UAEU Division of Information Technology (DoIT)

جامعة الإمارات العربية المتحدة
United Arab Emirates University

Th!nk IT

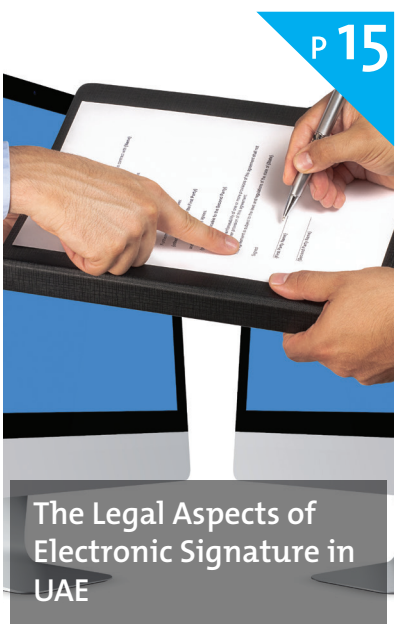
ISSUE 16, Jul 2018

Inside the **Pages**

Features

Two Factor Authentication (2FA)

Data Reduction- Deduplication and Compression



The Legal Aspects of Electronic Signature in UAE

Security Awareness

An overview of Web Services

In today's world, the need for agile, reusable and self-contained applications is at its peak. A web service can be described as a reusable software component that can be published and used by another software over the internet. The goal here is to provide an easy mechanism for applications to locate a service that provides the desired function and then implement it to achieve its goal.

Benefits provided with the use of Web Services

Many advantages are associated with the use of web services. In essence, the main advantage web services have over regular web applications lies in its interoperable nature, that is web services can communicate with different applications to provide a higher business level functionality despite the various underlying technologies of each application. Web services are hardware, programming language, and operating system independent. This independence is due to the use of the standardized XML technologies. Such technologies include SOAP, WSDL, and UDDI. Furthermore, web services offer additional advantages including reduced costs, application integration, and data integration.

Technologies used in Web Services

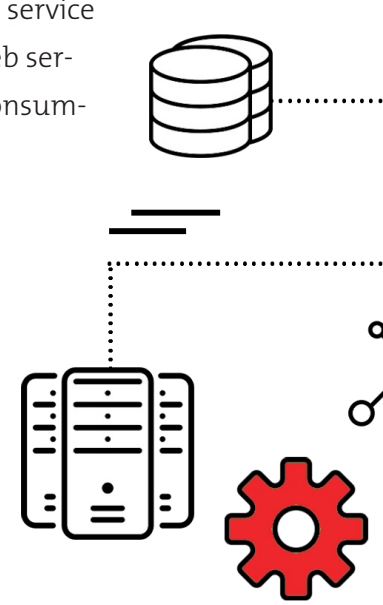
Several technologies support the process involved in the use of web services. These technologies are summarized below:

1. Simple Object Access Protocol (SOAP)

is a messaging protocol that enables data communication between web services.

2. Universal Description Discovery Interface (UDDI)

is a standard used by the service provider to describe a web service and is used by the consumer to locate a web service



3. Web Services Description Language (WSDL)

is a standard language used to describe the services offered and the functionality provided by each service.

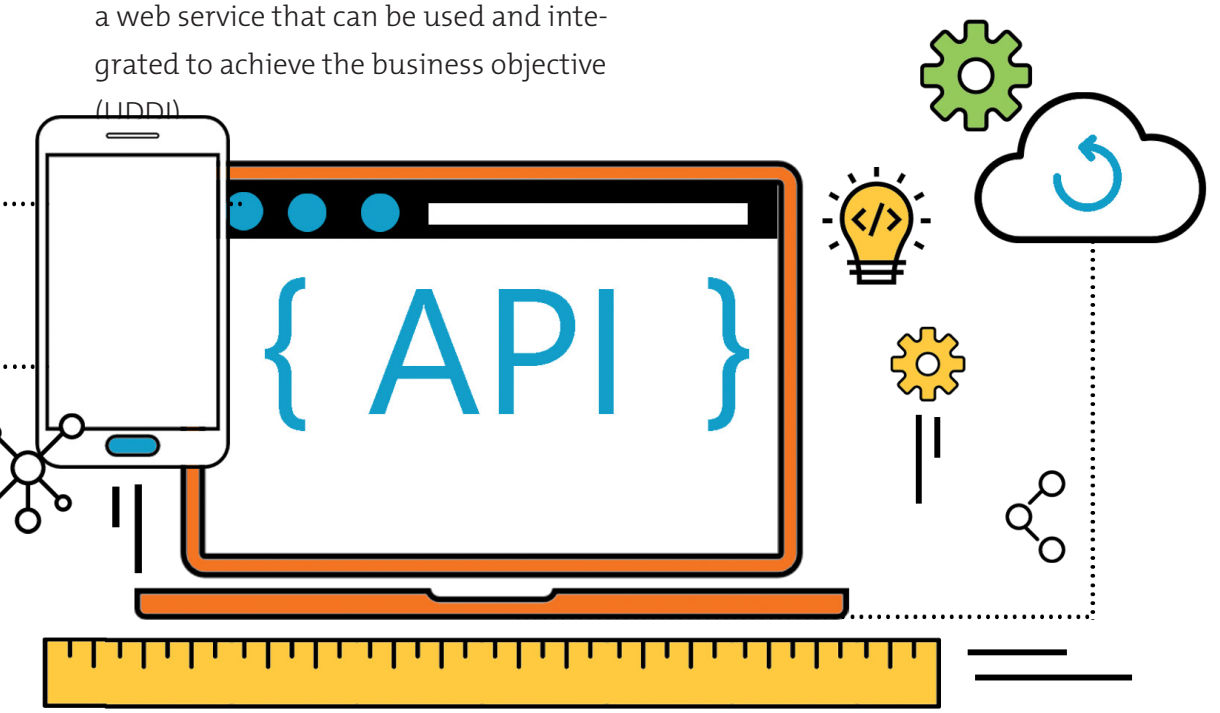
How do Web Services work?

So how is a web service used? Two entities collaborate with each other in a web service implementation: the web service consumer and the web service provider. A web service provider provides the interface and implementation for the web services it provides through SOAP, while a service consumer is a software that aims at achieving a business objective (i.e. performing a task) that can be accomplished with the use of a web service. Each web service provider registers its service in a web services directory, next, the web service consumer searches the directory for a web service that can be used and integrated to achieve the business objective (UDDI).

Using web services!

There is a number of web service providers. Such providers include Google, Amazon, eBay, PayPal, and FedEx. A web service can perform simple tasks such as calculations, google calendar operations, weather forecasts to more advanced tasks such as data transfer between applications and performing banking transactions.

In short, web services provide means of integration, agility, and reusability for enterprises and can greatly enhance business operations.




مركز الابتكار
Innovation Hub
بدعم من Google powered by
مبادرة جمعية البيت متوحد في الإمارات العربية المتحدة
An Initiative by Al Bayt Mitwahid in UAE

UAEU Innovation HUB Website

We have successfully implemented the UAEU Innovation-Hub website. The Innovation Hub is a collaborative community center built with the goal to develop a robust and innovative community, passionate about growing the UAE's technology and talent pipeline.

The Hub equips youth in the UAE with the skills needed to develop mobile applications, design products, create prototypes, and develop an understanding of Artificial Intelligence and Machine Learning.

In addition, the hub runs a program of Tech Talks, featuring technology experts, practitioners, and entrepreneurs. The Hub welcomes learners from diverse backgrounds, including teachers, school-age children (from age 8 upwards), university/vocational students and members of the community interested in developing their understanding of the latest technologies.

The Innovation-Hub website was built using a Content Management System (CMS). It allows users to create and maintain websites without any knowledge of HTML, and facilitates the creation of page layout with different content sections and other digital content. It is also a bilingual, responsive website, which means it is suitable for every device and every screen size, no matter how large or small, mobile or desktop. It integrates seamlessly with google analytics data, which can be viable within CMS in a flexible dashboard gadget.

Finally, the website has added accessibility tools such as contracting, changing color theme, and increasing or decreasing font size.

Author: Raed Shehada

The Subscription System

The Enterprise Applications & Integration Section from the Department of IT (DoIT) at UAEU has successfully launched the subscription system in 2018, in line with UAE vision 2021 that foresees high quality of life built on world-class public digital services.

This online solution is developed to fully automate the registration, activation, subscription, online payment, approvial and management processes. The integration with the ePayment system equips customers with a flexible range of payment options. In addition, it sends automatic emails to the payer, tracks failed payments and generates reports for providers to track their revenues.

The Subscription System interface was designed according to the modern interface design standards. It is user-friendly, bilingual, responsive and offers various role-based access depending on the user role (Super admin, admin, group admin, subscriber, approver, and the viewer). Moreover, this solution has plenty of supporting features for people with special needs; for example, increasing and decreasing font size, contrast and screen reader.

The system was built to improve customer service and supports a wide range of subscription types from journals to clubs, conferences, and others. The subscription portal provides customers with such self-service capabilities including subscription management and renewal, and editing personal information. Subscription providers are able to create different pricing structures, configure plans, and manage both subscriptions and subscribers' accounts.

Currently, the College of Law is utilizing this system for SL Journal subscription. They offer different types of subscription plans (individual, groups, hardcopy, and softcopy). Group subscribers have the power to maintain their group accounts. In addition, softcopy journal subscription allows users to browse easily SL journal issues online in the management system.

This Subscription system is capable of launching new services without writing extra code. It has been designed in a way that fits most possible scenarios and is capable to handle thousands of subscriptions. Migrating the manual subscription processes to the Subscription system will reduce complexities and billing operations.

Author : Safea Matar Ali Al Senani

ePayment v2.0

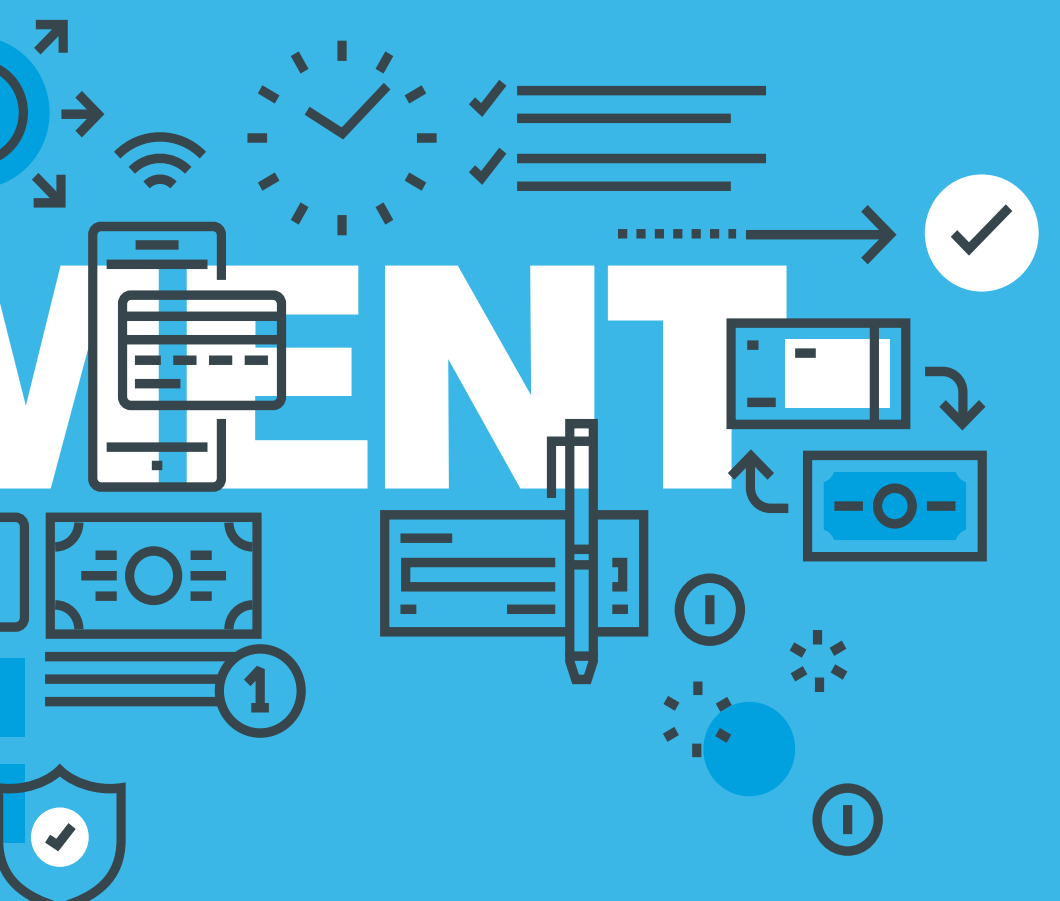
ePayment is an application that facilitates the delivery of services across other applications. Any UAEU application that requires payment is configured in the ePayment system, for example:

- **Student ePayment allows students to pay for tuition and housing.**
- **Admission allows applicants to pay for application fees.**
- **eProcurement allows vendors to pay for registration and tendering documents.**

On 25 April 2018, ePayment v2.0 was released, thus enhancing the User Interface (UI), adding new features and fixing issues. The application has been revamped with a new UI that improves user experience. For example, the Finance Operations department has been provided with better views of the payment transactions performed through the system, which in turn, allows better follow-up. In addition, the system is enabled with notifications to deliver the payment receipt via email.

ePayment v2.0 covered two major required changes related to VAT collection and shipment fees processing for some services like student eDocuments, Alumni eDocuments. Also, the application integration with Banner Finance has been enhanced to reflect the revenue generation in a more effective way. This allows Finance Operation Section to spend less time reviewing and reconciling transactions.

Author: Mariam Al Ketbi



UAEU Software Portal

UAEU Software Portal

Before implementing Citrix Application & desktop solutions, it was a struggle to maintain educational software across computer labs and students' laptops, and to manage the day-to-day software and hardware changes. Additionally, the university had a number of aging desktop machines in the Labs that could no longer adequately handle the latest software. Furthermore, the demand for various college-related student and faculty applications is increasing sharply.

With Citrix® XenApp™ technology, applications are being delivered virtually over the UAEU campus to any device, consistently and efficiently. The UAEU community can use heavy applications like Matlab, Minitab, Adobe Suite and many more without having to install them on personal computers or to struggle with device compatibility limitations.

Features & benefits

- With Citrix licensing feature, multiple users are sharing the same application simultaneously, without the hassle of managing individual user licenses.
- Ease of access from any device, anywhere.
- With few clicks, Windows 10 available on IOS & Android
- Reduction in hardware costs and application licenses.
- Application delivery & desktop deployment provide strong data governance techniques.
- An easy-to-manage platform, with applications and desktops rolled out across the campus very quickly.
- Highly efficient IT operations.

Authors: Farrukh Fayyaz & Thanseer Ahammed

To Experience the service,
visit : store.uaeu.ac.ae

Social Engineering

What is Social Engineering?

Social Engineering is a term originally connected to social sciences, but it has now found applications in the field of computer and information security. It is a type of non-technical attacks, where it is not necessary to compromise a system or software. Unlike with other technical attacks, social engineers rely on human interactions to fool users. They can reach their goals by infecting their victim's computer with malware, manipulating them into disclosing their confidential data, or tricking them to open infected sites using a URL link. As a result, legitimate and authorized access to confidential information can be given to the attacker.

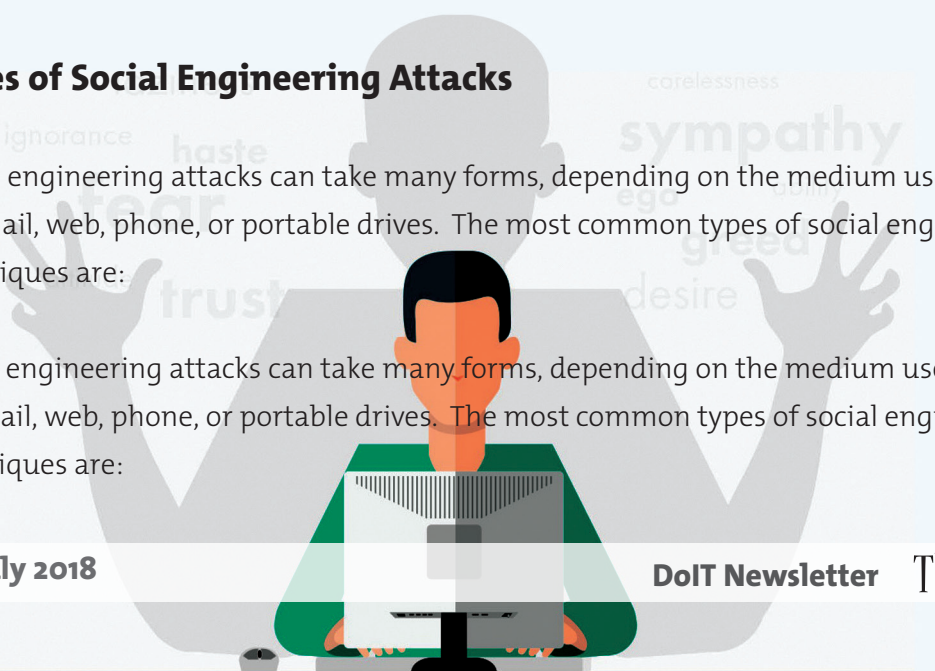
Social Engineering attacks are much easier to implement than you think

Social engineering criminals use many ways to launch an attack, be it on a building or a computer system. Either way, they rely primarily on the human tendency to trust. For example, an attacker may get access to a secure building just by asking someone to ket him in. On te other hand, he can pretend to be a co-worker and have an urgent need to gain access to network resources to solve it, or just fool a victim to give him the password rather than try to hack his machine. These two examples show clearly that the human element is the weakest link in the security chain.

Types of Social Engineering Attacks

Social engineering attacks can take many forms, depending on the medium used such as email, web, phone, or portable drives. The most common types of social engineering techniques are:

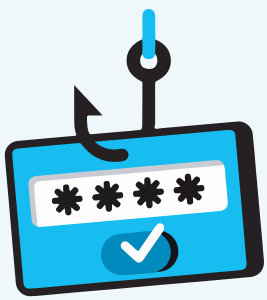
Social engineering attacks can take many forms, depending on the medium used such as email, web, phone, or portable drives. The most common types of social engineering techniques are:



» **Phishing**

Phishing is the most popular type of social engineering activity. It is a fraudulent attempt at acquiring a victim's sensitive information such as passwords, credit card details, etc. by pretending to be a legitimate and trusted company or institution in an electronic message. In most cases, this attack can be launched via email; however, it is also possible to get exposed through chat applications, phone calls, social media or spoofed websites.

Spear phishing is basically the same as phishing, except that it targets a specific victim or organization that is more likely to be tricked into revealing confidential information. The attacker tries to use specific victim's personal information to gain trust and appear as a legitimate user. This information can be gathered from online activities related to the victim, or his social accounts. If the attack succeeds, the attacker will gain the access and victim's sensitive data will be compromised.



» **Spear Phishing**

» **Baiting**

As its name sake, baiting involves luring a victim with something they desire. A good example is an infected flash drive with inscriptions like "Confidential", "My music" or the like. The victim is enticed to take the flash drive and unknowingly install the malware in his own device, thus giving access to the attacker.

Pretexting is, in essence, the practice of creating a plausible enough scenario that makes a victim feel comfortable to reveal confidential information, usually over the phone. Sometimes, impersonation is also involved. The more credible the impersonation or the scenario is, the more willing to provide sensitive information the victim is.

» **Pretexting**

Protection Against Social Engineering

Updating security network and preventing data theft - anti-virus software, firewalls, and email and spam filters - is no doubt important. However, focus should be on the human element when it comes to social engineering. Education of your staff, teachers, students, etc. is your first line of defence against social engineering attacks. Organisations should increase security awareness among all employees by providing comprehensive training programs so that they are not tricked into revealing sensitive information.

Below are some tips that would help protect against attacks:

1. For any unrequested email you receive, make sure it came from a trusted source, even if it is from what looks like a trusted company you deal with. For example, you could check their phone number.
2. Before you click on that link or open/download attachment, make sure it is safe even if it comes from a sender you trust because it could be a Trojan. Call the phone number and ask about the attachment.
3. Never reply to unsolicited email messages with confidential or financial information. Remember legitimate organisations and companies do not contact you to provide help unless you request it.
4. Write policies or review existing ones related to outgoing transactions and make sure they are followed.

Security experts recommend the implement of social engineering penetration tests to help administrators identify assets most-at-risk and types of attacks. This would help provide focused security training to specific employees.

Author: Mariam Al Mahrooqi


MESSENGER
CYBER SECURITY
Login Problem,
Wrong username or password
Report
Close

The Legal Aspects of Electronic Signature in UAE

Electronic signatures provide businesses and individuals involved in online transactions with an effective mechanism for ascertaining their identity. They also ensure authenticity and integrity of the electronic message, much like hand-written signatures, that is, to confirm that the message has not been altered since it was signed. All electronic signatures are represented digitally. They may be created by a number of technologies and be of different types such as a digitized fingerprint, a pin number, a retinal scan, or a digitized image of a handwritten signature attached to an electronic message, or even a name typed at the end of an e-mail. Perhaps the most sophisticated type of e-signature is the "digital signature", which is created through the use of public key cryptography.

In the UAE, the use and admissibility of electronic signatures is governed by Federal Law No.1 of 2006 regarding Electronic Transactions and E-Commerce. This law defines electronic signature in Article (1) as "any letters, numbers, symbols, voice or processing system in Electronic form applied to, incorporated in, or logically associated with a Data Message with the intention of authenticating or approving the same". Article (17) states that an electronic signature shall be treated as a Secure Electronic Signature if, through the application of prescribed secure

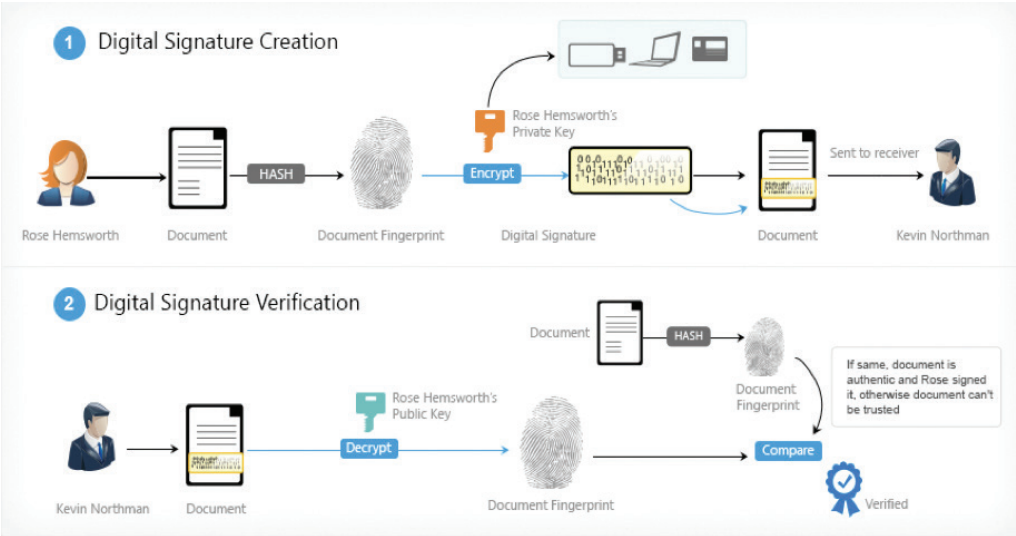
authentication procedures or commercially acceptable authentication procedures agreed upon by the parties involved, it meets the following requirements:

1. It is uniquely linked to the signatory and to no other person;
2. It is capable of identifying its owner;
3. It is created using means of its owner and under his sole control; and
4. It is linked to the record to which it relates in such a manner that does not allow modification to that record after signing without altering the signature so that any change made after the time of signing is detectable.

In addition, Article (18) allows the parties to rely on an electronic signature or electronic authentication certificate to the extent that such reliance is reasonable. It also provides that the relying party in respect of such signature shall bear the legal consequences of its failure to take reasonable and necessary steps to verify the validity and enforceability of the certificate, as to whether it is suspended or revoked, and of observing any limitations with respect to the certificate.

It should be noted here that the Electronic Transactions and E-Commerce law and all subsequent regulations, regulatory policies, and legal instruments in UAE are intended to be technologically neutral, hence the omission of a specific technology for secure electronic signatures.

Later, the UAE Federal Law No. 36 of 2006 amended certain provisions of the Evidence Law in Civil and Commercial Transactions issued by Federal Law No. 10 of 1992. According to this Law, both electronic signatures, and electronic writing, instruments and documents shall have the same evidential weight as written signatures, and official and customary writing and instruments respectively if they comply with the provisions prescribed in the Federal Law No. (1) of 2006 concerning Electronic Transactions.

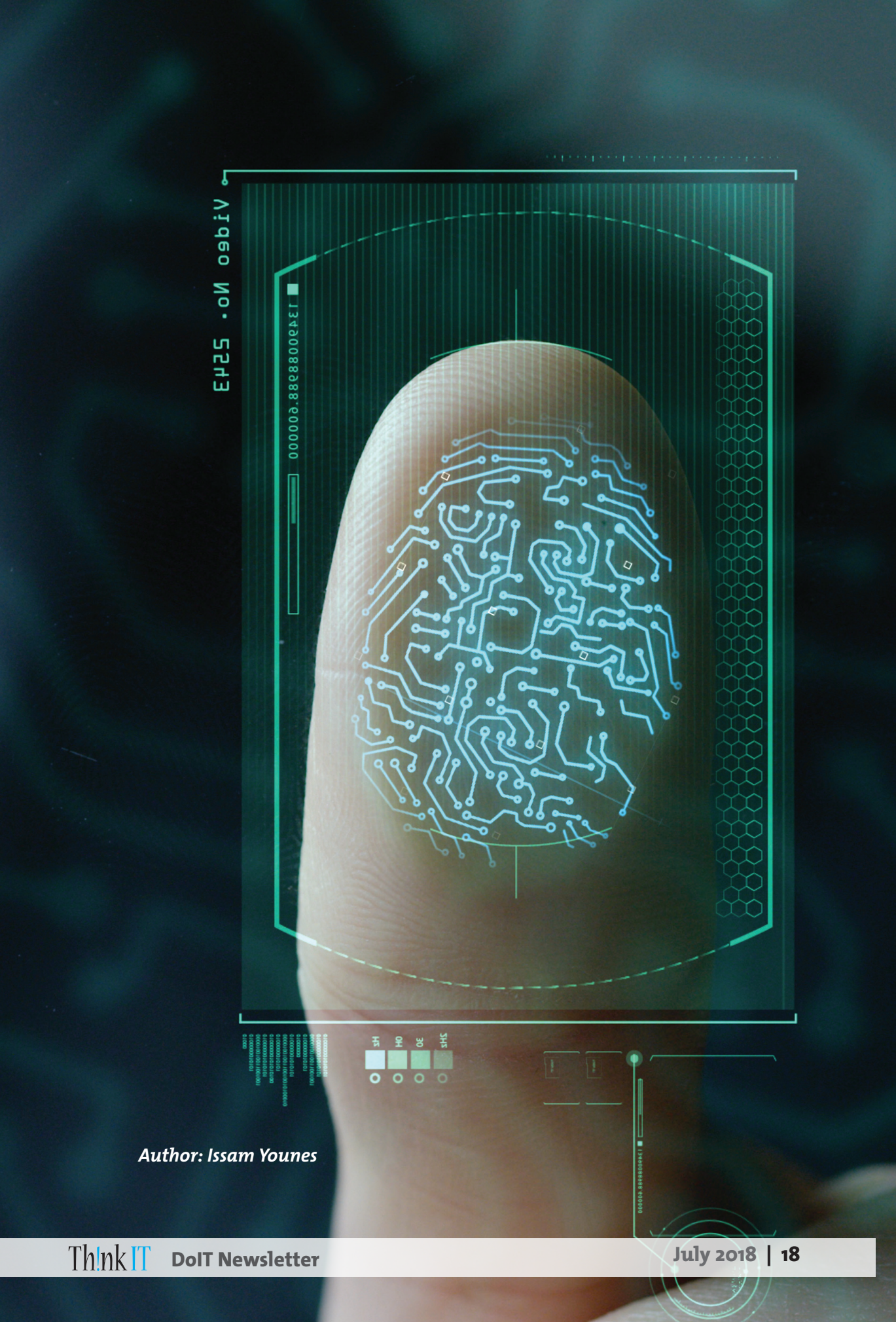


Conclusion

Electronic signatures make business transactions over the Internet easier and more reliable for both businesses and consumers. The UAE law has authorized the use of electronic signatures and electronic records to create binding agreements and made it clear that no electronic signature can be refused legal effect merely on the grounds that it is in electronic form. It has also declared the functional equivalence of the electronic with the hand-written signature as a generic matter together with its admissibility as a measure of proof. There are, however, specific categories of transactions and documents for which electronic signatures may not be used. These include transactions pertaining to personal law such as marriage, divorce and wills, as well as deeds of title to immovable property, and negotiable instruments.

Emad Dahiyat, The Legal Recognition of Electronic Signatures in Jordan: Some Remarks on the Electronic Transactions Law, Arab Law Quarterly 25 (2011), p. 298.

For more information, see Thomas J. Smedinghoff & Ruth Hill Bro, 'Moving with change: Electronic signature legislation as a vehicle for advancing e-commerce', 17 J. Marshall J. Computer & Info. L. (1999) 723, p. 730.



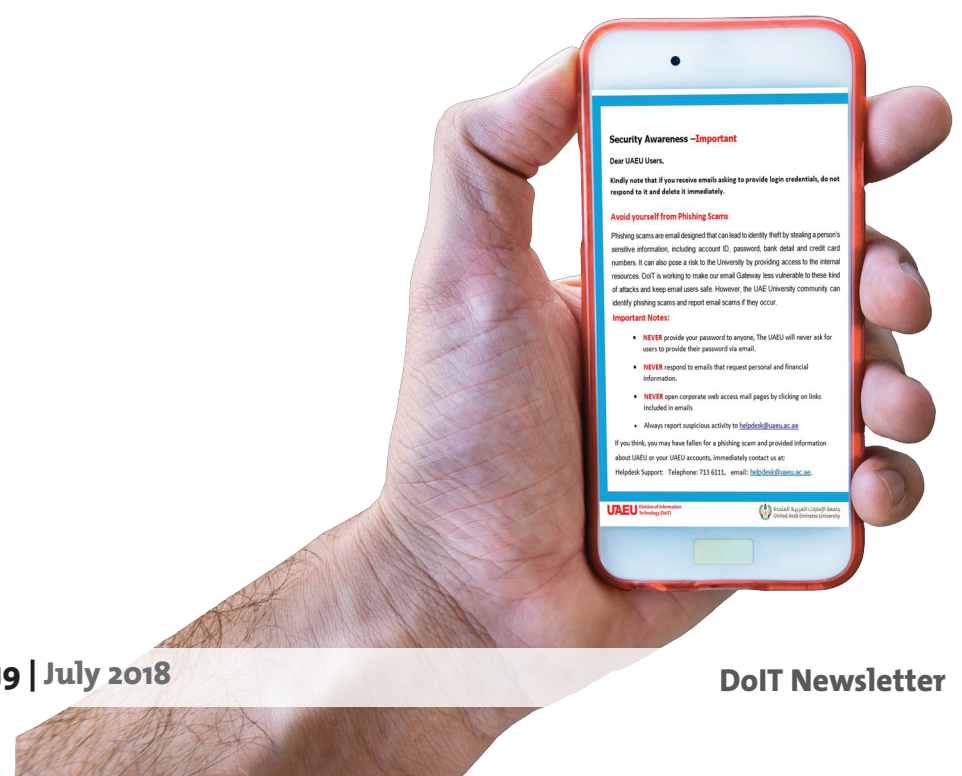
Author: Issam Younes

Security Awareness

Information security is the practice of protecting information, particularly in its electronic form, from unauthorised access, use, disclosure, disruption, modification or destruction.

"Security is the responsibility of everyone" is a widely used phrase in information technology these days, which reflects both the huge growth of information technology and the risks associated with it. Thus, the importance of Confidentiality, Integrity, and Authenticity (CIA) of information is now emphasized by both the public and private sectors.

Awareness of the threats that may jeopardise CIA is therefore paramount, as the European Network and Information Security Agency points out, 'Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks.'
By 2020, there will be approximately 200 billion connected devices, which shows the size of the industry and its importance towards overall growth. Importantly, research suggests that almost 43% security breaches happen internally, hence the importance of security awareness. Users play a key role in the prevention of information security breaches targeting them and their organisations.



Indeed, as a requirement of ISO 27001 (SMS) certification, UAEU is already conducting security awareness sessions on a regular basis. Also, given the exponential increase in the number of malware, 230,000 new samples daily in March 2018 according to Cybint News, the Department of Information Technology (DoIT) at UAE University is taking serious steps towards security awareness on the internal front, i.e. targeting its users (Faculty, Staff, and Students).

These steps include email broadcast, posters and training sessions, which lead to better security for IT infrastructure. Major topics covered in regular security awareness training sessions are Password Protection, Tailgating, Secure Use of the Internet, Secure Use of Email, and Read, Understand and Adhere to UAEU InfoSec Policies.
DoIT also ensure major IT policies and procedures of are available online at (https://www.uaeu.ac.ae/en/about/policies/). Below, we have a few examples of security awareness content which we normally communicate to users.

Author: Asad Mukhtar Malik

Data Reduction-Deduplication and Compression

Data growth is the biggest data center hardware infrastructure challenge for large enterprises; Capacity-optimization technologies play a critical role in today's environment where companies need to increase storage efficiency and reduce costs – To do more with less .

Data Reduction is the process of minimizing the amount of data that needs to be stored in a data storage environment which can be achieved using several different types of technologies. The best-known data reduction technique is Deduplication and Compression.

Deduplication is the process of identifying duplicate data contained within a set of block storage objects and consolidating it such that only one actual copy of the data is used by many sources. This feature can result in significant space savings depending on the nature of the data. It can be done at source, inline or post-process. For example, suppose the same 10 MB PowerPoint presentation is stored in 10 folders for each sales associate or department. That's 100 MB of disk space consumed to maintain the same 10 MB file. File deduplication ensures that only one complete copy is saved to disk. Subsequent iterations of the file are only saved as references that point to the saved copy, so end-users still see their own files in place. Similarly, a storage system may retain 200 e-mails, each with a 1 MB attachment. With deduplication, the 200 MB needed to store each 1 MB attachment is reduced to just 1 MB for one iteration of the file .

Compression is the process of reducing data to use less capacity than the original format. Compression basically attempts to reduce the size of a file by removing redundant data within the file. By making files smaller, less disk space is consumed, and more files can be stored on disk. For example, a 100 KB text file might be compressed to 52 KB by removing extra spaces or replacing long character strings with short representations. An algorithm recreates the original data when the file is read. For example, a 2:1 compression ratio can ideally allow 400 GB worth of files on a 200 GB disk (or 200 GB worth of files would only take 100 GB on the disk). It's very difficult to determine exactly how much a file can be compressed until a compression algorithm is applied.

References:

https://en.wikipedia.org/wiki/Data_deduplication

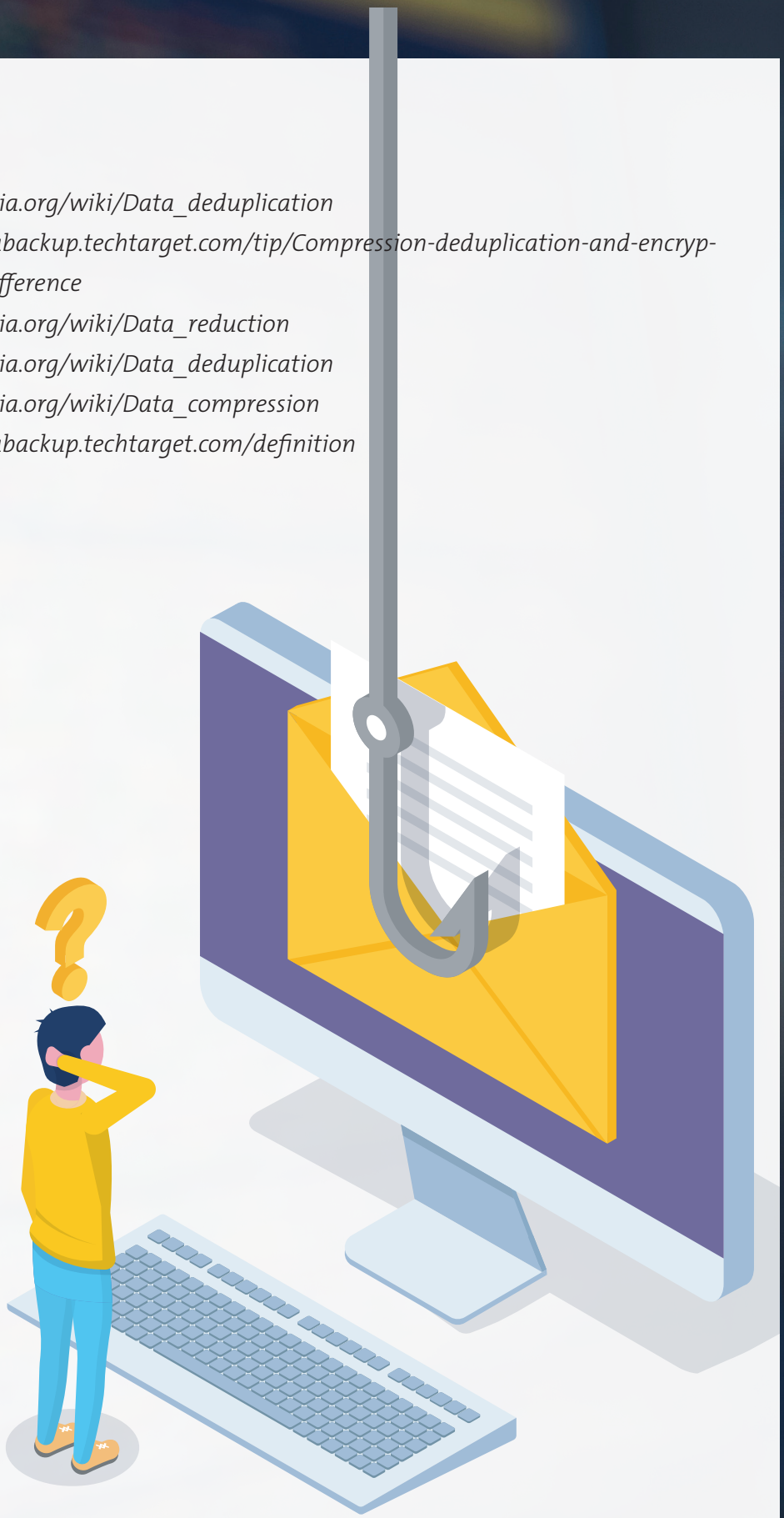
https://searchdatabackup.techtarget.com/tip/Compression-deduplication-and-encryption-Whats-the-difference

https://en.wikipedia.org/wiki/Data_reduction

https://en.wikipedia.org/wiki/Data_deduplication

https://en.wikipedia.org/wiki/Data_compression

https://searchdatabackup.techtarget.com/definition



Two Factor Authentication (2FA)

What is 2FA?

To provide added protection to University data, UAEU employs 2-factor or "multi-factor" authentication. In addition to using their username and password (first factor of authentication), under certain circumstances, users must also authenticate using a phone (second factor of authentication). The advantage of adding a second factor of authentication is that in the event that a user's credentials (username/password) are compromised, that alone will be insufficient for someone to gain access to sensitive university data. They would also need to gain possession of the users' phone in order to make use of the compromised credentials. DoIT uses F5 Networks and Etisalat SMS services to provide this second factor of authentication and increase the protection of UAEU data.

Factors of Authentication

» **Something you know**
- Username and password/passphrase
- Pin
- Security question

» **Something you have**
- A device such as a phone, token, security badge, etc

Author: Sajid Ali


User name
Sign in
Bank name
Bank name
0123 4567 8901 2345

UAEU Infrastructure upgrade – Phase 4

UAEU upgraded its data center and crescent building in the first two phases of infrastructure upgrade and later upgrade highly populated C-series Building continuing UAE University's promise to deliver ubiquitous, high bandwidth connectivity throughout the campus. As per university's plan to continue with the upgrades in phases keeping in view the advancement in networking technology and the introduction of features such as internet of things (IoT), 4th generation access protocols, cloud applications as well as bandwidth hungry gaming application such as Poke'mon go, all remaining buildings comprising E-series and F-series, G-seres and H-series were upgraded constituting phase-4 of the upgrade project. This upgrade enables the infrastructure to meet the exorbitant bandwidth demands and to satisfy the requirement for ever-present internet connectivity providing a switching backhaul of 40 Gbps, highly resilient, non-blocking state-of-the-art infrastructure. The upshot of this change would be a higher bandwidth for the end user by reducing the bandwidth contention ratio and oversubscription on the uplink.

Figure 1: Cisco Catalyst 9500 series

For the campus, Catalyst 9500 40 Gbps switch form the distribution layer while the Multi-Gigabit Catalyst-3850 constitutes the access layer. The Cisco Catalyst 9500 Series is the first 100/40-Gbps switch purpose-built for the enterprise campus. It was recently recognized as CRN's 2017 Overall Network Product of the Year. Designed for security, the Internet of Things (IoT), and the cloud, Catalyst 9500 fixed-core switches are high-density building blocks for a next-generation, intent-based network.

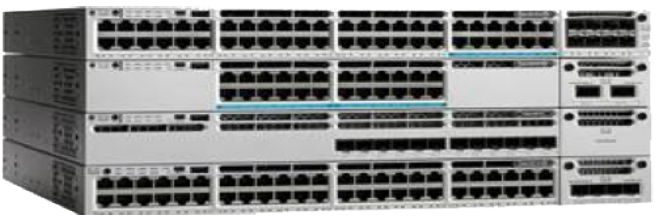
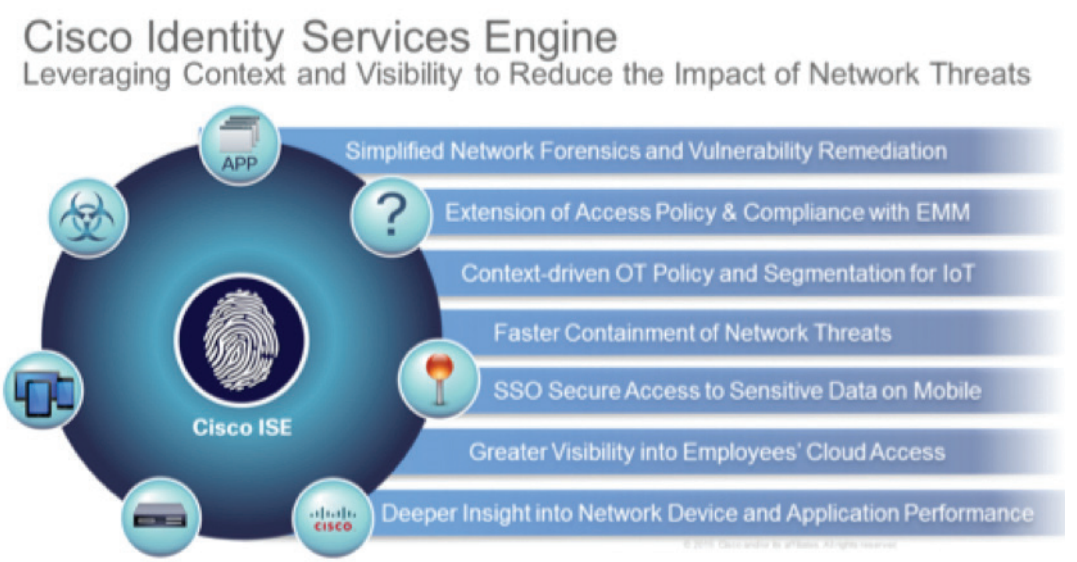


Figure 2: Cisco Multigig 3850 Series

UAE University has also added Cisco ISE integration as part of phase 4 to secure the infrastructure, which helps reliably enforce compliance, enhance infrastructure security, and streamline service operations. Cisco ISE is a context-aware, identity-based platform that gathers real-time information from the network, users, and devices. System-wide visibility showing you who and what is on the network - wired, wireless, or VPN. Integrated AAA, profiling, posture, and guest services to simplify deployments and cut costs. Accurate device identification using ISE-based probes, embedded device sensors, active endpoint scanning. Cisco ISE also provides simplified BYOD onboarding through self-service registration.



References:

Cisco Catalyst 9500 Series Switches Data Sheet
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/data_sheet-c78-738978.html

Cisco Catalyst 3850 Series Switches Data Sheet
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/datasheet_c78-720918.html

Author: Salman Sadiq

Authors

Ahmed Talal , Alsajir M Basheer, Amna Khamis Saif Alhassani , Asad Mukhtar Malik Mukhtar Amin, Awatef Alshamsi , Eiman Rashed Al Manei , Luke D'Silva , Mohammad Awad Toma Makadmeh, Nithin Damodaran,Saeed Alloghani, Sajid Ali, Salman Sadiq Muhammad Sadiq, Shaikha Hareb Al Neyadi

Editors

Omar Hachimi, Naeema Al Nuaimi

Design & Layout

Sharan Ramalingam

Newsletter & Publisher

Think IT is published for UAEU Community by
Division of Information Technology (DoIT)

You can send your feedback or suggestions via

Email : thinkit@uaeu.ac.ae
Tel: 7136111 3 971+ | Fax: 7136999 3 971+