Quality and Security Usability

Luis Sousa Cardoso

Abstract — Telecommunications industry's customers are demanding comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks and should have high availability, appropriated response time, reliability, integrity, scalability, and provide accurate billing information. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solutions. To achieve such a solution in multi-vendor environment, network security should be designed around a standard security framework. For the majority of users and applications, increased security cannot be achieved with technology that decreases usability. Then, it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized

Keywords — availability, authentication, access, confidentiality, control, integrity, quality, risk, security, threat, usability, vulnerabilities

I. INTRODUCTION

In today's society, much depends on networks and information systems. Quality is already a key work and additional requirements for security will rapidly increase as networking and computing develop further and electronic communications become part of all aspects of our daily lives. For instance broadband connections offer people the possibility to be "always on". This, of course, increases the vulnerability of systems and multiplies the probability of some sort of cyber-attack. Enhanced security is therefore a key element for the success of broadband.

New wireless applications will enable people to access the Internet from anywhere. The tendency to connect to the Internet everything from printers to central heating systems will continue. Just as people expand the ways they use the Internet, so the potential security risks multiply.

The malfunctioning of networks and information systems concerns everybody: citizens, businesses and public administrations.

Various events in the past, such as serious security holes in the operating systems on routers, denial of access attacks on web servers, intrusion into the routers changing RSVP parameters, and others, shook the networking community. The question is out there if network QoS and security are still orthogonal to each other or should one consider security as another QoS parameter and integrate it with the performance-related QoS results.

So the main question is "Can network QoS and security live in symbiosis or not"?

Our belief is that network QoS and security can live in symbiosis if security is put in the right places and at the right time. Problems such as protection of crucial QoS parameters during connection setup, protection of data packets during their transmission in a timely manner, protection against intrusion and denial of service attacks are only some issues which security and QoS need to consider when marrying each other. If security mechanisms, such as authentication, access control, encryption, denial-of-access-sensitive admission control, are enforced during the QoS connection setup, this should be sufficient to distribute the QoS requirements and provide proper resource reservation/allocation/ access in a secure fashion. If security mechanisms and policies at routers, gateways and firewalls, such as intrusion detection, digital signature and encryption with variable key lengths, scalable key management, security policy management are available, this could provide for a secure transmission path, content protection and end-to-end QoS provision.

As the bandwidth of data channels increased and transmission latencies were reduced, it became feasible to consider adding services with strict latency and jitter requirements to the internet traffic mix. One- and two-way audio and video are good examples. For these services to be considered usable, both the time between transmission and delivery (delay) and the regularity with which delivery occurs (jitter) must be carefully controlled. This is often done by reserving the resources necessary to ensure that the delivery goals are met. This can interact with security in a number of interesting ways:

- Services requiring assured delivery can deny service to services that are security (but not QoS) critical by reserving excessive resources.

- The protocols used for negotiating QoS agreements may be subject to attack or interference by non-participating parties.

- Security services such as encryption can prevent delay requirements from being met by introducing additional latencies. Algorithms whose timing is data dependent may introduce additional jitter, as well. Irregular operations such as re-keying may do this also.

- Security services can benefit from QoS measures, as well. To the extent that QoS measures limit delay and jitter, control of such features as a covert signaling measure is depreciated.

- To the extent that QoS operates under a business model that requires assurance of network management services for provisioning, auditing, and billing, the QoS mechanisms may well take advantage of existing network security services.

Yet to fully realise the advantages of the information society, people need to be able to trust the systems. This is why security is becoming such an important issue, but for the end user everything can be resumed to a single word QUALITY.

Then, Security is one of the criteria of the Quality of Service (QoS) together with other criteria such as the speed, the accuracy, the availability, the reliability, the simplicity and the flexibility. This is clear on ITU-T Rec. G.1000. According with this ITU-T Recommendation the quality of service (QoS) and, hence, the security features might define not only the communication session (i.e. the phases of the connection establishment, information transferring and the connection release) but also other phases of the relationship between Network and User (i.e. sales, pre-contract activities, service support, billing, network/service control by the customer etc.).

Network makes available for User the QoS level (including the security level) according to the agreement concluded between them. If Network could provide not one QoS level but a number of the *QoS classes* User may select the security level needed. Such selection might be used for one telecommunication session or for an agreed subscription period. In such a case the supplementary service is used for selecting the security level, as follows:

- The QoS class selection, or
- The security level selection, or
- The selection the value of any security dimension parameter.

The ITU-T Rec. E.860 proposes to conclude the Service Level Agreement (SLA) between the communication operator and User (and also between the communication operators). The SLA aims to define the characteristics of the service offered, the responsibility and the priority of each party. In fact, the SLA is the document dividing the responsibilities of both parties. It is advisable the security characteristics being provided by each party should be included into the SLA between the communication operator and User.

Inherently, QoS involves user requests for (levels of) services which are related to performance-sensitive variables in an underlying distributed system. For security to be a real part of QoS, then, security choices must be presented to users, and the QoS mechanism must be able to modulate related variables to provide predictable security service levels to those users.
This raises the question of whether it makes sense within the context of coherent system security paradigms to provide such security choices to users. It is also of interest to understand how the limits on these choices are defined, and how those limits relate to existing resource security policies.

The notion of security ranges may, at first, seem strange or even an oxymoron. For many, security is thought to be binary: either you have it or you don't. On a gross scale, this is true. Without some minimum level of security, a system will be considered inadequate for user requirements. Yet if a user's minimum requirements are met, can there not be some choice with respect to what *is* adequate? Our answer is "yes." As an initial example, suppose that a user requires medium assurance at end systems where a distributed task will be executed. If potential target platforms range between medium and high assurance, there is a choice. In fact, if the medium assurance system is over-subscribed while the high assurance system is idle, the user may realize better overall service by electing to execute the task on the high assurance processor.

Security and quality of service (QoS) are two critical network services in today's inter-networked world. Security mechanisms are used to provide proof of identity, preserve protected information, and ensure that information received has not been tampered with. Quality of service enables multi-media and other real-time services to use public data networks instead of more expensive dedicated networks.

Security and quality of service mechanisms are not independent. Choices of security mechanisms impact the effectiveness of quality of service and vice versa. Quality of service requires security mechanisms to ensure appropriate service assignment and billing. Poor security mechanism selection and placement can reduce the performance of a carefully queued network. Inappropriate service level selection can leak extra information about the importance of packets in the traffic stream, but clever manipulation of quality of service parameters might even help to reduce leaking of information through covert channels.

Without a good understanding of these interactions, poor network design choices may result in weaker than expected security and/or less effective quality of service guarantees. Therefore, both services must be considered together when designing and implementing a network infrastructure to achieve the best possible security and quality of service levels.

Both QoS and security are resource management problems and conflicting demands for limited resources are to be expected. Prior experience with similar problems indicates that the treating the conflicts as a risk management problem and applying the risk driven process model is a useful way to design and build systems that have conflicting requirements. Under this approach, risk factors, such as the resource conflict between QoS and security services, are identified at each stage of the development from requirements gathering to deployment and maintenance. Development does not proceed until adequate risk mitigation has been worked out. Risk mitigation techniques that are applicable to resource allocation and performance conflicts include analytical models, simulations, and prototyping.

Quality of service (QoS) and security services are both vital and affect the entire network infrastructure. While both services are necessary for safe and adequate network operations, in many organizations separate groups are responsible for security and QoS. However, security and QoS implementations will have an impact on each other. Without information about QoS requirements, a poor choice of encryption endpoints may reduce the effectiveness of QoS performance queuing. Without information on security requirements, a poor assignment of QoS performance levels may lead to denial of service for vital but low bandwidth data.

Therefore, QoS and security requirements must be considered together, but it is quite difficult to find people who are expert in both areas. A network policy framework can fill this expertise gap and identify conflicts in security and QoS requirements. Security and QoS requirements can be entered in to the policy framework through a single organization policy, or the security policy and QoS policy can be entered separately. In either case, if the policy framework has sufficient information about the network system, security requirements, and QoS requirements, the framework can resolve or at least identify conflicting requirements.

Enforcing both security requirements and QoS requirements can be viewed as resource allocation problems. When the policy framework is the single point that is solving both resource allocation problems, conflicts can be found or allocations can be altered to deal with the global set of requirements. When security or QoS requirements are considered separately some resource allocation decisions can be arbitrary. For example, when considering encryption requirements, two routers in the network may satisfy the security requirements equally well, but when QoS requirements are also considered, the choice may not be so arbitrary.

Current policy framework systems can adequately deal with static resolution of requirements for security or QoS. It is not a big leap to deal with security and QoS together. The policy framework systems will have to continue to evolve to deal with interactions between administrative domains, more dynamic network requirements, and new network services.

It is also clear that the security research community has recognized that user behavior plays a part in many security failures, and it has become common to refer to users as the 'weakest link in the security chain'. However, blaming users will not lead to more effective security systems.

Security designers must identify the causes of undesirable user behaviour, and address these to design effective security systems.

It is widely believed that security and usability are two antagonistic goals in system design. A classic example of this argument is passwords: systems without passwords are thought to be usable, but not very secure, while systems with long passwords that must be frequently changed are thought to be secure, but not very usable. We believe that this reasoning is flawed. Systems that sacrifice security for usability may work fine in the laboratory, but they fail when exposed to the hostile environment of the outside world. Alternatively, systems that sacrifice usability in favor of security fail because users disable the security features, or because the systems are used far less than they would be otherwise.

We support that for the majority of users and applications; increased security cannot be achieved with technology that decreases usability. Then, it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors."

In other words, it must to be easier to use security mechanisms than to bypass them.

Consequently, security and usability can be simultaneously improved by the adherence to a set of design principles. These principles can be inferred from a critical examination of existing systems and tested by relying upon them in the design of new systems.

It is concluded that existing human/computer interaction knowledge and techniques can be used to prevent or address these problems, and outline a vision of a holistic design approach for usable and effective security.

REFERENCES

[1] "Security Usability" – Peter Gutmann, IEEE Computer Society

[2] "Framework for Network Security«– ETNO WG on Fraud Control & Network Security

[3] "Transforming the weakest link – a human/computer interaction approach to usable effective security" - M.A. Sasse, S.Brostoff and D. Weirich, BT Technol J Vol 19 Nº3 July 2001

[4] "Aligning Security and Usability" - Ka-Ping Yee, IEEE Compiter Society

[5] "Usability of Security: A Case Study" - Alma Whitten and J.D.Tygar, CMU-CS-98-155

[6] "Overview of Quality of Security Services" – Cynthia Invirne and Tim Levin, Center for INFOSEC Studies and Research Naval Postgraduate School

Luis Sousa Cardoso is employed by Portugal Telecom. He is FIINA President, QSDG/ITU Chairman, ETNO - Head of Fraud & Network Security WG.

He was born in Lisbon, Portugal, in 1948. He was educated in Electronic Communications Engineering at Lisbon University and joined to CPRM-MARCONI in 1970 to work in the Network Operations area. He is currently a Senior consultant and is engaged as Quality of Service and Network Security Director within Portugal Telecom/Wholesale International Direction. His previous assignments have included technical and management positions in the areas of planning, quality control and traffic engineering, and revenue assurance. Since March 92 he is acting as *Chairman* of Quality of Service Development Group (ITU) and as Coordinator of Fraud Prevention Project. In addition he has been the Company representative in FIINA (Forum International Irregular Network Access) in which he became member of the Executive Committee during 1995 and was appointed as *President* in October 2001. He is participating in the ETNO Working Groups on matters as Information Security, Telecommunications Fraud Control and Quality of Service, and since September 2001 he is acting as *Chairman* of the Working Group on "Fraud Control and Network Security".

He has working as consultant in Quality, Revenue Assurance and Security areas, for several Telecommunications Operators.

He has served for four years in the Portuguese Army as a Management Engineering Officer. He has worked as a Consultant on the Telecommunications Security area for several companies in USA, Europe, China and Africa and acting as Vice President of the Portuguese National Quality Committee for Information Technology. He is member of the Institute of Electrical and Electronics Engineers, Inc. and of Computer Society. Since June of 1996 he is an active member of the New York Academy of Sciences.