Introducere în Securitatea informatică

Securitate informatică

March 18, 2020

Mihai-Lica Pura

Cuprins

Nevoia de securitate informatică/Motivație

- Carduri bancare
  - operații la bancomat
  - plăți prin POS
  - plăți electronice prin Internet
- Internet banking/Mobile banking
- Email account and other accounts
- acces WiFi
- ANAF - depunere declații fiscale (persoane fizice și juridice)
  `https://static.anaf.ro/static/10/Anaf/Declaratii_R/instructiuni/etape_depunere.htm`
  `https://static.anaf.ro/static/10/Anaf/Declaratii_R/instructiuni/Instructiuni_D200.htm`

Nevoia de securitate informatică/Motivație

- CNAS - raportări pentru furnizorii de servicii medicale, medicamente și dispozitive medicale
  `http://www.cnas.ro/casmb/page/procedura-de-inregistrare-a-certificatelor-digitale.html`
- MySMIS 2014 - Access EU funds – Ministry of European Funds
  `https://2014.mysmis.ro/`
  `http://www.fonduri-ue.ro/mysmis`
- SEAP - Sistemul Electronic de Achiziții Publice
  `http://licitatiiseap.ro/seap/`
  `https://www.e-licitatie.ro/`
- Centrul Național de Administrare a Registrelor Naționale Notariale - Infonot
  `https://www.infonot.eu/`
- etc.

Nevoia de securitate informatică/Motivație

- "Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitable protected." (ISO 27002:2005)
- "Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected." (ISO 27002:2005)
- Informația este un bun valoros atât pentru persoanele fizice, cât și pentru organizații, și trebuie să fie protejată.

Security services and security mechanisms

- Open Systems Security Architecture (X.800)
  - the first stage in the development of a suite of standards to support security services and mechanisms
  - general description of security services and the related mechanisms that can be used to provide these services
  - Security services:
    - Authentication;
    - Access Control;
    - Data Confidentiality;
    - Data Integrity;
    - Non-Repudiation.

Security services

- ISO 7498-2 (1989) and X.800:
  - **Identification and authentication** - the ability to identify and uniquely authenticate all users of a system
  - **Authorisation/access control** - the ability to allow or prohibit users from accessing the information assets of an organisation
  - **Confidentiality** - the ability to ensure that information assets are only available to those who are authorised to access them
  - **Integrity** - the ability to ensure that information is complete and uncorrupted and that it has not been altered in any way
  - **Non-repudiation/non-denial** - the ability to ensure that users do not deny their actions

Security services

- ITU-T Recommendations Report X.805 in support of the X.800 and ISO 7498-2 (1989)
- adds 3 new dimensions:
  - Privacy
  - Availability
  - Communication Security

Security services

- **Authentication** - serves to confirm the identities of the communicating entities
  - the recipient of the message should be sure that the message came from the source that it claims to be
  - all communicating parties should be sure that the connection is not interfered with by unauthorized party
- **Access Control** - protects against unauthorised use of network resources
  - who can have access to a resource
  - under what conditions access can occur
  - what those accessing are allowing to do
- **Data Confidentiality** - protects data from unauthorised disclosure; ensures that the data content cannot be understood by unauthorised entities (passive attacks)

Security services

- **Data Integrity** - ensures the correctness or accuracy of received data
  - no modification
  - no insertion
  - no deletion
  - no replay
  - protection from active attacks
  - it may be
    - integrity with recovery
    - integrity without recovery (detection only)

Security services

- **Non-repudiation** - provides the means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent or commitment; proof of data origin, proof of ownership, proof of resource use)
- **Privacy** - provides for the protection of information that might be derived from the observation of network activities
- **Availability** - ensures that there is no denial of authorised access to network elements, stored information, information flows, services and applications due to events impacting the network
- **Communication security** - ensures that information flows only between the authorised end points

Security mechanisms

The security services referred to by the X.800 and ISO 7498-2 (1989) standards are supported by eight security mechanisms:

- **encipherment mechanisms**
  - encryption or cipher algorithms
  - can help provide confidentiality of data and traffic flow information
  - can provide the basis for some authentication and key management techniques
- **digital signature mechanisms**
  - can be used to provide non-repudiation, origin authentication and data integrity services
- **access control mechanisms**
  - provide a means for using information associated with a client entity and a server entity to decide whether access to the resources of the server is granted to a client
  - e.g. access control lists and security labels

Security mechanisms

- **data integrity mechanisms**
  - are used to provide data integrity and origin authentication services
- **authentication exchange mechanisms**
  - also known as authentication protocols
  - can be used to provide entity authentication
- **traffic padding**
  - describes the addition of 'pretend' data to conceal the volumes of real data traffic
  - can be used to help provide traffic flow confidentiality but is only effective if the added padding is enciphered

Security mechanisms

- **routing control mechanisms**
  - can be used to prevent sensitive data from using insecure communications paths
  - e.g. depending on the properties of the data, routes can be chosen to use only physically secure network components
  - data carrying certain security labels may be forbidden to enter certain network components
- **notarisation mechanisms**
  - can be used to guarantee the integrity, origin and/or the destination of transferred data
  - a third party notary, who must be trusted by the communication entities, will provide the guarantee typically by applying a cryptographic transformation to the transferred data

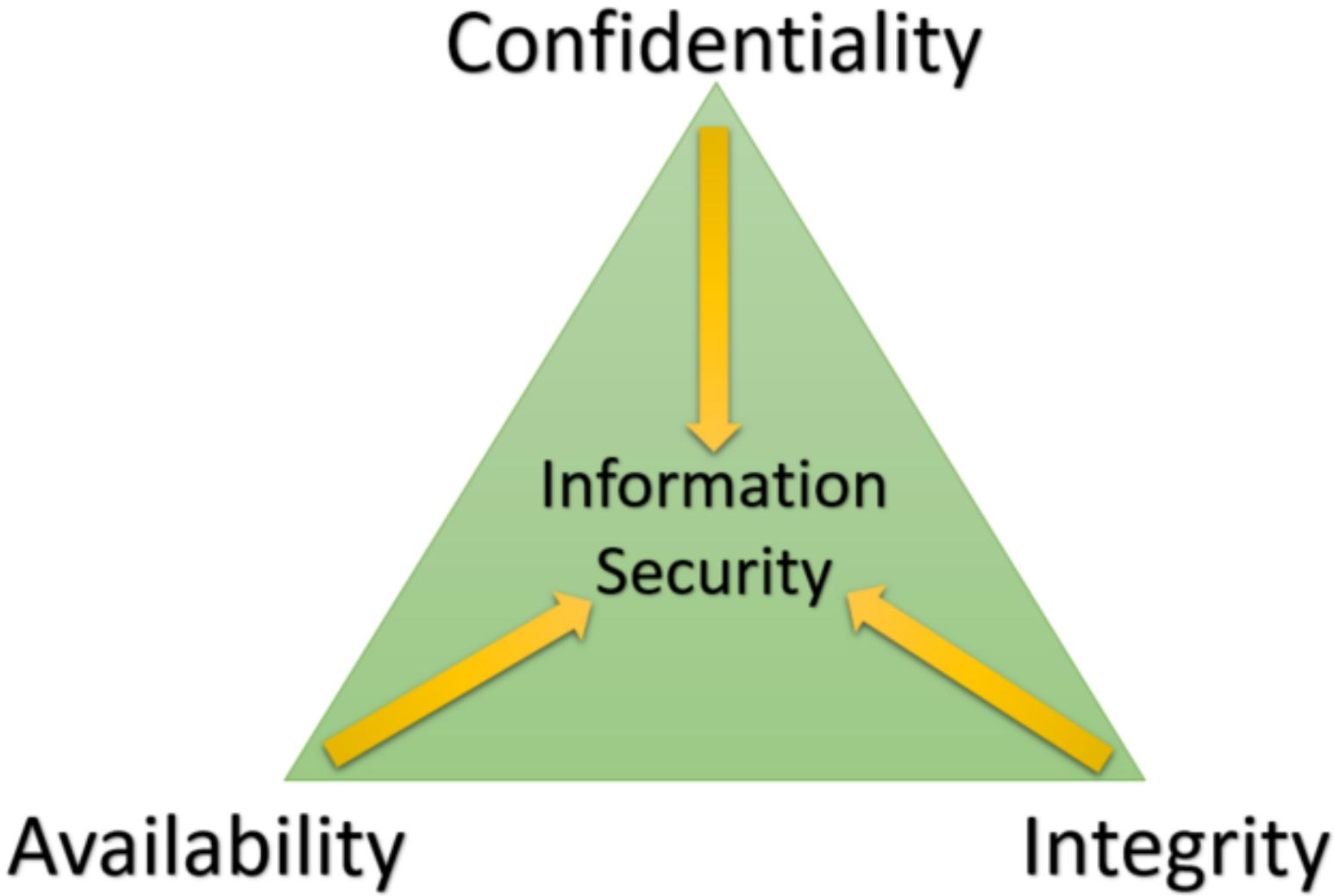
Security mechanisms

- Other new security mechanisms:
- **Data anonymization**
  - type of information sanitization whose intent is **privacy protection**
  - the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous

Information security principles

- Information security is the protection of information and systems from unauthorized access, disclosure, modification, destruction or disruption.
- ISO 27002:2005 - Information security principles/goals/objectives:
  - Confidentiality
  - Integrity
  - Availability
- the **CIA triad**

Information security principles



Definitie

- Securitatea informației este domeniul care se ocupă de **studiul mecanismelor de protecție a informației**, în scopul asigurării unui **nivel de încredere în informație**.
- Nivelul de încredere în informație depinde de nivelul mecanismelor de securitate care îi garantează protecția în fața riscurilor care apar asupra securității ei.
- **Information Systems Security (INFOSEC)***: **protecția** sistemelor informatice împotriva:
  - **accesului neautorizat**
  - sau a **modificării informației**, fie stocată, procesată sau în tranzit,
  - și **împotriva refuzului de servicii** către utilizatorii **autorizați**
  - sau **asigurării de servicii** către utilizatorii **neautorizați**,

  incluzând acele metode necesare detectării, documentării și respingerii acestor amenințări.

  * CNSS, (2006), NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY

Definiție

- Information Security requires for an information system **trust**.
- The system:
  - was designed properly
  - was independently evaluated against a set of explicit security standards
  - maintains proper operation during its lifetime, face of malicious attacks/human error

Vulnerabilități

- Cum ajunge adversarul la sistemul informatic?
  - Securitatea fizica
  - Securitatea electronică
- Information system's vulnerabilities affect 3 levels of human activities:
  - personal security (privacy)
  - companies/organization security
  - national security

Vulnerabilități

- In securitatea informației, cuvantul **vulnerabilitate** se refera la un punct slab in sistem care permite unui atacator să încalce unul sau mai multe dintre principiile/obiectivele acesteia.
- Regula: un sistem nu este mai sigur decât cea mai vulnerabilă componentă a sa.
- Clasificare vulnerabilitati:
  - **vulnerabilități de proiectare** (ex. proiectarea greșită a unui protocol de comunicare)
  - **vulnerabilități de implementare** (ex. overflow)
  - **vulnerabilități de utilizare/exploatare** (ex. alegerea unor parole slabe, etc.)

Vulnerabilități

- A vulnerability can exist either only in theory, or could have a known **exploit**.
- Vulnerabilities are of significant interest when the program containing the vulnerability:
  - operates with special privileges,
  - performs authentication,
  - or provides easy access to user data or facilities (e.g. network server).

Cauze ale vulnerabilităților

- vulnerabilitatea unei primitive criptografice ce poate fi amplificată de protocolul de securitate
  - multe funcții criptografice au vulnerabilități ascunse
  - chiar și folosirea celei mai solide funcții criptografice în mod necorespunzător poate duce la pierderea totală a securității
- asumarea unor garanții de securitate care sunt supra-specificate sau prost înțelese
  - e.g. utilizarea unei funcții de criptare și prezumția faptului că aceasta va asigura și faptul că datele nu vor fi alterate
- neatenția în aplicarea unor principii generale aplicabile unei clase mai largi de primitive
  - e.g. criptarea folosind un mecanism cu cheie publică a unei informații de entropie scăzută

Cauze ale vulnerabilităților

- lipsa definițiilor formale
- lipsa unui buget de securitate incremental
- absența expertizei necesare în domeniul securității
- incapacitatea de a instala ușor tehnologia necesară
- politici de securitate inadecvate
- sisteme slabe de control ale rețelelor
- proasta configurare a sistemelor
- comunicare wireless neadecvată
- autentificare neadecvată la comunicare

Cauze ale vulnerabilităților

- lipsa mecanismelor de detecție și restricționare a drepturilor de acces la sisteme de control
- absența uneltelor pentru detecția și raportarea activităților anormale
- utilizarea rețelei pentru trafic neautorizat
- lipsa mecanismelor de detecție a erorilor ce pot conduce la epuizarea bufferelor
- lipsa mecanismelor de control a schimbului de software
- lipsa educației utilizatorilor cu privire la bunele practici în vederea asigurării securității

Cauze ale vulnerabilităților

- Computer systems and programs have become **more complex**.
- **Quality control** hasn't been able to keep up due to market pressures, programming skill deficiencies, etc.
  - Quality control is a real issue when it comes to determining if a piece of code is "secure".
  - Most companies simply don't have the time to check ALL the possibilities because of a number of reasons
  - e.g. Since there was no central UNIX development group, it was up to the individual programmers to check their code.
- So Many Systems, Not Enough Time - 2.3 million hosts are connected to the Net each month.
- **The Prime Directive: Keep the system up!**
- **Patch the system? When I will have time . . .**

Disclosure of vulnerabilities

- The method of disclosing vulnerabilities is a topic of debate in the computer security community.
  - Some advocate **immediate full disclosure** of information about vulnerabilities once they are discovered.
  - Others argue for **limiting disclosure** to the users placed at greatest risk, and only releasing full details after a delay, if ever. Such delays may allow those notified to fix the problem by developing and applying patches, but may also increase the risk to those not privy to full details.
- This debate has a long history in security.
- More recently a new form of commercial vulnerability disclosure has taken shape, see for example TippingPoint's Zero Day Initiative which provides a **legitimate market for the purchase and sale of vulnerability information** from the security community.

Disclosure of vulnerabilities

- From the security perspective, only **a free and public disclosure** can ensure that all interested parties get the relevant information.
- Security through obscurity is a concept that most experts consider unreliable.
- Most often a channel is considered trusted when it is a widely accepted source of security information in the industry (e.g. CERT, SecurityFocus, Secunia and FrSIRT).

Disclosure of vulnerabilities

- The **time of disclosure** of a vulnerability is defined differently in the security community and industry. It is most commonly referred to as "a kind of public disclosure of security information by a certain party".
- The time of disclosure is the first date a security vulnerability is described on a channel where the disclosed information on the vulnerability has to fulfil the following requirement:
  - the information is freely available to the public
  - the vulnerability information is published by a trusted and independent channel/source
  - the vulnerability has undergone analysis by experts such that risk rating information is included upon disclosure

Vulnerabilități

- Many software **tools** exist that can aid in the discovery (and sometimes removal) of vulnerabilities in a computer system.
- Though these tools can provide an auditor with a good overview of possible vulnerabilities present, **they can not replace human judgement**. Relying solely on scanners will yield false positives and a limited-scope view of the problems present in the system.
- Vulnerabilities have been found in **every major operating system**, including Windows, Mac OS, various forms of Unix and Linux, OpenVMS, and others.

Vulnerabilități

- The only way to reduce the chance of a vulnerability being used against a system is through **constant vigilance**:
  - **careful system maintenance** (e.g. applying software patches),
  - **best practices in deployment** (e.g. the use of firewalls and access controls)
  - and **auditing** (both during development and throughout the deployment lifecycle).

Vulnerabilități

- Software tools
  - Altiris SecurityExpressions (Symantec)
  - Citadel Security Software (McAfee)
  - GFI LANguard (Network Security Scanner-GFI Software)
  - FusionVM (Critical Watch)
  - QualysGuard (Qualys)
  - Retina Network Security Scanner (Beyond Trust)
  - STAT Guardian Vulnerability Management Suite (Harris Corporation)

Amenințări

- Any good hacker can write the attack tool.
- A small minority of hackers have the technical expertise to write some of the attack tools commonly in use.
- There are lots of hacker web sites where one can get these tools.
- These sites try to outdo each other by designing the best, baddest, user-friendly site. Sites like:
  - www.metasploit.com,
  - www.insecure.org,
  - www.kali.org,
  - www.securityfocus.com

  are examples of where one can download a wide variety of attacks tools.
- These sites **make it easy for anyone** who knows how to use a browser to get these tools.

Cine este adversarul?

- **Hackerii** dispun de resurse de calcul și financiare scăzute și atacă sisteme în general doar motivați de dorința de a brava sau pentru amuzament.
- **Clienții unei rețele** au putere de calcul limitată și sunt motivați de interese economice, de exemplu: fraudarea valorii facturate în rețeaua termo-electrică, etc.
- **Comercianții** dispun de putere de calcul modestă și de resurse financiare apreciabile având interes în aflarea sau manipularea secretelor pentru câștigarea avantajelor financiare.
- **Crima organizată** are putere de calcul modestă și putere financiară ridicată având interes în alterarea parametrilor la care funcționează sistemele pentru câștigarea unor avantaje financiare.

Cine este adversarul?

- **Teroriștii** dispun de putere ridicată de calcul și financiară fiind motivați de rațiuni politico-religioase cu scopul de a răspândii panică și pagube de ordin financiar.
- **Guvernele** statelor adversare, dispun de putere de calcul și financiară ridicată, și mai mult, de operatori pricepuți și antrenați cu experiență în domeniu. Scopul acestora este în general de a afecta infrastructurile în atacuri complexe de natură fizică sau electronică.
- **Oamenii din sistem** sunt persoane care dețin informații de detaliu și au acces la elementele cheie în funcționare, sunt motivați în general de interese sau nemulțumiri de ordin salarial/financiar.
- O combinație a variantelor de mai sus este cel mai periculos tip de adversar; în practică este posibilă orice combinație și aceasta are cele mai mari șanse de succes într-un atac.

Cine este adversarul?

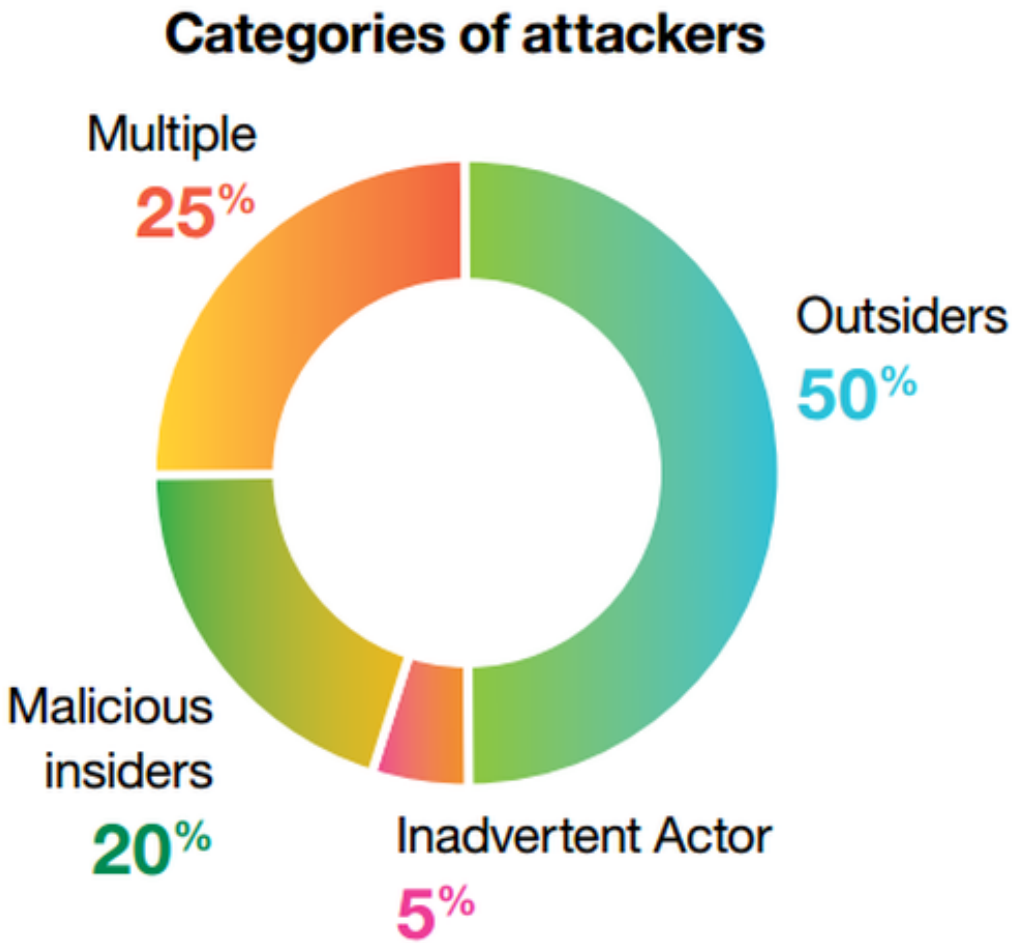


Figure: IBM Security Services Cyber Security Intelligence Index 2013

Cine este adversarul?

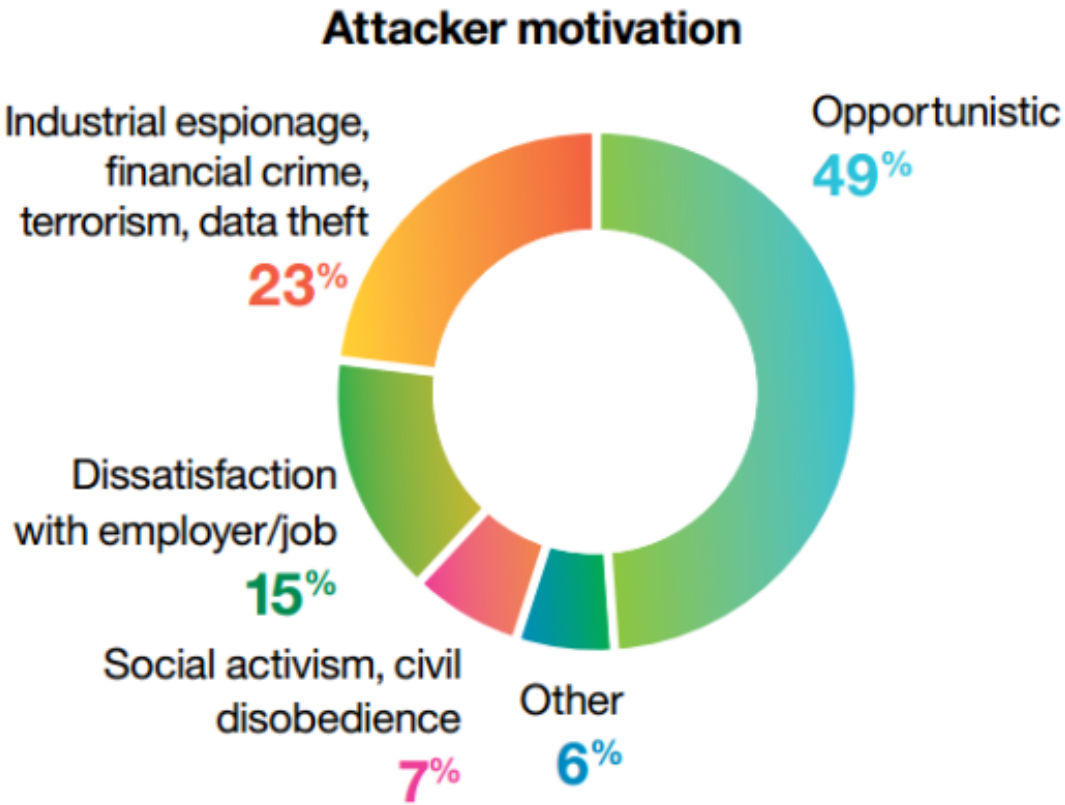


Figure: IBM Security Services Cyber Security Intelligence Index 2013

Amenințări

177 Security Threats identified by ENISA (2016)

- Identity theft (Identity Fraud/ Account)
- Denial of service
- Malicious code/ software/ activity
- Social Engineering
- Abuse of Information Leakage
- Manipulation of hardware and software
- Unauthorized installation of software
- Generation and use of rogue certificates (A false digital certificate used to secure Web sites)
- Compromising confidential information (data breaches)
- Remote activity (execution)
- Targeted attacks (APTs etc.)

...

Amenințări

- **Malware** is software designed to infiltrate or damage a computer system without the owner's consent.
  - It is a blend of the words "malicious" and "software".
  - The expression means a variety of forms of hostile, intrusive, or annoying software or program code.
- **Spyware** is a type of program that watches what users do with their computer and then sends that information over the internet.
  - Spyware can collect many different types of information about a user.
  - More benign programs can attempt to track what types of websites a user visits and send this information to an advertisement agency.
  - More malicious versions can try to record what a user types to try to intercept passwords or credit card numbers.
  - Yet other versions simply launch popup advertisements.

Amenințări

- **Adware** or advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed or while the application is being used.
- **Phishing** is a criminal activity using social engineering techniques.
  - Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.
  - Phishing is typically carried out using email or an instant message, although phone contact has been used as well.

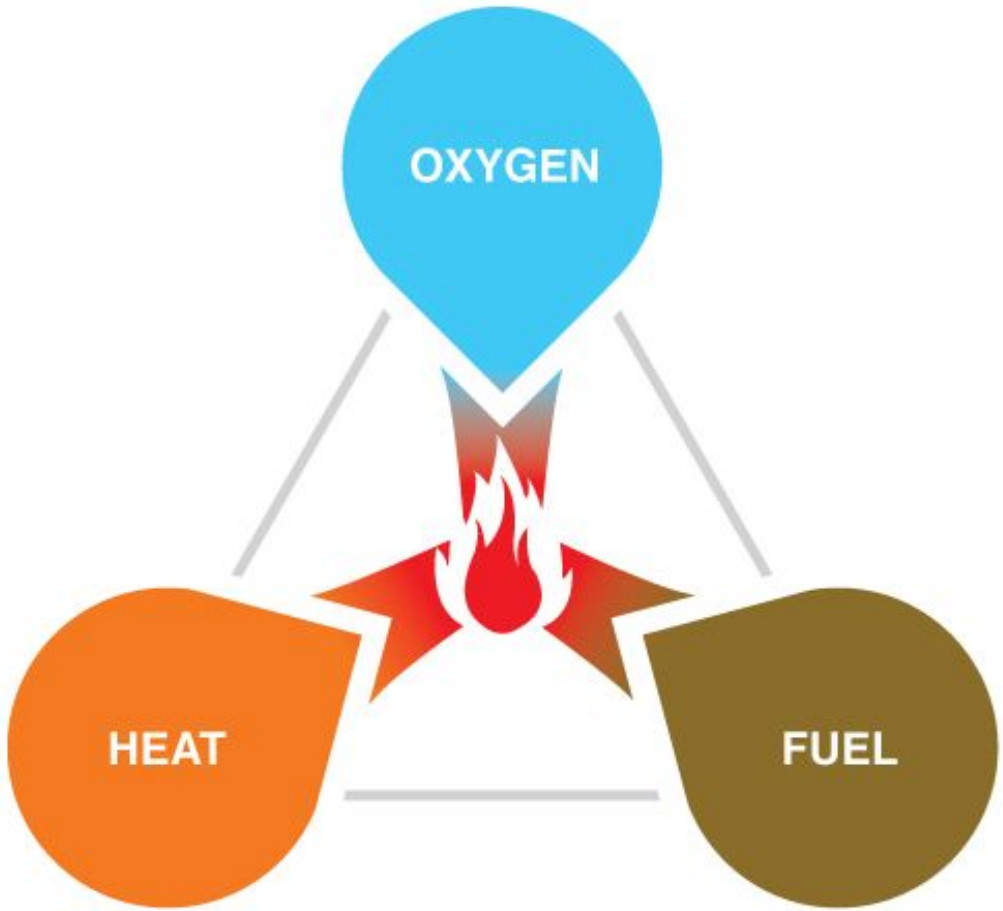
Amenințări

- **Ransomware** is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
  - some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse
  - more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them

Amenințări

- A **computer virus** is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code.
  - Viruses almost always corrupt or modify files on a targeted computer.
- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.
  - Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.
  - Worms almost always cause at least some harm to the network, even if only by consuming bandwidth.

Riscuri de securitate

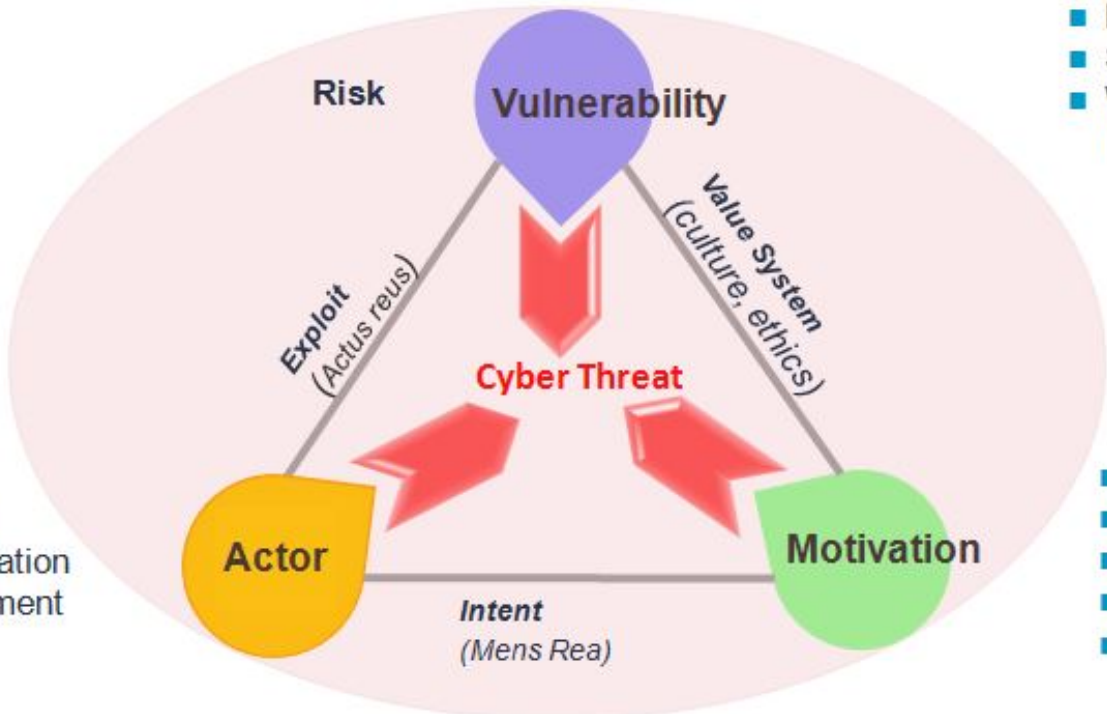


Riscuri de securitate

Atacator + Motivatie = Amenințare
Vulnerabilitate + Amenințare = Risc de securitate

- Concluzia de pana acum: există riscuri de securitate!
- Consecință a:
  - unor vulnerabilități în sistem
  - a existenței unor potentiali adversari cu o anumită motivație
- Riscurile de securitate trebuie acoperite cu garanții de securitate

Riscuri de securitate



- Design Flaws
- Software Bugs
- Weakness

(Human and Technology vectors)

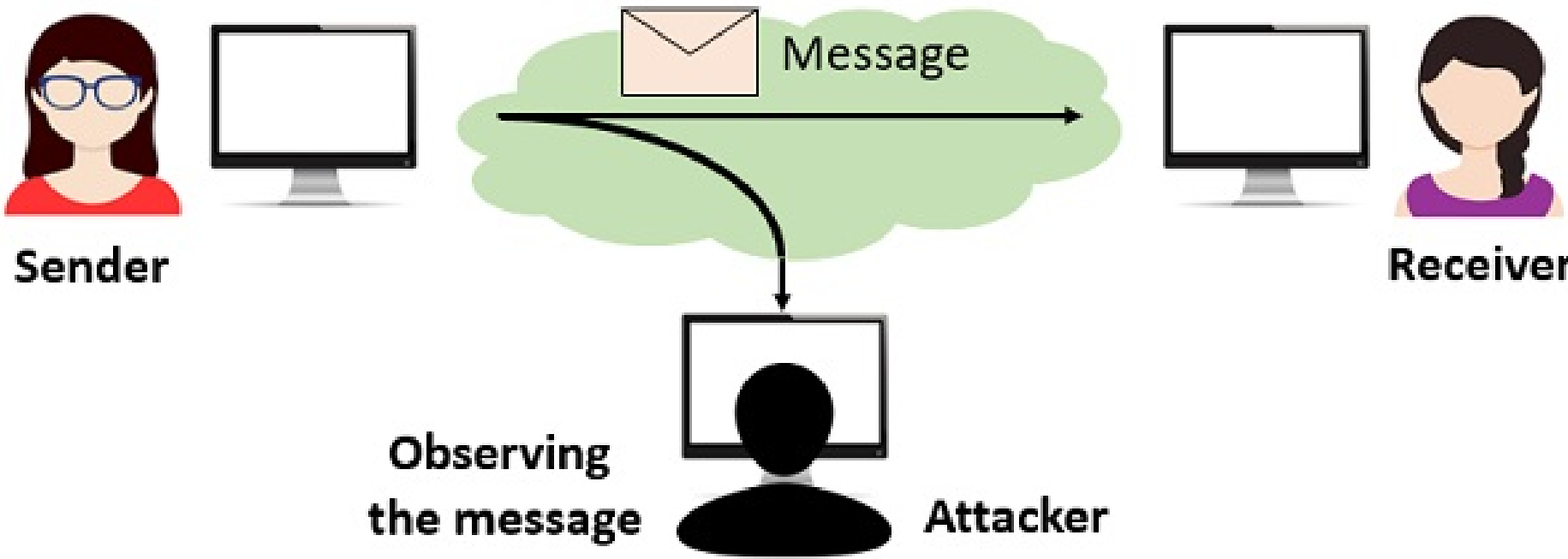
- Person
- Organization
- Government

- Financial
- Political
- Publicity
- (H)activism
- Revenge (malicious insider)

Atacuri cibernetice

- **Atac cibernetic** - agresiune asupra unui obiectiv de securitate
- Clasificare:
  - **atacuri pasive**
    - modalitate: interceptare
    - scop: citirea datelor, analiza de trafic, etc.
  - **atacuri active**
    - modalitate: întrerupere, modificare, fabricare
    - scop: impersonare, replay, modificare, denial of service

Atacuri pasive



Atacuri active

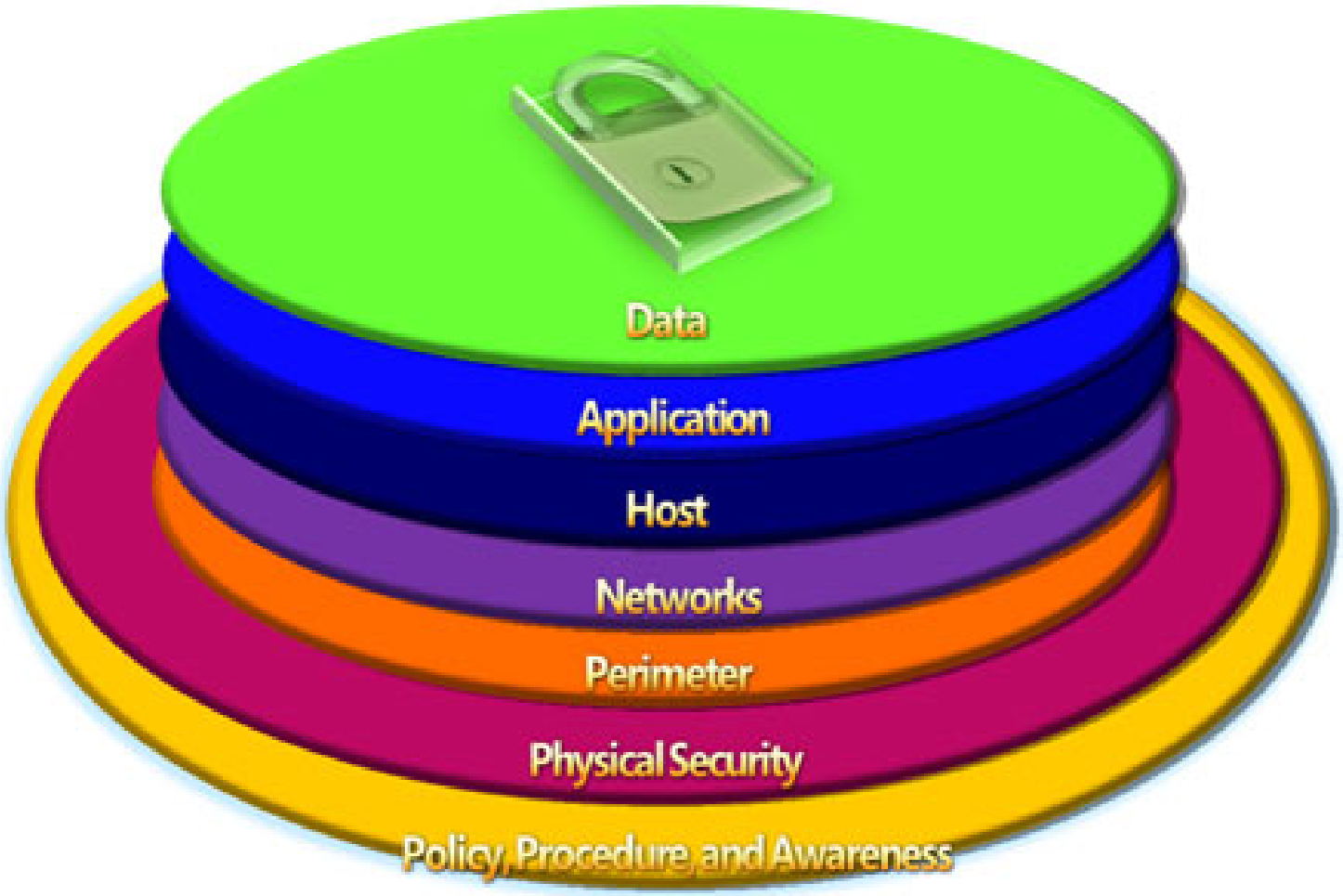
Atacuri pasive versus Atacuri active

Basis for comparison	**Active Attack**	**Passive Attack**
Basic	Active attack tries to change the system resources or affect their operation.	Passive attack tries to read or make use of information from the system but does not influence system resources.
Modification in the information	Yes	No
Harm to the system	Yes	No
Threat to	Integrity and availability	Confidentiality
Attack awareness	The entity (victim) gets informed about the attack.	The entity is unaware of the attack.
Task performed by the attacker	The transmission is captured by physically controlling the portion of a link.	Just need to observe the transmission.
Emphasis is on	Detection	Prevention

Security Reports

- **Symantec 2018 Internet Security Threat Report**, vol. 23
  https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
- **Akamai - State of the Internet Security Report**
  https://www.akamai.com/
  https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/
- **APWG Phishing Attack Trends Reports**
  https://www.antiphishing.org/
  https://www.antiphishing.org/resources/apwg-reports/

Layers of security



Layers of security

Data security

- concerns the protection of data from accidental or intentional but unauthorised modification, destruction or disclosure.
  - **Data Encryption** - converting the data into a code that cannot be easily read without a key that unlocks it.
    - disk encryption software
    - disk encryption hardware
  - **Data Masking** – masking certain areas of data so personnel without the required authorisation cannot look at it.
  - **Data Erasure** – ensuring that no longer used data is completely removed and cannot be recovered by unauthorised people.
  - **Data Backup** – creating copies of data so it can be recovered if the original copy is lost.

Layers of security

- the chief principle - to offer protection to a data user's collections or sources of data
- General Data Protection Regulations (**GDPR**) being enforced by the EU on 25 May 2018

Layers of security

Application security

- applications are links between the data and the user (or another application)
- **application security versus software security**

Layers of security

Software security (pre-deployment) activities include:

- Secure software design
- Development of **secure coding** guidelines for developers to follow
- Development of **secure configuration procedures and standards** for the deployment phase
- **Secure coding** that follows established guidelines
- **Validation of user input** and implementation of a suitable encoding strategy

Layers of security

Software security (pre-deployment) activities include:

- **User authentication**
- User **session management**
- Function level access control
- Use of strong cryptography to **secure data** at rest and in transit
- Validation of third-party components
- Arrest of any flaws in software design/architecture

Layers of security

Application security (post-deployment) activities include:

- Post deployment **security tests**
- Capture of flaws in software environment configuration
- **Malicious code detection** (implemented by the developer to create backdoor, time bomb)
- **Patch/upgrade**
- **IP filtering**
- Lock down executables
- Monitoring of programs at runtime to enforce the software use policy

Layers of security

Host security

Host Based Security Best Practices - Department of Computer Science Computing Guide - Princeton University:

- Install and configure a host based firewall
- Choose good passwords for any accounts on the system, and change any default or well known accounts on the machine
- Install and keep up with operating system patches and also hardware firmware patches
- Configure and continue to monitor logs on the device

Layers of security

- Disable services and accounts which are not being used, or are no longer necessary
- Replace insecure services (such as telnet, rsh, or rlogin) with more secure alternatives such as SSH
- Restrict access to services which cannot be disabled where possible
- Make and test backups of the system in a consistent manner

Layers of security

Network security

- consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources
  - authentication
  - firewalls
  - antivirus and antimalware software
  - intrusion detection systems (IDS) and intrusion prevention systems (IPS)
  - virtual private networks (VPN)
  - honeypots

Layers of security

Physical security

- security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm
- deter potential intruders (e.g. warning signs and perimeter markings)
  - Physical barriers - for external threats: fences, walls, and vehicle barriers
  - Combination barriers - for internal threats of fire, smoke migration as well as sabotage
  - Natural surveillance - architects seek to build spaces that are more open and visible to security personnel and authorized users, so that intruders/attackers are unable to perform unauthorized activity without being seen
  - Security lighting - intruders are less likely to enter well-lit areas for fear of being seen

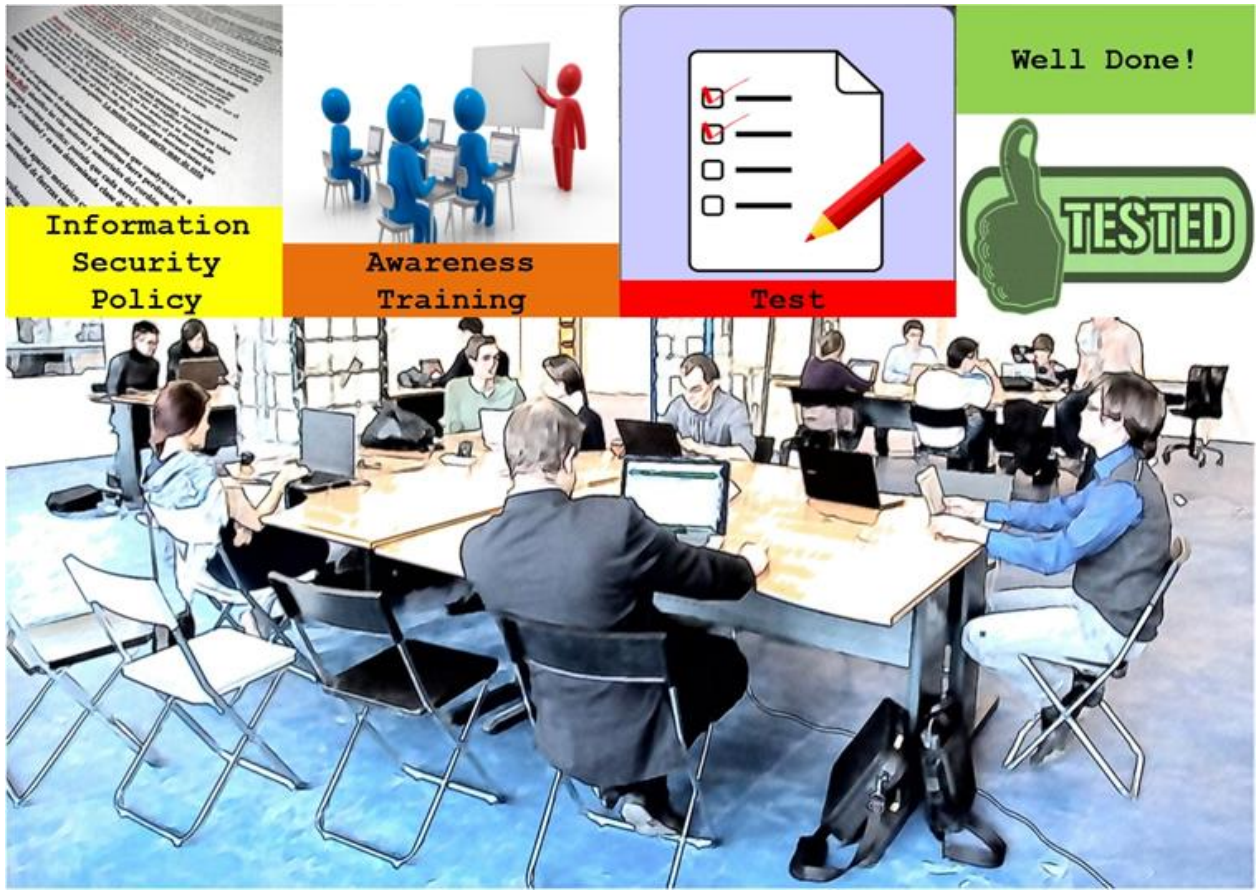
Layers of security

- detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems)
  - Alarm systems and sensors
  - Video surveillance
  - Access control
  - Security personnel
- trigger appropriate incident responses (e.g. by security guards and police)

Policy, Procedure and Awareness

- Information security policy is a **set of policies** issued by an organization to **ensure that all information technology users** within the domain of the organization or its networks **comply with rules and guidelines related to the security of the information** stored digitally at any point in the network or within the organization's boundaries of authority.
- Key Elements of an Information Security Policy (see references)

Policy, Procedure and Awareness



Policy, Procedure and Awareness

Key Elements of an Information Security Policy (see references)

- 1 Purpose
- 2 Scope
- 3 Information security objectives
- 4 Authority & Access Control Policy
- 5 Classification of Data
- 6 Data Support & Operations
- 7 Security Awareness Sessions
- 8 Responsibilities, Rights and Duties of Personnel
- 9 Reference to Relevant Legislation
- 10 Other Items

Program licenta - Ingineria și securitatea sistemelor informatice militare - ATM

Curriculum

- Fundamente de securitate cibernetică
- Securitatea sistemelor de operare
- Securitatea aplicațiilor de baze de date
- Tehnici de analiza de cod malițios
- Criptografie
- Testarea securității sistemelor informatice
- Managementul securității sistemelor informatice
- Sisteme biometrice

Program master - Securitatea Tehnologiei Informației - ATM

Curriculum

- Matematici aplicate in ingineria securitatii informatiilor
- Criptografie computationala
- Semnaturi electronice si infrastructuri de securitate
- Protocoale de securitate
- Securitatea retelelor de calculatoare
- Securitatea sistemelor si aplicatiilor
- Securitatea bazelor de date
- Sisteme biometrice
- Securitatea multimedia
- Securitatea sistemelor electronice de plati

Program master - Securitatea Tehnologiei Informației - ATM

- Reglementari privind securitatea cibernetica
- Strategii si politici de securitate cibernetica
- Razboi cibernetic
- Tehnologii pentru asigurarea continuitatii operationale
- Planificarea continuitatii operationale
- Evaluarea si managementul riscurilor
- Evaluarea si certificarea securitatii sistemelor
- Managementul securitatii informatiilor
- Criminalitatea informatica, colectarea si investigarea probelor

Information Security Standards and Best Practices

- consist of a specific **set of rules, procedures or conventions** that are agreed upon between parties to perform business operations more uniformly and effectively
- can be viewed as a **set of predetermined guidelines** in which the **issues, considerations and effects of doing something have already been analysed** by someone **authorised, experienced and qualified** in the specified area
- standards reflect industry best practices
- security and software development standards reflect industry best practices

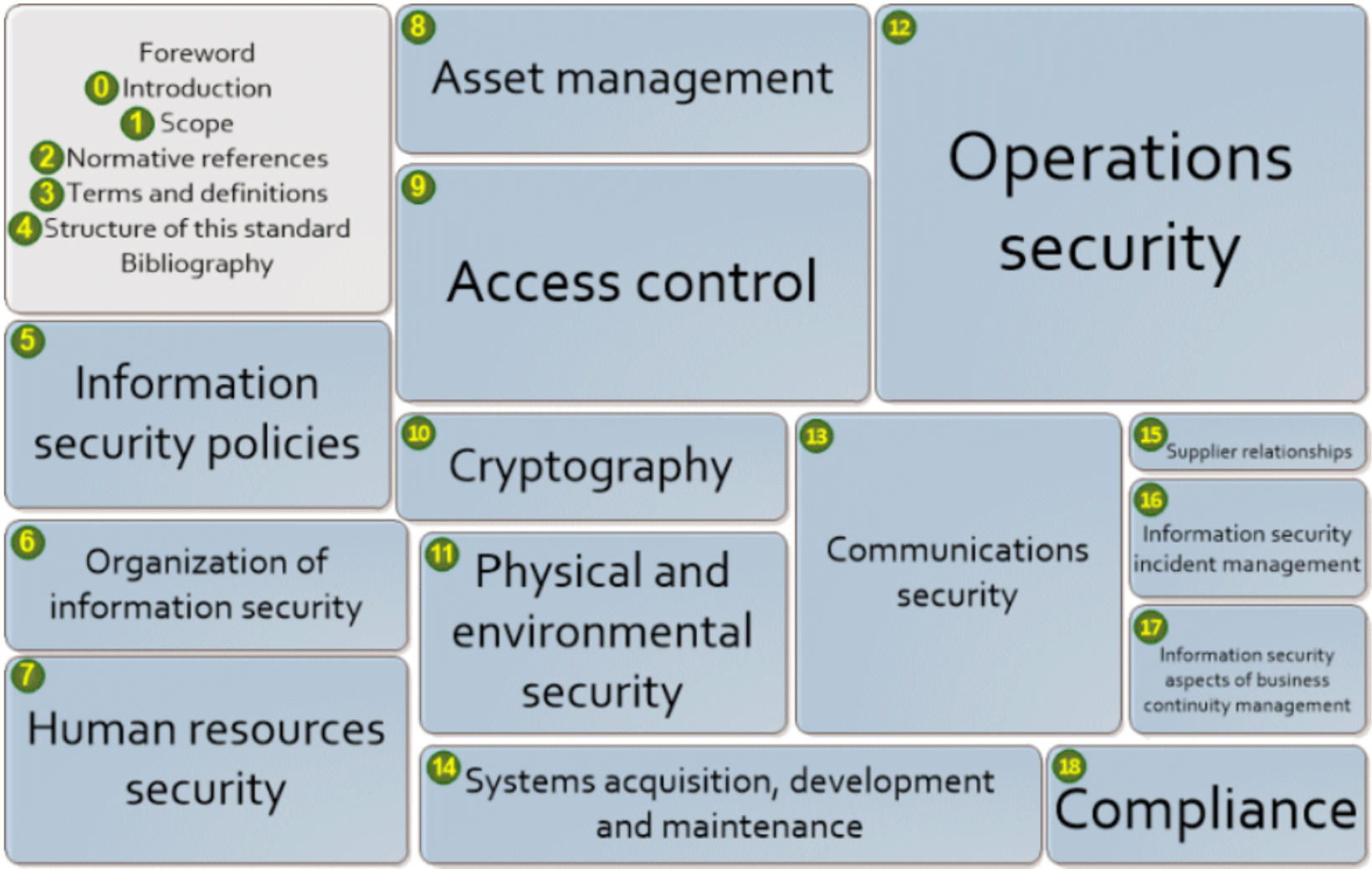
Information Security Standards and Best Practices

ISO/IEC 17799:2005 / ISO/IEC 27002:2007 / ISO/IEC 27002:2013

- ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition)
- provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems
- information security is defined within the standard in the context of the CIA triad
- objective: "**to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties including an organisation's customers**"

Information Security Standards and Best Practices

ISO/IEC 17799:2005 / ISO/IEC 27002:2007 / ISO/IEC 27002:2013



ISO/IEC TR 13335 guideline

- guidelines for the management of IT security
- Part 1: Concepts and Models
- Part 2: Managing and Planning IT security
- Part 3: Techniques for the Management of IT security – the complex topic of IT security risk assessment
- Part 4: Selection of Safeguards
- Part 5: Safeguards for External Connections

Information Security Standards and Best Practices

NIST security models

- **The NIST Cybersecurity Framework** (NIST CSF) "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes."
  - It is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties.
- **Special publication 800-12** provides a broad overview of computer security and control areas.
  - It also emphasizes the importance of the security controls and ways to implement them.
- **Special publication 800-14** describes common security principles that are used.
  - It provides a high level description of what should be incorporated within a computer security policy.
  - It describes what can be done to improve existing security as well as how to develop a new security practice.

Information Security Standards and Best Practices

- **Special publication 800-26** provides advice on how to manage IT security. Superseded by NIST SP 800-53 rev3. This document emphasizes the importance of self assessments as well as risk assessments.
- **Special publication 800-37** provides a new risk approach: "Guide for Applying the Risk Management Framework to Federal Information Systems".
- **Special publication 800-53** rev4, "Security and Privacy Controls for Federal Information Systems and Organizations", specifically addresses the 194 security controls that are applied to a system to make it "more secure".
- **Special Publication 800-82**, Revision 2, "Guide to Industrial Control System (ICS) Security" describes how to secure multiple types of Industrial Control Systems against cyber attacks while considering the performance, reliability and safety requirements specific to ICS.

Open systems security (interconnection standards)

- ITU-T X.800 Recommendation: Security architecture for Open Systems Interconnection
  - a general description of security services and the related mechanisms that can be used to provide these services
  - was developed specifically as the Open Systems Interconnection (OSI) security architecture, but the underlying concepts of X.800 have been shown to have much broader applicability
- ITU-T X.805 Recommendation: Security architecture for systems providing end-to-end communications

Bibliography

Cărți clasice despre Criptografie

- A.J. Menezes, P.C. Oorschot, S.A. Vanstone, (1996), Handbook of Applied Cryptography, CRC Press, 816 pagini, ISBN 0849385237.
- D. R. Stinson, (2005), Cryptography: Theory and Practice, Hall/CRC, 616 pagini, ISBN 1584885084.
- B. Schneier, (1996), Applied Cryptography, John Wiley & Sons, 784 pagini, ISBN 0471117099.
- N. Ferguson (2003), B. Schneier, Practical Cryptography, Wiley

Bibliography

Cărți moderne despre Criptografie

- W. Mao, (2003), Modern Cryptography: Theory and Practice, Prentice Hall, 740 pagini, ISBN 0130669431.
- Jonathan Katz, Yehuda Lindell, (2007), Introduction to Modern Cryptography: Principles and Protocols, Hall/CRC Cryptography and Network Security Series, ISBN-10: 1584885513, ISBN-13: 978-1584885511.

Cărți despre Teoria Numerelor

- V. Shoup, (2004), Computational Introduction to Number Theory and Algebra

Bibliography

Cărți despre Securitatea informației

- R. J. Anderson, (2001), Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 640 pagini, ISBN 0471389226.
- W. Stallings, (2005), Cryptography and Network Security (4th Edition), Prentice Hall, 592 pagini, ISBN 0131873164.
- M.Togan, I. Florea, Infrastructuri de Securitate pentru Servicii Electronice în Internet, Ed. Matrix-Rom, 2017

Bibliography

Articole științifice în cadrul conferințelor de specialitate

- Crypto `https://crypto.iacr.org/2018/`
- Eurocrypt `https://eurocrypt.iacr.org/2019/`
- Asiacrypt `https://asiacrypt.iacr.org/2018/`
- International Conference on Practice and Theory of Public Key Cryptography (PKC) `https://pkc.iacr.org/2018/`
- Fast Software Encryption (FSE) `https://fse.iacr.org/2018/`
- Theory of Cryptography (TCC) `https://tcc.iacr.org/2018/`
- Cryptographic Hardware and Embedded Systems (CHES) `https://ches.iacr.org/2018/`
- Real World Crypto Symposium (RWC) `https://rwc.iacr.org/`
- International Association for Cryptologic Research (IACR) - since 1982

Bibliography

Digital Libraries, search engines, indexing services (some are free)

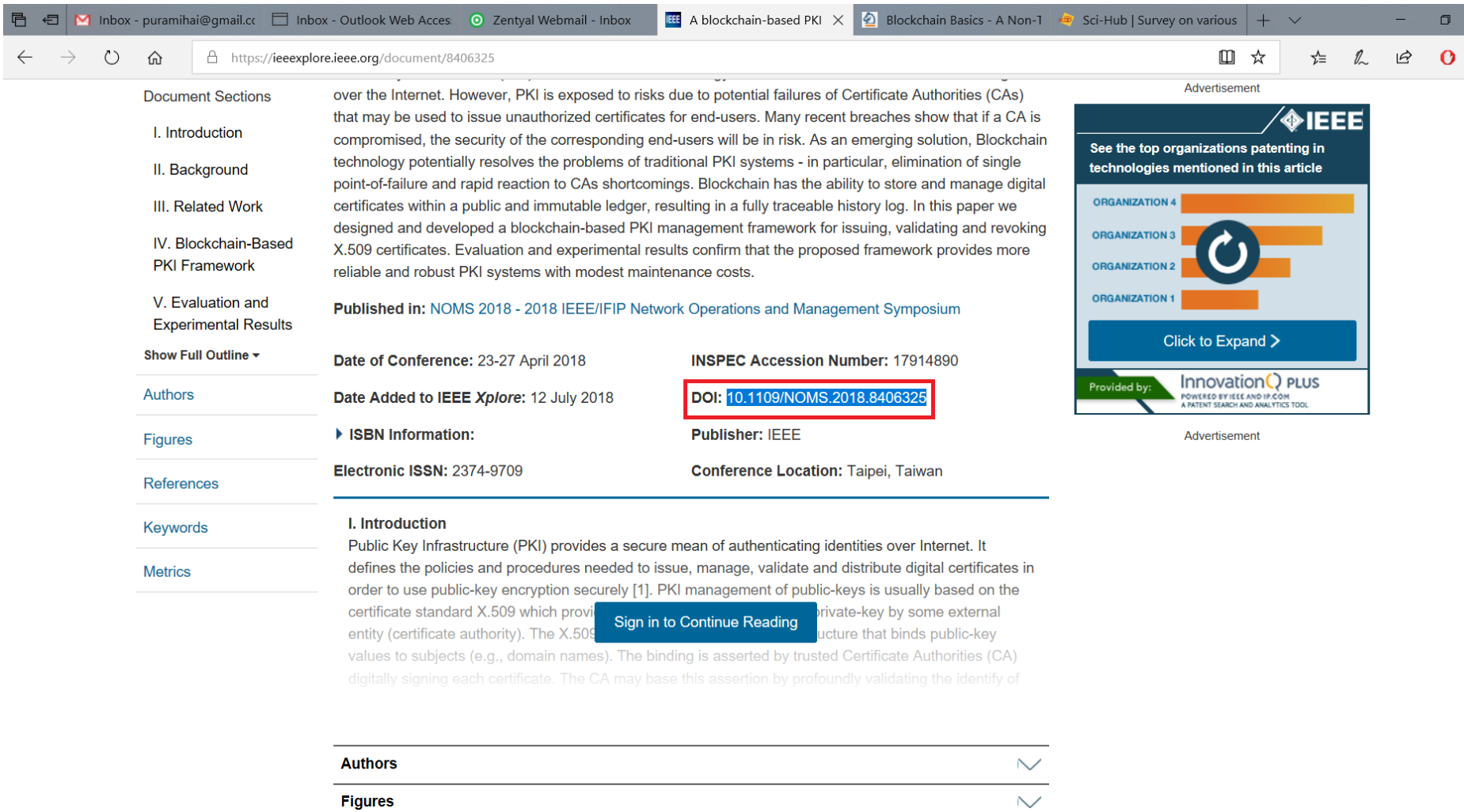
- Google Scholar `https://scholar.google.ro/`
- Microsoft Academic Search `https://academic.microsoft.com/`
- CiteSeerX `http://citeseerx.ist.psu.edu`
- Springer `https://www.springer.com/`
- IEEE Xplore Digital Library `https://ieeexplore.ieee.org/`
- SCI-HUB `https://sci-hub.tw/`
- etc.

Bibliography

Search for the content of an article using SCI-HUB

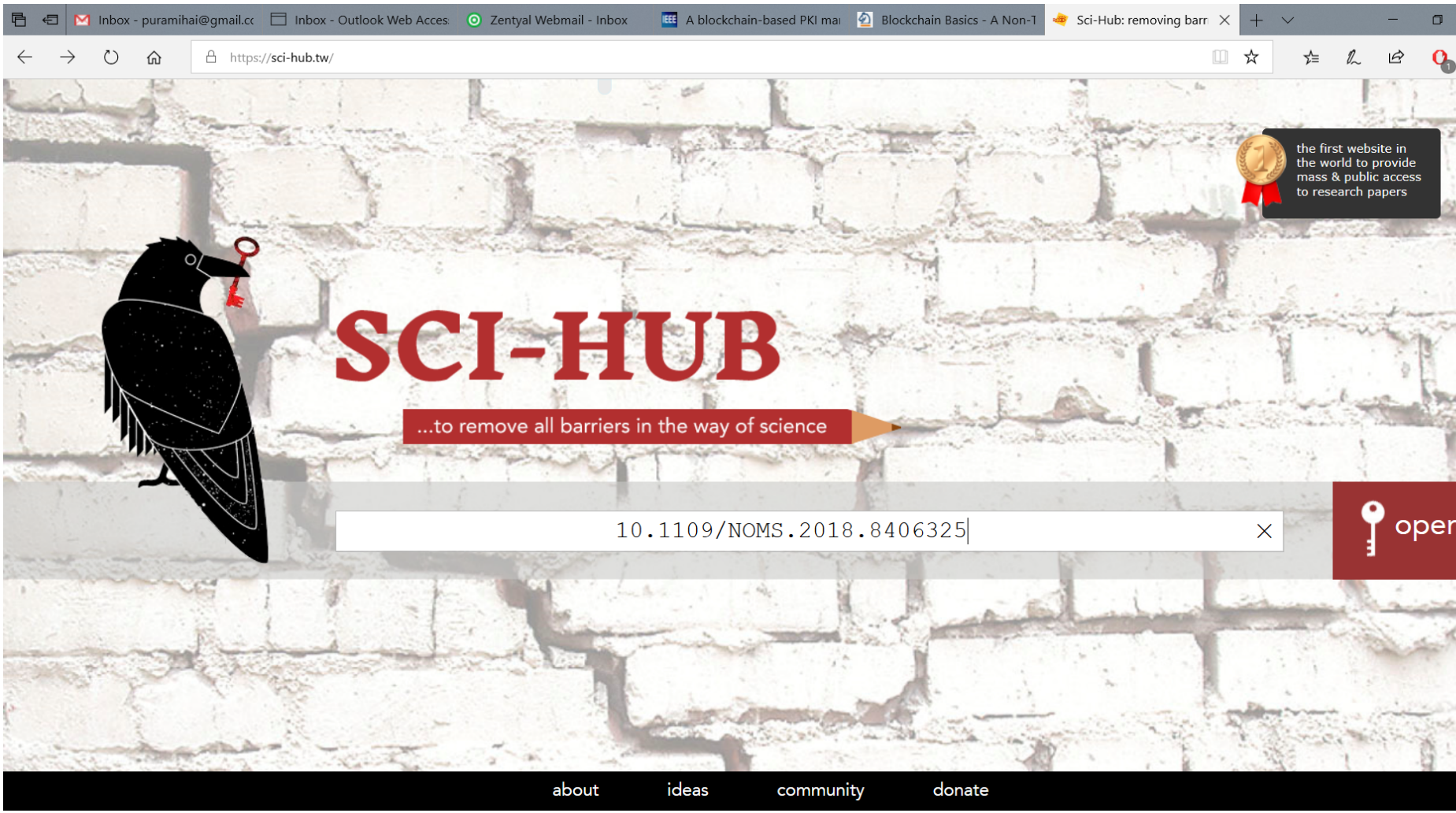
Bibliography

Search for the content of an article using SCI-HUB



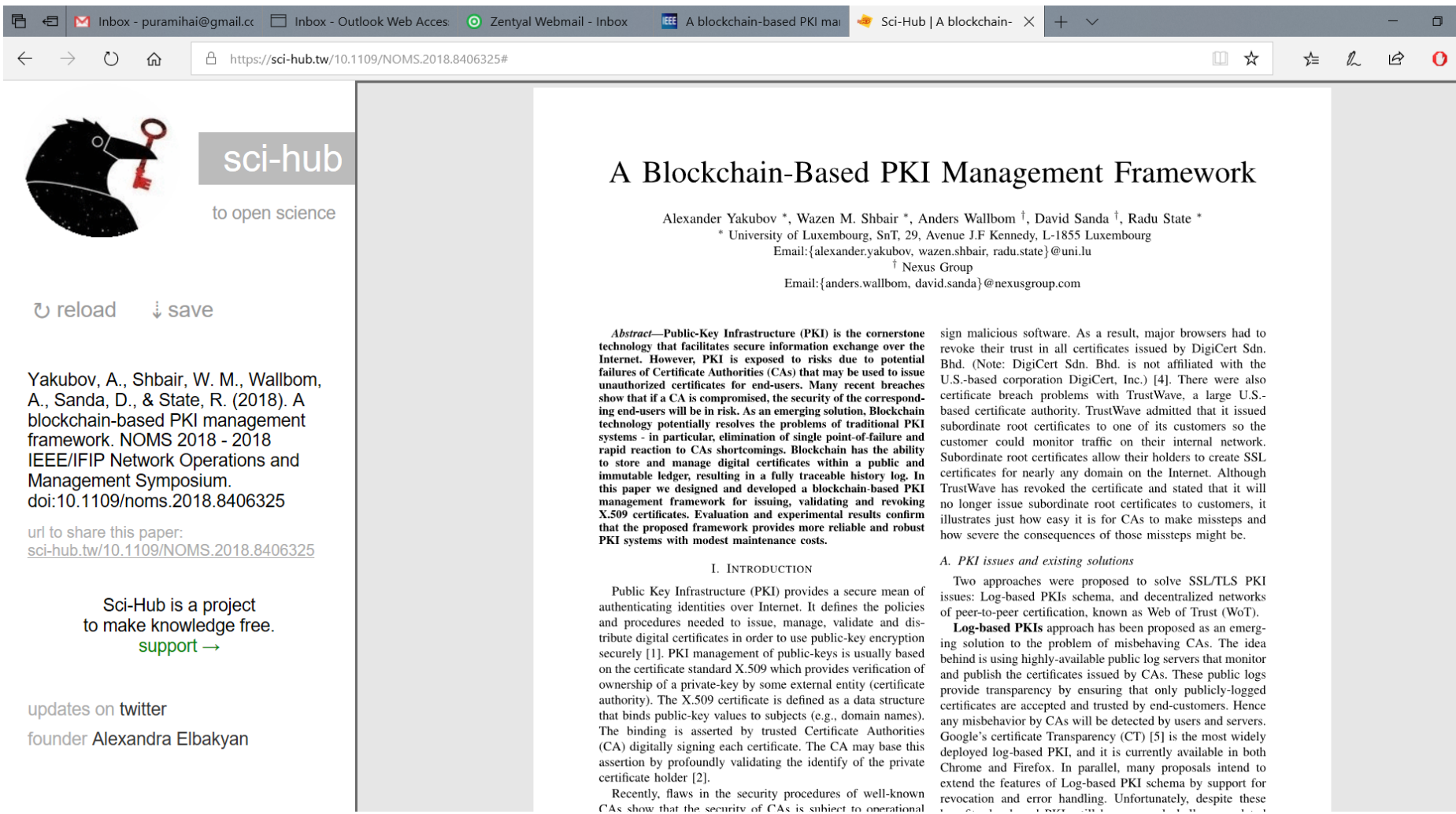
Bibliography

Search for the content of an article using SCI-HUB



Bibliography

Search for the content of an article using SCI-HUB



Epilogue

Security is a process, not a product.

Bruce Schneier, prefață la lucrarea Secrets and Lies

References

- Riham Yassin et al., Information Security https://www.slideshare.net/ahmedmoussaa/information-security-8332632
- Lynn Ann Futcher, A Model for Integrating Information Security into the Software Development Life Cycle, MD Thesis, Nelson Mandela Metropolitan University, 2007 https://www.academia.edu/745826/A_Model_for_Integrating_Information_Security_into_the_Software_Development_Life_Cycle
- ENISA Threat Taxonomy - A tool for structuring threat information, 2016 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-inf

References

- Illusion of CyberSecurity Part 2
  https://www.capgemini.com/2015/03/illusion-of-cybersecurity-part-2/
- Andra Zaharia, Corporate Security Checklist – a CEO's Guide to Cyber Security
  https://heimdalsecurity.com/blog/corporate-security-checklist-a-ceos-guide-to-cyber-secu
- Difference Between Active and Passive Attacks
  https://techdifferences.com/difference-between-active-and-passive-attacks.html
- Host Based Security Best Practices - Department of Computer Science Computing Guide - Princeton University:
  https://csguide.cs.princeton.edu/security/host

References

- Monika Chakraborty, Application security vs. software security: What's the difference?
  https://www.synopsys.com/blogs/software-security/application-security-vs-software-security/
- Key Elements of an Information Security Policy
  https://resources.infosecinstitute.com/key-elements-information-security-policy/
- ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition)
  http://www.iso27001security.com/html/27002.html
- Wikipedia