НАБЛЮДЕНИЯ ВЪРХУ СЪВРЕМЕННИ ИНТЕРФЕЙСИ ЧОВЕК-МАШИНА ПРИ СИСТЕМИТЕ ЗА КИБЕРСИГУРНОСТ

Симеон Ангелов Ангелов
Омнител ООД, бул. Цариградско шосе № 125, бл.2, ет 3, 1113, София,
моб. 088 850 1755, email: angelov&omnitel.bg

OBSERVATIONS ON CONTEMPORARY HUMAN-MACHINE INTERFACES IN CYBER SECURITY SYSTEMS

Simeon Angelov Angelov
Omnitel Ltd., 125, Tsarigradsko Shosse Blvd., Bl. 2, 3th Floor, 1113 Sofia,
Mobile: +35988 850 1755, Email: angelov&omnitel.bg

Резюме: Докладът е посветен на съществената роля на интерфейса човек-машина в съвременните системи за наблюдение и контрол. В частност се набляга на изключителното значение на този интерфейс при системите за киберсигурност. При тях често действията, предприемани от операторите, са вследствие на решения, които се взимат в реално време и са повлияни от качеството и коректното предоставяне на информация от интерфейса човек-машина. Като най-ефективен тип интерфейс е определен типът „Контролно табло". Разгледани са неговите характеристики и са посочени техните предимства при системите за киберсигурност. Очертани са и вероятните насоки на развитие на "контролните табла" като следствие от разширяващите се функции, които се поемат от системите за киберсигурност.

Ключови думи: интерфейс човек-машина, системи за наблюдение и контрол, системи за киберсигурност

Abstract: The report focuses on the essential role of human-machine interface in modern systems for monitoring and control. In particular, it emphasizes the crucial importance of this interface in cyber security systems. There, the actions taken by the operators often follow decisions made in real time which are influenced by the quality and the correctness of the information coming from the human-machine interface. The report defines "Dashboard" type of interface as the most effective one. It discusses the characteristics of this type and outlines their advantages in systems for cyber security. It outlines the likely directions of development of "Dashboard" as a consequence of the expanding functions of the cyber security systems.

Key words: human-machine interface, systems for monitoring and control, cyber security systems

Както интерфейсът човек-машина, така и киберсигурността са важни фактори в съвременния ИКТ свят. Днес те заемат съществено място, работейки съвместно.

Още преди време ролята на интерфейса човек-машина е оценена най-вече при управление на важни и критични процеси. Казвано е, че добрият интерфейс човек-машина е предпоставка за коректен анализ на ситуацията и последващо изпълнение на правилни решения и действия.

Недвусмислено е доказано, че недобрият интерфейс човек-машина е причина за лоши последствия и дори за трагични инциденти.

Повечето от вас си спомнят за следобеда на 23-и март 2005 г., когато рафинерията на Бритиш Петролеум в Тексас беше разтърсена от серия експлозии при препълване на дистилационната кула в участък за въглеводородна изомеризация. Тогава изригна гейзер от течността, който формира облак от лесно запалима пара. Впоследствие облакът се възпламени от наблизо спрял, но с работеш двигател, камион. Петнадесет работника бяха убити и сто и осемдесет ранени. прозорците на сградите в радиус от един километър и двеста метра бяха изпочупени. Съветът по химическа безопасност на Съединените американски щати разследва близо две години инцидента. Окончателният доклад посочваше различни причини, включително незадоволително обучение, неспазване на процедури за безопасност, неточни измервателни уреди, слаба поддръжка и ***„лошо проектирана компютърна система за контрол, която е възпрепятствала възможностите на операторите да установят, че кулата се препълва.”***

Компютърната система за контрол е индикирала на един екран колко течен рафинат се влива в кулата, докато същата система е индикирала на съвършено друг екран колко рафинат се е изливал вън от кулата. За да може да се проследява нивото на запълненост на кулата е било необходимо непрекъснато да се превключва от единия към другия екран, което не е било правено било поради недобра обученост на операторите или по-вероятно поради това, че последните са решили да „избегнат” това „неудобство”. Категорично е и заключението на Съветът по химическа безопасност на Съединените американски щати относно компютърната система, наблюдаваща и управляваща процесите в предприятието: „Представяйки двата потока на различни екрани се е намалила видимостта и е попречило да се установи очевидния дисбаланс между входа и изхода.”

Долната илюстрация 1 нагледно показва резултата от тази трагедия.

Илюстрация 1

Днес, когато кибер заплахите и кибер атаките са част от ежедневието ни, става задължително интерфейсът човек-машина на всяка система за кибер сигурност да ни предоставя най-добрите възможни начини да разберем и впоследствие да реагираме правилно на това, което се е случило, на това, което се случва и на това, което е възможно да се случи в бъдеще.

Какъв е добрият интерфейс човек-машина в една система за кибер сигурност?

Може би ще бъдете разочаровани, но аз не мога да отговоря дефинитивно на този въпрос днес.

От една страна динамичното развитие и постиженията на когнитивната наука оформят все по-нови и прецизни изисквания към функционалностите на компютърните интерфейси с човека. Опознаването на това как възприема човешкия мозък води след себе си до задания за създаване на иновативни методи на взаимодействие между човека и машината.

От друга страна ролята и обхвата на действие на системите за кибер сигурност се променя в посока на разширяване. Преди около десет години установяването на проникване в дадена компютърна мрежа бе основното, което извършваше една такава система. Днес използваме широкоспектърни, многофункционални, с големи възможности за анализ и предикция системи. Очертава се тенденция за въвеждане на атакуващи функции заедно с традиционните защитни задачи на системите за кибер сигурност.

Поради тези причини е трудно да се даде еднозначна дефиниция на един добър интерфейс човек-машина. Най-малкото тази дефиниция ще бъде валидна за кратък период от време.

Вместо да се заемам с тази непосилна за мен задача, аз ще се опитам да очертая някои от необходимите характеристики, които притежава съвременния и ефективен интерфейс човек-машина. В никой случай не претендирам обаче те да са достатъчни. Тези характеристики са изведени от реални системи за кибер сигурност на световни производители, с които Омнител си партнира.

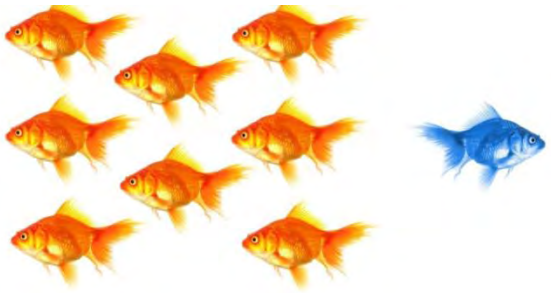
Едно от основните предизвикателства, които срещат операторите на центрове по кибер сигурност е необходимостта да се обработят огромни количества данни от многобройни потребители на кибер услуги. Казват, че една картина струва колкото хиляда думи. Долните две илюстрации № 2 и 3, отразяват едно и също събитие, заснети са от една и съща перспектива, но са с разлика от осем години във времето. Те показват недвусмислено според мен порядъка от данни и задачи, с които ще се срещне един център по кибер сигурност на телекомуникационен оператор.

Илюстрация 2

Илюстрация 3

За един компютър е само въпрос на процесорна мощност, обем памет, комуникационен капацитет, за да се справи с големите данни. За хората, които взимат решения и действат въз основа на тях, е невъзможно обаче в обозрим период от време да обработят „суровия“ материал, произвеждан от компютъра. Тук, на помощ идва интерфейсът човек-машина, който показва и „обрисува“ на операторите по един разбираем за тях начин кибер ситуацията по възможно най-простия начин.

Вероятно долното изображение на Фигура 1 ще е иделната продукция на една съвременна система за кибер сигурност.



Фигура 1

За съжаление обаче това все още не е възможно, тъй като реалните кибер ситуации са достатъчно сложни, така щото днешните компютри и тяхното програмно осигуряване не са в състояние да ги анализират и „осъзнаят” напълно. Хората са тези, които могат да начертаят дефинитивно тази фигура, но разбира това не би било възможно без безценната помощ на компютърните системи.

Друго основно предизивкателство, с което се сблъскват операторите е необходмостта да се изучават нови инструменти, всеки от които е с различни спецификации, правила на взаимодействие и функции. Операторите искат виждат различните аспекти на развиващата се ситуация като визуални карти на атаките, развитието им във времето, географска информация, компроментираните ИКТ средства и др. И за да станат нещата още по-сложни, често различни инструменти и то на различни екрани предоставят фрагменти от исканат информация. В такава среда не етрудно да се направи заключението, че операторите ще страдат от недостиг на капацитет и дори е възможно да изпаднат в невъзможност да анализират и взимат решения. Напълно вероятно е

да се провокира ситуацията в рафинерията на Британиш Петролеум в Тексас и то дори с още по-лоши последствия, тъй като ние говорим и за злонамерено поведение на кибер атакуващи хакери.

Какъв е съвременния подход, който позволява да се справим с тези предизвикателства?

Взаимствано от съвременните индустриални процес контрол системи и използвано не само там е „Контролното Табло” – фигура 2.

Фигура 2

Контролните табла предлагат уникално и мощно решение на много от проблемите, с които се сблъскват операторите. Те са от решаващо значение при развитието на интерфейса човек-машина в системите за кибер сигурност. Конкретно, ако операторите са претоварени с твърде много данни, контролните табла са един ефикасен инструмент, който увеличава разбирането и намалява когнитивното натоварване. Те позволяват на операторите да изпълнят своите цели, вписват се изцяло на един компютърен екран и са обозрими само с един поглед. Съвременните контролни табла са евристични, могат да бъдат адаптирани към желания процес за наблюдение, към изискванията на самия наблюдаващ, към типа дисплей, към наличните данни и към честотата на обновяване на данните.Тъй като контролните табла са адаптивни, те могат да бъдат настроени за стратегически цели, т.е. да са фокусирани върху общия изглед, който показва по-скоро дългосрочните трудности, отколкото непосредствените моментни проблеми. Също, те могат да се модифицират за аналитични нужди със специфични показатели, сравнения и оценители на ефективността. Разбира се, когато бъдат настроени за оперативни нужди, те ще показват моментната информация в реално време.

Естествено контролните табла имат силни комуникативни способности, които осигуряват съвместната работа на екипите по кибер сигурност.

И накрая, може би най-важната характеристика на контролните табла е възможността им да интегрират в себе си съществуващите инструменти, които вече са усъвършенствани от операторите, като по този начин се свежда до минимум когнитивно натоварване на персонала.

REFERENCES

[1] Radka Nacheva, "The significance of cognitive user profiles for improving usability of computer systems' interfaces", *International Conference "Human systems integration approach to cyber security",* Sofia, Bulgaria http://rnda.armf.bg/wp-content/uploads/000s/EN/Activities/Konference/index.php, Sep. 28-29, 2015

[2] S. Radeva, A. Bozhanova, D. Radev, D. Stankovski, "Human-computer interface for estimation of basic emotional states via recorded electrophysiological signals", *Proceedings* "*International Conference Automatics and Informatics'2015",* Sofia, Bulgaria, pp. 99-102, Oct. 4-7, 2015