Identifying Risk Profiles and Mitigating Actions for Business Communication Services

Rebecca Copeland, Noel Crespi
Institute Mines Telecom, Telecom SudParis, Evry, France

Abstract— Enterprises embracing Bring-Your-Own-Device encounter increased risk to data, applications and network resources. The dilemma is how to address threats with mitigating actions that do not unduly disrupt business, yet protect vulnerable assets. This paper proposes a model that identifies risk context and automatically selects appropriate actions. Risks are detected by conflicting observations, timeline discrepancies and risk-indicating behavior patterns. Detected risks are used to construct risk profiles that capture enterprise's risk mitigation policies via customizable prioritization, and business attributes are used to determine business profiles. It is proposed to utilize a novel multi-dimensional weighting to highlight relationships of risks with assets/actions. Best-fit profiles for both business and risk are selected via 'if-the-shoe-fits' process. Then, mitigating actions are determined by fusing the risk and business profiles, and precise actions are established via score 'tolerance bands'.

Keywords— BYOD; MCDM; context profiling; Fuzzification; AHP; OWA; eignvector; OLS; SAW; WPM

I. Introduction

The enterprise world, which is rapidly embracing BYOD (Bring Your Own Device) [6], now has to cope with difficult problems of security and network resource management. BYOD blurs the distinction between personal and business usage. Coupled with enhanced mobility, Cloud and Virtual Office, the new corporate communication environment is becoming the lifeline for business, and it is getting complex and risky. The advent of mobile broadband and smart devices means that personal usage of enterprise resources could ramp up too fast, forcing the enterprise to invest much more in their infrastructure, while contributing nothing towards productivity. This means that the enterprise needs to prioritize business traffic, while personal communication is curtailed.

Paradoxically, while cyber-crime increases, adopting BYOD is often associated with relaxing controls. In [12], two opposing approaches are described: 1) Hands-off; and 2) MDM (Mobile Device Management) with strict control of BYOD terminals. In fact, both are required, hands-off for personal usage and firm control for business. Employees feel that they are entitled to use personal devices unfettered by enterprise restrictions and IT managers still need to control risk. The dilemma is how to grant 'freedom of enjoyment' while defending confidential information and network resources.

BYOD necessitates not only intensified security, but most importantly - *commensurate* actions that mitigate the risk at the appropriate level. Any mitigating measures must accurately respond to the situation, to avoid frustration that is caused by frequent false alarms. If security rules are too stringent, users will bypass them. Frequent demands for additional authentication can be obstructive, and denying service is assumed to be system failures. The choice of security-based actions must be in proportion to the risk impact and severity, but as the number of mitigating actions and options rises to provide greater flexibility, the number of required distinctive observations also increases. The challenge is to construct a model that manages many-to-many match-making, yet generate conclusive decisions.

This paper proposes a method to meet this challenge. The proposed enterprise Business Context & Risk (eBCR) model determines risks associated with enterprise connectivity requests and recommends appropriate mitigating action, moderated by business context. The paper structure is: in section II related work is discussed; in section III, risk mitigation requirements are outlined; in section IV, the model structure is introduced; in section V, identifying risks and defining defenses are described; in VI methods of computing weights, scores and tolerance bands are specified; and in section VII, the conclusions are given.

II. Related Work

The notion of risk profiling is approached differently in every study. In [14], behavior ontology is modelled by attack pattern trees, for multiple activities over sustained periods. In [22], behavior of consuming CPU resources is profiled automatically by a requested-used-estimated model. The need for real-time risk awareness of changing IT systems has been highlighted in [15]. Simple profiling by CIA (Confidentiality, Integrity and Availability) is explored in [2], but over-generalization of risks cannot provide conclusive decisions. In [24], context-based policies are associated with business concerns for network management, but not actively accounted for. In [21], cost-effective actions are optimized by asset vulnerability, but not per service requests context. Dynamic routing of enterprise communication by context is proposed in [4], but it is based on agents' fixed roles. Static role analysis based on RBAC (Role Based Access Control) is very common [5] [19], but not in real-time context.

The profile context computation requires a reliable aggregation method, such as provided by the MCDM (Multiple Criteria Decision Making) family of methods. MCDM, which is still expanding as predicted in [3], now includes heuristics and behavior analysis, not just pure optimality. The most popular are SAW (Simple Additive Weighting) and WPM (Weighted Product Model) that are compared in [14] and [13]. AHP (Analytic Hierarchical Process) is used in [17] to calculate preferences for inter-company links. AHP is also used in [23] to determine fuzzy scale of risk severity and impact on network security. However, none of the MCDM methods

978-3-901882-48-7 (c) 2012 IFIP

provide proportional corroborative aggregation that handles conflict reliably and incorporates the evidence credibility, hence the author's method, as in [16], is deployed.

Modelling realistic business/risk status requires a wide scope of sources. Extracting meaningful information from computer log files, which is feasible, according to [25], can add vital insights. Spatial and temporal factors are crucial to service request analysis. In [18], temporal/spatial events are correlated to identify past security risks, but not attempting to evaluate the request. In [1] temporal dimensions are used for spotting anomalies, but without profiling behavior, and many other risks are listed in [13].

III. Risk Profiling Solution Requirements

A. Scope

The proposed solution is based on modelling context for the request. The eBCR model determines service delivery parameters for each request according to business context, as is proposed in [20]. This is extended in this paper to support risk context too. The requested service can be of any IP connectivity type, both IP Voice and Data, but excluding legacy Voice. Devices may access the network via corporate WLAN/LAN, MNO's network (3G/4G) or via WLAN hotspots. Service requests may be internal - with destinations on the enterprise network (Person-to-Person or Data applications), or external - with destinations on the internet or mobile networks. Thus, the policies for such service requests need to be enforced on both the enterprise internal networks and on the users' personal mobile carriers' network.

Unlike the common *asset-centric* approach to establishing security measures, this solution is *request-centric*. It is designed to establish policy rules for every service request. Using internal information, the model allows the enterprise to recognize undesirable behavior, determine the appropriate mitigating action and service delivery option, and convey the results to the network providers (both internal corporate network and external mobile network) to be enforced during the service delivery. The main issue is to identify the prime risk per connectivity request, for which there is a commensurate action, with determinable level of severity. The eBCR approach considers usage pattern (profiles) from the innocuous to the extremely damaging. The model covers circumstances ranging from high priority service request that needs assured quality, to aggressive attacks that require banning access. Establishing these behavior profiles is not an exact science, so this model has to deal with varying degrees of uncertainty, yet it must produce a clear decision for the request 'admission' process. The allowable responses, i.e. delivery options, communication parameters, service access parameters, funding levels and so on, depend on the organization's preferences.

The holistic approach interprets all the evidence, both business and risk. This is crucial for deciding whether to apply tolerance rather than restriction. For example, if a bona fide user may become 'rogue' and start exploiting enterprise resources, requesting re-authentication will not help, but a gentle nudge of capping data may suffice. On the other hand, if there are locations discrepancies, the device may be used illegally, so tougher authentication is appropriate.

B. Vulnerable Assets

The model accuracy hinges on definitive and discoverable linkage between risks, assets, and actions. The enterprise decides which risks need monitoring according to their perception of their most threatened and most valued assets. The impact of the risks is assessed according to a number of criteria: the potential damage to assets (lost confidential data, downtime of critical systems, poisoned data); the impact (lost reputation, lost competitive edges); vulnerability (susceptibility to unauthorized access, level of confidentiality); and consequential damage (work disruption, loss of business). A comprehensive list of risks and related vulnerable assets is available from ISMS (information security management system) guidelines, including ISO/IEC 27001.

The assets are represented by the 'mitigating actions', which are associated with different risk profiles. These mitigating actions reflect the assets vulnerability via a severity level. The higher the risk score, the more severe is the chosen action. The quantification of severity varies from one organization to another, according to their type of business, the nature of the workforce and the style of management. For example, some organizations put greater emphasis on data confidentiality, and others on optimizing network usage. Hence, the prioritization of risks and potential actions must be governed by customizable variables.

C. Profiling Behavior

In order to manage the many-to-many model (risks and actions), patterns of behavior are profiled for both business and risk. Risk profiles are tightly linked to assets that need protecting, while business profiles are related to resources (also 'assets') that need to be optimized. The process requires determining asserted risks first, then prioritizing them for each pre-defined profile. The prevailing profile is that which attains the highest score. The profile points to specific vulnerable assets, with their associated mitigating actions. For example, user's credentials asset is threatened by risk of stolen identity, for which a two-step verification action can be assigned. This mitigating action is triggered by conflicting geo-locations that are asserted as a risk under the 'Intrusive' profile. The many-to-many correlation is therefore performed in steps: assets define risks; risks are characterized by profiles; profiles link to actions, and actions protect assets. Figure 1 shows the matching of observed risks on one side with the potential actions, on the other.

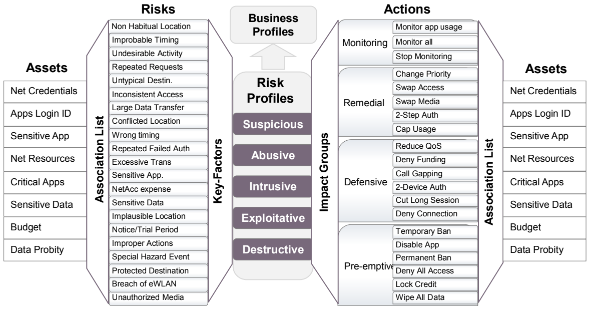


Fig. 1. Vulnerable Assets and Mitigating Actions

Where several risks are manifested, the profile scoring identifies the ‘prime’ risk, with the most suitable action, which relates to the most affected asset.

D. Mitigating Actions

To protect vulnerable assets, suitable mitigating actions are defined, ranging from denying service when a serious attack is perpetrated, to enhancing quality of service for essential business. Actions have strong association with vulnerable assets, but this relationship is not unique, i.e. there may be more actions for one asset or vice versa. Therefore, mitigating actions are classified by type: *Monitoring* (stop/start); *Remedial* (alternatives, limiting potential damage); *Defensive* (stricter security measures, curbing excessive /damaging activities); and *Pre-emptive* (preventing damage by temporary banning and time-gapping). These types of actions are *commensurate* with the type of risk and its severity.

Mitigating actions can start with wait-and-see (Monitoring) but they escalate up to complete takeover of devices remotely, wiping out enterprise credentials and banning access to enterprise applications (Pre-emptive). Re-authentication is a defensive action, but for higher risk, a pre-emptive access ban can be imposed. Mitigating actions can also be used obliquely, as alternative options of service delivery, i.e. remedial rather than defensive. For example, abusive behavior can be met with reducing session priority or QoS, instead of denying access altogether, and expensive media choice, such as roaming interactive video, can be downgraded to text messaging. A bolder remedial action for more severe threat is deferring a non-business exploitative request to the personal MNO, so that the user, not the enterprise, incurs the cost. Remedial actions foster more responsible behavior by way of a gentle ‘nudge’, which may be more effective.

IV. Structuring The Risk Model

A. Business Context and Risk Context Profiles

To assess risks for each service request, situational aspects (activity, urgency, integrity) need to be observed, as well as the usual environmental (space and time) and digital aspects (types of network, media and destination) that are obtained from the request details. These are business status attributes that are used to capture Business Context Profiles (*BCP*). To establish Risk Context Profiles (*RCP*), separate risk assertions are evaluated, under the same key factors. They may analyze the same information with different filtering and logic, but could have additional observations, e.g. from historical databases.

The *Sources* of observations that are used to detect threats are linked to the assets that are threatened, e.g. confidential data risks involve sources that detect accessing this data. The sources of business attributes as well as risks have varying degrees of trustiness that constitute their ‘inherent’ ratings, as in [16]. When observations are made, the severity of the risk is assessed, via filtering tables and pre-defined fuzzy indices that convert subjective estimates to normalized numeric scales. Hence risks and business attributes are evaluated by static sources’ *Credibility* and dynamically observed *Intensity*. Risk Context Profiles (RCPs), as in Table IIa, describe behavior patterns with associated actions. Business Context Profiles (BCPs) as in Table IIb, capture business status, with associated policies, using the same techniques.

Table IIa: Risk Context Profiles and Actions

No.	***Risk Context***	***Risk Profile Description***	***Actions***
RCP1	**Suspicious** Rogue user	Spatial-temporal discrepancies, Inconsistent access, erratic behavior	Monitor
RCP2	**Abusive** Excessive	Untrusted non-business destinations Long duration, large data	Pause, Cap
RCP3	**Intrusive** Invasive	Repeated logins, repeated failures, Exceeding authority,	Re-Auth. Two-step Auth
RCP4	**Exploitative** Unauthorized	Corp. apps heavy usage Exploiting network facilities	Gap, cap Temporary ban
RCP5	**Destructive** Damaging	Extreme acts, Improper usage, Sensitive data and apps	Bar access/apps Wipe-data

Table IIb: Business Context Profiles and Policies

No.	***Business***	***Business Profile Descriptions***	***Policies***
BCP1	**Routine** On-site	Everyday tasks, normal work, training, unassigned time	Swap Access, Standard QoS
BCP2	**Home Working**	Regular or casual home working, part time or overtime	Swap Media, Change Access
BCP3	**Travelling** Locally	Not in the office, partners’ sites or other branches	Swap Media, Swap Access
BCP4	**Essential Job** Critical	Mission-critical, urgent activity or chargeable time	High Priority QoS
BCP5	**Abroad-on-Business**	On business, roaming or hotspots, long-distance media	Swap Media, Swap Access

The *Destructive* behavior may damage the assets if service request is granted, e.g. poisoning database, or overloading a server. *Suspicious* behavior requires that further requests are monitored. The *Intrusive* profile indicates that an outsider is gaining access to internal systems. The *Abusive* profile denotes unwarranted heavy resource usage, especially of non-corporate applications, but no lasting damage, while the *Exploitative* profile is demonstrated by excessive usage of corporate resources that impacts on their performance. These behavior patterns also imply certain *consequential gravity* level, e.g. ‘Suspicious’ profile denotes lower potential impact than the ‘Destructive’ profile. This translates to varying degrees of mitigating actions, i.e. remedial, defensive, or pre-emptive. Business profiling is described in [26].

These profiles are, therefore, key to linking behavior and vulnerable connectivity assets. Combining risk and business profiles enables risk mitigation to account for business policies as well as risks. Although these profiles could be merged at the attribute/risk level, the choices are more clearly laid out when separate profiles are computed, and their results are fused only at the final stage. This delivers two separate scored patterns of key-factors, which retain as much knowledge as possible, while keeping profiles lighter and simpler.

B. Risk and Business Attributes Classification

Both RCPs and BCPs contain *Risks/ Attributes* that are associated with *Key-Factors*, i.e. they are classified in the same way. This is logical since the key-factors describe the input data, the hints, the evidence and the causal facts. They describe where (Spatial), when (Temporal), why (Activity), how (Integrity of data), during (Urgency), what (Destination), with (Network), and which way (Media). Risks are built from observations relating to current service requests, which are filtered to reveal situations and anomalies. In Table III, example of risks and business attributes per factor are shown.

Table IIIa: Risk Context Profile Key Factor Classification

Factor	*S*	*T*	*A*	*I*	*U*	*D*	*N*	*M*
Group	*Spatial*	*Temporal*	*Activity*	*Integrity*	*Urgency*	*Destined*	*Network*	*Media*
Disturbing **Remedial**	Non-Habitual	mprobable Timing	Un-desirable Activity	Unauth. data change	Repeated Requests	Un-typical Destin.	Inconsist. Access	Large Data Transfer
Disruptive **Defensive**	Location Conflict	mplausible Timing	Repeated ailed Auth	Repeated DB hits	Excessive Trans.	Sensitive App.	Network expense	Sensitive Data
Damaging **Pre-emptive**	Im-plausible Location	Notice Period	Im-proper Actions	Conflict change	Special Event	Sensitive Destin.	Breach of eWLAN	Unauth Stream

Table IIIb: Business Context Profile Key Factor Classification

Priority Business **Raise QoS**	Work Place	Any Time	On-Duty Shift	Unhabitual Spat-Temp	On-duty role	Corp. Apps	LAN, WLAN	Special Needs
	Home	Normal hours	Corp. Apps	WLAN/3G	Emergency event	Internal P2P	Mobile 3G/4G	Email/FT
Business as-usual **Lower QoS**	Regular Visit	After Hours	Emailing	Roster	Emergency	Special (Cloud)	Mobile Roaming	Browse Internet
	Branch	Lunch break	White List (WL)	Voice Destin	To Priority	Approved WL	Home BB	Chat Text
	Abroad	Booked time	Browsing (Not BL)	Apps Media	To-duty-officer	External P2P	Hotspots	Stream Video
Not Business **Deny/defer**	Roaming	Public Holidays	Social Media	Hotspot Location	To critical System	Not Banned	Partner	Voice
	Out	Not Absent	Not Business	Un-approved	Alarms	Home	Other	Live Video

To select which profile best describes the context, a selection procedure of '*If-the-shoe-fits*' is applied: Observed features are prioritized by elemental weighting rate and their key-factors. Scores are aggregated for each profile type, according to their prioritization templates, as in [20], and the maximum score indicates which one is the prevailing profile. Only a handful of profile types can be accommodated, in order to keep them well differentiated. Increasing the number of profiles may unduly blur their characteristics, and produce inconclusive results.

V. IDENTIFYING RISKS AND MATCHING ACTIONS

A. *Anomalies and Inconsistencies*

Inconsistencies and anomalies are revealed when concurrent activities have conflicting status, e.g. consecutive service requests are implausible if they are positioned at two distant geo-locations. Anomalies are also discovered though relative analysis (as in [27]), where certain features cannot occur concurrently, e.g. network attribute 'home broadband' is incompatible with spatial attribute 'abroad', thus indicating intrusion or fraud. Discrepancies must also be considered in the light of users' status, e.g. 'on-duty' users or emergency officers merit some leeway for extreme behavior, e.g. excessive logins. By contrast, employees on notice period may hold a grudge, so their behavior is considered more suspicious. Hence, risks are found by contradictory *observations*, implausible *timeline*, incompatible *features*, and conflicts with *users' status*.

B. *Timeline Analysis of Requesting Patterns*

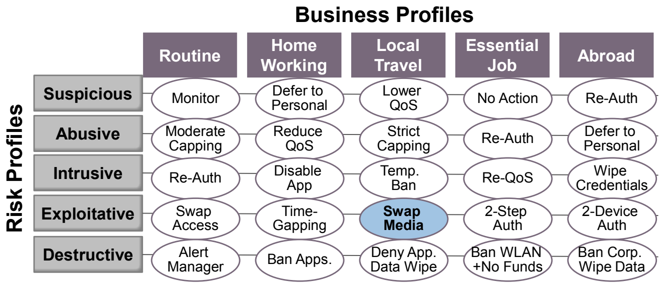
The manners in which streams of requests arrive provide further insight to the user's frame of mind. This requests' timeline analysis of recent requests can assist in action selection, e.g. call-gapping of future granted requests. Gaps that are progressively shortened show some urgency or intent to intensify the attack. When intruders invade corporate systems, they are likely to fire up numerous service requests, which individually may appear normal, but together reveal a threatening pattern. Such a pattern can be *erratic* (unexplained) or *excessive* (over the 'norm' that was recently exhibited). It may be *Aggressive* (an intensifying trend) or *Overactive* (overlapping), which indicates hacking.

Such timeline analysis requires definitions of 'time-slicing' that determines what is 'quick succession' or 'overlapping', as noted in [27]. These timeline patterns indicate the mitigation nature: '*erratic*' leads to *monitoring* actions, '*excessive*' indicates *remedial* actions, '*aggressive*' points to *defensive* actions and '*overactive*' needs *pre-emptive* actions.

C. *Course of Action*

As described so far, profiles provide a package of mitigating actions, and the precise selection is defined by the score level and optionally, by timeline behavior patterns, as above. Equally important is to avoid actions that are not necessary, or are disproportionate to the risk level. Actions provide effective defense only when they address the precise threat within the business context. For example, business profile for Essential-job implies that the user is engaged in critical business matters, which may involve long duration session and costly usage of media, so actions such as disconnecting or barring access should be avoided.

Business profiles determine policy for the service delivery in a similar process. The next step is to moderate the selected risk mitigation action by the level of assessed business priority. If the risk profile type is '*Abusive*', defensive actions focus on capping traffic volumes and durations on the non-corporate resources, e.g. internet access. If the profile type is '*Destructive*', the actions protect vulnerable internal databases from deliberate damage, by banning or delaying access to them. The business profile adjusts the action selection according to business priority and status, so that '*Exploitative*' actions are moderated for 'Local Travel' to become 'Swap Media', and not 'Swap Access', for example, as in Figure 2.



Business Profiles / Risk Profiles	Routine	Home Working	Local Travel	Essential Job	Abroad
Suspicious	Monitor	Defer to Personal	Lower QoS	No Action	Re-Auth
Abusive	Moderate Capping	Reduce QoS	Strict Capping	Re-Auth	Defer to Personal
Intrusive	Re-Auth	Disable App	Temp. Ban	Re-QoS	Wipe Credentials
Exploitative	Swap Access	Time-Gapping	**Swap Media**	2-Step Auth	2-Device Auth
Destructive	Alert Manager	Ban Apps.	Deny App. Data Wipe	Ban WLAN +No Funds	Ban Corp. Wipe Data

Fig. 2. Matching Actions with Business-Risk Profiles

VI. THE COMPUTATION METHODS

A. *Hierarchical and Multi-Dimensional Prioritization*

Profiles are differentiated by their customizable weights that characterize each profile type. For example, the *Network* key-factor has high priority weighting in the *Intrusive* profile, as does the *Large-Data* risk in the *Exploitative* profile. The classification hierarchy allows different prioritization weights to be applied in each layer, so the classification granularity ([26]) has great influence on the scores. Weights are assigned by *relative* significance within each class, where the sum of the weights equals 1. An atomic element is ultimately affected by the weighting of its sub-class and key-factor, as in Figure 3. While the normal prioritization associates risks to behavior patterns, there is also a requirement to associate risks with actions. This is achieved by novel *multi-dimensional* classification that allows introducing '*impact groups*' as an independent 'virtual' layer of relationships across the whole set, as shown in Group 1 and Group 2. The relative significance ratings encompass all atomic elements across the model, regardless of their hierarchical position, but they relate to the level of action for the risk.

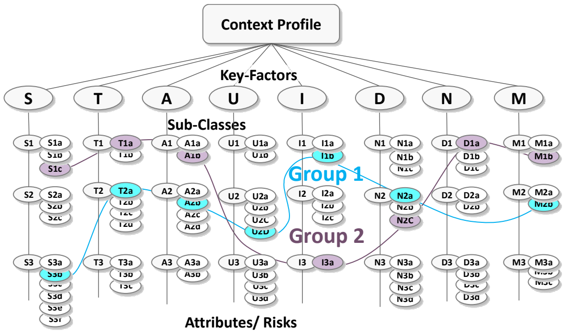


Fig. 3. Three-dimensional weighting model

The 3rd dimension groups provide a different approach to allocating relative weights. While risk weighting by key-factors are *causal* (Incompatible location /unauthorized data change), the impact groups are *consequential* (Unsettling/ Disturbing/ Disrupting/ Damaging) which are equated with action types (Monitoring/ Remedial/ Defensive/ Pre-emptive). This mechanism can also apply to the Business Model, with impact groups (Priority-Business/ Business-as-Usual /Not-Business) that equate to service delivery options (Raise Priority/ Lower Priority/ Deny-Defer). By conveying entirely different viewpoints, the prioritization of atomic members is enriched, and the profile scores become more distinctive.

B. Aggregation of Impact Groups

Weights for impact groups populate the third-dimension in the weighting matrix. This matrix has a non-linear effect on the aggregated values, so it resists result manipulation. To compute, each atomic (a_{ak}) element (either attribute or risk) is multiplied by its own weight, as well as its factor and group, as in (2). The assigned weights for Key-Factor *KF* are in *WKF* with scalar members as wkf_{k},. Weights for Group *G* are in vector *WG* with wg_g members. Atomics weights wa_a *are in vec*tor *WA*. The *xth* Context Profile (CP_x) with *k'* factors, *g'* Groups and *a'* atomic members, is then computed using SAW (Simple Additive Weighting), to select the highest scoring profile. When the prevailing context profile is established, the relevant group of actions is selected. However, the precise action still needs to be ascertained. This can be achieved by the corresponding score band, which points to a specific action. Impact group weighting can provide more precise result, if instead of applying a single group rate to all the members of the impact group in the 3rd dimension, the members are ranked within each impact group and weighted individually. This allows for actions to be relatively weighted within the impact group, thus differentiating actions more accurately.

$$Profiles\ 1 \le x \le x',\ Attributes\ 1 \le a \le a', \qquad (2)$$
$$Factors\ 1 \le k \le k',\ Groupsings\ 1 \le g \le g'$$
$$Attribute\ Vector:\quad A = \{a_1, \dots a_{a=a'}\}$$
$$WA_x = \begin{bmatrix} wa_{11} \dots & wa_{1x'} \\ \vdots \ \ddots & \vdots \\ wa_{a'1} \dots & WA_{a'x'} \end{bmatrix},\ \textstyle\sum_{a=1}^{a'}(wa_a) = 1$$
$$WKF_x = \begin{bmatrix} wkf_{11} \ \dots & wkf_{1x'} \\ \vdots \qquad \ddots & \vdots \\ wkf_{k1} \ \dots & wkf_{k'x'} \end{bmatrix},\ \textstyle\sum_{k=1}^{k'}(wkf_k) = 1$$
$$WG_x = \begin{bmatrix} wg_{11} \dots & wg_{1x'} \\ \vdots \ \ddots & \vdots \\ wg_{g'1} \dots & wg_{g'x'} \end{bmatrix},\ \textstyle\sum_{g=1}^{\hat{g}}(wg_g) = 1$$
$$CP_x = \textstyle\sum_{111}^{a'k'g'} a_{akx} wa_{akx} wkf_{akx} wg_{gx}$$

To distinguish the score further and increase the confidence in the decision, a proportional corroborative aggregation of scores within the impact groups is performed. The eBCR uses the author's new Cedar (Corroborative Evidential Diminishing Aggregation Rate) method for this purpose [16]. Cedar augments the 'prime' risk score, which has the highest score value within the group, by the proportional values of other supportive risks, in the order of rank. The impact of lesser risks is gradually diminished, due to a recursive coefficient (the residual after subtracting all previous contributions). As shown in (3), risks (R_r) are sorted in descending order, so that R_1 is the prime. They are weighted by individual group rate (wg_{rga}) as well as atomic, sub-class and factor weights. The augmented groups (GR_{gx}) are compared to establish the prevailing group of actions for the request.

$$1 \le g \le g'\ group,\quad R_{r-1} > R_r\ risk \qquad \textit{Cedar Aggregation}\ (3)$$
$$1 \le r \le r' \qquad \textit{Number of risks in each dimensional group}$$
$$\left(1 - |R_{rg-1}|\right) \qquad \textit{Recursive residual coefficient}$$
$$R_{rg} = a_{akx} wa_{akx} wkf_{akx} wg_{arg}$$
$$f(R_{rg}) = R_{rg-1} + R_{rg}\left(1 - |R_{rg-1}|\right)$$
$$GR_{gx} = \begin{cases} R_0 = 0 & r = 0 \\ (f(\,R_{rg-1}) + R_{rg}(1 - f(R_{rg-1})) & r > 1 \end{cases}$$
$$selected\ GR_{gx} = \max\,(GR_1 \dots GR_{g'})$$

C. Thresholds and Tolerance Bands

To distinguish between actions, scores are segmented into bands of *tolerance*. The number of bands is designed to fit the classification of actions: no-action, monitoring, remedial, defensive and pre-emptive categories, as in Figure 4.

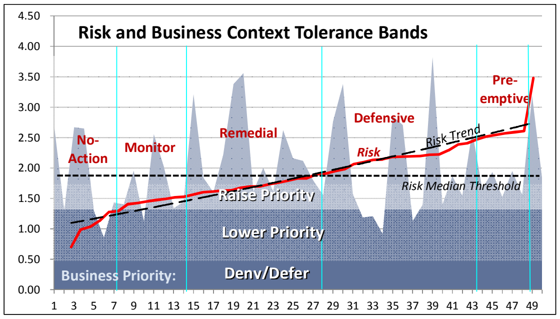


Fig. 4. Tolerance Risk Bands and Business Priorities

The initial equal tolerance bands are set up by finding the median, in order to correlate scores to a numbers of affected requests, as in (4a). Further refinement is produced by a process that adjusts the bands according to the required security levels and the number of affected requests. When a threshold is changed from point A(q1, p1) to point B(q2, p2), the number of affected requests is the delta q1 to q2. Applying OLS (Ordinary Least Squares), the regressor (q) is fixed (i.e. the request sequence numbers), and is only dependent on the score values (p). The delta of requests is computed in (4b).

$$(y, x) \in \mathbb{Z},\ Requests\ y > 1,\quad profile\ types\ 0 < x < x' \quad (4a)$$

$$\left\{CP_{x1}, \dots CP_{xy}\right\} :\rightarrow\ CP_{xy} <\ CP_{xy+1}$$

$$p = a + \beta q,\ \ p = \frac{1}{\beta}(p - a),\ \ 0 < i \leq n\ \ \textit{Adjust Threshold} \quad (4b)$$

$$\beta = \frac{Cov(q,p)}{Var(q)} = \frac{\sum q_i p_i - \frac{1}{n}\sum q_i \sum p_i}{\sum q^2 - \frac{1}{n}(\sum q_i)^2}$$

$$\Delta q = \frac{1}{\beta}(p2 - a) - \frac{1}{\beta}(p1 - a) = \frac{1}{\beta}(p2 - p1) \qquad \textit{Coefficient } \beta$$

$$\Delta q = \frac{1}{\frac{\sum q_i p_i - \frac{1}{n}\sum q_i \sum p_i}{\sum q^2 - \frac{1}{n}(\sum q_i)^2}}(p2 - p1) \qquad \textit{Delta of affected requests}$$

VII. Conclusions

Users expect BYOD terminals to be available for personal services, unencumbered by corporate rules and restrictions, but enterprises still have to defend their assets. Hence, mitigating responses should be triggered in proportion to both risk and business status. This is achieved by the proposed enterprise Business Context and Risk (eBCR) model, which profiles behavior and selects the appropriate course of action.

The risk model applies multi-dimensional as well as hierarchical prioritization, to provide fine tuning of decisions. Profiles are associated with appropriate mitigating actions, and the precise action is determined by adjustable 'tolerance' bands. For more accurate scoring, the Cedar algorithm is used for aggregation of corroborative data.

The model can manage a wide range of threat types that are prevalent in the corporate environment. It also deals with uncertainty via assigning inherent values to risk/attributes that is generated from the estimated credibility of the digital sources. It can manage conflicting evidence of risk when using the Cedar aggregator. It is based on fresh observations per connectivity request, thus allowing for unpredictable behavior to be detected.

Risk profiling has further use in many applications, especially those with digital sources of variable quality. Future research could examine the impact of mitigating actions on the connecting parties, who remain unaware of the business and risk policies of each other.

References

[1] V Jakkula, D Coo "Temporal Pattern Discovery for Anomaly Detection in a Smart Home" 2007 Washington State University

[2] P Leskinen, J Kangas "Rank reversals in multi-criteria decision analysis with statistical modeling of ratio-scale pairwise comparisons" 2005 Journal of the Operational Research Society

[3] J Dyer, P Fishburn, R Steuer, J Wallenius, S Zionts "Multiple Criteria Decision Making, Multi-attribute Utility Theory: The Next Ten Years" Management Science Vol. 38 No. 5 1992

[4] M De Choudhury H Sundaram A John Dorée D Seligmann "Context aware routing of enterprise user communications" IEEE 2007

[5] Yi Deng, J Wang, J Tsai, K Beznosov "An Approach for Modeling and Analysis of Security System Architectures" IEEE 2003

[6] Gartner "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes" http://www.gartner.com/newsroom/id/2466615 2013

[7] Y Zhang, F Li "A Model of Context Awareness Agent System based on Dynamic Fuzzy Logic" IEEE 2007

[8] M Huebscher, J McCann, N Dulay "Fusing multiple sources of context data of the same context type" Xplore 2006

[9] S Ahmad, R Ahmad "Design of Algorithm for Environment based Dynamic Access Control Model for Database Systems" International Journal of Computer Applications May 2011

[10] R Bhatti, E Bertino, A Ghafoor "A Trust-Based Context-Aware Access Control Model for Web-Services" Springer 2005

[11] A Dersingh, R Liscano, A Jost "Context-aware access control using semantic policies" Ubiquitous Computing and Communication Journal , UBICC 2008

[12] A Scarfò "New security perspectives around BYOD" IEEE 2012

[13] M Kajko-Mattsson "Risk Profiles" IEEE 2009

[14] S Woo, J On, M Lee "Behavior Ontology: A Framework to Detect Attack Patterns for Security" IEEE ICAINA Workshop 2013

[15] S Güven, C Barbu "A Real-time Risk Assessment and Mitigation Engine based on Dynamic Context " IEEE 2011

[16] R Copeland, N Crespi "Rating Credibility of Sources for Profiling Risk and Business Context of Service Requests" SCC, IEEE 2014

[17] J Nurse, J Sinclair "Towards A Model to Support the Reconciliation of Security Actions across Enterprises" 2012

[18] G. Jiang, G. Cybenko, "Temporal and Spatial Distributed Event Correlation for Network Security," IEEE 2004

[19] A Ferrara, P Madhusudan, G Parlato "Security analysis of role-based access control through program verification" IEEE 2012

[20] R Copeland, N Crespi "Implementing an enterprise Business Context model for defining Mobile Broadband Policy" IEEE CSNM 2012

[21] L Hajjem, S Benabdallah,F Abdelaziz "A dynamic resource allocation decision model for IT security" IEEE 2012

[22] J Onroy,J Becerra,F Bellas, R.Duro, F López-Peña "Automatic Profiling and Behavior Prediction of Computer System Users" 2006 IEEE

[23] D Zhao, J Wang, J Ma "Fuzzy Risk Assessment of the Network Security" IEEE 2006

[24] J Strassner, S Meer, D O'Sullivan, S Dobson "The Use of Context-Aware Policies and Ontologies to Facilitate Business-Aware Network Management" Springer Journals 2009

[25] J Leite "Analysis of Log Files as a Security Aid" 2011 Porto University

[26] R Copeland, N Crespi "Classifying and Aggregating Context Attributes for Business Service Requests -No One-Size-Fits-All" SSC IEEE 2014.