IEEE Spark

IEEE

ENGINEERING INSIDE:

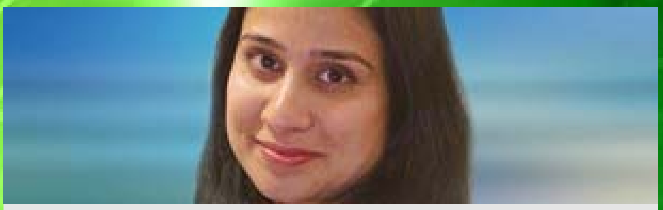
CYBERSECURITY

2016 ISSUE 2

Securing Cyber Space

May 2016

Your phone, your watch, your home, your car: These days more and more of the objects we use every day are connected to the Internet and more and more of our personal data is being stored online. This increasing reliance on networked technology means that cybersecurity breaches have the potential to bring about devastating damage.



Meet Anuja Sonalker!

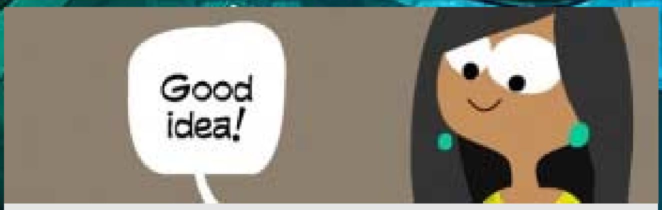
May 2016

Dr. Anuja Sonalker is an expert in cyber security for embedded and distributed networked systems. She brings together a broad set of technical skills, demonstrated leadership and experience from working with government, academia and with industry leaders. She has lead various efforts in the past 16+ years in automotive cyber security, intrusion detection, internet infrastructure security, wireless systems security, sensor networks, security protocol design and cryptography.

Encryption and Code Breaking

May 2016

A huge amount of personal information is stored on our computers and on the Internet. Just like spies use codes to send secret messages, computers encrypt data so it's more difficult to access and understand. In this activity, you will pair up with a friend to learn some basic code making techniques to explore how computers encode and decode information and how hackers can exploit weak encryption and bad passwords to access sensitive information.



Maximum Security

See what the Spark crew is up to in this issue!

IEEE Spark Challenge

Think you know IEEE Spark? Test your knowledge of engineering, computing and technology with the IEEE Spark Challenge! Answer questions correctly to help your team move to the top of the leaderboard.

TIPS AND ADVICE

Secure Your Cyber Skills with Online Training, Camps, and Competitions

The world needs more well trained cybersecurity experts and there are plenty of resources and programs available to help you to become one of them.

POPULAR TOPICS

3D printing aerospace animation at-home activity careers comic comics cybersecurity engineering forensics get involved green technology IEEE interview light

IEEE SPOTLIGHT

Setting Standards for Safety: The IEEE Cybersecurity Initiative

The IEEE has been helping engineers identify and fight against cyberattacks for more than three decades. The IEEE Symposium on Security and Privacy just marked its 35th anniversary in 2015.

FIND A UNIVERSITY

Search for accredited engineering degree programs throughout the world.

IEEE Spark

IEEE

ENGINEERING INSIDE:

CYBERSECURITY

2016 ISSUE 2

Securing Cyber Space

May 2016

by Robin Hegg

Your phone, your watch, your home, your car: These days more and more of the objects we use every day are connected to the Internet and more and more of our personal data is being stored online. This increasing reliance on networked technology means that cybersecurity breaches have the potential to bring about devastating damage.

There have been a string of recent large-scale cyber attacks that have highlighted how unprepared and under secured most institutions are. In 2013 a Ukrainian hacking ring broke into Target Corporation computers and stole roughly 40 million customer credit cards. In 2014, the same group broke into Home Depot computers, making off with between 53 and 56 million credit card numbers. In 2014 a group of hackers allegedly working for the North Korean regime used malware to break into the internal servers of Sony Pictures Entertainment. It is believed that this was a phishing attack in an employee clicked on a link in an email causing malware to be downloaded. The attack was able to go on for months before it was detected. The hackers accessed internal financial reports, employee health data, executives' emails, even unreleased movies and scripts, all of which were released. In 2015 a teenager in Northern Ireland was able to use a distributed denial-of-service attack and malicious code to access the names, birth dates, addresses, and phone numbers of more than 150,000 customers. In 2016, the IRS received a large number of false tax returns, filled out with stolen personal data. Attacks of this kind are extremely costly and put people's privacy and safety at risk.

Cyber attacks have now been used to cause physical damage as well. In late 2014 hackers attacked steel mill in Germany. The attackers were able to access the steel mill through the plant's business network using a spear-phishing attack in which an employee received an email that appeared to be from a trusted source. They clicked on a link or downloaded an attachment that caused malware to be downloaded to their computer. From there, the attackers were able to move into the production networks and access the systems controlling plant equipment. The attacks resulted in the plant becoming unable to shut down a blast furnace in a regulated manner, causing massive damage to the system. With more of our transportation and utilities systems online, the risks of an attack are huge and can effect our physical security as well.

While some institutions, such as banks, have learned to prioritize cybersecurity, others, like hospitals, haven't invested as much in cybersecurity, and are beginning to become major targets of cyber attacks. It is increasingly important that all organizations learn to prioritize cybersecurity so their data and their property are safe. On the hardware and software side, security is often low on the list of priorities for designers. In all industries and in all areas of technology

IN THIS ISSUE:

Unlock the intriguing world of cybersecurity in this issue of IEEE Spark. Learn about data protection techniques, meet a cybersecurity expert, practice code breaking, and check out resources to build your cyber skills.
Read this issue!

and networking, security must be kept in mind and prioritized throughout their design, development, and production.

Cyber criminals generally aim to steal data, damage hardware, software, or information, or disrupt services. Attackers use many different methods to exploit vulnerabilities and gain access to restricted systems and data. Cyber criminals will sometimes find and exploit a product’s back door—a way for the creators to access otherwise protected areas—or find a way to create one themselves. Other attacks involve physically tampering with a computer or network, or escalating an attacker’s privilege level on a network, allowing them to access areas they shouldn’t be able to.

A denial-of-service attack involves making a machine or network data unavailable to its users. This can happen by locking the users out of a system or by overloading a machine or network. Sometimes blocking access to the system is the goal of the attack. Other times, ransoms are demanded for access to the effected system or data to be reinstated.

Eavesdropping or Man-in-the-Middle attacks involve eavesdropping on data conversations by intercepting communications over networks. There are also eavesdropping concerns involving Internet-connected products that contain cameras and microphones. These concerns have been raised for products ranging from smart televisions to children’s toys.

Other attacks rely on tricking the user or using social engineering—gaining the trust of users to get important information. Clickjacking or User Interface redress attacks trick a user into clicking on a button or link on one webpage while they think they are clicking on another. This method can also be used to hijack a user’s keystrokes. Spoofing attacks involve an attacker using false data to pretend to be another person. Phishing attacks attempt to gather important information like passwords, usernames, and credit card numbers directly from users, usually through emails or instant messages, which often direct users to a fake website that is almost identical to the real one. Users are directed to enter their information into the fake website or to email it directly to the attacker.

Some of the strategies to strengthen cybersecurity and prevent these sorts of attacks are fairly simple, while others are far more complex. One of the most basic ways to make networks and data more secure is the use of strong passwords. It’s estimated that 91 percent of user passwords appear on the list of the top 1000 passwords. SplashData, a cybersecurity company, puts together a list each year from millions of stolen passwords and then ranks them by popularity. The top ten passwords for 2015 were 123456, password, 12345678, qwerty, 12345, 123456789, football, 1234, 1234567, and baseball.

User-created passwords also tend to follow certain rules and patterns. They often include some version of a person’s name or a family member or pet’s name. Numbers are usually at the end of the password and are often someone’s birthday or an old address. Hackers will find out as much information as they can about a target, then develop a list of possible passwords based on that information. They can use the lists of common passwords along with their targeted guesses and use a computer to quickly try all the possible passwords.

Limiting user privileges on a computer or network is another simple but effective step toward increasing security. This means only allowing users to access the levels of information they need and nothing more.

Cybersecurity experts are using a variety of strategies to fight back against cyber attacks. One is analyzing behavioral data to spot spoofing and other suspicious activities. They can create behavioral profiles of users and then use this information to notice any changes that are out of the ordinary, signaling a potential security breach. Using location tracking can also help set off alarms, particularly if a device is seen to be logging into accounts from an unusual location. Other techniques involve analyzing data from past attacks to determine what sites may be hacked in the future.

Virtual Dispersive Networking (VDN) is a technique developed to protect against Man-in-the-Middle (MiM) attacks, which eavesdrop on data conversations. By dispersing the message being sent into multiple parts, encrypting those parts, and then routing them over different protocols on independent paths, they become almost impossible to intercept or understand.

Many technology companies are also working to secure smart grids. Technologies are being developed to encrypt communications between central stations and field devices and to detect physical and digital tampering. Some monitor networks to make sure that only known and allowed communications are taking place and others allow for quick vulnerability assessments and compliance audits to check system security.

Cybersecurity experts are also working to develop active defense strategies—ways to actively track and fight back against hackers. Some gather counterintelligence, having a cyber expert learn about hackers and their techniques to learn about malware. Other techniques seek to lure in and then gather information on hackers. Sinkholing involves creating a sinkhole or a standard DNS server that hands out non-routeable addresses for all domains. This allows experts to intercept and block malicious traffic so it can be analyzed. Honeypots work by tempting hackers. A honeypot is a computer or network site that is created to attract hackers, allowing security experts to gather information on attacks and hackers.

While it’s important that cybersecurity experts are able to detect and respond to attacks, another important step toward increasing security is prioritizing security at the point of product design. Software and hardware should be designed with security in mind and new devices and software must be tested before they are released to the public in order to discover their vulnerabilities and address them..

Tracking down an attacker presents a huge challenge and law enforcement often isn’t up to the task. A lack of technological sophistication, time, and resources leaves many cases untouched, but some security software is helping police to track down cyber criminals. Even when an attacker can be identified, there is often little that can be done to prosecute them. There is still little international agreement on cyber law and since viruses can cross multiple jurisdictions, this can leave prosecutors’ hands tied. Many organizations, including the IEEE, are working to develop standards and policies that can help to keep machines, networks, and utilities safer, to help prevent and prosecute cyber crimes, and to help train more skilled cybersecurity experts.

The world is increasingly reliant on computers and the Internet. Users are trusting their devices and networks with their personal, financial, and medical information. Everyday devices like our cars, homes, appliances, toys, and televisions are now connected to the Internet. All of this makes strong cybersecurity all the more important. The world is in serious need of more skilled cybersecurity experts and engineers in all disciplines need to know the ins and outs of cybersecurity so it can be a priority through every part of the design process.

IEEE Spark

IEEE

ENGINEERING INSIDE:

CYBERSECURITY

2016 ISSUE 2

Meet Anuja Sonalker!

May 2016

Anuja Sonalker, Ph.D is Vice President of Engineering & Operations, North America for TowerSec where she leads engineering, operations and market facing R&D for the North American market.

Dr. Anuja Sonalker is an expert in cyber security for embedded and distributed networked systems. She brings together a broad set of technical skills, demonstrated leadership and experience from working with government, academia and with industry leaders. She has lead various efforts in the past 16+ years in automotive cyber security, intrusion detection, internet infrastructure security, wireless systems security, sensor networks, security protocol design and cryptography.

Prior to TowerSec, Anuja led innovation in automotive cyber security at Battelle, and systems security at IBM TJ Watson, and Fujitsu Labs.

In her spare time, Anuja mentors high school kids towards STEM disciplines and women through the Scholarships for Women Studying Information Systems (SWSIS).

1. Why did you choose to study the computer engineering and network security field?

I was always fascinated with electronics from childhood. My father was an engineer and we would do many household robotic and science projects all the time. I wanted to be a scientist when I grew up. If I didn't make it, I wanted to be a detective and solve crime. Then, I also belong to the generation that saw computers as commodities as a child. When we bought our first home computer – a 286, it opened up a whole new world for me. I knew right then, that this is what I wanted to do when I grow up – use a computer, because that's what scientists did! I didn't know at the time that no matter what field you are in, everyone would be using a computer in some way shape or form in the future world. Formally, I was introduced to network security only in college, and that too because of hearing about the first malware for a computer. It was a natural extension to what I was learning and doing, and was a cross between a scientist and a detective. Solving cyber crime! What better field could there be?

2. What do you love about engineering and network security?

I love the fact that you can tinker with things in your own way. There isn't just one right way of doing things in engineering. It's en-gin-eering! With network security there is a sense of defending and protecting that I love the most. There is a sense of responsibility and a sense of building responsible technologies. Then there is the constant need to stay two steps ahead of the bad guys.

3. How did you first get involved with cybersecurity? Share a project or inspiration with us please that prompted your involvement…

I first got involved in cyber security in college. There was a multimillion-dollar

USEFUL LINKS:

Tower Sec
Battelle Cyber Innovations
NSF Cybersecurity Programs

EDUCATIONAL BACKGROUND:

PhD, Network Security, University of Maryland College Park
Master of Science, Computer Engineering-Distributed Systems Security, North Carolina State University
Bachelor of Engineering, University of Mumbai

ADVICE TO STUDENTS:

...The best advice would be to find a mentor, someone in the field who is willing to guide you to gain skills relevant to today. Also, keep up with cyber security news as much as you can...

grant that a new group of professors had won and they were looking for students to join them. I interviewed and got a spot on the project. It was about creating a joint space in the internet where people could share resources, computing power, storage, save their stuff in a secure manner (Little did I know that this was the ancestor of the modern day cloud)

4. Can you explain a little about how the tools and techniques used and work done in cybersecurity has changed during the course of your career thus far?

Cyber security has come a long way. In the beginning there were rudimentary tools, and frankly limited capabilities to cyber damage. It was the days of C and object oriented programming was being introduced. Then came java and other internet programming technologies. As internet technologies advanced, people started focusing on security of network protocols and internet security. As the cat and mouse game with hackers began, we started going lower and lower in the stack to thwart off malicious hackers. If they would try to attack at the network (IP level) we would be defending and monitoring at the data link layer (Ethernet) and so on. With the advancement in silicon technologies, hardware suddenly pivoted and computing started moving to smaller devices. Computers no longer meant being on your desk or laptop, but were now your phones, your tablets, TVs, toasters and cars. This changed the network security game tremendously. Embedded systems security has now emerged as the single biggest, most pervasive challenge this century. And we still haven’t figured it out completely.

5. Is there a particular application or industry that you think could benefit the most from developments in cybersecurity in the future? Does it impact every field?

It absolutely impacts every field, simply because computers and electronics are used in every field today. Robots and telematics is used in surgeries and medicine, electronics are used in telecommunications, we have smart electronics like nest and smart TVs and refrigerators in our homes, industrial automation is based on computers and IP enabled electronic controllers, fitness devices and personal electronics are ever so common, banking and financial industry relies heavily on computers and electronic networks, e-commerce (all the online shopping we do) relies on electronic banking. Even our cars today have more electronics than a typical computer. Needless to say, imagine subverting any of these systems above and you can easily realize what havoc it can cause in our daily lives. Even though we don’t see it, we depend heavily on cyber security to be able to use all these services and systems reliably.

6. What are the current challenges in the field of cybersecurity? What’s the biggest obstacle at the moment?

The current challenges in cyber security come from embedded computing devices, in my opinion. In the past few years, we have progressively started moving from traditional desktops and laptops to smaller hand held or more pervasive devices for our computational needs. Smart phones of today can do everything a typical laptop can do. Most devices in our homes are capable of doing a lot of data processing, intelligence and are connected to the Internet. This shifts the focus from securing certain end points on a traditional enterprise network (corporate organizational network) to now trying to secure every end point on every commercial network all the time. And these devices can connect to different networks as they move around so a compromised device can be a new entry point to another otherwise unaffected network. The problem is huge.

7. Whom do you admire and why?

Personally, I admire my parents because of all the support and encouragement they gave us to each follow our dreams. They made sacrifices so we didn’t have to. Professionally, I admire Dr. Abdul Kalam, the 11th president of India who was a scientist turned politician. He spent his life dedicated to the advancement of science, and then to take science to every child and youth in the country.

Outside of my work, I would love to do the same someday.

8. What do your think the future holds for cybersecurity applications?

Cyber security applications will become a part of everything we do in our lives. In this ultra digitized world, there cannot be an application of technology that does not need cyber protection. It is not a luxury any more, but a cost of doing business, a cost of owning technology and a cost of using tech features. Cyber terrorism, cyber espionage, and cyber criminal activity is at an all time high, and will only get worse. I believe that in a few years, cyber security will need to be cross-disciplined with other disciplines in order for those disciplines to survive. For example, automotive engineering. Today, automotive engineers must understand cyber security in order to build secure cyber robust cars.

9. What's the most important thing you've learned through your work in cybersecurity? Are there still challenges that surprise you?

The most important thing I've learned is that there is no such thing as 100% cyber secure (unless it's a brick or its dead). It's always a game of making it hard for the adversary to the point where it's infeasible for the adversary to try to penetrate a system. Then, I've also learnt that infeasibility exists for a short time. There are technological shifts (hardware gets cheaper over time, some one always comes up with an open source version of some software) and then the attack becomes feasible and worthwhile for the adversary again. Then you have to up the challenge again. It's a live game. And it never ends. You have to try to stay two steps ahead of the adversary.

Surprises? Yes, every now and then it surprises me to learn how someone accidently stumbled upon a new way of getting into someone's system. That's a scientist in the making, in my opinion. They've just discovered a way to do something that no one else thought about. And it just happens to be a security flaw, so it caught my attention. I would love to groom such a person into a scientist and use their knack for the betterment of society.

10. What advice would you give to recent graduates interested in working in cybersecurity? Are there degrees that make the most sense…activities that would help?

I would say, cyber security is a mindset. First of all, you have to think like an attacker, and then think like a defender. How can you better create a system that you just broke into? If you are good at this type of thinking, you are naturally inclined to build cyber secure systems. You may be interested in traditional computers, or computer networks, or embedded devices, or cryptographic techniques for protection, it all requires the same mindset. The best advice would be to find a mentor, someone in the field who is willing to guide you to gain skills relevant to today. Also, keep up with cyber security news as much as you can. Most reporters today have discovered that cyber security news sells and there is a lot of coverage of anything cyber security. Reading up on recent events will show you where the state-of-the-art needs to move and you will be ahead of the pack. There are 200,000 vacancies today in cyber security. These are jobs that cannot be filled because we cannot find the talent. There could not be a better time to enter this field. When I graduated in cyber security, it was the norm that 80% of graduates went into academia because only 20% could find jobs. Today there is a scarcity.

11. If you weren't focused on the field of cybersecurity, what would you be doing?

If I weren't focused on cyber security, I would be mentoring students in STEM, and/or raising more awareness about cyber security in the world. The general population needs to know more about how cyber security impacts their daily lives and how to follow good cyber hygiene.

IEEE Spark

IEEE

ENGINEERING INSIDE:

CYBERSECURITY

2016 ISSUE 2

Encryption and Code Breaking

May 2016

by Robin Hegg

A huge amount of personal information is stored on our computers and on the Internet: names, phone numbers, addresses, credit card numbers, social security numbers, and more. All of this information is vulnerable to cyber attacks. But good cybersecurity skills and strategies can make accessing this information extremely difficult.

Just like spies use codes to send secret messages, computers encrypt data so it's more difficult to access and understand. In this activity, you will pair up with a friend to learn some basic code making techniques to explore how computers encode and decode information and how hackers can exploit weak encryption and bad passwords to access sensitive information.

Materials

Paper

Pen or pencil

A friend

Steps

1. Create a simple letter shifting code by creating a cypher wheel. In a letter shifting code, each letter of the alphabet is shifted a certain number of spaces. If you do a one-letter shift, A becomes B, B becomes C, and so on. In a two letter shift A becomes C, B becomes D, etc. You can create a key to your code by writing out the alphabet on one line, then your shifted code alphabet on the second line.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

WXYZABCDEFGHIJKLMNOPQRSTUV

In this example A=W, X=T, etc.

Or, you can create a cypher wheel using the same method. In a cypher wheel, you will write out the alphabet on two strips of paper then turn the strips into circles, taping the ends together so you have two separate rings or wheels. When you place the wheels side by side, all you have to do is turn one wheel until the letters line up how you'd like them to be for your code. Then the wheel serves as an easy key for this and future codes.

2. Write a message to your friend and use your letter-shifting code to encode the message. Have your friend do the same. Exchange your encoded messages and try to decode them.

DID YOU KNOW?

The most expensive virus of all time, MyDoom, caused an estimated $38.5 billion in financial damage!

A recent report cites ransomware (malware that demands a ransom to remove its restrictions) as the most problematic cyberthreat.

Two thirds of big UK businesses cite being targeted by a cyber attack in the past year.

FIND OUT MORE:

You can also visit **TryEngineering.org** to explore other engineering activities and resources. Additional activities and lessons can be found **here**.

3. Next, you and your friend will each create a new code. It can be a variation on the letter-shift code or something completely different. You can study different code systems if you'd like to help you develop your new code system. Think about what strategies you were able to use to break the simple letter shifting code. What were that code's weaknesses? Try to make it harder for your friend to decode your next message. Create a key for this code.

4. Write another message to your friend and encode it using your new code. Have your friend do the same. Exchange messages and try to decode them.

Questions

1. How did trying to decode the first message compare to trying to decode the second? Were you able to create a more difficult-to-crack code the second time? What elements of your code do you think made a difference?

2. What do you think were the weaknesses of the letter-shifting code? What elements of the code or the coded message itself were you able to exploit to begin to decode it?

3. How do you think what you experienced here relates cyber security? How do you think your experience decoding encrypted messages relates to password strength and how hackers might be able to guess passwords? Drawing from your experience, what do you think you could do to make a stronger password to better protect your accounts and information?

Additional Activities

1. Take a look at a list of the most commonly used passwords. Review the passwords and make a list of the patterns you notice. What categories do the passwords fall into? What do they have in common? What are they missing that a stronger password might include? Looking at the list, what should you avoid when creating your own passwords?

2. Try your hand at the games on **OverTheWire**. The games are designed to help you to learn and practice security concepts.

IEEE Spark

IEEE

ENGINEERING INSIDE:

CYBERSECURITY

2016 ISSUE 2

Secure Your Cyber Skills with Online Training, Camps, and Competitions

May 2016

by Robin Hegg

The world needs more well trained cybersecurity experts and there are plenty of resources and programs available to help you to become one of them.

Hacker Highschool is a collection of lessons designed to teach teens the art of ethical hacking and how to defend themselves against fraud, identity theft, privacy leaks, and other attacks they can become vulnerable to online. The lesson workbooks, which can be downloaded for free from the website and are designed to be self-guided, were researched and designed by **ISECOM** (the Institute for Security and Open Methodologies). You can also try to get a Hacker Highschool class or club set up in your school or community.

There are also a number of summer camps throughout the United States that can help to teach you cybersecurity skills. **GenCyber** is a summer camp developed by the National Science Foundation (NSF) and the National Security Agency (NSA) to introduce middle and high school students to cybersecurity basics. The camp was developed in the hopes that it will nurture a new generation of skilled cybersecurity professionals and fill America's need for more highly trained cybersecurity experts. GenCyber began with a pilot program in 2014 that included six camps with a total of about 265 students. The following year, 29 universities in 19 states hosted a total of 43 camps. The camps are free and teach students how to monitor networks and detect vulnerabilities that might lead to cyberattacks.

Other cybersecurity camps include **Bulldog Bytes**, a GenCyber camp run by Mississippi State University's Bagley College of Engineering, a camp for high school students run by the **Community College of Baltimore County** in Maryland, **Cyber Discovery** run by the National Integrated Cyber Education Research Center in Louisiana, and Cybercamp run by the **Lowcountry Tech Academy** in Charleston, South Carolina.

Cybersecurity competitions designed for high school students are another way to develop and test out your skills. The **CyberCenturion** competition in the United Kingdom and the **CyberPatriot** competition in the United States were designed to inspire students toward careers in cybersecurity.

The National Initiative for Cybersecurity Careers and Studies (NICCS) has a number of **resources** for students, including a list of cybersecurity degree programs, scholarships, and internship opportunities.

IN THIS ISSUE:

Unlock the intriguing world of cybersecurity in this issue of IEEE Spark. Learn about data protection techniques, meet a cybersecurity expert, practice code breaking, and check out resources to build your cyber skills.
Read this issue!

IEEE Spark

IEEE

ENGINEERING INSIDE:

CYBERSECURITY

2016 ISSUE 2

Setting Standards for Safety: The IEEE Cybersecurity Initiative

May 2016

by Robin Hegg

The IEEE has been helping engineers identify and fight against cyberattacks for more than three decades. The **IEEE Symposium on Security and Privacy** just marked its 35th anniversary in 2015. Moving forward with their work, in 2014, the **IEEE Computer Society** and the **IEEE Future Directions Committee** joined together to form the **IEEE Cybersecurity Initiative (CYBSI)**. CYBSI works to improve the understanding of cybersecurity and to bring focus to the areas where more security and knowledge is needed.

CYBSI launched the **IEEE Center for Secure Design (CSD)** to shift the focus in cybersecurity from identifying viruses and bugs to identifying common design flaws that leave software vulnerable to attacks. Flaws in software's architecture and design are responsible for about half of all security breaches. Studying the most common of these flaws can help software architects to learn from these mistakes and build software that is more secure by design. CYBSI's chair, IEEE Senior Member Greg Shannon, says, "Now is the time not only for better defensive measures but also for cybersecurity standards and best practices that consider the entire technology life cycle."

The CYBSI is also working to set standards for professional credentials for cybersecurity specialists. This will help to ensure that trained and experienced cybersecurity experts are available and that those hiring them can feel confident that their employees have the skills needed. The largest cybersecurity certification program currently available is the **Certified Information Systems Security Professional (CISSP)**. CYBSI is calling for additional certifications within specialized fields and for a corresponding code of ethics. Since one way of ensuring a program's safety is learning how to break into it, a code of ethics would help to keep experts with these skills working on the side of security.

IEEE also hosts a number of cybersecurity conferences, including the **IEEE Symposium on Security and Privacy**, the **IEEE International Symposium on Hardware-Oriented Security and Trust**, and the **IEEE International Symposium on Technologies for Homeland Security**. IEEE publications like **IEEE Security and Privacy** help to keep cybersecurity professionals informed and sharing their knowledge with one another.

IN THIS ISSUE:

Unlock the intriguing world of cybersecurity in this issue of IEEE Spark. Learn about data protection techniques, meet a cybersecurity expert, practice code breaking, and check out resources to build your cyber skills.
Read this issue!

IEEE Spark

IEEE

ENGINEERING INSIDE:

CYBERSECURITY

2016 ISSUE 2

Maximum Security

May 2016

My internet passwords are complex, so I have them all stored in Sparkbot's memory.
Good idea!
Except I can't remember the password to turn Sparkbot on!
LOGIN FAILED
*****

IN THIS ISSUE:

Unlock the intriguing world of cybersecurity in this issue of IEEE Spark. Learn about data protection techniques, meet a cybersecurity expert, practice code breaking, and check out resources to build your cyber skills.

Read this issue!

IEEE Spark Challenge: Cybersecurity

Think you know IEEE Spark? Test your knowledge of engineering, computing and technology with the IEEE Spark Challenge!

1) Malicious code that copies itself and spreads to other computers without the use of a host file is known as a:
   a. Trojan
   b. Virus
   c. Hoax
   d. Worm

2) In what decade was the first worm released?
   a. 1960's
   b. 1970's
   c. 1980's
   d. 1990's

3) Which are common techniques of cyber criminals?
   a. Finding and exploiting a product's back door
   b. Physically tampering with a computer or network
   c. Escalating an attacker's privilege level on a network
   d. Making a machine or network data unavailable to its users
   e. all of the above

4) Spoofing involves an attacker using false data to pretend to be another person.
   a. True
   b. False

5) Clickjacking attacks that trick a user into clicking on a button or link on one webpage while they think they are clicking on another in order to hijack a user's keystroke are also known as:
   a. Interface redress attacks
   b. Spoofing
   c. Phishing
   d. None of the above

6) Virtual Dispersive Networking (VDN) is a technique developed to protect against:
    a. Phishing
    b. Spoofing
    c. Man-in-the-Middle attacks (MiM)
    d. Clickjacking

7) Technologies that analyze phone calls to identify malicious behavior are known as:
    a. Bioprinting technologies
    b. Phoneprinting technologies
    c. 3D call printing technologies
    d. Audio Imprinting technologies

8) A computer or network site that is created to attract hackers, allowing security experts to gather information on attacks and hackers is known as a:
    a. Jam jar
    b. Honeypot
    c. Syrup sieve
    d. Sugar bowl

9) Redirecting traffic in order to record and analyze the efforts of hackers is known as:
    a. Lagooning
    b. Hollowing
    c. Quicksanding
    d. Sinkholing

10) Seventy-one percent of passwords appear on the list of the top 1000 passwords.
    a. True
    b. False

IEEE Spark Challenge: Cybersecurity

Answer Key

Think you know IEEE Spark? Test your knowledge of engineering, computing and technology with the IEEE Spark Challenge!

1) Malicious code that copies itself and spreads to other computers without the use of a host file is known as a:
    a. Trojan
    b. Virus
    c. Hoax
    d. Worm

2) In what decade was the first worm released?
    a. 1960's
    b. 1970's
    c. 1980's
    d. 1990's

3) Which are common techniques of cyber criminals?
    a. Finding and exploiting a product's back door
    b. Physically tampering with a computer or network
    c. Escalating an attacker's privilege level on a network
    d. Making a machine or network data unavailable to its users
    e. all of the above

4) Spoofing involves an attacker using false data to pretend to be another person.
    a. True
    b. False

5) Clickjacking attacks that trick a user into clicking on a button or link on one webpage while they think they are clicking on another in order to hijack a user's keystroke are also known as:
    a. Interface redress attacks
    b. Spoofing
    c. Phishing
    d. None of the above

6) Virtual Dispersive Networking (VDN) is a technique developed to protect against:
   a. Phishing
   b. Spoofing
   c. Man-in-the-Middle attacks (MiM)
   d. Clickjacking

7) Technologies that analyze phone calls to identify malicious behavior are known as:
   a. Bioprinting technologies
   b. Phoneprinting technologies
   c. 3D call printing technologies
   d. Audio Imprinting technologies

8) A computer or network site that is created to attract hackers, allowing security experts to gather information on attacks and hackers is known as a:
   a. Jam jar
   b. Honeypot
   c. Syrup sieve
   d. Sugar bowl

9) Redirecting traffic in order to record and analyze the efforts of hackers is known as:
   a. Lagooning
   b. Hollowing
   c. Quicksanding
   d. Sinkholing

10) Seventy-one percent of passwords appear on the list of the top 1000 passwords.
   a. True
   b. False