# An Approach for Enhancing the Security of Remotely Accessible, Sensitive Services with On-Site Monitoring

Tuomas Kekkonen
*VTT Technical Research Centre of Finland*
*Oulu, Finland*
*tuomas.kekkonen@vtt.fi*

Teemu Kanstrén
*VTT Technical Research Centre of Finland*
*Oulu, Finland*
*teemu.kanstren@vtt.fi*

***Abstract*—Commonly, the deployment environment of software based services cannot be predicted in advance, which leads to need to have specific solutions to monitor their security and reliability during runtime. These services are also commonly accessed remotely, leading to further complexity in their monitoring and analysis. The work presented in this paper proposes a solution for enhanced security monitoring of such services, providing for increased confidence in the service security and reliability. The proposed solution uses near-real time information collected about the service and its environment during its use. The approach is evaluated using a case study of monitoring a mobile payment service showing increased awareness and confidence of service security.**

***Keywords-network monitoring; security situation awareness; security management; security policy; network capture***

## I. INTRODUCTION

Modern software intensive systems are increasingly pervasive and used to perform critical and sensitive operations. In many cases, the service is provided as remotely accessible through various terminals, such as mobile devices. For example, a push-mail service can be used to deliver email to mobile devices from corporate and Internet service provider networks, or a mobile payment system can be used to make payments with a mobile device over various vendor and provider networks. These services deal with sensitive corporate or personal information, and handle transactions related to real world assets such as money. These types of services are commonly deployed in unpredictable environments, where their security and reliability are impacted by varying constraints and evolves over time. The hosting infrastructure itself varies across deployments and the clients used to access these services can be varied and mobile.

Typically for such services, their criticality and sensitivity is recognized and thus a security policy is defined describing their security aspects and the required countermeasure to possible security threats. However, extensive and relevant management of such security policies is an exhaustive and resource draining task. Tasks such as monitoring of specific services and their auditing are important but often difficult to make cost effective. Especially in multi-domain environment where services are widely deployed and serving sensitive data, such as described above, the assurance of the operation is vital but difficult to maintain. The operating environment sets limitations to the monitoring and also affects the operation efficiency. However, the affected efficiency may not be perceived without some means of monitoring.

A perceived weakness of security monitoring is also the inability to respond to different situations during monitoring. In a complex system the management of countermeasures is often tedious and handled by the administration. However, in case of remotely accessed services, it is often possible to apply an approach where a certain profile of the expected system behavior is defined and a specific response is defined for such observed situations. As a response, for business purposes it is often enough to deny the service when problems are observed until the situation has been analyzed and resolved. If this early response is not applied, later problems can escalate into more serious issues, complaints and reclamations.

This paper presents an easily deployable and flexible monitoring solution for remotely accessed services. It gives the security management a source of information for the observed services and the ability to evaluate the capability of the service prior to transactions. We present our approach from the viewpoint of generally monitoring different aspects of software-intensive remotely accessible services, and use a case study of its application on a mobile payment system to evaluate the efficiency of the approach. The nature of the mobile payment service as widely spread to multiple and technically varying locations helps illustrate the different aspects of the approach.

The rest of the paper is structured as follows. In Section II, we discuss the problem domain of monitoring networked services. In Section III, we present our approach for security monitoring. In section IV, we describe a case study of applying our approach on a mobile payment system. In Section V, we discuss the results and the observed applicability of our approach. Finally, conclusions end the paper.

## II. NETWORK MONITORING

Network monitoring can have different motives and targets. A common goal is to detect failing or slow components to be able to address possible issues promptly and

 ISBN: 978-1-61208-010-9

to gain more successful operation. Network monitoring is also used to enhance security or performance. Typical solutions applied for network security monitoring are intrusion detection and prevention systems [1]. These solutions are based on detecting anomalies and tracking signatures on network traffic and behavior (e.g., [2], [3]). These systems can support a wide range of analysis and reaction, providing protection for, and information about, vulnerable states in a system. They operate best in large scale networks and can identify great amount of different types of events. However, due to their operational constraints such as the vast amounts of information for large-scale network traffic that needs to be processed, they generally can only focus on a shallow analysis of e.g., network packet headers. A comprehensive analysis would require deep packet inspection level of analysis, which would require large-scale resources that would make their applicability non cost-effective. This enhancement is studied by [4].

The effectiveness of these tools also depends on the quality of their signature databases and algorithms that are used to analyze the captured information. These are provided and updated by the product manufacturer or community. Thus their relevance depends on the activity of the signature providers.

The target of intrusion detection and prevention is specifically to provide information about the activity the system is facing. This information is usually used to block some traffic in the network and is an administrative task. Security management on the other hand has the intent to define security policies and to know that the system is implemented according to the specification. In a growing and dynamically changing systems where maintenance and installations are done regularly the upkeep of the security policy requires audits on systems to evaluate its conformity with security policy.

In any case, continuous monitoring of the defined security policies is needed to gain confidence on the secure and reliable operation of the deployed services. To be commonly applicable, such monitoring solutions need to be defined as addressing the security and reliability requirements while at the same time to be defined within capabilities of network capture based feature inspection. The goal should be to minimize the intrusiveness of the monitoring by making the implementation of security monitoring possible without requiring additional installation or changes in the environment where the product is delivered.

Requirements and capabilities for network monitoring are set by the target network and service. Optimally, we should be able to monitor as much as possible with a minimal set of deployed monitoring points. For example, a single Ethernet based subnet environment could be monitored from a single accessible location when all data is broadcast to all parties. When possible, the network architecture can also be optimized for the monitoring purposes by adding monitoring to a central location.

### *A. Network Security Management*

A product, which requires to be deployed in varying types of environments can face various issues such as malicious users and excessively loaded networks. When deployed to such unsafe environments, the operation cannot be assured and the cause for this can be difficult to track down. Again, security management needs to assure that the system implements the required security policy. In an optimal case, this can be assured by providing the service product with a complete setup including hardware and software that is configured according to all the security policy requirements. Other approaches include providing just the software to be run on the customer environment, which is often a more practical scenario, especially for smaller customers. The choice of deployment strategy impacts also the complexity of governing the service security and reliability in its environment. A more complete deployment can mitigate the possible risks but not completely eliminate them, including the need to manage the infrastructure, its updates and other security and reliability aspects.

Most network security breaches originate from poorly defined or implemented security and lack of security management. According to annual Symantec survey [5], the most common reason for data breaches in 2009 was the theft or loss of material. The second highest category of the survey is named insecure policy, referring to the failure to create and administer policies to enhance security, including the user operation.

Technical breaches in software security are caused by vulnerabilities, which are exposed to the hacker through their own investigation or through other venues. Effective security management needs to react to the discovery of these vulnerabilities before they are widely in use by the hacker community. The required responses such as software updates and counter-measure configurations need to be managed by the users or the administration.

Overall, we can state that the overall security of a network is a sum of the combined operation of all participants in the network. Therefore the behavior of all users in the network is of interest to the different parties using the network and should be monitored. For example, the presence of clients with diverging traffic patterns or outdated software can be taken as indicators of potential security and reliability confidence lowering aspects in the overall system. Similarly, any issues observed on the server side are obvious indicators for the expected service quality. Our approach adds the valuable information of the network monitoring to cover the shortages of typical security management solutions to make it more interactive.

 ISBN: 978-1-61208-010-9 

## III. Our approach

The goal of the work presented in this paper is to enhance security awareness for remotely deployed services handling sensitive information. Here this information is provided not only for the service administration but also the end user as a mobile payment application. This includes defining a security policy for the remotely deployed software that can be used as a basis to provide assurance of its operation. Because we cannot assume to have complete knowledge of the actual deployment environment, the policy needs to specify generic requirements that reflect security awareness in the context of that specific service. To cover the security policy, the available monitoring information in an actual deployment environment is mapped to each requirement specified in security policy. This model is then used as a basis to monitor the system and to evaluate its security capabilities in a continuous manner.

Security management usually defines the monitored policy by evaluating the risks the system might encounter. In business minded information security the risks can be classified into assets, vulnerabilities, countermeasures and threats [6]. Here these classes are used to define an example security policy and security features based on this risk analysis. This is to show an example of the process of adapting a risk analysis into security policy and network monitoring features. We will present an example of a concrete security policy for a mobile payment system in Section IV-D.

Our approach consists of the following steps

1) Risk analysis
2) Security policy definition
3) Infrastructure analysis
4) Monitoring point definition
5) Continuous monitoring
6) Information synthesis and presentation to user

We focus in this work on the monitoring aspects, but it is worth noting that we use input from the previous steps that are assumed to be present. In this work we build on the work presented in [7]. As a security policy definition assume the presence of documents such as Assurance Profiles as described in [8].

Risk analysis evaluates the key points in the system and determines the value of their successful operation. It also attempts to list the situations the system might face and prioritize the risks related to those situations according to their severity. These risks are covered with certain security measures defined in a security policy. It specifies, which features the system components need to implement to lower the possibility of a risk and to decrease its effect in case of occurring. What also needs to be defined is the details of the actual monitored variables used to determine the state of requirements on the security policy.

After this it is up to the security management to assure that the policy is followed. To arrange an automated monitoring on the security awareness inside the system the security management needs to analyze the infrastructure to identify the points where a certain security policy should be present. This analysis is a source of information when the monitoring is deployed into the system. Successful deployment of monitoring with appropriate security policy definitions results in providing a continuous view of the security policy compliance on the system.

A multi-domain monitoring solution has to be flexible in supporting different types of target network environments. This includes being able to perform within the limitations set by the communication protocols and network monitoring capabilities available. To organize the monitoring information, we use a four way model based on security events, traffic rations, security presence and online testing. The following subsections describe each of these attributes and the type of variables they consist of. Variables are defined in accordance to security policy that is defined according to the risk analysis. In addition to these aspects, the security policy needs to define the expected values for the variables, including the limits for each value to remain within accepted range. Practically, choosing the variables is also affected by what is possible to monitor in the service infrastructure, which is affected by factors such as infrastructure access and available monitoring tools.

### A. Security events

With the term security events we refer to the input events generated from security monitoring tools such as intrusion detection systems. Security situation awareness is a related term used in research to gather, combine, and understand constantly updating security state of the overall system. Methods for security situation awareness are presented, for example, by [9] and [10], largely based on combining of observed security events. The security events are the events that are used as a basis to for the analysis of the current security situation, providing a basis for assessing the confidence in the security and reliability status of the observed system.

For example, an intrusion detection system generates alerts based on rules, which have different priorities and cause different types of alarms. Alarm priority can also be used to provide added value for security situation awareness, for example, to make a more informed decision on how to respond. Automated analysis systems such as intrusion detection systems often cause false alerts and therefore the response needs to be managed manually.

In this work, the information provided by security events constitutes of alerts generated by Snort intrusion detection system and errors reported by the target mobile payment service. When the analysis of their combination is observed as revealing a potential issue, the security situation in the network is considered reduced.

 ISBN: 978-1-61208-010-9 

### B. Traffic Ratios

We define expected network traffic patterns in terms of network protocol distributions. This describes the expected ratio of observed traffic in terms of different protocols, including the encrypted and non-encrypted versions of the same protocols. Additionally, specific protocols can also be classified as insecure and thus their presence at all can be considered a feature for analysis. For example, existence of bittorrent protocols can lead to high traffic loads and decreased performance on network, and thus bittorrent can be classified as unwanted because of possibly causing decreased availability.

The ratio of these different types of protocols is compared to the amount of total observed traffic and to observed ratios between different types of communication in the network. These defined ratios are taken as rules for the expected traffic distribution between the different traffic types. Traditional methods of anomaly detection or pattern recognition methods can be applied to enforce these rules. However, more specific rules can also be defined to monitor specific protocols in a presumably known network, simplifying the required monitoring process.

### C. Security Presence

Security presence is a term we use to refer to a system having security related features and mechanisms present in the network. Its security value is in estimating the general security awareness. Security presence related variables are those detected from the application variables communicated over the network protocols.

Practically, security presence is detected by monitoring identifiers in the traffic such as short passwords, clear text passwords, old software versions and insecure operating system versions reported in communication messages and security events. Those are mainly gathered from HTTP messages and this is implemented by analyzing pcap files produced by Wireshark.

### D. Online Testing

Online testing refers to active stimulation of running service elements and observation and analysis of the results. An online testing tool can test the service with simulated requests and evaluate the correctness of responses. While it is possible to create customized tools for these purposes, we prefer to use existing tools for genericity and cost-effectiveness purposes. Basic examples of online test tools available on existing systems, which are also used in this work are ping and port scanning tools such as nmap.

Online tests provide information of the systems conformity with requirements and current capability to serve requests with tests that simulate actual operation. A false reply to a request can identify an issue in the authenticity of the communication partner. Additionally the delay in responses imply a general failure in service to respond to requests. These are clear indication of service operation capabilities.

## IV. Mobile Payment Case Study

In this section, we present a case study of applying our approach in the domain of mobile payment. Based on a previously performed risk-analysis and the available monitoring options for the service infrastructure of a mobile payment service, we define a set of relevant security events and network traffic properties and ratios. From this we define what we consider the relevant properties for observing the security presence of the mobile payment service in our environment. Further, we show how using a set of existing network monitoring tools we monitor this security presence from the service infrastructure and use the information in the process of the mobile payment.

### A. Mobile Payment

Mobile payment services allow customers to make purchases using their mobile devices as means of payment. A scenario with monitoring goals and end user delivery is presented on Figure 1 Presented is the typical architecture for a mobile payment that includes:

- Vendor node that receives information of payment for the product delivery.
- Cellular operator provides a phone number for the product and informs the mobile payment operator that a call has been made.
- Payment network instructs the vendor node to commit the delivery when cellular operator informs about the call. Also manages the communications to possible mobile vendor nodes.
- Client device makes a call to the cellular operator provided number that is operated by the mobile payment operator.

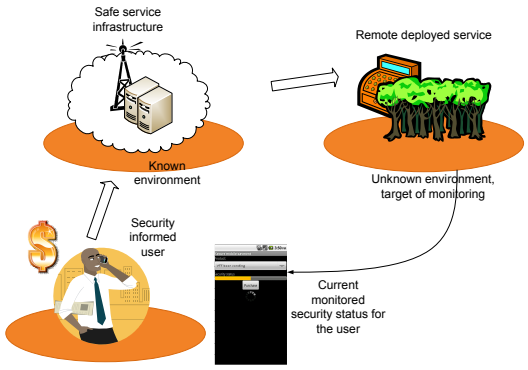


Figure 1. Architecture of the monitoring approach including the mobile payment process with the user, mobile payment provider and a product.

Mobile payment systems are not standardized and implementations in different countries and companies are varied

 ISBN: 978-1-61208-010-9 

[11]. Connection from the mobile payment provider to the vendor node is implemented by the mobile payment provider and does not have specific standards. The different aspects of the provided service such as the information security vary and their quality is up to the different operators. Our target systems operate in Finland, where currently most implementations use a premium billing method based on billing the customer through the cellular provider. As mobile payment systems operate over networks provided by different operators and varying communication links to vendor nodes, it serves as a suitable case to evaluate our approach.

In premium billing the customer places a call to a given number and uses the phone keypad to provide input to the service. Product is billed as a normal service number without any form of identity verification, allowing anyone to use the service with any available phone. This can be a negative factor enabling the illicit use of the device but also a usability enhancing feature increasing sales because of the ease of use. Downsides in this form of billing is the traceability of transaction and reliability of delivery. Network provider might charge the customer even if theres a problem with delivery and the customer needs to place a reclamation to get refunded. The mobile payment provider and cellular network provider operate as separate entities without direct communication, which makes tracing the transactions over network boundaries difficult. Possible technologies in mobile payment field to address these issues include secured simcards capable of requesting pin code on authorization request, near field communication and credit card involvement but none of these are standardized for this domain.

There is a need to improve the reliability of the delivery of products and security of the information exchange. The system cannot observe if the product is successfully delivered. Therefor it is beneficial to have a solution to monitor that the system is operating in desired conditions. Even if we cannot completely remove these issues, we need to strive for an optimal operational environment for the service. We cannot monitor the mobile payment service parameters directly due to confidentiality requirements and due to available access over different networks. For this reason, we aim to monitor generic network parameters according to monitoring parameters defined as relevant for the service in the security policy definition phase.

For confidentiality reasons, we describe here a simulated service environment rather than a production system. We constructed our simulation system using actual production systems as input to define a realistic environment for our evaluation. This also included defining a security policy and test scenarios to address real situations on network operation and typically appearing problems according to input gathered from a mobile payment operator.

To illustrate how the provided monitoring information could be utilized by the service end user, we developed a mobile phone application to display the observed payment service security status to the user. This application is described in Section IV-E.

Considering our general targeted domain of remotely accessed services being hosted over several partners infrastructure, we see mobile payment as a good example. It needs to have parts installed in every vendor that provides possibility for the payment to be done with a mobile phone. Because of this, the environment for those services is varying and assuring its operation through monitoring is beneficial.

### *B. Environment*

Our test environment was constructed with a set of virtual machines, requiring some specific monitoring approaches. To optimize our ability to capture monitoring information, the network in a virtual environment can operate in a way where all the virtual hosts receive all the traffic. This is possible because the typical network latencies and transmission capabilities are not limited in a way they are in actual networks. Ease of setup and maintenance also helped us in our experiments.

The virtual network environment consisted of three hosts. One host was running the target service and had been set up as described below on Table I. Second was running monitoring software. All the tools required for monitoring were installed on this host and run on intervals. Third host was running simulation software, responsible for generating traffic and different situations on the network. These situations are described in Table II.

The tests were run on two different systems. Both were put under test with two different usage scenarios. With this setup the capability of the measuring system for providing useful information was evaluated. The first system was to demonstrate a typical dated system, which cannot perform according to todays security requirements. The second system was an up to date system with operating system less vulnerable to security attacks and up to date software. The setups of both systems are described in Table I. The setups and simulations were set so that not only mobile payment related features but general security features that can affect performance in the target could be detected. This is why HTTP server and browser types are relevant.

### *C. Simulation Scenarios*

Both systems were put under test with two types of simulation. This results in four different scenarios where reaction of the two systems can be observed. The scenarios are described on Table II.

Network load and behavior was simulated using ping flooding and simulated HTTP requests. This is used to cause computers to suffer from the increased network and therefor processing load. HTTP requests were made with the Curl application and scripted to be performed in intervals. Slowloris is a HTTP flooding tool that attempts to create a denial of service situation by sending partial HTTP requests

 ISBN: 978-1-61208-010-9 

Table I
DESCRIPTION OF SYSTEMS USED IN TEST RUNS.

| Type | Feature | State |
|---|---|---|
| Less secure | Operating system | Windows XP |
| | Operating system version | SP2 retail |
| | Apache version | 2.2.10 |
| | Browser type | Internet Explorer |
| | Browser version | 6 |
| | Other services | 2 |
| Highly secure | Operating system | Linux |
| | Operating system version | Kernel 2.6.32-26 |
| | Apache version | 2.2.16 |
| | Browser type | Mozilla Firefox |
| | Browser version | 3.6.8 |
| | Other services | 0 |

Table II
DESCRIPTION OF USAGE SIMULATION DURING TEST RUNS.

| Load level | Description | Method | Value |
|---|---|---|---|
| Low load | Network load | ping flood | none |
| | System load | cpuburn | none |
| | HTTP load | Timed requests | normal |
| | HTTP vulnerability | Slowloris | none |
| | Payments | Scripted | few |
| | Logins | scripted ssh logins | few |
| | Behavior | HTTP passwords | none |
| High load | Network load | ping flood | full |
| | System load | cpuburn | full |
| | HTTP load | Timed requests | 10/second |
| | HTTP vulnerability | Slowloris | run |
| | Payments | Scripted | 10/second |
| | Logins | scripted ssh logins | 1/second |
| | Behavior | HTTP passwords | few |

to keep multiple sockets to the server open. It was used to exploit the old version of apache HTTP server.

The goal of the scenarios was to evaluate the ability of the monitoring system to prevent the billing of any excess payment from the customer. This can be handled either at the service provider end or at the customer end. The service provider can refuse the service request based on observed issues in the service infrastructure when a request is received. At the client end the terminal can produce a warning to the user about potential security and reliability issues observed in the mobile payment service that is being accessed, when this information is available.

Payment requests are included in the simulation scenarios. Their success rate is the measure of successful operation of the mobile payment system. The success rate of providing useful security status information to the monitoring system client (service provider or customer) in terms of correctly identifying the simulated security problem scenarios is the measure of our approach in evaluation. Payments were simulated with tool developed by a mobile payment service provider.

### D. Monitoring

As described before, our solution is mainly targeted as an automated and easily deployed security policy monitoring system. For our case study we defined a security policy to see different levels of implemented security in the set of chosen scenarios. The policy defines a feature and a risk type it is covering. Some features target the host running the service and some measure the relevant properties of the overall network environment. The target system was desired to comply with features specified on Table III. In this table examples of monitoring sources used are also described. Single requirement is usually covered with multiple sources.

Table III
DEFINED SECURITY POLICY. DESCRIBES THE SECURITY REQUIREMENTS ORDERED BY THE RISK TYPES THEY ARE COVERING. ONE MONITORING SOURCE IS ALSO DESCRIBED FOR EACH.

| Definition | Source |
|---|---|
| Asset | |
| Hardware operates properly. | Produces traffic |
| Stays connected to network. | Ping response time |
| Responds quickly to requests. | Service response time |
| Service is not under heavy load. | No service errors |
| Vulnerability | |
| Follows generally secure behavior. | Vulnerability scan |
| Does not have extra ports open. | Port scan |
| Traffic profile. | Ratio of HTTP |
| Does not send clear text passwords. | HTTP passwords |
| Does not use short passwords. | HTTP auth |
| Uses latest software versions. | HTTP Server field |
| Uses secure operating system. | TCP fingerprint |
| Countermeasure | |
| Uses firewall. | Port scan |
| Encryption is used. | HTTPS messages |
| Uses secure browser. | HTTP agent field |
| Monitor system does not fail. | New monitor data |
| Threat | |
| Non familiar users on network. | Failed SSH logins |
| Service is not abused. | IDS alerts |
| Host is not under attack. | IDS alerts |

This model was constructed to detect issues in implementation of the security policy and the relevant security features. This is based on identifying security related features through monitoring the messaging in the on-site network. The monitored values were combined to derive a binary statement of each defined security feature. These statements construct the model for the overall security. Variables from network traffic were chosen to provide needed information to cover the points defined in security policy. The variable types are described on Section III.

### E. Deployment

A mobile application was developed to list available mobile payment services and to display their current security level. This was to demonstrate the usability of the information also for the service end user. Information was delivered through a socket connection from the monitoring network to a mobile application. The information was visible to the user at any time as a status bar indicating the current level of security in terms of the number of features reported as ok. Then it is up to the users decision to determine when the security level is acceptable. In a more refined version the service provider can decide how a certain security level

 ISBN: 978-1-61208-010-9

affects the transaction and the detailed security information can be hidden from the end user if that is desired.

## V. Results and Discussions

The goal of our case study was to evaluate the effectiveness of the applied approach in detecting any reliability and security issues in the current security implementation level and the usage of the network. Gained benefit would have been shown as better success rate on service. This would result in reduction of failed attempts due to early rejection of requests, which is desired for the transaction process.

Running the tests shows that the pre defined rules are easily detected in the deployed systems and the security features are correctly mapped. Results of each scenario is listed on Table IV. This specific set of scenarios also shows that the information is usable in determining the reliability of the service delivery. The less secure system setting is clearly vulnerable. This is mainly based on the research on outdated software being less secure and effect of security awareness of users in overall security. Outdated Windows system and Apache server alone constitute vast amount of vulnerabilities. This is caused by the fact that they are highly popular and therefor highly exploited. Resulted product delivery effect was however only observed as slight increased delay. The best scoring scenario is the high security setup with low load. On that scenario the monitoring detects the situation to be less loaded and security setup to be proper. This is what was intended to be discovered with the monitoring.

A more detailed simulation scenario could have exploited the target systems more and affected the operation more dramatically. This was not intended but a general simulation scenario was more useful to illustrate the capabilities to detect general security situation, not a scenario where the system is under carefully planned attack.

With this monitoring two aspects of the network security are known. The intrusion detection system style monitoring provides information about the current usage the target system is facing. Here this is combined with knowledge of the level of security implemented in the target system. This information is used to evaluate the capability of the system under different circumstances since both details are known. Then the service requests can be rejected when there is a bigger change of information leakage or failed transaction.

The viewpoint here is to observe the monitoring as the service provider. Their goal is not to let consumers make requests when there is a high possibility that the request will fail or information will get captured. They can define rules to remain in a certain level of confidence in the successful delivery. They do not need to require all the requirements to be fulfilled but some might complement others. For illustration in this work the service provider sets their rules as defined here:

- Hardware must not fail.
- Must respond on network.

Table IV
Results from the four scenarios. 1. low security, high load 2. high security, high load 3. low security low load 4. high security low load

| Feature | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| Hardware operates properly. | OK | OK | OK | OK |
| Stays connected to network. | OK | OK | OK | OK |
| Does not have extra ports open. | FAIL | OK | FAIL | OK |
| Uses firewall. | FAIL | OK | FAIL | OK |
| Responds quickly to requests. | FAIL | FAIL | OK | OK |
| Traffic profile. | FAIL | OK | OK | OK |
| Follows generally secure behavior. | FAIL | FAIL | OK | OK |
| Encryption is used. | FAIL | OK | OK | OK |
| Does not send clear text passwords. | FAIL | FAIL | OK | OK |
| Does not use short passwords. | FAIL | OK | OK | OK |
| Uses latest software versions. | FAIL | OK | FAIL | OK |
| Uses secure operating system. | FAIL | OK | FAIL | OK |
| Uses secure browser. | FAIL | OK | FAIL | OK |
| Service is not abused. | FAIL | FAIL | OK | OK |
| Host is not under attack. | OK | OK | OK | OK |
| Service is not heavy load. | FAIL | FAIL | OK | OK |
| Non familiar users on network. | FAIL | FAIL | OK | OK |
| Monitor system does not fail. | OK | OK | OK | OK |

- If service is under load software needs to be up to date.
- If service is abused firewall has to be used.

With these rules the service provider would refuse requests on scenario 1. When put under loaded situation the system evaluated as a high security system would still allow requests to be made according to the rules specified. The low security system would reach a state of refusing requests when facing the load. The efficiency to reject requests in early stage based on the assumption that the request would fail later anyway is the key to provide enhanced operability for the system in business sense. Without this type of information, each failed transaction has to be dealt individually to refund the customer.

Various viewpoints can be taken on the application of the monitoring information we provide. From the service provider viewpoint it may be bad to show detailed security level information to the user. Instead it may be better to just refuse service and notify the administration to address any observed issues. However in some cases the user can make better use of the information such as when reading email using a publicly accessible network. Simple level of security was presented to the user in our case as illustrated on Figure 1. In this case, the more detailed information can be provided to let the user make a more informed decision. This is ultimately a business decision based on different properties such as the operating environment and the business domain.

Depending on the interests of the company in question and the liability responsibilities the service provider may or not have interests in securing the service or identifying the customer. In an environment where the legislation is highly consumer protective the provider needs to have mechanisms for traceability and strengthened security.

In implementing any monitoring solution there is also always the trade-off between implementing specific moni-

 ISBN: 978-1-61208-010-9

toring for a chosen service and system and in implementing more generic monitoring approaches. Here we apply a generic monitoring approach that aims to make use of generic network parameters, although the same approach could also be used to make use of more service specific parameters. However, in many cases there are factors such as legislation that prevent the use of specific service information such as customer identifiers or email message identifiers for any such purposes and the generic approach is the best suited one. The generic approach is also easier to reuse across different systems. On the other hand, we recognize the possibility of more specific monitoring approach to provide more service specific information. Here our environment and domain has limited our access to service specific information and thus we apply a more generic approach. In other cases, an analysis of different possibilities is needed to identify the best suitable approach in this regard.

The used infrastructure was based on virtualized network, which slightly affects the credibility of the results. The virtual network has greatly reduced latencies and higher transfer rate capabilities than physically built network. However if the monitoring was deployed on a physically implemented network, the results could actually be more accurate. Then the effect of the simulations would be more easily observable because of the reduction in performance. The latencies measured from the network could be affected by load more easily since the physical network performs worse than virtual one. Switching into physical network would cause the need of monitoring to be deployed in a way where the network infrastructure would allow the monitoring to see all the traffic in the network.

## VI. Conclusion

In this paper, we have presented a monitoring approach for providing increased confidence in the security and reliability of remotely accessed services. While it is not a silver bullet, it helps in providing increased confidence in the service operation and to mitigate damage from observed issues. The presented approach is based on six specific steps starting from risk analysis and ending in information synthesis and presentation, and makes use of four types of monitoring information. The application of the approach in a mobile payment case study was used to illustrate the approach in practice.

Results of our case study show a benefit in maintaining a security situation aware monitoring and using it when determining the current capability of the service. The used simulation scenarios can be more refined to show a higher or lower advantage and the monitored security policy can be further developed. While our use of a virtualized environment is slightly different from a typical situation in the mobile payment domain, it can also be taken to provide insights into the increasingly virtualized domain of services and cloud computing of today.

## References

[1] F. Sabahi and A. Movaghar, "Intrusion detection: A survey," in *3rd International Conference on Systems and Networks Communications, 2008. ICSNC '08.*, oct. 2008, pp. 23 –26.

[2] G. Shen, D. Chen, and Z. Qin, "Anomaly detection based on aggregated network behavior metrics," in *International Conference on Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007.*, Sept. 2007, pp. 2210 –2213.

[3] H. A. Nguyen, T. Tam Van Nguyen, D. I. Kim, and D. Choi, "Network traffic anomalies detection and identification with flow monitoring," in *5th International Conference on Wireless and Optical Communications Networks, 2008. WOCN '08.*, May 2008, pp. 1 –5.

[4] H. Salehi, H. Shirazi, and R. Moghadam, "Increasing overall network security by integrating signature-based nids with packet filtering firewall," in *International Joint Conference on Artificial Intelligence*, April 2009, pp. 357 –362.

[5] M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwisle, B. Graveland, D. McKinney, J. Mulcahy, and C. Wueest, "Symantec Global Internet Security Threat Report–Trends for 2009," Technical Report XIV, Symantec Corporation, Tech. Rep., 2009.

[6] A. Herzog, N. Shahmehri, and C. Duma, "An Ontology of Information Security," *International Journal of Information Security and Privacy*, vol. 1, no. 4, pp. 1–23, 2007.

[7] E. Bulut, D. Khadraoui, and B. Marquet, "Multi-agent based security assurance monitoring system for telecommunication infrastructures," in *Communication, Network and Information Security*, July 2007, pp. 1 –5.

[8] B. Marquet, S. Dubus, and C. Blad, "Security assurance profile for large and heterogeneous telecom and it infrastructures," in *The 7th International Symposium on Risk Management and Cyber-Informatics: RMCI 2010*, July 2010, pp. 1 –5.

[9] Z. Yong, T. Xiaobin, and X. Hongsheng, "A novel approach to network security situation awareness based on multi-perspective analysis," in *International Conference on Computational Intelligence and Security, 2007*, 15-19 2007, pp. 768 –772.

[10] F. Lan, W. Chunlei, and M. Guoqing, "A framework for network security situation awareness based on knowledge discovery," in *2nd International Conference on Computer Engineering and Technology (ICCET), 2010*, vol. 1, 16-18 2010, pp. V1–226 –V1–231.

[11] S. Mohammadi and H. Jahanshahi, "A study of major mobile payment systems' functionality in europe," in *11th International Conference on Computer and Information Technology, 2008. ICCIT 2008.*, dec. 2008, pp. 605 –610.

 ISBN: 978-1-61208-010-9 