Your users are under attack

Whether you are trying to protect your remote access or online customer accounts, user ID and password theft is a problem. As these threats evolve and become more pervasive and dangerous, one thing remains constant: criminals are after personal information and login credentials. By simply obtaining a user ID and password, today's criminals can remotely access bank accounts, sensitive patient databases and internal corporate networks, and can wreak havoc on individuals and the companies that serve them.

Defending our most sensitive accounts with only a user ID and password simply isn't adequate. When the Gartner security team was asked the question "If an organization were to spend $100 a year more per employee where should it spend it to get the greatest improvement in security," they had no problem coming back with the answer "strong authentication."[1] Strong authentication was defined as any authentication process that requires more than a single authentication method, typically a user's password. This sort of authentication is typically referred to as two-factor or multifactor authentication (MFA). Today's threat environment demands stronger multifactor authentication to prevent account takeover and data theft.

Multifactor authentication isn't new. It has been around for years and significantly reduces the risk of account takeover. So why isn't it more pervasive? Simply put, the MFA solutions available to date have been too complex to manage, have had a bad user experience, and have been too expensive for many organizations to implement. Solutions ranging from one-time password tokens to biometrics have all been offered to a market with lukewarm adoption by only the most security conscious of organizations.

While MFA solutions can provide a stronger security mix that makes it harder for criminals to access accounts, there are a number of barriers that providers need to overcome before multifactor authentication can gain broader adoption and user acceptance. These requirements include:

- Easy to install and administer
- Minimal user and customer impact
- Flexible options to meet various user and customer preferences
- Low per-user costs

Duo Security offers cost-effective, flexible and extendible MFA solutions that overcome these barriers. A cloud-based MFA service, Duo requires virtually no end-user configuration, no hardware or software installation at the customer site, and leverages an easy-to-use web interface for managing user credentials. This whitepaper will address the rising sophistication and frequency of attacks targeting account credentials and how Duo's MFA service is uniquely suited to address this problem. Duo's MFA service allows organizations to dramatically increase their protection around their most sensitive remote access and customer accounts in an unobtrusive, cost-effective way.

More insidious and subtle online crimes

The risk for online transactions is increasing because it is easier than ever to steal user IDs and passwords and use them to remotely access sensitive corporate and customer accounts. Where attacks were once difficult to carry out and were mounted only on "high value" targets, criminals are now turning their sights towards the "tail end" of the market. Stealing credentials is now as simple as spamming thousands of users with innocuous looking emails that can infect PCs with malware or Trojans —software that is silently installed on the user's PC and can steal credentials. In fact, in 2010 alone, malware authors produced over 20 million strains of malware accounting for over 1/3 of all active malware programs.[2]

Unfortunately, a significant amount of corporate, personal and financial data is stored on worldwide-accessible websites, which are protected by a username and a password only. This is a notoriously weak security mechanism subject to easy compromise. This problem is compounded by the increasing requirement for businesses to provide their users and customers

1 "Time to Move to Better Authentication," Richard Stiennon, http://www.focus.com/briefs/information-technology/time-move-better-authentication/

2 "Malware Authors Crank Engines, Reach 20 Million Mark in 2010, " Brian Prince, eWeek, http://www.eweek.com/c/a/Security/Malware-Authors-Crank-Engines-Reach-20-Million-Mark-in-2010-693089/

617 Detroit Street
Ann Arbor, MI 48104
1 (855) 386-2884
info@duosecurity.com

with access to their accounts from any device, whether it is an approved corporate PC, a home machine, a mobile device, or a kiosk. Defending against credential theft is nearly impossible these days. Cyber criminals employ a variety of tactics to obtain credentials, including:

Phishing

This is an extremely common technique used to steal user credentials. Hackers set up a fake website that appears identical to a target site such as a bank. Users are then sent en-masse or highly targeted emails asking them to "verify" their personal information, or reminding them to log in. These emails contain a fake link redirecting the users to a malicious site, which then collects their usernames, passwords, and personal information. These credentials are then used in the users' stead to transfer monies into the assailant's accounts.

Malware

Through drive-by surfing attacks (these involve malicious code on innocuous websites that exploit vulnerabilities in the client operating system), hackers install software on the unsuspecting users' PCs. This software intercepts keystrokes and sends out personal information and user credentials to the attackers' servers, sometimes silently performing operations on the users' behalf in target sites. Sometimes malware is designed to "pharm", a technique which redirects users' browsers to bogus sites even without having them click on a bogus link. Similar, yet more dangerous attacks can also redirect an entire swath of users by attacking servers that govern the resolution of domain names to Internet addresses.

Persistence and Social Engineering

Passwords are often easily guessable and often attackers simply attempt guessing users' passwords in order to gain unauthorized access. Another common technique is to contact the user and convince them to provide their password of their own volition. For instance, an attacker might call under the guise of a technician and report technical problems in his account that need to be resolved. After convincing the user that they are of the target company, the scammers will ask for the users' username and password. They often will comply.

Online crime is accelerating, not waning

These tactics are becoming more and more pervasive and dangerous. Online crime, fraud, and theft have been steadily and rapidly rising. In 2009, the money lost as result of Internet crime has more than doubled to $559.7 million from $264.6 million in 2008, according to IC3.[3] Gartner estimates that 5 million consumers lost a total $1.8 billion[4] in 2008 to phishing attacks — and this in the US alone. Furthermore, Gartner estimates that most fraud costs were born by the financial service providers themselves. Faced with increasingly more sophisticated attackers, banks, healthcare portals and corporations that have an online presence or mobile workers are struggling to keep sensitive information safe. The boom in online services and the increasing rates of cyber crime are on a dangerous collision course.

Users are also increasingly accessing their accounts from a variety of devices that each present their own unique challenge and threat vectors. Authentication security methods that might have worked for a PC — like a USB token — won't work on a mobile device. Accounting for the variety of login machines is important when considering a strong authentication option.

Barriers to wide-scale multifactor authentication (MFA) adoption

Given the increased threat and the value of online data, it would make sense that more organizations than ever would be looking to deploy MFA to defend their user and customer accounts. Unfortunately, strong MFA adoption remains low despite its significant security advantages. There are two primary barriers preventing MFA adoption: cost and user experience.

For starters, it's not hard to see why cost remains a significant inhibitor to adoption of MFA. A single token can cost upwards of $100 per user and this doesn't take into account the fact that the tokens will frequently have to be replaced due to loss, theft, damage or malfunction. In addition, this expense doesn't include support costs, deployment costs, or take into account the fact that even in the best case scenario, tokens need to be replaced every three years.

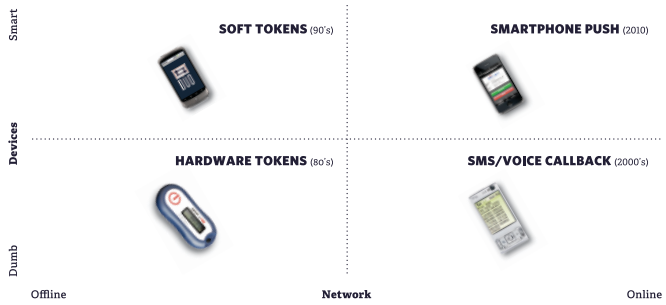
3 Internet Crime Complaint Center: 2009 Internet Crime Report

4 Gartner: "The War on Phishing is Far from Over"; 5 million US consumers, average loss $351

Poor user experience both for users and administrators is another large barrier to adoption. Implementing an MFA solution typically requires dedicated hardware and software on site, ongoing maintenance and administration, and distribution and management of tokens to their users, or even worse, to their customers. These requirements not only increase upfront capital investments, but also impact the overall total cost of ownership. Additionally, IT administrators often find their hands full with support requests and complaints after rolling out a token-based MFA solution. Because individuals don't like being required to carry around tokens to access their important accounts, many companies that have tried MFA have ended up utilizing it only where required by Government regulations or not at all.

Stronger authentication as a service

Duo provides cost-effective, scalable multifactor authentication (MFA) as a service to curb these problems. Leveraging consumers' mobile devices for strong, useable, risk-adaptive secondary authentication, the cloud-based security service requires virtually no end-user configuration, no hardware installation at the customer site, and includes an easily used web interface for management of user credentials.



Duo is authenticator agnostic and flexible enough to allow users to select whatever fits their environment. Whether they are working online or offline, or have smart or dumb devices, Duo allows businesses to offer their users a variety of two-factor authentication options that fit their needs. For standard cell phones or traditional land lines, users logging into a secured service receive a call to their phone to authenticate they are the ones making the transaction. In other cases, when performing high-risk transactions, users receive a notification on their smartphone to inform them of the transaction details and ask for confirmation. If they have no phone reception at the time of access, they can receive One-Time Passcodes via SMS ahead of time, or generate them using Duo's mobile app.

This eliminates the vast majority of risks from attackers compromising a PC, with the following benefits:

No complicated installation or configuration

Administrators no longer need to issue tokens to users or install certificates on their PC. Getting up and running with Duo is as simple as integrating with your existing remote access solution and you are ready to go.

Flexible user self enrollment

There is no complicated management process associated with running Duo's service. Users simply log in for the first time and choose the authentication option your organization allows that best suits them, i.e. a call back or a smart token.

No clutter

Users don't have to carry additional hardware devices, cards, etc. They only need their mobile phone, which they already carry.

No need for special hardware

There is no need for expensive card readers or requirements to use the same PC to access their services. Users utilize a variety of end devices or a PC to access the data.

Breaking the barriers of multifactor authentication

Duo provides an array of authentication models that fit the specific needs of any organization. Duo's service-based model overcomes many of the deployment and management barriers that have hampered broader adoption of multifactor authentication, including:

Easy installation

A simple drop-in solution for VPNs and an extendible, easy-to-use API allows users to set up within minutes, not months.

617 Detroit Street
Ann Arbor, MI 48104
1 (855) 386-2884
info@duosecurity.com

No cumbersome server integrations or hardware purchases

Duo customers don't need to buy expensive hardware appliances or exorbitantly pricey authentication tokens that require replacement every three years. There is no need for expensive card readers, and users can utilize a variety of end devices or any PC to access the service.

Cloud-based architecture and administration

With multifactor authentication services hosted on the cloud, there is no capital expenditures or costly infrastructure maintenance required.

Flexible options to meet customer needs

Supports applications for all major mobile platforms (i.e., Windows mobile, Windows Tablet PC, iPhone, Android, Blackberry, etc.), in addition to voice callback and SMS authentication so users never have to carry another device.

Improved security & reliability

Markedly improved security model provides dynamic protection against virtually all malware and phishing risks, and other evolving threats. Led by a seasoned security team with deep experience in the telecom and consumer Internet markets, Duo service is hosted by top-tier, SAS70 Type II certified datacenter providers servicing NIST 800-53, PCI, HIPAA, and ISO 27000 regulated customers, with 7 Tier-1 upstream ISPs.

Cost-effective subscription model

Due to a softer economy, small and mid-sized businesses are extremely cost conscious and pragmatic. Despite lacking the IT resources that larger companies have, they still must supply a service to their customers. Many of these companies don't want to sign multi-year contracts, but are looking for stronger authentication solutions such as Duo's, which provide APIs and charge for usage of its network on a per-user basis.

User convenience

Supplying users with a service that is convenient and has cost-effective means of authentication reduces barriers for service adoption. Users that use a cell phone for purposes other than authentication lowers the risk of a user handing over his credentials to a third party.

No upfront charges (pay as you go)

Duo customers are not required to invest thousands of dollars upfront, regardless of usage. They pay only for what they use, on a yearly basis, and avoid hefty upfront expenses for things like high availability, which is supplied free of charge.

Simple, affordable, per-user pricing

For less than the cost of a cup of coffee per user per month you can be up and running with strong authentication.

Painless integration

Whether you are protecting your remote access users or securing your web based logins, Duo makes getting up and running easy. For web based logins the IFRAME or REST-based web SDK makes for an easy remote access integration with any custom web application.

For remote access implementations, Duo has simple drop-in modules for SSL VPNs (such as Juniper, Cisco, and Sonicwall, among others) and an extendible, easily used API allow a user to set up a system in minutes, not months. Duo's also supports standard RADIUS and LDAP integration. Offering a broad range of integration options that protect any application or login gives organizations:

- Easy integration with any custom web application
- Optionally specify phone number with each request, with no storage of user phone numbers
- Fine-grained access control – Duo can protect individual transactions as well as login sessions
- Firewall-friendly proxy traversal for internal applications
- Strong SSL encryption provides mutual authentication and privacy of all authentication transactions

Flexible user enrollment

The Duo system allows users to leverage their mobile device as a secondary authentication factor, which greatly increases the security of their accounts. The self-service enrollment process allows users to quickly and easily activate the multifactor

617 Detroit Street
Ann Arbor, MI 48104
1 (855) 386-2884
info@duosecurity.com

authenticator via web integration without requiring any administrator setup.

Compatible with all OATH compliant tokens, Duo offers a mixture of hardware tokens, soft tokens on the phone, one-time-use SMS tokens, and phone calls to a user's cell phone to provide various costs and strengths of authentication that fit any environment. As was highlighted in the graphic illustrating the variety of two-factor authentication options, after enrolling, users can choose a variety of methods for their second factor of authentication whether they are online or offline and are using either a smart or dumb device.

Simple ongoing management

Duo's flexible intuitive web-based administrative interface allows for easy manageability and supports multiple administrator accounts.

Easy user provisioning and revocation

There is no need for special training for the IT department or for expensive software to manage authentication. A simple web admin console is all you need to provision users or change settings.

Built-in reporting and management

Centralized, real-time reporting and analytics for individual users and groups enable full, searchable audit trails of both successful and failed authentication attempts to audit and analyze all administrative actions.

Conclusion

With more and more users accessing their sensitive corporate accounts and personal and financial data online, organizations are struggling to keep their sensitive information safe. While a stronger authentication mix makes it harder for the bad guys to access accounts, there are still a number of barriers that providers need to overcome before multifactor authentication gains broader adoption and greater user acceptance.

Duo Security's cloud-based, authentication as a service overcomes those barriers by delivering a flexible, cost-effective multifactor authentication solution that's easy and more cost-effective to install and manage. With today's cyber threats more evasive and dangerous, now is the time organizations need to implement multifactor authentication solutions to prevent account holders from becoming victims of more sophisticated attacks without impacting the customer experience.

Duo Security makes two-factor authentication easy and convenient. Led by accomplished security visionaries, Duo Security provides authentication as a service built to prevent account takeover and data theft without the hassle and cost of traditional solutions. Duo's multi-factor authentication uses a mobile device or phone as a second factor to make integrations simple and the user experience flexible and pain-free. At Duo Security we aim to frustrate the bad guys, not your users.

More Information

Visit our website
http://www.duosecurity.com

Speak with a product specialist
Call 1 (855) 386-2884

About Duo Security

Duo Security's hosted two-factor authentication service brings strong, scalable security to organizations of any size. Every day, over 500 organizations in 40+ countries around the world rely on Duo to secure their logins and transactions.

Duo is led by seasoned security executives and researchers with deep experience in enterprise, telecom, and consumer Internet markets. Duo Security is a privately held company whose investors include Google Ventures and True Ventures.

Headquarters
617 Detroit Street
Ann Arbor, MI 48104
1 (855) 386-2884
info@duosecurity.com