only available on private networks. With tunneling, a message packet is encapsulated within an IP packet for transmission across the public network, with the encapsulating information being stripped off upon arrival at the target network, such as the corporate local area network” – MicroSoft

of error cases. It might also provide the interface to enterprise resource planning (ERP) systems operating a unified supply chain management. This additional functionality derived from the VPI Portal does not affect the transparent communication flow between client and devices.

● A VPI Portal may increase security, by providing SSL-connectivity, a security encryption technology not yet easily integrated into embedded web servers[2].

Compatibility issues may resolve themselves through the centralised device access implicit with a VPI Portal. Modem control passes from the client device to the Portal – which may be located at an Internet Service Provider who holds the know-how to run the infrastructure and its variety of protocols. This shares the investment and running cost over a large number of customers.

VPI-Initiative

The situation described above was understood by many companies and their engineers. A number of them gathered together in August 2002 to found the Virtual Private Infrastructure (VPI) Initiative[3]. VPI embraces companies operating at various levels along the value creation chain: There are engineering companies, device and system manufacturers and service providers. All have an interest in creating a common platform for their customers in the face of proprietary solutions in the embedded Internet world. The VPI Initiative is a non-profit organisation led by a board of six industry personnel.

VPI Initiative pursues several objectives on its way to a unified infrastructure for remote web services.

Baseline standards. In order to unify infrastructure, the VPI Initiative has developed a set of baseline standards. Evolution of the standard will occur as unification of additional services progress. This holds true for unification of data models, database access, etc. In its first version, the standard describes a basic communication model of commonly encountered internet and web architecture.

Open certification. Standards are only useful if they can be understood and observed by market partners. Therefore, a certification authority within the VPI Initiative is required to test compatibility against the standard and interoperability between systems from different suppliers. ▶

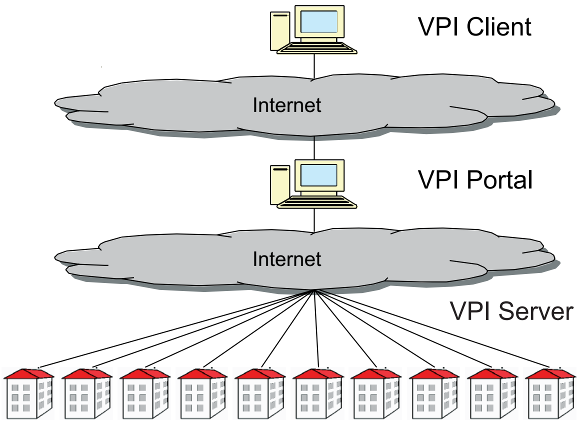


Fig. 2. Portal-based architecture for Teleservices

Marketing activities. The VPI Initiative envisages the deployment of existing web technologies for many new and existing applications. Members companies will be expected to promote advances in technology, products and markets based on VPI concepts.

VPI Standard

VPI is an open standard enabling evolutionary compliance for many systems. It principally requires that all transactions between devices on the network should be handled via HTTP 1.1 as described by RFC 2068 and 2616[4]. Other protocols may be implemented as well but the ability to work with HTTP is of vital importance. HTTP is the common platform for all VPI-based transactions for components and systems provided by different suppliers. This ensures that functions will be accessible as web services via public Internet.

Integration into third-party applications is also possible using an optional VPI agent to widen the potential applications base. The VPI Agent renders accessible from the VPI Portal devices enclosed by an intranet. The operator of the intranet has control over the VPI Agent and can define at any time which target systems should be visible on the Internet.

Additionally, available procedures, variables and devices are provided as process points. In most cases the VPI Agent will be a software module which can be used on any system within the intranet, for example on a PC, a server or a suitable embedded device. Operability behind firewalls requires that the VPI Agent's HTTP server works via TCP Port 80.

The VPI Standard also sets rules for portability of systems by excluding absolute links or addresses, etc. And last but not least, security is a major stepping stone towards ubiquitous embedded computing.

References

1. Sikora, A., The Ethernet roadmap from office to industry; *The Industrial Ethernet Book*, September 2004, pp. 12-16.

2. Rescorla, E., *SSL and TLS – Designing and Building Secure Systems*, Boston 2001.

3. http://www.vpi-initiative.com

4. Fielding, R., et.al., *Hypertext Transfer Protocol – HTTP/1.1, RFC2616*, available at, e.g.: http://www.ietf.org/rfc

Prof. Dr.-Ing. Axel Sikora is head of the Department of Information Technology at the University of Cooperative Education, Lörrach, Germany, and a member of the Board VPI Initiative
sikora@ba-loerrach.de

Peter Brügger heads iniNet Solutions and is chairman of the VPI Initiative
bruegger@ininet.ch