IDENTITY & ACCESS

Providing Cost-Effective Strong Authentication in the Cloud

a brief for cloud service providers

gemalto
security to be free

Introduction

Interest and use of the cloud to store enterprise resources is growing fast. Gartner estimates public cloud services to reach $131 billion worldwide in 2013, an 18.5 percent increase from the previous year[1]. Despite the increasing interest and use of cloud services, security continues to be a barrier to the cloud for many organizations. A recent poll found that 66 percent of organizations stopped or delayed at least one cloud project because of concerns with data security and privacy[2].

This white paper for Cloud Service Providers (CSPs) outlines the benefits and security concerns of the cloud, and proposes cost-effective and simple ways for public and private CSPs to provide users with secure access to resources through the use of one-time password (OTP) strong authentication.

The Cloud: Effective, Efficient and Productive

Enterprises are attracted to the idea of storing data and applications in the cloud

Storing data and applications in the cloud is attractive to enterprises for its promise of cost-effective and efficient storage, ease of use, and promoting remote productivity, and being cost effective, efficient and more environmentally-friendly than in-house servers.

Cost Effective and Efficient

- Pay-as-you-go for usage-based storage. The cloud enables organizations to only pay for the space required and add more as the need arises.
- No licensing, software, or product fees.
- Easy to introduce, use, maintain, and upgrade. The cloud is easy to use for everyone and the CSP takes care of maintenance and upkeep.
- IT staff no longer has to spend time on server maintenance.
- Merging and data transfer is smooth and inexpensive with the cloud. Data can be available instantly to pre-approved users through Internet access.

[1] Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion, *Gartner*, February 28, 2013
[2] Data Security, Privacy Halt or Delay 66 Percent of Cloud Implementations, *Erin Harrison*, October 18, 2012

Remote Access and Productivity

- With the cloud, employees can work from any device with Internet capabilities. They are no longer restricted to working from the office.
- Research shows people are more productive when they telecommute than when they work inside an office.
- All documents and apps are shared simultaneously to everyone, and the data is automatically synched up and saved. This allows for productive collaboration between employees. Notifications are set to alert users of changes.
- Bypass time zone and geographic restrictions through instantaneous sync capabilities.

Environmentally Friendly

- Most servers emit CO_2 and other gasses believed to harm the environment. The cloud has a smaller carbon footprint than on-premise server rooms.
- The cloud saves energy. Researchers at the Lawrence Berkeley National Laboratory predict an 87% reduction in primary energy use for companies that move their business software to the cloud[3].

Barriers to Cloud Adoption: Security Concerns

Despite numerous proven benefits of the cloud, some enterprises are still hesitant to make the move. Statistics show that two of the main barriers to broader cloud adoption are:

1. CIOs aren't convinced of its security, and
2. CIOs sometimes see increasing security as a complex process that is not user friendly

For enterprises, turning data over to the cloud means they have to forfeit some control, especially if they are used to tangible servers. Others are concerned that placing severs outside of direct supervision and in the cloud could signify giving up ownership rights. However, security is the biggest concern. In a study performed by North Bridge Venture Partners[4], of their 855 business users, IT decision makers, and cloud vendors surveyed, 46 percent cited security and mishandled information as the main barrier to cloud adoption.

---

[3] Bourne, James, "Cloud computing saves energy on huge scale, says new study – but how?" *Cloud Tech,* July 2013 http://www.cloudcomputing-news.net/news/2013/jun/12/cloud-computing-saves-energy-huge-scale-says-new-study-how/

[4] Cloud Computing Survey, North Bridge Venture Partners, *North Bridge,* 2013, *http*://northbridge.com/cloud-computing-survey-0

CIOs also aren't willing to make big investments in stronger security controls. In another study of CIOs, 56 percent said that the cost of more resilient security was the foremost reason they have not upgraded digital security.

Though it may seem like a challenge, there are ways for CSPs to overcome security and cost barriers and increase adoption of their services by providing higher levels of security in a cost-effective way. First, it is important for CSPs to understand why today's practice of accessing services using a username and password does not provide suitable security to users.

Weak Credentials Lead to Network Intrusions

One of the biggest worries for enterprises today is a data breach, which are occurring more frequently. The average cost of a data breach is $5.5 million or $194 for each record breached, according to a study by the Ponemon Institute, an organization that tracks data breaches.[5] When considering the costs of damaged reputations, diminished consumer confidence, and class-action lawsuits, the costs can increase.

One of the reasons data breaches persist is because many enterprises are still using basic usernames and passwords to access cloud services and networks. A 2013 study showed that 47 percent of CIOs believed a simple log-in and password was secure and would protect their network and applications from hacking and other cybercrimes.

According to the Verizon's 2013 data breach report, about 76% of network intrusions in 2012 involved weak credentials[6]. Authentication-based attacks, which include guessing passwords, cracking using specific tools, or trying out passwords from other sites on the target system, factored into about four of every five breaches that was classified as a hacking incident in 2012.

Stolen passwords played a role in 48% of the data breaches that involved hacking, Verizon found. This could have been accomplished by using stolen password lists from previous data breaches, keylogging malware or phishing attacks. Verizon estimated 80% of data breaches would have been stopped or forced to change tactics if a "suitable replacement" (such as strong authentication) to passwords had been used.

[5] Lax Security at LinkedIn Is Laid Bare, Nicole Perlroth, *New York Times,* June 10, 2012
[6] 2012 Data Breach Report, *Verizon*, 2013

Strong Authentication: A Brief Introduction

Many past security breaches potentially could have been avoided with the use of stronger access controls and the use of strong authentication technology. Authentication is proving the user's identity to an information system or service provider. For many organizations accessing cloud services, this is usually done with a login ID (username) and password. The use of this simple security is no longer sufficient in securing the important information stored in the cloud. Strong authentication adds layers of identity verification including something you know (a username and/or password) and something you have (a digital security device) to ensure only authorized users are able to access the cloud and network.

If someone steals a login ID and password but does not have the security device, they cannot access the cloud network, applications, or information.

Strong authentication is a necessary component to increase user confidence in the security of a CSP's cloud, and to differentiate the service from competitors.

Cost-Effective Strong Authentication

A cost-effective and simple way that CSPs can implement strong authentication is through one-time passwords. A one-time password (OTP) is a mechanism for users of cloud services to log on to a network or service using a unique password which can only be used once. This prevents different forms of identity theft by ensuring a username/password combination cannot be used a second time. Typically the individual's login name stays the same, and the one-time password changes with each login.

How it works: When the user needs to access corporate data resources on the cloud, they simply enter their username and the numeric code provided by the OTP device. The

How it works

OTP-based strong authentication for cloud computing

1. Local or remote user is prompted to create a **one-time password (OTP)** for authentication to cloud services.

2. User **creates an OTP** by pushing a button on the OTP device, or by using a mobile application to generate the OTP.

3. The OTP appears on the device screen or mobile phone, and **the user enters it along with his username.**

4. The **cloud service verifies** the username and OTP and the **user is securily authenticated** to the cloud service.

gemalto
security to be free

authentication server validates the code and access is granted to appropriate network resources. This increases the security of the login process by ensuring the person accessing the network is in possession of two factors of identity verification. In this case, the something you have is the OTP device, such as a token, and the something you know is the username and potentially a password. This means that someone cannot simply find a password that was written down or obtain it through social engineering, they would actually need to have the OTP device and the right code in conjunction with the user's other information to gain access.

Options for OTP Devices

The OTP is provided through a security or authentication token, available in multiple form factors

OTP tokens, mobile devices, and OTP/PKI tokens are all effective ways to implement strong authentication, but are also good examples of different solutions for different needs. An OTP token is a cost effective way to provide OTP that can easily be attached to preexisting items without being cumbersome. Mobile SMS and Mobile OTP are even less expensive ways to provide OTP, especially to employees that already carry their personal Internet-capable devices, such as smart phones, on their person.

Benefits of OTP for Strong Authentication

There are many benefits of OTP for both public and private CSPs. Implementing this form of strong authentication provides a simple and cost effective way to:

OTP: Form Factor Options

OTP Token: A thumb-sized device that produces a new OTP at the push of a button. Each newly generated OTP remains active for a limited amount of time before it expires. For example, once the button is pressed, the user may have only one minute before the password expires.

Card token: same functionality as the OTP thumb toke, but in a credit card sized device.

Mobile SMS OTP: The OTP is sent to the user via SMS, or text, message

Mobile OTP: Rather than receiving a text message, the user would request the OTP by opening an application on their mobile device.

Dual OTP/PKI: This method would require the user to use any of the previously mentioned OTP methods, but the chip embedded in the device (OTP token or mobile device) would be programmed to take the extra step and use digital certificates/Public Key Infrastructure (PKI), where the server validates the user's authenticity by data stored in the device.

- **Alleviate the threat of imitation for sensitive accounts**: OTP prevents opportunities for duplication of passwords and PINs in order to access data and information.
- **Enable secure access for off-site workers**: Bring your own device (BOYD) is no longer a major risk for companies that have employees in remote locations.
- **Increase convenience by removing the need for complex and costly password policies**: Security devices generating OTPs eliminate simple passwords entirely; no need for password rules.
- **Lower password maintenance costs**: No time spent on password recovery or resetting passwords means no wasted IT payroll.

Case Study Snapshot: Strong Authentication at Amazon Web Services and Windows Azure

Amazon Web services (AWS) is one of the first CSPs to offer strong authentication, called Amazon Web services multi-factor authentication (AWS-MFA), to allow more secure account access.
When a user signs in to an AWS website, they will be prompted for their username and password (the first factor – what they know), as well as for an authentication code from their AWS MFA device (the second factor – what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

More recently, Microsoft announced the availability of multifactor authentication on its Windows Azure cloud platform. Besides using a user name and password, users can authenticate through an application on their mobile device, automated voice call, or a text message with a passcode.

PKI: The Next Level of Protection

While OTP authentication for network access is a significant step-up from user name and password, certificate-based authentication raises the bar even further. Public Key Infrastructure (PKI) is a system that

validates a user's digital identity over a public or private network. It does so by associating a pair of public and private keys with the individual's identity credentials. These keys are created with a cryptographic algorithm and shared by a certificate authority (CA) that links them to the user's unique identity. The CA stores this information in a database and issues digital certificates, which include the public key or information about the public keys, in order to verify the user's identity. This also allows for the opportunity to use OTP and PKI technology together in order to create an even more secure security measure.

Deploying Strong Authentication with OTP

For CSPs, the deployment of OTP credentials is very straightforward. There are software as a service (SaaS) solutions available that can be implemented on any existing infrastructure. Services today include complete fulfillment and provisioning services, so CSPs can focus on cloud delivery.

In addition, as CSPs are evaluating their current infrastructure to start providing strong authentication to users, they should look for these components in a SaaS solution:

- **Authentication modules** that perform end-user validation using OTP
- A **customer care interface** that easily manages devices, authentication policies, roles, users, keys, and other functions
- A **user care interface** that enables end-users to register and manage their passwords and account information
- A **dedicated reporting portal** that enables efficient operation and administration with multiple report types available
- An **administrative interface** to add multiple LDAP directory and manage multi tenants

Additionally, these features are important for CSPs to look for when choosing a strong authentication solution:

- **Risk appropriate security.** The solution should support a broad portfolio of end-user devices for multi-factor authentication, giving IT administrators the flexibility to provide and manage different authentication devices based on user need. For example, OTP tokens may be adequate for the general employee population, but executives and privileged users may need a stronger, certificate-based solution.
- **A virtual token generator** in case a device is lost or stolen. Once the user or helpdesk provides the right answers to the secret questions, the service provider will create a virtual token and generate a number of OTPs the user can provide to login until the device is replaced. The OTPs can either be provided on a website, through email, or messaged (SMS) to the user.

- **Multi-tenant support**. Multi-tenant support ensures an organization's data is stored separately on a unique OTP server. When an authentication request is triggered, it is automatically routed to and administered by the appropriate tenant.

Thank You for Reading

The purpose of this brief was to give CSPs an overview of cloud benefits, barriers to adoption and options for strong authentication. We hope these ideas can help you to start planning on how to best provide strong authentication for users of your cloud service.

What did you find most useful? What would you like to know more about? We look forward to hearing your feedback and questions.

Where do you go from here? To start, we hope you share this brief with you colleagues. Work with them so that everyone understands the need for strong authentication for access to your public and/or private ways, and the ways to implement OTP security for access to your cloud.

About Gemalto

As the global leader in digital security, people all over the world rely on Gemalto to assist in accessing cloud services, verifying identities and protecting privacy.