Dr. Marek Miśkiewicz

2020

Color scheme based on Dracula theme by Zeno Rocha

Marek Miśkiewicz 2021

mmiskiewicz@pjwstk.edu.pl

/public/mmiskiewicz/BSI

Exam in the form of a multiple-choice test based on the material presented in lectures

Literature

William Stalling - "Security of Information Systems. Principles and Practice", Helion 2019

William Stallings - Network Security Essentials: Applications and Standards, Pearson 2011

William Stallings - Cryptography and Network Security Principles and Practice, Pearson 2017

Simson Garfinkel, Alan Schwartz, Gene Spafford - Practical Unix & Internet Security, O'Reilly 2003

Janusz Stokłosa, Tomasz Bilski, Tadeusz Pankowski - Data Security in Information Systems, Wydawnictwo Naukowe PWN, Warsaw–Poznań 2001

A. J. Menezes, P. C. van Oorschot, S. A. Vanstone - Applied Cryptography, WNT, Warsaw, 2005

Michał Szychowiak - Security of Computer Systems, http://wazniak.mimuw.edu.pl

RFC 2828 defines information as "facts and ideas that can be represented (encoded) as various forms of data," and data as "information in a specific physical representation, usually as sequences of symbols that have a specific meaning; especially data that can be processed or produced by a computer."

RFC (Request for Comments) – a collection of technical and organizational documents in the form of a memorandum related to the Internet and computer networks. Each has a unique identification number, usually used for all references. The publication of RFCs is handled by the Internet Engineering Task Force.

Information is a Resource

Resources have specific value.

"Everything is information."

The protection of resources lies directly in the interest of the entity that owns them or is necessary to achieve designated goals.

Data as a physical representation of information should and must be protected.

Security (Computer Security)

Protection provided by an automated information system to achieve and maintain the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications).

Confidentiality

Ensures that private or confidential information is not made available or disclosed to unauthorized individuals (data confidentiality).

Ensures that individuals control or influence what information related to them may be collected and stored and by whom and to whom it may be disclosed (privacy).

NIST: Maintaining authorized restrictions on information access and disclosure, including means for protecting privacy and proprietary information. Loss of confidentiality is the unauthorized disclosure of information.

Integrity

Data has not been altered or destroyed in an unauthorized manner (data integrity).

The system performs its intended function in an unimpaired manner, free from unauthorized manipulation, intentional or unintentional (system integrity).

NIST: Protection against improper information modification or destruction, including ensuring information non-repudiation and authenticity. Loss of integrity is the unauthorized modification or destruction of information.

Availability

The property of being accessible and usable upon demand by an authorized entity.

NIST: Ensuring timely and reliable access to and use of information. Loss of availability is the disruption of access to or use of information or an information system.

Authenticity

The identity of a subject or resource is as claimed; applies to users, processes, systems, or institutions.

The property of being genuine, verified, and trusted; confidence in the validity of a transmission and its origin. Also means verifying whether users are who they claim to be.

Accountability

The property that ensures that the actions of an entity can be uniquely traced to that entity.

Accountability enables non-repudiation, deterrence, fault isolation, intrusion detection, and prevention.

Non-repudiation

Protection against false denial of a transaction:

By the sender of having sent the data

By the recipient of having received the data

Identification

The ability to distinguish users, e.g., in an operating system, users are identified by UID (user identifier).

Authentication

The process of verifying the identity of a user. Often based on:

What the user knows (knowledge factor)

What the user has (ownership factor)

Who or what the user is (inherence factor)

Authorization

The process of granting a user access rights to resources.

Access Control

A system composed of devices, software, and organizational procedures aimed at identifying the subject and monitoring adherence to access rights to resources.

Computer and Software Security

Cryptographic tools

Access control

Database and cloud resource security

Malware

Denial-of-Service attacks

IDS (Intrusion Detection Systems)

Firewalls and IPS (Intrusion Prevention Systems)

Software Security and Trusted Systems

Buffer Overflow attacks

Application security

Operating system security

Multilevel security and Trusted Computing

Risk Management

Security and risk management

Security policy

Infrastructure and resource security

Human resource security

Security audits

Network Security

Network security protocols and standards

Network authentication (PKI)

WiFi network security

What else does security mean?

A computer system is secure when:

The user can rely on it,

The software operates according to the specification.

Data entered into the system:

Maintains its attributes (sufficiently),

Is not lost,

Is not modified in an uncontrolled manner,

Is not accessed by an unauthorized entity.

Security vs. Reliability

A computer system is reliable when it is:

Secure (secure) - ensures data protection,

Safe (safe) - does not pose risks to the environment,

Available - operates continuously,

Reliable - resistant to attacks and failures.

ATTACKER

A person consciously attacking an information system to gain benefits (cracker, intruder, hacker, vandal, criminal).

Types of Attacks

PASSIVE - The attacker has access to data (also in the communication channel) - can read it but does not modify it.

ACTIVE - The attacker modifies or fabricates data.

MAN IN THE MIDDLE - The attacker intercepts data in the communication channel.

Types of Attacks

LOCAL - Initiated by an entity within the security perimeter ("insider"). A person with confidential information is authorized to access system resources but uses it in a manner not approved by those who granted permission.

REMOTE - Initiated "from outside" by an unauthorized or unauthenticated system user ("outsider"). Potential external attackers on the Internet are amateur pranksters, organized criminals, international terrorists, and hostile governments.

Forms of Attacks

EAVESDROPPING - Listening, often analyzing network traffic.

REPLAYING - Replaying, the attacker reuses previously collected data.

MASQUERADING - Impersonation, the attacker pretends to be a trusted or authenticated entity.

TAMPERING - Manipulation, the act of intentionally modifying (destroying, manipulating, or editing) data through unauthorized channels.

EXPLOITING - The attacker uses knowledge of a known software bug or a ready-made tool exploiting such a bug.

Phases of an Attack

Scanning – searching for weaknesses, e.g., probing services.

Target designation, e.g., unsecured service, known exploit.

System attack.

System modification allowing later return.

Trace removal.

Attack propagation.

Crimes Related to Security

Computer system break-in,

Unauthorized information acquisition,

Data and program destruction,

Sabotage (paralyzing operations) of the system,

Software piracy, software theft,

Computer fraud and forgery,

Computer espionage.

According to experts from the Council of Europe, computer crimes are divided into groups:

Fraud related to computer use,

Computer forgery,

Data or program destruction,

Computer sabotage,

Insulting others online,

Unauthorized system access (cracking, hacking),

Computer eavesdropping,

Illegal copying, distribution, or publication of legally protected computer programs,

Illegal copying of semiconductor topographies,

Impersonating other people or companies,

Data or program modification,

Computer espionage,

Unauthorized computer use,

Use of legally protected computer program without authorization,

Salami method.

Areas where legal protection of data and information is required

Personal data protection law

Educational law

Banking law

Financial law

Industrial law

Archival law

State informatization law

Telecommunications law

Public statistics law

Copyright law

Health protection law

Selected Legal Acts Requiring Information Security

Personal Data Protection Act

Classified Information Protection Act

Electronic Signature Act

Act on Providing Services by Electronic Means

Public Finance Act

Accounting Act

Access to Public Information Act

Educational Information System Act

National Archival Resource and Archives Act

Copyright and Related Rights Act

Criminal Code - Chapter XXXIII concerns crimes against information protection

Law

Art. 267. §1. Whoever, without authorization, obtains information not intended for them by opening a closed letter, connecting to a wire used for transmitting information, or breaking electronic, magnetic, or other special protection, shall be subject to a fine, restriction of liberty, or imprisonment for up to 2 years.

§2. The same penalty shall apply to anyone who, in order to obtain information to which they are not entitled, installs or uses a listening device, visual device, or other special device.

§3. The same penalty shall apply to anyone who discloses to another person information obtained in the manner specified in § 1 or 2.

§4. Prosecution of the crime specified in § 1–3 is initiated upon the request of the injured party.

Law

Art. 268. §1. Whoever, without authorization, destroys, damages, deletes, or alters the record of significant information or otherwise prevents or significantly hinders an authorized person from accessing it, shall be subject to a fine, restriction of liberty, or imprisonment for up to 2 years.

§2. If the act specified in § 1 concerns a record on a computer medium, the perpetrator shall be subject to imprisonment for up to 3 years.

§3. Whoever, by committing the act specified in § 1 or 2, causes significant property damage, shall be subject to imprisonment from 3 months to 5 years.

§4. Prosecution of the crime specified in § 1–3 is initiated upon the request of the injured party.

Law

Art. 269. §1. Whoever, on a computer medium, destroys, damages, deletes, or alters a record of special importance to national defense, communication security, government administration functioning, another state authority, or local government administration, or disrupts or prevents the automatic collection or transmission of such information, shall be subject to imprisonment from 6 months to 8 years.

§2. The same penalty shall apply to anyone who commits the act specified in § 1 by destroying or replacing a medium of information or destroying or damaging a device used for automatic processing, collection, or transmission of information.

Law

Art. 287. §1. Whoever, for the purpose of gaining financial benefits or causing harm to another person, without authorization, influences the automatic processing, collection, or transmission of information or changes, deletes, or introduces a new record on a computer medium, shall be subject to imprisonment from 3 months to 5 years.

§2. In the case of a minor offense, the perpetrator shall be subject to a fine, restriction of liberty, or imprisonment for up to 1 year.

§3. If the fraud is committed to the detriment of a close person, prosecution is initiated upon the request of the injured party.

Law Requires Us to Do Something

How to Do It

Standards

ISO/IEC 270XX Family of Standards

ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements

PN-EN ISO/IEC 27001:2017-06 Information technology -- Security techniques -- Information security management systems -- Requirements

ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

PN-EN ISO/IEC 27002:2017-06 Information technology -- Security techniques -- Code of practice for information security controls

ISO/IEC 27003:2017 Information technology -- Security techniques -- Information security management systems -- Guidance

ISO/IEC 27004:2016 Information security management -- Monitoring, measurement, analysis, and evaluation

PN-ISO/IEC 27004:2017-07 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis, and evaluation

ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management

PN-ISO/IEC 27005:2014-01 Information technology -- Security techniques -- Information security risk management

ISO/IEC 27006:2015 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

PN-ISO/IEC 27006:2016-12 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2017 Information technology -- Security techniques -- Guidelines for information security management systems auditing

PN-ISO/IEC 27013:2014-01 Information technology -- Security techniques -- Guidelines for the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

PN-ISO/IEC 27017:2017-07 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity

www.pkn.pl www.iso.org

Common Criteria

International standard Common Criteria (CC) defines evaluation criteria for the security of IT systems.

ISO/IEC 15408 Common Criteria for Information Security Evaluation (Common Criteria for Information Technology Security Evaluation) consists of three parts:

ISO/IEC 15408-1 (CC Part 1) includes: introduction, description of the risk management model, and creation of justified trust and the structure of basic documents, developed for the certification of a product or system;

ISO/IEC 15408-2 (CC Part 2) contains a catalog of functional components for modeling security functional requirements;

ISO/IEC 15408-3 (CC Part 3) contains a catalog of assurance components for modeling trust requirements for security functions.

Common Criteria

Common Criteria recommends the use of rigorous requirements for the development, production, and maintenance processes of IT products so that users can be sure that the security measures used in these products are correct and effective. Product trust is further confirmed by independent evaluation and certification performed by accredited laboratories and institutions.

PN-ISO/IEC 15408-1:2016-10 Information technology -- Security techniques -- Criteria for the evaluation of IT security -- Part 1: Introduction and general model

PN-ISO/IEC 15408-2:2016-10 Information technology -- Security techniques -- Criteria for the evaluation of IT security -- Part 2: Security functional components

PN-ISO/IEC 15408-3:2016-10 Information technology -- Security techniques -- Criteria for the evaluation of IT security -- Part 3: Security assurance components

Orange Book

Trusted Computer System Evaluation Criteria

The document was initiated by the National Security Agency of the Department of Defense (NSA DoD) and the National Institute of Standards and Technology (NIST). Published in 1983 in the

form of an orange booklet, which gave it its unofficial name. This document describes the basic requirements that protection measures in a computer system must meet to process protected information. The document was updated in 1985 and then replaced by the international standard Common Criteria.

Orange Book

Trusted Computer System Evaluation Criteria

The document focuses on ways to ensure the confidentiality of information and distinguishes 4 levels of criteria:

D1 — C1 C2 — B1 B2 B3 — A1

Orange Book

Trusted Computer System Evaluation Criteria

D1

Minimal Protection

Includes systems that only have physical protection against access. In systems of this class, anyone with physical access to the computer has unrestricted access to all its resources. An example of such a system is an IBM PC with an MS-DOS system without password protection.

Orange Book

Trusted Computer System Evaluation Criteria

C1

Discretionary Protection

Provides basic security for users working in a multi-user environment and processing data of the same level of secrecy. C1 systems use hardware or software mechanisms for user identification and authorization. The system protects identification data and passwords from unauthorized access. User identification should be used in every access mode to the resource. Each user has full control over the objects they own. Most Unix systems fall into this category.

Orange Book

Trusted Computer System Evaluation Criteria

C2

Controlled Access Protection. Provides for the recording of events related to security for each user individually and means to determine the scope of recorded events (Audit subsystem). Systems of this class have event logging and extended user identification. The C2 level also imposes additional requirements for password encryption, which must be hidden in the system (inaccessible to regular users).

Orange Book

Trusted Computer System Evaluation Criteria

B1

Labeled Security Protection. The first level introducing different degrees of secrecy (e.g., "secret", "confidential", etc.). In systems of this class, labels indicating the degree of secrecy for subjects (processes, users) and objects (files) are used. Access to data recorded in a file is granted to subjects based on label analysis. Labeled processes, files, and devices contain a full description of the secrecy level of the object and its category.

Orange Book

Trusted Computer System Evaluation Criteria

B2

Structured Protection.

Defines requirements including labeling each object in the system, structural, formalized security policy, conducting penetration tests to detect potential "holes" in the model. Authorization for changes to access permissions to objects is reserved for authorized users. It is not possible to recover deleted information.

Orange Book

Trusted Computer System Evaluation Criteria

B3

Security Domains.

Enforces the isolation of certain areas. Parts of the system essential for secure processing should be separated from parts providing certain useful functions to the user but unrelated to secure processing. Memory management mechanisms protect a given domain from access or modification by software operating in another domain. A multi-layered structure of abstract, mutually separated machines with distinct protection rights is created. The design process of the system is also subject to oversight to meet requirements.

Orange Book

Trusted Computer System Evaluation Criteria

A1

Verified Design

Requires a formal mathematical proof of the security model correctness, as well as a formal system specification and secure distribution. So far, very few systems have obtained this level of certification.

There is no such thing as absolute security.

Security is always linked to economics.

Maintain the level of all protections at the same level.

The attacker will not "break through" the security, they will bypass it.

Use multi-level protections.

Do not rely on security through "obscurity."

Do not give a person or program more privileges than they need to complete the task.

Security should be an integral part of the design.

A program or protocol is considered "unsafe" until its security is proven.

Security is a compromise with convenience.

Keep it simple

Security of Information Systems

Dr. Marek Miśkiewicz

October 23, 2020

Institute of Computer Science, UMCS

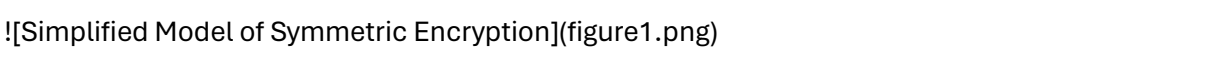
Elements of Cryptography

- Symmetric and Stream Cryptography
- Message Authentication
- Asymmetric Cryptography - Public and Private Keys
- Digital Signatures

Elements of Cryptography

Symmetric Cryptography

- The basic method for ensuring the confidentiality of transmitted data.
- Based on a single encryption key.
- To ensure security, the following are required:
  - A strong algorithm
  - The sender and receiver must have (share) the same key (kept secret).



Symmetric Cryptography - Attacks

- Cryptanalytic attacks:
  - Based on:
    - The "nature" of the algorithm
    - Knowledge about the characteristics of plaintext
    - Samples of plaintext and ciphertext
  - Use algorithm features to discover properties of the plaintext or key used. The goal is often to reveal the key, compromising all ciphertexts associated with that key.

- Brute-force attacks:

  - Scans the entire key space, decrypting the ciphertext to find "sensible" plaintext. Typically, examining half of all keys is sufficient.

Comparison of DES, 3DES, and AES

Algorithm	Plaintext Block Size (bits)	Ciphertext Block Size (bits)	Key Size (bits)
DES	64	64	56
3DES	64	64	112, 168
AES	128	128	128, 192, 256

Symmetric Cryptography

- DES (Data Encryption Standard):
  - Until recently, the most widely used.
  - Uses 64-bit plaintext blocks and a 56-bit key, producing a 64-bit ciphertext.
  - Vulnerabilities:
    - Most studied algorithm (analytically)
    - With modern computational speed, the key length is "woefully" insufficient.

Triple DES (3DES)

- Repeats the DES algorithm three times using two or three unique keys.
- ANSI standard X9.17 for financial operations (1985).
- Advantages:
  - 168-bit key makes brute-force attacks significantly harder.
  - Based on the ordinary DES algorithm.
- Disadvantages:
  - Slow hardware implementation.
  - Still only 64-bit data blocks.

Advanced Encryption Standard (AES)

- Need to replace 3DES, which was not suitable for long-term use.

- NIST competition:

  - Security level no lower than 3DES

  - High performance (algorithm speed)

  - Symmetric block cipher

  - 128-bit blocks and key sizes of 128, 192, 256 bits

- Rijndael (November 2001) chosen as AES.

Security Issues

- Typically, symmetric encryption is used for data blocks of 64 or 128 bits, necessitating dividing the input data into blocks.

- ECB mode (Electronic Code Book) - each block is encrypted with the same key - the simplest but most dangerous approach, as multiple ciphertexts are encrypted with the same key.

- CBC mode (Cipher Block Chaining) - successive plaintext blocks are XORed with preceding encrypted blocks before encryption.

ECB Mode

CBC Mode

CFB Mode

OFB Mode

PCBC Mode

CTR Mode

Block Ciphers vs. Stream Ciphers

- Block ciphers:

  - Input data is processed one block at a time.

  - An output block is created for each input block.

  - The key is used multiple times.

  - Widely used.

- Stream ciphers:

  - Encrypt input data continuously.

  - Byte (bit) input → byte (bit) output.

  - Very high speed ↔ very simple algorithms.

  - Maximum ciphertext entropy for a "random key".

At Home

- Three examples of block ciphers.

- Three examples of stream ciphers.

Message Authentication

- Protection against active attacks.

- The message is verified as "authentic":

  - The content has not been altered - integrity.

  - The source is confirmed - non-repudiation.

  - Time and proper sequence.

- Symmetric cryptography can be used (assuming only the sender and receiver share the key).

Message Authentication Without Confidentiality

- Encrypting a message does not provide a secure form of authentication.

- Authentication and confidentiality can be combined in one algorithm by encrypting the message and the authentication signature.

- Most commonly, the message signature is forgotten through a separate function.

- Situations where authentication without encryption may be preferred:

  - Plaintext messages broadcast to many recipients (network).

  - "Heavy load" - no time for decryption.

  - Signing computer programs.

Symmetric Cryptography

Asymmetric Cryptography

- Concept proposed by Diffie and Hellman in 1976.
- Based on discrete algebra.
- Asymmetry:
  - Two "paired keys":
    - Private key - kept secret.
    - Public key - publicly available.
  - Solves the key distribution problem.

- Systems based on the public key concept:
  - RSA: Digital signature, key distribution, symmetric key encryption.
  - Diffie-Hellman: Key distribution only.
  - DSS: Digital signature only.
  - Elliptic Curve: Digital signature, key distribution, symmetric key encryption.

Asymmetric Cryptography Requirements

- Easy calculation of key pairs.
- Efficient public key distribution system.
- High computational complexity for attempts to derive the private key from the public key.
- Easy decryption of the message using the private key.
- Strong encryption algorithm.

Asymmetric Cryptography Algorithms

- RSA - Rivest, Shamir, Adleman:
  - Invented in 1977 and widely used.
  - Based on the problem of factoring (data are numbers from the range of 0 to n−1 for some n).

- Successful factorization of a 768-bit key.

- Accepted keys (for security reasons): 2048 and 4096 bits.

- Significant threat from "quantum computers".

- Diffie-Hellman Key Exchange Protocol:

- Allows two users to securely exchange a key or secret - the only function of the algorithm (extensions possible for more users).

- An intruder in the communication channel cannot determine the key value from intercepted data → however, a "man-in-the-middle" attack is possible.

Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:

- "The result of a cryptographic transformation of data that, when implemented properly, provides a mechanism for verifying the origin, data integrity, and non-repudiation of the signature."

- A digital signature is a data-dependent bit pattern, generated by an algorithm as a function of a file, message, or other data block.

Digital Signatures

- FIPS 186-4 specifies the use of one of three digital signature algorithms:

- DSA - Digital Signature Algorithm.

- RSA Digital Signature Algorithm.

- ECDSA - Elliptic Curve Digital Signature Algorithm.

Certificate Authentication

Digital Envelope - Encrypting Large Amounts of Data

- Symmetric cryptography has an input data limit for encryption!

At Home

- GnuPG and PGP.

- Public Key Infrastructure.

Information Systems Security

Dr. Marek Miśkiewicz

November 15, 2020

Institute of Computer Science UMCS

MIME and S/MIME

MIME

MIME (Multipurpose Internet Mail Extension) is an extension of the old RFC 822 standard (Standard for The Format of ARPA Internet Text Messages, 1982) containing the specification of the internet mail format. RFC 822 defines a simple header with fields such as To, From, Subject, and other fields used to route email messages through the internet.

MIME provides many new header fields that define information about the content of the message, including content format and encoding, facilitating its transmission.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extension) is a set of additional MIME content types. New features include:

- Enveloped data - encrypted content and associated keys

- Signed data - encoded message + signed digest

- Clear-signed data - cleartext message + encoded signed digest

- Signed and enveloped data - nesting of signed and encrypted entities

S/MIME Content Types:

Type	Subtype	S/MIME Parameter	Description
Multipart	Signed		Clear-signed message in two parts: one is the message, the other is the signature
Application	pkcs7-mime	signedData	Signed S/MIME entity
		envelopedData	Encrypted S/MIME entity
		degenerated singleData	Entity containing only public key certificates
		CompressedData	Compressed S/MIME entity
	pkcs7-signature		Content type of the signed message part

Encryption and signing of messages

Decryption and verification of messages

SSL and TLS

SSL - Secure Sockets Layer

TLS - Transport Layer Security

- The most commonly used security mechanisms

- A set of general-purpose protocols based on the TCP protocol

- SSL evolved into TLS over time (RFC 4346)

- Mechanisms can be implemented as protocol components or used independently

TLS Protocol Stack

Session - a connection between a client and a server

- Sessions are created using the Handshake protocol

- Sessions define a set of cryptographic security parameters that can be shared across multiple connections

- Sessions are used to avoid costly negotiations of new security parameters for each connection.

Connection - enables transport (according to the OSI layer model) that provides the appropriate type of service. In TLS, such connections are peer-to-peer relationships. Connections are short-lived. Each connection is associated with one session.

TLS Protocols

The Record Protocol (SSL protocol) provides:

- Confidentiality

- Integrity

During Handshake, keys for symmetric encryption of payloads and a secret key used to create MAC are defined.

TLS Record Protocol Operation

Change Cipher Spec Protocol

- The simplest protocol

- Consists of one message containing one byte with the value 1

- The only purpose of this message is to copy the pending state to the current state

- Updates the cipher suite in use

Alert Protocol - used to convey TLS-related alerts to the peer entity.

Consists of two bytes:

- First byte: 1 - warning, 2 - critical error

- Second byte: message code

For example: Critical alert: invalid MAC address

Non-critical alert: close_notify (the sender will not send any more messages in this connection)

Handshake Protocol allows the server and client to authenticate each other and negotiate encryption and MAC algorithms, exchange cryptographic keys to be used for protecting data sent in the TLS record.

The Handshake protocol is called before any data is transmitted using TLS.

Phase I

Mutual authentication

Phase II

Negotiation of encryption and MAC algorithm

Phase III

Exchange of cryptographic keys

TLS Handshake

ECDHE Elliptic Curve Diffie-Hellman Exchange - key exchange

RSA Rivest-Shamir-Adleman Cryptosystem - public key authentication mechanism (for certificate verification)

AES_128_GCM cipher_key size_Galois/Counter Mode encryption system

SHA256 hash function used for MAC

TLS Handshake Operation, Part 1

TLS Handshake Operation, Part 2

TLS Heartbeat

Heartbeat Protocol:

- A periodic signal generated by hardware or software to indicate normal operation or synchronization with other parts of the system

- Usually used to monitor the availability of a protocol entity

- Defined in 2012 in RFC 6250

- Operates based on the TLS Record protocol, its use is established during Phase 1 of the Handshake protocol (heartbeat_request and heartbeat_response).

- Each partner indicates whether and how it supports the "heartbeat"

TLS Heartbeat

The Heartbeat protocol serves two purposes:

- Ensures the sender that the recipient is "alive"

- Generates activity in the connection during idle periods

Attacks on the TLS Protocol

Attack vectors:

- Handshake Protocol

- Record Protocol and application data protocols

- PKI (Public Key Infrastructure)

- Others

Heartbleed Attack

Heartbleed Attack - exploit (source: BAE Systems)

HTTPS

HTTPS - HTTP over SSL (port 443)

- Combination of HTTP and SSL to implement secure communication between a web browser and a web server

- Built into all modern web browsers (URLs start with https://)

- Documented in RFC 2818, HTTP Over TLS

- The agent acting as the HTTP client also acts as the TLS client

- Closing an HTTPS connection requires TLS to close the connection with the peer TLS entity on the remote side, which will involve closing the underlying TCP connection

What is encrypted:

- URL of the requested document

- Contents of the document

- Contents of browser forms (filled in by the browser user)

- Cookies sent from browser to server and from server to browser

- Contents of HTTP header

IPsec

Why IPsec?

- Authentication - the received packet was actually sent by the party identified in the packet header as the source (also integrity)

- Confidentiality - allows communicating nodes to encrypt messages to prevent eavesdropping by third parties

- Key management - security of key exchange

The current version of IPsec, referred to as IPsecv3, includes authentication and confidentiality. Key management is provided by the Internet Key Exchange standard - IKEv2.

The main feature of the IPsec protocol, which allows it to support various applications, is its ability to encrypt and (or) authenticate all traffic at the IP level. This enables securing all applications, including remote login, client-server applications, email, file transfer function, web access, and similar.

When IPsec is implemented on a firewall or router, it provides "robust" security that can be applied to the entire protected area. Traffic with the company or workgroup does not involve processing overhead related to security.

IPsec in a firewall is resistant to bypass if all traffic from the outside must use the IP protocol, and the firewall is the only point where network traffic enters and exits the organization.

IPsec is "below" the transport layer (TCP, UDP) and therefore is transparent to applications. There is no need to change software in the user or server system if IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, it does not affect higher-layer software, including applications.

IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue key-related materials to individual users, or revoke key materials when users leave the organization.

If necessary, IPsec can provide security for individual users. This is useful for offsite employees and for configuring a secure virtual subnet within the organization for sensitive applications.

IPsec can also play a key role in the routing architecture required in the network.

- Router announcement (a new router announces its presence) comes from an authorized router.

- Neighbor announcement (a router attempts to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router.

- Redirect message comes from the router to which the initial packet was sent.

- Routing update is not falsified.

Without such security measures, an attacker could disrupt communication or redirect some traffic. Routing protocols, such as Open Shortest Path First (OSPF), should run based on security associations between routers defined by IPsec.

Security Associations

Security associations:

A unidirectional relationship between sender and receiver providing traffic security.

If a peer relationship is needed for two-way secure exchange, two associations are required.

It is uniquely identified by:

- SPI - Security Parameter Index

- IP - destination IP address

- ESP or AH - protocol identifier

IPsec Protocols

AH - Authentication Header - provides authentication functions (not used in IPsec v3)

ESP - Encapsulating Security Payload - provides confidentiality services, including message content confidentiality and limited traffic flow confidentiality. Optionally, the ESP protocol may also provide authentication services.

ESP

ESP Packet:

- SPI Index (32 bits) — identifies the security association.

- Sequence number (32 bits) — a monotonically increasing counter value.

- Payload data (variable) — a transport-level segment (transport mode) or IP packet (tunnel mode) protected by encryption.

- Padding (0 – 255 bytes) — may be necessary if the encryption algorithm requires plaintext to be a multiple of a certain number of octets.

- Padding size (8 bits) — indicates the number of padding bytes immediately preceding this field.

- Next header (8 bits) — specifies the type of data contained in the Payload data field by identifying the first header in this payload (

e.g., IPv6 protocol extension header or higher-layer protocol such as TCP).

- Variable ICV (Integrity Check Variable) — a variable-length field (must be a multiple of 32-bit words) that contains the integrity check value computed for the ESP packet minus the Authentication data field.

ESP Frame

ESP protocol frame in IPsec

IPsec Modes

Transport mode - primarily provides protection for higher-layer protocols:

- Transport mode protection extends to the data payload of the IP packet

- Used for end-to-end communication between two hosts

- IPv4 - the payload includes data that usually follows the IP header

- IPv6 - the payload includes data that usually follows the IP header and all IPv6 extension headers

- ESP in transport mode encrypts and optionally authenticates the IP data payload but not the IP header.

Tunnel mode - provides protection for the entire IP packet, treating the entire packet and security fields as the payload of a new outer IP packet.

- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.

- Tunnel mode enables the creation of virtual private networks (VPNs), which are the primary use case for IPsec.

Security of Operating Systems

Marek Miśkiewicz

Lecture 4

Authentication on the Internet

Kerberos

- Initially developed at MIT

- Software tool available both in the public domain and as commercially supported versions

- Released as an internet standard and is the de facto standard for remote authentication

- Authentication involves a trusted third party (Third Party)

- Requires the user to prove their identity for each requested service and requires servers to prove their identity to clients

Kerberos Protocol

- Involves clients, application servers, and the Kerberos server

  - Designed to counter various threats to client/server dialogue security.

  - A common security threat is impersonation.

  - Servers must be able to verify the identity of clients requesting services.

- Authentication Server (AS)

  - The user initially negotiates with the AS to verify their identity.

- The AS verifies the identity and then passes the information to the application server, which then accepts service requests from the client.

It must be done securely: If the client sends the user's password to the AS over the network, an attacker could intercept it. The attacker could impersonate the AS and send a false confirmation.

COMPUTER SECURITY: PRINCIPLES AND PRACTICE, Fourth Edition; ISBN 0134794109; by William Stallings, and by Lawrie Brown, Pearson 2018

Kerberos Domain

- Kerberos environment:

  - Kerberos server

  - Clients, all registered on the server

  - Application servers sharing keys with the server

- Domains - networks of clients and servers within different organizations

- For many interacting domains, Kerberos servers must trust each other

COMPUTER SECURITY: PRINCIPLES AND PRACTICE, Fourth Edition; ISBN 0134794109; by William Stallings, and by Lawrie Brown, Pearson 2018

Kerberos Version 5

- The first widely used version of the Kerberos protocol was version 4, published in the late 1980s.

- Improvements in version 5:

  - The encrypted message is marked with an encryption algorithm identifier. This allows users to configure the Kerberos protocol to use an algorithm other than DES.

  - Supports authentication delegation

    - Allows a client to access a server and that server to access another server on behalf of the client

    - Supports inter-realm authentication with fewer secure key exchanges than version 4

Kerberos Performance Issues

- Client-server environment size problem

- For large environments, if the system is correctly configured, the impact of using the Kerberos protocol on performance is minimal.

- The best way to ensure the security of the Kerberos protocol is to place the Kerberos server on a separate, isolated computer.

- Multiple separate domains are more of a geographical requirement than a hardware one.

Certification Authorities

Certification Authorities - CA

A certificate generally includes:

- The owner's public key (with a precisely defined identity)

- The signature of a trusted third party (TTP) - the certificate issuer

Typically, the third party is a CA trusted by user communities (such as a government agency, telecommunications company, financial institution, or other trusted organization). The user can securely present their public key to the CA and obtain a certificate. The user can then publish the certificate or send it to others. Anyone needing the user's public key can obtain the certificate and verify its validity using the attached trusted signature.

X.509 Standard

The ITU-T X.509 standard, also specified in RFC 5280, is the most widely accepted public key certificate format. X.509 certificates are used in most network security applications, including IP Security (IPSEC), SSL (Secure Socket Layer), TLS (Transport Layer Security), SET (Secure Electronic Transactions), and S/MIME, as well as in eBusiness applications.

COMPUTER SECURITY: PRINCIPLES AND PRACTICE, Fourth Edition; ISBN 0134794109; by William Stallings, and by Lawrie Brown, Pearson 2018

Types of Certificates

- Conventional certificates

  - CA and "end-user" certificates

  - Typically issued for validity periods from months to years

- Short-term certificates

  - Used for authentication in applications such as network processing while avoiding some of the overhead and limitations of conventional certificates

- Have validity periods from hours to days, limiting the misuse period in case of compromise

- Since they are usually not issued by recognized CAs, there are verification issues outside their issuing organization

- Proxy certificates

- Commonly used for authentication in applications such as network processing while considering some short-term certificate limitations

- Identified by the presence of a "proxy certificate" extension

- Allow the "end-user" certificate to sign another certificate

- Enable users to easily create credentials for access to resources in a specific environment without needing to provide the full certificate and entitlements

- Attribute certificates

- Use a different certificate format to link the user's identity with a set of attributes, typically used for authorization and access control

- A user can have many different attribute certificates, with various attribute sets for different purposes

- Defined in the "Attributes" extension

Public Key Infrastructure

Public Key Infrastructure

- A set of hardware, software, people, policies, and procedures necessary to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography

- Developed to enable secure, convenient, and efficient public key acquisition

- "Trusted Store"

- List of certification authorities and their public keys

COMPUTER SECURITY: PRINCIPLES AND PRACTICE, Fourth Edition; ISBN 0134794109; by William Stallings, and by Lawrie Brown, Pearson 2018

Wireless Network Security

Wireless Network Security

Key factors contributing to the higher security risk of wireless networks compared to wired networks:

- Channel

  - Wireless networks typically involve broadcast communication, which is much more susceptible to eavesdropping and jamming than wired networks

  - Wireless networks are also more prone to active attacks exploiting communication protocol vulnerabilities

- Mobility

  - Wireless devices are much more portable and mobile, leading to various threats

Wireless Network Security

- Resources

  - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources to counter threats and malware

- Availability

  - Some wireless devices, such as sensors and robots, may remain unattended in remote and/or hostile locations, significantly increasing their vulnerability to physical attacks

Wireless Network Security

Wireless network threats:

- Accidental connection

- Malicious connection

- Ad hoc networks

- Non-traditional networks

- Identity theft (MAC spoofing)

- Man-in-the-middle attacks

- Denial of service

- Network injections

Wireless Network Security Measures

Securing wireless transmissions:

- Signal hiding techniques

  - Making it harder for an attacker to locate wireless access points

  - Disabling SSID broadcasting by wireless access points

- Assigning cryptic names to SSIDs

- Reducing signal strength to the lowest level ensuring required coverage

- Placing wireless access points inside buildings, away from windows and external walls

- Using directional antennas and signal shielding techniques

- Encryption

Wireless Network Security Measures

Using encryption and authentication protocols is the standard method of countering attempts to modify or insert into transmissions.

Wireless Network Security Measures

Securing wireless networks:

- Use encryption

- Use antivirus and antispyware software and firewalls

- Disable SSID broadcasting

- Change the router's default identifier

- Change the router's default administrator password

- Allow access to your wireless network only to specified computers (MAC)

Wireless Network Security Measures

Securing wireless access points:

- The main threat associated with wireless access points is unauthorized network access

- The primary approach to preventing such access is the IEEE 802.1X standard for network access control based on ports

- The standard provides an authentication mechanism for devices wishing to connect to a LAN or wireless network

- Using the 802.1X standard can prevent unauthorized devices from becoming dangerous backdoors

Mobile Device Security

Paradigm Shift

Security of

computers and networks in

companies

Distributed

elements

Paradigm Shift

What to consider:

- Increasing use of new devices

- Cloud applications

- Deperimeterization

- External business requirements

Mobile Device Threats

The NIST SP 800-124 document (Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013) highlights seven major security issues related to mobile devices:

- Lack of physical security controls

- Use of untrusted mobile devices

- Use of untrusted networks

- Use of untrusted applications

- Interaction with other systems

- Use of untrusted content

- Use of location services

Mobile Device Threats

Device security:

- IT department verifies each device (BYOD) (rooted, jailbroken)

- Enable automatic locking

- Enable password or PIN protection

- Avoid using auto-fill features to remember usernames or passwords

- Enable remote wiping

- Ensure SSL protection is enabled if available

- Keep software, including operating systems and applications, updated

- Install antivirus software as soon as it becomes available

- Allow remote access to devices for wiping all data

- Security policy may require location services to be disabled on all mobile devices

Mobile Device Threats

Traffic security:

- All traffic should be encrypted and transmitted using secure protocols (SSL, IPv6, VPN)

- The preferred strategy is to have a two-layer authentication mechanism that includes device authentication followed by user authentication.

Border Security:

- The organization should have security mechanisms to protect the network from unauthorized access. The security strategy may also include firewall rules specific to mobile device traffic.

IEEE 802.11 Standard

IEEE 802.11 Standard

IEEE 802 is the committee that developed standards for a wide range of local area networks (LANs). In 1990, the committee

established a new working group called IEEE 802.11, tasked with developing a protocol and transmission specifications for wireless LANs (WLANs). Over time, the demand for WLANs with different frequencies and data transmission rates has grown rapidly. To keep up with this demand, the IEEE 802.11 working group has published a growing list of standards.

IEEE 802.11 Standard

IEEE 802.11 terminology:

- Access Point (AP)

- Any entity that has the functionality of a workstation and provides access to the distribution system for associated stations via the wireless medium.

- Basic Service Set (BSS)

  - A set of stations controlled by a single coordination function.

- Coordination Function

  - A logical function that determines when a station operating within a BSS may transmit and receive PDU data units.

- Distribution System (DS)

  - A system used to connect a set of BSSs and integrated LANs to form an ESS.

- Extended Service Set (ESS)

  - A set composed of one or more interconnected BSSs and integrated LANs, which are seen from any station associated with one of these BSSs as a single BSS at the LLC layer.

IEEE 802.11 Standard

IEEE 802.11 terminology:

- MAC Protocol Data Unit (MPDU)

  - A data unit exchanged between two peer MAC entities using physical layer services.

- MAC Service Data Unit (MSDU)

  - Information delivered between MAC users as a unit.

- Station

  - Any device that has an IEEE 802.11-compliant MAC address and physical layer.

Based on: William Stallings, Lawrie Brown, Computer Security: Principles and Practice (4th Edition), Helion 2019

IEEE 802.11

- The first widely accepted standard - 802.11b

- In 1999, the Wireless Ethernet Compatibility Alliance (WECA) industry consortium was formed.

- Over time, it was renamed the Wi-Fi Alliance (Wireless Fidelity) and created the Wi-Fi certification set (802.11b) -> 802.11g -> 802.11a.

- The Wi-Fi Alliance developed certification procedures for the IEEE 802.11 security standards, known as Wi-Fi Protected Access (WPA). The latest version, WPA2, includes all features of the IEEE 802.11i WLAN security specification -> WPA3.

Security of Operating Systems

Marek Miśkiewicz

Lecture 5

Malware

Terminology

APT (Advanced Persistent Threat): Cybercrime aimed at economic or political targets using a wide range of hacking and malware techniques, characterized by persistence and efficiency in attacks on intentional targets over long periods, often against state-subsidized institutions.

Adware (Advertising-Supported Software): Advertising integrated with software. It can cause additional advertisements to pop up or redirect the browser to commercial websites.

Attack Kit: A set of tools for generating new malware, automatically utilizing various included mechanisms for spreading and payload delivery.

Terminology (continued)

Auto-rooter: Malicious hacker tools used for remote break-ins into new machines.

Backdoor: Any mechanism bypassing normal security controls; it may result in unauthorized access to functions in a program or an attacked (unprotected) system.

Downloader: Code installing other units on the attacked machine. Usually appended to malware code initially inserted into the compromised system, then importing a larger malware package.

Terminology (continued)

Drive-by-download: An attack using code on a compromised website, exploiting a vulnerability in the browser to attack the client system while browsing the site.

Exploit: Code targeting a specific weakness or set of weaknesses.

Flooders: Used to generate large amounts of data to attack networked computer systems by executing a variant of a "denial of service" (DoS) attack.

Keylogger: Captures keystrokes in the attacked system.

Terminology (continued)

Logic-bomb: Code inserted into malware by an intruder. The logic bomb remains dormant until a predetermined condition is met; then the code triggers the execution of some payload.

Macro Virus: A type of virus using macro definitions or script code, usually embedded in a document or document template, activated when viewing or editing the document to execute and replicate in other such documents.

Mobile Code: Software (e.g., script or macro definition) that can be sent in unchanged form to different platforms and operate there with identical semantics.

Terminology (continued)

Rootkit: A set of hacker tools used after an attacker breaks into a computer system and gains administrator (root) access.

Spammer Programs: Used to send large quantities of unwanted mail.

Spyware: Software collecting information from a computer and sending it to another system by monitoring keystrokes, displayed data, and/or network traffic, or scanning system files for sensitive information.

Terminology (continued)

Trojan Horse: A computer program masquerading as a useful function but also hiding a potentially dangerous function that bypasses security mechanisms, sometimes using the legal privileges of the system entity that invoked it.

Virus: Malicious software that, when executed, attempts to reproduce itself on another running machine or script code. Code that has succeeded in this is said to be infected. If the infected code is executed, the virus also runs.

Worm: A computer program capable of running independently and spreading a complete, functioning version of itself to other computers in a network, exploiting software weaknesses in the target system or captured authorization credentials.

Terminology (continued)

Zombie, Bot: A program installed on an infected machine, which activates to launch attacks on other machines.

Malware - Classification

- Initially based on how it spreads or propagates to achieve desired goals.
- Then based on the actions or payloads it executes after reaching the target.

- Those requiring a host program (parasitic code, such as viruses)
- Those that are independent, standalone programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam)
- Malware that replicates (viruses and worms)

Attack Kits

- Initially, creating and deploying malware required significant technical skills from software authors.
  - The development of virus creation kits in the early 1990s, and later more general attack kits in the early 21st century, greatly facilitated malware development and deployment.
- Kits are often known as "crimeware".

- Include various propagation mechanisms and payload modules that even novices can deploy.
- Variants generated by attackers using these toolkits pose a significant problem for defenders.

Examples:

- Zeus
- Angler

Sources of Attack

A significant reason for the development of malware is the shift in motivation from demonstrating technical skills to peers to more organized and dangerous attack sources.

This shift has resulted in a significant change in available resources and motivation for creating malware, leading to the development of a large gray area involving the sale of attack kits, access to infected hosts, and stolen information.

- Political motivation
- Crimes and organized crime
- Direct profit
- State agencies

Advanced Persistent Threats (APT)

- Well-equipped, persistent use of a wide range of hacking and malware technologies against selected targets (usually business or political).
- Typically attributed to state-sponsored organizations and criminal enterprises.
- Different from other attack types by careful target selection and hiding over long periods.
- Highly specialized attacks: Aurora, RSA, APT1, Stuxnet.

APT Characteristics

Advanced

- Attackers use a wide range of hacking and malware technologies, including creating custom malware if needed.

- Individual components do not necessarily need to be technically advanced but are carefully chosen to fit the selected target.

Persistent

- Determined use of attacks over a long period against a chosen target to maximize chances of success.

- Various attacks may be used gradually until the target is compromised.

Threats

- Threats to selected targets from organized, capable, and well-funded attackers intending to breach specific targets.

- Active human involvement in the process significantly raises the threat level due to automatic attack tools and the likelihood of successful attacks.

Objective: Spectrum of objectives - from stealing intellectual property or security and infrastructure-related data to physically disrupting infrastructure.

Methodology: Social engineering, spear-phishing email, drive-by-download from selected compromised sites likely to be visited by target organization personnel.

Intentions: To infect the target with sophisticated malware with multiple propagation mechanisms and payloads. Once initial access to the target organization's systems is gained, further attack tools are used to maintain and expand their access.

Malware - Viruses and Worms

Virus Components

- **Infection Mechanism**

  - Means by which the virus spreads or replicates.

  - Also known as the infection vector.

- **Trigger**

  - Event or condition determining the activation or delivery of the payload, sometimes called a logic bomb.

- **Payload**

  - What the virus does besides spreading.

Virus Lifecycle

1. Dormant Phase: The virus remains idle until activated. Not all viruses have this phase.

2. Propagation Phase: The virus places its copy in other programs or special system areas on the disk (polymorphism).

3. Triggering Phase: The virus is activated to perform its function. The triggering phase can be caused by various system events, including executing a certain number of its copies.

4. Execution Phase: The intended function is executed. This can be a harmless function, like displaying a message on the screen, or damaging, such as destroying programs and data files.

Macro Viruses

NISTIR 7298 defines a macro virus as:

- "A virus that attaches itself to documents and uses the document's macro programming capabilities to execute and spread."

Macro viruses infect script code used to handle active content in various types of user documents.

Macro Virus Characteristics:

- Platform-independent

- Infects documents, not executable code

- Easily spread

- Since they infect user documents, not system programs, traditional file system access control mechanisms have limited application in preventing their spread, as users should be able to modify them (files).

- Much easier to write or modify than traditional executable viruses.

Example:

- Melissa virus pseudocode (fragment)

Virus Classification

Objective:

- **Boot Sector Infector**: Infects the master boot record or boot record and spreads when the system boots from the infected disk.

- **File Infector**: Infects files considered executable by the operating system or shell.

- **Macro Virus**: Infects files with macros or script code interpreted by an application.

- **Multipartite Virus**: Infects files in multiple ways.

Hiding Strategy:

- **Encrypted Virus**: Part of the virus creates a random encryption key and encrypts the rest of the virus.

- **Stealth Virus**: A form of virus specifically designed to hide from antivirus software detection.

- **Polymorphic Virus**: Mutates with each infection.

- **Metamorphic Virus**: Mutates and completely rewrites itself in each iteration and can change behavior and appearance.

Worms

- A program actively seeking more machines to infect, with each infected machine serving as an automatic launch platform to attack other machines.

- Exploits security weaknesses in client or server programs.

- Uses network connections to spread from system to system.

- Spreads through shared media (USB drives, CDs, DVDs).

- Email worms spread in macro or script code contained in attachments and files sent via instant messaging.

- Once activated, a worm can replicate and re-propagate.

- Usually contains some form of payload.

- The first known implementation was done at Xerox Palo Alto Labs in the early 1980s.

Worm Propagation

Models:

- **Random**: Each compromised host probes random addresses in the IP address space using a different seed. Causes significant Internet traffic, which may cause general disruption even before the actual attack starts.

- **Hit-List**: The attacker first compiles a long list of potentially vulnerable machines. Once the list is created, the attacker starts infecting the machines on the list. Each infected machine gets a portion of the list to scan. Causes a very short scan period, which may make it difficult to detect that an infection is occurring

.

- **Topological**: Uses information contained on the infected victim machine to find more hosts to scan.

- **Local Subnet**: If the host can be infected behind a firewall, it then looks for targets in its local network. The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall.

Propagation Model Similar to a Biological Virus:

Infection Count Over Time

Susceptible Count Over Time

Reproduction Rate

Worm Propagation (continued)

Notable Worms:

- **Melissa (1998)**: Email worm. First to include virus, worm, and Trojan in one package.

- **Code Red (July 2001)**: Exploited Microsoft IIS bug. Probes random IP addresses. Consumes significant Internet capacity when active.

- **Code Red II (August 2001)**: Also targeted Microsoft IIS. Installs a backdoor for access.

- **Nimda (September 2001)**: Had worm, virus, and mobile code characteristics. Spread using email, Windows shares, web servers, web clients, and backdoors.

- **SQL Slammer (Early 2003)**: Exploited a buffer overflow vulnerability in SQL server compact and spread rapidly.

- **Sobig.F (Late 2003)**: Exploited open proxy servers to turn infected machines into spam engines.

- **Mydoom (2004)**: Mass-mailing email worm. Installed a backdoor in infected machines.

- **Warezov (2006)**: Creates executables in system directories. Sends itself as an email attachment. Can disable security-related products.

- **Conficker (Downadup) (November 2008)**: Exploits a Windows buffer overflow vulnerability. Most widespread infection since SQL Slammer.

- **Stuxnet (2010)**: Restricted rate of spread to reduce the chance of detection. Targeted industrial control systems.

WannaCry Worm

- Ransomware attack in May 2017 that spread extremely quickly within hours or days, infecting hundreds of thousands of systems belonging to public and private organizations in over 150 countries.

- Spreads as a worm, aggressively scanning local and random remote networks, trying to exploit a vulnerability in the SMB file-sharing service in unpatched Windows systems.

- This rapid spread was slowed only by the accidental activation of a "kill switch" domain by a British security researcher.

- Once installed on infected systems, it also encrypts files, demanding ransom payment for their recovery.

Worms - Current State of Technology

Mobile Code

NIST SP 800-28 defines mobile code as:

- "Programs that can be sent in unchanged form to a heterogeneous set of platforms and execute with identical semantics."

- Sent from a remote system to a local system, then executed in the local system.

- Often acts as a mechanism for a virus, worm, or Trojan horse.

- Exploits vulnerabilities to perform its own exploits.

Common Vehicles:

- Java Applets
- ActiveX
- JavaScript
- VBScript

Common Ways Mobile Code Is Used for Malicious Operations:

- Cross-site scripting
- Interactive and dynamic websites
- Email attachments
- Downloads from untrusted sites or untrusted software

Mobile Worms

- **Cabir (2004)**
- **Lasco and CommWarrior (2005)**
  - Communicate via Bluetooth or MMS.
  - Can completely disable the phone, delete phone data, or force the device to send expensive messages.
  - The most important aspect is that illegal code implemented in a mobile device can be used to collect information.
  - Currently, the simplest way to deliver illegal code is to use a "trojan".

Drive-by-Downloads

- "Drive-by-download" - exploits browser and plugin vulnerabilities when the user views a website controlled by the attacker. The site contains code that exploits a flaw (in the user's system) to download and install malware on the system without the user's knowledge and consent.
- In most cases, the malware does not actively spread like a worm.

Watering-Hole Attacks

- A variant of the drive-by-download attack used in highly targeted attacks.

- The attacker studies their victims to identify sites they are likely to visit, then scans those sites to identify vulnerabilities.

- They wait for one of their victims to visit one of the compromised sites.

- The attack code may even be written to infect only systems belonging to the target organization and take no action against other visitors to the site.

- This significantly increases the likelihood that the site compromise will go undetected.

Social Engineering

- **Unwanted Email**: One of the largest sources of malware. Used to steal any data. Contains hidden code. Can be used for indirect actions that the attacker cannot perform directly.

- **Privilege Acquisition (Jail-Break)**: Lack or poor quality control of software.

Prevention

- **Ideal Solution (nearly impossible to achieve)**: Prevention. The main elements of prevention are:

  - Security policy

  - Awareness

  - Reducing vulnerabilities

  - Mitigating threats - detection, identification, removal

Antivirus Programs:

- **First Generation**: Signature analysis (same or similar bit pattern), concerning already known malware.

- **Second Generation**: Heuristic scanners - searching for patterns in code fragments (e.g., encryption loops).

- **Third Generation**: Resident programs - analyzing program activities.

- **Fourth Generation**: Comprised of various antivirus techniques used together. Includes scanning components and activity traps.

Sandbox

- Running potentially malicious code in an emulated "sandbox" or virtual machine.

- Allows code to execute in a controlled environment where its behavior can be closely monitored without endangering the actual system's security.

- Running potentially malicious software in such environments allows for the detection of complex, encrypted, polymorphic, or metamorphic malware.

- The most challenging design problem with sandbox analysis is determining how long to run each potentially harmful code.

Dynamic Analysis

- **Host-Based Behavior-Blocking Software**: Integrates with the host computer's operating system and monitors program behavior in real-time for malicious activities.

  - Blocks potentially malicious activities before they can affect the system.

  - Blocks software in real-time, providing an advantage over antivirus detection techniques such as fingerprints or heuristics.

Monitored Behaviors May Include:

- Attempts to open, view, delete, and/or modify files.

- Attempts to format disks and perform other unrecoverable disk operations.

- Modifications of executable file logic or macros.

- Changes to critical system settings, such as boot parameters.

- Scripting email client actions to send executable content.

- Initiating network communications.

Distributed Scanning

- Antivirus software typically included with email and web proxy server services operating on the organization's network firewall and IDS system.

- Can also be included in the IDS traffic analysis component.

- May include intrusion prevention measures, blocking the flow of suspicious traffic.

- This approach is limited to scanning software content.

- Network traffic analysis - detecting anomalies.

Security of Operating Systems

Marek Miśkiewicz

Lecture 6 and 7

Denial-of-Service Attacks

DoS

The NIST Computer Security Incident Handling Guide defines a DoS attack as:

"An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space."

- A form of attack on the availability of a service.
- Categories of resources that can be attacked include:
  - Network link
  - System resources
  - Application resources

Classic DoS Attacks

Ping flood (ICMP packets)

- The goal of this attack is to overload the network connection bandwidth to the target organization.
- The traffic must be handled by higher bandwidth links en route to the target; packets are dropped as capacity decreases.
- The source of the attack is clearly identified unless a fake address is used.
- Network performance is noticeably reduced.

Address Spoofing

- Fake source addresses are used.
  - Usually through raw socket interface in operating systems.

  - This makes the attacking systems harder to identify.

- The attacker generates large amounts of packets with the target system as the destination address.

- Congestion would cause the router to connect to the last link with lower bandwidth.

- Requires special requests for information flow from engineers' routers.

- Backscatter traffic.

SYN Spoofing

- Uses the specifics of the TCP protocol to overload connection tables.

- Based on the "three-way handshake" (the TCP protocol is reliable, unlike IP).

- SYN spoofing vs. SYN flooding.

Flooding Attacks

- Classified based on the network protocol used.

- The goal is to overload the network bandwidth at some link to the server.

- Any type of network packet can be used.

- **ICMP flood**:

  - Ping flood using ICMP echo request packets.

  - Traditionally, network administrators allow such packets in their networks as ping is a useful network diagnostic tool.

- **UDP flood**:

  - Uses UDP packets directed to a port number on the target system.

- **TCP SYN flood**:

  - Sends TCP packets to the target system.

  - The attack's goal is the overall volume of packets, not system code.

Distributed Denial-of-Service (DDoS)

- Uses multiple machines to carry out the attack.

- The attacker exploits a vulnerability in the operating system or popular application to gain access and install their program (zombie).

- Large collections of such systems can be created under the control of a single attacker, forming a botnet.

SIP Flood

- **SIP (Session Initiation Protocol)** - VoIP protocol, text-based similar to HTTP.

- A single INVITE consumes significant resources.

- The attacker can flood a SIP intermediary with a large number of INVITE requests with fake IP addresses or perform a DDoS attack using a botnet generating many INVITE requests.

- The attack burdens SIP intermediary servers in two ways:

  - Resources are exhausted processing INVITE requests.

  - Network capacity is consumed.

HTTP-Based Attacks

HTTP Flood:

- An attack that bombards web servers with HTTP requests.

- Consumes significant resources.

- **Spidering**: Bots starting to send requests from a given HTTP link and recursively following all links on the provided website.

Slowloris:

- Uses a popular technique of using multiple threads to handle many requests in the same server application.

- Attempts to "monopolize" sessions by sending HTTP requests that never complete - no "empty line" ending the request.

- Eventually leads to the consumption of the web server's connection bandwidth.

- The technique uses legitimate HTTP traffic.

- Existing intrusion detection and prevention solutions relying on signatures to detect attacks generally do not recognize Slowloris.

Prevention Methods for Slowloris:

- Limiting the rate of incoming requests from a specific host.

- Changing the waiting time for (active) connections based on the number of connections and delaying the binding - waiting to send the request until the client sends correct patterns with end-of-line characters.

Reflection Attacks

- The attacker sends packets to a known intermediary service with the spoofed source address of the actual target system.

- When the intermediary responds, the response is sent to the target.

- The goal is to generate enough packets to flood the link to the target system without alerting the intermediary.

- Basic defense against these attacks is to block packets from spoofed sources.

Amplification Attacks

- A variant of reflection attacks.

- Most commonly uses packets directed to a legitimate DNS server as the intermediary system with fake source addresses (victim).

- Generating many response packets can be achieved by directing the initial request to the broadcast address in some network.

- Potentially all computers in that network may respond to the request.

- Uses ICMP and UDP protocols (echo).

- TCP protocol and services are not suitable for this type of attack.

DNS Amplification Attacks:

- A variant of the DNS reflection attack using protocol features.

- The attacker creates a series of DNS requests containing a fake source address, being the address of the attacked system.

- Requests are directed to several selected DNS servers.

- Servers respond by sending replies to the fake source, which they consider a valid requesting system, causing the target to be flooded with their responses.

- There is a variant of this attack where the DNS server accepting recursive queries is used because amplified DNS packets are responses to recursive DNS queries.

DoS and DDoS Defense

- These attacks cannot be completely prevented.

- High traffic volume may be justified.

- High temporary popularity of a specific site.

- High temporary activity in a very popular site.

- Phenomena described as slashdotted, flash crowd, or flash event.

Prevention and Mitigation:

- Preventing and thwarting attacks (preemptive attack).

- Detecting and filtering attacks (during the attack).

- Identifying and tracing back to the attack source (during and after the attack).

- Responding to the attack (post-attack).

DDoS Prevention:

- Blocking fake source addresses on routers as close to the source as possible.

- Filters can be used to ensure the return path to the desired source address is the one used by the current packet.

- Filters must be applied to traffic before it leaves the ISP network or at the entry point to its network.

- Using modified TCP connection handling code - cryptographically encrypting critical information in a cookie sent as the initial sequence number by the server. A legitimate client responds with an ACK packet containing the cookie with an increased sequence number.

- Removing incomplete connection entries from the TCP connection table in case of overflow.

General Defense Practices:

- Block IP-directed broadcasts.

- Block suspicious services and combinations.

- Manage application attacks using CAPTCHA to distinguish legitimate human requests.

- Good general system security practices.

- Use mirror and replicated servers when high performance and reliability are required.

DoS and DDoS Response

- Identifying the type of attack.

  - Capture and analyze packets.

  - Design filters to block attack-related traffic.

  - Identify and fix the system/application bug.

- Assign ISP to track packet transmission (reverse path analysis).

  - May be difficult and time-consuming.

  - Necessary for planning legal actions.

- Implementing a contingency plan.
  - Switch to alternative backup servers.
  - Deploy new servers at a new site with new addresses.
- Updating the incident response plan.
  - Analyze the attack and response for future actions.

Intrusion Detection

Intruder Classification - Cybercriminals

- Individuals or members of organized crime groups targeting financial gain.
- Activities:
  - Identity theft.
  - Theft of financial credentials.
  - Corporate espionage.
  - Data theft or data extortion.
- Young hackers, often from Eastern Europe, Russia, or Southeast Asia, conducting business online.
- The very high and growing costs resulting from cybercriminal activity necessitate steps to minimize this threat.

Intruder Classification - Hacktivists

- Individuals usually working inside an organization or members of larger external attacker groups motivated by social or political causes.
- Also known as hacktivists - their skill level is often quite low.
- Their attack goals are often to promote and publicize their cause, usually by:
  - Defacing websites.
  - Denial-of-service attacks.
  - Theft and distribution of data leading to negative publicity or endangering targets.

Intruder Classification - State-Sponsored Organizations

- Groups of hackers sponsored by governments for espionage or sabotage activities.

- Known as advanced persistent threats (APT) due to their covert nature and persistence over long periods associated with any attacks from this class.

- Periodically disclosed information indicates the extensive nature and scope of such activities conducted by large groups of countries.

Intruder Classification - Others

- Hackers with motivations other than those listed previously.

- "Classic" hackers or crackers motivated by technical challenge or respect and reputation within a peer group.

- Many individuals in this category are responsible for discovering new vulnerability categories and can be considered members of this class.

- Considering the wide availability of attack toolkits, there is a group of "hobbyist hackers" using these toolkits to test system and network security.

Intruder Classification - Level I

- Hackers with minimal technical skills who mainly use existing attack toolkits.

- Likely the largest number of attackers, including many criminals and hacktivists.

- Given their use of existing known tools, they are the easiest to defend against.

- Also known as "script-kiddies" due to the use of existing scripts (tools).

Intruder Classification - Level II

- Hackers with sufficient technical skills to modify and extend attack toolkits to exploit newly discovered or "purchased" vulnerabilities.

- May be able to find new vulnerabilities to exploit, similar to some already known.

- Hackers with such skills are

likely found in all intruder classes.

- Capable of customizing tools used by others.

Intruder Classification - Level III

- Hackers with high technical skills capable of discovering entirely new categories of vulnerabilities (APT).

- Write new attack toolkits.

- Some are employed by state-sponsored organizations.

- Defending against these attacks is the most difficult.

Examples of Breaches and Violations

- Remote takeover of email server administrative functions.
- Destruction of web server.
- Guessing and cracking passwords.
- Copying a database containing credit card numbers.
- Unauthorized viewing of confidential data, including payroll and medical information.
- Running a packet sniffer on a workstation to capture usernames and passwords.

General Scheme

Recognition of the Target and Information Gathering

Initial Access

Privilege Escalation

Information Gathering or System Exploitation

Maintaining Access

Covering Tracks

Intrusion Detection - Concepts

Security Intrusion: An illegal act of bypassing the security mechanisms of a system.

Intrusion Detection: A hardware or software function collecting and analyzing information from various areas within a computer or network to identify potential security violations.

IDS (Intrusion Detection System): A system for detecting intrusions.

IPS (Intrusion Prevention System): Systems for preventing intrusions.

IDS - Logical Components

Sensors: Responsible for collecting data. The sensor's input can be any part of the system containing evidence of intrusion. Types of sensor input data include network packets, log files, and system call traces. Sensors collect and transmit this information to the analyzer.

Analyzers: Receive data from one or more sensors or other analyzers. The analyzer determines whether an intrusion has occurred. The output of this component is an indication (suggestion) that an intrusion may have occurred.

User Interface: Allows the user to view results from the system or direct the system's behavior.

IDS Classification

- **Host-Based IDS (HIDS)**: Monitor characteristics of a single network computer (such as process identifiers) and events occurring within it (such as system calls made by processes) to reveal suspicious activities.

- **Network-Based IDS (NIDS)**: Monitor traffic on specific network segments or devices and analyze network, transport, and application protocols to identify suspicious activities.

- **Distributed or Hybrid IDS**: Combine information from multiple sensors, often both located on computers and in the network, collecting it in a central analyzer that can better identify and respond to intrusion activities.

IDS Detection Approaches

Anomaly Detection:

- Involves collecting data about the behavior of legitimate users over a period.

- The currently observed behavior is analyzed to determine if it is that of a legitimate user or an intruder.

Signature (Heuristic) Detection:

- Uses a set of known malicious data patterns or attack rules compared with current behavior.

- Also known as misuse detection.

- Can only identify known attacks for which it has patterns or rules.

Anomaly Detection Methods

Statistical: Analyzing observed behavior using univariate or multivariate models or time series models of observed metrics.

Knowledge-Based: Methods using expert systems classifying observed behavior according to a set of rules modeling legitimate behavior.

Machine Learning: Methods automatically determining the appropriate classification model based on training data using data mining techniques.

Signature-Based Detection Methods

Signatures:

- Match a large set of known malicious data patterns to data stored in the system or transmitted over the network.

- Signatures must be sufficiently large to minimize false positives while detecting a large portion of malicious data.

- Widely used in antivirus products, network traffic scanning proxy servers, and NIDS.

Host-Based IDS (HIDS)

- Adds a specialized security software layer to sensitive or vulnerable systems.

- Can use anomaly or signature and heuristic methods.

- Monitors activity to detect suspicious behavior.

- Main goals are detecting intrusions, logging suspicious events, and sending alerts.

- Can detect both external and internal intrusions.

HIDS Data Sources and Sensors

Typical Data Sources Include:

- **System Call Traces**: Logs of system call sequences made by processes in the system are widely recognized as valuable data sources for HIDS (Linux - okay, Windows - problematic).

- **Audit Records (Log Files)**: Advantage: No need for additional software to collect them; Disadvantage: Audit records may not contain needed information; intruders may try to manipulate these records to hide their attacks.

- **File Integrity Checksums**: Periodic scanning of critical files for discrepancies from the desired pattern by comparing current cryptographic checksums of these files with known good values.

HIDS - Distributed

HIDS - Agent Architecture

Network-Based IDS (NIDS)

- Monitors traffic at selected points in the network.
- Examines packet-by-packet in real-time or near-real-time.
- Can examine protocol activity at the network, transport, and/or application levels.
- Consists of multiple sensors, at least one management server, and at least one management console with a user interface.
- Traffic pattern analysis can occur at the sensor or management server.

Inline (Active) Sensors: Can block an attack.

Passive Sensors: Generally faster.

NIDS Sensor Placement

NIDS Sensor Location

Sensor 1:

- Detects attacks from the outside (external firewall).
- Problems related to the adopted firewall policies or its operation.
- Attacks targeting the web server or ftp server.
- DS can sometimes recognize signs of an attack in outgoing traffic.

Sensor 2:

- Can monitor all unfiltered network traffic.
- Documents the number of attacks originating from the Internet targeting the given network.
- Documents the types of attacks originating from the Internet.

Sensor 3:

- Protects main backbone networks, such as those providing resources for internal servers and databases.

- Monitors large amounts of network traffic, increasing the ability to detect attacks.

- Detects unauthorized actions performed by legitimate users within the organization.

Sensor 4:

- Detects attacks targeting critical systems and resources.

- Allows focusing limited resources on network assets rated highest.

Intrusion Detection Methods

Signature Detection:

- Application layer protocol analysis - buffer overflows, password guessing, and malware transmission.

- Transport layer protocol analysis - unusual packet fragmentation, port scanning, and TCP protocol-specific attacks.

- Network layer protocol analysis - spoofed IP addresses and unacceptable IP header values.

- Unexpected application services - unauthorized host performing some application service.

Anomaly Detection:

- Traffic intensity - DoS attacks.

- Scanning - application layer, transport layer, network layer.

- Worms - anomalous traffic between hosts, anomalous ports, scanning.

Stateful Protocol Analysis (SPA)

Stateful protocol analysis identifies protocol state deviations similarly to anomaly-based methods but uses predefined universal profiles based on "accepted definitions of benign activity" developed by providers.

Example: Monitoring requests along with corresponding responses; each request should have a predictable response, and those responses that deviate from expected results will be flagged and further analyzed.

The main disadvantage is significant resource requirements.