СЕРВЕР АВТЕНТИФІКАЦІЇ ДЛЯ ВЕБ-ЗАСТОСУНКУ

Земляной О.О., Корнієнко Б.Я.

Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ, Україна

Основними методами забезпечення безпеки є шифрування, ідентифікація / автентифікація, впровадження фізичних заходів безпеки. Система безпеки повинна бути спроектована так, щоб передбачити захист для пристроїв і шлюзів, мережі передачі, а також додатків, які розгортаються для забезпечення функціонування пристроїв.

Шифрування широко застосовується, є ефективним і досить гнучким рішенням для забезпечення конфіденційності інформації та створення систем захисту. Однак будь-яке шифрування, а особливо надійне, вимагає збільшення продуктивності і додаткових обчислювальних ресурсів, що є не завжди можливим.

Що ж стосується автентифікації, то дослідниками було запропоновано досить велика кількість підходів, які могли бути впроваджені для вирішення проблем безпеки. Одним з поширених методів є двофакторна автентифікація. Наприклад, автентифікація на основі одноразових паролів (OTP). При такому підході після надання ідентифікаційних даних, користувачеві або пристрою необхідно пред'явити ще й одноразовий пароль, згенерований центром розподілу ключів, тим самим підтверджуючи свою справжність. Такий метод не вимагає від пристроїв додаткових обчислювальних ресурсів або сховищ, проте є непридатним для пристроїв, які, наприклад, просто не можуть підтримувати можливість введення отриманого одноразового пароля.

Інші дослідження пропонують використовувати для автентифікації концепцію «цифрових спогадів», яка вирішувала б проблему запам'ятовування користувачами складних паролів. Однак такий метод накладає обмеження на ресурси пристроїв.

Пропоновані методи також включають і автентифікацію із застосуванням криптографії на основі еліптичних кривих. Незважаючи на те, що в цьому випадку необхідні базові параметри еліптичних кривих вираховують не самі

пристрої, після обчислення потрібна передача досить великого обсягу даних, яка може бути обмежена пропускною здатністю мережі.

Таким чином, різні існуючі методи автентифікації можуть бути застосовними для окремого сервісу і окремого класу пристроїв. Застосування єдиних методів і засобів ускладняється відсутністю стандартизації.

Для забезпечення безпеки мережі може бути запропонований підхід, який має в своїй основі концепцію «профілів безпеки». Введені метрики безпеки повинні відповідати таким основним показникам:

1. Конфіденційність і цілісність - найбільш важливі властивості інформації, що забезпечуються стандартними методами з урахуванням особливостей пристроїв мережі;

2. Надійність - дана метрика особливо актуальна для критично важливих об'єктів, де збої в роботі можуть привести до серйозних наслідків;

3. Масштабованість - мережа повинна підтримувати можливість розширення без шкоди функціональності або безпеки;

4. Підтримка працездатності (стабільність) - підтримувані протоколи, технології та програми повинні мати можливість своєчасного оновлення та збереження працездатності пристроїв;

5. Виявлення вторгнень - в мережі повинні бути реалізовані заходи щодо своєчасного виявлення атак або будь-яких інших спроб порушення роботи;

6. Своєчасність - виражає здатність мережі реагувати на події, що відбуваються;

Розглянемо автентифікацію з використанням токенам. Такий спосіб автентифікації найчастіше застосовується при побудові розподілених систем Single Sign-On (SSO), де один додаток (service provider або relying party) делегує функцію автентифікації користувачів іншому додатку (identity provider або authentication service). Типовий приклад цього способу - вхід в додаток через обліковий запис в соціальних мережах. Тут соціальні мережі є сервісами автентифікації, а додаток довіряє функцію автентифікації користувачів соціальних мереж.

Реалізація цього способу полягає в тому, що identity provider (IP) надає достовірні відомості про користувача в вигляді токена, а service provider (SP) додаток використовує цей токен для ідентифікації, автентифікації і авторизації користувача.

На загальному рівні, весь процес виглядає наступним чином:

- Клієнт автентифікується в identity provider одним із способів, специфічним для нього (пароль, ключ доступу, сертифікат, Kerberos, і тд.);
- Клієнт просить identity provider надати йому токен для конкретного SP-додатки. Identity provider генерує токен і відправляє його клієнту;
- Клієнт автентифікується в SP-додатку за допомогою цього токена.

Процес, описаний вище, відображає механізм автентифікації активного клієнта, такого, який може виконувати запрограмовану послідовність дій (наприклад, iOS / Android програми). Браузер в свою чергу є пасивним клієнтом в тому сенсі, що він тільки може відображати сторінки, запитані користувачем. В цьому випадку автентифікація досягається за допомогою автоматичного перенаправлення браузера між веб-додатками identity provider і service provider.

Існує кілька стандартів, що в точності що визначають протокол взаємодії між клієнтами (активними і пасивними) і IP / SP-додатками, а також формат підтримуваних токенів. Серед найбільш популярних стандартів - OAuth, OpenID Connect, SAML, і WS-Federation. Деяка інформація про ці протоколах наведена нижче в статті.

Сам токен зазвичай являє собою структуру даних, яка містить інформацію, хто згенерував токен, хто може бути одержувачем токена, термін дії, набір відомостей про самого користувача (claims). Крім того, токен додатково підписується для запобігання несанкціонованих змін і гарантій автентичності.

При автентифікації за допомогою токена SP-додаток повинен виконати наступні перевірки:

- Токен був виданий довіреному identity provider додатком (перевірка поля issuer);

- Токен призначається поточному SP-додатку (перевірка поля audience);
- Термін дії токена ще не закінчився (перевірка поля expiration date);
- Токен справжній і не був змінений (перевірка підпису).

У разі успішної перевірки SP-додаток виконує авторизацію запиту на підставі даних про користувача, що містяться в токені.

Існує кілька поширених форматів токенів для веб-додатків:

- Simple Web Token (SWT) - найбільш простий формат, який представляє собою набір довільних пар ім'я / значення в форматі кодування HTML form. Стандарт визначає кілька зарезервованих імен: Issuer, Audience, ExpiresOn і HMACSHA256. Токен підписується за допомогою симетричного ключа, таким чином обидва IP- і SP-додатки повинні мати цей ключ для можливості створення / перевірки токена;
- JSON Web Token (JWT) - містить три блоки, між якими ставлять крапку: заголовок, набір полів (claims) і підпис. Перші два блоки представлені в JSON-форматі і додатково закодовані в формат base64. Набір полів містить довільні пари ім'я / значення, до того ж стандарт JWT визначає кілька зарезервованих імен (iss, aud, exp і інші). Підпис може генеруватися за допомогою і симетричних алгоритмів шифрування, і асиметричних;
- Security Assertion Markup Language (SAML) - визначає токени (SAML assertions) в XML-форматі, що включає інформацію про емітента, про суб'єкта, необхідні умови для перевірки токена, набір додаткових тверджень (statements) про користувача. Підпис SAML-токенів здійснюється за допомогою асиметричної криптографії. Крім того, на відміну від попередніх форматів, SAML-токени містять механізм для підтвердження володіння токеном, що дозволяє запобігти перехоплення токенов через man-in-the-middle-атаки при використанні незахищених з'єднань.

Література

1. Корнієнко Б.Я. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. Моделювання та інформаційні технології. 2018. Вип. 83. С. 34-41.

2. Корнієнко Б.Я. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. Наукоємні технології. 2017. № 4 (36). С. 316 - 322.

3. Корнієнко Б.Я., Максімов Ю.О., Марутовська Н.М. Прикладні програми управління інформаційними ризиками. Захист інформації. 2012. № 4 (57). С. 60 – 64. DOI: 10.18372/2410-7840.14.3493 (ukr).

4. Корнієнко Б.Я., Галата Л.П. Оптимізація системи захисту інформації корпоративної мережі. Математичне та комп'ютерне моделювання. Серія: Технічні науки, Випуск 19, 2019. - С. 56-62.

5. Korniyenko B., Galata L. Implementation of the information resources protection based on the CentOS operating system. Conference Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON - 2019) July 2 – 6, 2019, Lviv, Ukraine. - pp. 1007-1011.

6. Галата Л.П., Корнієнко Б.Я., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. Наукоємні технології, Том 43, № 3, 2019. – С. 300 – 306.

7. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. Conference Proceedings of 2019 IEEE Inernational Conference on Advanced Trends in Information Theory (IEEE ATIT - 2019) Dezember 18 – 20, 2019, Kyiv, Ukraine. - pp. 244-248.

8. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019) Kyiv, Ukraine, November 28, 2019. Vol-2577. P.281-291.

9. Корниенко Б.Я. Кибернетическая безопасность – операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2017. – 122 с.

10. Korniyenko B.Y., Galata L.P. Design and research of mathematical model for information security system in computer network. Наукоємні технології. – 2017, № 2 (34), С. 114 - 118.

11. Корниенко Б.Я. Информационная безопасность и технологии компьютерных сетей : монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с.

12. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. Sciences of Europe. – 2016. – V. 2. – No 2 (2). – P. 61 -63.

13. Korniyenko B. The classification of information technologies and control systems. International scientific journal. – 2016. –№ 2. – P. 78 - 81.

14. Корнієнко Б.Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив :монографія. – К.: Вид-во Аграр Медіа Груп, 2014. – 288 с.

15. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources / B. Korniyenko, //CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) Kyiv, Ukraine, November 27, 2018, Vol-2318, - P. 176-187, urn:nbn:de:0074-2318-4

16. Korniyenko B.Y., Borzenkova S.V., Ladieva L.R. Research of three-phase mathematical model of dehydration and granulation process in the fluidized bed / B.Y. Korniyenko, S.V. Borzenkova, L.R. Ladieva // ARPN Journal of Engineering and Applied Sciences Volume 14, Issue 12, June 2019, Pages 2329-2332.

17. Zhulynskyi A.A., Ladieva L.R., Korniyenko B.Y. Parametric identification of the process of contact membrane distillation/ A.A. Zhulynskyi, L.R. Ladieva, B.Y. Korniyenko // ARPN Journal of Engineering and Applied Sciences Volume 14, Issue 17, September 2019, Pages 3108-3112.

18. Korniyenko B., Ladieva L. Mathematical Modeling Dynamics of the Process Dehydration and Granulation in the Fluidized Bed. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing, vol 1247. Springer, Cham, pp. 18-30. https://doi.org/10.1007/978-3-030-55506-1_2

19. Korniyenko, B., Ladieva, L., Galata, L. Control system for the production of mineral fertilizers in a granulator with a fluidized bed. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, pp. 307–310.

20. Ladieva, L., Kozanevych, Z., Klusta, T., Korniyenko, B. System of control of the process of alkylation of benzene with peripene in the liquid phase. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, pp. 311–314.