VTT RESEARCH NOTES 2589

Pasi Ahonen

Constructing network security monitoring systems

MOVERTI Deliverable V9

VTT TIEDOTTEITA – RESEARCH NOTES 2589

Constructing network security monitoring systems

MOVERTI Deliverable V9

Pasi Ahonen

MOVERTI – Monitoring for network security status in modern data networks
(A project funded within TEKES Safety and Security Program)

ISBN 978-951-38-7769-9 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 5, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

Pasi Ahonen. Constructing network security monitoring systems (MOVERTI Deliverable V9). Espoo 2011. VTT Tiedotteita 2589. 52 p.

Keywords network security, monitoring systems, data networks

Abstract

This report analyses and describes the basic construction of network security monitoring systems. The viewpoint is mainly research perspective, we aim for defining system constructions or elements which are also commercially relevant, but still maintain the open minded approach of research oriented work. The focus is on clarifying the overall network security follow up, but also on methods for investigating the “difficult to identify” or zero-day attacks or the preparation of such attacks, which try to exploit the application vulnerabilities that are currently unknown to operators and software developers.

The necessary network security system construction depends much on the operator’s targets for security monitoring. The threat environment of some specific operator may require a deeper analysis of the output from various security device logs, events and alarms. The needs of such operator may be to adjust the different alarm thresholds for the security devices accurately, according to the evolving network data traffic characteristics. Another operator, instead, would require holistic security monitoring of the production area, where e.g. the status information within physical access control systems and electronic access control systems shall be combined, and the aggregated summary results shall be presented to the operator for sanity checking.

Therefore, we present in this report some building blocks that can be used to construct a security monitoring system, not a complete system that shall be feasible as such for all possible security monitoring needs and requirements.

Contents

List of figures

List of tables

Terminology

AV	Antivirus
CC	Common Criteria
CPU	Central Processing Unit
CSRF	Cross-Site Request Forgery
DB	Database
DDoS	Distributed Denial-of-Service
DMZ	Demilitarized-Zone
DoS	Denial-of-Service
ESP	Encapsulating Security Payload
FW	Firewall
GMM	Generalized Method of Moments
HMM	Hidden Markov Model
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IaaS	Infrastructure-as-a-Service
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
O&M	Operation & Maintenance
OS	Operating System

RF	Radio Frequency
RSS	Really Simple Syndication
RTT	Round-Trip Time
SCAP	Security Content Automation Protocol
SFTP	Secure Shell File Transfer Protocol
SIEM	Security Information and Event Management
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SVM	Support Vector Machines
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
WAN	Wide Area Network
XSS	Cross-Site Scripting

1. Introduction

1.1 Challenges & needs

For what purposes the network security monitoring is currently needed? The needs shall vary, of course, depending on the case. The rising trends in the technological development and also in attacker environment have introduced many serious challenges which may be difficult to cope with, such as:

- Actions of organized cyber criminality
- Easily available attack- and exploit development tools
- Exploiting the zero-day weaknesses of complex applications due to large attack surface
- Appearance of botnets, fraud, wikileaks, blackmailing, distributed denial of service (DDoS) attacks, etc.

So, the main problem is perhaps that the operating defences of the network should be able to protect not only against fully targeted specific attacks, but also against massive information overflows, etc. Therefore, there are various strong needs in order to maintain the secure network management and operation. Such needs include, among other things:

- International co-operation for knowledge sharing
- Efficient security vulnerability and patch management
- Off-line analysis of recorded data & network based forensics after illegal activity
- Governance, contracting and co-operation procedures of vendors, partners and operators.

The feasible network security monitoring system construction depends on the operator's targets for security, but at the same time on the concurrent threat and risk environment where the network is operating.

1.2 Threats

1.2.1 Different threat environments

The different threat environments exist – In certain operator environments, where the system data communication is the only major security concern, and the system is based on the usage of public networks, such as the Internet, the threat landscape of the system may be much the same as that of the Internet. As the Internet applications are much based on the usage of web technologies, it is perhaps relevant also here to emphasize on the web based threats. The major web application security risks include, for example: i*njection flaws* (e.g. SQL, OS, and LDAP injection), *cross-site scripting (XSS)*, weak *authentication & session management*, insecure *object references*, *cross-site request forgery (CSRF)* and poor *security configuration*, see http://www.owasp.org/ for more. For such network operator, these risks often require a closer analysis of the output from various (security) device logs, events and alarms, and perhaps also from network data captures and net flows. For example, the operator may need to adjust the different alarm thresholds for the running relevant security devices & software accurately, according to the evolving network data traffic characteristics. Otherwise, the bulky and complex flow of different notifications, events, alarm messaging shall be impossible for the operator to manage and utilize online or even offline.

However, another operator, instead, would require holistic security monitoring for the corporate wide, global production e.g. of parcelled goods, bulk material, or energy production. There, in the multi-vendor and multi-operator production field, the cyber security of a device is not the only factor to worry about for the responsible global utility security administrator. (Even though, the information security systems really require proper maintenance and updating effort.) For example, the status information from the *personnel access* control systems, production area *physical environment* conditions & surveillance, *diagnostics*, and devices *electronic access* control systems need to be made available and used effectively. The aggregated summary results should be presented to the utility operator personnel for sanity checking and for possible corrective actions. The main target of the global operator is to ensure the consistent public safety and the continuous operation, both for the local and global responsible production business. Hence, the information network security is just a small portion of the overall responsibilities of the operator.

Numerous of other relevant “use cases” for networked security monitoring systems could also be described here, but they are omitted here for practical reasons.

1.2.2 General threats in networks

Next, we list some generic threats that may exist in current fixed and wireless networks. The main reference that we used in constructing the table below was Annex A of ISO/IEC 27033-1:2009, Information technology – Security techniques – Network security – Part 1.

Threats in networks

Table 1. Some general threats in common networks.

	LAN – Local Area Network	**WAN – Wide Area Network**	**Wireless LAN**	**Radio networks**
Intrusion, unauthorized access and modification of devices, attacks towards network management systems or gateways	X	X	X	X
Un-patched devices, poor patch management	X	X	X	X
Hardware failure, device failure, cable failure, power failure, misconfiguration of switches, physical security	X	X	X	X
Rogue access points	(x)	(x)	X	X
Unexpected latency, jitter	X	X	X	(x)
Eavesdropping, traffic analysis	X	X	X	X
(D)DoS attacks	X	X	X	X
RF jamming		(x)	X	X
Session hijacking	X	X	X	X
Fraud	(x)	(x)	(x)	X

NOTE: The estimated major threats are indicated with “X” and minor threats with “(x)”.

1.3 Trends

1.3.1 Concurrent trends in information network infrastructure protection

It is commonly believed that the intruders remain to have some advantage over the analyst, i.e. intrusions seem inevitable also in the future. However, let's still have a look on data networking security trends, or more generally, the trends in information network infrastructure protection. We might conclude that (See a book by Richard Bejtlich *"The Tao of Network Security Monitoring, Beyond Intrusion Detection"*):

- Data network management shall be security enabled
- Endpoint protections have been developed and are converging
- Concentrated, focused attacks are still difficult & resource consuming to avoid
- Protection "in-the-cloud" has been emerging
- Technology (e.g. IPv6) migration continue further and adds some challenges, e.g. doubled security policy and new threats in devices
- The crime investigation demands network based forensics
- The trend for acquiring automatically knowledge of network internal behaviour (e.g. flow details) has increased.

If we look after the protective status of today's networks, we can see that there are already several specialized protection technologies in use, or soon coming into use:

- Firewalls, deep packet inspection firewalls
- Log monitors, data traffic monitors
- Network intrusion protection systems, event management & sharing
- Safeguarding against (D)DoS attacks
- Security enabled web gateways
- Security within cloud services and networks
- IPR management software (e.g. usage and licensing of software rights).

However, concurrent solutions are not good protection forever. For example, a deep inspection firewall perhaps handles its limited role well, but shall not be effective for capturing some of the new threats, such as zero-day attacks and insider abuse.

The future trends in network security monitoring include:

- Remote packet capture & Centralized analysis
  - The need to collect content & session related data for evidence collection in forensics cases
- Integration of several security assessment tools
  - Integrating and comparing the attack data of several security assessment tools with target's known vulnerabilities
- Increased network awareness
  - Developing formal models for valid traffic patterns so that new devices or new traffic types shall be detected
  - Watching for unauthorized or suspicious activity within nodes and inside the network; any network infrastructure product may be attacked (router, switch, etc.).

2. Constructing network security monitoring systems

2.1 The purposes of network security monitoring systems

The basic reasons or objectives of particular network security monitoring system may include a wide variety of different purposes for an organization. Some organizations might just need to follow up that their current security enforcement systems are fully operational. Much on the contrary, other organizations might even collect special background information for the purposes of planned risk analyses in the future.

The purposes of network security monitoring systems may include, for example:

- Network security & continuity *level or status monitoring*
- Security *attack detection & defence*
- Security *enforcement system follow up*
- Security related *event monitoring*
- Attack or problem *alarming*
- Security vulnerability *identification*
- Security vulnerability or risk *mitigation*
- Risk analysis *information gathering*
- *Gathering experience* for protection development
- *Follow up* of configuration *conformance.*

When considering the procurement process for network security monitoring systems or elements, the organization should consider defining the feasibility criteria for vendors and service providers. Such criteria could include wide variety of special topics, such as (not a complete list):

- System security requirements, product security certifications
- System performance requirements, scalability issues
- Costs of purchases, licenses & continuous operation
- Operation and maintenance support & services, upgrading & updating
- Extension capabilities & services, future proof system architecture
- Deployment & commissioning issues, recovery from failures
- Security of communication and database services & techniques.

2.2 Basic principles

The construction of a network security monitoring system shall vary a lot depending on the operational or organizational case. For example, in some cases the security monitoring may be focused more on tracking of system logs but not so much on the network data traffic analysis. Naturally, this will affect strongly to the needed investments for monitoring equipment & software. Also, the results of security risk analysis, operational needs & limitations will affect strongly to the construction and technical properties needed to fulfil the security monitoring need for a particular case. To summarize, the main reasons for the large variability of technical requirements include:

- Different security needs and capabilities in organizations & operations
- Different assets and valuables to protect
- Different threat environments against the networked systems.

2.2.1 Design principles of network security monitoring

Someone may claim that securing a network doesn't require much more than someone to manage the firewall rules and access control lists, and to maintain and update such rules whenever needed. They might continue perhaps by claiming that the network security monitoring is a rather simple task. However, we don't agree with such claims for any operating networks with some reasonable business value, mostly because those few simple security solutions are only providing network protection in one or two different layers of security. For example, the lack of layered protection often leaves plenty of unguarded room for e.g. an insider to prepare & operate some malicious tasks.

In order to successfully design a network security monitoring system for a specific purpose, we need to write down and take into use some basic principles and tasks that shall guide us through the process. A typical process constitute of *feasibility analysis*, *design*, *procurement*, *implementation*, *configuration*, *deployment, operation & maintenance (O&M)* and even *disposal* of such a monitoring system. Note that the party who should carry out each task below might be the operator of the network, but depending on the case, often the relevant ICT support personnel, representative of vendor, system integrator, developer, etc., should be invited to participate in such a process as well. The basic principles or tasks to apply in each step for successfully designing a feasible network security monitoring system shall include:

2.2.1.1 Feasibility analysis

The feasibility of a network security monitoring system is mainly dependent on the value of operation & assets, which shall require security guarding in some level. The requirements for continuous operation & the value of related assets must be balanced with the security assurance efforts & investments. However, the budget is not the only limiting factor here, also the legal and regulatory requirements and restrictions must be resolved for the country or region where the security monitoring system is to be planned for.

Of course, the technical & operational risk landscape must be investigated for the planned networked system, its operation & personnel. This threat & risk analysis should be carried out by a wide interest group that allocates team members e.g. from the company's management, production, operator, security, admin, IT, acquisition, and also possibly appropriate vendors & service providers.

The essential issues in the feasibility analysis & design phases are the motivation for (proactive) security assurance in all layers of the organization, and the adequate competence & security training programs for personnel and at partners and subcontractors. The motivation starts from the management's commitment to systematic security improvement. The feasibility analysis work for a network security monitoring system should also include the tasks listed in following table:

Table 2. Feasibility analysis for network security monitoring system.

Area	Principles/Tasks
Feasibility analysis	First, clarify and list the main assets, goals and critical operational criteria of the networked system & data to be protected using monitoring and other controls.
	Ensure the sufficient intake and implementation of critical requirements, e.g. protection against new risks & threats, during the whole lifecycle of the system. Invite participants from all relevant areas for the risk & requirement analysis work.
	Define the major things that need to be monitored in the network. Divide these into the *baseline attributes* that are continuously monitored, filtered and prioritized, but also to detailed logs that shall constitute the *basis for forensic* analysis (e.g. of information leaks).
	Identify the best products & references of security monitoring and analyse how these match to your goals for monitoring.
	Analyse the feasibility of candidate monitoring platforms according to your critical operational criteria.
	Decide whether the required security monitoring investments & operating costs are in balance with the benefits of operation continuity and the value of business assets.

2.2.1.2 Design

If the previous feasibility analysis proved that the networked system should be complemented with a security monitoring system, how such a monitoring should be designed? The most important point is, of course, that the designed system shall be reliable and practical enough for effective network security monitoring within the organization. Because the networked environment is often rather complex and difficult to maintain, other important design requirements include the simplicity of operation & maintenance and standard extensibility/upgrading capabilities, which enable for future-proof security monitoring functionality.

The architectural design of the monitoring system is a key factor for its continued success. The standard communication architecture, including the specification for protocol stacks and data presentation formats, shall ensure the scalability of the solution also in the cases of competitor acquisition, etc. For example, web-based architectures and messaging applications independent from underlying communication technology are probably very feasible solutions also for

large scale security monitoring data exchanges. Data storage, on the other hand, should be designed with enough redundancy, backup, and recovery capabilities in mind. Single points of failure are to be avoided, even in centralized solutions.

Last but not least, it is very essential how the selected mature monitoring technology (hardware and software) platforms & standards shall be applied into practise. E.g. what security properties are utilized? What kind of authentication and authorization systems shall be taken into use for secure access and maintenance? What security protocols shall be used? Using which algorithms & key lengths? Standard, publicly assessed standards should be selected and certified vendors selected.

In addition, during the design phases of your network security monitoring system, you should consider to carry out the following tasks:

Table 3. Design of network security monitoring system.

Area	Principles/Tasks
Design	Ensure the scalability of your security monitoring system & operation using open standards and scalable architectures that have proven cost efficiency
	Divide the analysis tasks of monitoring results based on your strengths and topology, e.g. using local *internal analysis* and suitable *external services* for your particular security monitoring goals
	Ensure the secure design of the monitoring system elements by using & mandating defined security assurance methods, tools & processes for the monitoring platforms and products
	Ensure the correct focus for the security monitoring functionality by carrying out repetitive reviews with users and process owners

2.2.1.3 Procurement

The networked systems constitute of various devices, hardware, middleware, system software, management software, application software and perhaps involve usage of outsourced services, as well. Therefore, it is crucial to consider the security requirements before committing to large scale network infrastructure investments. Organizations should define “baseline” security requirements and capabilities that any purchased item should fulfil, while feasible. The security

requirements concerning procurement include such areas as logging functionality, log format & -capacity, secure SW updating & maintenance, strong device & user authentication, security protocol support, vulnerability follow up and perhaps 24/7 support for continuous operation. The mutual contracting about the key service elements is important in ensuring the security and continuity of delivered network products & services.

Especially, the critical area of subcontractor management has turned out rather problematic in many organizations. There is a clear need to synchronize the operation and maintenance policies and procedures according to user organization's requirements. However, often the secure management requirements and practices are not adequately defined and mandated for partners by the user organizations. Also, the penalty driven contracting using e.g. service level agreements (SLA) which include security, continuity & recovery requirements attain today too little emphasis. There is a real lack of security emphasis in many of the contracting cases for provisioning of network services or Infrastructure as a service (IaaS) contracts.

When considering company's procurement process from the viewpoint of network security monitoring, one should consider involving the following tasks:

Table 4. Procurement for network security monitoring.

Area	Principles/Tasks
Procurement	Define the baseline requirements for the security monitoring functionality that shall be used in purchasing network equipment, systems and software. Follow the standards and your targeted needs for the requirement baseline creation
	Estimate your future monitoring needs and question & explore the candidate vendor system's extension possibilities
	Question with each of your network product vendor about the security monitoring capabilities in their current & future networking products
	Ensure that also the status of load or load balancing of any procured critical network service can be monitored when needed. Load monitoring capability should exist in network devices as well
	Avoid any proprietary solutions and protocols when implementing security monitoring. Avoid vendor dependence whenever possible

2.2.1.4 Implementation

Usually, implementation is the problem phase in the development process, where most of the mistakes and errors to the system shall be made. Therefore, lots of quality assurance and security assurance effort should be spent to ensure that the implementation errors, flaws and vulnerabilities shall be detected and removed before the coming deployment phases. In practice, the checklists used for documentation & source code reviews should include security specific questions and the programmers should be trained to apply secure coding rules in all of their implementation efforts. Standard or tailored source code analysis software should be run before module testing. Also, the security related testing (e.g. fuzz testing) should be run during the system testing phase.

Another important way to ensure the security and quality of the purchased network software modules and devices is to require security certified products. E.g. Common Criteria (CC) certified products may exist within your functional interest area of products, and those can often be used as good reference products, or at least a starting point for further exploration of vendors that can support your special requirements.

The implementation related tasks to be applied for network security monitoring products & functionality should include:

Table 5. Implementation of network security monitoring functionality.

Area	Principles/Tasks
Implementation	Ensure that security monitoring functionality shall not interfere with the basic objective of the networked system, even under exceptional circumstances
	Separate the network management, monitoring & control equipment from your other networked systems
	Implement also the management of your network security controls in a way which enables you to minimize the damage done soon after identifying a problem in some network location via monitoring
	Review and test repetitively the quality and security of your monitoring system implementation
	In addition to protecting the secrecy of your secret security keying material and credentials (exchangeable), protect the implementation details of your security monitoring system from potential attackers

2.2.1.5 Configuration

Today, it is admitted that the installed security systems & solutions may also bring vulnerabilities or continuation risks to the target system that was supposed to be protected. The understanding of these risks is extremely important for systems which have high availability and dependability requirements. Therefore, good service and configuration management practices must also be employed to security (monitoring) systems. Specifically, the security system's maintenance must be well coordinated with the critical services of company's business operations, for the purpose of producing continuously value for the stakeholders. Of course, the main task for security maintenance is to maintain the risk-free configuration in security systems, which shall be in compliance with the security & continuity requirements for the operation.

When the deployment scale is large, implying that there are hundreds or thousands of devices or systems to be monitored, an automated security configuration compliance tool shall often be necessary. These tools should utilize well established standards such as Security Content Automation Protocol (SCAP) for automated follow up of vulnerability & security configuration. This may also guide the security monitoring implementation into more future-proof and extensible direction.

An important viewpoint is also the physical configuration, which shall define the safe locations and positioning of monitoring equipment for reliable operation. Then, what is the complete set up constituting from essential appliances, power, backup devices & media, cabling, etc, shall complete the secure configuration of a monitoring system. Also the physical system inventory & set up should be well managed, controlled, and documented for always being up-to-date after any approved change.

Finally, the baseline data groups (e.g. *normal*, *malicious*, *abnormal* and *unclassified*), and the signatures of rule based systems, must be established, preset & maintained for the secure configuration.

Configuration security related tasks for the network security monitoring system include:

Table 6. Configuration of network security monitoring system.

Area	Principles/Tasks
Configuration	Ensure that the configuration of your security monitoring system shall not change unintended. Manage the configuration of each device or virtual system using a well controlled change management process
	Test the feasibility of any changes to the monitoring configuration before applying, when possible. Do not test new configurations in the production system
	In addition to protecting the integrity of your configuration information, do not disclose the detailed configuration information of your security monitoring system to potential attackers

2.2.1.6 Deployment, O&M and disposal

Both the deployment process and the operations & maintenance (O&M) of network security monitoring systems are rather broad topics to be discussed here extensively, but a few advices may be given, anyhow.

The device and software installation procedures and the bootstrapping of trust & secure channels between the monitoring components require good deployment plans and some compact guidance for the field install crew. For example, the credential and certificate installation tasks by the field crew shall be usually out of question. Such functions must be carried out before installation, or at least installed automatically during the field installation process. A rather big issue may also be to successfully and securely integrate the security monitoring systems to the existing network environment. For example, often some new rules, data mirroring, log memory, and access rights need to be defined for the switches, firewalls, access control systems, and perhaps even some application service configurations.

For O&M, perhaps the most import issue is to define accurately the roles & responsibilities for the operations & maintenance personnel. It must be clear which authorization procedures are mandated for upgrading and updating the systems, hardware and software. This includes patching, vulnerability fixes, firmware upgrades, etc. In the case of service agreement, it must be contracted with the service provider that how, when and by whom their systems shall be updated & configured.

The deployment, operation & maintenance and disposal activities of network security monitoring system should consider the following:

Table 7. Deployment, O&M & disposal of network security monitoring system.

Area	Principles/Tasks
Deployment	Ensure that the possible remote configuration process and access control are secure before deploying a network- or monitoring device
	Keep the elementary system operations, such as information generation & bulk data transfer, rather simple & basic for the most of the networked devices. Allow for more flexible configuration and online adjustment for higher level devices and monitoring systems
O&M	Ensure simple & understandable usage, update and maintenance process for the security monitoring system
	Update and reconfigure your security monitoring system according to continuously identified new vulnerabilities and risks targeting your network
Disposal	Ensure that the confidential information is saved and destroyed from any of your monitoring equipment before disposal. Preserve the identification information of any monitoring HW & software product versions that you may need e.g. for spare part & upgrade acquisition

2.2.2 Assessing and selecting the basic indicators of an attack

As in any other (automated) supervision system, also concerning network security monitoring systems perhaps the most important starting point for accurate observations are the identification of basic attributes that should be followed up more closely. Obtaining an optimal attribute- or parameter set for a specific monitoring purpose shall not, however, always be a simple task. On the contrary, many IDS vendors for example may suggest that their system shall monitor all those attributes and all related behaviour that is needed to capture any kind of attacker. Unfortunately, this rarely is the whole truth in many cases.

2.2.2.1 Workflow for deducing the security monitoring attributes

In order to solve this “attribute selection problem” fully in advance, we should have a clear overview of all the concurrent and future attacks and other abuse, including their implementation details. Obviously this is an impossible task. What we can realistically do, however, is that we select such solution components which allow for flexible attribute and method selection, in addition to the capability to monitor the currently known attacks & abuse types. Note however that added system flexibility often adds also complexity and vulnerability, which means that the components and solutions must be implemented very carefully using secure development processes. Also the baseline- and trend analysis may suffer if the monitored attributes are to be changed too often. Therefore, the best way to apply these attributes is a compromise between flexibility and simplicity, and also many other issues, of course.

In an ideal world, we should create and maintain a mapping between the various attack and abuse types and the list of attributes to be monitored for capturing each of them. Actually, we should also have a list of analysis methods to apply, using the captured attribute values, and perhaps also a visualization scheme for each abuse. But we shall go wrong if we believe that this approach and even very flexible security monitoring system in general shall always be able to identify any new abuse and the suspected subsystems related to it. Clearly, the required security data collection & analysis functionality shall grow when we add a new feature to the networked system, and this emphasize also, e.g., the increase of performance and configuration problems towards our security monitoring systems.

In high level, the principal monitoring attributes of a network security monitoring system for each case should be identified according to the following workflow. NOTE: In the presented workflow the network security monitoring functionality is added to an existing networked system. In an ideal world, however, all security monitoring systems should be planned and built-in already during the construction of the networked system.

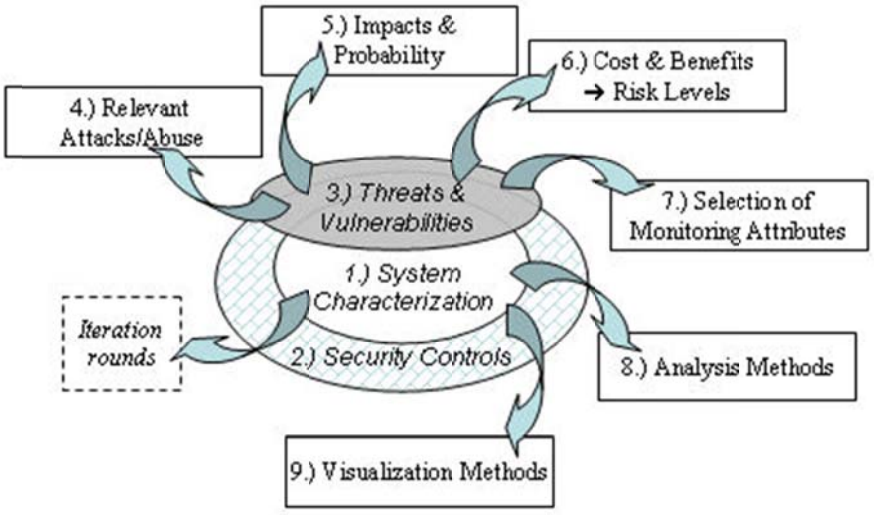

Figure 1. The developed workflow for deduction of the monitoring attributes.

Table 8. The steps for deducing the principal security monitoring attributes to existing network.

Step #	Task description
1	Characterization of the *system to be monitored*
2	Analysis of *security controls* in the current system
3	*Threat & vulnerability* identification of the system
4	Sorting out the relevant *attacks, criminal activity & abuse* against the system
5	Analysis of *impact & probability* of each relevant abuse case
6	Estimation of *risk levels* – costs & benefits calculation of resolving abuse
7	Selection of the *attributes for security monitoring* according to abuse risk levels
8	Testing & selection of the *analysis methods* for processing the attribute flow
9	Testing & selection of the *visualization schemes & tools* of analysis results
10	Return to earlier steps & continue the deduction *iteratively* (at any step)

Unfortunately, the above workflow that we have developed seems to be rather wide-ranging and extensive. However, this is in line with our findings that perhaps the most difficult problem in network security monitoring is the questions – *What should be monitored?* and *What really pays off to monitor*?

In next subsections, we clarify each of these deduction steps, together with few examples.

2.2.2.1.1 Step # 1: Characterization of the system to be monitored

First, we need to understand the basic operation of our current networked system. Clarification is often needed to properly appreciate the basic objectives & operation of the system that should be protected and potentially monitored. In many cases, the best way to do this is to arrange a meeting where the experts & key persons (who contributed into the requirements & development of the system from different aspects) shall explain the current system and the design- and operational choices made.

The system characterization should include the following topics:

- Main objectives for the system operation
    - Why this system exists? What purposes it serves according to contracts?
    - What are the objectives and goals of the system?
    - Which customers are served? Which stakeholders are affected if the system fails?
- Description of basic system operation & employee tasks
    - The operating environment
    - Main operations
    - The most important functionality
    - Support operations
- Results of already conducted risk- and vulnerability analyses should be recalled
    - Organization initiated self-analysis results (e.g. standard risk- & vulnerability analysis methods)
    - Results should have included the prioritized listing of risks & reasoning
    - The weak spots of the system have been identified.

2.2.2.1.2 Step # 2: Analysis of security controls in the current system

All serious security work starts from ensuring that we understand not only the current system operation but also the security controls already put in place to protect the system from unwanted disturbances & potential malicious activity. This analysis is needed to properly understand the meaning and capabilities of the existing security solutions & security controls currently planned or in use for our system. The security controls should typically include:

- Enforced security policies (administrative & technical policies)
- Instructions for secure operations & secure ways of working
- Security requirements for systems and subsystems development
- Instructions of work and defence in the cases of emergency, security incident & updating/upgrading
- Processes for establishing & maintaining the security of outsourced systems.

Another task related with the security controls analysis should be to the map security controls with the capabilities of feasible security monitoring systems. Which of our security policies and requirements can be supported in meaningful ways using some security monitoring methods? At this point, we could even have first ideas that what kind of security monitoring functionalities could be realistic and meaningful for our system?

2.2.2.1.3 Step # 3: Threat & vulnerability identification of the system (targeted attacks)

Threat identification & analysis is a process where the system is analysed and estimated from the perspective of external or internal threats. A threat may be kind of a traditional criminal activity such as theft of information, software or equipment, or intentional harm to the system such as weakening the service or causing the denial of services and/or data. Threat vector is a path or tool used to attack towards target.

Vulnerability identification & analysis involves a systematic investigation of the target system's security and quality properties. Vulnerability is a flaw or weakness in the system (or its O&M), which could be exploited. Often, vulnerability scanners, such as port scanners, network enumerators, network vulnerabil-

ity scanners and database security scanners are used as automated tools during vulnerability analysis process.

However, a very important part of the threat analysis is to analyse what kind of activities the potential attacker is allowed to perform in our environment (with prerequisites). Often, the attackers (insiders and outsiders) may utilize multitude of methods & practices to plan and execute a partial or full abuse of the target system, its assets or data. The generic attack/abuse ingredients may include:

i. Information gathering (if information available)
ii. Learning of a system (if time & motive exist)
iii. Searching of vulnerabilities (if information available)
iv. Identifying ways to attack/abuse (if competence available)
v. Planning of attacks/abuse (if time & motive exist)
vi. Development of exploits (if tool & competence available)
vii. Planning the destruction of abuse traces (if competence available)
viii. Initiation of abuse (if motive & opportunity exist)
ix. Reactive actions against defence (if tool & competence available).

Using the learned attack background information and previous abuse case experiences, the (professional) attacker may develop even better abuse capabilities for future use:

- Identifying new asset types that are worth to be targeted and abused
- Identifying the vulnerabilities and/or persons that might enable a new attack/abuse in the future
- Resolving the technical interfaces & human relations/intercourse that successful abuse requires
- Collecting the vulnerable configuration data
- Clarifying the capabilities required for successful abuse in each case
    - Attacker competence requirements
    - Access permissions (legal & illegal) required for initiating or enabling abuse

- Best attack/abuse tools for the purpose (e.g. tool evaluation for criminal motives)
- Listing the available exploits for entering to abuse case.

2.2.2.1.4 Step # 4: Sorting out the relevant attacks, criminal activity & abuse against the system

Using the threats and vulnerabilities identified for the system, we need to analyse which of the potential attacks or abuse cases are really relevant against our system and its current protection. In practise, this means that we should combine the information attained in previous Steps (2) and (3). Following example clarifies what kind of attack vectors might be possible within organization, if not extra-guarded. Specifically, such lists should help us in concluding which of the hypothetical abuse cases seem realistic against our system. In other words, we would need to sort out the irrelevant cases and concentrate only on really potential abuse cases.

Example - Insider abuse: We might conclude during our case analysis that the following attack vectors might be relevant against our system:

- An employee (insider) uses social engineering to collect unauthorized information (All our employees are not trained against social engineering)
- A user bluffs administrator to reveal his administration practices (Our administrators lack precaution or responsibility)
- An employee uses other person's user account (Our users commit insecure user account practices)
- An employee uses other person's user rights (Employee can stole session or user credentials)
- An employee exploits system's internal vulnerability (Mole or ex-employee present in premises?)
- An employee manipulates system log files (Might we possess a wounded administrator, log files are stored insecurely)
- An employee generates system error to hide unauthorized access (Might we have an improper configuration of logging system? Do we really keep track of log files systematically in all cases?).

Typically, the number & exploitation potential of attack vectors depend much on the weaknesses that specifically exist in common working processes and personnel's ways of working. Of course, sometimes a companion of technical fault or vulnerability is also required to enable the enemy to finalize the abuse, who may then commit "a perfect crime" without perception.

2.2.2.1.5 Step # 5: Analysis of impact & probability of each relevant abuse case

For this step there should be a standard practice in each organization, in which the company's critical operations are analysed against relevant security abuse cases, possible attacks and incidents. Such an analysis requires profound system & business knowhow (e.g. for impact analysis) and also feasible expertise of information security & value management (e.g. for probability analysis). The impact and probability analysis tasks for security are briefly introduced in the following:

Impact analysis has few profound questions to be answered for each relevant abuse case:

- What is the value of the affected asset? What is the value of potential loss?
  - Value of protected information
  - Value of missed production
  - Value of lost company image/brand
- What kind of behaviour the system and related systems shall undergo due to the attack/abuse?
  - What are the direct and indirect consequences of an abuse case?
- What it requires to restore the normal operation after realized attack/abuse case?
  - How long does the restoration to normal takes?
  - Value of required extra effort & equipment due to realized security incident

The *probability analysis* for each abuse case has also specific questions to be answered:

- Technical & operational difficulty of abuse? Division to abuse classes such as:

  - Abuse is available/obvious (1: Easy)
  - Abuse requires basic engineering skills (2: Basic)
  - Abuse with professional attitude & skills (3: Professional)
  - Organized professional abuse planning & design (4: Organized)

- Direct & indirect expenses to the abuser? How big value can be attained by the abuser?
  - Expenses to abuser. Classes, e.g.: < 1000 €, < 10 000 €, < 100 000 €, > 100 000 €
  - Value to abuser. Classes, e.g.: < 10 000 €, < 100 000 €, < 1 000 000 €, > 1 000 000 €

- How easily the results of abuse can be exploited? E.g. Ease of exploit -classes (from easy towards more difficult) such as:
  - Can be easily exploited in public marketplace (Easy)
  - Can be exploited in public marketplace with preparations (Exploitable)
  - Requires a sort of launderer or mediator (Mediator)
  - Suitable for criminal usage only (Criminal).

2.2.2.1.6 Step # 6: Estimation of risk levels – costs & benefits calculation of resolving abuse

Next we need to continue with the estimation of risk levels. We need to compare the endangered value of assets and (business) operations with the costs of protection mechanisms & processes. Obviously, the continuity & other benefits of protection must overweight the cumulative costs of protection. So, we should carry out the following activities to complete the estimation of risk levels.

Estimating the costs of elimination & mitigation of each relevant abuse case:

- Costs of doing efficiently the following:
  - Abuse & attack identification
  - Abuse block out
  - Incident reporting
  - Abuse prevention planning & management.

Estimating the benefits of preventing an abuse case. To accomplish this task, we may simply recall the results of previous step: *impact analysis* (costs of lost value, production & brand, restoration costs) and *probability analysis.*

Finally, we should to carry out the *comparison of costs & benefits* for each abuse case. Obviously, this could be done according to each company's preferences, but e.g. 3–5 different *abuse risk criticality levels* could be defined, for example:

- Critical risk (critical benefits in prevention, at feasible prevention costs)
- High risk (benefits in prevention, at feasible prevention costs)
- Medium risk (benefits in prevention, at probably non-feasible prevention costs)
- Low risk (uncertain benefits in prevention, at non-feasible prevention costs).

2.2.2.1.7 Step # 7: Selection of the attributes for security monitoring according to abuse risk levels

Eventually, the security monitoring attributes for abuse monitoring may be (initially) selected using the estimated risk levels. Being an organizational and extremely case dependent issue, the monitored attributes may be selected, for example, only for the Critical- & High risk abuse cases. While identifying & selecting the monitoring attributes, consider the following:

- From each relevant abuse case, identify the key information & data, assets, and system services & states that needs to be guarded
- *Identify the attributes* that should be monitored from the key information & data, assets, and system services & states. For attribute examples, see subsection "Examples of security monitoring attributes". The critical topics to be monitored include:

  - Key information (business secrets, credentials, emergency system controls, maintenance- and updating information)
  - Key data (log data, access control data, network management data, control & signalling data, routing tables, hardware-, equipment- & software specifications, system configuration, network topology, firewall configuration & rules, etc.)
  - Assets (network equipment, workstations, cables, switches, base stations, communication channels, application software, databases, configuration files, partners & subcontractors)
  - System services (operating system services, application software services, maintenance services, user authentication, access control, audit trail, diagnostics, analysis, updates, backup & recovery, remote monitoring, system development)
  - System states (states of memory & CPU, network interfaces, enterprise service bus, configuration, updating, reboot, filtering, error, recovery)
- *Analyse the identified attributes* in detail to understand which of these are practical to be automatically recorded by the local system:
  - Is it possible to automatically record the attribute?
  - Is it practical & cost effective to arrange for secure attribute data recording, storage and data transfer?
  - Are there any legal or regulatory obstacles in the attribute data collection?
  - Note: Sometimes it may require an expert to estimate which of the attribute recordings require a new system or software to be installed
- *Estimate* whether the practically recordable monitoring attribute data shall be enough for reliable *abuse case identification* (or to complement it)
  - Consult a security (solution) expert about the reliable security monitoring *analysis methods* and *input requirements*
- Clarify the maturity, availability & overall costs of each analysis method to your available attribute data

- For scalability reasons, prefer using & recording such attribute data that are supported by (standard) local devices, if there are no special reasons such as suspected industrial espionage, for the usage of tailored attributes.

2.2.2.1.8 Step # 8: Testing & selection of the analysis methods for processing the attribute flow

The feasible analysis of attribute data can usually contain two principal method families. When there are lots of data to be analysed, together with modest computing and memory capabilities, then the "statistical analysis" methods may be feasible. Statistical analysis methods are feasible for identifying suspect behaviour in the network, but they are not 100 % accurate.

On the other hand, the "distinct analysis" methods are feasible against known attacks. However, the drawbacks include a mandatory data inspection system, which often requires e.g. powerful processing, lots of memory, and also some manual maintenance work for its rule-base updates.

More of the analysis method selection is discussed in subchapter "3.4 Data analysis methods".

2.2.2.1.9 Step # 9: Testing & selection of the visualization schemes & tools of analysis results

After the attribute data flow has been processed, it needs to be combined & correlated with the previously preset data and visualized to the user.

The presentation of the aggregated results can be done, for example, visualizing the:

- *malicious data groups (match to malicious)*
- *abnormal data groups (match to abnormal), and*
- *unclassified data groups (no match)*

in different ways than the *normal data groups (match to normal)*. The optimal, automated way to recognize & formulate these groups should be tested using various visualization tools. These results, the best tools & their visualization schemes, should then be mapped to the relevant abuse cases.

More of the data aggregation topic is discussed in section "3.4.2 About network data aggregation methods".

2.2.2.2 High level monitoring scope to be deployed

Each of the various operators of the networks and systems should be able to develop a reasonable monitoring deployment with a feasible direct scope for them. Of course, this should not exclude the co-operation and exchange of relevant monitoring information between the (interoperating) network & system operators, while still working according to laws & regulations. Next, there are presented some examples of various high level monitoring scopes of interest.

2.2.2.2.1 Example scopes for Enterprise systems monitoring

Table 9. Example scopes for Enterprise systems monitoring.

High level monitoring scope	**Examples of high level monitoring scope**	**Event types to be monitored**
Enterprise systems	Status of various enterprise & engineering systems (e.g. operation, configuration, upgrading)	*System events*
	Status of business processes per user (access log, application log, messaging status, presence)	*Process events*
	Updates to business processes (e.g. a new instruction/module taken into use)	*Process changes*
	Status of assets & inventory systems, system general properties	*System events, Physical events*
	Employee status (e.g. role, access control status, work tasks/activities, user rights/permissions)	*System events, Physical events*
	Officer & partner clearance	*Human actions*
	Other human actions & context of action	*Human actions*

2.2.2.2.2 Example scopes for Outsourced systems monitoring

Table 10. Example scopes for Outsourced systems monitoring.

High level monitoring scope	Examples of high level monitoring scope	Event types to be monitored
Outsourced systems (e.g. cloud services)	Outsourced system's operation: requests, responses, SLA monitors	*System events, etc.*
	Outsourcing resource allocation & demolition	*System events*
	Load balancer operation, load monitoring, usage profiling	*System events, Network events*
	Changes in outsourced configuration & environment	*System events, Network events*
	System health-, availability-, and performance trends, triggers & thresholds of the system	*System events, Network events*

2.2.2.2.3 Example scopes for Production systems monitoring

Table 11. Example scopes for Production systems monitoring.

High level monitoring scope	Examples of high level monitoring scope	Event types to be monitored
Production systems	Status of production systems (operating mode, system services, system states, usage history, maintenance cases, diagnostics, configuration)	*Process events, System events, Physical events*
	Safety & security systems status	*System events, Physical events*
	Operations management (e.g. control centre events, operation control status)	*System events, Process changes*

2.2.2.2.4 Example scopes for Network systems monitoring

Table 12. Example scopes for Network systems monitoring.

High level monitoring scope	**Examples of high level monitoring scope**	**Event types to be monitored**
Network systems	Network management system operations	*Network events, System events*
	Network device status & (remote) management	*Network events, System events*
	Network border/gateway device status	*Network events, System events*
	Application service interfaces within network system	*Network events, System events*
	Status of network service interfaces, changes in status	*Network events, System events*
	Filtering- & access control rules and log files	*System events, Security events*
	Network bindings & actual connection flows	*System events, Network events*
	Protocol messaging between endpoints	*Network events*
	Parameter messaging between endpoints	*Network events*

2.2.2.2.5 Example scopes for Control systems monitoring

Table 13. Example scopes for Control systems monitoring.

High level monitoring scope	Examples of high level monitoring scope	Event types to be monitored
Control systems	Security control (room) events & alarms	*Any event*
	Status of security monitoring, anti-malware & IDS & SIEM systems	*Security events*
	Activation or deactivation of monitoring data collection & related systems	*System events, Network events*
	User account management events	*System events*
	Access control systems status, usage profiling	*System events*
	Logging systems, audit trail, log monitoring	*System events*
	Configuration control events	*System events*
	Control of other changes (incl. any software, firmware, hardware)	*System events*
	Session control events	*System events, Network events*
	Keep-alive messaging follow up	*Network events*

2.2.2.3 Examples of security monitoring attributes

We are also aiming to give some concrete support for the detailed attribute selection task. Therefore, we introduce and assess briefly below some indicators & attributes, which could be captured and analysed to effectively recognize the potentially malicious phenomena, for the purposes of network security monitoring.

Unfortunately, more concrete case studies are needed that should enable us for presenting even more extensive attribute lists. Each network operator or administrator shall define a list of their own, according to feasible risks and limitations of their networked technological environment. The deployed (risky) software applications shall probably affect a lot into the selection of the most relevant security monitoring attributes.

See a table below as a simple example list.

Table 14. Some possible attributes for security attack & abuse analyses.

Type	Indicators	Attribute type	Notes about capturing / processing
Unusual load	Sudden network traffic load	# of frames / time unit	Network traffic analyser probes or MIBs of devices
	Slower access to network devices than normally	Round-trip time (RTT)	ICMP (ping), test data transfers, other RTT monitors
	Sudden problems with disk space	% of free disk space	System status monitoring SW
	High CPU load without reason	% of CPU usage	System status monitoring SW
Usage of user accounts	New user accounts	Account log entry	Log monitoring
	Unexpected use of admin-user accounts	Account log entry	Log monitoring
	User accounts locked	Account log entry	Log monitoring
Deviations in log entries	Log files or entries deleted	System log entry	Log monitoring, system status monitoring SW
	Sudden bulk of log entries	System log entry	Log monitoring
Unusual device/server activity	Boom of alerts from antivirus & IDS software	AV & IDS events	Typically vendor specific events and formats
	Errors in servers	Thrown exceptions & error messages, TCP/HTTP keepalives	Monitoring of application specific error messages, protocol specific keepalives
	Sudden changes in files and directories	Filenames and directories	Tracking the file system changes
	Unexpected OFF of security controls	Security software & configuration status	Tracking the changes in security configuration and status
	Sudden changes in patches	Patch changes	Tracking the patch changes in system
	Unexpected shutdowns	System shutdown event	Tracking the system shutdown events
Unexpected configuration changes	Unexpected configuration changes	Configuration change	Remote configuration attestation, configuration follow-up
	Unexpected embedded software	Installed SW	Tracking the software that are installed and running
	Disabled logging functionality	Logging settings	Systems that validate logging correctness. Secured logging follow up
	Deleted recovery systems	Status of recovery systems	Systems that validate recovery functions and data

Suspicious network behaviour	More data sent towards external networks	Alteration in data flows, FW logs & events	Flow analyser emphasizing applications, protocols, conversations, endpoints
	More data sent from external networks	Alteration in data flows, FW logs & events	Firewall log analysis tool. Or flow analyser emphasizing applications, protocols, conversations, endpoints
	Unexpected data flows	Alteration in data flows, FW logs & events	Flow analyser emphasizing the flows (NetFlow, cFlow, jFlow, sFlow)
	Unexpected behaviour similar to device error	Faulty messages or sent error codes	Analysis of error codes or diagnostic tool results
Social engineering activities	Unexpected information requests	Junk emails, phone calls, queries, social abuse	Following up the activities that were not related to assigned tasks
	Suspicious content	Suspect text strings or data formats	Content based filtering & alarming systems
Application specific indicators	"Various application specific abuse indications"	"Application specific attributes"	Application monitoring systems. Also following up the implications of application usage, etc.

2.2.3 Few concerns about data network architecture

In today's ICT networks, it is essential that the network architecture is designed & constructed according to the critical protection needs of each operating site. For example, the server cluster should often be separated into its own subnetwork so that any user device malfunction doesn't propagate risky data traffic to application or infrastructure services provisioning segments. Some general principles include:

- Design LAN topology by separating the critical & non-critical functions.
- Isolate logically the critical (or vulnerable) protocols to segregated subnetworks.
- Use the DMZ and firewalls between the separated subnetworks, if some connectivity is needed.
- Prepare for the alternative communication paths that protect against sudden data media errors.
- Select the feasible user data & content segregation mechanisms.
- Maintain separate test subnetworks, where e.g. new device configurations can be tested before installation to the production network.

Typically, the edges of such deployed LAN shall be the potential physical locations for installing the major security monitoring probes or SIEM. This is due to better potential of capturing larger amounts of data with representative scope for further analysing the incoming & outgoing data, traffic, flows, etc.

2.2.4 About security monitoring data communication architecture

While the physical data network architecture might explain the wiring, node location, network topology and other such issues, it may not clarify how the different devices should communicate with each other. For communicating the data that shall be used as input for the security monitoring systems, there are few basic alternatives on how the transfer of such data may be arranged. These alternatives are discussed briefly in below subsections.

2.2.4.1 Local monitoring data collection

In the next figure, a local network monitoring data information collection is presented in a generic case (not including peer-networking cases).

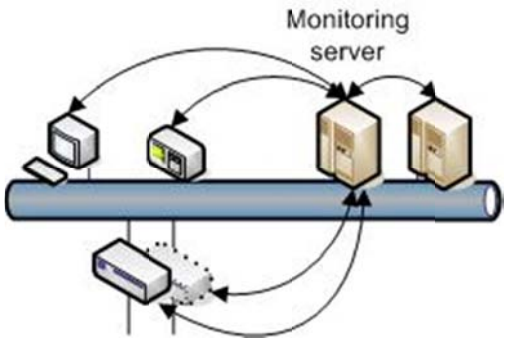

Figure 2. Communicating the local network monitoring data to local monitoring service.

NOTE: It is NOT a good design principle to allow the transfer of detail monitoring data from each client to site major monitoring data server through firewalls or DMZs. The local serving node should instead send the local subnetwork's aggregated data to the higher layers of the monitoring solution. This reduces the risk of (site-level) monitoring data flooding.

Within the local subnetwork, the communication alternatives include:

- *Server broadcasting* a request for monitoring data to all devices, the clients shall respond when available.

- *Server polling* each client individually using request/reply messaging, each client responds to the request when available.
- Each *client* is independently and periodically *pushing* monitoring data *batches* to the server.
- Each *client* is *pushing* monitoring data to the server independently, but only after any important *event/alarm* at the client.
- Each *client* is *publishing* monitoring data independently (e.g. using RSS feed, messaging application, etc.).
- A *database synchronization* of monitored data is run between server and the clients. Each client has its own entry in the server database.

In the subnet level, it might not always be necessary to use open standards for transferring the monitoring data, for example in such cases where the local equipment is very proprietary or a standard communication solution is not feasible.

In below, there is a table about the Pros & Cons of each local communication alternative.

Table 15. Comparison of local monitoring data communication choices.

Communication alternative for monitoring data	Pros	Cons
Server broadcasting	Simple	Broadcast signalling
Server polling	Proven, de-facto	Limited scalability, state-based
Client pushing batches	Distributed operation, scalable	Not real-time
Client pushing at events	Distributed operation, real-time	Bulk of events
Client publishing	Distributed operation, scalable	Web service risks
DB synchronization	Functionality, flexible	Database system risks

2.2.4.2 About corporate level monitoring data collection

The cost-effective arrangements for monitoring data transfer at corporation level shall depend largely, of course, on the corporation's common data communication architecture. While these architectures may be based on various communication technologies, we would still like to try and give couple of security advices at this level also.

Applying for corporation & group levels, the necessary data collection facilities for the network security monitoring purposes should be planned, managed & maintained in secure ways, such as:

- The basic topics to be monitored shall be defined in the planning phase. Risk analysis for the necessary information transfers should be made.
- It should be agreed about the usage of common corporate level communication standards for monitoring supervision data – which may often be Internet based for cost-efficiency.
- It should be planned and arranged for the centralized monitoring data services where all (summary) data is collected to and from where it may be further analysed. Also, one alternative might be to contract with the (outsourced) security service provider, when feasible.
- By default, all the network management & monitoring data connections should be authenticated, integrity, replay & confidentiality protected.
- Network administrator's system access should be restricted – e.g. only allowing access from network supervision & management workstations.
- User accounts for network supervision should only allow the reading of log files, not modification. Modification of log files should be made impossible by default.

Note that the global network security co-operation- & data collection principles are currently as work-in-progress in various global research & standardization communities. Unfortunately, it has not often been possible to arrange truly open security information exchange networks, due to risks for attacker community follow up. Where applicable, however, feasible secure Internet standard protocols should be used for the security information exchanges due to fast interworking, security and integration capabilities.

3. Discussion – Some example elements of a monitoring system

3.1 Overall system outlook

Next, we shall introduce the reader briefly to some example elements of the network security monitoring system, such as basic networking devices, netflow analysers, or other software elements to be used in the monitoring entirety. For example, the elements of network security monitoring system shall include:

- The capturing of network data and events within each critical subnetwork
- Pre-analysing network data locally (e.g. summary handling of SNMP trap messages or logs of events and alarms)
- Transmitting the pre-analysed results to the central security monitoring server of the network
- Central security monitoring server that may aggregate all the incoming data together, compare it to the existing baseline data using various threshold values, and serve the monitoring operator by generating various graphical presentations using various visualization techniques, presenting by default the major security event information, possibly warnings, etc.

In addition, it would be beneficial if various kinds of trends might be followed up, including the capability to taught new instruction sets enabling for particular trend analysis, setting up the allowed threshold values to the particular trend analysis for alarm identification, which may be tailored for each network traffic- or use case. For example, a new ICMP monitor instance could perhaps be activated enabling the locally focused monitoring, if e.g. a serious malfunction,

problem or threat in some device or subnetwork has been suspected after the trend analysis. Using the synthesis results, the observer could even try to recognize zero-day attacks or abuse using flexible companion of the network security monitoring system capabilities, by comparing various network behaviours to the network's normal operation. Effective trend-, comparison- & synthesis methods could be found, developed, or even automated after the experimentation, which could be used to identify the security problems in the network, and preferably also to suggest the origin (i.e. the root cause) of the problem.

3.2 Basic networking element

Adequate audit trail must be possible to collect within each network element to be monitored, system log collection must be enabled, and there must be enough resources in the device (e.g. memory and CPU capacity) to store and process the log files, even during exceptional circumstances, like alarm storms. The process of network element procurement must integrate all the applicable functional security requirements for devices' monitoring capability and remote monitoring data exchange standards that the purchased device or system must fulfil. However, for some cases, just standard ICMP & secured SNMP requests by the server and the corresponding client replies could do enough for the required security monitoring functionality.

Generally speaking, many of the deployed monitoring clients within network elements have recently been implemented as proprietary application layer software, even if there are also middleware or firmware software implementations available for some systems.

Monitoring should often concentrate on the *device's* basic *status* properties, such as:

- Device: On / Off?
- An interface: Operating / Overbooked / Shut down?
- Device's remote admin control: Enabled / Disabled?
- Status of current configuration: Approved / Changed?
- Device's real time logging setting: On / Off?
- Throughput values: Within limits (upper – lower)?

The reason for the basic properties follow up is that the bulk generation of monitoring data can thus be avoided in most situations.

3.3 About traffic flow analysis

If feasible, organize the data traffic flows using (standard) flow analysis tools, which have good extension properties and capability to gather the captured flow data and to present the flows as grouped according to well known protocol / application categories. Note that the flow analysis is rather resource consuming task, and it usually requires the purchasing and usage of special flow analyser equipment and software. For example, some ad-hoc developed or operated open source netflow analysers could cause more harm and effort to the network administration, than real benefits & value for the network security monitoring.

After estimating the various risk levels of your relevant network abuse cases, consider developing a system where you can:

- Identify, characterize, and classify such *flow* groups that have *normal behaviour*
- Identify, characterize, and classify such *flows* that are *unclassified* earlier
- Identify, characterize, and classify such *flow* groups that have *abnormal behaviour*
- Identify, characterize, and classify such *flows* that are due to *malicious abuse.*

Gather, set up and store the baseline data for the abovementioned flow group families. It would also be beneficial if you could add certain identification and *metadata* characteristics to such a baseline data, for example, a certain change occurred in system circumstances, abnormal occasion or happening, e.g. a visitor audience or maintenance work happened during the day, etc. The most important capability is to be able to reuse the different baseline data, in order to later compare e.g. the abnormal and unclassified flows behaviour with the specific known baseline flow behaviour.

3.4 Data analysis methods

The feasible analysis of aggregated data can usually include two principal method families. When there are lots of monitoring data to be analysed, together with modest computing and memory capabilities, then *statistical analysis* methods may be feasible. Statistical analysis methods are feasible for identifying suspect behaviour or traffic flows in the network, but they seldom are 100 % accurate.

Instead, the *distinct analysis* methods, such as the deep packet inspection, are feasible for investigating particular, already suspected data connections. However, the drawback of deep packet inspection is, usually, the required expert for manual inspection, or relatively expensive data inspection system that requires e.g. powerful processing, lots of memory, but still expensive manual maintenance work for the rule base definitions, etc.

We shall concentrate here more on statistical methods than on e.g. deep packet inspection or other distinct methods. This is due to the generic applicability of statistical methods and also due to the fact that many statistical methods may be used to automatically analyse big amounts of data, still with only moderate administration effort, or algorithm teaching time.

3.4.1 Statistical methods

Statistical methods for monitoring the data communication security policy conformance

There is usually a defined security policy – e.g. within a company, corporation, operative alliance, or simply within industrial plant – that is intended to be enforced by the firewalls, hardened host configurations, secure change management practices, and other measures in place. For example, only certain secure communication protocols and services such as HTTPS (SSL/TLS), SFTP, SSH, SNMPv3, etc., could be allowed for transfer through certain critical network segment. Also the application data carried inside these protocols are often governed, for example, any streaming application protocols might be forbidden according to company policy. However in reality, there might be occasional violations or data leaks against this common policy, which needs to be recognized and then reacted by the responsible system administrators. The main goal might be to proactively avoid that the evolving networked system will eventually break out the defined security controls.

So, some practical methods should be taken into use to classify the potentially numerous communication data flows to help in the (real-time) identification of the policy violating data traffic. Traffic analysis is a generic term for the process of intercepting data communication and examining (encrypted) messaging to deduce the important information out by the recognized traffic patterns, using e.g. statistical methods.

The statistical analysis methods for the identification of policy violating data traffic include, but are not limited to:

- **K-means clustering.** A learning algorithm that assigns observations into various clusters. Each observation is put to a cluster that has the nearest mean value. The observation can be n-dimensional vector
- **GMM (Generalized Method of Moments)-**based classification. GMM is a general method for estimating the parameters of statistical models
- **SVM (Support Vector Machines).** Supervised learning methods for statistical pattern recognition. May also be used for classification and analysing the regression
- **HMM (Hidden Markov Model).** A statistical Markov model, often considered as the simplest dynamic Bayesian network.

To be able to identify security policy violations, what kind of data traffic strings should be investigated and what kind of method should be used to analyse more closely the revealing data strings or signalling behaviour being buried in the bulk of network data traffic? In the next, we shortly discuss about some potential analysis methods and network traffic data attributes.

The potential statistical methods shall include:

- Flow analysis: Analysing the IP packet header information and dividing the traffic to individual data flows, e.g. protocol session flows, based on *IP source and destination addresses, -ports, services, time stamping*, etc. information. Also identifying the sessions of various encryption protocol (SSL, SSH, ESP, etc.) based flows, if possible
- Analysing the internals of at least the exceptional and/or unknown data flows and statistically classifying the flows into specific number of groups. Success in this often requires some earlier teaching of the statistical method, using fixed (known) baseline traffic data. The attributes that are used as inputs in the statistical methods often include *packet size, -direction, time duration between the packets*, etc., within the exceptional flow.

Finally, some of the potential policy violations might be detected no sooner than e.g. from the graphics or summary presentations for the user. Of course, the grouping of data flows should be automated, when possible, at least between the

two groups of “according-to-policy” / “not-according to policy”. In most statistical methods, the number of input attributes is not limited. This means that various different attributes and combinations can be experimented to find out the most effective solution for each case.

The feasibility analysis of these statistical analysis methods shall not be presented here more closely. However, each of them might be used in various ways, with different benefits & drawbacks.

3.4.1.1 Example – K-means clustering

In this short example, we give some advice for the usage of K-means clustering method:

- Select the most effective basic transmission attributes as inputs for the k-means clustering. Examples include *message size*, *packet interval*, *round trip time*, *retransmissions*, *acknowledgements*, *auto-diagnostic messaging*, *error messages*, etc. Try for example to figure out or postulate using the existing knowledge - What is the most important attribute set typically changing during attack execution or attack preparation?
- Experiment with various different formulas that take the attribute set as input, or ask consultation from the method or application area expert. Aim for setting up such formula(s) that shall produce an easily modelled output in an equation. E.g. any linear dependence between the formula and values constitutes a perfect equation, or even a new network behavioural law
- Within the method, experiment with and use alterations in the number of clusters setting. For example, using a small number of clusters may help the user to quickly learn some of the basic properties of a new *unclassified* flow type. By setting up the number of clusters much higher, however, one might be able to distinguish the various different functions (e.g. the effects of applied remote commands within a session) into different flow types, but that setting is far more resource consuming. For normal situations, it is recommended to use a fixed number of clusters, which has been proven effective for the abuse case
- Sometimes (e.g. in recognizing the Zero-day attacks), it may require exceptional modelling configuration to recognize a risky flow or a

family of risky flows. The use of exceptional attributes and formulas might be required to recognize such attacks, as they might be designed as invisible in the current network monitoring tools. Usually, you should also monitor (in parallel) within the upper & lower thresholds of *normal* traffic flows, whether there are any slighter implications of some pending abuse case

A procedure for enabling successful clustering of a “single function”

To begin with, study what shall be the best analysis method for identifying reliably and accurately the distinguishing characteristics of *each particular flow type*.

- Measure the principal characteristics of each functionally and operationally separate flow type. E.g. you need to filter out all the other flows to separate apart only the candidate flows that need a new model
- Try out and run various different method constructions to develop a robust method. Try also with various attributes. The new method construction (method, inputs, outputs) must be able to reliably identify the particular flow type
- Specify a preliminary model for each distinguishing functional flow type. To do this, use the experimented method construction with test runs and your labelled data
- Practice each model (to the extreme) to find “the nominal” result and the acceptable range of output values that still fit to this model. E.g. test generators & traffic can be used to practice each model, aim at finding the final form of the model
- Specify finally the robust model for each distinguished, functional flow type. Each model should be strict and catch only the intended flow type, as you have the objective to reliably identify and recognize a particular functional trace from the bulk of network flow data.

3.4.2 About network data aggregation methods

The presentation of aggregated analysis results can be done, for example, using 2–3-dimensional fields/maps, where e.g. the *unclassified*, *abnormal* and *malicious* flows/groups are highlighted in some way over the *normal* groups. Possibly an initially estimated risk rating for the suspected groups should also be cal-

culated and shown to the user, based on e.g. modelled data from previous groups. However, the risk rating shall be difficult to estimate reliably, but it should help in (re-)directing the user's attention to potentially risky network phenomena.

The groups may be presented visually in different contexts, depending on the needs of the security monitoring system. The context examples include:

- Physical map, or distance (e.g. logarithmic) from the critical network points
- Perceived policy versus currently defined security zones
- Time duration from unusual / critical behaviour or occasions
- Application behaviour, e.g. the difference rate of a suspect group's behaviour from the allowed or denied applications group behaviour.

It is difficult to monitor that the contents of the communication was according to pending corporate security policy, especially if the communication was end-to-end encrypted. For that, we need either a brute force opening of the encryption which is illegal without a legal case, or some statistical methods that shall only reveal the violations against, for example, corporate security policy, without injuring user's legal rights for privacy.

Also a special case in network security monitoring, especially relevant in *forensics cases*, is to combine and correlate the information of particular node's data flows to the node's detail log information. In principle, the highest user permissions and access rights, according to which users were logged in, were specified in the used access control services, and should not be smaller than those observed from all users data traffic, flows and applications at the duration of the login sessions. To make the sanity check or correlation easier, the nodes should also log the sessions that each user name are committed to during login time span. A big problem area is obviously the internal attacks. For example, how to security monitor (a privileged) user initiated programmatic changes or executable based configuration changes of systems, or configuration data exchanges efficiently in a scalable way, and at the same time using only methods that preserve the privacy of the user? Eventually, a root cause for the possible system malfunction or misuse should be possible to sort out accurately.

4. Conclusions

Some guideline for the development of effective network security monitoring systems.

Plan and construct an experimentation system for the purposes of security monitoring, according to your operations risk profile.

Using an ideal, advanced security monitoring system, the system operating user should be able:

- To select the *monitored attributes* as freely and as multifaceted as possible, according to various needs and hypotheses
- To select the occupied *analysis algorithm* purely according to the needs of the investigated phenomenon, without laborious development and configuration efforts for the algorithm or its interfaces
- To select the most feasible (or experimental) *analysis parameters* and *threshold values* according to the needs of the investigated phenomenon in question
- To *visualize* the outcome of the analysis methods and algorithms, and summarize and combine it in *flexible ways* using graphical presentation tools and user interfaces
- When necessary, also to extend the analysis using external, private, or public analysis tools suitable for specific purposes.

In this way, the most feasible measurements, methods and configurations could be used to monitor the various security situations, case per case, within the monitored ecosystem.

What seems to remain irreplaceable is the network operators' own thinking & gathered knowledge about the operating environment, their goal setting and enforced processes that enable the correct way to manage the network securely, also at the time when future challenges suddenly realizes.

Series title, number and
report code of publication

VTT Research Notes 2589
VTT-TIED-2589

Author(s)
Pasi Ahonen

Title

Constructing network security monitoring systems (MOVERTI Deliverable V9)

Abstract

This report analyses and describes the basic construction of network security monitoring systems. The viewpoint is mainly research perspective, we aim for defining system constructions or elements which are also commercially relevant, but still maintain the open minded approach of research oriented work. The focus is on clarifying the overall network security follow up, but also on methods for investigating the "difficult to identify" or zero-day attacks or the preparation of such attacks, which try to exploit the application vulnerabilities that are currently unknown to operators and software developers.

The necessary network security system construction depends much on the operator's targets for security monitoring. The threat environment of some specific operator may require a deeper analysis of the output from various security device logs, events and alarms. The needs of such operator may be to adjust the different alarm thresholds for the security devices accurately, according to the evolving network data traffic characteristics. Another operator, instead, would require holistic security monitoring of the production area, where e.g. the status information within physical access control systems and electronic access control systems shall be combined, and the aggregated summary results shall be presented to the operator for sanity checking.

Therefore, we present in this report some building blocks that can be used to construct a security monitoring system, not a complete system that shall be feasible as such for all possible security monitoring needs and requirements.

ISBN
978-951-38-7769-9 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN	Project number
VTT Tiedotteita – Research Notes 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	32923

Date	Language	Pages
June 2011	English	52 p.

Name of project	Commissioned by
MOVERTI – Monitoring for network security status in modern data networks	ABB Oy, Empower Oy, L M Ericsson Ab, Nethawk EXFO, Nokia Siemens Network, Nokia Oyj, Tekes

Keywords	Publisher
Network security, monitoring systems, data networks	VTT Technical Research Centre of Finland P.O. Box 1000, FI-02044 VTT, Finland Phone internat. +358 20 722 4520 Fax +358 20 722 4374

VTT Tiedotteita – Research Notes

2574 Marko Jurvansuu. Roadmap to a Ubiquitous World. Where the Difference Between Real and Virtual Is Blurred. 2011. 79 p.

2575 Towards Cognitive Radio Systems. Main Findings from the COGNAC project. Marja Matinmikko & Timo Bräysy (eds.). 2011. 80 p. + app. 23 p.

2576 Sebastian Teir, Antti Arasto, Eemeli Tsupari, Tiina Koljonen, Janne Kärki, Lauri Kujanpää, Antti Lehtilä, Matti Nieminen & Soile Aatos. Hiilidioksidin talteenoton ja varastoinnin (CCS:n) soveltaminen Suomen olosuhteissa. 76 s. + liitt. 3 s.

2577 Teuvo Paappanen, Tuulikki Lindh, Risto Impola, Timo Järvinen & Ismo Tiihonen, Timo Lötjönen & Samuli Rinne. Ruokohelven hankinta keskisuomalaisille voimalaitoksille. 2011. 148 s. + liitt. 5 s.

2578 Inka Lappalainen, Ilmari Lappeteläinen, Erja Wiili-Peltola & Minna Kansola. MULTIPRO. Vertaileva arviointi¬konsepti julkisen ja yksityisen hyvinvointipalvelun arviointiin. 2011. 64 s.

2579 Jari Kettunen, Ilkka Kaisto, Ed van den Kieboom, Riku Rikkola & Raimo Korhonen. Promoting Entrepreneurship in Organic and Large Area Electronics in Europe. Issues and Recommendations. 2011. 69 p. + app. 7 p.

2580 Оса Нюстедт, Мари Сеппонен, Микко Виртанен,Пекка Лахти, Йоханна Нуммелин, Сеппо Теэримо. ЭкоГрад. Концепция создания экологически эффективного района в Санкт-Петербурге. 2011. 89 с. + прил. 12 с.

2581 Juha Forsström, Pekka Lahti, Esa Pursiheimo, Miika Rämä, Jari Shemeikka, Kari Sipilä, Pekka Tuominen & Irmeli Wahlgren. Measuring energy efficiency Indicators and potentials in buildings, communities and energy systems. 2011. 107 p. + app. 5 p.

2582 Hannu Hänninen, Anssi Brederholm, Tapio Saukkonen, Mykola Evanchenko, Aki Toivonen, Wade Karlsen, Ulla Ehrnstén & Pertti Aaltonen. Environment-assisted cracking and hot cracking susceptibility of nickel-base alloy weld metals. 2011. VTT, Espoo. 152 p.

2583 Jarmo Alanen, Iiro Vidberg, Heikki Nikula, Nikolaos Papakonstantinou, Teppo Pirttioja & Seppo Sierla. Engineering Data Model for Machine Automation 2011. 131 p.

2584 Maija Ruska & Juha Kiviluoma. Renewable electricity in Europe. Current state, drivers, and scenarios for 2020. 2011. 72 p.

2585 Paul Buhanist, Laura Hakala, Erkki Haramo, Katri Kallio, Kristiina Kantola, Tuukka Kostamo & Heli Talja. Tietojärjestelmä osaamisen johtamisessa – visiot ja käytäntö. 2011. 36 s.

2589 Pasi Ahonen. Constructing network security monitoring systems (MOVERTI Deliverable V9). 2011. 52 p.

ISBN 978-951-38-7769-9 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)