ЛАБОРАТОРИЯ № 80
«КИБЕРФИЗИЧЕСКИХ СИСТЕМ»

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ПРОБЛЕМ УПРАВЛЕНИЯ
ИМ. В.А. ТРАПЕЗНИКОВА
РОССИЙСКОЙ АКАДЕМИИ НАУК

МЕТОДЫ УСИЛЕННОЙ АУТЕНТИФИКАЦИИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Мещеряков Роман

д.т.н., профессор, г.н.с. ИПУ РАН

mrv@ieee.org

ipu.ru

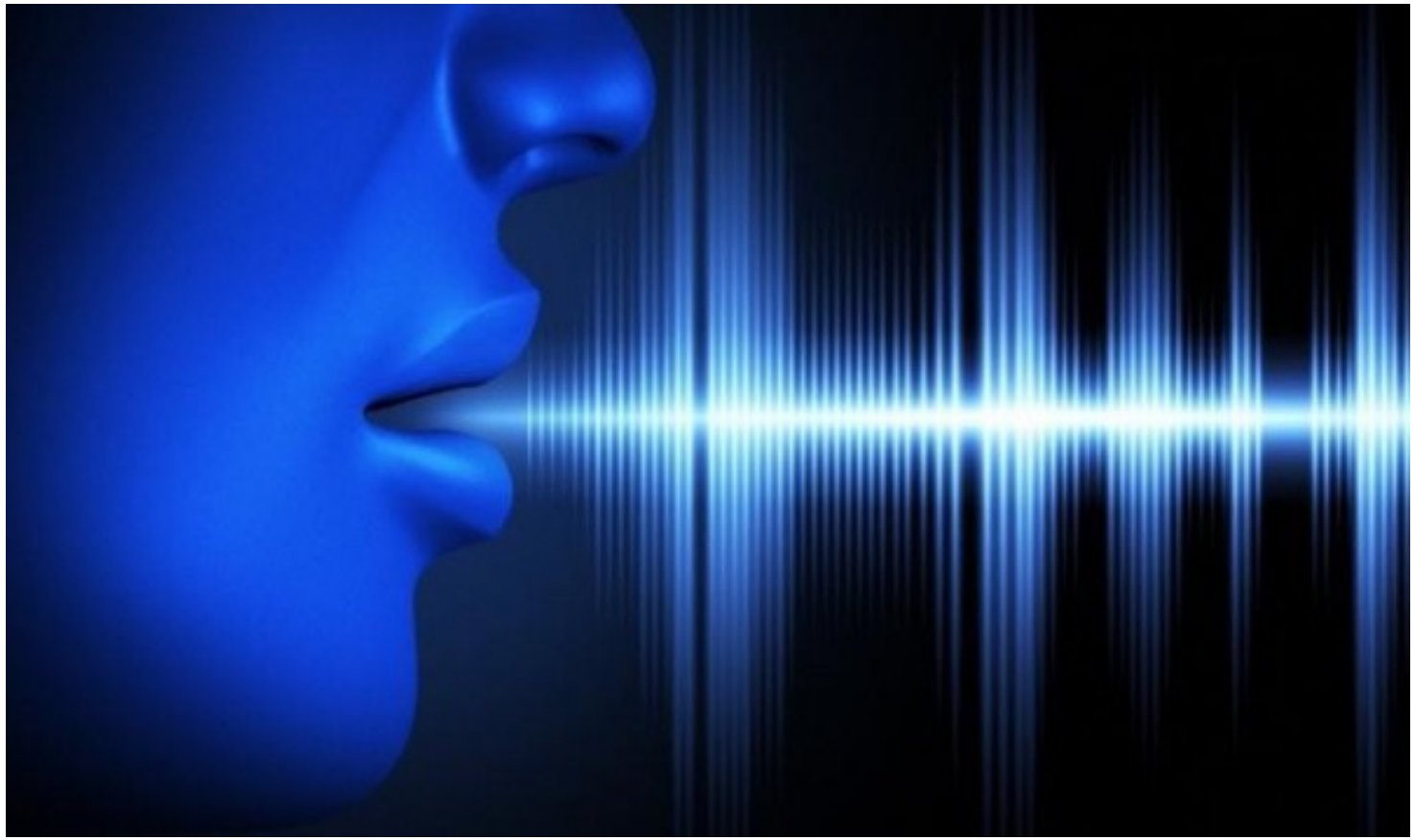
Современные вызовы

By adopting this approach for B2B and B2C operations alike, organizations can:

- **Enhance the user experience:** By making logins more seamless and eliminating the need for users to remember their passwords. This could even drive improved sales if fewer shopping carts are abandoned due to login issues.
- **Improve security:** If there are no passwords to steal, organizations can remove a key vector for compromise. It's claimed that passwords were to blame for 84% of breaches last year. At least, you'll be making the bad guys work a lot harder to get what they want. And credential stuffing attacks, currently attempted in their billions each year, would become a thing of the past.
- **Reduce costs and reputational harm:** By minimizing the opportunities for financially damaging ransomware and data breaches. It will also reduce the IT admin costs associated with password resets and incident investigation. One report claims this could cost as much as £150 ($200) per password reset and 30,000 hours in lost productivity per year. That's not to mention the extra time freed-up for IT teams to spend on higher value tasks.

Современные вызовы

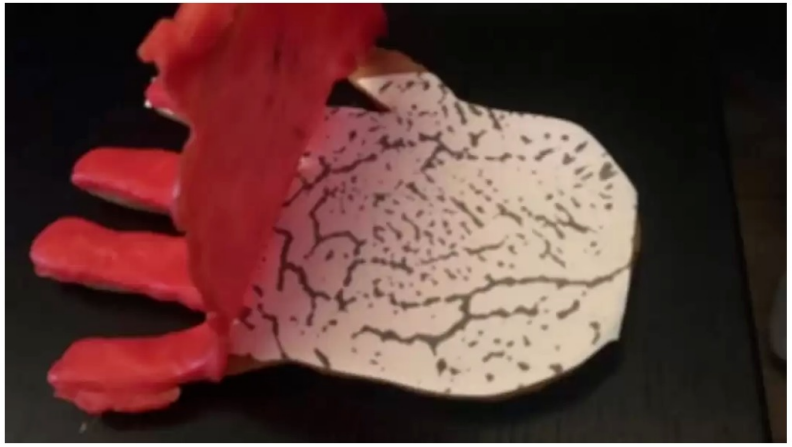
1. Дипфейк-голос



Подробнее: https://www.securitylab.ru/news/525649.php

Современные вызовы

2. Муляжи



Подробнее: https://events.ccc.de/congress/2018/wiki/index.php/Main_Page
https://eadaily.com/ru/news/2020/09/14/svetodiody-kepka-i-ochki-kak-obmanut-sistemy-raspoznavaniya-lic

Современные вызовы

3. COVID

Подробнее: https://securityrussia.com/blog/raspoznavanie-v-maske.html

Современные вызовы

4. 2FA – не панацея

Home > Techniques > Enterprise > Use Alternate Authentication Material > Web Session Cookie

Use Alternate Authentication Material: Web Session Cookie

Other sub-techniques of Use Alternate Authentication Material (4)

Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.[1]

Authentication cookies are commonly used in web applications, including cloud-based services, after a user has authenticated to the service so credentials are not passed and re-authentication does not need to occur as frequently. Cookies are often valid for an extended period of time, even if the web application is not actively used. After the cookie is obtained through Steal Web Session Cookie, the adversary may then import the cookie into a browser they control and is then able to use the site or application as the user for as long as the session cookie is active. Once logged into the site, an adversary can access sensitive information, read email, or perform actions that the victim account has permissions to perform.

There have been examples of malware targeting session cookies to bypass multi-factor authentication systems.[2]

ID: T1550.004
Sub-technique of: T1550
Tactics: Defense Evasion, Lateral Movement
Platforms: Office 365, SaaS
Data Sources: Authentication logs, Office 365 audit logs
Defense Bypassed: System Access Controls
CAPEC ID: CAPEC-60
Contributors: Johann Rehberger
Version: 1.1
Created: 30 January 2020
Last Modified: 16 September 2020

Подробнее: https://www.bleepingcomputer.com/news/security/cisa-hackers-bypassed-mfa-to-access-cloud-service-accounts/

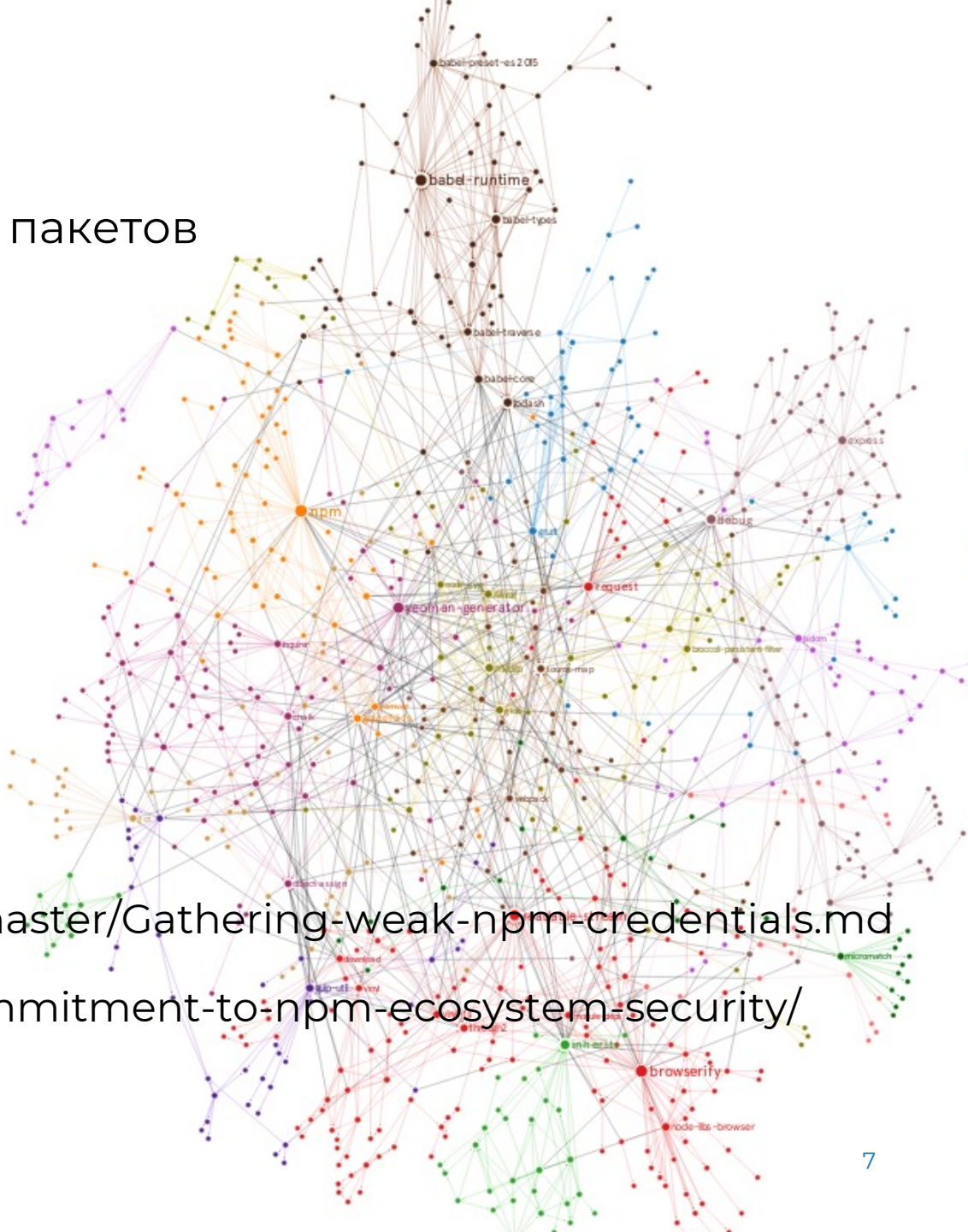
Современные вызовы

5. «Хитросплетения» крупнейших менеджеров пакетов

```
                    === npm audit security report ===

# Run  npm update @progress/kendo-angular-editor --depth 1  to resolve 1 vulnerability
```

High	**Cross-Site Scripting**
Package	@progress/kendo-angular-editor
Dependency of	@progress/kendo-angular-editor
Path	@progress/kendo-angular-editor
More info	https://npmjs.com/advisories/1549

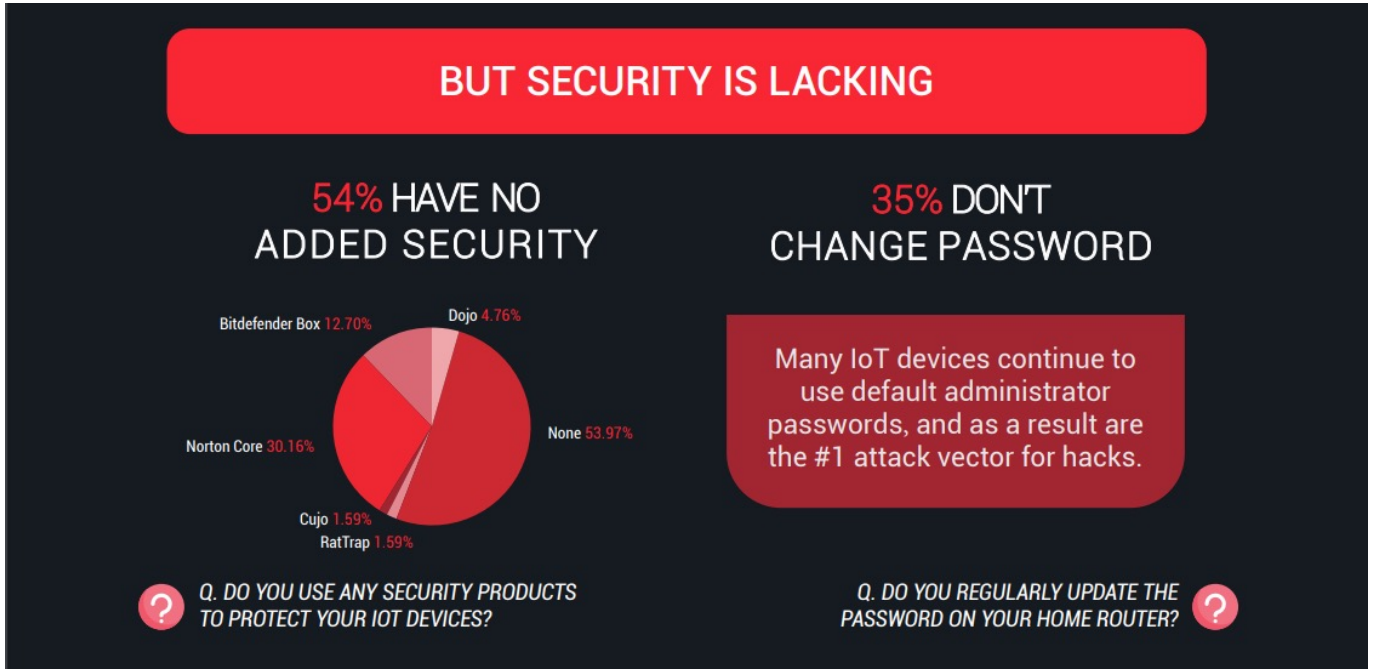


Подробнее: https://github.com/ChALkeR/notes/blob/master/Gathering-weak-npm-credentials.md

https://github.blog/2021-11-15-githubs-commitment-to-npm-ecosystem-security/

Современные вызовы

6. Атаки на элементы IoT



Подробнее: https://habr.com/ru/company/kauri_iot/blog/473532/

Предпосылки

Проблемы ИИ в кибербезопасности

Covid-19: влияние удаленной работы, повсеместное применение масок, новые методы фишинга и т.д.

Усиление инсайдерских угроз

Усиление атак на облачные сервисы, IoT и M2M

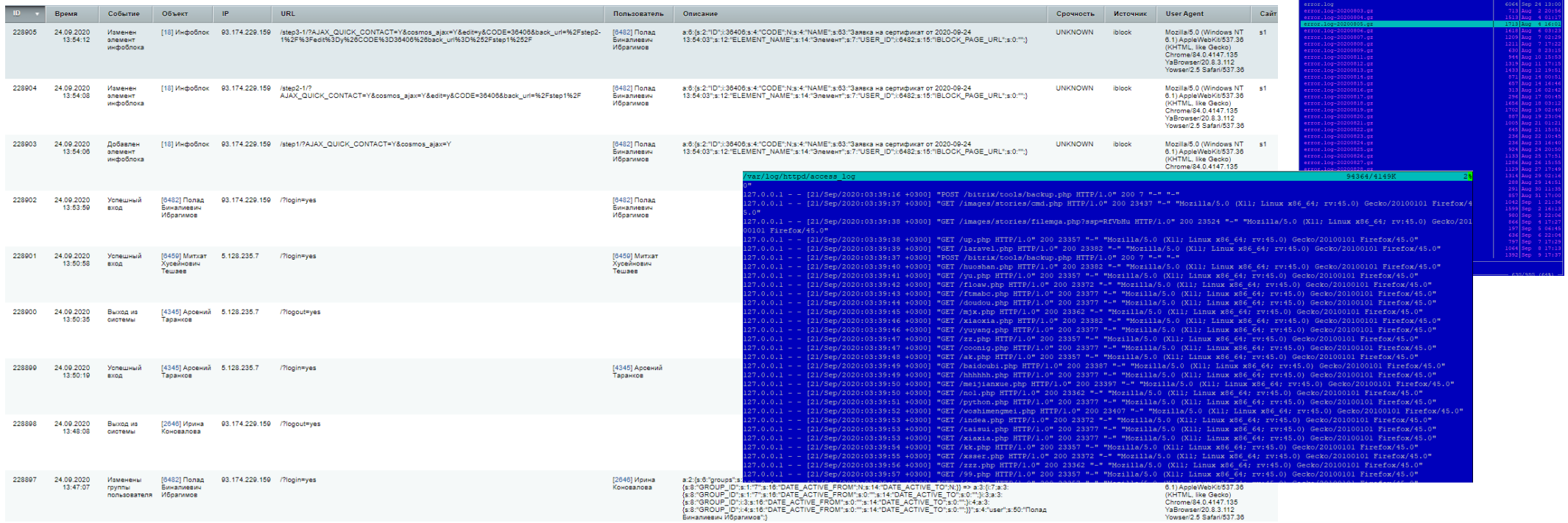
Результаты

- **Новые уязвимости OTP и MFA**
- **Биометрия - не панацея от всего**
- **Аутентификация «по подписке»**

Подробнее: https://www.anti-malware.ru/analytics/Threats_Analysis/2021-Cyber-Threats-and-Information-Security-Forecast

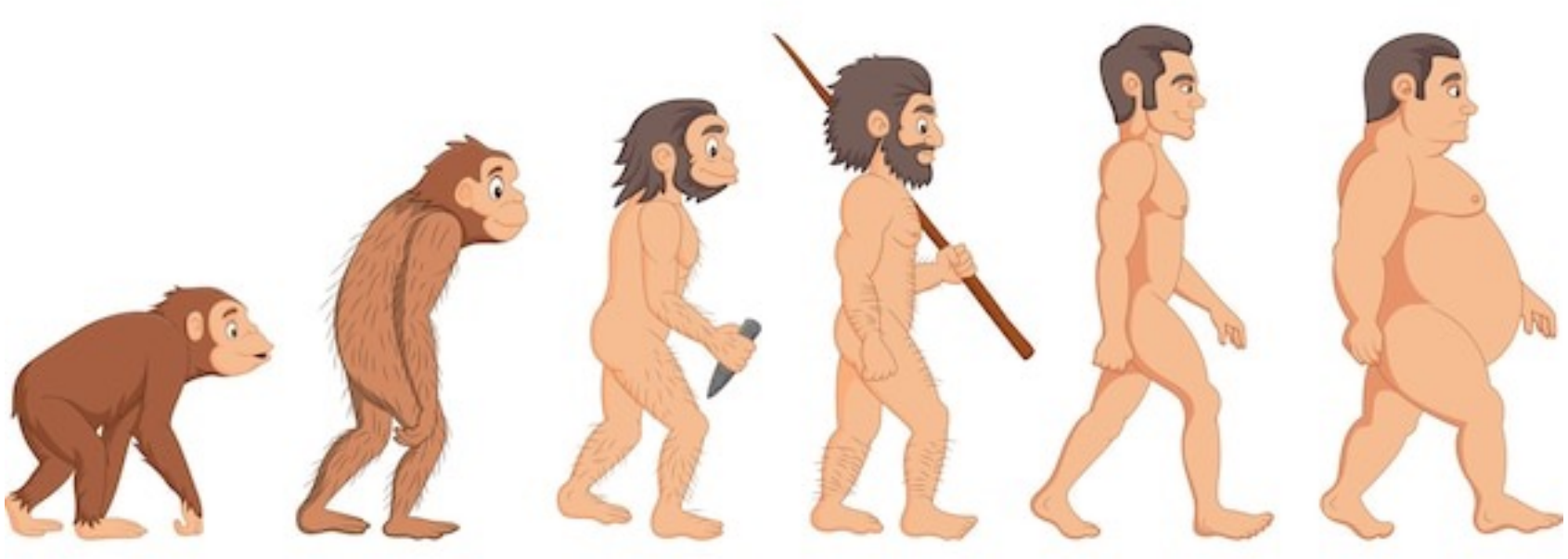
Адаптивная аутентификация

Решение, позволяющее по определённому набору признаков определить уровень риска тех или иных действий пользователя, и выбрать соответствующий способ/фактор аутентификации.



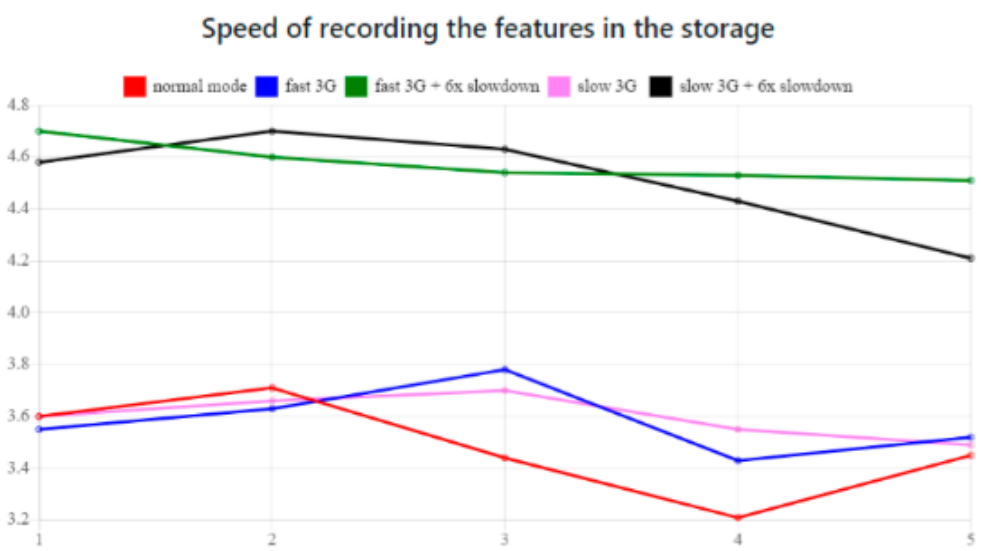
ID	Время	Событие	Объект	IP	URL	Пользователь	Описание	Срочность	Источник	User Agent	Сайт
228905	24.09.2020 13:54:12	Изменен элемент инфоблока	[18] Инфоблок	93.174.229.159	/step3-1/?AJAX_QUICK_CONTACT=Y&cosmos_ajax=Y&edit=y&CODE=36406&back_url=%2Fstep2-1%2F%3Fedit%3Dy%26CODE%3D36406%26back_url%3D%252Fstep1%252F	[6482] Полад Биналиевич Ибрагимов	a:6:{s:2:"ID";i:36406;s:4:"CODE";N;s:4:"NAME";s:63:"Заявка на сертификат от 2020-09-24 13:54:03";s:12:"ELEMENT_NAME";s:14:"Элемент1";s:7:"USER_ID";i:6482;s:15:"IBLOCK_PAGE_URL";s:0:"";}	UNKNOWN	iblock	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 YaBrowser/20.8.3.112 Yowser/2.5 Safari/537.36	s1
228904	24.09.2020 13:54:08	Изменен элемент инфоблока	[18] Инфоблок	93.174.229.159	/step2-1/?AJAX_QUICK_CONTACT=Y&cosmos_ajax=Y&edit=y&CODE=36406&back_url=%2Fstep1%2F	[6482] Полад Биналиевич Ибрагимов	a:6:{s:2:"ID";i:36406;s:4:"CODE";N;s:4:"NAME";s:63:"Заявка на сертификат от 2020-09-24 13:54:03";s:12:"ELEMENT_NAME";s:14:"Элемент1";s:7:"USER_ID";i:6482;s:15:"IBLOCK_PAGE_URL";s:0:"";}	UNKNOWN	iblock	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 YaBrowser/20.8.3.112 Yowser/2.5 Safari/537.36	s1
228903	24.09.2020 13:54:06	Добавлен элемент инфоблока	[18] Инфоблок	93.174.229.159	/step1/?AJAX_QUICK_CONTACT=Y&cosmos_ajax=Y	[6482] Полад Биналиевич Ибрагимов	a:6:{s:2:"ID";i:36406;s:4:"CODE";N;s:4:"NAME";s:63:"Заявка на сертификат от 2020-09-24 13:54:03";s:12:"ELEMENT_NAME";s:14:"Элемент1";s:7:"USER_ID";i:6482;s:15:"IBLOCK_PAGE_URL";s:0:"";}	UNKNOWN	iblock	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135	s1
228902	24.09.2020 13:53:59	Успешный вход	[6482] Полад Биналиевич Ибрагимов	93.174.229.159	/?login=yes	[6482] Полад Биналиевич Ибрагимов					
228901	24.09.2020 13:50:58	Успешный вход	[6459] Митхат Хусейнович Тешаев	5.128.235.7	/?login=yes	[6459] Митхат Хусейнович Тешаев					
228900	24.09.2020 13:50:35	Выход из системы	[4345] Арсений Таранков	5.128.235.7	/?logout=yes						
228899	24.09.2020 13:50:19	Успешный вход	[4345] Арсений Таранков	5.128.235.7	/?login=yes	[4345] Арсений Таранков					
228898	24.09.2020 13:48:08	Выход из системы	[2646] Ирина Коновалова	93.174.229.159	/?logout=yes						
228897	24.09.2020 13:47:07	Изменены группы пользователя	[6482] Полад Биналиевич Ибрагимов	93.174.229.159	/?login=yes	[2646] Ирина Коновалова	a:2:{s:6:"groups";s:[illegible] {s:8:"GROUP_ID";s:1:"7";s:16:"DATE_ACTIVE_FROM";N;s:14:"DATE_ACTIVE_TO";N;}} => a:3:{i:7;a:3:{s:8:"GROUP_ID";s:1:"7";s:16:"DATE_ACTIVE_FROM";s:0:"";s:14:"DATE_ACTIVE_TO";s:0:"";}i:3;a:3:{s:8:"GROUP_ID";i:3;s:16:"DATE_ACTIVE_FROM";s:0:"";s:14:"DATE_ACTIVE_TO";s:0:"";}i:4;a:3:{s:8:"GROUP_ID";i:4;s:16:"DATE_ACTIVE_FROM";s:0:"";s:14:"DATE_ACTIVE_TO";s:0:"";}}";s:4:"user";s:50:"Полад Биналиевич Ибрагимов";}			Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 YaBrowser/20.8.3.112 Yowser/2.5 Safari/537.36	

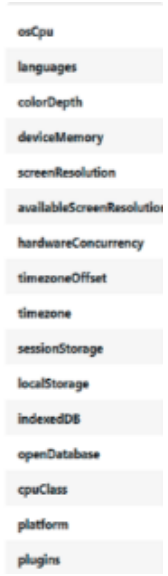
О развитии систем аутентификации



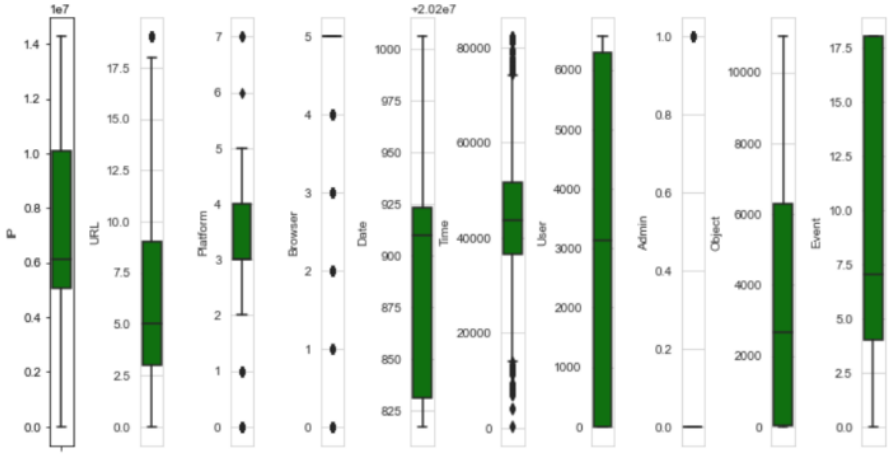
Без проверок → Однофакторная → Двухфакторная (2FA) → Многофакторная (MFA) → Адаптивная (риск-ориентированная) → Адаптивная в киберфизических системах

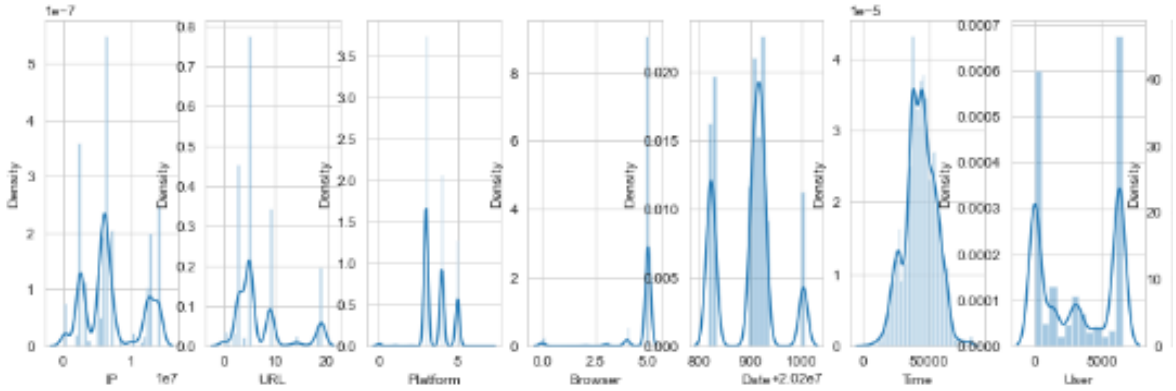
Адаптивная аутентификация оператора киберфизической системы





S	|P|	Best accuracy for profile, %	Best accuracy after expanding the feature space, %	Frequency of factor change
CPS #1 |C|=14 |A|=3	12	89	91	0.5
	32	87	87	0.52
	45	87	88	0.71
CPS #2 |C|=23 |A|=4	30	91	88	0.60
	50	84	86	0.64
	70	79	79	0.71





Алгоритмическое обеспечение

Вход:

- S – совокупность информационных систем, требующих реализации аутентификации оператора:

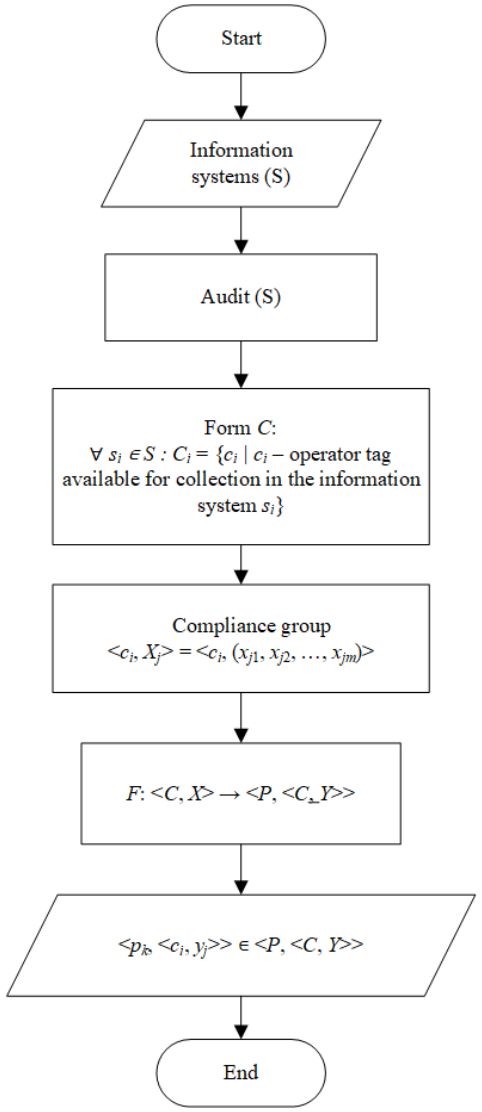
$$S = \{s_1, s_2, \ldots, s_n\},$$

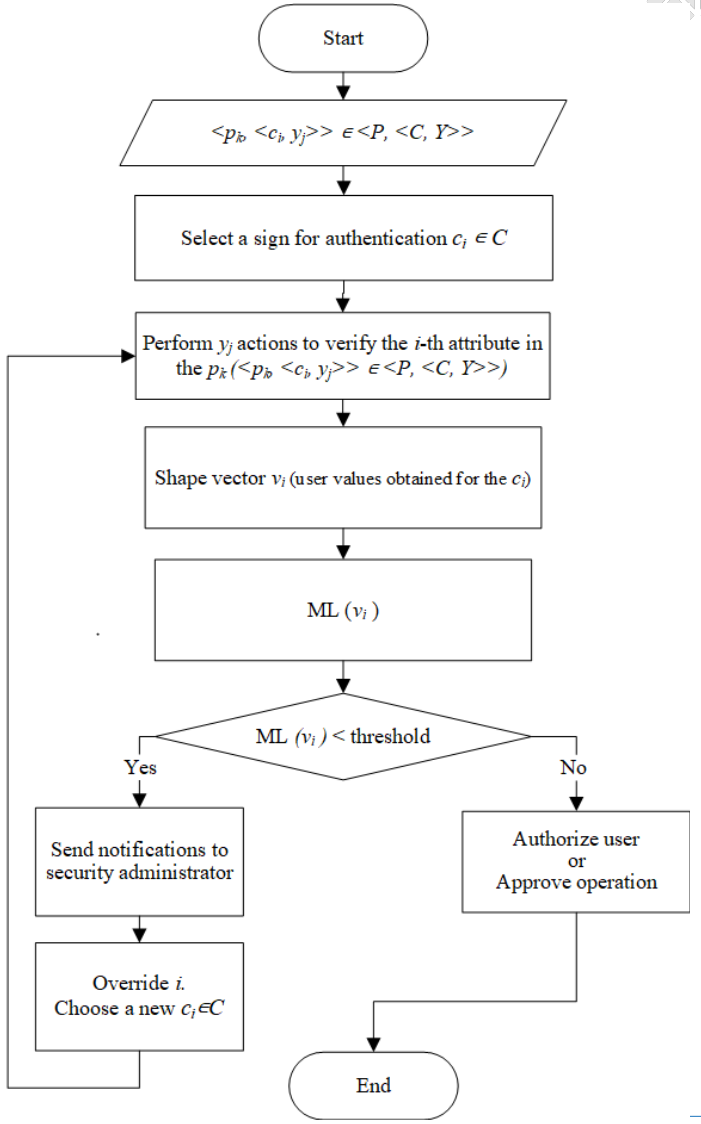
где n – количество таких систем;

- A' – множество возможных методов аутентификации.

Выход:

- Кортежи вида $\langle P, \langle C, Y\rangle\rangle$, определяющие пары профилей аутентификации и оптимизированный и ранжированный набор тегов и действия по его выполнению;
- Алгоритм адаптивной аутентификации на основе полученных профилей, отличающийся возможностью определения набора тегов на основе доступных системе методов аутентификации, с учетом анализа тегов, не прошедших проверку.





Алгоритмическое обеспечение

Необходимо проводить анализ безопасности протокола аутентификации для M2M

- MiTM attacks;
- Data Integrity;
- Confidentiality;
- Replay Attack;
- Session key attack;
- Physical attack of Control Device Disconnection
- и т.д.

~~SSO, NFC, hardware token etc~~

Заключение

«Аутентификация, как и другие элементы информационной безопасности, – это всегда гонка вооружений.

Производители улучшают свои системы, потом приходят хакеры и ломают их, а затем все начинается снова»

ЛАБОРАТОРИЯ № 80
«КИБЕРФИЗИЧЕСКИХ СИСТЕМ»

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ПРОБЛЕМ УПРАВЛЕНИЯ
ИМ. В.А. ТРАПЕЗНИКОВА
РОССИЙСКОЙ АКАДЕМИИ НАУК

Спасибо за внимание

Мещеряков Роман

г.н.с., д.т.н.


mrv@ieee.org

ИПУ РАН

Россия, 117997, Москва
ул. Профсоюзная, д. 65

+7 495 334-89-10

www.ipu.ru