Towards an Internet Selling Layer

Martin Gutbrod

Technical University of Braunschweig,
Institute of Operating Systems and Computer Networks,
38106 Braunschweig, Germany,
gutbrod@ibr.cs.tu-bs.de

Abstract. Today buying for internet content is a tedious thing for both vendors and consumers. We are working on a solution which is layered between network and transport and makes the selling process more easy and secure than present implementations.

1 Scenarios

Traditional the buyer has to choose the content, authenticate the other party and himself, choose the preferred billing method and pay it. This must be done on every application and supplier again. Redundant implementations are an overkill and higher probability of errors. On a legal view it's not clear where the transfer of perils from digital goods is over IP networks [5, 2]. Next unclear thing is how to bill for machine to machine communication, as well as directly by socket connections or grid computing? There are handmade solutions for every scenario, but we think further valuable services and content consumptions need a common solution for very most applications on IP based networks to boost online revenue.

In our concept the operating system and certificates support the selling process straightforward. Whenever the consumer requests valued content, he will authenticated by his certificate and – depend on his personal policy – be asked for payment acceptance. Content could be websites, video streams, sound files, documents, software or any other IP based services. No application on the upper internet layer has to be modified to support buying. On buyers task bar an icon about his consumptions status is displayed and informs about the exactly amount purchased.

On seller side the application or the host system prices the content it provides and hands over this pricing information down to the trading infrastructure. On buyers site the application should not know anything about the costs for its received content. Both sides are freed from security, authentication and accounting processes.

2 Selling Layer Between Network and Transport

Our selling infrastructure is placed below the transport layer on top of the network layer. This intermediate "selling protocol" with extra header handles the

payment and delivery process and maps between customer and consumed content (accounting).

Pricing the packets is done in only some packets. Tokens are defined in the packet saved from replay by sequence numbers. The tokens could correspond directly to currency amounts or according to volumes and quality of service parameters. This implies a transparency cost structure on the whole network route and new straightforward routing methods are possible which e.g. prefer expensive content.

Doing accounting on consumer's and vendor's site gives trust to the buyer and moves transfer of perils to buyer's host. Cause of payment and content are close-knit the consumer could check his costs in a fine granularity during the receiving process.

With this architecture it is also possible to sell application transparency between hosts, gateways or host and gateway and especially also for content selling without any user interactions.

3 Principal Constituents

An Order Policy Service (OPS) supervises the consumptions process and interrupts if defined guidelines are violated. Some examples for policies are maximum price per site, per video, per megabyte, per day or month etc. The OPS is bonded on personally certificates. If the consumer requests non cost free content the OPS pop up a window and asks for ratification, if it is not auto-ratified. The OPS is working close together with the Accounting Service (AS) which collects the amounts of consumed (buyer) or provided (seller) content.

The security services authentication, integrity check, confidentiality, replay protection and key management are done by IPSec [3, 4]. In the further *Trusted Computing* [1] can curing the program binaries for OPS and security processes.

Trading partners are trusted by Certificate Authorities (CAs). In case of anonymous selling, a trust third party hides the real seller. This is the CA itself or a Payment Provider (PP). The PP handles the payment process by credit card or any other electronic payment method. A PP is not necessary, if the seller handles billing and payment traditionally by himself.

References

[1] T. C. P. Alliance. *TCPA*, 2004. `http://www.trustedcomputing.org`.

[2] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, Network Working Group, Dec. 1998.

[3] S. Kent and R. Atkinson. IP Authentication Header. RFC 2402, Network Working Group, Nov. 1998.

[4] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406, Network Working Group, Nov. 1998.

[5] J. Postel. Internet Protocol. RFC 791, Information Sciences Institute, Sept. 1981.