2017/1

American Journal of Research, Education and Development

RED

ARS SCIENTIAE
DEV L'ART
SCIENTIA ARTIS

ISSN 2471-9986

American Journal of Research, Education and Development

IMPRESSUM

American Journal of Research, Education and Development
ISSN: 2471-9986

Publisher: DEVLART LLC
250 Camelback Ridge Ave. Henderson, NV 89012
red@devlart.hu

CONTENT

New methods to protect our network systems

Péter Török, Budapest Business School, Hungary

Dr. János Rikk, National University of Public Service, Hungary

Abstract

In the last few years the number of security incidents has significantly increased. There were twice as much DDoS attacks than before in the previous year, and this number is still steadily growing. Attaining a reliable defense is growing into a more demanding task as the array of threats is continuously widening.

Security Information and Event Management systems (SIEM) is attempting to deal with this problem. The goal of this system is to function by warnings, alarms, and logs based on software and hardware actions, and to gather and analyze this data in real time, ensuring that security related acivities and events are resolved.

Major functions of SIEM systems are:

- Log consolidation, log management
- Log normalization
- Correlation
- Incident management
- Reporting
- Asset management

The main goal of this paper is to offer a brief overview of an open source implementation of a SIEM system. Different lists exist about hostile IP addresses or signatures of malicious code across the internet. Collective Intelligence Framework (CIF) is a framework which's purpose is to gather this data. If collected, then this data is stored in a database, and an interface is provided for external programs to question the data, which ensures that they can handle the actual network pertinently. A reliable real-time first line of defense can be maintained as a result.

Keywords: network, security, CIF

Introduction

Recently the Internet, the World Wide Web has become an important tool for working, searching information and learning. We use it for storing data or maintaining relationships, and a mean of community life for many. By now almost everything is connected to the Internet. The Cisco foresees that 50 billion of devices will be connected to each other till 2020 (Cisco 2016). Nowadays the amount of the devices connected is only 5% of this prognosis. The Internet of Things connects large number of users to the system, in a different way than the usual hardware environment and programming (uo.) The large number and different kinds of access introduce some unforeseen dangers and vulnerabilities, threatening more and more the connected world. According to the statistics of Virus Bulletin (Cobb 2015) the lifetime of most computer viruses is between 6 and 14 months, meaning that even after one year from their occurrences they are infectious, even though defensive softwares provide updates in hours or a few days after the first occurrence of infection. The case is similar with the known program vulnerabilities. Even if the developers provide corrections for the vulnerabilities, one can find many unpatched versions in the network even after long time, even after a year. The network behind the Internet has scale-independent topology (Barabási–Albert 1999). This is the explanation why it is possible for a moderately infective virus to spread and stay active for a long time (uo.).

The Internet is self-organizing. It is constructed from the individual acts of billions of users. Tracking down unusual events, anomalies, attacks and interfering becomes difficult over time and needs more and more competence, time and resource. As many businesses are executed over the net, the web services have become primary targets of attacks. The number of vulnerabilities and attacks is increasing in a fast pace, for example the number of DDoS attacks is doubled in the last year. According to the Cisco reports (CISCO 2016) 92 per cent of the devices in the Internet contain known vulnerabilities. There are 15435 discovered vulnerabilites in 2015, and more than 83 per cent of them has security patches provided. This number will be increased by 40 per cent according to the Researchers of National Vulnerability Database (Arnav Prabodh Joshi 2013). It is appalling that every eighth webpage has critical vulnerability, and 85 per cent of them contain some kinds of vulnerability (Su Zhang, Doina Caragea – Xinming Ou 2011). In these days the number of web malwares has considerably increased, due to automatic malware tools and exploit kits. Hackers use a number of hostile softwares that spread malicious softwares using automatic attacks, infecting computers. New attack methods require new defensive methods. One solution can be the Security Information and Event Management (SIEM) systems for the problem.

Security Information and Event Management (SIEM)

The tasks of the SIEM systems are to identify security events and help security personnels to apply defensive solutions as soon as possible. Audit analysing and incident handling features provide solutions for centralised log handling of network and security equipment, operating systems and databases, executing searches using data mining algorithms on the collected data, detecting security events, searching correlations among them, and handling incidents (Bedwell 2014) .

Main features of a SIEM:

– Network discovery
– Network scanning
– Network monitoring
– Equipment inventory enumeration
– Host based software inventory enumeration
– Monitoring behaviour
– Analyzing network traffic
– Service availability health-checking
– Packet capturing
– Collecting logs

Security discovery

– Correlation analyzis
– Event handling
– Report and alarm
– Vulnerability scan
– Testing network vulnerabilities

– Monitoring vulnerabilities
– Threat detection
– Network IDS
– Host IDS
– File integrity monitoring

SIEM systems implement such security monitoring that unravels intrusions into the examined systems. Actually they form an Intrusion Detection System (IDS). SIEM systems try to answer questions like: What kind of devices are there in the network, realising a potential attacker device. What are users doing? What kinds of known vulnerabilities can be found in the network? Is there any attacker trying to intrude the system? Are there active threats in the network? SIEM adds risk analysis and increases reliability to the system besides these. This way the data provided by SIEM system are useful to design a secure system and provide overview of the status of security for the maintainers.

As security related logs are created by many equipment in many formats, it is important for a SIEM system to be able to normalise collected data, and provide them in a standard format to the maintainers, aiding to observe trends and patterns that differ from the usual behaviour. SIEM unifies Security Information Management (SIM) and Security Event Management (SEM) functions in the same security system. A SEM system centralises log storage and analysis, nearly real time. A SIM system collects data in a central database for tendency analysis and automatic report generation. Merging these two functions SIEM systems are capable of faster identification, analysis and recovery triggered by security events. They can also be used to measure security compliance (Syed – Pazardzievska 2012).

Most SIEM systems collect information about security events using agents: from servers, network devices, special security equipment like firewalls. Collectors forward the event logs to a centralised maintenance console which executes analysis and reports anomalies. In order to be capable of detecting unusual events, SIEM administrators need to create a profile about normal behaviour first (Bourgeois 1999).

One problem of SIEM systems is the extreme resource requirements. In order to store and search large volume of data maintainers need large amount of storage, processors and memory, so installation can be expensive and requires deep understanding of network technology (Formicola et al.).

One SIEM implementation that is available also for smaller organisations is the Open Source Security Information Management (OSSIM). OSSIM is an open source security information and control management system that integrates features that helps maintainers to develop their secure network. It includes IDS and IPS. This project started in 2003, then it was taken over by AlienVault in 2008, and became part of the commercial AlienVault Unified Security Management System. The AlienVault OSSIM contains many well-known open source security software, which are available through a web based user interface. Many of these software components can be accessed through command line interface. Logs are inserted into a text file and the webinterface makes centralised configuration management possible.

OSSIM features the following software components:
PRADS, used to identify hosts and services by passively monitoring network traffic.
OpenVAS, used for vulnerability assessment and for cross correlation of IDS alerts Vulnerability Scanner information.
Snort, used as an IDS and also used for cross correlation with Nessus.
Suricata, used as an IDS, this is the IDS used in the default configuration.
Tcptrack, used for session data information which can grant useful information for attack correlation.
Nagios, used to monitor host and service availability information based on a host asset database.
OSSEC, a Host-based intrusion detection system (HIDS).
Munin, for traffic analysis and service watchdogging.
NFSen/NFDump, used to collect and analyze NetFlow information.
FProbe, used to generate NetFlow data from captured traffic.
OSSIM also includes self developed tools, the most important being a generic correlation engine with logical directive support and logs integration with plugins.

The list above shows that a well configured SIEM system can collect necessary data, normalises them and recognises correlations, and summarises the security status of the network. For this, expertise and financial resources are necessary (Suarez-Tangil et al. 2015).

Collective Intelligence Framework (CIF)

In this paper I would like to introduce a different approach in developing computer security. As stated earlier, the Internet community tends to be self-organising. There is an open source project that uses this social community to build first line defence (Toret–Calleja 2014).
There are blacklists available over the Internet, in which operators collect event logs about their security incidents. If we could collect these blacklists and integrate to our defence system, then we could build a strong first line defence. Consider a DDoS attack. The most difficult problem we face when defending against a DDoS attack is that it is impossible to decide if a connection belongs to a legitime user or to an attacker, thus we need to serve the request or decline it. A collective intelligence can provide much help. In case a host (IP address) is part of a botnet and had already been reported

by an operator, then we can assume malicious activity when connecting to our network too, thus rejecting the connection. Collective Intelligence Framework can help creating such knowledge (Nair Sabari Girish – Puri 2015).

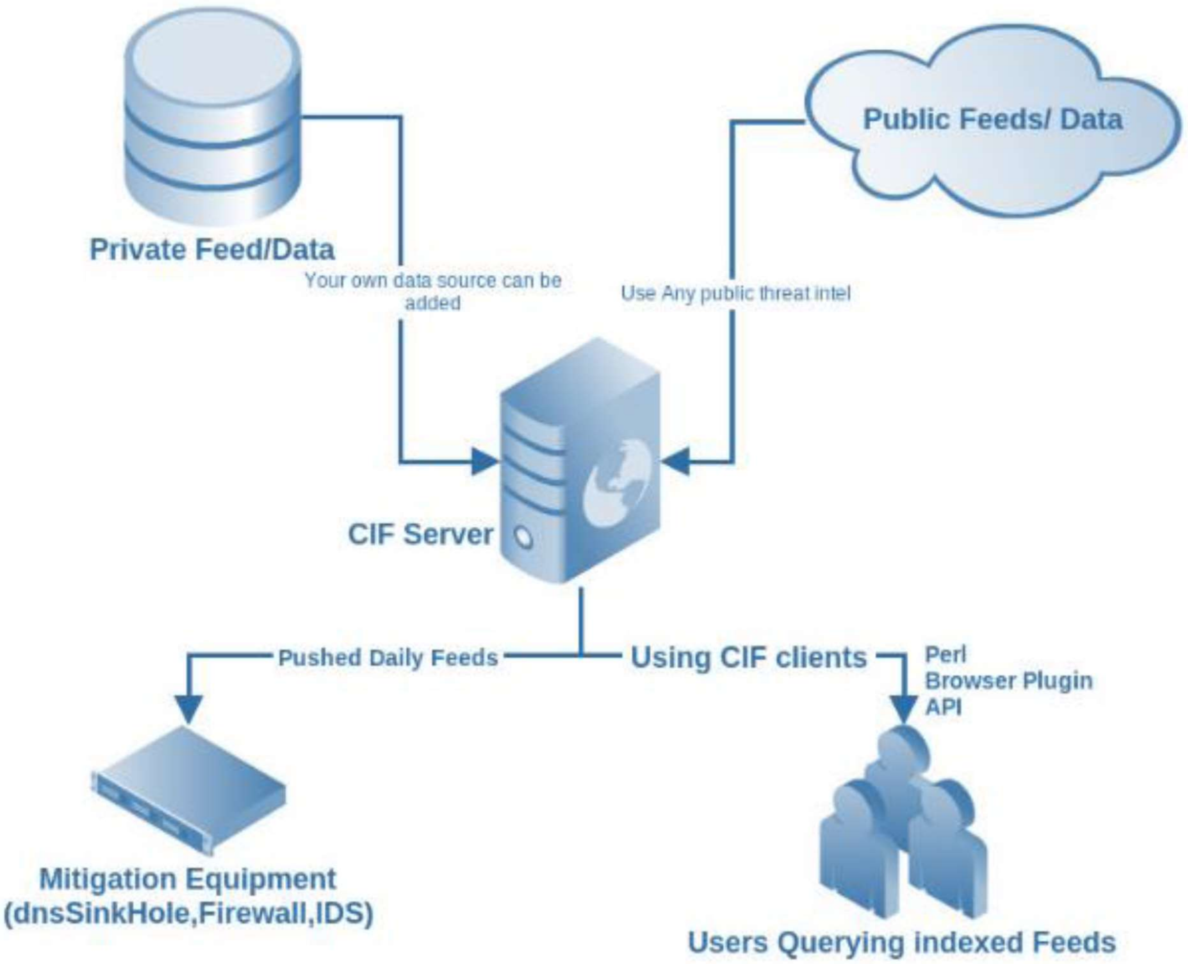


Fig. 1:. *The structure of CIF*

Source: http://csirtgadgets.org/collective-intelligence-framework/ (16. 02. 2016)

CIF is a community-developed framework that periodically collects data from external observers who provide feed files, stores them in a database, thus creates collective intelligence. An API is provided to query data, this way we can integrate the collective intelligence into our own defence system.

Trustworthiness is always an important question when using community-maintained sources in production environment. A less reliable observer might misinterpret a host as attacker or might deliberately mark a legitime webpage as malicious. Attacking these blacklist services can insert many legitime users to blacklists too. If we trust every sources unconditionally, we might deny legitime users from our systems.

In order to solve this problem, CIF introduces a confidence numerical value, assigned to these sources. Using this value we can put these sources into the following categories: Certain, Very confident, Somewhat confident, Not confident and Unknown. In our search requests we can filter by the confidence value too, taking trustworthiness into consideration when allowing or declining connections.

This can be used in the following way too: During average load we use only Certain and Very confident entries. When the load increases for example because of a DDoS attack, we might consider the Somewhat confident and the Not confident categories too.

Assigning confidence values is done by configuration files, we can assign confidence value to feed files and entries.

The second release of CIF: CIFv2 natively supports the format of Kibana, Snort, Bro, Bind, Tipping Point, PassiveDNS, FireEye for integration. In case we want to use our own format or have more fine-grained control over the output, then there is an API provided to query data. The API is implemented as a http service, thus accessing the API is easy using open source softwares. API supports authentification, preventing unauthorised access to the collective intelligence, and supports basic defence against attacks that target CIF directly (for example DoS). Besides the Representational State Transfer (REST) API there is a command line interface for interrogation, which can be used for testing, or for integration as well. Queries can be based on IP, FQDN, URL, email address, tag (like malware, botnet, phising, scanner, zeus, hijacked), country code, ASN provider, confidence, application (http, ssh etc), group, date or any combination of such indexes.

CIF operates on feed files. A configuration file belongs to each of them. The configuration file contains the location of the feed file and the structure of its data. Following parsers are supported by CIF: regex, json, xml, rss, html, text. The default CIF configuration contains many pre-defined configuration files, so the basic installation is a good starting point to have a good quality collective intelligence. Based on the pre-defined files, or using the documentation, one can create their own configuration file for other feed files, further improving collective intelligence. The configuration files are in Yet Another Markup Language (YAML) format, thus they are easily understandable and modifiable.

CIF iterates through the list of active feeds in every hour, and assimilates their content to the collective intelligence. The parsing of some feed files can be resource-consuming, so it is not practical to process them paralelly at the same time. Avoiding denial of service condition, CIF shifts the processing of each files by a random interval, somewhere in the first half of every hour. This way the load generated by feed file parsing is distributed on the interval.

The data coming from feed files are saved into CIF's own database. Feed files typically contain reports only of the last few days, operators need to take care of long-term storage, because the information about old DoS attacks might be useful when building current defences.

CIF uses resources extensively during operation. This is an uncomforting issue, because extreme resouce requirements and thus increased costs hold back the wide usage of a community-driven product. According to the documentation, the following hardware is recommended for small, large, and extra large installations:

Small Instance:

an x86-64bit platform

at-least 16GB RAM

at-least 8 cores

at-least 250GB of free (after OS install) disk space

Large Instance

an x86-64bit platform

at-least 32GB RAM

at-least 16 cores

at-least 500GB of free (after OS install) disk space

RAID + LVM knowledge

xLarge Instance:

an x86-64bit platform

at-least 64GB RAM

at-least 32 cores

at-least 500GB of free (after OS install) disk space

RAID + LVM knowledge

Examining the parsing of large files, it turns out that sometimes small or even large instance does not provide enough resources (memory, CPU, storage) for reliable and long-term operation.

As data should be stored for a long time backwards, we can explain the large storage requirements. Memory and the number of CPU cores are needed when serving requests. The database engine is ElasticSearch in CIFv2, which is based on Java, and has high memory consumption. In case of high traffic, we can expect many queries, thus the high number of CPU cores is required, further increasing the resource consumption of ElasticSearch and Java engine. CIFv3 will support other database engines too, so that one can try out different solutions.

In every SIEM systems, searching is a key element. Choosing the right engine is not an easy question. If we examine the CIF framework, the first release uses PostGreSQL, the second release uses Elasticsearch, and the third version uses SQLite for the development cycle.

CIFv2 is written in Perl, the development version was rewritten into Python. Checking the code, one can see there are many databases that are planned to be supported, as the question is not trivial, the problem concerns other SIEM systems as well, because it has high effect on CPU and memory usage.

Data storage and usage considerations:

A database engine can be certainly used as a search engine, but they contain such features that are unnecessary for a SIEM system. Such features are for example real time data availability or transactions. SIEM systems collect data periodically from some distribution sources, for example once in every hour, so real time data availability is not a requirement. Also, because of the types of data these systems usually store, there is no need for transactions.

Elasticsearch is a search engine that can be suitable for this task, and is very efficient to do complex searches on high volumes of data. It supports horizontal scalability. It runs on a Java virtual machine, which makes scalability easier from an implementational point of view, and also makes the product available on multiple platforms.

Although Elasticsearch does not support real time data availability - reindexing takes 1 second before the new data is available -, it supports high availability through redundancy in a cluster environment using fine grouping of data into shards: master shards and replica shards.Shards are the entities that store the data. Search indexes are mapped to shards. Shards are elastic, which means they are to be moved around in a cluster environment, distributing the load equally.

Due to the complexity of the product, it might be challenging to configure Elasticsearch. For example, on a single host enviroment, there is no need to have more than one shard per index. Also, memory sharing between processes is a complex question. Elasticsearch can use unlimited memory to increase efficiency. If an operator runs multiple services on the same node, then some restrictions should be configured for Elasticsearch not to saturate memory. Besides, efficiency depends on the configuration of Java virtual environment, so the configuration of JVM also needs special attention.

Results

From now on we examined the memory consumption of CIFv2. The chosen feed is the Bambenek Consulting DGA feed file, its size is typically around 95MB. The feed file is available in the following location: http://osint.bambenekconsulting.com/feeds/dga-feed.txt.

Examining the structure of the feed file, it is a csv file prepended by a few lines of header. Attacker, description, date, source can be extracted from the file.

The short sample of the beginning of the feed file below shows its structure:

```
####################################################################
## Domain feed of known DGA domains from -2 to +3 days
##
## Feed generated at: Sun Feb 14 00:15:01 UTC 2016
##
## Feed Provided By: John Bambenek of Bambenek Consulting
## jcb@bambenekconsulting.com // http://bambenekconsulting.com
##
## Use of this feed is governed by the license here:
## http://osint.bambenekconsulting.com/license.txt
## For more information on this feed go to:
## http://osint.bambenekconsulting.com/manual/dga-feed.txt
##
####################################################################
xysmythakdfvx.com,Domain used by Cryptolocker - Flashback DGA for 14 Feb 2016,2016-0214,http://osint.bambenekconsulting.com/manual/cl.txt
nqeovvlipilgt.net,Domain used by Cryptolocker - Flashback DGA for 14 Feb 2016,2016-0214,http://osint.bambenekconsulting.com/manual/cl.txt
bojcqeprglovk.biz,Domain used by Cryptolocker - Flashback DGA for 14 Feb 2016,2016-0214,http://osint.bambenekconsulting.com/manual/cl.txt
olgiamdgqktlr.ru,Domain used by Cryptolocker - Flashback DGA for 14 Feb 2016,2016-0214,http://osint.bambenekconsulting.com/manual/cl.txt
cjlvuuhphnwbr.org,Domain used by Cryptolocker - Flashback DGA for 14 Feb 2016,2016-0216,http://osint.bambenekconsulting.com/manual/cl.txt
```

This is such a feed file that is not possible to parse in the current implementation because of high memory usage.

During parsing this feed file, we continuously measured memory using free -m linux command, calling it in each second. We appended a timestamp before the result.

The following script was used for this:

while [1]; do echo -n "`date '+%H:%M:%S'` : "; free -m | grep Mem | awk '{ print $3 }'; sleep 1; done;

Sorting by the second column, one can easily see the range of memory usage: more than 18GB of memory was used in each case, after parsing again the same file 25GB of memory was used, and each reparsing increased memory consumption. Only restarting CIF helps to restore 4-5GB memory usage.

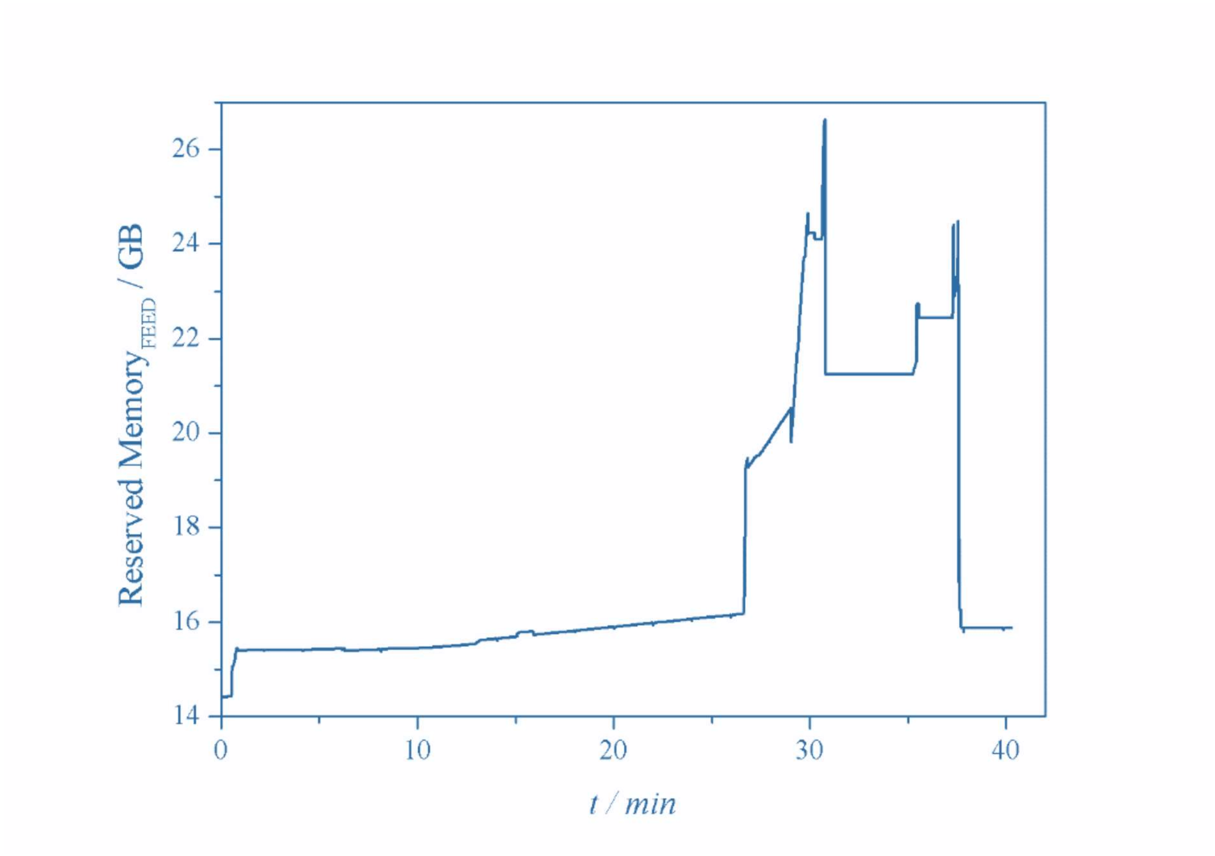


Fig. 2.: *The memory usage of selected Feed*

Parsing other feed files follows a similar pattern. It is clearly visible on the diagram that memory consumption starts with low usage, then raised slowly with short bursts to higher values. Values are not restored to the initial values after finishing the parsing. This concludes there is 1GB memory leak after each parse. This memory leak is mitigated by periodically restarting the CIF service.

Conclusions

SIEM systems and CIF can be very useful products in an organization's defence system. But improving resource consumption is certainly necessary so that they can be reliably used in small systems. It should not be obscure when to the restart system because reliable operation is not assured because of memory issues. Further research is needed to develop a new storage and searching framework, or to improve existing ones, so they can satisfy the expectations mentioned above, and provide data efficiently. Because CIF needs to store data for a long time, storage requirements are acceptable. However CPU and memory consumption needs to be improved. CPU and memory resources are used by the search engine. Choosing the appropriate search engine is challenging, further pieces of research are necessary. In my opinion the solution is connected to further pieces of research on methods of noSQL databases.

It is important to further optimise resource usage in case of CIF, because such systems are most efficient when more and more providers use and share their knowledge, building collective intelligence.

References

1. CISCO 2016 Annual Security Report. *Cisco,* January 2016.
2. Barabási, Albert-László – Réka Albert, [(1999]:): Emergence of scaling in random networks, . *Science,* 286: 509–512.
3. Cobb, Stephen ([2015]:): VB2015 paper – Sizing cybercrime: incidents and accidents, hints and allegations, . Virus Bulletin.
4. ARNAV Prabodh Joshi ([2013]:): Linked Data for Software Security Concepts and Vulnerability Descriptions. 2013 – DTIC Document, pp 8–98.
5. Su Zhang, – Doina Caragea, – Xinming Ou, ([2011]): An empirical study on using the national vulnerability database to predict software vulnerabilities, . DEXA 2011, Part I, LNCS 6860, pp. 217–231.
6. PATRICK Bedwell, P. ([2014]): Finding a new approach to SIEM to suit the SME environment, , *Network Security*, 7: 12–16.
7. Raheel Hassan Syed, – Jasmina Pazardzievska, ([2012]): Fast attack detection using correlation and summarizing of security alerts in grid computing networks, . *Springer Science+Business Media,* LLC: 804–827.
8. JULIEN BOURGEOIS (1999): Emergence of scaling in random networks. *Science,* 286: 509–512.
9. VALERIO Formicola, - ANTONIO Di Pietro, – ABDULLAH Alsubaie, – SALVATORE D'antonio, – JOSE Marti, [(2014]): Assessing the impact of cyber attact on wireless sensornodes that monitor independent physical systems, . IFIP International Federation for Information Processing, pp 213–229.
10. GUILLERMO Suarez-Tangil – ESTHER Palomar, ARTURO Ribagorda, IVAN Sanz, (2015): Providing SIEM systems with self-adaptation, *Information Fusion,* 21: 145–158.
11. JAVIER Toret, – ANTONIO Calleja, (2014): Decentralised citizens engagement technologies. D2.1 Collective intelligence framework. UOC, 2–89.
12. Sabari Girish Nair, – Dr.Priti Puri, [2015): Open Source Threat Intelligence System. *International Journal of Research, 2*(4): 360–363.

Firtst results of automatizing the unit management system in the US Army

Dr. Négyesi Imre; National University of Public Service, Hungary; negyesi.imre@uni-nke.hu

Abstract:

This article is the next partial result of a planned long-term research. The ultimate goal of the research is to present a history of the REVA service from the perspective of technical devices. Continuing the previous part, this article presents the artillery subsystem (TACFIRE), one of the three subsystems of the field army automated command and control systems in the US Army, and some other artillery systems and this article presents the Combat Service Support System (CS3), one of the three subsystems of the field army automated command and control systems in the US Army, and some other the military supply system to automate tasks.

Keywords: computers, information, management, history

The large scale scientific and technical improvement of the decades following World War II had a great impact on the weaponry and other technical tools of the army. This huge technical improvement resulted in such fast locomotion in military affairs too, that the registration and evaluation of the combat situation was only possible through the process of large amounts of data, however, that couldn't entirely be done manually. Most forces, but especially the ones of leading world powers made great efforts in researching the usage of electronic computers on the field to solve this problem. Automatizing the duties of the artillery received special attention, because these duties always included processing large amounts of data.

The aim of this article was to present the Tactical Fire Direction System of the artillery (TACFIRE), but primarily from the perspective of the IT devices facilitating automation. I was trying to present the duties of the artillery to an extent that helps the presentation of the technical background and provides a basis for future analysis. It was my sub-goal to introduce a new possibility for automatizing military activities which can be an example for the Hungarian military leadership.

In the second part of the article I present the third main system of the data processing system of the US ground forces, the Combat Service Support System (CS3), primarily from the perspective of the IT devices facilitating automation. In this part of the presentation too I was trying to introduce the duties of the military supply service to an extent that helps the presentation of the technical background and provides a basis for future analysis.

In addition to these the aim of the article was to also introduce and analyze the contemporary American and Hungarian principles which had an impact on the control of automatization and the vision.

The beginnings of automatization in performing the duties of the artillery

In ground units the automatized team management system of the field (all-arms) army had three subsystems: Tactical Operations System (TOS) and the aforementioned TACFIRE and CS3. From these the TACFIRE, despite its name containing the word 'tactical' based on further interpretation used in the US Army, was an operational-tactical automatized fire direction system.

The operational-tactical automatized fire direction system was an integrated electronic computer system working in on-line mode, which was made suitable for operation in field conditions from 1971 to 1974 and was adapted in the artillery units of the ground forces.

The development of the TACFIRE began in the beginning of 1960 within the framework of an artillery live firing codenamed "White Plan". The drill sequence held in Fort Huachuca (USA, Arizona) was intending to examine the possibilities of the usage of electronic computers in firing tasks in the artillery.

Based on the experiences in the end of the drill sequence the composition of the TACFIRE system was defined, which was approved by officials in January 1966. They entered into contracts with the manufacturers of electronic computers selected according to the approval until December 1967. The contracts included development, production, the trial of the developed system in field conditions, the direct participation of the producers and the army in experiments, and they specified the service and technological requirements for the experiments. For one of the main goals of the program they specified the creation of a universal military electronic computer that could also be used in other data processing systems (mainly TOS-75) of the land forces.

Trough automatic data processing the system served as a great help for artillery commanders and their staff in carrying out their tasks. The authorized electronic computers were able to reduce the workload of the computing and information processing tasks of the artillery, which was mostly done manually until then. The goal of the system was to increase the efficiency of the artillery support while enhancing the accuracy, be able to process and use the information concerning the targets fast and well, reduce the reaction time, to assure bigger efficiency in determining the ability to fire and the distribution of the targets among the artillery sub-units.

Using the automatized data processing technology the automatized fire direction system could help completing the following tasks of the artillery:

- technical preparations
- artillery fire detection
- artillery inspection
- fire control
- fire planning
- processing meteorological data
- registering the status of the ammo
- registering the position of artillery units

The large scale scientific and technical improvement of the decades following World War II had a great impact on the weaponry and other technical tools of the army. The ever-growing amount of information required – taking advantage of the large technological improvement – the commencement of automatization of completing tasks in military affairs too. Great efforts were made to examine the usability of electronic computers on the field in favor of solving the problem. Automatizing the duties of the artillery received special attention, because these duties always included processing large amounts of data, one of its systems was the TACFIRE.

In conclusion we can say that this chapter only offers a general description which, however, shows that there is no change in the tasks of the artillery, so the amount of data to process will continue to constantly grow. It follows directly that the development of the technical tools of automatization will continue to be on the agenda.

Technical background of the TACFIRE-system

Let’s take a look at what parts was the TACFIRE made of and what parameters did it have. The nerve center of the system was the third generation computer manufactured by the Control Data Corporation (CDC), which besides being designed for military use also made the further increase of the available capacity possible.

The question may arise that why did the CDC get this order from the military. The computer manufacturing company was one of the bigger American computer companies which were well known and honored in the USA in the 1960s. The others (IBM, Burroughs Corporation, NCR, General Electric, Honeywell, DEC, RCA and UNIVAC) could also boast significant results. The background of the decision if of course not known, but it is a fact that the CDC already made the Naval Tactical Data System (also known as NTS), which after its introduction in 1950 was successfully used as an information processing system by the US Navy until 1960. It is also a fact, that the CDC considered IBM to be their biggest rival, and it was one of their principles to produce 10% faster devices 10% cheaper. (Cheaper manufacture could be a determinant factor because after World War 2 the military had a smaller budget). It could also influence the decision that the TACFIRE was part of the Automated Data Systems within the Army in the Field (ADSAF) it adjusted to the other important part, the operational-tactical control’s automatized data processor system (TOS), whose core was provided by a CDC 1700 type supercomputer.

Naturally this would be too much of an easy answer to the question, especially knowing that the third system belonging to ADSAF, the logistic supply's automatized data processing system, the CS3 used IBM computers. However, it can be safely stated that the CDC developed the computer on the picture below in 1964 under the name CDC 6600, which may not have been the cheapest, but it was surely the fastest computer of its time. The 6600 CP (Central Process) containing 10 parallel functional units was able to process multiple commands at a time. Today this is the superscalar design, which was unique in its time.

The acknowledgement of the CDC6600 type computers' achievements was indicated by the fact that the institution dealing with the analysis of the USA's defensive problems stated referring to their own research that by 1975 bodies of the Department of Defense will need 125 computers like this only for the elaboration of meteorological information.

After the analysis of the financial and economical background of the beginning of the automatization let's move on to the analysis of the technical background. To every computing center belonged an artillery control desk, which provided the program's supervision for the operating staff. This appliance was able to draw up messages during the input to the computer, the highlighting of the supplied data according to the messages, and it could also retrieve them, put messages and data in the computer and indicate mistakes. For filling the computer's internal memory and for the containment of large amounts of data they used external memory devices which were most likely drum or replaceable disk memories. In every computing center a line printer was placed. The line printer was directly attached to the output of the computer and provided necessary amounts of prints of the stored data. For the depiction of the current combat situation they used a digital map drawer attached to the computer, which had pages sized 122x122 centimeters. In higher level artillery centers they also installed a CRT indicator to the map drawing unit. This appliance was also operated by the computer and it was used for magnifying certain parts of the map.

Outsourced message input units belonged to the system, which could transmitted the data to the computing centre from great distances. Two types of these were developed. The standard shaped message input unit was a small sized, portable appliance, which were installed at forward observers. The messages were forwarded as a digital sign via the ground radio or telephone news system to the computer. The variable shaped message input unit provided transmission without the use of the standardized form trough radio or telephone. To the artillery batteries they provided the needed information visually represented. The connection of the news system with the computer, the input units, the electronic plan boards, and coder tools was possible trough the data input terminal.

The system's software consisted of such computer programs that provided the possibility of completing artillery tasks. In line with the tasks the application of the software happened in different areas:

- utilities (translation programs);
- controller programs operating peripheral units;
- programs completing TACFIRE's tasks, which made the constant supervision of the program possible, and also the indication and elimination of malfunctions and their causes.

First the camp artillery units, then the division artillery strains were equipped with the TACFIRE system. The other elements belonging to the artillery units and division artillery strains (forward observers, exploratory groups, meteorological departments, etc.) were connected to the computing centers with input/output tools. The system was connected in the camp artillery's news system. The transmission of the digital and analog signals was provided based on time-sharing.

The time-sharing allows the sharing of the computer's sources between multiple users and/or processes trough a possible method of multitasking. During the time-sharing a central server distributes its sources between the users/processes by assigning "time slots" to every user/process. If the time slot is chosen, the machine runs the program of the user assigned to it, but only if it's not currently carrying out input/output activities.

The pace-setter module of the operation system controls the distribution of the time slots between the users. If the control picks a certain user, then the pace-setter sets the new or saved program parameters and starts running the certain program. When the assigned time slot expires it stores the metadata, then it could retrieve the program with it.

The length of the time slot depends on the number of users and the other parameters of the system; usually it varies between a few milliseconds and a few hundred milliseconds. The implementing of the time-sharing was made possible by increased speed and the realization that while the currently running program is waiting for the user, the machine in fact is not doing anything, so these times are unproductive, and could be used for other purposes. The possibility of reaching the mainframe (computer networks) from a great distance also had to be provided.

The TACFIRE system was installed to S-280 type cross-country vehicles with a container-like solution, which provided running order, deployment, fast reaching of viability and also transportation on land, water and air.

The TACFIRE appliances of the artillery unit were installed to one, and the appliances of the divisionary staff were installed to two S-280 vehicles. According to the plans the system also provided help for the tactical-operational center’s fire support element in the preliminary aim analysis and in the prediction of the nuclear waste’s fall-out.

The operation of the system is not complicated. The forward observer, with the help of a message input unit trough the connection of the camp radio or telephone, transmitted the request related to induction of fire to the computer in the fire control central of the artillery unit. The computer analyzed the aim, calculated the ballistic data and compiled the advised fire order or fire orders. After this the computer marked the location of the aim on the digital map drawer, and gave the fire order on the control panel. The report of the forward observer reached the control desk in the duration of 6,3 seconds. If the fire controlling officer decided to ignite fire, the computer forwarded the fire order in the form of a digital signal to the battery which’s cannons had to fire.

The fire control officer was of course able to change the input data anytime, however, this meant that the computer had to work out new commands and instructions. The computer automatically transmitted the commands to the computer placed in the division’s fire control center, where they were registered for fire planning and aim registration purposes.

The problems and possibilities of the automatization of logistic supply tasks in the 1950s and 1960s

The principles

The third main system of the US land forces’ data processing systems was the CS3. The system was created with the intention to satisfy the needs related to the automatization of basic data processing systems in both war and peace. In the 1950s it was already stated that the possibility of fixing logistic supply operations can be provided by the usage of automatic data processing systems in personal, administrative, accounting and supply areas. The CS3 was based on the principles and methods already in force. They offered a completely new perception in the area of logistic supply data processing rather than support methods. The aim of the system was:

- to increase the influence of the all-arms commanders by decreasing the amount of administrational work in supply, personal, and administrative issues;
- to offer an opportunity for the maximal usability of the tools at hand by decreasing the demand for human resources (conditions);
- the appliance to be able to respond to the informational demand of superiors in high-speed.

The system's creation made the automatization of the following areas possible:

- financial and technical preparedness of the troops
- making systematic and special reports
- financial management
- military salaries
- military police service
- reporting losses of manpower
- medical service
- any material supply
- financial preparedness, being stocked up, and maintenance service
- technical constructions
- army-scale transportation

The Hungarian political and military leadership also recognized that for waging modern wars the usage of great amounts of military technology is necessary, which is only possible trough the automatization of the management. The problem of management mechanization was of particular importance for the logistics supply, because the data communication tasks occurred in great numbers. The increased requirements for the logistics supply management were unanimously concerning every process of the management, which were summarized in the following:

- clarification of the task, collecting data related to logistics supply;
- fast and punctual processing of the data at hand;
- decision making for the logistics supply;
- operations related to the logistics supply, fast transmission of commands to the ancillary;
- registering of tasks, supervision of completed tasks;
- analyzes, drawing conclusions based on the completed tasks.

All these tasks were such a major burden for the management that modern mechanical and automatic management systems became essential. The good example was before the eyes of the Hungarian management of logistics supply, because the automatization of the fire control and the mechanization of the movement of troops were relatively advanced. Naturally the improvement of leadership tools was not able to provide the fast fulfillment of logistics supply tasks by itself.

Step by step, in parallel with the modernization of management tools the forms of the logistics supply management corps had to be improved, and changes also had to be made in the staff of the logistics supply troops and the organization of work (the two latter were not part of this article).

The tools

Functioning as a part of the automatic camp data process system of the USA ground forces the base of the logistics supply's automatized data processing system was a camp edition IBM 360/40 computer, which was built in to a trailer just like they did with the TOS. The following units belonged to the IBM 360/40 computer's system in the US ground forces:

- IBM 2040 central data processing system.
- IBM 2540/1 punch-card reader/puncher unit.
- IBM 1403-N1 line printer unit.
- IBM 2821 control unit for controlling the line printer.
- IBM 1443-N1 line printer unit (printing 600 lines or 10 pages in a minute).
- IBM 2520 punch-card reader/puncher unit.
- IBM 2314 changeable disc storage unit.
- IBM 2401 magnetic tape storage unit.
- IBM 2702 data transmission supervisor unit (the 2702 could accept up to 31 communicational lines, but slower than the 2701).
- IBM 1012 perforated tape punching unit.
- IBM modulator-demodulator unit.
- IBM 557 punch-card puncher unit.
- IBM 029 punch-card puncher unit.
- IBM 059 punch-card supervisor unit.
- IBM 1056-1 card reader unit.
- IBM 1013 punch-card transmission terminal.

- IBM 1051 supervisor unit.
- IBM 2740 informant terminal.

The computer centrals and various data transmission stations were compiled from these units and appliances depending on the application (army, corps, and divisions). The building of the system made land, air and water transportation possible.

The testing of the system took place at the 3rd army corps stationing in Fort Hood. The 1st and 2nd armored corps were each given a computer to try. The employees of the IBM corporation took part in the experiments as the hardware's transporters and the employees of the URS corporation who tested the transported softwares.

In Hungarian relations in the beginning of the 1960s significant arrear could be experienced in the areas of automatization. In means of the automatizaton of logistics supply two basic functions were involved: management and data communication. In the areas of simplification of management, the recording and storage of data certain accomplishments were already made. Such as:

- formation of operative registers;
- unification of mobilization plans;
- formation of the content and form of reports and commands;
- preparation of coded data transmission.

The used technical tools were tabulated according to the following considering the tasks to be carried out:

- Sound recording (magnetophones, Dictaphones). Aim: reporting and reconstructing measures and reports with portable appliances made for military use.
- Transmitting graphic data (picture telegraphs). Aim: speeding up the data transmission from the command post to the logistics supply point. Encryption was not possible.
- Sound-based data transmission (wired dispatcher and radio dispatcher). The wired dispatcher system could not be used on the move. The radio dispatcher was restricted by the danger of wire-tapping.
- Automatic encryption technology (perforated tape appliances) (hectographs and document photo applications). Colored copies of a graphic document could be made in the duration of

2-3 minutes with a colored duplicator. Tempocop copy machines were used to make black and white copies in 1,5-2 minutes.

- Registry appliances (edge punch-card registry pages). On the edge of the paper classification, manipulation openings were placed, so they could be summarized fast after settlement. It was first used by the transportation service.
- Tabletop mechanic, electromechanic calculators. They were able to carry out four basic operations in operational conditions. The results were recorded on a punch tape and forwarded to a data processing center. The next step were accounting automats which could also carry out more complicated accounting tasks.
- Tabletop electronic computers (IME-84, HUNOR-131 and their descendants).

Conclusions

The main aim of this article was to introduce the TACFIRE system, but mainly from the viewpoint of IT appliances' automatization. The tasks of the artillery were introduced in a level that helped to present the technical background and served as a base for the following events.

My aim was to demonstrate the technical environment trough the presentation of automatization endeavors in which later the REVA service was born. The process of the improvement can be easily followed up in those times and today too, so I'm planning to write additional articles in the topic of automatization of the artillery.

The second main aim of the article was to introduce the USA land forces' camp data processing system's third main system, the CS3 system, but mainly from the viewpoint of IT appliances' automatization. All this was limited to a certain part of the technical background, which was used to introduce and analyze the American and Hungarian principles and methods influencing the directions and future of automatization. Besides these I made a short outlook on the calculator (computer) market of the 1960s, and I introduced the beginnings of the Hungarian development trough the short presentation of the HUNOR machine-family.

References

1. Dr. habil. Négyesi Imre: A csapatvezetés automatizálásának egyes tapasztalatai az USA fegyveres erőinél az 1950-es évek közepétől az MN REVA Szolgálat szemszö-géből. Hadtudományi szemle, 2014/4. szám, 33–42. oldal. HU ISSN 2060-0437
2. Rikk János: Kutatásmódszertan; Budapest, 2014. (ISBN 978-963-08-9495-1)
3. Dr. habil. Négyesi Imre: Az Informatikai Szolgálat megalakulása I. Hadtudományi szemle, 2014/4. szám, 42–50. oldal. HU ISSN 2060-0437
4. A számítástechnika katonai alkalmazásának perspektívái. MN REVA Szolgálat Fő-nökség kiadványa (Nyt.szám: 91/317, 1979)
5. Bertalan József: Az amerikai szárazföldi csapatok automatikus tábori adatfeldolgozó rendszereinek fejlesztése. Honvédelem, 1970/2. 38–50. o.
6. Távadatfeldolgozás az automatizált rendszerekben. MN REVA Szolgálat Főnökség kiadványa, Nyt. szám: 91/362, 1980
7. V. M. Bondarenko – A. F. Volkov: A csapatvezetés automatizálása. Budapest, 1980. Zrínyi Katonai Kiadó. (A mű eredeti címe: Автоматизация управления войсками методологические проблемы, Moszkva, 1977)

The Roman Disciplina according to Vegetius

Mónika Beatrix Rikk; Metropolitan University, Budapest

Flavius Vegetius Renatus was neither a soldier, nor a historian, he worked as a clerk, possibly as a *comes sacranum largitorum*.[1] His work, the Epitoma Rei Militaris is the only source about the roman military that was preserved in its entirety.[2] It's dating is uncertain, it was most possibly written sometime between 383 and 450, most likely during Theodosius' residence in Italy, between August 388 and June 391.[3] The work is essentially a collection, it contains various sources. Vegetius' aim was to impress his reader[4], that's why he frequently mentions his sources like Frontinus, Cato, Paternus, Augustus, Traianus, and Hadrianus' Constitutiones. It consists of four books, each covers a different topic. The first one is about enlistment, the second is about the military arrangement, the third is about tactics, and the fourth is about fortresses and water warfare. The Epitoma Rei Militaris is not only important because of it's description of the roman military, but also because it had a great impact on medieval warfare.[5]

In the first chapter of the first book Vegetius explains the roman disciplina, and the reasons behind the greatness of the empire and its (military) superiority over others. He states thet the well-trained soldoer must be confident so he can conquer the enemy easily:

„Scientia enim rei bellicae dimicandi nutrit audaciam: nemo facere metuit quod se bene didicisse confidit. Etenim in certamine bellorum exercitata paucitas ad victoriam promptior est, rudis et indocta multitudo exposita semper ad caedem."[6]

He explains that it is very important to prepare the soldiers for every challange they may have to face on the battlefield with continous training. He emphasizes the necessitiy of strict punishment of idleness.

[1] Watson, G. R. 1972.; 1111.
[2] Watson, G. R. 1972.; 1111.
[3] Watson, G. R. 1972.; 1111.
[4] Watson, G. R. 1972.; 1111.
[5] Watson, G. R. 1972.; 1111.
[6] Vegetius 1885.; 6.

The enlistment officer was the *capitularius* ot *temonarius*. This title was considered a burden, and an officer did everything he could to avoid having to do it.

Vegetius does not mention this in his work, but the primary requirement for enlistment was being born free.[7] Slaver were only enlisted in case of emergency, such as Radagasius' invasion in 407.[8] Initially the enlistment was voluntary because Tiberius stated in 23 that if somebody wouldn't want to be a soldier on their own accord then they are not brave enough for the army. Obligatory enlistment was introduced by Diocletianus, we don't exactly know when, buti n 313 it was already in practice for sure.[9] According to a law by Diocletianus veterans and sons of soldiers were obligated to enlist in case of emergency. Consantinus changed this law in 326, so the sons of soldiers were able to join join the local *curia* instead of enlistment.[10] Sons of soldiers often tried to avoid enlistment by cutting of both of their thumbs thus becoming unfit for military service.[11] However, this practice entailed serious punishment. A veterans son could only join the cavalry if he could afford a horse for himself plus two other horses, or one horse and a slave.

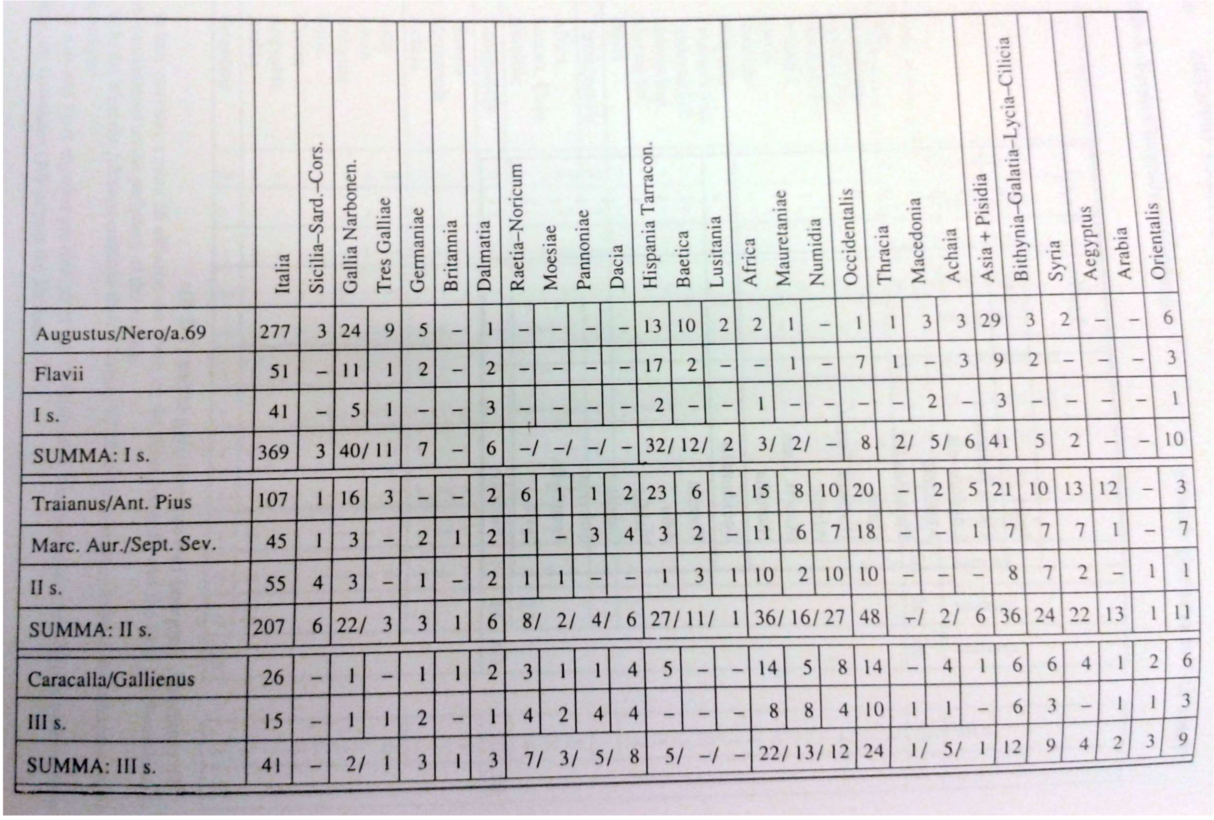
Vegetius considered certain nations to be more fit for military service, mostly because he thought certain climates affect body composition:

„Sed tamen et gens gentem praecedit in bello et plaga caeli ad robur non tantum corporum sed etiam animorum plurimum valet; quo loco ea, quae a doctissimis hominibus conprobata sunt, non omittanus."[12]

Most soldiers of barbarian origins were germanic. Barbarians often elnisted voluntarily to the Roman military because their quality of life lured them. Roman soldiers often didn't want to be deployed too far away from their homes so they didn't mind barbarians being enlisted and being deployed instead of them (however, sometimes they weren't happy about deployment either). The *origo* of the cavalry is often unknown, only 5% of known sources contain surely specified origos.[13] Géza Alföldy located the *origo*s of cavalries according to a *diplomata militaria*.[14] The composition

[7] Davies, R. 1989.; 9.
[8] Jones, A. H. M. 1973.; 614.
[9] Jones, A. H. M. 1973.; 615.
[10] Jones, A. H. M. 1973.; 615.
[11] Davies, R. 1989.; 7.
[12] Vegetius 1885.; 6.
[13] Devijver, H. 1992.; 112.
[14] Devijver, H. 1992.; 112.

of the *ordo equester* was relatively unified, they left their homes so they can participate in centralized management.[15] Barbarians didn't always join the military voluntarily. Sometimes they were prisoners of war or refugees. There were several units named after barbarian tribes, such as *cohors Ituraeorum*, but these didn't entirely consist of barbarians. It was not dangerous to enlist barbarian sodiers, because they were romanized very quickly, and they didn't have too much 'national pride'. Also, they mostly had conflicts with each other, rather than with the Romans so they did not join their forces against them. It was mandatory for them to learn latin, and most of them managed to leanr it very quickly and very well, so they din't even use their mother language anymore.



	Italia	Sicilia–Sard.–Cors.	Gallia Narbonen.	Tres Galliae	Germaniae	Britannia	Dalmatia	Raetia–Noricum	Moesiae	Pannoniae	Dacia	Hispania Tarracon.	Baetica	Lusitania	Africa	Mauretaniae	Numidia	Occidentalis	Thracia	Macedonia	Achaia	Asia + Pisidia	Bithynia–Galatia–Lycia–Cilicia	Syria	Aegyptus	Arabia	Orientalis
Augustus/Nero/a.69	277	3	24	9	5	–	1	–	–	–	–	13	10	2	2	1	–	1	1	3	3	29	3	2	–	–	6
Flavii	51	–	11	1	2	–	2	–	–	–	–	17	2	–	–	1	–	7	1	–	3	9	2	–	–	–	3
I s.	41	–	5	1	–	–	3	–	–	–	–	2	–	–	1	–	–	–	–	2	–	3	–	–	–	–	1
SUMMA: I s.	369	3	40/	11	7	–	6	–/	–/	–/	–	32/	12/	2	3/	2/	–	8	2/	5/	6	41	5	2	–	–	10
Traianus/Ant. Pius	107	1	16	3	–	–	2	6	1	1	2	23	6	–	15	8	10	20	–	2	5	21	10	13	12	–	3
Marc. Aur./Sept. Sev.	45	1	3	–	2	1	2	1	–	3	4	3	2	–	11	6	7	18	–	–	1	7	7	7	1	–	7
II s.	55	4	3	–	1	–	2	1	1	–	–	1	3	1	10	2	10	10	–	–	–	8	7	2	–	1	1
SUMMA: II s.	207	6	22/	3	3	1	6	8/	2/	4/	6	27/	11/	1	36/	16/	27	48	–/	2/	6	36	24	22	13	1	11
Caracalla/Gallienus	26	–	1	–	1	1	2	3	1	1	4	5	–	–	14	5	8	14	–	4	1	6	6	4	1	2	6
III s.	15	–	1	1	2	–	1	4	2	4	4	–	–	–	8	8	4	10	1	1	–	6	3	–	1	1	3
SUMMA: III s.	41	–	2/	1	3	1	3	7/	3/	5/	8	5/	–/	–	22/	13/	12	24	1/	5/	1	12	9	4	2	3	9

[16]

1. Disrtibution of the recruited cavalry

The author explains that people from rural areas were more used to physical activity and harsh circumstances so they became better soldiers. The less a person is exposed to the easier urban lifestyle the more suitable he is for military service:

[15] Devijver, H. 1992.;113.
[16] Devijver, H. 1992.; 118.

„Ex agris ergo subplendum robur praecipue videtur exercitus; nescio quomodo enim minus mortem timet qui minus deliciarum nouit in uita."[17]

However, he also states that if a person of urban origin is enlised they must undergo strict training and teach them to endure such things just like their companions. They must get used to sleeping in tents or even in open air, limited food and the complete abscence of luxury. Their enlistment was less of a problem during the era of the republic, because the conditions in the city were far away from luxurious, for example the only place for taking a bath in Rome was the Tiberis. During those times it was possible for someone to be a soldier and a farmer at the same time, for example Quintius Cincinnatus was plowing his land when he was invited to de dictator. Vegetius states that is the unit stations in one place for a long time, they must resist the temptations of the city.

According to Vegetius the most ideal time for beginning the training of the soldiers is when they reach adolescence. He mentions that Sallustus said that in his time training began when a boy was able to carry the weapons. He thought that it important to start training before „their age would make their limbs stiff". Complete census before enrollment was introduced by Theodosius I. in 383, which is a great source about the age of enlisted soldiers. Studies showed that the enlisted soldiers were aged between 13 and 36 years (the maximum age is 35 according to Cassius Dio)[18], but 75% of them was between 18 and 23. According to Cassius Dio's works enlisting soldiers whose age was inappropriate was punished, ab epistulis officers were forced to resign because of it.

They primarily chosed the tallest men, accouding to certain sources the minimal height for enlistment was 6 feet[19], buti t was certainly well above 5 feet.[20] However, Vegetius thought that height shouldn't be a primary concern: he said that what a soldier lacks in height can be made up for with bravery. The most essential thing was that a soldier must be stronger than a civilian. In later times it was even less typical for soldiers to be tall, because there were far less candidates to choose from.

Vegetius exactly describes the ideal traits of a soldier. He thought that their face is very important, most specifically their eyes (they must be bright-eyed) and also their limbs. Only those

[17] Vegetius 1885.; 8.
[18] Davies, R. 1989.; 7.
[19] ~178 cm
[20] Davies, R. 1989.; 4.

candidates should be chosen whose traits suggest that they will become good soldiers after the training.

„Sit ergo adulescens Martio operi deputandus vigilantibus oculis, erecta ceruice, lato pectore, umeris musculosis, valentibus brachiis, digitis longioribus, uentre modicus, exelior clunibus, suris et pedibus non superflua carne disentis sed neurorum duritia collectis."[21]

After describing their qualities he states again that if they have all these qualities their lack of height can be disregarded:

„Cum haec in tirone signa deprehenderis, proceritatem non magnó opere desideres. Utilius est enim fortes milites essequam grandes."[22]

On the other hand Frontinus, who Vegetius names as one of his most important sources states that a soldier must be tall, because their advantage in height would give them confidance thus making them brave.[23]

He thought that people with certain occupations are more eligible for military service than others:

„Sequitur, ut, cuius artis vel eligendit vel penitus repudiandi sint milites, indagemus. Piscatores aucupes dulcarios linteones omnesque, qiu aliqud tractasse, videbuntur ad gynaecea pertinens, longe arbitror pellendos a castris; fabros ferrarior carpentarios, macellarios et cervorum aprorumque venatores convenit sociare militiae."[24]

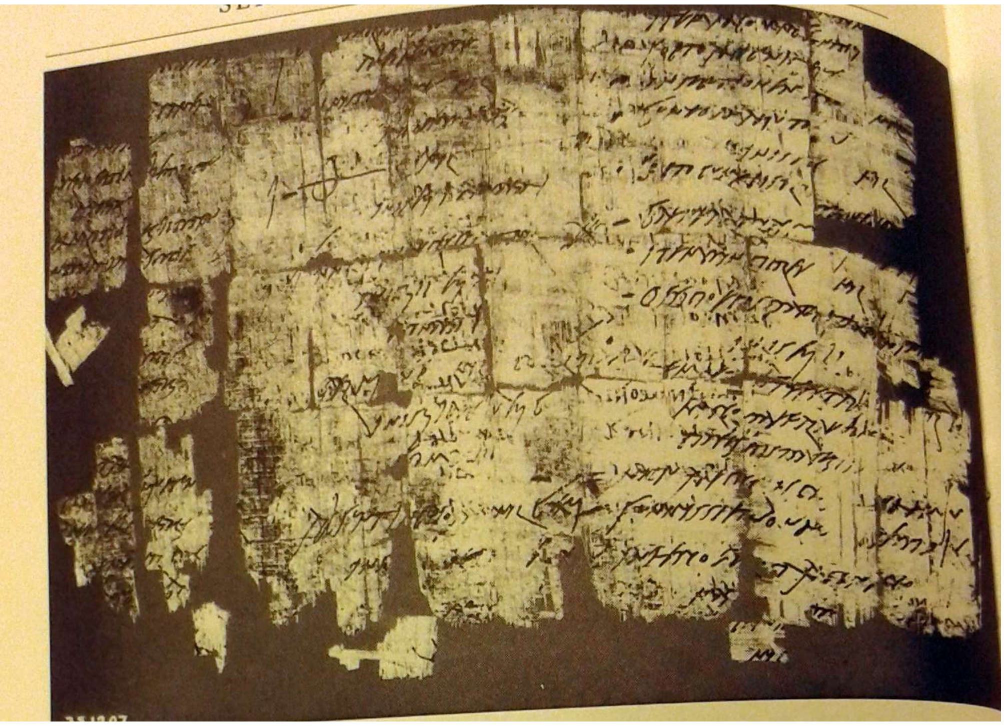
He thought blacksmiths, carpenters, butchers and hunters to be especially fit for service, however, he thought fishermen, fowlers, weavers, cooks, and people doung cerain occupations considered feminine should not be enlisted. For the cavalry units, such as the tribuni angusticlavii legionis they only enlisted from the elite, mostly from Italy.[25] The fate of the empire depended on them, so they only chose the most trustworthy men, criminal record was a ground for refusal (for example people who were exiled but ran away often tried to join the military – this was forbidden).[26]

[21] Vegetius 1885.; 10.
[22] Vegetius 1885.; 10.
[23] Davies, R. 1989.; 8.
[24] Vegetius 1885.; 10-11.
[25] Devijver, H. 1992.; 111.
[26] Davies, R. 1989.; 11.

He tought the most important virtues to be *honestas, verecundi„* and *industria*.[27] He thought that honor would restrain them from breaking the rules and lead them to victory. He thought that the reason behind every past failure and defeat is the inadequate selection of soldiers.

The enlistment process

Every step of the enlistment was precisely documented, it took a long time, because it was a highly complex process. Candidates had to go to an enlistment office and bring a letter of recommendation (*epistula commendatica*), where they underwent the probatio.[28] The candidate was called *probatus*, they examined their physical endowement, sight, they went trough various medical exams.[29] They recorded their name and regognizances (*iconismi*). When their name was recorded to their unit, they earned the *signatus* status, and their arrival was documented in the *acta diurna*.[30]



2. Records about a soldier's fitness on a papyrus from Egypt[31]

[27] Davies, R. 1989.; 6.
[28] Davies, R. 1989.; 3.
[29] Davies, R. 1989.; 7.
[30] Davies, R. 1989.; 18.
[31] Davies, R. 1989.; 34.

However, it wasn't unusual for candidates to escape before before they were even assigned to their units. It was also common, that they got assigned, but they deserted, and tried to apply to an other unit. If somebody deserted, but returned after a short time it was condoned, but if they did it again they had to face serious consequences, especially if they tried to sell their weapons which was a major crime (since Caracalla). [32]

The records written during the probatio were sent to their units, but their kept a copy in the recruitment office. After these the training began, and after completing it they earned their *numerus relatus* (*miles*) status, and they got their military insignias. The *signaculum* was a lead sheet with their name hanging around their neck, which was given to them over a ceremony along with their complete equipment. Vegetius thought that it is important to test the newly enlisted soldiers on duty, because there were candidates who seemed promising, but failed the probation. He stated that these soldiers must be immediately rejected, and replaced with better candidates.

Vegetius ofren refers to a long period of peace, which resulted in the disappearance of the training practice, which can be evoked trough various writings by historians. The physical training is crucial, because soldiers need to go trough it before they were given weapons. It lasted for at lest 4 months, and their results were recorded. The training took place on the campus (*in campo*), but there were also an indoor area for bad weather conditions (*sub tecto*). However, they often trained in open air even in bad weather, because they needed to get used to the conditions of the battlefield. There was a platform next to the *campus*, and the training officer watced them from there (sometimes audience too). Religious events also took place here, they also offered their sacrifices here (mostly gazelles)[33] to the *campestres* at the *campestres* altar. The campestres were the (probably) Gaul gods of the training ground, Iuppiter Optimus Maximus and after the second part of the 2nd century Mars Militaris and Victoria Augusta. The training officer was the *campidoctor*, the weapon instructor was the *doctor armorum* or *doctor armatura*, the trainer of the battalion was the *doctor cohortis*, and the trainer of the cavalry was the e*xercitatores* and the *magister campi*.

The first thing the soldiers had to learn wa sthe parade step, which was acquired trough constant fast marching.

[32] Davies, R. 1989.; 11.
[33] Davies, R. 1989.; 119.

„Primis ergo mediationum auspiciis tirones militarem edcendi aunt gradum. [...] Militari ergo gradu XX milia passum horis quinque dumtaxat aestiuis conficienda sunt."[34]

It was very important to keep their place, because an irregularly marching unit is more likely to be defeated. If they march too close they can impede each other's free movement, but if they march too loosely, the enemy can easily get amongst them. Regular marching was called ambulatio, they had to march 20 miles in 5 summer hours, 25 miles in the faster version. They never went faster than this, because they would have tor un, and that way they couldn't keep their place. However, they trained by running, which, according to Vegetius was important because this way they could approach the enemy more confidently, and could also run away if necessary. They were also trained to jump so they can go trough uneven grounds and trenches. Vegetius said that the goal was to intimidate the enemy, and to defeat them before they even had the chance to defend themselves. Through the summer months the young soldiers were taught to swim, because it was possible that they had to cross rivers, for example if the bridge fell, or if there were a flood.

„Natandi usum aestiuismensibus omnis aequaliter debet tiro condiscere. [...] Non solum autem pedites sed equites ipsosque equos uel lixas, quos galiarios vocant, ad natandum exercere percommodum est, ne quid imperitis, cum necessitas incumbit, eveniat."[35]

Vegetius said that according to old sources the drills took place next to the Tiberis and they refreshed themselves after it by taking a swim in the river.

„Ideoque Romani veteres, quos tot bella et continuata pericula ad omnem rei militaris erudiverant artem, campum Martium vicinum Tiberi delegerunt, in quo innuentus post exercitum armorum sudorem pulueremque dilueret ac lassitudinem cursus natandi labore deponeret."[36]

If they only had the chance to swim far away from the camp, they lived in tents next to the water.[37]

The method for learning to use arms was called *armatura*. The drills took place every morning and afternoon by the poles (*palus*) on *the campus*. These were 6 feet tall, which indicates that this

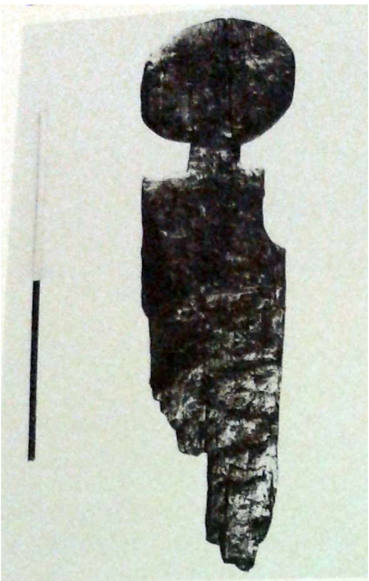
[34] Vegetius 1885.; 13.
[35] Vegetius 1885.; 15.
[36] Vegetius 1885.; 15.
[37] Davies, R. 1989.; 118.

must have been the minimum height for soldiers.[38] They were given weapons two times heavier than the real ones (wooden swords and spears), so they could use the regular ones with ease.

„Antiqui, sient inventur in libris, hoc genere exercuere tirones. Scuta de vimine in modum cratium conrotondata texebant, ita ut duplum pondus cratis haberet, quam scutum publicum habere consuevit. Idemque clausas ligneas dupli aeque ponderis pro gladiis tironibus dabant."[39]

This method was also used for training gladiators.

„Palorum enim usus non solum militibus sed etuam gladiatoribus plurimum prodest."[40]



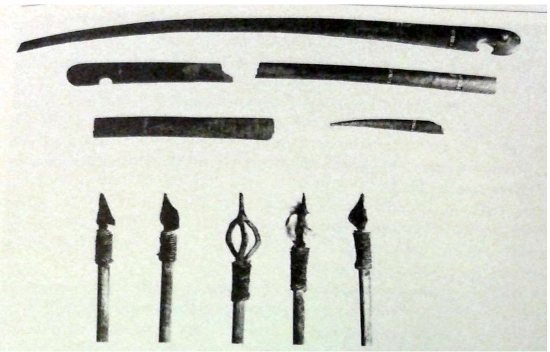
3. Palus; Annerwell street, Carlisle[41]

They were taught not to cut but to pierce with their swords, because iw was more likely to be fatal. People who fought by using the edge of their sword was ridiculed, and considered a weak opponent. During the use of the sword it was inevitable for the left arm and side to be uncovered.

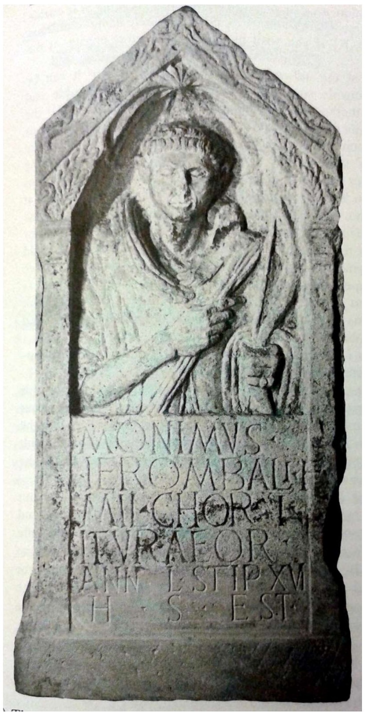
They taught about one third or one quarter of young soldiers to use bow and arrow by the palus with daily training. Vegetius emphasizes that the trainers of the archers must be chosen very

[38] Davies, R. 1989.; 6.
[39] Vegetius 1885.; 15.
[40] Vegetius 1885.; 15.
[41] Davies, R. 1989.; 78.

carefully. They were taught the proper way to hold and tighten the bow, and to concentrate their attention to one point. They had to learn to use the bow and arrow on horse as well as on foot.



4. Arrowheads; Bar Hill, Scotland[42]



5. Epitaph of Monimus, archer of the cohors Ituraeorum. Ituraea privided archers for the Roman army since the early republican era[43]

They were taught to throw rocks both by hands and sling. This was useful because this way they didn't have to carry weapons (primarly on rocky terrains), so they used slingers in every battle.

[42] Davies, R. 1989.; 111.
[43] Davies, R. 1989.; 109.

Every soldier bought five spears (*martiobarbuli*) with them in the hollow of their shields. The advantage of this weapon was that it could both seriously injure people and horses.

They constantly parcticed jumping to the saddle on wooden horses so they could quickly jump onto their horses in unexpected situations. At first they had to complete the task without their weapons, then with them, from both sides, with their swords drawn then with their spade.

Marching with weights was also part of the training, so they got used to carrying their own weapons and supplies from time to time. The author quotes Vergilius on the topic:

„Non secus at patriis acer Romanus in armis

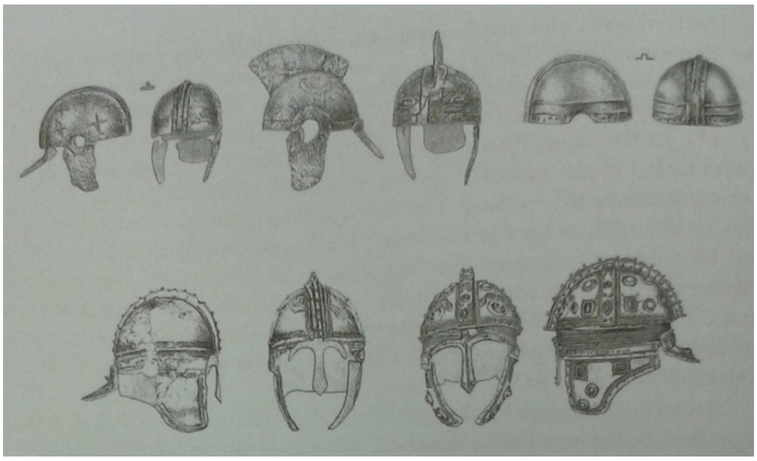
Iniusto sub fasce uiam cum carpit, et hosti

Ante expectatum positis stat in agmine castris.”[44]

They had to (both the infantry and cavalry) comlete a march (10 miles from the camp and back) three times a month. It had to be done in full equipment and with weapons, completely in order with a specified speed, which was occasionally made faster during the march. The cavalry also marched fully armed, they also practiced chasing the enemy.

Their weapons were developed in the example of Goths, Alans, and Huns. From the foundation of Rome to the age of Gratianus the infantry wore armour, but they thought itt o be too heavy, so after some time they refused to wear it thus becoming vulnerable against the Goths' arrows.

[44] Vegetius 1885.; 21.



6. Late Roman helmets from Pannonia[45]

Vegetius thought that is shouldn't be condoned that they take off their armour, but they should be accustomed to wearing them. Their protective armoir consisted of a helmet, a breast plate, iron greaves, and a gauntlet on the left arm for the archers. Vegetius emphasizes that defense is just as important as offense. Soldiers have been accustomed to wearing helmets by making them wear Pannonian leather helmets.

The weapon of the infantry was the spade (*piles*), that had a triangular iron head that was up to 1 foot long. It was designed this way because due to the triangular shape it was impossible to pull it out from a shield, and it could also injure the armour more easily. When Vegetius wrote his work he said these were not in use anymore. The primary weapon for the barbaric heavy infantry was the bebrae, they brought 2 or 3 of them to every battle.

Soldiers fighting in the first line were called *principes*, the second row *hastati*, and the tird *triarii*. While the others were fighting, the *triarii* were waiting in a kneeling position, protecting themselves with their shields. There were battles won by the *triarii* after the *principi* and the *hastati* were already destroyed.

It was important to teach recruits how to set their camps properly, so they could be safe in the view of the enemy both by day and night. They had to set the camp so its size would accomodate to their headcount, and the shape to the terrain. On the ideal side there is plenty of wood, water, food and forage, and isn't surrounded by high grouns (that would make the enemy and also floods very

[45] Kovács, P. 2003.; 36.

dangerous).[46] Vegetius stated that if they weren't faced by immediate danged the ideal size of the trench is 9 feet wide and 6 feet deep, the rampart on the inside should be 3 feet tall, and if there was danger, the trench 9 feet wide and 6 feet deep, and the rampart 4 feet tall with palisades on top. If somebody didn't do their job well they were punished, because someone who recieved their training should be able to doh te job fast, quickly, and without making mistakes.

Part of the drill was to learn to organize into various formations. It was important to organize into a straight line in the shortest time possible while keeping equal distance from each other. This was practiced until they could do it without any difficulties.

In the conclusion of the work Vegetius addresses the emperor, he ensures him about his loyalty:

„Haec fidei ad deutionis intuitu, Imperator inuicte, de uniuersis auctoribus, qui rei militaris disciplinam litteris mandauerunt, in hunc libellum enucleata congessi, út in dilectu atque exercitatione tironum si qui diligens uelit existere, ad antiquae uirtutis imitationem facile conroborare possit exercitum."[47]

He repeats again what he emphasized during the work: a good army can only be achieved along the lines of the ancestors, the superiority of the Roman Empire can only be restored trough the revival of *disciplina*.

[46] Davies, R. 1989.; 127.
[47] Vegetius 1885.; 29.

Bibliography:

Devijver, H.: *The Equestrian Officers of the Roman Imperial Army*. Mavors Roman Army Researches 9. Stuttgart 1992.

Davies, R.: *Service in the Roman Army*. Edinburgh 1989.

Jones, A. H. M.: *The Later Roman Empire 284-602. A Social, Economic and Administrative Survey 11.* Oxford 1973.

Army in Pannonia. *An archaeological guide of the ripa pannonica*. Pécs, Szekszárd 2003.

Watson, G. R.: Vegetius Renatus, Flavius. in. OCD 1110-1111.

Vegetius Renatus, Flavius: *Epitoma Rei Militaris.* Oxford 1885.

RED

7234 5610 33

ISSN 7234561-6

2017/1