March 2007

ETNO Reflection Document on "Baseline Security for Network Operators"

Executive Summary

The ITU-T Study Group 17 set up a Focus Group (FG) on Baseline Security for Network Operators with the objective to develop such security baseline. Participation in this activity is encouraged of members of other standards organisations, including experts and individuals who may not be members of ITU. An operators's implementation of the developed recommended practices may be a factor that other operators, users and law enforrcement authorities take into account in determining a network operator's readiness and ability to provide secure network services. The Focus Group is submitting for approval as ITU-T standard a new Recommendation, with the provisional title of X.Sbno, that could have an impact on the activities of ETNO Members. This paper presents an overview of issues that require resolution and a proposal for changes in the current text developed by the Focus Group.

The focus of this activity is the ITU-T Sector.

Issues

The current text of X.Sbno proposed by the ITU-T Focus Group and to be approved as a new standard represents the minimum set of recommendations whose implementation would guarantee a certain level of information security of communication services, at the same time maintaining the balance of interests of operators, users and the state.

Several issues are presented that have been identified as requiring further consideration. The issues are both specific, e.g. those related to operators entreprise security management, and general e.g. those related to the application of such recommendations.

Conclusion

In order to assist the ITU-T Study group 17 in developing further work on the document it is proposed that as a minimum clarification is given, and a model for Network Security is described in very general terms. In addition maintaining security is a continuous challenge. Just when a user thinks an airtight system is in place a new hacker technology or an especially diabolical adversary enters the picture. Regardless of the type or location of a perceived threat, an effective system for securing the integrity of information while maintaining availability of information assets must:

- Allow access to information by authorized parties only
- Implement policies determining who is authorized for what level of access to which information
- Employ a strong user authentication system
- Deny malicious or destructive access to any information assets
- Protect data from end to end

It is also felt that the current Draft X.Sbno, instead of being a future Recommendation, should be considered as a Supplement to Recommendation X.805 "Security architecture for systems providing end-to-end communications".

Proposal

To achieve the conclusions outlined above, it is proposed that this ETNO Position be used as a basis to make a submission to ITU-T Study Group 17 Question Q 4/17. The cornerstone of making such submission is to ensure the successful introduction of our views in any future standard developed on the basis on the current document and reduce the impact on our usual business processes.

NOTE: Annex 1 contains the first submission based on this Reflection Document, and is attached here for information. It is in standard ITU meeting document format and will be separated from this RD when addressing ITU.

Annex 1 Contribution on Issues related to SBNO

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

COM 17 – C XX – E

April 2007

English only

Original: English

Question(s): 4/17

STUDY GROUP 17 – CONTRIBUTION XX

Source: ETNO

Title: New ITU-T Recommendation X.sbno

Executive Summary

ETNO recognises the advantages to adopt as Supplement to Recommendation X.805 some recommendations based on the proposed principles described in X.sbno. ETNO considers that these principles must be agreed on as a common ground and enforced by all countries. The proposed recommendations describe a network operator's readiness and ability to collaborate with other entities (operators, users and law enforcement authorities) to counteract information security threats, and can be used by network operators to provide meaningful criteria against which each network operator can be assessed if required.

As our internationalised economy and social context are becoming increasingly dependent on communications networks, more attention must be paid to the security and integrity of the components and interfaces of this critical infrastructure - by all interconnected service providers, vendors and users. The old adage that the chain is only as strong as the weakest link has never been as true as it is today when applied to the issue of network security and integrity. It is with that tone that this Supplement should be written to help identify the potential information warfare threat and address the cascading vulnerable infrastructure on which the information superhighway is being built.

Position

A model for Network Security can be described in very general terms. A message is to be transferred from one party to another across some sort of network. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the network from source to destination and by the cooperative use of communications protocols by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission against an opponent who may present a threat to message confidentiality, authenticity, etc.

Maintaining security is a continuous challenge. Just when a user thinks an airtight system is in place, a new hacker technology or an especially diabolical adversary enters the picture. Regardless of the type or location of a perceived threat, an effective system for securing the integrity of information while maintaining availability of information assets must:

- Allow access to information by authorized parties only

- Implement policies determining who is authorized for what level of access to which information
- Employ a strong user authentication system
- Deny malicious or destructive access to any information assets
- Protect data from end to end

It is also ETNO's view that the current Draft X.Sbno, instead to be a future Recommendation, should be considered as a Supplement to Recommendation X.805 “Security architecture for systems providing end-to-end communications”.
Also we would like to call the attention to the Recommendation X.1051 – “Information Security Management Guidelines for telecommunications based on ISO/IEC 27002” that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications. This Recommendation provides a general guideline on the commonly accepted goals of information security management for telecommunications.
This is one more reason why we cannot recommend the use of document X.Sbno with a Recommendation status

Discussion

It is clear that the Supplement seems to be a simple statement of good practice which could apply to any IT based industry and not to telecom operators only. ETNO is not able to see how this Supplement takes things forward for telecommunications operators in particular.

In addition it seems that it is necessary to synchronize this draft with the ISO27000 family of documents. There is a need to look at the Draft-ISO/IEC 27031 and ITU-T X.1051 (2006-11-15). At least a check is needed to avoid unnecessary contradictions.

Another point that needs highlighting is that in the technical part – attention is very easily “guided” towards the Internet world. And what about other data networks – what about PSTN, ISDN, cable TV or mobile? In certain circumstances the protection of these networks may need the same or even more attention than the Internet world.

Other comments on the Draft document are as follows:

- Point 3.4 - *"It is recommended the operator installs updates and patches recommended by the manufacturer."*

Hopefully this does NOT mean that network operators - without further consideration - will update their systems as soon as patches are released from the vendor. In fact - Operators do have rather specific procedures implemented in this area (notifying customers, pre-testing a.o.). Also there is a “Time to patch” that is associated with the cost of patches implementation.
Patch management is a crucial component of security programs. An important problem within this context is to determine how often to update the systems with necessary patches. Keeping the systems patched with more frequent patch updates increases operational costs while reducing security risks. On the other hand, leaving the systems un-patched with less frequent patch updates decreases operational costs while increasing security risks. It is necessary to

develop a theoretical model to derive the optimal frequency of patch updates to balance the operational costs and damage costs associated with security vulnerabilities.

Given that patch management is costly and vulnerabilities are defects caused by software vendors, recently security experts started questioning the implications of cost sharing in patch management. Since firms currently bear the cost of patching, and firms cannot keep up with the sheer number of patches released by vendors every day, it may help operating firms if software vendors share this burden.

The argument is very simple: Since you do not have to pay to repair your car when a manufacturer defect such as faulty brakes is found, why should firms pay for the cost of patching? What if the vendor's release policy prevents the patch from being released? Then the question changes to a liability issue in security. Using the previous analogy, if faulty brakes cause an accident, the car manufacturer can be held liable in court. What if a server is attacked because of a specific vulnerability for which a patch has not yet been released by the vendor? Therefore we examine cost sharing and liability as possible coordination schemes to achieve the socially optimal levels of patch release and update cycles.

- point 3.9 - "*It's recommended that each front-end e-mail server has installed spam detecting system for incoming messages and possibility to mark the unsolicited advertisement*."

Also this sounds very rational - but... are Operators immediately capable to unambiguously decide what is spam? The filter either has to be very restrictive (so other than spam is captured) OR less restrictive (so some spam will pass through).

- point 3.15 - "*It's recommended to apply intrusion detection and intrusion prevention services (IDS/IPS) with the real time traffic checking and up-to-date signature base that allow selectively context users and other operators traffic checking*."

In general - the entire technical paragraph have to state more exactly, if the recommendations applies to operators own systems - or applies to products/services (for instance the customer-offered Internet Service). In fact - there is a major difference in implementing IDS/IPS on back-office systems or on the public IP networks.

- point 4.1 and 4.7 - *"It's recommended to have means to identify users, partners and other operators which are involved in the direct interaction"* and *"It's recommended the operator has a round-the-clock incident response team (IRT) or applies an outsourcing IRT service*"

Trusted inter-service-provider communication is also an important point. ETNO recognises the practical needs of communication in special circumastances e.g. priority communication services for functions such as emergency management, emergency support and emergency relief operations without disturbing the probably already difficult public services situation at that moment. For economically critical functions a major service improvement in critical situations could be expected if more diverse services would be implemented. The communications systems supporting emergency management, emergency support and emergency relief operations should be part of the national readiness systems**.**

- Extra point to be considered - *Consumer protection*.

Based on national regulatory and industry sector guidelines there is a need to protect customers (end-users, small, media and corporate businesses) and to protect service providers against risks that might exist using a network service. Measures are recommended to ensure that customer orders are verifiable down to their source. Also customers have a right to get informed about found network risks so they could take preventive and damage limiting measures themselves.

Finally, the document needs correction of the English wording by a native speaker (multiple misspelling of “its” instead “it is” or “it’s”…

Based on these comments, and bearing in mind that ETNO considers the document as a Supplement to Recommendation X.805 the following changes to the Draft document X.Sbno are proposed:

Draft X.Sbno – Security Baseline for Network Operators

To be used as Supplement to Recommendation X.805 – “Security architecture for systems providing end-to-end communications”

Summary

This ~~Recommendation~~Supplement – defines a security baseline against which network operators can assess their network and information security posture in terms of what security standards are available, which of these standards should be used to meet particular requirements, when they should be used, and how they should be applied. This ~~Recommendation~~Supplement – describes a network operator's readiness and ability to collaborate with other entities (operators, users and law enforcement authorities) to counteract information security threats. This ~~Recommendation~~ Supplement can be used by network operators to provide meaningful criteria against which each network operator can be assessed if required.

1. Introduction

The “Security Baseline for Network Operators” represents the minimum set of recommendations which implementation would guarantee a certain level of information security of communication services, at the same time maintaining the balance of interests of operators, users and the state.

Nowadays there are thousands of network operators, ranging from the old established national carriers (who have trusted each other to a large extent) to small, start-up networks with no track record and no real basis for establishing trust, new problems that did not exist in the traditional regulated environment have emerged. It is necessary for operators to know who

they are dealing with and the extent to which they can trust other operators to avoid the security problems. Security Baseline is the response for this new challenge.
Use of recommendations might be different from country to country, according to regulatory regime. Some regulatory regimes may wish to impose the recommendations that a certain level of the security be met as a condition of licensing. Some network operators may themselves require that other network operators meet certain level of security as a prerequisite to interconnection.
It is recommended that an operator provides telecommunication service for users with the security level that is guaranteed by the implementation of this Supplement.~~Recommendation~~.
The services of higher security level on client's demand may be provided by the operator at a cost to the user.
The set of recommendations is separated into three directions (operator's policy baseline, technical tools baseline, collaboration baseline).
All of the included recommendations are verifiable. Testing might be realized by an operator itself as a declaration procedure or with the assistance of the evaluation body through the conforming certification. A testing methodology will be designed additionally.

2. Operator's policy baseline

2.1. Its recommended the operator in accordance with the internal procedures approves security policy that is based on the best practice and risk assessment.

2.2. Its recommended the operator's security policy has a section dedicated to delimitation of the responsibility between the operator's staff, between the operator and its partners, and between the operator and its users.

2.3. Its recommended the information security aspects include in the labour contract (job specification, list of duties) for all employees dealing with the publicly-accessible information resources.

2.4. Its recommended an operator avoid methods of protection of its own and its customers' resources and such measures of counteracting threats, that may incur harm to third parties of the information exchange, or when the side effect of their application exceeds the damage being prevented.
2.5. – It's recommended ~~an~~ operators ~~will~~should publish ~~the~~ a security policy statement to~~p~~ inform customers and interested parties.

3. Technical tools baseline

3.1. Its recommended the operator applies any hardware and software in the strong correspondence with the license agreement conditions, defined by the manufacturer. The implementation of the users' and corporate users' hardware and software for network and communication facilities is not recommended.

3.2. Its recommended to apply only personal accounts to access to the management interfaces of the communication hardware. The usage of the group accounts is not recommended if the communication facility provides enough personal accounts unless the use of a group account is necessary (e.g. root).

3.3. Its recommended not to apply non-authorized access and default password (installed by the manufacturer of the facility or software) access to the management interfaces, operator interfaces or management and administrative accounts of any communication facility.

3.4. Its recommended the operator installs stable updates and patches recommended by the manufacturer.

3.5 – It is recommended that the operator shares with the vendors the cost of installing non-stable patches. Given that patch management is costly and vulnerabilities are defects caused by software vendors, recently security experts started questioning the implications of cost sharing in patch management. Since operating firms currently bear the cost of patching, and firms cannot keep up with the sheer number of patches released by vendors every day, it may help firms if software vendors share this burden.

3.65. Its recommended to separate strictly operations and management networks. the confidential information related to network management system is protected by the network security facilities or by using isolated network segments.

3.67. Its recommended to install all stub network gateways (including multihomed stub networks) anti-spoofing filters, which exclude packages transmission with return addresses, that are not belong to this network, as well as receiving packages with return addresses, that are belong to this network, or receiving packages with private and loopback (multicast) return addresses.

3.87. Its recommended that each front-end e-mail server has installed anti-viral software with up-to-date signature base.

3.98. Its recommended to have a possibility to deactivate infected messages by marking them and optionally delete.

3.109. Its recommended that each front-end e-mail server has installed spam detecting system for incoming messages and possibility to mark the unsolicited advertisement. Operators are free to implement other mechanisms to stop spam; e.g. disconnect the users affected by bots.

3.110. Its recommended that the operator should filter the network spam if it is not prohibited by national legislation.

3.121. Its recommended that each e-mail server has a possibility to limit the amount of the outgoing messages from one user in unit time for spam prevention (if it is not prohibited by national legislation).

3.132. Its recommended to have a possibility to limit the excess of the bound for the outgoing messages and to hold the sending till server administrator confirmation.

3.143. Its recommended to apply an automated system for discovering traffic anomalies on a statistical basis as an essential part of the billing verification system. For effective counteraction against DDoS-attacks it is recommended that such traffic anomalies analysis be used even if the operator does not use the billing.

3.154. Its recommended the operator to apply technical and organizational measures that allow finding the sources of the violations in security system (first of all – DDoS attacks) and allow blocking (deactivation) of the attacks.

3.165. Its recommended to apply intrusion detection and prevention services (IDS/IPS) with the real time traffic checking and up-to-date signature base that allow selectively context users and other operators traffic checking.

3.176. Its recommended to provide confidentiality of the transmitted and/or stored information of the management and billing systems as well as personal users' data and services provided (from the operator-user agreements).

3.187. Its recommended to store detected incident logs for a sufficient period to facilitate the investigation of incidents and to use correlation technical facilities for initial stream of events filtering to optimize logs.

3.198. Its recommended to have a possibility to filter or "blackhole" the undesirable users' traffic by means of regular facilities on users' demand.

3.20 It's recommended to have an implementation and ongoing verification of secure configuration settings on operations and management components (including firewalls, routers and servers).

3.2 It's recommended to adhere very strictly to security best practice (eg OWASP) in the design and development of applications/services provided to end users of the network [e.g. for customer self service capabilities].

4. Collaboration baseline

4.1 - Based on national regulatory and industry sector guidelines there is need to protect customers (end-users, small, mediuma and corporate businesses as well) and to protect Sservice providers against risk that might exist using a network service. Measures are recommended to iensure that customer orders are verifiable as coming frorm the right customer. Also customers have a right to get be informed about found network risks so they could take preventive and damage limiting measures themselves too.

4.1.1 Its recommended to have means to identify users, partners and other operators which are involved in the direct interaction.

4.1.2. Its recommended for each public content resource to have a possibility to determine the originating jurisdiction (that is, the territory or state in which the resource resides).

4.1.3. Its recommended for each public content resource to have a possibility to obtain information about its owner (administrator) to the extent allowed by the national legislation (that is, all credentials with the exception of those forbidden by law to be transmitted).

4.1.4. Its recommended the operator in case of losing the users', its own or interconnected operators databases shortly informs interested parties about the incident.

4.1.5. It is advisable that t~~The~~ operators ~~should~~ recommend to~~that~~ corporate users that they should have special staff members ~~who are~~ responsible~~s~~ for the security of corporate resources. ~~These staff should have enough qualifications and authority to counteract threats.~~

4.1.6. Its recommended the operator informs users on widespread threats aspects, connected with the service usage and content resources or provide users with a corresponding link to reputable resources on the item.

4.1.7. Its recommended the operator has a round-the-clock incident response team (IRT) or applies an outsourcing IRT service.

4.1.8. Its recommended the operator's IRT are accessible by phone and e-mail from the authorized under the operator's policy and/or agreement on the communication service users, partners and other operators. Incidents should be examined according to recognized best practices.

4.1.9. It is advisable to ~~establish~~ mention in the General Usage Conditions ~~in~~of the Service ~~l~~Level ~~a~~Agreement ~~established~~ with ~~U~~users ~~to~~a recommended ~~a~~ process ~~that~~ allowing~~s~~ the operator to speedily ~~shortly~~ inform~~s~~ users ~~and manufacturers~~ about discovered vulnerabilities of ~~the~~ hardware ~~(~~or software~~)~~ that can cause negative consequences. Similar information exchange system should be ~~applied~~ used with manufacturers.

4.1.10. It is advisable to recommend~~ed~~ to corporate users that they install anti-spoofing filters on their ~~(CPE)~~ Customer Premises Equipment (CPE) when they are using a boundary central processing element ~~(CPE)~~ facility.

4.1.11. Its recommended that shelf time of the logs is not less than the lawsuit limitation period and chain- of- evidence procedures should be maintained.
