

Sample Paper for Poster 2015 Conference for L^AT_EX

First Student AUTHOR¹, Second Student AUTHOR²

¹Dept. of Radioelectronics, Czech Technical University, Technická 2, 166 27 Praha, Czech Republic

²Dept. of Physics, Another University, Another Street 123, Another City, Another Country

First.author@fel.cvut.cz, secauthor@supermail.com

Abstract. *The abstract of the paper brings very brief information about the contents of the paper. The abstract should not be shorter than 80 words and should not exceed 200 words. For the text of the abstract use the environment abstract.*

For typing the paper in L^AT_EX use the documentclass poster15, the basic commands and environments are re-defined according to the specific conference format.

*For the title of the paper use the command \title{}. The name, the affiliation, and the e-mail address of the author(s) are of the styles author{}, \affiliation{} and \email{}. The affiliation is required being specified as shown in this example. All authors must have a student status! **Failure to comply with this rule may lead to rejection of the paper.***

Keywords

Paper formatting, Poster2015, electronic publishing, templates, styles.

1. Introduction

Currently there can be seen move toward context aware application. It is caused by emerge of the huge amount of the mobile technologies and users demand for personalized applications. Applications provide personalized context based on user's context or the application's context. That brings completely new experience for the applications operators as well as for users.

However securing the applications is done the old way. Mostly users got some roles in applications or permissions for resources and those security rules are independent on context. There is very few, if any, applications which has security based on context. We can expect that users and application owners would take advantage of application security based on context to provide specific security rules based on users context.

Applications using context aware security can be much less obtrusive for users. They can be asked for different authentication methods based on context, they can be authorized for same resource various ways depending on their context. They can even sometimes omit authentication because their context is trustworthy by itself (for example access from inner company network). Same as the users can profit from the context based authentication operators of the applications. They might define more strict security rules for suspicious users behavior (for example access to confidential resources in system from internet in night). Using context allows system administrators for more fine grained security rules which would be otherwise unsustainable for maintenance.

Application operators and software developers are good aware of the added value of context aware security. Even there are various proposals how to do context aware security none of them is widely used. Reason why they are not widely used can be that they are either too complicated or they are too innovative and it is hard to incorporate them into existing solutions.

In this paper I will present solution which extends standard security architecture with context aware elements. This extension is based on giving users security level based on their context. Resources would require user to posses that level in addition to his normal rights to be accessed. That way we can extend any existing security architecture with context aware elements.

2. Background

Large applications or information systems which has more then one user needs some form of authentication and authorization. Such systems are here for many decades and are almost as old as computers itself. Therefore for many decades there exist problem with security applications and it was solved various ways.

Two of the oldest principles for securing application resources is mandatory access control (MAC) and discretionary access control (DAC). Those two principles does not

define how the application security should be implemented, but rather define core principles in authorization. In MAC there is some authority which grants permissions to all resources. In DAC on the other side can grant permission everyone with sufficient permission for the resource.

However granting permissions to every user in system is unpractical for larger amount of users. Role based access control provides another level of abstraction. In that approach the permission is given to an abstract role and users are assigned roles. Typically there is in application many times less roles than permissions and the roles does not change significantly over time unlike users.

Nevertheless those authorization principles and method are very static. They does not reflect the changing state of the system and users. Once they are set they do not take in account any other factors and any fine tuning is if not impossible very difficult.

Context aware security can overcome those difficulties and provide even new experience for user and application operator. Context aware applications are much more personalized then the static ones and same comes for the security. Application can get a lot of information about user from context and therefore it does not annoy user with request for additional information. For example application knows his IP address and therefore does not need to re-verify him. The context is also valuable source of information for application owner. For example he might restrict some IP ranges, days of time, etc to access resources in application.

Also with the emerge of the context aware application there is naturally need of context aware security. ADD DATA ABOUT CONTEXT AWARE APPs ADD DATA ABOUT CONTEXT AWARE APPs ADD DATA ABOUT CONTEXT AWARE APPs ADD DATA ABOUT CONTEXT AWARE APPs ADD DATA ABOUT CONTEXT AWARE APPs ADD DATA ABOUT CONTEXT AWARE APPs ADD DATA ABOUT CONTEXT AWARE APPs

To illustrate how can context aware security improve applications consider following example. We have a information system in company. To make it more comfortable let users from inner company network access some noncritical resources. But if the user comes from internet or access some sensitive resources he needs to authenticate itself normal way. But not only users would benefit from it. Context aware security can determine suspicious users behavior. For example if users log in to system in short time frame from different parts of world it can rise flag and the incident can be investigated further. Or the company can set some access hours for various resources, to limit possibility of their abuse (for example limit access in non working hours).

3. Related Work

something

4. Osnova

1. Intro - co je security, proc je dulezity pro aplikace, proc je stavajici security spatna, jake ekonomicke nevyhody nese, jak husta je security co bere v potaz kontext, ze to ukazu na RBAC

2 - Background - vysvetleni kontextu, co je MAC/DAC, co je RBAC, detailnejs popsat jak kontextova security pomuze jak uzivatele, tak provozovatele systemu

3 - Related work - z diplomky mam 7 praci, najit dalsi?

4. Vlastni obsah - resit pomoci levelu - popsat svoje reseni (a na RACS nechat to, ze autentizacni metoda je cast kontextu?)

Koment od Tomase: 1 ma rici co je problem a co vlastne resis, i naznacit co prinese tve reseni 2. ano, ac mel by jsi stavet na tom ze exituje nejaka obtiz, a jak ji pomohou resit tyto typy zabezpeceni 3. ok 4. zde rici i jak to resi problem, jake to ma vyhody a naznacit i omezeni ci co to nedela 4. pokud lze neco oddelit a nechat to na RACS pak idealni. 5. shrnuti

5. Headline of a Section

The abstract of the paper is followed by the headline *Keywords*. Below the headline, three to six terms featuring the area of the technical or scientific orientation of the paper have to be given. Use the environment `keywords`

Headlines of sections should be typed using the command `\section{}`. Headlines of subsections are of the style `\subsection{}`. If those styles are used, numbering of headlines is performed automatically. Subsections of the third or even further levels are not recommended.

6. Headline of a Section

If the basic text is interrupted by an equation or by a figure, then the paragraph is not indented.

6.1. Headline of a Subsection

The header at the top of the page is of a special form for even pages and for odd ones. Therefore, the content of the header for the even pages consists of the abbreviated names of the authors and the paper title and is defined by the command `\headtitle{}`. The headers of the all pages are then generated automatically.

10	20	30
40	50	60

Tab. 1. Descriptions of figures and tables are of the same style.

Tables are centered in the text column. For the text in the table, we use the font command `\tablefont`. Use standard environments `table` and `tabular`, see the example above (Tab. 1). For the two-column table use the environment `table*`.

Figures are also centered in the text column. Use standard environment `figure`, see the example above. For the two-column figure use the environment `figure*`.

Descriptions of figures or tables are of the style `\caption{}`. Short captions, which take one line only, should be centered. For the two-column caption use the command `\captionwide{}`.

Equations in the paper should be typed using the common math environments (e.g. `\equation`). Equations are numbered automatically as shown in the following example:

$$\frac{2B \sin^2 + A \sin 2}{10g^2 \kappa T + A \cos^2 + B \sin} = 2\gamma\delta. \quad (1)$$

No comma should be put before an explanation of symbols in the equation, e. g.

$$\lambda_g = \frac{1}{\sqrt{1 - \left(\frac{\lambda}{\lambda_m}\right)^2}} \quad (2)$$

where λ_g is the wavelength... etc.

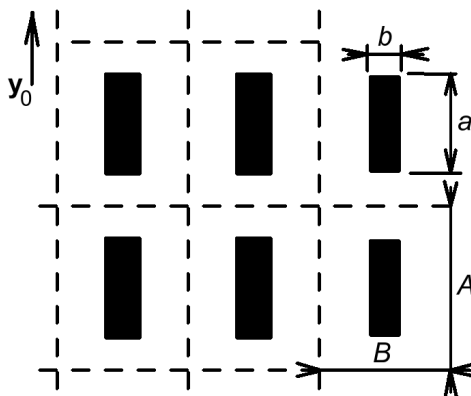


Fig. 1. The description of a figure is of the same style as the description of a table; the figure itself is of the environment `figure`.

7. Headline of a Section

Finally, we would like to ask authors for keeping the following rules:

- All authors must have a student status! The supervisor can be mentioned only in the *Acknowledgements* section. **Failure to comply with this rule may lead to rejection of the paper.**
- Authors are requested to submit their papers electronically to the conference web site, **which is the moment when you register for the conference**. Please, do NOT send the papers by e-mail.
- The file size in the pdf format (all fonts embedded) is limited to maximum 3.5 MB. Always use the up-to-date version. **Make sure that all fonts are embedded.**
- The length of the paper should depend on its contents (balance between the text and figures). The Program Committee will assess the completeness of the information presented. The text body of the paper itself might not exceed 5 pages.
- Authors are invited to include their short professional curriculum and an ID-sized photo at the end of their papers.

Acknowledgements

Research described in the paper was supervised by Prof. A. Supervisor, FEE CTU in Prague and supported by the Czech Grant Agency under grant No. 102/ 01/9999, by the Czech Ministry of Education under grant No. 9999/2002 and by the research program MSM 444222.

The headline *Acknowledgements* is of the style `\section*{}`.

The authors are asked to pay special attention to the form of references. The NAMES OF AUTHORS should be typed in capitals, the *Titles of Journals, Books or Proceedings* in italics with the first capital letter in all significant words. The titles of articles are typed similarly as the basic text without the first capital letter in all words. Use the standart environment `thebibliography`.

References

- [1] JAKUBOVÁ, I., RAIDA, Z. Exemplary Document for the paper in Radioengineering. *Radioengineering*, 2006, vol. 15, no. 1, p. 1 - 2.
- [2] AUTHOR, F., AUTHOR, S., AUTHOR, T. F. *The Book*. 2nd ed. Humpolec: Nupish&Publish, 1901.
- [3] HUSNÍK, L., LHOTSKÁ, L. About Poster 2005. In *Proceedings of the 9th International Student Conference on Electrical Engineering POSTER 2005*. Prague (Czech Republic), 2005, p. 1 - 2.

About Authors...

First AUTHOR was born in ... The biography is typed using the environment `authorcv{First AUTHOR}`.

For one author, one paragraph of the biography is devoted. The **Name** of the author is typed in `\textbf{ }`, the **SUR-NAME** is written in capitals. All authors must have a student status!