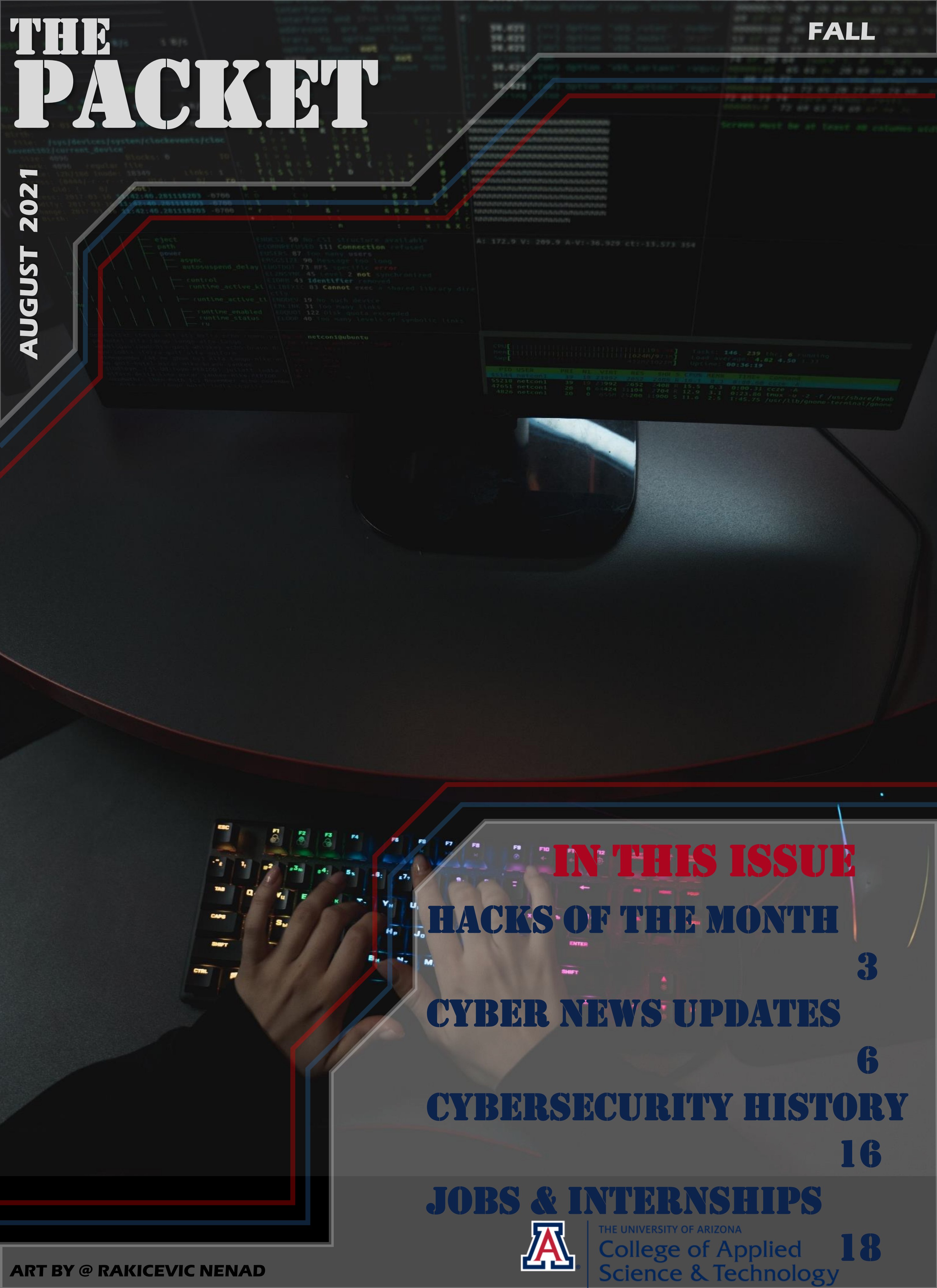


THE PACKET

FALL

AUGUST 2021

IN THIS ISSUE

THE UNIVERSITY OF ARIZONA
College of Applied Science & Technology

ART BY @ RAKICEVIC NENAD

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- **BEGIN MESSAGE** ---

Welcome to the **AUGUST** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I welcome all of you to the Fall semester which starts at the end of this month. It feels like Summer just flew by and the month of July was a very busy month. First off, this is the month of DEFCON, and it will take place between the 5th and 8th of August. I am excited for this and depending when this edition comes out, I will be in Vegas with every other hacker who decided to make this annual pilgrimage. This year will again be a little different compared to previous years due to COVID-19 restrictions still in place, but talks will still be taking place. There is a virtual ceremony taking place as well so please take advantage when you can. The amount of research presented in these few days is exciting and can also be confusing if you don't know where to look. With so many presentations, villages, workshops and events its hard to know how to make the most of it. It is always a good idea to network and build a DEFCON engagement plan. If you get a chance to attend a SKYtalk, I highly recommend those as they are not recorded and go into more detail on topics you won't find in an academic paper due to industry restrictions or sometimes questionable legalities. This year however they will not be taking place, but they are my favorite type of talks. The fall semester will be staring up this month as well and I am excited to see everyone who will be taking any of my classes. I hope you all had an amazing summer, and I will see you when classes start up here soon!

--- END MESSAGE ---

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

HACKERS REPORTED TO TARGET IRAN TRANSIT WEBSITES

Websites of Iran's transport and urbanization ministry Saturday went out of service after a "Cyber disruption" in computer systems of its staff, the official IRNA news agency reported. On Friday, Iran's railroad system came under cyberattack, a semiofficial news agency reported, with hackers posting fake messages about train delays or cancellations on display boards at stations across the country. The semiofficial Fars news agency reported that the hack led to "Unprecedented chaos" at rail stations. Earlier in the day, Fars said trains across Iran had lost their electronic tracking system. The announcement was made after the electronic tracking system on trains across Iran failed. It was not clear if the reported attack caused any damage or disruptions in Iran's computer and internet systems, and whether it was the latest chapter in the U.S. and Iran's cyber operations targeting the other. Iran disconnected much of its infrastructure from the internet after the Stuxnet computer virus - widely believed to be a joint U.S.-Israeli creation - disrupted thousands of Iranian centrifuges in the country's nuclear sites in the late 2000s.

SUSPECTED CHINESE HACKERS TARGET TELECOMS, RESEARCH IN TAIWAN

Researchers noticed intrusions from the group, which investigators called TAG-22, in June targeting telecommunications organizations including the Industrial Technology Research Institute in Taiwan, Nepal Telecom and the Department of Information and Communications Technology in the Philippines. The new findings play into a larger backdrop of apparent Chinese hackers snooping on global competition in the telecommunications space, which has become an arena of political and economic conflict between China and the United States. "In particular, the targeting of the ITRI is notable due to its role as a technology research and development institution that has set up and incubated multiple Taiwanese technology firms," researchers wrote. "In recent years, Chinese groups have targeted multiple organizations across Taiwan's semiconductor industry to obtain source code, software development kits, and chip designs," researchers added. The telecommunication sector was among the sectors most targeted by Chinese hackers in the first half of 2020, according to a report from CrowdStrike last year. Outside of the telecommunication industry, the threat group has targeted academia, research and development, and government organizations in Nepal, the Philippines, Taiwan and less recently Hong Kong. The threat group appears to use backdoors used by other Chinese state-sponsored groups, including Winnti Group and ShadowPad. It also employs open-source security tools like Cobalt Strike.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

MARYLAND TOWN KNOCKED OFFLINE AS PART OF MASSIVE RANSOMWARE ATTACK

A Maryland town network was taken offline during a massive ransomware attack through Miami-based technology firm Kaseya. The Washington Post reported Thursday that Leonardtown in Southern Maryland fell victim to the cyberattack, and town administrator first learning of the problem when they logged in. The town's IT management company JustTech is a client of Kaseya's and uses products that had been affected by the hack, the Post reported. The WashingtonPost learned that the city of Leonardtown had been informed by JustTech that the ransomware gang REvil was demanding $45,000 per computer, and also learned that the town's government never seriously considered paying. All but two of the town's 19 computers were affected - a computer used by an employee who was on vacation was unaffected, along with an older computer that had been left at an employee's home. JustTech has said it will be able to restore the town's system, the Post reported, but it is unclear how long this will take as the IT company itself was impacted by the breach. The Dutch Institute for Vulnerability Disclosure revealed this week that it had detected multiple vulnerabilities in Kaseya's system earlier in April, with one of the vulnerabilities ultimately being exploited by the hackers.

CODE EXECUTION VULNERABILITY DISCOVERED IN SCHNEIDER ELECTRIC MODICON PLCS

A vulnerability discovered in Schneider Electric Modicon programmable logic controllers (PLC’s) allows full takeover of the industrial chips. Discovered by Armis researchers, the vulnerability can be used to bypass existing security mechanisms in PLCs to hijack the devices and potentially impact wider industrial setups. Without authorization, it is possible for attackers to abuse undocumented commands and obtain full control over one of these chips, overwriting memory, leaking a hash required to take over secure connections, and executing code - which, in turn, can impact the security of workstations that manage the PLCs. SE Modicon PLCs are used to control Industrial Internet of Things devices in the construction, energy, machinery, and utility sectors, among others. Armis says that to trigger an attack, only network access is required to the target PLC. Armis says there are inherent security issues in Modbus, an industry-standard protocol - and as SE's proprietary UMAS is based on the protocol, PLCs linked to UMAS may be beset by known, weak encryption and authentication mechanisms in the original Modbus standard. "SE has stated in the past its intent to adopt the Modbus Security protocol that offers encryption and authentication mechanisms that are not part of the classic Modbus protocol," Armis says. "Due to inherent shortcomings of the Modbus protocol that powers SE's Unified Messaging Application Services protocol used by Modicon PLCs, Armis will continue working with SE and additional vendors to address these issues," the company says. In 2018, a zero-day vulnerability was exploited in SE Triconex controllers by attackers attempting to disrupt industrial operations in the Middle East.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

FASHION RETAILER GUESS DISCLOSES DATA BREACH AFTER RANSOMWARE ATTACK

American fashion brand and retailer Guess is notifying affected customers of a data breach following a February ransomware attack that led to data theft. "A cybersecurity forensic firm was engaged to assist with the investigation and identified unauthorized access to Guess' systems between February 2, 2021, and February 23, 2021," the company said in breach notification letters mailed to impacted customers. Guess began mailing breach notification letters to affected customers on June 9, offering complimentary identity theft protection services and one year of free credit monitoring through Experian to all impacted individuals. "On May 26, 2021, the investigation determined that personal information related to certain individuals may have been accessed or acquired by an unauthorized actor," Guess said. While the breach notification letters do not reveal the number of affected individuals, information filed with the office of Maine's Attorney General shows that just over 1,300 people had their data exposed or accessed during the February attack. Guess has implemented additional measures to boost its security protocols and is cooperating with law enforcement as part of an ongoing incident investigation. Even though Guess did not provide any info on the identity of the threat actor behind the ransomware attack, DataBreaches.net reported in April that the DarkSide ransomware gang listed Guess on their data leak site.

NEW EUROCONTROL DATA SHOWS AIRLINES INCREASINGLY BECOMING TARGETS FOR CYBER ATTACKS

The latest in a series of Think Papers, Eurocontrol used data collected from its European Air Traffic Management Computer Emergency Response Team, which reported a 530 percent increase in the number of cyber-attacks that were reported to or identified by the team between 2019 and 2020. None of the cyber attack methods or attempts reported by (EATM-CERT) were directly against safety-critical aircraft systems or passenger mobile devices connected to in-flight internet. EATM-CERT's report notes its system identified or received reports on a total of 775 cyber-attacks on airlines over the course of 2020, a significantly higher number than the next two aviation sectors combined, just over 200 for aviation OEMs and 150 for airports. Aviation manufacturers are highlighted in the report as being the most targeted for data theft, with 122 of the 206 total reported cyber-attacks against them coming in the form of cybercriminals seeking to monetize their intellectual property. The new report also highlights some of the attacks that were successful against high-profile companies, including a successful one against EasyJet that the U.K.-based low-cost carrier reported in May 2020. More recently, in March, well-known aviation IT supplier SITA reported that it was the victim of a cyber-attack leading involving certain passenger data that was stored on SITA's airline passenger service system servers. A March 2021 ransomware attack against Spirit Airlines that the U.S.-based carrier still has not acknowledged is also highlighted by EATM-CERT. "Every week, an aviation actor suffers a ransomware attack somewhere in the world, with big impacts on productivity and business continuity, let alone data loss and/or costly extortion demands paid in order to restart operations," the EATM-CERT team writes in the report.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

BIDEN WARNS PUTIN ON RUSSIAN RANSOMWARE ATTACKS

President Biden spoke by phone with Russian President on Friday, July 9th and urged him to take action to disrupt criminal groups operating in Russia that are behind recent ransomware attacks in the United States. The conversation came after a ransomware attack last week on software company Kaseya impacted up to 1,500 companies, many of which were vulnerable small businesses U.S. Cybersecurity experts have attributed the attack to the Russian-based "REvil" cyber criminal group. The White House press secretary told reporters at a press briefing Friday that the U.S. government does not have new information suggesting the Russian government directed recent ransomware attacks but said, "We also know, and we also believe that they have a responsibility to take action." During the meeting, Biden gave Putin a list of 16 critical infrastructure entities that Russia could not attack without consequences and warned him against allowing further malicious cyber activities against the United States. "President Biden also spoke with President Putin about the ongoing ransomware attacks by criminals based in Russia that have impacted the United States and other countries around the world," the White House readout of Friday's conversation between the two leaders said. "President Biden underscored the need for Russia to take action to disrupt ransomware groups operating in Russia and emphasized that he is committed to continued engagement on the broader threat posed by ransomware."

Debilitating ransomware attacks in May on Colonial Pipeline, which supplies 45 percent of the East Coast's fuel supply, and on JBS USA, the nation's largest beef provider, were attributed by the FBI to two separate Russian-based cyber criminal groups.

DEFENSE DEPARTMENT INCREASING MOBILE DEVICE SECURITY

To better protect mobile devices that warfighters use, the Pentagon's Defense Innovation Unit is readying a mobile threat application that analyzes and looks for problems on Defense Department-issued devices and shares findings in the cloud. "DOD must protect mobile devices from attacks such as phishing, malicious risky apps, operating system exploitation and network attacks," Rick Simon, cyber portfolio program manager at DIU, wrote in an email response to GCN's questions. The department recognizes that warfighters' mobile endpoints face the same threats consumers' devices do, but the loss of confidential information and credentials at DOD could lead to a national security issue, Simon said. Zimperium's app gets pushed to the devices and checks what networks they're connecting to, what apps are being downloaded and the security of links users click on.

SOLARWINDS ISSUES HOTFIX FOR ZERO-DAY FLAW UNDER ACTIVE ATTACK

SolarWinds has issued a hotfix for a zero-day remote code execution vulnerability already under active, yet limited, attack on some of the company's customers. Though the current threat appears to be from a sole actor and "Involves a limited, targeted set of customers," SolarWinds wanted to remedy the situation before it could escalate, the company said. SolarWinds does not currently know how many customers may be directly affected by the flaw, nor has it identified the ones who were targeted. SolarWinds likely still has fresh memories of a global supply-chain attack targeting the company's technology that was discovered late last year and stretched well into 2021. Specifically, attackers installed the Sunburst/Solorigate backdoor inside SolarWinds.Orion.Core.BusinessLayer.Dll, a SolarWinds digitally signed component of Orion. SolarWinds stressed in its advisory that the latest vulnerability is not related to that previous scenario - which cost the company $3.5 million in investigation and remediation expenses - in any way.

TRICKBOT ACTIVITY INCREASES; NEW VNC MODULE ON THE RADAR

Trickbot has been around since late 2016, when it appeared in the form of a banker and credential-stealing application. Drawing inspiration from Dyre (or Dyreza), Trickbot consists of an ecosystem of plugin modules and helper components. The Trickbot group, which has infected millions of computers worldwide, has recently played an active role in disseminating ransomware. Bitdefender's analysis team have been reporting on notable developments in Trickbot's lifecycle, with highlights including the analysis in 2020 of one of its modules used to brute force RDP connections and an analysis of its new C2 infrastructure in the wake of the massive crackdown in October 2020. Despite the takedown attempt, Trickbot is more active than ever. In May 2021, oBitdefender's systems started to pick up an updated version of the vncDll module that Trickbot uses against select high-profile targets. This module, known as tvncDll, is used for monitoring and intelligence gathering. It seems to be still under development, since the group has a frequent update schedule, regularly adding new functionalities and bug fixes. In addition to upgraded modules, Bitdefender has noted a significant increase in command-and-control centers deployed around the world. This new research focuses on an updated VNC module, which includes new functionalities for monitoring and intelligence gathering.

1/4

UNDERSTANDING CRYPTOGRAPHY

BY NAYLETH RAMIREZ

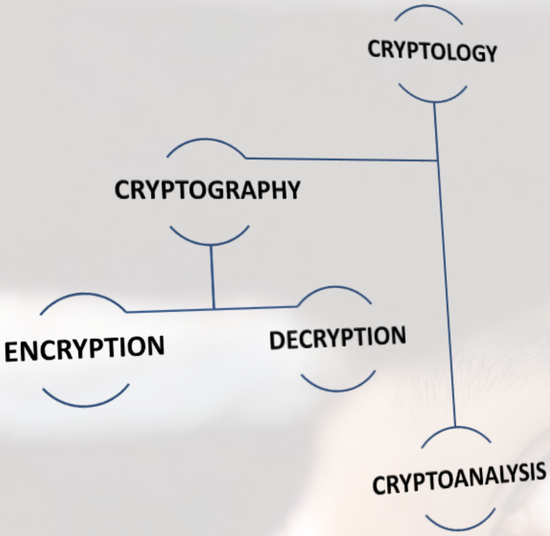
I decided to ask four friends to describe in two to three words what came to mind when they heard of the following terminology:
Cryptology, Cryptography, Encryption, and/or Decryption.
They responded with the following: clues, secrecy, important information, hidden, data, securing, locking, unlocking, and symbols. This was very eye-opening because even though none of them hold a cybersecurity background they were still able to associate the terminology to vocabulary that is easier to understand.
I personally became interested in cybersecurity after attending The Society of Hispanic Professional Engineering (SHPE) National Convention. During the convention I sat down in multiple seminars of distinct companies but became highly interested in the cybersecurity info session from Palo Alto Networks, it was then that my interest peaked and I quickly decided I wanted to get a minor in cybersecurity to become more aware of this fast-growing field. When I came from the convention, I wasted no time and soon scheduled a meeting with my advisor who helped me enroll in a few Systems Engineering courses with cyber focus and CYBV 301 and 385. After taking CYBV 385 with Professor Galde I became more interested in cryptography after having the opportunity to practice through the PGP assignment. For this assignment we used Mozilla Thunderbird which is an open-source cross-platform email client. Our task was to write and send an email to the professor using the End-to-End Encryption setting which allowed us to add a new OpenPGP key and digitally sign it, once he received our email, he would open it and import the public key, then respond back with an encrypted email that was digitally signed by him, once we (the students) received his email we needed to copy and submit the encrypted and decrypted message to ensure all information was correct and successfully sent and received. Now to better understand all this let us begin by learning the definitions, "cryptography is the science of secret writing" (CYBV385 Fundamentals of Cybersecurity Week 7 Slide 4).

2/4

UNDERSTANDING CRYPTOGRAPHY

BY NAYLETH RAMIREZ

Cryptography hides data against unauthorized access and encapsulates both encryption and decryption concepts. Encryption is the process of encoding a message so that the plain text is not easy to understand, by doing so the plain text becomes a cipher text. On the contrary, decryption is when the encrypted message (cipher text) is transformed back to the original legible text. To better understand the hierarchy of the terminology I created the following figure. Now of course with such complexity these cryptographic algorithms become highly infused with confusion and diffusion. The level of confusion depends on how complex you want it to be. If you think back to your childhood coloring books, these methods of encryption already existed, when you solved puzzles that consisted of symbols and needed to replace them with a different letter to create a word or phrase, that is an example of a substitution cipher. Presently, cryptography basics are the essence of cryptosystems; some examples consist of symmetric and asymmetric key cryptography and digital signatures just to name a few. Symmetric encryption uses a single key to both encrypt and decrypt the message. On the other hand, asymmetric encryption uses two different keys, one that is used to encrypt and the other to decrypt the messages. Digital signatures use a combination of public key encryption and hash algorithms to demonstrate authenticity by creating a digital signature on any digital document.



3/4

UNDERSTANDING CRYPTOGRAPHY

BY NAYLETH RAMIREZ

Key Management manages cryptographic keys within any cryptosystem. As the sensitivity of securing information increases, the actual lifetime of the encryption key will decrease. These keys have the ability of generating, storing, and exchanging keys to manage and save certain information that the user wishes to protect. Ensuring these key exchanges are secured from unauthorized parties is vital.

Logical security is meant to protect larger organizations from theft. In these cases, cryptographic keys can be used because they can encrypt data which decreases the ability for unauthorized users to decrypt that information. Personnel security is the act of assigning roles to specific people who with permission have special access to information / data.

Although these keys possess many benefits, with such complexity many challenges and problems might arise. Some of the primary problems associated with managing cryptography keys include correct use of procedure, frequent system updates before keys expire, dealing with proprietary information, keeping track of crypto updates with legacy organization systems and locating remote devices.

Vulnerabilities exist every time the sender sends information to the receiver. Some of the problems of securing can consist of inefficient processes. Exploitation might occur when the intruder tries different ways of accessing the information, for example they can block data. If they intercept it, this will allow the intruder to listen or read the message even before the receiver receives the message and can cause confidentiality issue. They can modify it, which would allow the message to be changed or manipulated. Finally, they can fabricate it which would create an authentic-looking message, that would then be arranged by the intruder to resend to the receiver. This encryption algorithm is based on some underlying problem of factoring large numbers in finite set called a field. The reason this is worldly used is because it can take up to years for the intruder to capture the correct keys. As of now, nobody has found an easier way to factor these large numbers in a field, making this cryptography

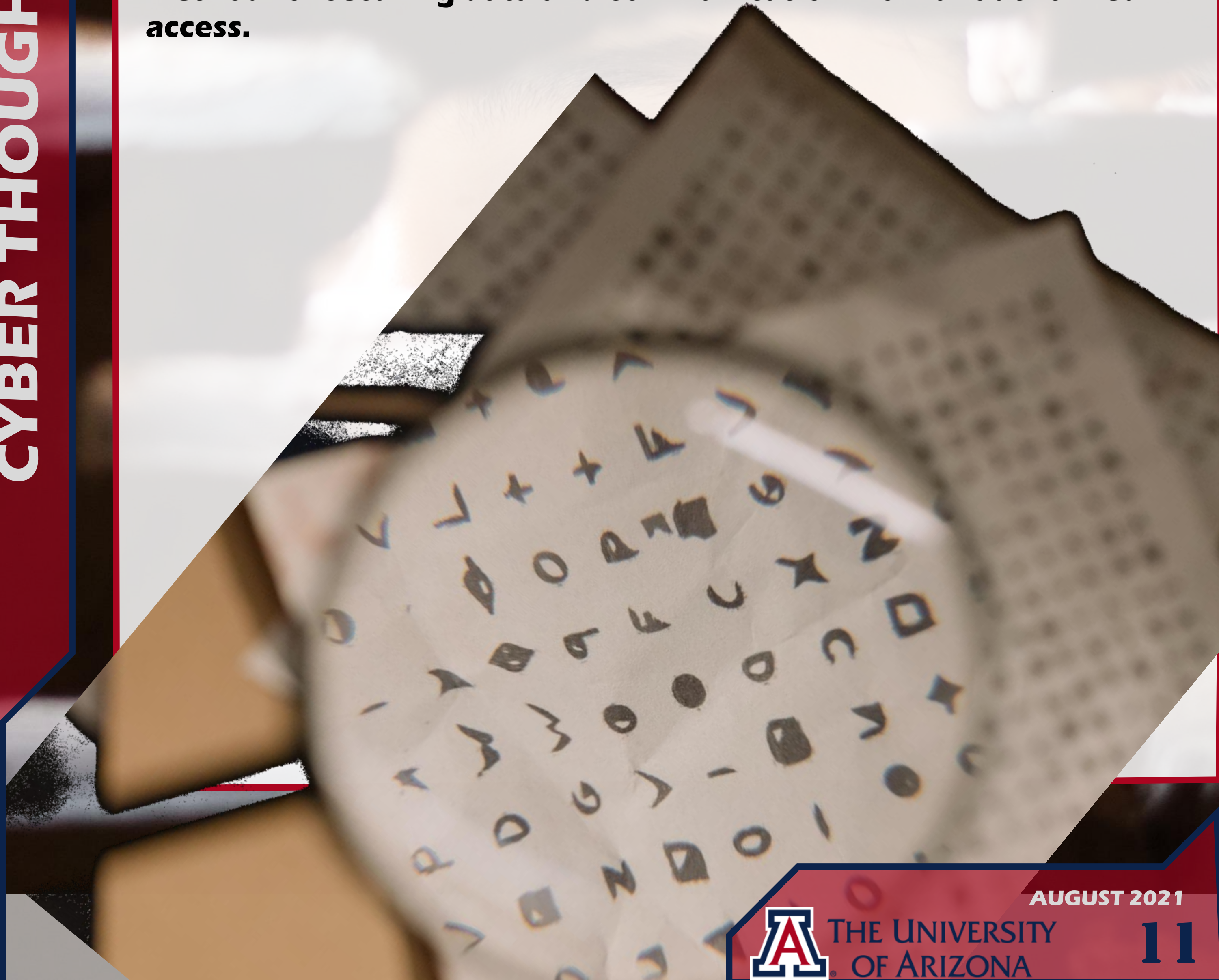
4/4

UNDERSTANDING CRYPTOGRAPHY

BY NAYLETH RAMIREZ

process very effective and secure. Dan Boneh, explains in a highly technical paper that all the known cryptanalytic attacks on RSA hold no significance, this is because the factorization problem has been open for many decades, most cryptographers consider this problem a solid basis for a secure cryptosystem.

IN CONCLUSION, as stated in Security in Computing 5th Edition, "Encryption or cryptography—the name means secret writing—is probably the strongest defense in the arsenal of computer security protection. Well-disguised data cannot easily be read, modified, or fabricated." (Pg. 114). Without a doubt cryptography is an important method for securing data and communication from unauthorized access.



SIGN UP FOR CLASSES SOON

NOTES FROM YOUR ADVISORS

FALL 2021 ENROLLMENT IS CURRENTLY OPEN. COURSES ARE FILLING QUICKLY! IF YOU HAVE NOT ENROLLED YET, DO SO ASAP! PLEASE TOUCH BASE WITH YOUR ACADEMIC ADVISOR TO VERIFY THE COURSES YOU PLAN ON TAKING ARE IN LINE WITH YOUR DEGREE PLAN. YOU CAN ALSO SCHEDULE AN APPOINTMENT WITH THEM IF YOU NEED ADDITIONAL SUPPORT WITH YOUR ENROLLMENT. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE: HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR

SIGN UP FOR CLASSES SOON

NOTES FROM YOUR ADVISORS

IF YOU ANTICIPATE GRADUATING IN FALL/WINTER OF 2021, AND HAVE NOT DONE SO, PLEASE APPLY TO GRADUATE!
THE DEADLINE TO APPLY FOR FALL/WINTER 21 GRADUATION IS SEPTEMBER 1ST. YOU MAY APPLY AFTER THIS DATE HOWEVER THERE WILL BE A LATE FEE.
TO APPLY YOU'LL FILL OUT THE ONLINE APPLICATION FOR DEGREE CANDIDACY AVAILABLE IN YOUR UACCESS STUDENT CENTER. HERE IS A TUTORIAL FROM THE REGISTRAR'S WEBSITE ON HOW TO DO SO: https://it.arizona.edu/sites/default/files/ApplyforGraduation.pdf. IF YOU ARE UNSURE OF YOUR GRADUATION DATE, PLEASE REACH OUT TO YOUR ACADEMIC ADVISOR SO YOU WILL HAVE A GENERAL IDEA OF WHEN YOU CAN PLAN TO GRADUATE.

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 303	WINDOWS SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	BOOK
CYBV 385	INTRODUCTION TO CYBER OPERATIONS	BOOK
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	BOOK 1, BOOK 2
CYBV 400	ACTIVE CYBER DEFENSE	BOOK 1, BOOK 2
CYBV 435	CYBER THREAT INTELLIGENCE	BOOK 1, BOOK 2, BOOK 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book 1, Book 2

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 437	DECEPTION & COUNTER-DECEPTION	BOOK
CYBV 450	INFORMATION WARFARE	BOOK 1
CYBV 454	MALWARE THREATS & ANALYSIS	BOOK
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	PENDING BOOK SELECTION
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	BOOK
CYBV 473	VIOLENT PYTHON	BOOK 1, BOOK 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	BOOK 1, BOOK 2
CYBV 479	WIRELESS NETWORKING AND SECURITY	PENDING BOOK SELECTION
CYBV 480	CYBER WARFARE	BOOK 1, BOOK 2
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION

BEFORE YOU KNOW WHERE YOU GO, YOU NEED TO KNOW WHERE YOU CAME FROM

CYBER SECURITY HISTORY

HACKERS DUMP SECRET INFO FOR THOUSANDS OF POLICE OFFICERS

Hackers said they posted the names, addresses, and other personal information of 7,000 law enforcement officers that were stolen from a training academy website they compromised. Many of the entries also included the officers' social security numbers, email addresses, and the usernames and passwords for their accounts on the Missouri Sheriff's Association training website. “Releasing the names, addresses, Social Security Numbers, telephone numbers, and credentials of hundreds and hundreds of law enforcement personnel is of tremendous concern.

AUGUST 1, 2011

THE ISS X-FORCE VULNERABILITY DATABASE DEBUTED

The IBM ISS X-Force Vulnerability Database debuted. It was one of the first public vulnerability databases. A vulnerability database (VDB) is a platform aimed at collecting, maintaining, and disseminating information about discovered computer security vulnerabilities. The database will customarily describe the identified vulnerability, assess the potential impact on affected systems, and any workarounds or updates to mitigate the issue. A VDB will assign a unique identifier to each vulnerability cataloged such as a number (e.g. 123456) or alphanumeric designation (e.g. VDB-2020-12345). Information in the database can be made available via web pages, exports, or API. A VDB can provide the information for free, for pay, or a combination thereof. IBM ISS X-Force. The IBM ISS X-Force Database is one of the world’s most comprehensive threats and vulnerabilities database. This database is the result of thousands of hours of work by X-Force researchers and developers, and much of the data is incorporated into IBM ISS’ own products.

AUGUST 2, 1997

THE CODE RED II WORM FIRST SEEN

Code Red II is a computer worm like the Code Red worm. Released two weeks after Code Red on August 4, 2001, it is similar in behavior to the original, but analysis showed it to be a new worm instead of a variant. Unlike the first, the second has no function for attack; instead, it has a backdoor that allows attacks. The worm was designed to exploit a security hole in the indexing software included as part of Microsoft's Internet Information Server (IIS) web server software. While the original worm tried to infect other computers at random, Code Red II tries to infect machines on the same subnet as the infected machine. Microsoft had released a security patch for IIS on June 18, 2001, that fixed the security hole, however not everyone had patched their servers, including Microsoft themselves.

AUGUST 4, 2001

COMPUTER WHIZ TERRY CHILDS GETS 4-YEAR SENTENCE

A former engineer was sentenced Friday to a four-year prison term. He was portrayed by prosecutors as a power mad techie who, facing reassignment because of workplace conflict, locked out his bosses from accessing the computer system by refusing to surrender vital codes he alone held. The 12-day incident in July 2008 cost the city close to $1.5 million, prosecutors said. Terry Childs ended up giving the passwords to Mayor Gavin Newsom and an aide after nine days in jail. "This case is about an individual who built a system, that he felt he owned," Jackson said. "He felt that - because of his blood, sweat and tears - this was his system. He was wrong. He was wrong and the jurors found he was wrong."

AUGUST 6, 2001

FALL

BEFORE YOU KNOW WHERE YOU GO, YOU NEED TO KNOW WHERE YOU CAME FROM

CYBER SECURITY HISTORY

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY V. ANDERSON, ET AL.

A temporary restraining order was granted to prevent 3 MIT students from presenting about MBTA (Massachusetts Bay Transit Authority) security vulnerabilities at DEF CON 16. Ten days later a judge rejected the MBTA's request to extend the restraining order. During the Spring of 2008, three students analyzed the security of the Boston transit fare collection system. The research was conducted as part of the MIT Computer and Network Security course 6.857. After several weeks of reverse-engineering, software development, testing, and analysis, they found several major security holes in the MBTA system.

AUGUST 9, 2008

INTRODUCTION OF NET-WORM.WIN32.BLASTER

The Blaster worm began spreading on Windows XP and 2000 systems. It exploited a buffer overflow vulnerability in the Distributed Component Object Model (DCOM) Remote Procedure Call (RPC) service. Within four days there were 423,000 reportedly infected systems. The worm was first noticed and started spreading on August 11, 2003. The rate that it spread increased until the number of infections peaked on August 13, 2003. Once a network (such as a company or university) was infected, it spread more quickly within the network because firewalls typically did not prevent internal machines from using a certain port. Filtering by ISPs and widespread publicity about the worm curbed the spread of Blaster. According to court papers, the original Blaster was created after security researchers from the Chinese group Xfocus reverse engineered the original Microsoft patch that allowed for execution of the attack.

AUGUST 11, 2003

13 DAIMLERCHRYSLER PLANTS KNOCKED OFFLINE BY WORMS

A round of Internet worm infections knocked 13 of DaimlerChryslers U.S. auto manufacturing plants offline for almost an hour, stranding some 50,000 auto workers as infected Microsoft Windows systems were patched. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware and Michigan were knocked offline at around 3:00 PM stopping vehicle production at those plants for up to 50 minutes. Farid Essebar, known as Diabl0, is a Moroccan black hat hacker. He was one of the two people (along with Turkish hacker Atilla Ekici) behind the spread of the Zotob computer worm that targeted Windows 2000 operating systems in 2005.

AUGUST 16, 2005

COMPUTER VIRUS BRINGS DOWN TRAIN SIGNALS

The Sobig Worm was a computer worm that infected millions of Internet-connected, Microsoft Windows computers in August 2003. Although there were indications that tests of the worm were carried out as early as August 2002, Sobig.A was first found in the wild in January 2003. Sobig.B was released on May 18, 2003. Sobig.C was released May 31 and fixed the timing bug in Sobig.B. Sobig.D came a couple of weeks later followed by Sobig.E on June 25. On August 19, Sobig.F set a record in the sheer volume of e-mails sent out to propagate its spread. The virus infected the computer system at CSX Corp.'s Jacksonville, Fla., headquarters shutting down signaling, dispatching, and other systems at about 1:15 a.m

AUGUST 20, 2003

>. CYBER PHYSICAL SYSTEMS RESEARCHER

≥ INTERNET OF THINGS DEVICES, CRITICAL INFRASTRUCTURE, AND SENSOR AND COMMUNICATION SYSTEMS ALL HAVE ONE THING IN COMMON: THEY INTERFACE THE DIGITAL AND PHYSICAL DOMAINS.

≥ THE CYBER-PHYSICAL SYSTEMS GROUP AT MIT LINCOLN LABORATORY CONDUCTS RESEARCH TO UNDERSTAND THE CYBERSECURITY IMPLICATIONS OF THESE PHYSICAL INTERFACES AND USE THE RESULTS OF OUR RESEARCH TO DEVELOP PROTOTYPES THAT SERVE AS PATHFINDERS FOR FUTURE TECHNOLOGICAL SOLUTIONS.

≥ THE CYBER PHYSICAL SYSTEMS GROUP TACKLES KEY PROBLEMS IN THE CONVERGENCE OF CYBERSECURITY AND THE PHYSICAL WORLD IN AN INTERDISCIPLINARY RESEARCH AND DEVELOPMENT ENVIRONMENT. WE FOCUS ON DEVELOPING NEW CAPABILITIES IN THE AREAS OF HARDWARE SECURITY AND CYBER-EW FOR THE DOD, INTELLIGENCE COMMUNITY, AND FEDERAL AGENCIES.

≥ KEY TECHNOLOGY DEVELOPMENT THRUSTS INCLUDE NOVEL SENSORS, TESTBED DEVELOPMENT AND INTROSPECTION, AND UNCONVENTIONAL METHODS OF SYSTEM EXPLOITATION.

≥ WE HAVE POSITIONS OPEN FOR FULL TIME AS WELL AS INTERNSHIP OPPORTUNITIES.

MIT
LINCOLN
LABORATORY

ALL SOURCE INTELLIGENCE ANALYST (35F) TRAINER

Jacobs

Full-time positions apply to anybody who has a background in Intelligence, ideally for personal with a security clearance and a background in intelligence. Must provide performance-oriented training using the TRADOC-approved Program of Instruction (POI). The full spectrum of training includes but is not limited to classroom (platform and group) training; hands-on/practical exercise training; role playing; simulation/virtual training; and field exercise training. Training may be for resident and non-resident training courses and in support of mobile training. Shall also participate as a Subject Matter Expert (SME) in developing revisions of the POIs, Lesson Plans and Training Support Packages (TSPs) to remedy any deficiencies or shortcomings identified during the preparation for and conduct of instruction. Conduct of instruction shall also be in support of specialized training requirements or the training of new systems.
Location: Sierra Vista, AZ

MI SYSTEMS MAINTAINER/INTERGRATOR (35T) COURSE TRAINER

Jacobs

Full-time positions apply to anybody who has a background in Intelligence, ideally for personal with a security clearance and a background in intelligence. Must provide performance-oriented training using the TRADOC-approved Program of Instruction (POI). The full spectrum of training includes but is not limited to classroom (platform and small group) training; hands-on/practical exercise training; role playing; simulation/virtual training; and field exercise training. Training may be for resident and non-resident training courses and in support of mobile training.
Shall also participate as a Subject Matter Expert (SME) in developing revisions of the POIs, Lesson Plans and Training Support Packages (TSPs) to remedy any deficiencies or shortcomings identified during the preparation for and conduct of instruction. Conduct of instruction shall also be in support of specialized training requirements or the training of new systems.
Location: Sierra Vista, AZ

COUNTERINTELLIGENCE (35L/35E) SENIOR- TRAINER

Jacobs

Full-time positions apply to anybody who has a background in Intelligence, ideally for personal with a security clearance and a background in intelligence. Must provide performance-oriented training using the TRADOC-approved Program of Instruction (POI). The full spectrum of training includes but is not limited to classroom (platform and small group) training; hands-on/practical exercise training; role playing; simulation/virtual training; and field exercise training. Training may be for resident and non-resident training courses and in support of mobile training. Shall also participate as a Subject Matter Expert (SME) in developing revisions of the POIs, Lesson Plans and Training Support Packages (TSPs) to remedy any deficiencies or shortcomings identified during the preparation for and conduct of instruction. Conduct of instruction shall also be in support of specialized training requirements or the training of new systems.

Location: Sierra Vista, AZ

Engineering Technician I

Jacobs

Part-time opportunities are located over at the Electronic Proving Grounds, also located in Sierra Vista. They part-time positions, come with benefits and 401K.Additionally, there are opportunities to obtain security clearances, which presents a lot of great job opportunities for so many. As a part of the test staff for the event, personnel will perform limited technical functions related to the support of testing activities such as operation, operator level maintenance and modifications. Person will be required to operate/maintain military tactical radios; send/receive and score voice/data transmissions and operate/maintain equipment within EPG's instrumentation suite. Appropriate boots and attire are required. May also be required to drive military vehicles (i.e., HMMWV – High Mobility Multipurpose Wheeled Vehicle) to accommodate test activity.

Location: Sierra Vista, AZ

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

RADIO FREQUENCY TEST LAB TEST AND EVALUATION ENGINEER

Jacobs

Part-time opportunities are located over at the Electronic Proving Grounds, also located in Sierra Vista. They part-time positions, come with benefits and 401K.Additionally, there are opportunities to obtain security clearances, which presents a lot of great job opportunities for so many. This position is responsible for supporting, conducting, and developing test plans and procedures for Ultra High Frequency (UHF) Satellite Communications (SATCOM), Very High Frequency (VHF)/UHF Line of Sight (LOS), Soldier Radio Waveform (SRW), and High Frequency (HF) standards and waveform conformance certification and assessment of various radio, radio systems, modems, waveforms and radio interoperability (IOP) assessments. Includes testing and data collection of the current MIL-STD-188-243 UHF Amplitude Modulation Frequency Modulation Phase Shift Keying Line of Sight Waveform Conformance Test Procedures (Revision 2), dated December 2007, or the most current version of the JITC approved test procedure. The current JITC test procedure is based on MIL-STD-188-243, DoD Interface Standard, Tactical Single Channel Ultra High Frequency (UHF) Radio Communications.

Location: Sierra Vista, AZ

IT INTERN - SECURITY

Phoenix Children's

This position assists the IT Security team within the Information Technology organization with cyber security activities, analysis and coordination. The IT Security team is a key part of Phoenix Children's Hospitals program to secure its information assets, services, and the products that depend on them, building trust with customers and stakeholders and protecting the privacy of PCHs patients and employees.

- Participates in security tool implementation, integration, and performance evaluation.
- Reviews security tool outputs, alerts, alarms, and reports.
- Conducts security log and event analysis.
- Analyzes system events, security alerts, network activity, and evaluates detection mechanisms.
- Participates in cyber security activities, communication, and coordination across the Enterprise.
- Works with the various teams to gather, evaluate, analyze, and report on metrics to ensure performance of security service delivery and identify trends.
- Performs miscellaneous job-related duties as requested.

RESEARCH INTERN

twosix TECHNOLOGIES

Two Six Technologies is seeking Research Interns to join projects on our Data Science, Cyber Capabilities, Mobile Embedded Systems, and Cyber Analytics teams. If you are passionate about cybersecurity and enjoy solving hard problems at the leading edge of technology, we are looking for you!

- Participate in cutting-edge research, and be encouraged to publish results
- Build deployable and scalable systems that solve real-world problems
- Be paired with a “lab buddy”, who will encourage and support your professional growth
- Present an end-of-internship project

Must have at least ONE of the following:

- Machine learning, natural language processing, computer vision, or data visualization
- Mobile and embedded system development or architecture
- Large scale data processing, such as Hadoop, Spark, or Cassandra
- Program analysis, reverse engineering, vulnerability research, cryptographic protocols
- Fundamental understanding of networking protocols, operating systems, or kernels
- Hacking skills (memory corruption, rootkits, MetaSploit, nmap, etc.)

CYBERSECURITY OPERATIONS ANALYST INTERN

ANDURIL

As a cybersecurity operations analyst intern, you will be sitting on the front lines of defending Anduril against determined cyber adversaries. You’ll investigate alerts across a wide spectrum of systems, including corporate, cloud, command and control environments, product telemetry, and everything in between. Your efforts will keep our company, people, and products safe from attackers' intent on stealing intellectual property and sabotaging our operations. You’ll stay abreast of emerging adversary cyberattack techniques across Mac, Windows, and Linux operating systems and utilize this knowledge to hunt for nefarious activity. You will also use the institutional knowledge gained from investigations to recommend and engineer new attack detections and defensive controls across the enterprise.

UPCOMING INTERNSHIPS OPPORTUNITIES – WE WILL HAVE MORE DETAILS ON OUR NEXT ISSUE IN SEPTEMBER

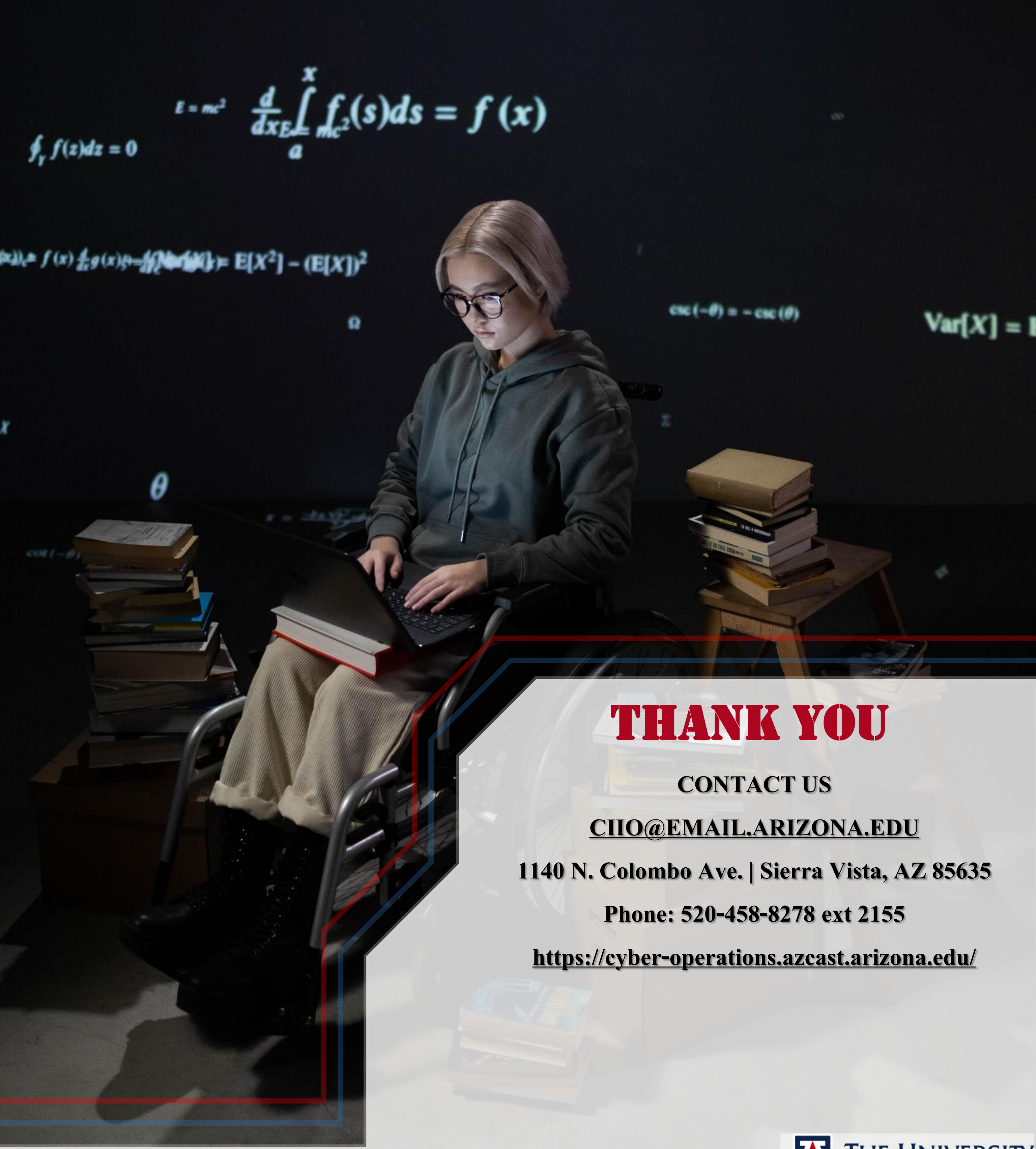
NSA – APPLICATION TIMELINE: SEPTEMBER 1ST TO OCTOBER 31ST

- CAE CO
- CSIP
- Cyber Summer Program (CSP)
- Colorado College Summer Internship Program

FBI

- Collegiate Hiring Initiative – Application on Fall 2021
  - Upcoming graduates must graduate by June of the program start year.
- FAIT Fellowship – Application on Fall 2021 for following year.

```
>.  ---CONNECTION ESTABLISHED---
>.  FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>.  HAVE A GREAT START OF CLASSES ON
>.  23 AUGUST 2021
>.  ---END TRANSMISSION---
```



THANK YOU

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

https://cyber-operations.azcast.arizona.edu/

ART BY @MIKHAIL NILOV

THE UNIVERSITY OF ARIZONA