Отже удосконалення системи перевірки знань студентів сприяє підготовці сучасних молодих спеціалістів.

ЛІТЕРАТУРА:

1. Аванесов В.С. Композиция тестовых задаиий: Учебиая книга для преподавателей вузов, учителей школ, аспирантов и студентов пед. вузов / Аванесов В.С. –[2-е изд., испр. и доп.]. –М. : Адепт, 1998. - 217 с.
2. Ингенкамп К. Педагогическая диагностика / К. Ингенкамп.- М. 1991.- 240 с.
3. Кедрович Гжегож. Теория и практика использования компьютерных технологий в общеобразовательных и профессиональных учебных заведениях Польши / Пер. с пол. Г. А. Цисовской. – К.: Вища школа, 2001. – 355 с
4. Крамаренко, И.С. Прогнозирование уровня учебных достижений учащихся средствами мониторинга / И.С. Крамаренко // Стандарты и мониторинг в образовании. - 2001. - №1. С.37-42.
5. Александр Черных. ЕГЭ явно переоценили. Рособрнадзор нашел серьезные нарушения в 77% перепроверенных работ. Перепроверка части высокобалльных работ ЕГЭ показала, что успехи школьников были кем-то сильно приукрашены. http://kommersant.ru/doc/2218633
6. Болотов В А. «Великая дидактика» и современность». В кн.: Тенденции развития образования. Двадцать лет реформ: что дальше? Материалы VI межд. научно-практ. конф. – М.: Университетская книга, 2009. -360 с.

Паламар С.

Науковий керівник – асист. Сіткар Т.В.

АУТЕНТИФІКАЦІЯ КОРИСТУВАЧА ЗА ДОПОМОГОЮ ГРАФІЧНОГО ПАРОЛЮ

Постановка проблеми. Люди живуть і взаємодіють в середовищі, де сприйняття зором є переважаючим для більшості видів діяльності, тому наш мозок здатний обробляти і зберігати великі обсяги графічної інформації з легкістю. Хоча нам, можливо, буде дуже важко згадати рядок з п'ятдесяти символів, ми можемо легко згадати обличчя людей, місць, які ми відвідали, і речі, які ми бачили. Ці графічні дані в електронному вигляді представляють мільйони байтів інформації та забезпечують великі можливості для унікальності вибору пароля. Таким чином, графічні схеми паролів дають спосіб зробити паролі більш зрозумілими людині при одночасному підвищенні рівня безпеки.

Постановка завдання. Метою є вивчення різних схем графічної аутентифікації, реалізація та впровадження схем графічної аутентифікації в операційних системах і оцінка ймовірності злому графічного пароля зловмисником.

Паролі є найбільш часто використовуваним методом для аутентифікації користувачів в комп'ютерних та комунікаційних системах. Як правило, паролі складаються з букв і цифр, тобто буквено-цифрові. Такі паролі мають великий недолік: їх важко запам'ятати.

Ми розглянемо графічні паролі, які складаються з будь-яких дій, які користувач виконує на зображенні. Такі паролі легше запам'ятати, але вони вразливі до підглядання через плече. Також ми розглянемо кілька схем графічних паролів, при використанні яких користувач може не побоюватися, що людина яка стоїть за його спиною побачить пароль або що його пароль буде знято на відеокамеру [2].

Виклад основного матеріалу. Буквено-цифрові паролі були вперше застосовані в 1960-і роки в якості вирішення проблеми безпеки, коли була розроблена перша багатокористувацька операційна система. Буквено-цифровий пароль - просто рядок з букв і цифр. Хоча майже будь-який рядок може служити в якості пароля, ці паролі забезпечують високу безпеку, поки вони складні настільки, що не можуть бути виведені або вгадані. Зазвичай використовуються такі принципи для буквено-цифрових паролів:

- Пароль повинен бути не менше 8 символів.
- Пароль не повинен мати відношення до користувача (наприклад, прізвище, дата народження).
- Пароль не повинен бути словом, яке можна знайти в словнику.
- В ідеалі, користувач повинен використовувати верхній і нижній регістри букв і цифри.

Ідея графічного пароля належить Грег Блондер (Greg Blonder, США), який запатентував її в 1996 р. Графічні паролі будуються з яких-небудь дій, які користувач виконує на зображенні.

Коли користувач робить спробу увійти за допомогою графічного пароля в систему, та оцінює намальовані ним графічні знаки або дії з ними і порівнює їх з графічними знаками і діями, які використовувалися при виборі графічного пароля. Далі система оцінює різницю між кожним графічним знаком та приймає рішення про те, авторизувати користувача чи ні, на підставі кількості помилок в комплексі. Якщо графічний знак помилковий або використаний не в тому порядку - намальована не та лінія, - то авторизація не пройде. Якщо типи ліній, точок, їх порядок і положення правильні, то система буде оцінювати, наскільки графічний знак відрізняється від того, який вона бачила раніше, і прийме рішення, чи є він досить схожим, щоб авторизувати відвідувача. З цієї причини, аутентифікацію на основі графічного пароля іноді називають графічної аутентифікацією користувачів (GUA) [1].

У більшості випадків графічні системи засновані на тому, що в якості пароля виступають або координати клацань миші, або певний набір символів, присвоєний графічним об'єктам.

Переваги систем графічного пароля перед іншими видами систем аутентифікації очевидні:

• Легкість запам'ятовування (користувач запам'ятовує не буквено-цифровий набір символів пароля, наприклад, jfhY7Je?I94, а якийсь набір графічних об'єктів та/або дії з ними).

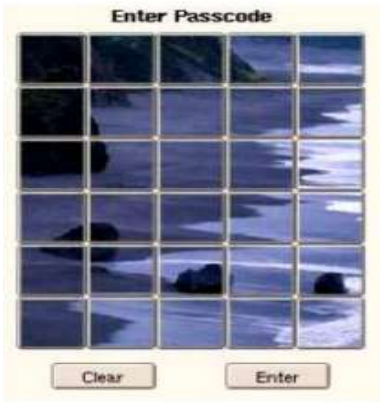
• Якщо величезний мінус біометричної аутентифікації - це складність заміни скомпрометованого пароля, то скомпрометований графічний пароль, як і буквено-цифровий, замінити легко і просто;

• Стійкість до методів злому графічних систем заснована на складності проведення проти графічних паролів автоматизованих атак (наприклад, за словником) або використовувати для підбору пароля широко поширені програми-шпигуни. Однак графічні паролі більш схильні до «атак через плече» - підглядання пароля при його наборі. Як контрзахід розробники розглядають створення схем для кишенькових комп'ютерів або робочих станцій, що дозволяють тільки одній людині дивитися на екран під час входу в систему.

• Порівняно недорога вартість розробки. [5]

Деякі схеми аутентифікації на основі графічних

1. **Passlogix** - користувач зазначає кліком мишки, деякі «парольні» зображення об'єктів на малюнку в строго визначеному порядку. Подальший розвиток схема отримала а технології Passpoints - користувачеві пропонується на вибір понад 100 можливих точок на картинці, парольний комбінація будується з 5-6 кліків мишки в певному порядку. Допускається, що при аутентифікації користувач потрапляє хоча б в окіл парольних точок. Так, для входу в систему користувачеві необхідно натиснути на 4 червоних кола в цій картині, обраних ним при створенні пароля. Точки і послідовність їх натискання зберігаються в хешованому вигляді (по стійкості схема порівнянна з буквено-цифровим паролем з 8 знаків). [7]



2. **Passfaces** - користувач повинен вказати певних осіб в наборі з дев'яти осіб (природно, це ті особи, які вибиралися при розробці пароля). Зазвичай пропонується декілька наборів. Особи з'являються в випадкових позиціях. Процес повторюється, поки користувач не виявить всі

«парольні» особи [4].

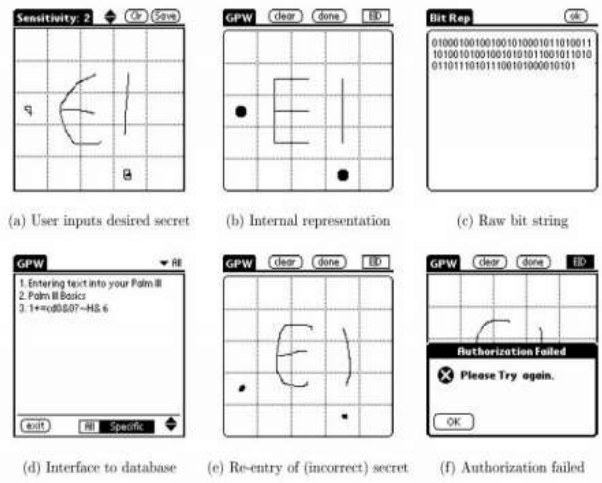
3. **Picture password** - графічний пароль, який часто використовується в мобільних телефонах. Картинка розбивається на фрагменти, а користувач фіксує вибирає послідовність фрагментів в якості пароля. Під час аутентифікації користувачеві необхідно ввести зареєстровані зображення в правильній послідовності. Кожному фрагменту зображення присвоюється числове значення і генерований числовий набір буде цифровим паролем [9].

4. **Pass-string** - система випадково розташовує N об'єктів на екрані. Користувач вибирає з них K об'єктів (пропускна підмножина) і запам'ятовує їх. При спробі входу в систему вона буде випадковим чином розташовувати N об'єктів. При цьому система випадковим чином вибере половину екрану, і випадково розставить K обраних об'єктів у цій половині. Для входу в систему користувач повинен знайти 3 парольних об'єкта, з'єднати їх подумки прямими і клацнути всередині нього. Процедура повторюється кілька (наприклад, 10) раз,

використовуючи інше розташування всіх N об'єктів. При N = 1000 і K = 10, число можливих паролів приблизно $2{,}6 \cdot 10^{23}$, що трохи більше, ніж число буквено-цифрових паролів довжиною 15.

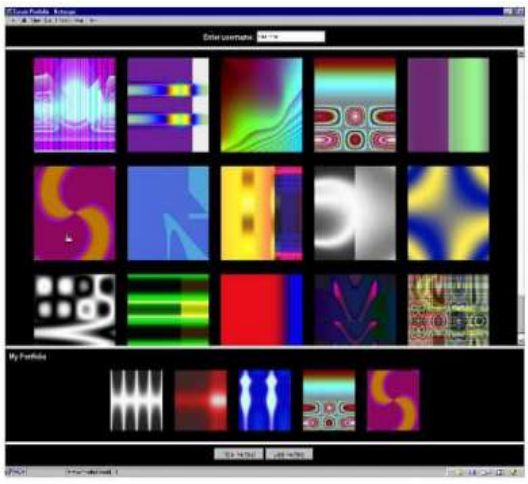
Існують й інші варіанти цієї схеми - клацнути об'єкт на перетині прямих, що проходять через чотири «парольних» об'єкта [3].

5. **Dej'aVu** - користувач запам'ятовує



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed



(заповнює портфель - portfolio) *p* малюнків, вибираючи їх з безлічі інших малюнків. Всі зображення створені за технологією «випадкове мистецтво», що переводить бітові рядки в безглузді абстрактні структуровані малюнки. Для аутентифікації користувача система видає йому набір з n малюнків, серед яких m малюнків містяться в його портфелі, а інші малюнки ні. Завдання користувача - правильно ідентифікувати зображення, які є частиною його портфеля.[6]

6. **Draw-a-secret** (намалюй секрет) - користувачу пропонується намалювати просту картину на сітці.

Під час аутентифікації, користувач повинен повторити картину. Якщо креслення стосується тих же ліній сітки і в тій же послідовності, що і при генерації пароля, то користувач проходить перевірку автентичності. [8]

Висновки. Встановлено, що одним з найкращих способів парольної аутентифікації є використання графічних паролів. Основною перевагою даного виду захисту пере усіма іншими є дешевизна – не вимагає додаткового обладнання, неможливість відтворення навіть при записі зловмисником процедури входу на відеокамеру.

Описаний спосіб введення графічного пароля буде корисним для співробітників банків із підвищеною функціональною відповідальністю, тобто для адміністраторів, аудиторів, менеджерів, співробітників служб безпеки та на тих робочих місцях, де наявність камери відеоспостереження передбачена технологічними вимогами – тобто для касирів, охоронців. Також доцільне використання такого пароля для клієнтів банкоматів із вбудованим тачпадом (touchpad), де присутність сторонніх осіб є постійною.

При в використанні графічного пароля у користувача формуватиметься сучасний погляд на проблему інформаційної безпеки, а людський чинник у методиці його запам’ятовування і використання буде зведено до мінімуму. Нові способи аутентифікації

ЛІТЕРАТУРА:

1. G.Blonder, "Graphical Passwords", United States patent 5559961, 1996.
2. Graphical passwords, Leonardo Sobrano, Jean-Camille Birget, The Rutgers Scholar, An Electronic bulletin of Undergraduate Research, vol 4., 2002. [http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm]
3. https://sparrow.ece.cmu.edu/group/pub/old-pubs/usenix.pdf
4. R. Dhamija and A Perrig, "Deja Vu: A User Study Using Images For Authentication", 9th USENIX Security Symposium, 2000.
5. Nali and J. Thorpe, "Analysing User Choice in Graphical Passwords", Technical Report TR-04-o1, School of Computer Science, Carleton University, Canada, 2004.
6. A. F. Syukri, E. Okamoto, and M. Mambo, “A User Identification System Using Signature Written With Mouse,” in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1948), 1998, pp. 403-441.
7. Passlogix, “www.passlogix.com,” last accessed in June 2005.
8. G. E. Blonder, “Graphical Passwords,” in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
9. L. D. Paulson, “Taking a Graphical Appraoch to the Password,” Computer, vol. 35, pp. 19, 2002.

Єднак Д.

Науковий керівник – Сіткар С.В.

АВТОМОБІЛЬНА ІНДУСТРІЯ: СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Для України надзвичайно важливо визначити пріоритетні галузі промисловості, на яких могла б базуватися економіка країни. Автомобілебудівну галузь України, яка є складовою машинобудівного виробництва, на сьогоднішній день якраз можна віднести до однієї з пріоритетних. Сучасна історія дає приклад десятків країн, що досягли процвітання за рахунок ставки на розвиток цієї галузі: Німеччина, Японія, США та ін. Від виробництва автомобілів безпосередньо залежить економіка Франції, Італії, Великобританії, Південної Кореї, Китаю тощо.

Отже, автомобілебудування в промислово розвинених країнах суттєво впливає на економічний і соціальний розвиток суспільства, дає могутній імпульс розвитку інших галузей, забезпечує стійке зростання зайнятості населення, підвищує товарообіг тощо.

При дослідженні автомобілів авто-концернів Японії, Європи і США американським журналом Consumer Reports був зроблений висновок: машини виробництва японських фірм, як і раніше лідирують за надійністю практично у всіх категоріях, випереджаючи автомобілі європейських і американських марок. Розрив між конкурентами в цьому році скоротився до мінімуму. Так, на кожні 100 японських автомобілів в середньому припадало 15 випадків зафіксованих власниками неполадок, в порівнянні з 23 у європейських і 24 у американських машин.

Наведені вище дані та роздуми, на мою думку, повинні відповісти на запитання, чому при покупці автомобіля слід звернути особливу увагу на виробників японських автомобілів.

Мета даної роботи полягає в дослідженні питань, пов'язаних з сутністю, сучасним станом, проблемами та перспективами розвитку автомобільного транспорту. Для досягнення поставленої мети вважаємо за доцільне:

- визначити сутність, значення та характеристику видів автомобільного транспорту;