universität
wien

Security Engineering – Basic Principles

Chapter 3

VU Information Management & Systems Engineering

Wolfgang Klas

Planned Kahoot Sessions

Subject to change (see Moodle)

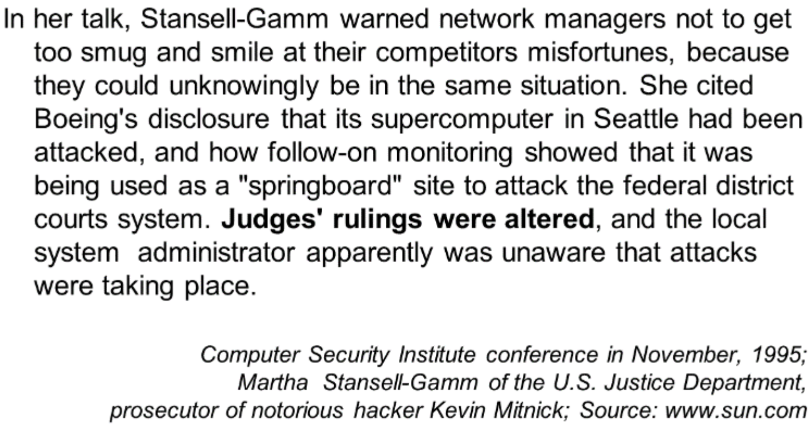
Typ	Date	Loc	Comment / Tentative Schedule	Kahoot
L	Fri 07.03. 13:15-14:45	HS 1	Kickoff + Organization	Kahoot-Test
A	Tue 11.03. 15:00-16:30	online	Assignment-Instruction Session	
L	Fri 14.03. 13:15-14:45	HS 1	Data Engineering 1	
L	Fri 21.03. 13:15-14:45	HS 1	Data Engineering 2	Kahoot
A	Tue 25.03. 15:00-16:30	online	Q/A Milestone 1	
L	Fri 28.03. 13:15-14:45	HS 1	Data Engineering 3	Kahoot
L	Fri 04.04. 13:15-14:45	HS 1	Data Engineering 4	Kahoot
L	Fri 11.04. 13:15-14:45	HS 1	Computing Infrastructure 1	Kahoot
S	Fri 11.04. 13:00	online	Milestone 1 (Submission Deadline)	
	Fri 18.04.		Easter break	
	Fri 25.04.		Easter break	
L	Fri 02.05. 13:15-14:45	HS 1	Computing Infrastructure 2	Kahoot
T	Fri 09.05. 13:15-14:45	tba.	Test 1	
A	Tue 13.05. 15:00-16:30	online	Docker Tutorial	
L	Fri 16.05. 13:15-14:45	HS 1	Security Engineering 1	Kahoot
A	Tue 20.05. 15:00-16:30	online	Q/A Milestone 2	
L	Fri 23.05. 13:15-14:45	HS 1	Security Engineering 2	Kahoot
L	Fri 30.05. 13:15-14:45	HS 1	- Reserve	
T	Fri 06.06. 13:15-14:45	tba.	Test 2	
T	Fri 13.06. 13:15-14:45	tba.	- Reserve (Test)	
S	Mon 16.06. 13:00		Milestone 2 (Submission Deadline)	
A	from 17.06.	online	Final Presentations	

Security Engineering – Basic Principles

Contents

- Motivation
- Security Controls (security countermeasures)
  - Basic Controls: Confidentiality, (Data) Integrity, Availability, Authentication,
  - Derived Controls: Accountability, (Data) Authenticity, Non-Repudiation, Access Control
  - Principles for protected IT systems
- Technical Security Concepts
  - Cryptography
  - Certificates, Digital Signatures, PGP-methods
  - HTTPS

Motivation - Intrusion



In her talk, Stansell-Gamm warned network managers not to get too smug and smile at their competitors misfortunes, because they could unknowingly be in the same situation. She cited Boeing's disclosure that its supercomputer in Seattle had been attacked, and how follow-on monitoring showed that it was being used as a "springboard" site to attack the federal district courts system. **Judges' rulings were altered**, and the local system administrator apparently was unaware that attacks were taking place.

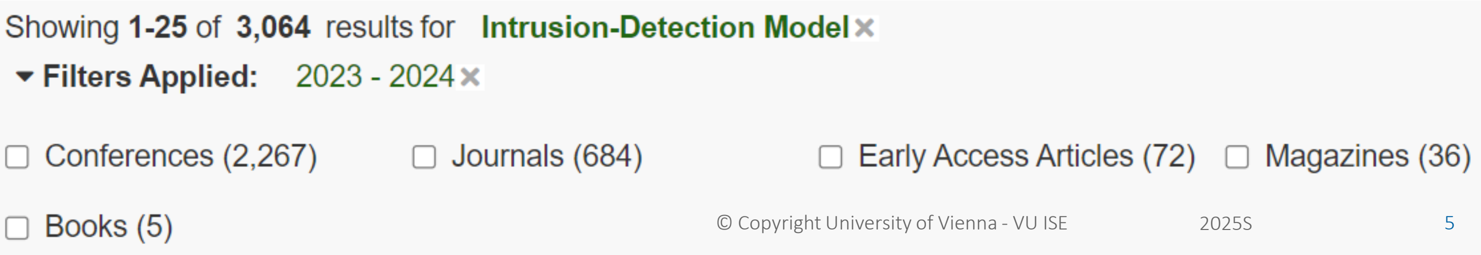
Computer Security Institute conference in November, 1995;
Martha Stansell-Gamm of the U.S. Justice Department,
prosecutor of notorious hacker Kevin Mitnick; Source: www.sun.com

History

1975 problem recognized:
J. H. Saltzer and M. D. Schroeder,
"The protection of information in computer systems,"
in *Proceedings of the IEEE*, vol. 63, no. 9, Sept. 1975,
doi: 10.1109/PROC.1975.9939.

1987 first models and system of Intrusion Detection
D. E. Denning, "An Intrusion-Detection Model,"
in *IEEE Transactions on Software Engineering*, vol. SE-13,
no. 2, Feb. 1987, doi: 10.1109/TSE.1987.232894

Today, IEEE Explore:



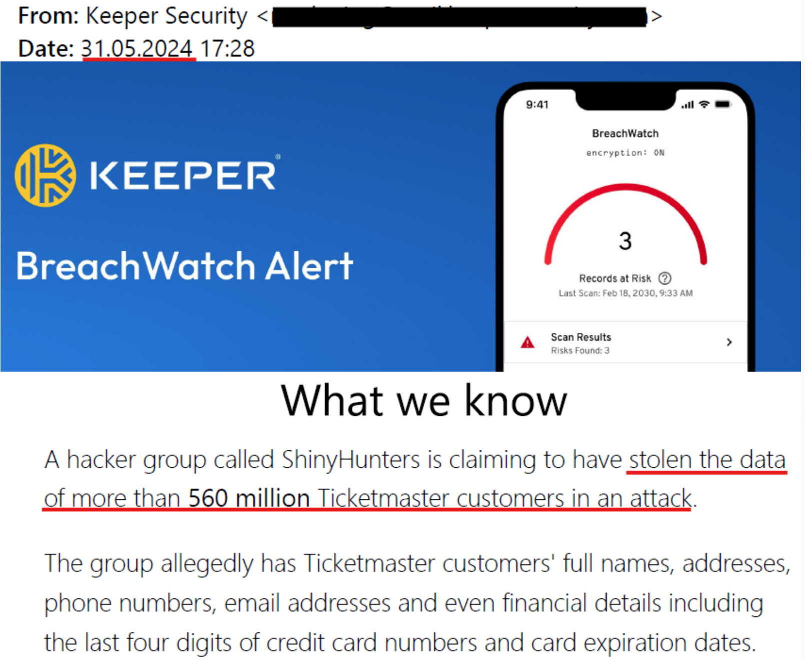
Showing **1-25** of **3,064** results for **Intrusion-Detection Model** ×

▾ **Filters Applied:** 2023 - 2024 ×

☐ Conferences (2,267) ☐ Journals (684) ☐ Early Access Articles (72) ☐ Magazines (36)

☐ Books (5)

Motivation - Theft

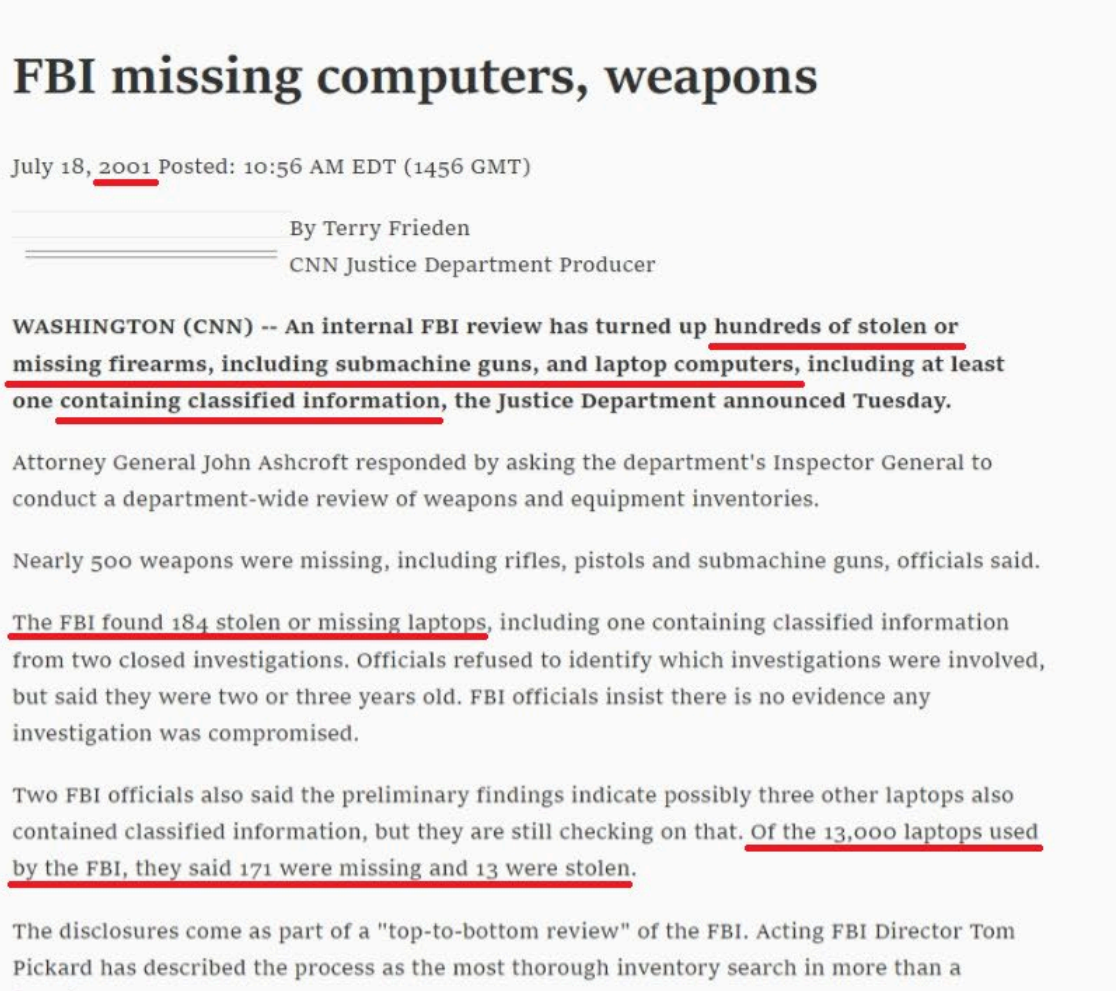


From: Keeper Security <[redacted]>
Date: 31.05.2024 17:28

What we know

A hacker group called ShinyHunters is claiming to have stolen the data of more than 560 million Ticketmaster customers in an attack.

The group allegedly has Ticketmaster customers' full names, addresses, phone numbers, email addresses and even financial details including the last four digits of credit card numbers and card expiration dates.



FBI missing computers, weapons

July 18, 2001 Posted: 10:56 AM EDT (1456 GMT)

By Terry Frieden
CNN Justice Department Producer

WASHINGTON (CNN) -- An internal FBI review has turned up hundreds of stolen or missing firearms, including submachine guns, and laptop computers, including at least one containing classified information, the Justice Department announced Tuesday.

Attorney General John Ashcroft responded by asking the department's Inspector General to conduct a department-wide review of weapons and equipment inventories.

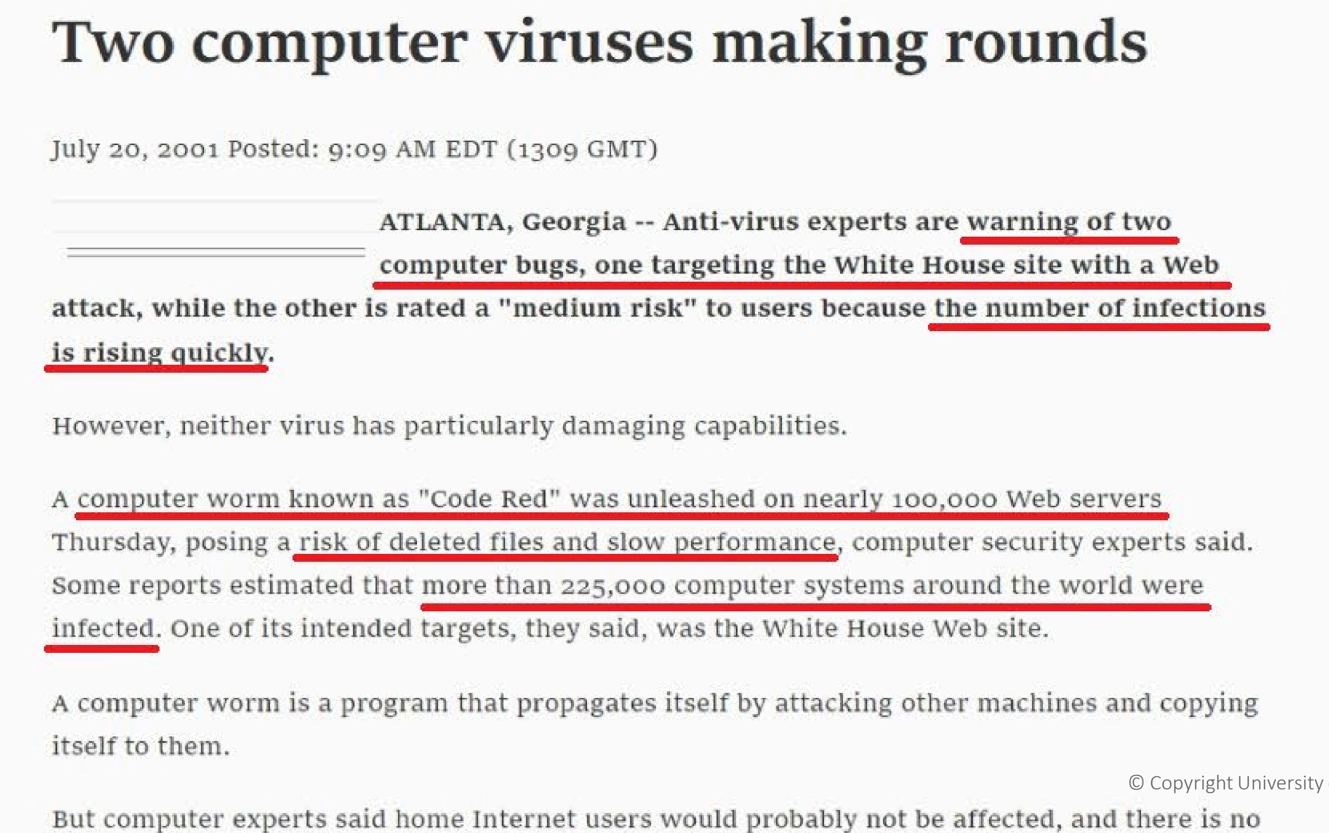
Nearly 500 weapons were missing, including rifles, pistols and submachine guns, officials said.

The FBI found 184 stolen or missing laptops, including one containing classified information from two closed investigations. Officials refused to identify which investigations were involved, but said they were two or three years old. FBI officials insist there is no evidence any investigation was compromised.

Two FBI officials also said the preliminary findings indicate possibly three other laptops also contained classified information, but they are still checking on that. Of the 13,000 laptops used by the FBI, they said 171 were missing and 13 were stolen.

The disclosures come as part of a "top-to-bottom review" of the FBI. Acting FBI Director Tom Pickard has described the process as the most thorough inventory search in more than a

Motivation - Maleware



Two computer viruses making rounds

July 20, 2001 Posted: 9:09 AM EDT (1309 GMT)

ATLANTA, Georgia -- Anti-virus experts are warning of two computer bugs, one targeting the White House site with a Web attack, while the other is rated a "medium risk" to users because the number of infections is rising quickly.

However, neither virus has particularly damaging capabilities.

A computer worm known as "Code Red" was unleashed on nearly 100,000 Web servers Thursday, posing a risk of deleted files and slow performance, computer security experts said. Some reports estimated that more than 225,000 computer systems around the world were infected. One of its intended targets, they said, was the White House Web site.

A computer worm is a program that propagates itself by attacking other machines and copying itself to them.

But computer experts said home Internet users would probably not be affected, and there is no

History

1949: Von Neuman starts working on self-replicating automata, published later 1966:

https://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf

1971 Creeper – considered first virus infecting ARPANET computers.
"I'M THE CREEPER. CATCH ME IF YOU CAN!" -> 1st Anti-virus program: "Reaper" was created to delete Creeper

Motivation – Back Doors in Software and IT Systems

SolarWinds cyberattack (2020): In 2020, a cyberattack on an unprecedented scale known as the Sunburst attack, targeted SolarWinds, a major software company based in Tulsa, Oklahoma. The attackers were able to gain access to the company's systems through a **back door in the SolarWinds Orion software**, which was then used to compromise the systems of thousands of SolarWinds' customers, including several U.S. government agencies, for up to 14 months.

NotPetya malware attack (2017): focused on Ukraine, inflicted enormous collateral damage across the globe. It's estimated that organizations collectively lost $1 billion because of the attack.

Ukraine power grid attack (2015): notable for being the first successful cyberattack on a power grid.

Cyberattacks on Estonia (2007): massively destabilized the Baltic state's infrastructure and economy, causing nationwide communication breakdowns, banking failures and media blackouts

Many, many more incidents underscore the potential for catastrophic damage

Motivation - Catastrophic Damage Resulting from Security Flaws

Gartner Study:

- Spending on **information security and risk management products and services** is forecast to grow 11.3% to reach more than $188.3 billion in 2023.
- Cloud security is the category forecast to have the strongest growth over the next two years (26,8% in 2023)

https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i

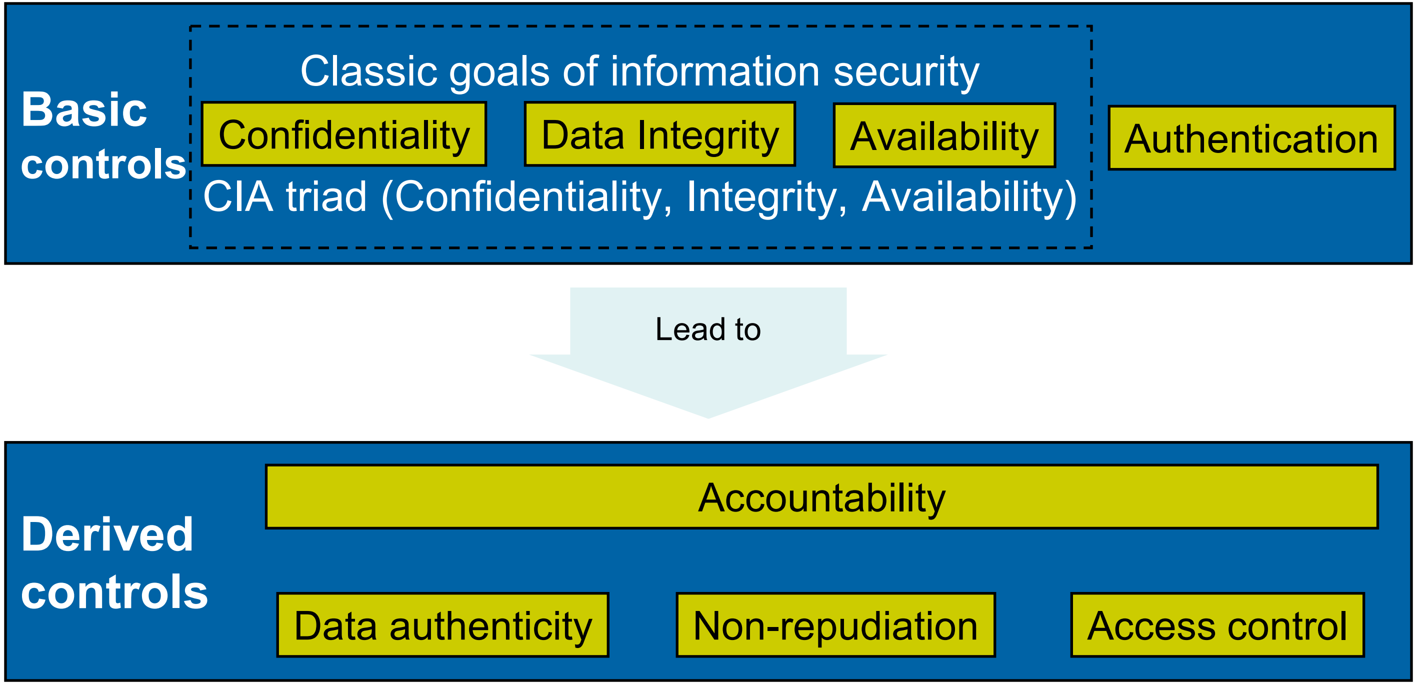
Reasons for Importance of Security

- Increase of data value
  - Huge data volumes
  - Strong connection of IT and companies (see IT Governance)
- Increase of number of potential attackers
  - Increasing number of users
  - Accessible Know-How of security holes
    - Problem Open Source Software
  - Decentralization

- Increased number of attacks
  - Lacking law regulations
  - Low ethical barrier
  - Lacking control mechanisms

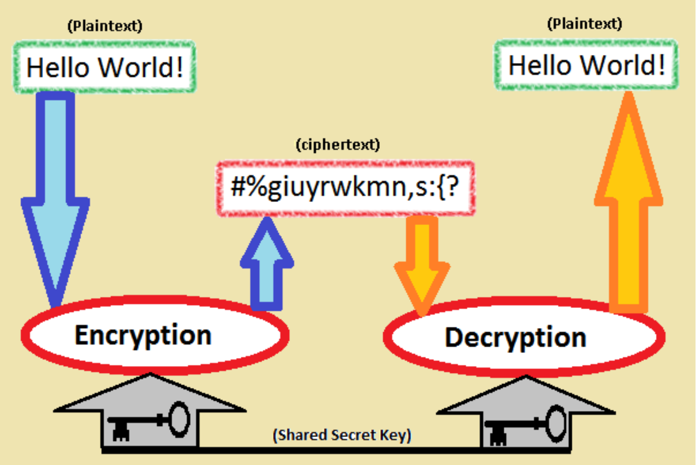
Security controls (security countermeasures)

The CIA triad of Confidentiality, Integrity, and Availability is at the heart of information security.



Confidentiality

- Confidentiality comprises all measures to prevent the access to secret information by an unauthorized third party
- Data is secured by **encryption**
  - Science of **Cryptography**
- Information in **plain text** is transformed into an apparently useless text string (**cypher text**) by a specific **method** applying a **key**
  - Method has to be reversible
    - Original information has to be receivable from the cypher text by a respective key
  - Example
    - Caesar-Code
    - SSL/TLS protocol for TCP/IP



Data integrity

- **Data integrity** is the maintenance and the assurance of the **accuracy** and **consistency of data** over its entire life-cycle
  - i.e., data keep their original form
  - Identification of **intentional** or **unintentional** (transmission error) changes of data, physical and logical integrity (e.g., database rules)
- Common techniques are the usage of **hash functions**
- A hash function can calculate a unique **hash-value (fingerprint)** for a given string
  - Hash-value is **typically shorter** than the original text, often 128 to 160 Bit
  - Hash-functions are usually **not reversible**, i.e., the original information (or other inferences) can not be calculated from the hash-value
  - **Secure hash functions** guarantee that it is (nearly) impossible to generate for two different messages the same hash-value (message digest)
- Examples: Secure Hash Algorithms (e.g., SHA-256, SHA-384), Message Digest (MD5, 128 Bit, deprecated by security experts)

Availability

- **Availability** guarantees information and services to be at an authorized user's disposal
  - In practice, this is the **probability that a system fulfils specific requests** within a defined time span

$$A = \frac{E[\text{uptime}]}{E[\text{uptime}] + E[\text{downtime}]}$$

  - Quality criteria and **KPI** of a system Key Performance Indicator(KPI) — like uptime, latency, or response time
- This control is mostly realized by technical provisioning

  Duplicate servers, storage, and systems ready to take over if something fails.
  - **Redundancy/Backup**-policy - THE most important method

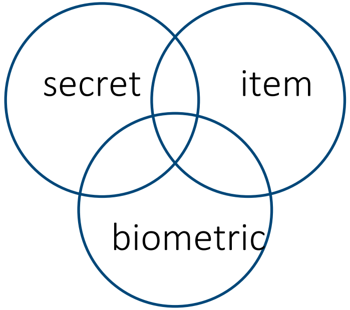
  Block attacks like ping floods (ICMP) that try to overload the system.
  - **Firewalls** - prohibits many attacks, e.g. ping (ICMP protocol) reject

  Define which system services are most important. Emergency services get higher priority than file downloads.
  - **Priorities** - Definition of priority hierarchy for all system services
  - **Administrative methods** - "Fair use"-principle, threat of implications, account lock, …

universität
wien

Authentication

- Authentication: the process of confirming the identity of a user or communication partner
- Authorization: identities of users are often assigned certain rights
- Generally, 3 approaches
  - Knowing of a Secret - Passwords, Pass phrases
  - Ownership of an Item - Chip cards (but copying must be difficult), security keys
  - Biometric characteristics - fingerprints, retina scans
- Often combination of these approaches!



Derived Controls (1)

- **Data authenticity:** data has not been modified while in transit (**data integrity**) and receiving party can verify the source of the message (**provenance of data**)
  - Typically, combine message authentication codes (MACs), authenticated encryption (AE) or digital signatures.
  - Does not include non-repudiation
  - Examples: **Digital Signatures,** PGP with emails
- **Non-repudiation:** assert the **assignment of an action to a subject**, a proof of authenticity of action, which cannot be denied by an authenticated party
  - Examples
    - Send (i) and receive (ii) of messages: **provide proof that (i) you indeed sent the message, (ii) sent indeed by the claimed sender, and message wasn't tampered with during transmission.**
    - Superuser/Administrator responsibilities: **track actions and tie them back to the specific administrator who performed the actions.**
  - Methods are typically **digitally signed acknowledgments**

Derived Controls (2)

- **Access control** is the **selective restriction of access** to a place or other resource
  - Permission to access a resource is called **authorization**.
  - Access control builds on correct **authentication** of user (or programs)
  - Examples: Access control of an OS for single users, group, or rest of world, ABAC (Attribute-Based Access Control) vs. RBAC (Role-Based Access Control)
- **Accountability** is a service **protocolling which user has accessed which resources** at what time
  - Needs working **access control** and **non-repudiation**
  - Examples
    - Transaction logs (date, time, number and duration of a used resource
    - Basis of commercial use (building block of cloud computing)

Classical Principles for Protected IT Systems (1)

- Saltzer and Schröder 1975, http://www.cs.virginia.edu/~evans/cs551/saltzer/
  - Historical starting point ensuring security in Multics operating system (1974), Unix (1974), …
- **Economy of mechanism**: Used security mechanisms and processes must be simple to use that they can be applied automatically and routinely
  - *„Keep the design as simple and small as possible.“*
- **Fail-safe defaults**: Base access decisions on permission rather than exclusion
  - *„The default situation is lack of access.“* The default setting should be no access. Permissions must be granted deliberately, not assumed.
- **Complete mediation**: It forces a system-wide view of access control and implies that a foolproof method of identifying the source of every request must be devised
  - *„Every access to every object must be checked for authority.“*
- **Open design**: The design of a system should not be secret, and all protection mechanisms must be open
  - *„No security through obscurity.”“*

Classical Principles for Protected IT Systems (2)

- Separation of privilege: No single accident, deception, or breach of trust is sufficient to compromise the protected IT system
  - *„Two keys“, „Multi-factor …“*
- Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job
  - *„Just-Need-to-know security rule“*
- Least common mechanism: Minimize the amount of mechanism common to more than one user and depended on by all users.
  - *„Restrict processes to one user only (if possible)“*
- Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly
  - *„Mental image of user’s protection goals matches the mechanisms to use“*

Security Engineering

- **Security Engineering** comprises all **tools**, **processes** and **methods** for **design**, **implementation** and **test** of **protected IT-systems**.
  - Structured engineering approach („Security by Design“)
  - Goal: Development of a comprising security model
- Two examples
  - IT-Grundschutz
    - The **IT Baseline Protection Catalogs**, or **IT-Grundschutz-Kataloge**, are a collection of documents from the German Federal Office for Security in Information Technology (BSI, Bundesamt für Sicherheit in der Informationstechnik) that provide useful information („**Best Practice**“) for detecting weaknesses and combating attacks in the information technology (IT) environment (IT cluster), https://www.bsi.bund.de/
  - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
    - The OCTAVE method is an approach used to assess an organization's information security needs based on **risk analysis**.
    - Developed in cooperation of Carnegie Mellon University, CERT (Computer Emergency Response Team) and support of department of defense of the USA, http://www.cert.org/octave/

Technical security concepts

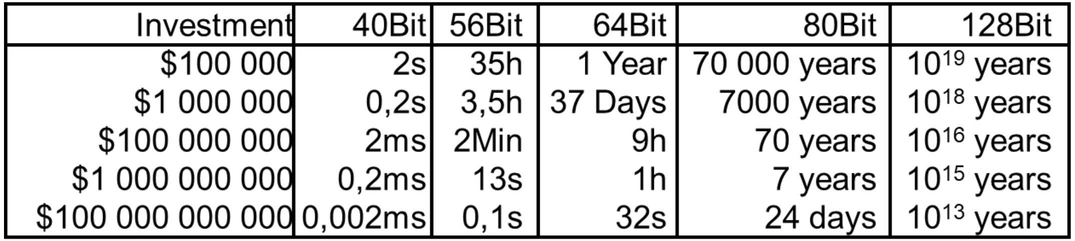
- Encryption
- Certificate
- Digital signatures
- PGP method
- HTTPS

Encryption (1)

- TCP/IP based protocols have originally no encryption
  - Communication in plain text, i.e., readable for third parties (sniffing attack)
- Led to development of **techniques for secure communication** in the presence of third parties (**Cryptography**)
  - **data confidentiality**, **data integrity**, **authentication**, and **non-repudiation** are central to modern cryptography
  - A **cipher** (or cypher) is a pair of algorithms that create the **encryption** and the **reversing decryption**. The **key** is a secret (ideally known only to the communicants), usually a (short) string of characters, which is needed to decrypt the ciphertext.
  - **(Bit-)length of key (=key space) proportional to security**, e.g., 56 Bits results in $2^{56} = 72{,}057{,}594{,}037{,}927{,}936$ possible keys, e.g., 256 Bits results in $2^{256} = 2^{200} * 2^{56}$
  - SHA-algorithms designed for fast computing, but BCrypt, PBKDF2 or SCrypt configurable to take much longer to compute (reduced hash rate - hashes/sec), hence, may be harder to break – depends on use case!!

Encryption (2)

- Necessary time to crack key with Brute-Force approach – only an estimate



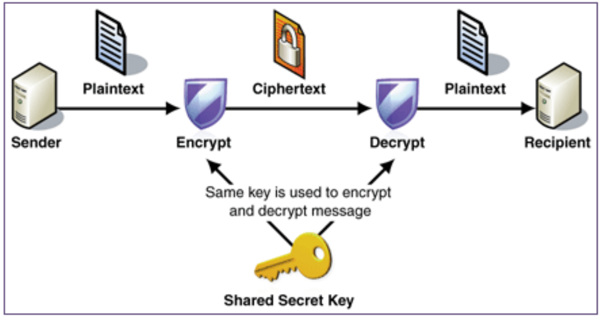
Investment	40Bit	56Bit	64Bit	80Bit	128Bit
$100 000	2s	35h	1 Year	70 000 years	10^{19} years
$1 000 000	0,2s	3,5h	37 Days	7000 years	10^{18} years
$100 000 000	2ms	2Min	9h	70 years	10^{16} years
$1 000 000 000	0,2ms	13s	1h	7 years	10^{15} years
$100 000 000 000	0,002ms	0,1s	32s	24 days	10^{13} years

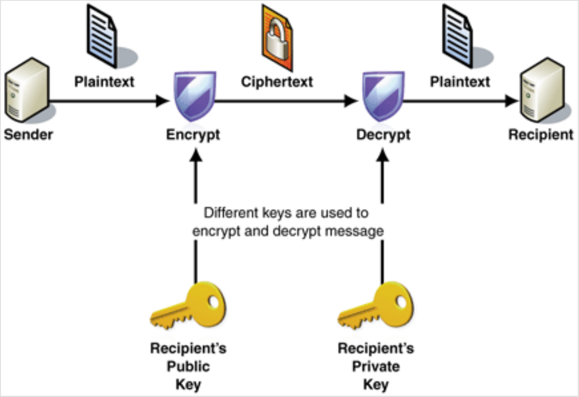
Source: TenFour

- In near future we expect significantly smaller numbers because of Optical Computing, Quantum Computing, …
  - Hence, such future computing paradigms will break todays security measures!

Encryption Methods

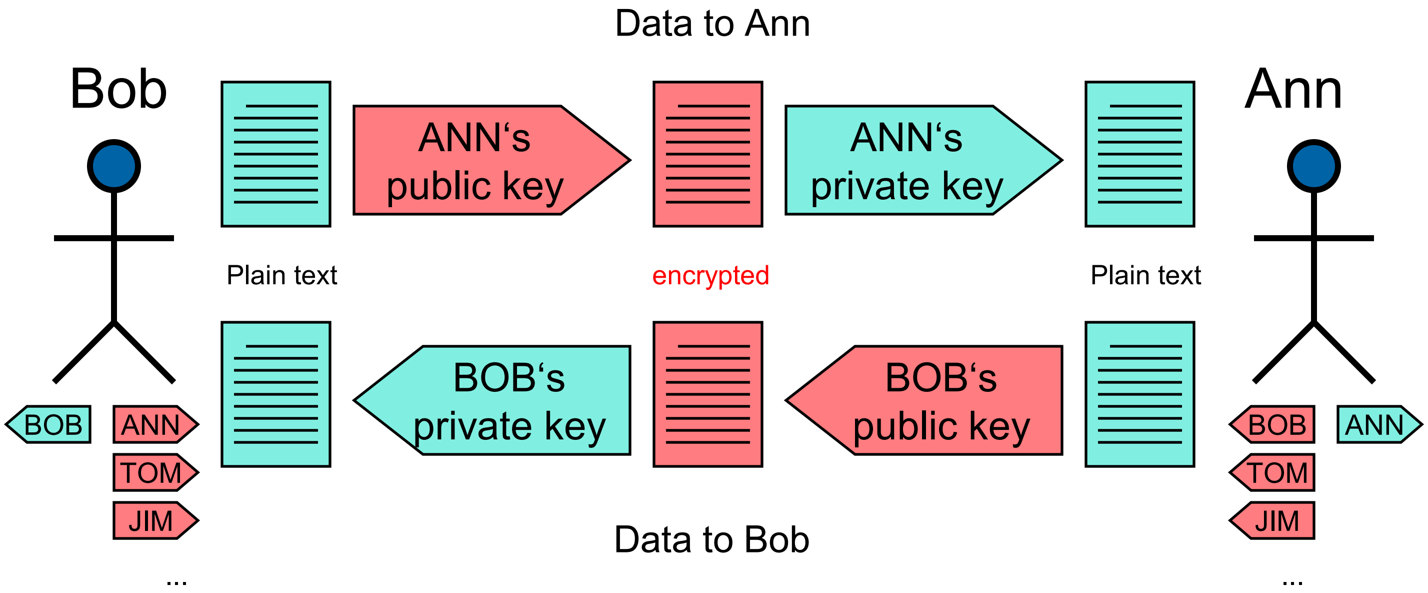
- Symmetric algorithms
  - One key (Single-key) is used/shared for Encryption and Decryption
    - RC2, RC4, Triple-DES
    - IDEA (International Data Encryption Algorithm), key length 128 Bit
- Asymmetric algorithms
  - Two mathematically related keys, first key encrypts, second key decrypts (or reverse)
    - One key can not be calculated from the other key
  - Public-Key, aka Encryption-Key, publicly accessible in the network
  - Private-Key, aka Decryption-Key, secret, only known by the owner
    - Diffie-Hellman, first method
    - RSA, Rivest-Shamir-Adleman, developed 1978, variable key length (usually 512-2048 Bit)
    - DSS, Digital Signature Standard, max. 1024 Bit





Asymetric (Public-Key) Encryption

Guarantees **Confidentiality**

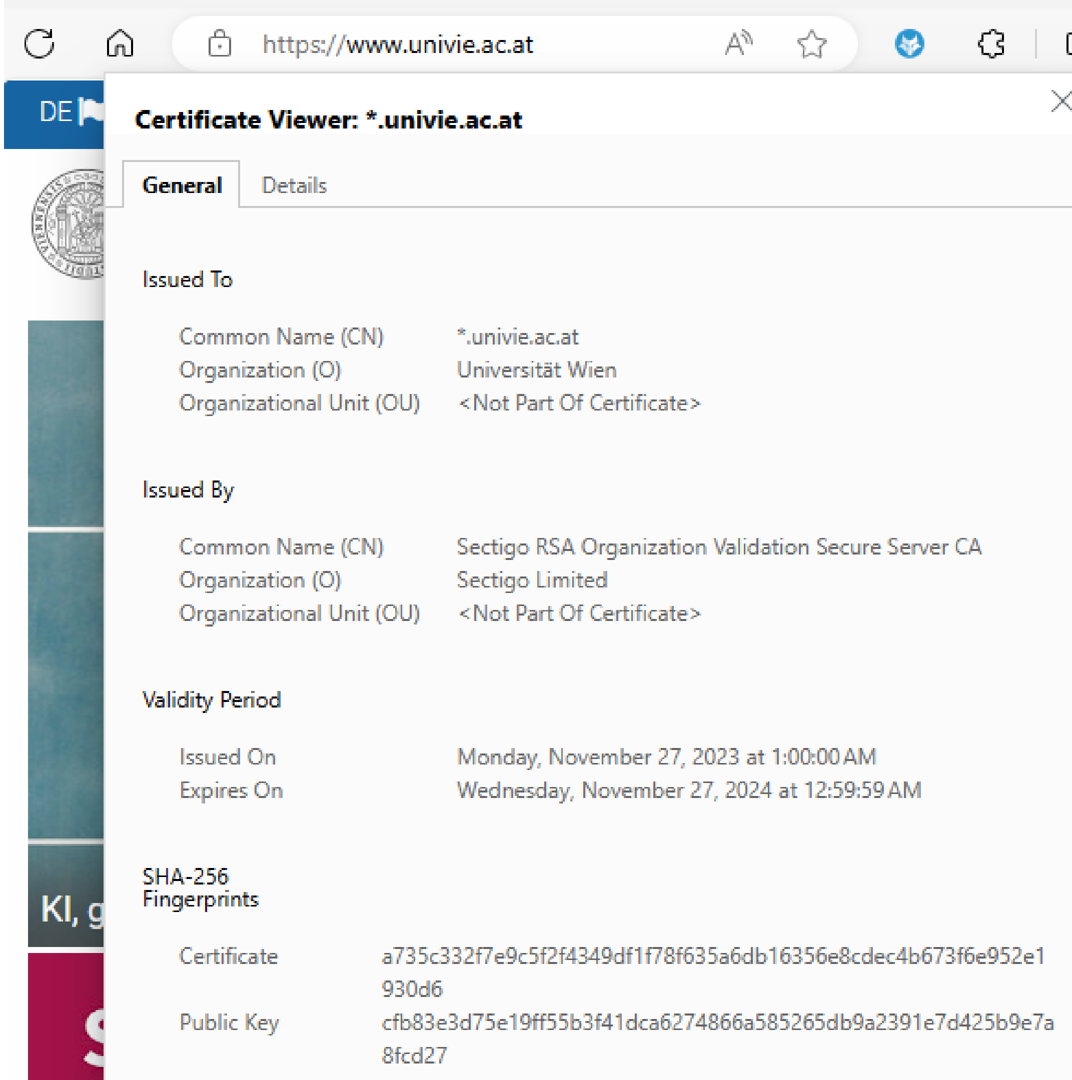


Certificate (1)

- A (Public Key) **Certificate** is a digital document that maps a public key to the identity of a person
  - **Certificate Authority** guarantees the identity of this individual (person)
  - With creation of certificate a **key-pair** (**private and public key**) is **instantiated** and assigned to the owner of the certificate
- Essential components
  - Serial number
  - Personal data (name, company)
  - **Public key** of person or organization
  - A **signature** of the **certificate authority** by the issuer's private key
  - A certificate contains **no secret information**!

Certificate (2)

- Validity duration of Certificate
  - Invalid after deadline
  - Possibility of Certificate Revocation
- Usually, a certificate follows Standard X.509, Vers. 3



Certificate Viewer: *.univie.ac.at

General | Details

Issued To

Common Name (CN)	*.univie.ac.at
Organization (O)	Universität Wien
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Sectigo RSA Organization Validation Secure Server CA
Organization (O)	Sectigo Limited
Organizational Unit (OU)	<Not Part Of Certificate>

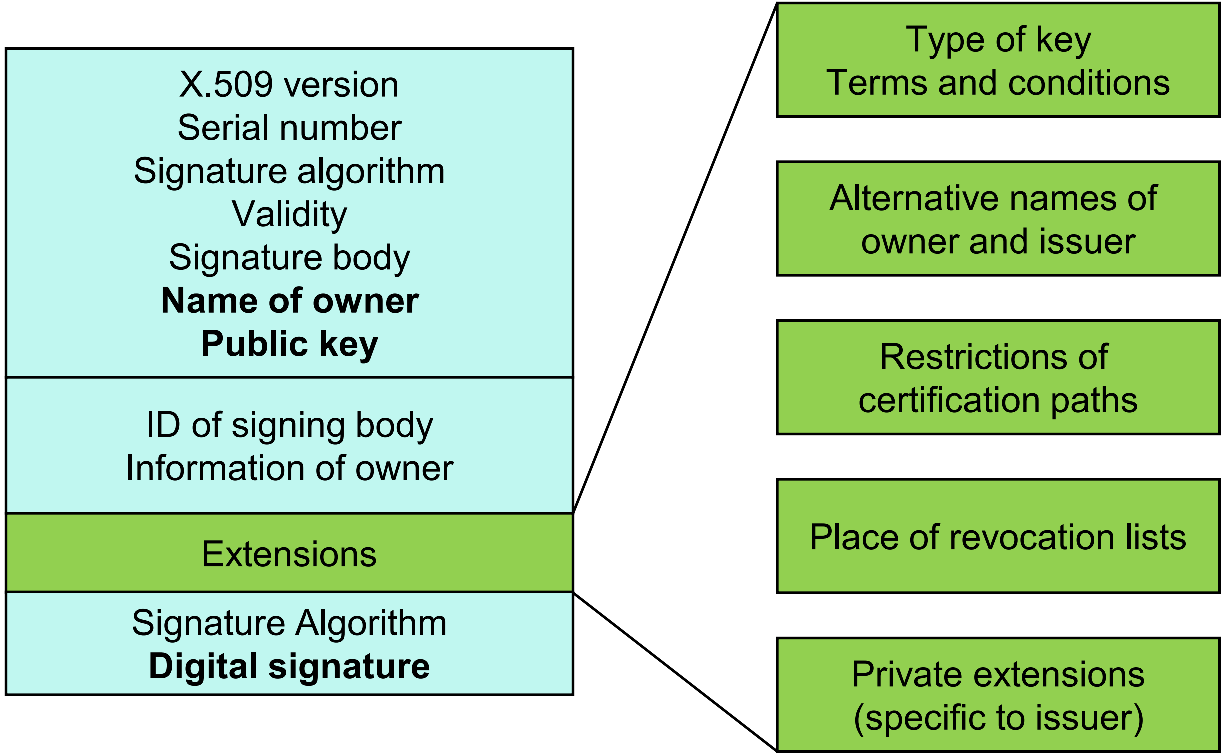
Validity Period

Issued On	Monday, November 27, 2023 at 1:00:00 AM
Expires On	Wednesday, November 27, 2024 at 12:59:59 AM

SHA-256 Fingerprints

Certificate	a735c332f7e9c5f2f4349df1f78f635a6db16356e8cdec4b673f6e952e1930d6
Public Key	cfb83e3d75e19ff55b3f41dca6274866a585265db9a2391e7d425b9e7a8fcd27

Certificate according to ITU-T X.509v3



X.509 version
Serial number
Signature algorithm
Validity
Signature body
Name of owner
Public key

ID of signing body
Information of owner

Extensions

Signature Algorithm
Digital signature

Type of key
Terms and conditions

Alternative names of owner and issuer

Restrictions of certification paths

Place of revocation lists

Private extensions (specific to issuer)

Certification Authority

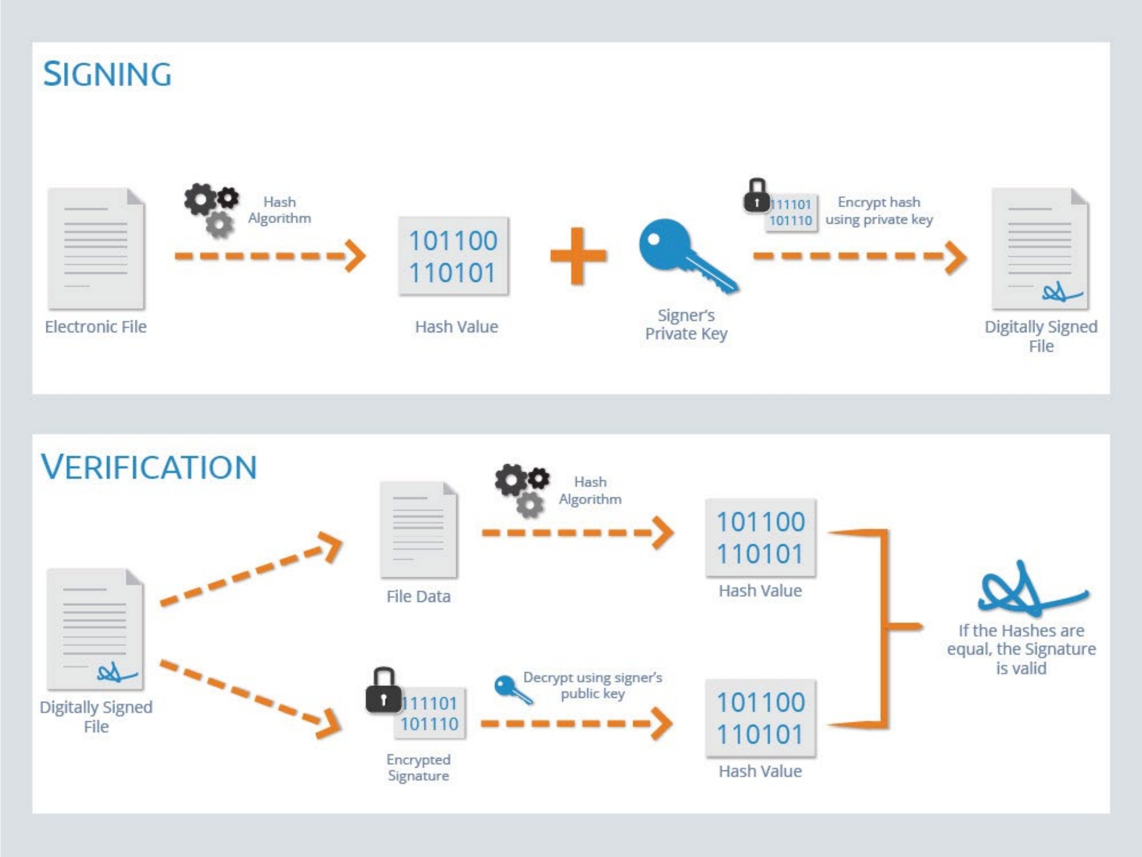
- A **Certification Authority** creates Certificates
  - Governmental and commercial organizations, …, e.g.,
    - MIT, Symantec/Verisign, Teletrust (www.teletrust.de), CERT (www.cert.dfn.de)
    - IdenTrust, DigiCert, and Sectigo
  - Free certificates, e.g.,
    - Let’s Encrypt (https://letsencrypt.org/) is a free, automated, and open Certificate Authority
  - In Austria, e.g.,
    - A-Trust Company (https://www.a-trust.at/)
    - Arge Daten – Österreichische Gesellschaft für Datenschutz (Verein)
- **Austrian signature law** (Österreichische Signaturgesetz)
  - Since 1.1.2000 (SigG, BGBl 190/99), based on EU law
  - **Equality between electronic signature and handwritten signature**
    - In law and business context valid as piece of evidence. Also used at University of Vienna.

Digital Signature

- A **digital signature** is a mathematical scheme for demonstrating the authenticity of digital messages or documents
  - A valid **digital signature process** gives a recipient reason to believe that the message was created by a known sender (**authentication**), that the sender cannot deny having sent the message (**non-repudiation**), and that the message was not altered in transit (**integrity**)
- Hereby the followings steps are performed:

1. A **digital fingerprint (digest**) is created from the information by a mathematical algorithm, i.e., a binary string identifier unique to the information is computed
2. This **digest** is **encrypted by the sender with its private key.** Encrypted digest plus information is sent.
3. The receiver can **decrypt the digest with the public key of sender** and, hence, can check if the digest was tempered

Checking a Digital Signature

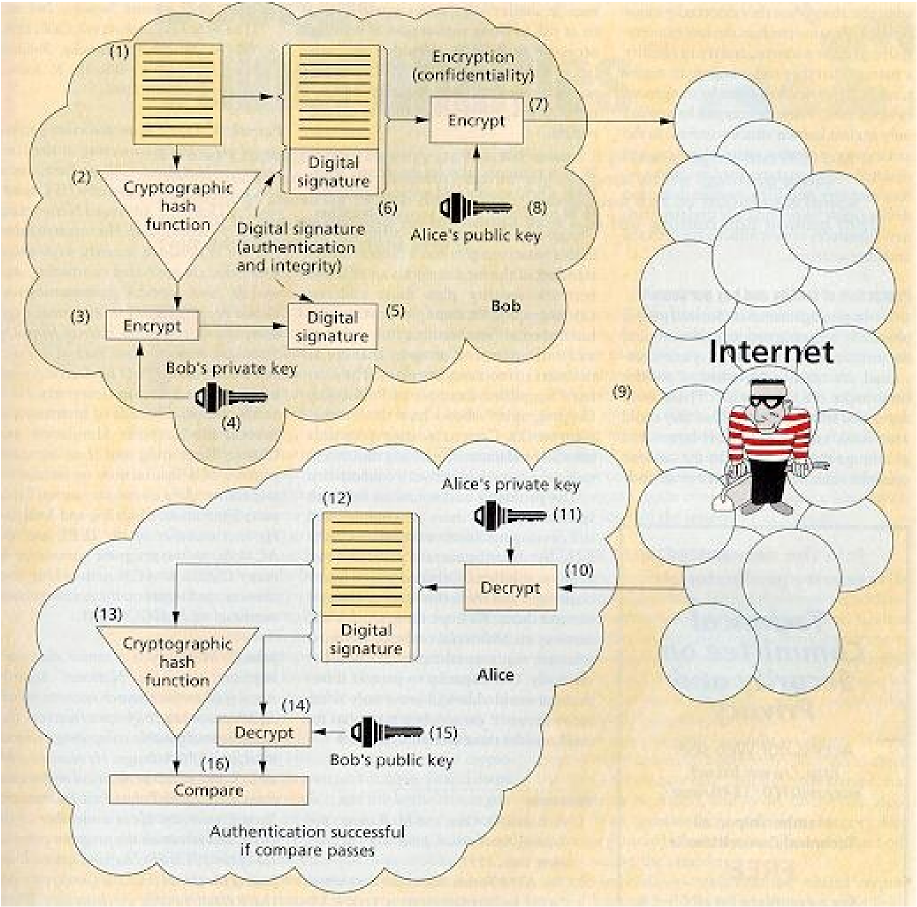


Hash Algorithms - Examples

- **Hash algorithms** for calculation of digest
- **MD5 algorithm** (Message-Digest Algorithm 5)
  - Widespread technique
  - Creates a 128 Bit hash vale from arbitrary message
  - MD5 was developed by Ronald L. Rivest in 1991 and is judged as insecure today
    - As of 2019, MD5 continues to be widely used, despite its well-documented weaknesses and deprecation by security experts.
- **SHA-series** (Secure Hash Algorithm)
  - The **Secure Hash Algorithms** are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST)
  - SHA-1 (160 Bit hash value), was judged as secure till 2010
  - SHA-2 algorithm with SHA-224, SHA-256, SHA-384 and SHA-512 (numbers denote the length of hash value), SHA-512/224, SHA-512/256
  - SHA-3 algorithms with SHA3-224, SHA3-256, SHA3-384, SHA3-512 + SHAKE-128 and SHAKE-256

PGP Method

- "Pretty-Good-Privacy" method
  - A program for secure transmission of emails guaranteeing confidentiality, integrity and authentication
- Combination of Public-Key encryption and Digital signature
  - Originally developed by Phillip Zimmermann
  - Worldwide distributed despite protection by US government



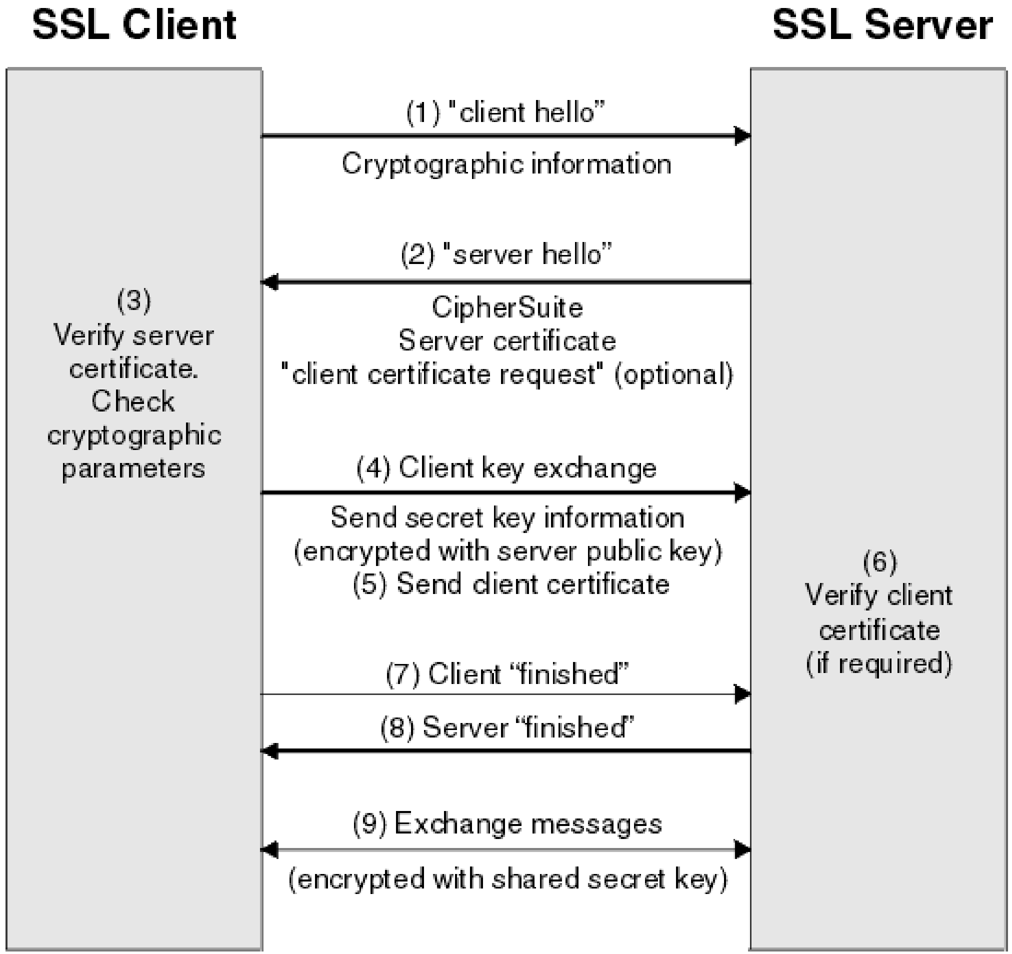
HTTPS Method

- HTTPS aka HTTP Secure is the usage of HTTP employing encryption and authentication
  - Encrypted connection with a browser denoted by "https://" (TCP-Port 443) instead of "http://" (TCP-Port 80)
- Goals:
  - Web-server authenticates to a client (asymmetric encryption)
  - End-to-end-encryption of the connection (symmetric encryption)
- For authentication and decryption: **SSL/TLS**
  - Secure Sockets Layer/ Transport Layer Security („Located“ between HTTP and TCP layer)
  - SSL/TLS is used also in other application protocols, e.g., SMTPS, IMAPS, and FTPS
  - SSL is transparent for the user
    - SSL was developed by Netscape till version 3.0 and then shifted to TLS by IETF; SSL versions deprecated since 2015.
    - Even today only TLS is used we speak of SSL
- Certification Authority (CA) and Public Key Infrastructure (PKI) for certificates are necessary

HTTPS Workflow (1)

1. The SSL or TLS client sends a "client hello" message that lists cryptographic information such as the SSL or TLS version and, in the client's order of preference, the CipherSuites supported by the client. The message also contains a random byte string that is used in subsequent computations. The protocol allows for the "client hello" to include the data compression methods supported by the client.
2. The SSL or TLS server responds with a "server hello" message that contains the CipherSuite chosen by the server from the list provided by the client, the session ID, and another random byte string. The server also sends its digital certificate.
3. The SSL or TLS client verifies the server's digital certificate.
4. The SSL or TLS client sends the random byte string that enables both the client and the server to compute the secret key to be used for encrypting subsequent message data. The random byte string itself is encrypted with the server's public key.
5. If the SSL or TLS server sent a "client certificate request", the client sends a random byte string encrypted with the client's private key, together with the client's digital certificate, or a "no digital certificate alert".
6. The SSL or TLS server verifies the client's certificate.
7. The SSL or TLS client sends the server a "finished" message, which is encrypted with the secret key, indicating that the client part of the handshake is complete.
8. The SSL or TLS server sends the client a "finished" message, which is encrypted with the secret key, indicating that the server part of the handshake is complete.
9. For the duration of the SSL or TLS session, the server and client can now exchange messages that are symmetrically encrypted with the shared secret key.

HTTPS Workflow (2)
SSL Scheme



SSL Client

SSL Server

(1) "client hello"

Cryptographic information

(2) "server hello"

CipherSuite
Server certificate
"client certificate request" (optional)

(3)
Verify server certificate.
Check cryptographic parameters

(4) Client key exchange

Send secret key information
(encrypted with server public key)
(5) Send client certificate

(6)
Verify client certificate
(if required)

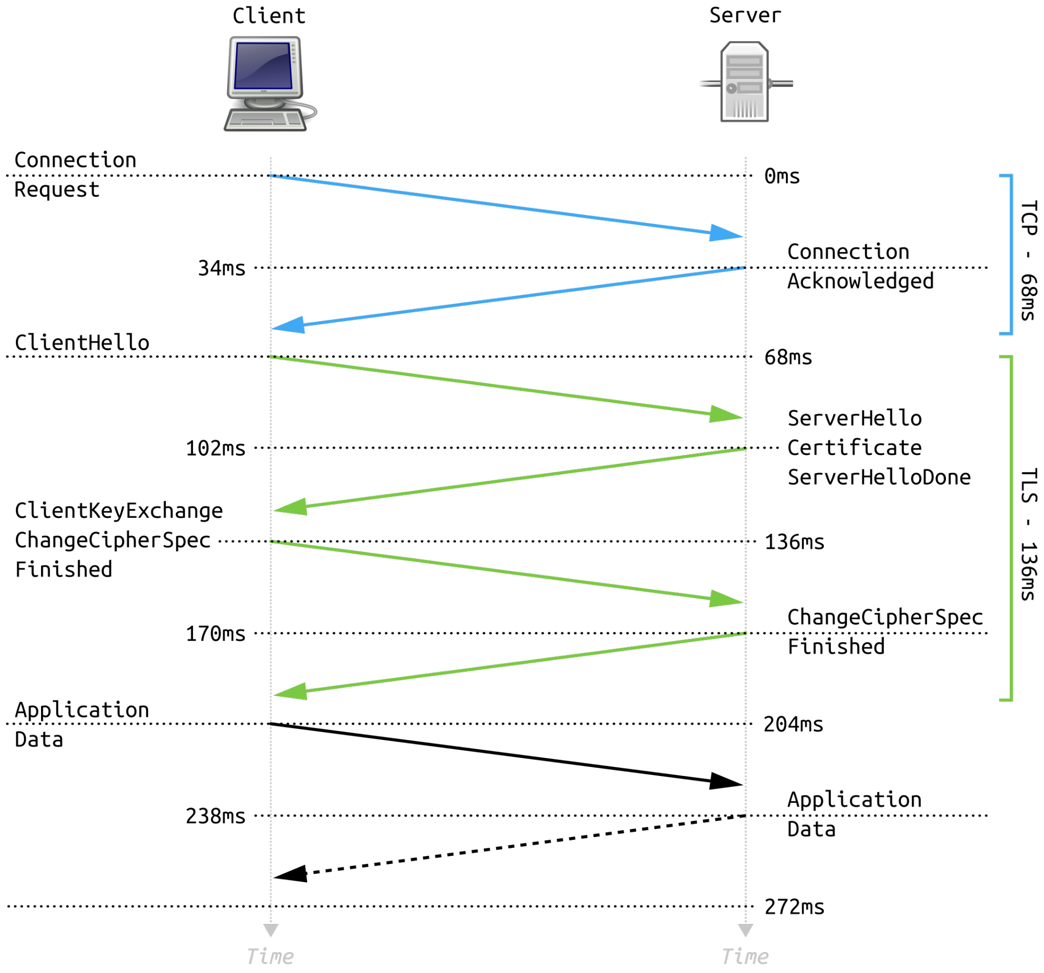
(7) Client "finished"

(8) Server "finished"

(9) Exchange messages

(encrypted with shared secret key)

HTTPS Workflow (3)
TLS Scheme



Client
Server
Connection Request
0ms
Connection Acknowledged
34ms
TCP - 68ms
ClientHello
68ms
ServerHello
Certificate
ServerHelloDone
102ms
ClientKeyExchange
ChangeCipherSpec
Finished
136ms
TLS - 136ms
ChangeCipherSpec
Finished
170ms
Application Data
204ms
Application Data
238ms
272ms
Time
Time