Improving the Protection of Assets in Open Distributed Systems by Use of X-ifying Risk Analysis

Ann FRISINGER

The Royal Institute of Technology

Department of Teleinformatics

Email: afri@it.kth.se

Phone: +46-8-7931321

Mobile: +46-70-7931321

Key words: *Information security, data security, open distributed system, risk analysis, X-ifying factors.*

Abstract: *Open distributed systems operate in a networked global space where parts are owned by - thus can be controlled by - the local system owner, but most parts are shared globally. The system boundaries are fuzzy and we can only count the system owner to control his/her assets at some point of time. The generic system parts - those shared globally - are data oriented. The specific system parts - those owned by the local system owner - are information oriented. This fact should have impact on the way we view assets when setting the right security requirements. Many approaches focus only on the generic parts, i.e. to protect the data. They thereby overlook the informational aspect of the asset. In order to find these specific requirements, it is important to analyze the risks related to information so that it can be protected in a satisfactory way. This paper will describe how the problem can be solved by use of a risk analysis approach with so called X-ification. X-ifying is a way of mating together the best available experience with values appropriate for the local target system X. X-ifying factors differ depending on if you look at assets from a data or informational point of view. They also change in importance from asset to asset, from industry to industry and from person to person.*

1. Introduction

Creating security and mutual trust in an open distributed environment, like the Internet, where exchange of data is an emerging phenomenon are essential but difficult to establish. Open distributed systems operate in a networked global space where parts are owned by - thus can be controlled by - the local system owner, but most parts are shared globally. The system boundaries are fuzzy and we can only count the local system owner to control his/her assets at some point of time. The generic system parts - those shared globally where the local system owner does not have control and where assets float around as uninterpreted bits and bytes - are data oriented. The specific system parts - those owned by the local system owner and where s/he has control and is in charge of media where the asset resides - are information oriented. This fact should have impact on the way we view assets when setting the right requirements for security.

A common view in industry is that you can buy a black box with technology which solves all your problems with security. "The majority of defense dollars go for essential functions such as firewalls" [FOR98, p 4]. Many efforts aiming to protect assets in open distributed systems focus on the generic parts, i.e. to protect the data. This is valid for baseline security approaches such as the British Standard 7799, BS7799, Code of Practice for Information Security Management [BS7799, SIS99], and also for traditional first generation risk analysis methods which base the risk assessment on statistics from before and then focus on selecting countermeasures from an existing limited list of solutions [BAS93, HAM96]. They thereby set a basic level of security for the data. However they overlook the informational aspect of the asset, i.e. where a piece of data is interpreted by a human being, i.e. put into context, and turned into information that may need specific protection. In order to find these specific requirements it is important to analyze the risks related to information so that it can be protected in a satisfactory way, considering also the costs that would entail.

The requirements for security differ from asset to asset, from industry to industry [FRI00b] and from person to person [JON99]. We call the variations X-ifying factors [FRI00b]. X-ifying factors could be wise to consider in a risk analysis. We can see that X-ifying factors also differ depending on if you look at assets from a data or informational point of view.

This paper will discuss the dilemma that asset's informational values are often overlooked when deciding the requirements for protection in an open distributed system. It will describe an approach to overcome that problem by utilizing risk analysis with so called X-ification. Furthermore

it will describe how these X-ifying factors differ from industry to industry and from person to person and how this impact the view of the asset values.

2. Information needs specific protection, data needs generic

System theory is a scaleable concept that gives a possibility to integrate delimited parts into a whole system, where sub-systems play together with relations and interactions. This is a base for a holistic perspective. A holistic approach is recommended as an instrument to structure the sub-systems into an integrated whole before the final solution is put into reality. This is to avoid that piecemeal security solutions are applied to isolated problem areas where no consideration is given to the integration [YNG96, FIL99].

In efforts to control, humans may choose to either assume that the reality is a system or could be looked upon as a system through the learning process i.e. humans can learn how the concept of a system reflects the real world. The control method in the first case could be labeled systematic engineering or hard systems thinking. The second one systemic or soft system thinking.

In soft systems thinking (the epistemological science) where we explore intangible areas that are difficult to capture, perceived realities are treated as problems and are solved in a systemic way. Soft systems thinking focus on the need to synthesize and to use induction to create value. It encourages an open living approach to open dynamic research objects [YNG96, MAG99]. This gives a possibility to delimit into subsystems, and to control when to move from a soft systems approach to a hard system approach going systematic. In addition to the holistic perspective a systemic approach is needed. When combining the systemic with the holistic view, the approach brings some useful principles [YNG96, p27]:

- Delimit the system of study from the environment,
- Define the existing environment,
- Define the inflow, throughflow, and outflow, and
- Structure the built-in control system so that it can deal with inner and outer variety,

In hard systems thinking (the ontological science) perceived realities are treated as existing systems and their problems are solved by systematic methods [YNG96, MAG99]. Deduction and proofs based on

exact rules of procedures are foundation for ontological science. A systematic or synonymously methodical approach can be defined as an orderly, regular procedure for obtaining an object.

[FIL99, p199] says “Information security is contextual in nature, and difficult to view as a system in itself” and Information security is contextual and not systemic” [FIL99, p187]. We agree that information security is contextual but as opposite to [FIL99] we see that open distributed emergent systems are well suited to be approached by soft systems thinking, where the meaning of the data is related to a context thus forming information.

The systemic view enables us to focus on our assets as information where we can control them and set specific security requirements for them. When dealing with parts that we do not control, we can still keep our requirements for assets that were decided when we took the informational view, but we have no control that the owner of the media where asset travels/resides will meet our desired level of protection, unless we find a way to totally encapsulate the asset. Similarly we will in our system host assets that are owned by others, thus we see those assets as data or we make our own interpretation of those asset’s values, however those might not agree with the owner’s wish, unless very clearly specified. To be able to set a basic level of security for hosted assets etc. it is recommended to take a systematic approach (hard systems thinking). Perhaps take help from a baseline security approaches such as the BS7799.

Soft systems and hard systems thinking are complementary to each other. The systematic and methodical view represents reality, stability, and consistency while the systemic and amethodical [TRU00] view represents interpretation, change and encourages innovation that leads to adaptation.

While a systematic approach would encourage the risk analyst to find patterns from the past to build future trends for incident risks and costs, the systemic and amethodical approach would guide us to adapt the best available experience.

The systematic approach is used in traditional approaches to security and usually produces solutions for data. When combined with a systemic and amethodical approach it is possible to also focus on information, thus produce specific solutions for assets.

3. How risk analysis with X-ification adds value

X-ifying is a way of mating together the best available experience with data appropriate for the target system X [FRI99]. System X is an open distributed system and X is the first system in its generation. X' is the successor of system X. The customizing data can be an assessment of asset attractiveness, actor capabilities, system and media vulnerabilities, and business values. By utilizing X-ification capabilities, we can compensate for errors and disbelief in estimates, non-existing or outdated experience numbers. The X-ification considers the meaning of the data, i.e. information, and adapts the best available previous experience (statistics) to the local application area.

A risk, R, can be calculated as the product of probability, P, and cost, C according to formula 1 [FRI00a]:

$$(1) R = P * C$$

The probability P and the cost C can each be compiled as the product of various elements, according to formula 2 and 3:

$$(2) P = \{(Capability_of_actor * Attractiveness_of_asset) * \\ Vulnerability_in_media_where_asset_resides\} * \\ Method_of_operation_used_to_force_the_system * \\ objective_of_actor$$

$$(3) C = (Direct_loss_value * Cost_to_recover_repair) * Indirect_cost$$

The various parameters and operations in the formulas can in a more or less extent be utilized when performing X-ification in a risk analysis. The range of the X-ifying effect depends much on the usage. If we for instance decide to use assessed values when calculating the first part of probability for attack, i.e. $\{(Capability_of_actor * Attractiveness_of_asset) * Vulnerability_in_media_where_asset_resides\}$, and if we then could find values for the second part, i.e. $\{Method_of_operation_used_to_force_the_system * Objective_of_actor\}$, that are based on prior experience, those could be used as an index key where the index sums up to 1 (i.e. what is the distribution if hit by an incident). With help of the index, linguistic variables and fuzzy set theory, we can transform/calibrate the assessed probability values into new. There are also other ways of consolidating risk/probability values into one. In [VEN99] the consolidation of the risk values was performed by calculating the average of risk values. The way you do it, the importance and weight you give to different parameters, will impact the result and the level of X-ification.

This method of splitting a variable into two, one representing an assessed value and one representing a statistical value (or best available experience from the past), could be done for several elements in the formula, depending on availability of values. We call it X-ification.

4. X-ifying factors' dependency on industry and person

X-ifying factors are useful in risk analysis, especially when considering information oriented aspects. The factors differ from industry to industry and from person to person.

Different sectors and application areas have specific features that would make it possible to use a generic model for risk analysis but apply an X-ified factor. This requires the analyst to know what differs a specific system from an average system. [FRI00b] looked at high level factors with influence on security which were labeled X-ifying factors. The research, performed in form of a survey, showed there exist characteristic factors that differentiate between industry sectors. For instance, there are more hackers in university environment, the security awareness is generally higher in bank and finance sector, and the result of an incidence within the healthcare sector could be disastrous with impact on human lives, etc. Table 1 shows a summary of assessed values of X-ifying factors/parameters for the selected industry sectors of bank&finance, education, government, healthcare, IT&telecom, manufacturing, sales&distribution. The assessed values, based on answers in the survey, for an industry sector relative the average system and are given by linguistic variables {l=low, m=medium, h=high}.

These characteristic areas could be translated into a weight in the risk analysis algorithm in the following way, for example propose that for a bank the direct cost should be weighted higher in the algorithm and indirect cost would be weighted much higher than the average system, while vulnerability level is lower due to high security awareness and well developed systems. This varies then from a university where the direct cost and indirect cost should be weighted a bit less than the average system while the vulnerability level should be weighted higher than average, due to low security awareness and a lot of hackers playing with the system. The information could be utilized as a source of ideas when X-ifying in a risk analysis and when bridging values from one industry to another.

X-ifying parameter	Bank & Finance	Educ.	Gover nment	Health care	IT & Telco	Manufact	S&D
Capability_of actor	m	h	h	l	m	l-m	l
Attractiveness_of_asset	h	l-m	h	l-m	m	m	m
Vulnerability_in_media_where_asset_resides	l	h	l-m	m-h	m	m	m-h
Direct_loss_value	h	l	m-h	h	m-h	l-m	l
Cost_to_recover_repair	m-h	l	m-h	h	m	l	l
Indirect_cost	h	l	h	h	m	m	m-h

Table 1: X-ifying parameters for industry sectors

A work to provide an understanding, verification, measurement, and prioritization of users' security requirements in a networked education system was performed in form of a survey, a web based questionnaire, divided into three parts investigating confidentiality, integrity, and availability aspects. The survey was targeting different selected user groups; teachers, students, system administrators. Each part of the survey included a number of scenarios where each scenario related to an asset (information) and which could afterwards be translated into a security requirement for that specific asset [JON99]. The study showed that users have high expectations on security in the selected system. Integrity of the assets was estimated very high, whereas availability of systems and assets was rated almost as important as integrity, and the confidentiality aspect was also valued quite high.

The [JON99] study also showed that different users values assets differently depending on how they are related to them. If the user can put the asset/data into context it is valued higher than if the opposite shows. If the asset is seen as data only, the user only requires it to have some generic protection. X-ification can in this case add a contextual view of data as well as the opposite, it can add a generic view of information. Thus it balances the two views and ensures both aspects are considered before a solution is selected and implemented.

5. Practical experience of using X-ification

A generic method for performing security evaluations of open distributed systems was developed in [FRI99]. The method was generic enough to handle all types of systems, real as well as virtual (i.e. emergent systems or system in a development stage). It enabled successive evaluations, invited feedback from the past and adjusted systems over time. One of the novel features of the method was the X-ifying capability.

The method was tested on a networked reference system in the education sector, but the method is general enough to handle other types of systems, for instance X. The education system, called NED, was evaluated twice, first in its virtual version, then in its real existence, i.e. the first generation of its kind. In the test of the NED, the general evaluation method was adjusted by "NED-ifying" our criteria. The NED-ifying capability introduced both testability and context into results. The method integrates thereby whatever objective and subjective data available with the aim of making the best possible decision within limited time and other resource constraints

During the first evaluation, NED was a virtual system and we did not have any NED incident related data but used the best available statistics from another system as an index thus blending it together with our own assessments for probabilities. The second evaluation used recently collected NED incident related data and we used that in a similar way, i.e. as an index melting it together with assessments. The second evaluation suggested to collect new incident data and limit the time span for the index key to 6-12 months in order to let the experience base reflect recent reality. In both cases the number of incidents used as experience was small. The experience from collecting incident related numbers from the NED system, supported also by previous studies like [BAS93] and [HOW97], indicates that seemingly low incident numbers is a fact to live with (during a six months period we managed to collect 12 incidents). This is especially true if the time for collection is short. We find the number of incidents sufficient to use as check and balance in the NEDification provided reevaluations are repeated on a regular basis. If not done so often, but still on a regular basis, the incident numbers will increase, but then the experience will not be recent and a risk is that the system has evolved much since starting collecting data. A suggestion would then be to balance experience collected from systems, say X+ X'+ X" with recent data from X" and apply it for X".

We used the knowledge of users' security requirements when forecasting costs. We divided the cost into a direct cost and an indirect cost. Furthermore the direct cost was split into a direct loss value and a cost to recover and to repair. We let the opinion of the owner of assets (teachers) reflect the direct loss values, we let the opinion of system administrators reflect the cost to recover and to repair, and lastly we let the end-users (students) decide the indirect cost values. We believe this approach is very suitable to use in environments where the costs or other impacts by tradition has not been estimated before (e.g. education sector) or where consequences are difficult to quantify due to their non-financial nature (e.g. health-care sector), although the approach is generic and could be useful in all sectors.

All in all we experienced that the integration of whatever objective and subjective data available was practical and helped us make the best possible decision considering both the data as well as the informational aspect of assets.

The method enabled the system to adjust to current reality over time where protecting system measures that are hit by many incidents could be replaced by new generations of protecting measures (this is excluding the event of system hit by a very severe incident with a high-level of damage, which will have impact on most of the protecting measures). The protecting measures that are best suited to solve the problem will be promoted to be used in the next version of the system.

7. Conclusions

A starting and essential point for creating security and mutual trust in an open distributed environment is to set the security requirements correctly for assets from the start and then monitor changes regularly.

In this paper we have discussed the importance of addressing both data and informational aspects of assets when setting the security requirements and how this can be achieved by use of a risk analysis with so called X-ification capability. Table 2 shows a brief comparison between data and information.

X-ifying factors differ depending on if you look at assets from a data or informational point of view. They also change in importance from asset to asset, from industry to industry and from person to person. It is thus important to be aware of the differences between how assets are viewed, as data or information. These differences should then be considered in the risk analysis. The outcome of a risk analysis which uses

X-ification techniques will be a prioritized list of security requirements which will balance a data and informational aspect of assets.

Data	Information
Data is uninterpreted bits and bytes	Information is data that is interpreted by someone and put into context
Data has generic value	Information has specific value varying from person to person, and from industry to industry
A methodical approach can be sufficient to decide generic security requirements with focus on media where data resides, e.g. baseline security or early generation risk analysis methods	Methodical approach with amethodical elements is required to decide specific security requirements with focus on the meaning of the data, e.g. risk analysis with X-ification
The media owner implements generic and specific protection based on requirements	The information owner sets specific requirements for protection

Table 2: A comparison between data and information

References

- [BAS93] Richard Baskerville, 'Information Systems Security Design Methods: Implications for Information Systems Development', 1993, ACM Computing Surveys, Vol.25, No.4, pp.375-414.
- [BS7799] BS7799: Code of Practice for Information Security Management, British Standards Institute 1995
- [FIL99] Helen Leslie Fillery-James, 'A Soft Approach To Management of Information Security', July 1999, Doctoral thesis, Curtin University of Technology.
- [FRI99] Ann Frisinger, Louise Yngström 'An approach to standardizing security analysis methods for virtual systems', IFIP WG11.1&11.2, Amsterdam, Sept. 30 1999
- [FRI00a] Ann Frisinger, Louise Yngström 'An approach to use knowledge about user's security requirements in a risk analysis', accepted paper for IFIP World Computer Congress 2000 -- Information Security, Beijing, Aug. 2000.
- [FRI00b] Ann Frisinger, 'An assessment of how high level factors with influence on security in an organization differ from industry to industry', NORDSEC 2000, Oct. 12-13, 2000, Reykjavik, Iceland.
- [FOR98] Forrester Research Inc. report by Carl D Howewith, John C. Mc Carthy, Tom Buss, Ashley Davis, "Economics Of Security", February 1998.
- [HAM96] Gustaf Hamilton, 'Risk Management 2000', Studentlitteratur 1996, ISBN 91-44-00082-0.
- [HOW97] John D. Howard, 'An Analysis Of Security Incidents On The Internet', Ph.D. dissertation, Carnegie Mellon University, April 7, 1997, URL: <http://www.cert.org/research/JHThesis>.
- [JON99] Katarina Jonsson, 'Users' security requirements in the Networked Education process' master thesis, September 1999, DSV, Stockholm University

- [MAG99] Christer Magnusson, 'Hedging shareholder value in an IT-dependent business society', December 1999, Doctoral thesis, Stockholm University, ISBN 91-7265-011-7.
- [SIS99] SIS Svensk Standard SS627799-1: 'Ledningssystem för informationssäkerhet - Del 1: Riktlinjer för ledning av informationssäkerhet (Information Security management - Part 1: Code of practice for information security management)', 1999
- [TRU00] Truex, D., Baskerville, R., and Travis, J. 'Amethodical Systems Development: The Deferred Meaning of Systems Development Methods.', 2000, Accounting, Management and Information Technology, 10, 53-79.
- [VEN99] Hein Venter, Les Labuschagne, Jan Eloff, 'Real-time risk analysis on the Internet: a prototype', IFIP 1999, WG11.1 (Information Security Management) & WG11.2 (Small Systems Security), Amsterdam Sept 30 - Oct 1, 1999.
- [YNG96] Yngström Louise, 'A systemic-holistic approach to academic programmes in IT security', Oct. 1996, Stockholm University/Royal Institute of Technology, Report series No. 96-021, ISSN 1101-8526, ISRN SU-KTH/DSV/R--96/21--SE.