MANAGING RISKS BY FEDERATING IDENTITIES IN DIGITAL ECONOMY

Marko Tmušić[1],
Mladen Veinović[2]

[1]Omnisecure,
Belgrade, Serbia
[1]Singidunum University,
Belgrade, Serbia

Abstract:

The paper focuses on the problem of managing multiple identities and access to them. Detailed insight in the field of research shows the concept and importance of federated identities and the necessity for their implementation into a business ecosystem. The solution for identity federation is presented, including detailed explanation of functionality and infrastructure of the security product. The significance and benefits of the security open standards are underlined. Recommendations and predictions are made, implying the need for change and different approach to IT security.

Keywords:

federated identities, IT security, access management.

1. INTRODUCTION

As the global digital economy grows, the number of digital identities rises. Consequently, the need to protect and manage collection, usage and distribution of personal information is greater than ever. Digital identities are the key factor in online world and finding the proper way to authenticate the legitimate users is the greatest challenge. When digital identities are not secured or distributed properly the exposure of information is certain. The information is then used for illicit purposes such as identity theft.

Stolen identity is a powerful tool in today's world. It can be used for a coordinated insider attack, selling digital identities on the deep web, credit card fraud, mail theft and other criminal acts. Attacks on digital identities are rapidly evolving and the highest level of attacks are on e-commerce and new accounts, where attacker uses personal information to create new financial accounts. As a result, companies endure extremely negative impact on their businesses, reputation and customer's trust.

Digital business is a dynamic environment, technologies are changing swiftly, and organizations have new ways of conducting business, thus implicating that information security risk becomes a top concern. Information security and risk management are the key components that ensure continuous improvement of planning, building and running security solutions adopted for business needs.

As a typical employee becomes more mobile and "Bring your own identity" trend continues to grow, accessibility and availability of

Correspondence:
Marko Tmušić

e-mail:
marko.tmusic@omnitechit.eu

DOI: 10.15308/Sinteza-2017-30-34

enterprise services need to be managed securely. Problem with multiple identities can be solved by using distributed identities. Distributed identity implies the secure exchange of identity information across one or multiple trusted domains, providing users with the ability to use one set of login credentials to access multiple applications.

To manage authentication mechanisms and ensure that every user interaction is truthful and rightful, distributed identity systems use federated identity ("web of trust") or brokered identity ("trusted third party").

2. OVERVIEW OF THE FIELD OF RESEARCH

As a leader in IT Security field with a wide range of security solutions, IBM provides security intelligence, helping companies protect their people, systems, data and improve their business. Security solutions for identity and access management include IBM Security Access Manager, IBM Federated Identity Manager, IBM Security Identity Manager, IBM Security Privileged Identity Manager, IBM Security Identity Governance, IBM Security IAM Cloud.

Although confidentiality, integrity and availability are crucial parts of every security system, the CIA concept is not enough in the digital business world. Digital explosion, interconnectedness of different systems, devices and the growing evolution of Internet of Things pushed the digital world into a physical world.

Protecting information is not enough, as providing safety for both people and their environments must be equally important. As a result, CIA concepts are to be expanded with one key component – safety. Necessity to protect not only the digital world but also a physical one is inevitable.[5]

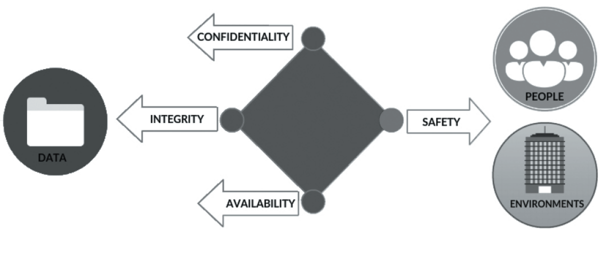

Fig. 1. "CIAS" model of digital security

The concept of safety includes both people and assets. Safety of people is very important, and with proper training, employees will know how to prevent physical unauthorized access, avert danger or disaster, react quickly and respond as a team. Safety of assets implies the physical security mechanisms such as locks, fences, surveillance, lighting etc. Both data and physical security play an important role in IT security, ensuring that with secured systems and with secured work environment high level security can be achieved.

Business data are now distributed via different dynamic environments, detached from the traditional enterprise. Managing risk is a crucial part in securing business data and making sure that businesses will have a desired outcome. Risk based approach will ensure flexible and responsive security solutions, adopted for business needs. Risk-Adjusted Value Management model can be created, integrating IT risk into corporate performance. As a result, the risk is addressed and business value is added.

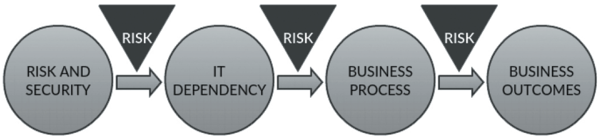

Fig. 2. Risk-adjusted value management model

When designing security solutions, it is important that security product is agile, modular, adopted for business needs and that it ensures smooth administration and usage. The main goal of identity and access solutions is to safely boost businesses, employee productivity and protect organization from inside and outside threats. Benefits from implementing such solution are various:

- Secured environment, data and people
- Effectiveness and efficiency
- Productive and motivated employees
- Simplified administration and management
- Reduced integration costs and pressure on support desks

Federated identity concept is based on the creation of globally interoperable online business identity, incorporating various applications and system identities. It is more effective and efficient to use a single sign-on type of accounts because a single user can have many accounts, passwords and usernames across dozens of systems. User weaknesses include slow input and forgetting of credentials, and weak, attack prone passwords. Federated identity also indirectly aims at improving the cost efficiency of a system, because it removes the need for many administrative roles which were needed within the previous system.

This approach undermines outside attacker efforts to compromise a system and also to halt a company workflow, sometimes for several days in a row. From this point on there is no need for creating and managing multiple accounts, passwords and users from other systems.

Federation represents the set of business, technical and policy agreements, allowing companies to interoperate by using shared identity management.

Functionality is based on the trust infrastructure implemented by the IBM Tivoli Federated Identity Manager trust service. Each solution can also be deployed separately, thus providing complete federation solution.

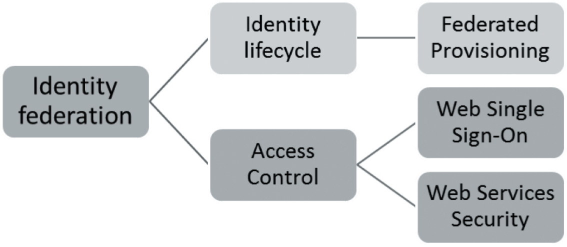

Fig. 3. IBM Tivoli Federated Identity Manager functionality

There are numerous benefits of implementing federated identity management in business environments. Identity management costs are reduced because companies only manage access to data and do not have to manage accounts or user account data that are not under their control. Using only one global identity for authentication and navigation through multiple web sites and applications improves user experience. Because of the federated identities, seamless integration between enterprise applications is ensured, enabling end-to- end security and trust capabilities.

3. OVERVIEW OF THE PROPOSED SOLUTION

IBM Identity and Access Management solution provides modular all-in-one security solution that helps companies protect their resources, make them easily accessible, boost business productivity and lower the integration costs. The modular nature of the IBM Identity and Access Management is the core operating principle, enabling a more scalable, flexible and maintenance friendly solution.

The solution provides a procedurally simpler and reduced risk approach to securing an uninterrupted user experience. This is achieved by shielding the vital assets with the use of strong multi-factor authentication and risk-based access. The IBM Identity and Access Management consists of the core module (Security Access Manager Platform), and can be extended by adding additional license-based modules. The additional modules are Advanced Access Control module and Federation module.

IBM Tivoli Federated Identity Manager represents a federated single sign-on solution, whose infrastructure enables identity propagation through SSO capabilities, eliminating the need for multiple user identities and passwords. Identities can be federated through multiple security infrastructures. The following deployment scenarios are supported, while each scenario can be deployed separately:

- Federated single-sign on
- Web services security management
- Provisioning
- Identity token exchange

Federated single-sign on scenario facilitates creation and management of federated single sign-on environments. Web services security management scenario represents an authorization solution, ensuring that only properly evaluated user requests can access resources through different domains. Provisioning scenario enhances current provisioning solutions across the internet by using web services standards. Identity token exchange deployment scenario provides the transmission of user credential information between different identity tokens.

During federation, business partners can have one of two roles: identity provider or service provider. Identity provider is responsible for authentication of the user and assertion of identity of that user for trusted business partner – service provider. The assertion consists of authentication statements, assuring that user is successfully authenticated. Identity provider is in charge of account creation, password management, provisioning and general account management.

As a result of a trust relationship between the identity and service provider, identity information about user is trusted and service provider delivers the required service or information to the user. Trust relationship is ensured by cryptographic keys used to encrypt and sign messages. By doing identity tasks, identity provider relieves business partners (service providers) from redundant identity management. Identity and service provider reduces the identity and access management cost and improves user experience.

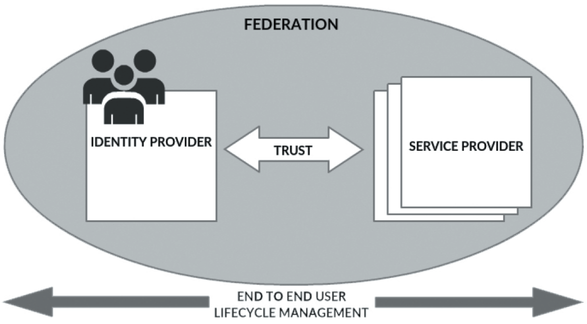

Fig. 4. End-to-end user life cycle management

Federated single sign-on is a process where the user authenticates to the business partner - identity provider. If the user is successfully authenticated, the identity provider affirms user's identity to the service providers, granting him federated access to applications and services. In order to accomplish interoperability both sides must agree upon technical terms.[2]

Firstly, format and content of the security token needs to be managed. The security token generated by one partner needs to be acceptable for the other partner. The terms on which information is sent inside the token and how it is interpreted must be agreed on. Generation and consumption of security tokens in Tivoli Federated Identity Manager are managed by the trust service and invoked by the SSO protocol service.

Secondly, the single sign-on protocol needs to be managed. SSO protocol specifies the communication between the parties. It describes how a client requests and presents a security token and how a token is defined. SSO protocol messages in Tivoli Federated Identity Manager are managed by the SSO protocol service.

On the communication layer, all communication and HTTP messages are managed by the point of contact server, in Tivoli Federated Identity Manager, that is, WebSEAL web server. On the protocol layer, SSO messages are exchanged with the third-party through the point of contact server. On the trust layer, security tokens are exchanged between the Tivoli Federated Identity Manager and the third party through the SSO Protocol Service.

Presently, companies are striving to embrace business on demand solutions. The business model needs to be responsive, adaptive, focused and resilient. In order to do so, deconstruction of the enterprise is inevitable. Deconstruction of infrastructure to partners, customers, suppliers can be accelerated by implementing open standards and service oriented architecture. Open standards are the key components that enable interoperability between different systems, services and applications.

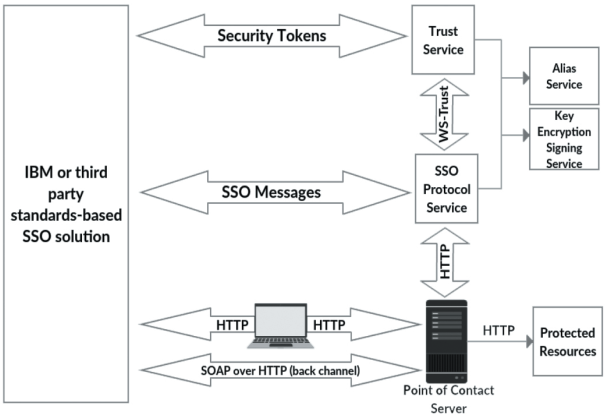

Fig. 5. Single sign-on components and communication between layers in IBM Tivoli Federated Identity Manager

With a wide range of supported open standards and cryptographic protocols, Tivoli Federated Identity Manager provides security customization and web service protection. Authentication information is managed through security open standards based identity and security tokens. Security token service (STS) is built into Tivoli Federated Identity Manager. It enables the identity mediation services, allowing the managing, mapping and propagating identities.[3] The module expands on the capabilities of the core federation solution for SSO and identity mediation for enterprise applications as well as SaaS.

IBM Tivoli Federated Identity Manager provides support for SAML 2.0, OpenID connect, OAuth, WS-Federation, WS-Security, WS-Trust, Information Card Profile, IBM Resource Access Control Facility, SHA-2, X509, Kerberos tokens.

Advanced Access Control Module has risk-based access capabilities, calculating the risk and protecting the information flow. Risk-based access enhances security of authentication and authorization mechanisms, estimates the risk and calculates the risk score. As a result, new policy rule is created and it determines whether user's request to access information will be permitted, denied or challenged to continue further authentication. The module is activated by explicit usage of an IBM license.

Integrated audit data collection and reporting generate the audit logs, tracking and incident reports to aid compliance activities. Tivoli Federated Identity Manager enables two- factor authentication with One-time password (OTP) capability. OTP improves authentication mechanism and can be implemented through configuration. The functionalities of the utmost importance for this module are OAuth support, context-based access, fingerprinting, multifactor authentication and device registration.

The business ecosystem needs to be carefully designed and connected. Federated SSO extends the availability and accessibility of applications to business partners, customers and consumers. As a result, resources are protected, easily accessible and the system integration cost is reduced.

As the digital era continues to grow and expand, the cyber security threats continue to evolve and adapt, creating a massive damage in digital economy. The uncontrolled and unsecured growth of Internet of Things will continue to threaten cyber security. If not secured, the increased growth of botnet networks made up of hacked IoT devices will produce a massive DDOS attacks. Physical security measures are going to be upgraded, in order to prevent insider attacks and use of external devices that are brought to fulfill one purpose - infect the system with malicious software.

The threat of ransomware has increased its potential to grow and become more frequent in 2017. Attackers will use more complex and sophisticated cryptographic algorithms. As enterprise data are more and more shifted towards cloud, the ransomware attacks will change focus on cloud systems. Cloud and mobile will definitely become common targets for various attacks and its security mechanisms will be questioned.

Business Email Compromise attacks are going to become more frequent and if employees are not aware of these types of attacks, serious damage can occur. CIAS concept and modern education techniques are the key factors in protection against these types of attacks. Employees must be aware of phishing techniques and properly trained to respond in critical situations.

Predictive analytics, machine learning and artificial intelligence will be essential parts of every security solution. These concepts will produce security solutions that are more intelligent and enable them to learn from previous activities so they can predict and prevent attacks on time. Adaptive and behavior based authentication will be commonly used, providing more effective and efficient authentication mechanisms.

„ *Companies will seek to quantify the costs and benefits of new technologies versus cost and likelihood of a breach, as information security becomes less an IT problem and more a risk management problem.* “ [10]

The cognitive era is coming and only business models which are agile, adaptive and secured will have the ability to successfully run a business and have a desired outcome. Rise of cyber risk management will have a great impact on businesses and become essential part of IT security.

4. CONCLUSION

In this paper, the concept of federated identities has been presented. Detailed insight in the field of research shows the modern approach regarding IT security principles and describes importance and a significant impact that federated identities have on IT security and business ecosystem. IBM security solution has been presented with detailed explanation of its structure, functionality and benefits.

Today, customers and companies are more and more reliant on well-structured interoperable systems in which the aspect of security solutions is significant. This ensures the greater and safer flow of information, especially considering the immense presence of large multinational corporations on the Internet.

The concepts of federated identities and access management will serve as pathways that will enable organizations to interconnect, giving lead to business productivity. IT security experts must be aware of the necessity to shift focus from designing more complex and secure systems to federation driven identity and access management and people-centric security, making systems more adaptive and resilient.

REFERENCES

[1] IBM - IBM Security Access Manager - Configuration federation topics, October 2015

[2] IBM Security - Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions, October 2005

[3] IBM Software - IBM Tivoli Federated Identity Manager, February 2013

[4] IBM Security - IBM Security Access Manager Federation Cookbook, May 2016

[5] Gartner - Managing Risk and Security at the Speed of Digital Business, February 2016, from https://www.gartner.com

[6] Gartner - Cybersecurity at the Speed of Digital Business, August 2016, from https://www.gartner.com

[7] ThreatMetrix - ThreatMetrix Cybercrime Report 2016, from https://www.threatmetrix.com

[8] RSA - Current State of Cybercrime 2016, from https://www.rsa.com

[9] Shahnawaz Backer, James Darwin, Vasfi Gucer, Chris Hockings, Trevor Norvill, Nilesh Patel, Martin Schmidt, Asha Shivalingaiah, Serge Vereecke, “IBM Security Access Manager Appliance Deployment Patterns”, October 2015

[10] Tyler Carbone, IBM Security LinkedIn Slideshare, Top 12 Cybersecurity Predictions for 2017