	of smell				
Robots	+/-	-	+++	+++	-
Humans	+	+	+	+	+

Table №1 Comparative table of feelings of the robot and the person

As you can see from table 1 the robots have advantages in some senses unlike us, thereby emphasizing their importance and our uselessness. We must immediately do something not to be ousted from our posts.

References:

1. 12 причин, почему машины всегда будут иметь преимущество перед нами (http://muz4in.net/news/12_prichin_pochemu_mashiny_vsegda_budut_imet_preimushhestvo_nad_nami/2014-12-29-37508)
2. Создан робот-клон датского профессора (http://www.vesti.ru/videos/show/vid/323785/#)
3. СТРАШНЫЕ ДОСТИЖЕНИЯ РОБОТОТЕХНИКИ (https://youtu.be/mDz31BndB4w)
4. Первый клон человека (http://www.1tv.ru/news/2004-02-12/246966-pervyy_klon_cheloveka)

CROSS-APPLICATION AUTHENTICATION

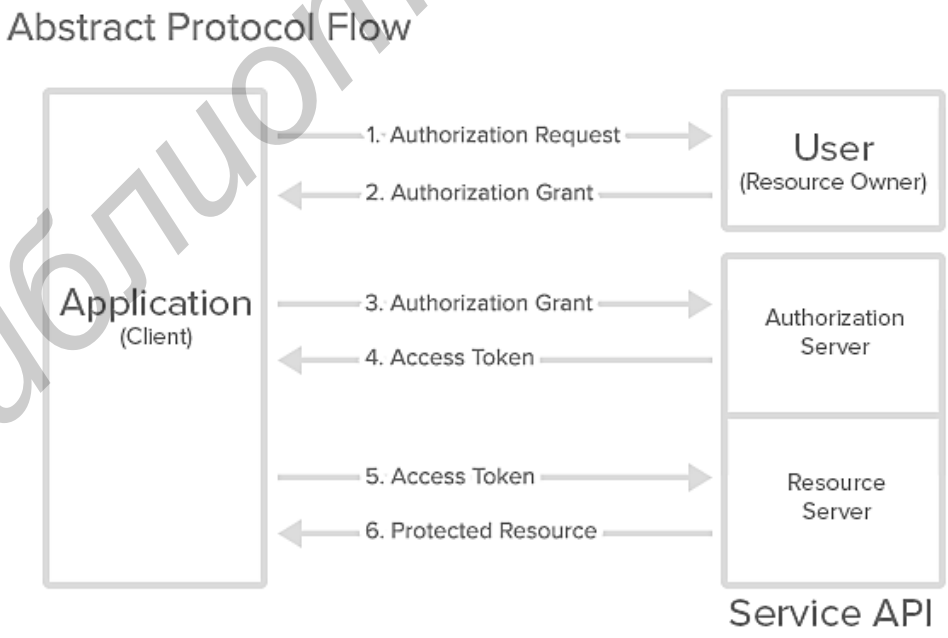
Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Isakov N.V.

Lazarenko A.M. - Senior Lecturer

The purpose of this paper is to provide you with the most important information about cross-application requests protocol based on authentication framework “oAuth 2.0”.

Nowadays we use more and more different web-resources that save our data. Sometimes we have the necessity to get the data from one application and transfer it to another one. But how can we make it work? It should be easier to use this protocol without giving an identifier and a password to the third person. For a developer it should be a protected, low loaded and easy to set up tool. The answer to all these questions is “oAuth 2.0”. This framework is very powerful and documented as RFC 6749.



1.2. Getting authorization grant (or just redirecting to resource server if it has api for it).
3.4. Swapping grant for token.
5.6. Getting necessary data from resource server.

As we can see this is a simple and secured protocol, where application gets a token that gives access to the user‘s data from the resource server. Another advantage is that a token gives access only to a part of the data that a user allows to provide for application. A user can always withdraw a token on the authorization server.

The main disadvantage of this protocol is: danger of xss-attacks (this is a secured and powerful tool for specialists, and it can make a lot of problems for young developers). Therefore we need to make a few requests with redirecting.

References:

1. https://tools.ietf.org/html/rfc6749
2. https://tools.ietf.org/html/rfc6750
3. https://habrahabr.ru/company/dataart/blog/262817/
4. https://ru.wikipedia.org/wiki/OAuth
5. https://oauth.net/2/