Kryptografie a počítačová bezpečnost

Úvod

Informace k předmětu

- Kontakt
  - Kancelář EA439
  - eliska.ochodkova@vsb.cz
  - Všechny důležité informace na www.cs.vsb.cz/ochodkova
- Organizace výuky
  - Materiály na MS Teams nebo LMS (doplňkově na mém webu k předmětu) – co Vám vyhovuje?
  - Sledujte web a emaily na své školní adrese
  - Omluvy ze cvičení předem
  - Konzultace osobně i přes MS Teams v předem domluveném čase

Informace k předmětu

- Požadavky na zápočet (45 bodů max, 25 min):
  - Povinná (bodovaná) docházka na cvičení
    - Pro obor IVT a PRM (zkrácený semestr, 2. ročník) min 8 bodů, max 10 bodů
    - Pro obor ICB min 9 bodů, max 12 bodů
    - V případě, že cvičení bude zrušeno se na náhradě bodů domluvíme
  - Splnění 3 dílčích úkolů (zadaných průběžně)
    - Dodržení termínu odevzdání!!!
    - IVT a PRM max 11, 12, 12 bodů
    - ICB max 11, 11, 11 bodů
- Písemná zkouška (ICB, IVT, PRM) 55 bodů max, 20 min

O čem to bude?

- O čem to bude?
  - Výlet do historie
  - Symetrická kryptografie
  - Asymetrická kryptografie
  - Kryptografické hashovací funkce
  - Digitální podpis
  - Protokoly
  - Kryptoanalýza
  - …
- To vše v kontextu kryptografie jako nedílné součásti zabezpečení ICT

Literatura

- https://ptgmedia.pearsoncmg.com/images/9780132789462/samplepages/0132789469.pdf
- https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf
  kapitola 1

Bezpečnost ICT

- Aspekty počítačové bezpečnosti (lépe bezpečnost ICT) jsou velmi široké, od hrozeb a zranitelných míst až po způsoby ochrany atd.
- Informace jsou strategickým zdrojem
  - ICT svěřujeme svoje know-how, soukromí, citlivé informace, …,
  - na ICT je závislá řada procesů (průmyslových, obchodních, medicínských, …),
  - ! požadavky na ochranu informací v rámci ICT jsou dány přímo v **právním řádu** (ČR i EU), např.:
    - Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů https://www.zakonyprolidi.cz/cs/2019-110
    - Zákon č. **181/2014 Sb.,** o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) https://www.zakonyprolidi.cz/cs/2014-181
    - eIDAS, nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce https://cs.wikipedia.org/wiki/EIDAS
    - Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze 23. listopadu 2001
    - …

Standardy (normy)

- Požadavky na ochranu informací v rámci ICT (a bezpečnost ICT) jsou dány také ! **profesními standardy**
- Standardy (normy) *de facto* a *de jure*
- *de jure*
  - Mezinárodní: ISO/IEC 27000 https://www.iso.org/news/ref2266.html je kodex norem, který je zaměřen na systémové řízení informační bezpečnosti
  - Národní: ČSN české normy, BS – britské standardy, atd. ….
  - Důležité jsou standardy vydávané americkým institutem NIST https://www.nist.gov/cybersecurity
- *de facto*
  - W3C standardy, viz https://www.w3.org/standards/xml/security, např. XML Signature (https://www.w3.org/TR/xmldsig-core1/)
  - RFC (https://www.ietf.org/standards/rfcs/), např. IP Security (IPsec) https://datatracker.ietf.org/doc/html/rfc6071, https://www.karlin.mff.cuni.cz/~tuma/ciphers/2_rfc.pdf
  - ITIL, COBIT, …

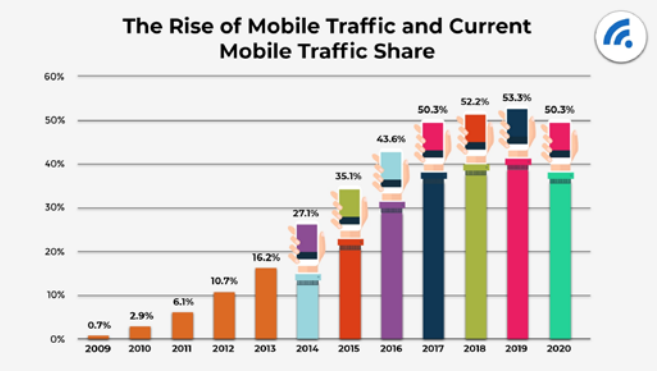
V minulosti

- Po dlouhou dobu byla bezpečnost většinou ignorována
- Počítačový průmysl "přežíval", především se snažil překonat technologické a ekonomické překážky. V důsledku toho bylo učiněno mnoho bezpečnostních kompromisů.
- Existovala sice teorie a dokonce i příklady systémů s velmi dobrou bezpečností, ale byly neúspěšné nebo byly ignorovány
  - např. jazyk ADA, 80. léta USA,
    - výkonný bezpečný a snadno použitelný, viz http://archive.adaic.com/intro/WhyAda.html (Ada has the only compilers that are validated by the U.S. Government and other agencies throughout the world, including the International Organization of Standards (ISO). Each compiler is tested on thousands of programs before it receives validation.) nebo http://www.root.cz/clanky/bezpecne-programovani-ala-ada/ (silný typový systém, integritní omezení, …)
    - pojmenován po Adě Lovelace (1815-1852), která je považována za první programátorku

Počátek tisíciletí

- „Počítače“ (rozuměj v širokém slova smyslu, tj. včetně vestavěných počítačů apod., od automobilových řídicích jednotek po průmyslové roboty) jsou všudypřítomné, jsou velmi výkonné a velmi levné.
- Internet a další typy sítí (senzorové apod.)
  - Počítače jsou propojeny a vzájemně závislé
  - Tato závislost zvětšuje dopad případných chyb, útoků…
- Od počátku tisíciletí došlo k prudkému nárůstu zájmu o bezpečnost ICT.

Současnost



- Global - 2021 Forecast Highlights https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf
- 2023 Global Networking Trends Report https://www.rmol.cz/sites/default/files/prilohy/xa-09-2023-networking-report.pdf
- Key Internet Statistics to Know in 2024 (Including Mobile) https://www.broadbandsearch.net/blog/internet-statistics
- WhatsApp Usage Statistics: How Many People Use It in 2023 https://techjury.net/blog/whatsapp-usage-statistics/
- How Many IoT Devices Are There in 2024? https://techjury.net/blog/how-many-iot-devices-are-there/#gref
- How Much Data Is Created Every Day in 2023? https://techjury.net/blog/how-much-data-is-created-every-day/#gref
- 25+ Impressive Big Data Statistics for 2024 https://techjury.net/blog/big-data-statistics/
- How Many Software Engineers Are There In The US? (2024 Statistics) https://techjury.net/blog/how-many-software-engineers-in-us/
- …

Kyberkriminalita

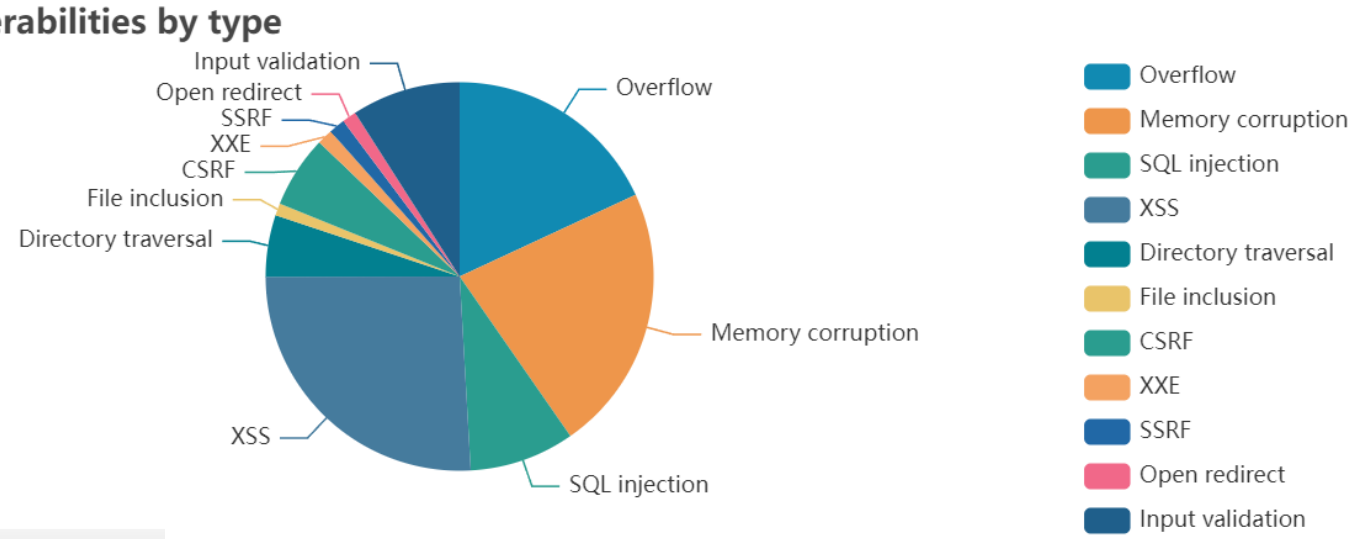
- Projevy kyberkriminality
- Sociální inženýrství (Sociotechnika), Malware, Ransomware
- Spam, Hoax, Podvodné nabídky
- Phishing, Pharming, Spear Phishing, Vishing, Smishing
- Podvodné webové stránky (firmy)
- Hacking, Cracking
- Internetové (počítačové) pirátství
- Sniffing
- DoS, DDoS, DRDoS (distributed reflection denial-of-service) útoky
- Šíření závadového obsahu, Kyberšikana, Sexting, Kyberstalking
- Krádež identity
- ….

Současnost

- Trendy:
  - Kyberzločinci se zaměřují mj. na deepfake, kryptoměny nebo mobilní peněženky (https://bezpecneit.cz/aktuality/).
    - Deepfake – zjednodušeně řečeno nahrazování obličejů třeba ve videích či na fotografiích díky umělé inteligenci
    - Fenomén poslední let, jen v říjnu 2019 se na sociálních sítích objevilo na 15 000 deepfake videí, které zaměnily původní tváře za falešné.
    - V listopadu roku 2020 došlo k případu, kdy hlas generovaný pomocí AI napodoboval jako deepfake výkonného ředitele jedné energetické společnosti a způsobil podvodný převod v hodnotě asi 5,5 milionu Kč.
- 20 Generative AI, ChatGPT & Deepfake Statistics You Should Know For 2024 https://www.thesslstore.com/blog/generative-ai-statistics/
- Top 10 Threats https://www.mcafee.com/enterprise/en-us/threat-center.html

The Most Vulnerable Software in 2023

https://www.cvedetails.com/top-50-products.php?year=2023



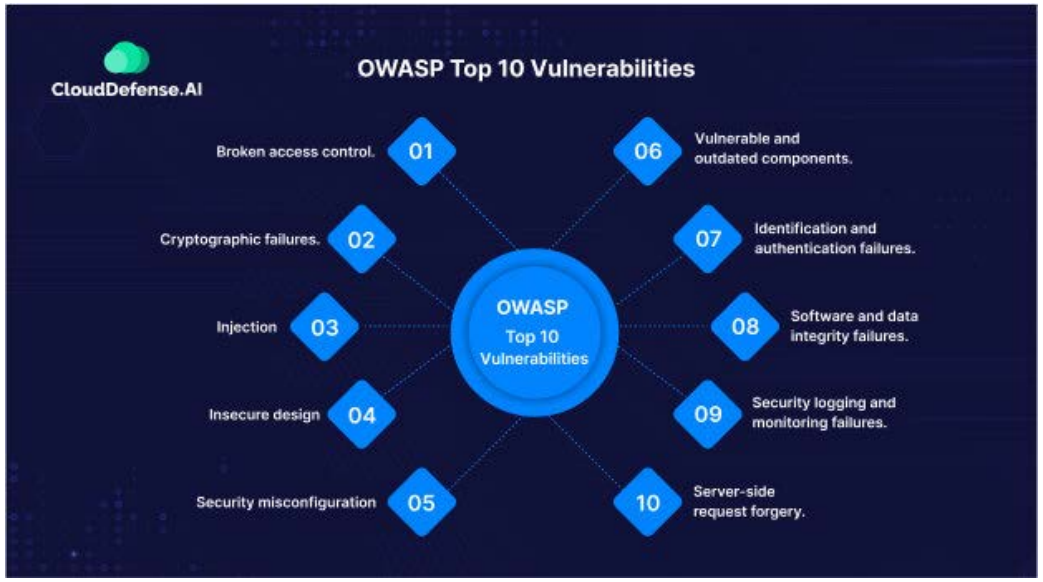
Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2023

Go to year: 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	1421
2	Windows Server 2022	Microsoft	OS	566
3	Windows Server 2019	Microsoft	OS	541
4	Fedora	Fedoraproject	OS	528
5	Windows 11 21h2	Microsoft	OS	509
6	Windows Server 2016	Microsoft	OS	501
7	Windows 11 22h2	Microsoft	OS	495
8	Windows 10 1809	Microsoft	OS	489
9	Windows 10 22h2	Microsoft	OS	483
10	Windows 10 21h2	Microsoft	OS	477
11	Debian Linux	Debian	OS	476
12	Windows Server 2012	Microsoft	OS	451

Zranitelnosti a hrozby (1)

- NÚKIB https://nukib.cz/cs/infoservis/hrozby/
- https://owasp.org/www-project-top-ten/
- https://www.clouddefense.ai/owasp-top-10-vulnerabilities/



NÚKIB › Infoservis › Hrozby

Hrozby a zranitelnosti

16.02.2024	Upozornění na kompromitaci routerů Ubiquity Edge OS aktérem sponzorovaným ruským státem
09.02.2024	Upozorňujeme na dvě kritické zranitelnosti v operačním systému FortiOS
05.01.2024	Upozorňujeme na hrozbu Terrapin útoku mířícího na SSH protokol
30.11.2023	NÚKIB upozorňuje na hrozbu spojenou s aplikací WeChat společnosti Tencent
24.10.2023	Upozorňujeme na zranitelnost CVE-2023-20273 v Cisco IOS XE (CVSS 7.2)
18.10.2023	Upozorňujeme na kritickou zranitelnost CVE-2023-20198 v Cisco IOS XE (CVSS 10.0)
29.09.2023	Upozorňujeme na kritické zranitelnosti v knihovnách webových prohlížečů
28.07.2023	Upozornění na zranitelnost MikroTik RouterOS CVE-2023-30799
20.06.2023	Upozorňujeme na zvýšené riziko ransomwarových útoků
12.06.2023	Upozorňujeme na kritickou zranitelnost FortiOS CVE-2023-27997
15.03.2023	NÚKIB upozorňuje na zranitelnost CVE-2023-23397

Zranitelnosti a hrozby (2)

- Americký NIST
  - https://nvd.nist.gov/vuln
  - https://nvd.nist.gov/vuln/search
- https://www.exploit-db.com/
- https://cve.mitre.org/
- A různé blogy o bezpečnostním výzkumu, doporučení výrobců, zpravodajské platformy a zpravodajské servery o kybernetické bezpečnosti

Definice bezpečnosti

- **Bezpečnost** je („well-being“) stav systému, kdy je možnost úspěšné dosud nezjištěné krádeže, falšování, narušení informací a služeb udržována na nízké nebo přípustné úrovni.
- Pod pojmem bezpečnost ICT obvykle rozumíme ochranu odpovídajících systémů a informací, které jsou v nich
  - uchovávány, zpracovávány a přenášeny.
  - Součástí takto obecně chápané bezpečnosti ICT je také
    - fyzická bezpečnost (ochrana před přírodními hrozbami a fyzickými útočníky)
    - a personální bezpečnost (ochrana před vnitřními útočníky, …).

(Počítačový) systém

- **(Počítačový) systém**, ve kterém jsou zpracovávána, uchovávána, přenášena data, která jsou nositeli informací, obsahuje následující tzv. **aktiva**:
  - **hardware** – síťové prvky, procesor, paměti, terminály, atd.,
  - **software** - aplikační programy, operační systém atd.,
  - **data** - data uložená v databázi, výsledky, výstupní sestavy, vstupní data atd.
- **Entita** (subjekt) – osoba, proces, síťový prvek apod.

Bezpečnostní funkce (1)

- **Bezpečnostní funkce** (cíle, služby) - služby podporující a zvyšující bezpečnost datových procesů a přenosů v daném subjektu.
- Bezpečnostní funkce zajišťují (implementují) **bezpečnostní mechanismy**. Jsou to mechanismy navržené tak, aby detekovaly útoky, zabraňovaly jim, ev. pomohly zotavení se z útoků.
  - Bezpečnostní funkce jsou obvykle k dispozici uživatelům jako sada bezpečnostních služeb prostřednictvím API nebo integrovaných rozhraní

Bezpečnostní funkce (2)

- **Důvěryhodoná** (trustworthy) entita je ta, o které se věří (je o tom podán důkaz), že je implementovaná tak, že splňuje svou specifikaci == můžeme se na ni spolehnout, chová-li se tak, jak očekáváme, že se bude chovat.
- **Autorizace** (Authorization) entity pro jistou činnost rozumíme určení, že je z hlediska této činnosti důvěryhodná. Udělení autorizace si vynucuje, aby se pracovalo s autentickými entitami.
- **Utajení** (Confidentiality) - k aktivům mají přístup (== aktiva jsou čitelná) pouze autorizované subjekty.
- **Integrita** (Integrity) – aktiva smí modifikovat jen autorizované subjekty.
- **Dostupnost** (Availability (také accessibility)) - aktiva jsou autorizovaným subjektům dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo.
- **Autenticita** (autentication) – entita nebo např. původ informací je ověřitelný. Autentizací se rozumí proces ověřování pravosti identity entity (tj. uživatele, procesu, systémů, informačních struktur apod.)
- **CIA** == Confidentiality, Integrity, Availability

Bezpečnostní funkce (3)

- **Nepopiratelnost odpovědnosti** (non-repudiation) - nelze popřít účast na transakci,
- **Prokazatelnost odpovědnosti** (accountability == účtovatelnost) - záruka, že lze učinit subjekty zodpovědné za své aktivity,
- **Spolehlivost** (reliability) - konzistence zamýšleného a výsledného chování.
- Bezpečný systém je ten, na který se můžeme spolehnout že např. :
  - Udržujte naše osobní a jiné citlivé údaje v tajnosti
  - Povoluje pouze autorizovaný přístup ke zdrojům nebo jejich modifikaci
  - Poskytuje správné a smysluplné výsledky
  - Poskytuje správné a smysluplné výsledky vždy, když je chceme mít
  - …

Příklad - AAA

- **AAA** - authentication, authorization and accounting.
- Např. RADIUS protokol, RFC 2865 http://tools.ietf.org/html/rfc2865
  - Autentizace (ověření identity uživatele autentizační autoritou, v tomto případě serverem RADIUS s použitím protokolu EAP).
  - Autorizace - přidělení přístupových práv uživateli, který úspěšně absolvoval proces autentizace, respektive nepřidělení těchto práv uživateli, který autentizačním požadavkům nevyhověl.
  - Accounting (účtování) - sběr provozních informací o autorizovaném uživateli, typicky se jedná o údaje o přeneseném množství dat, trvání připojení k síti a identifikaci přístupového bodu, ze kterého bylo k síti přistupováno.

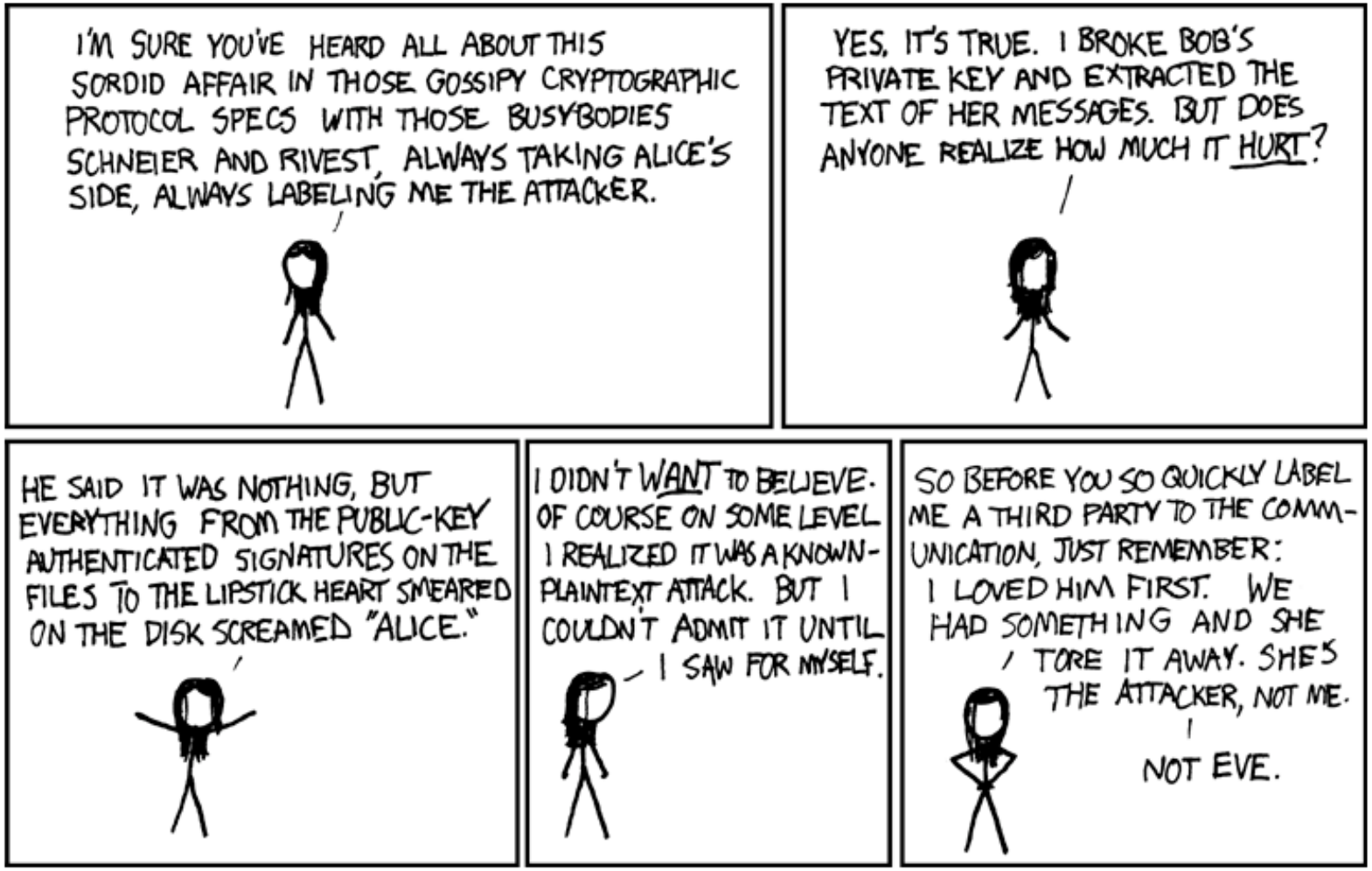
Soukromí, bezpečnost

- **Soukromí** (privacy) lze definovat jako „informational self-determination„, tj. jako možnost řídit, kontrolovat informace o své osobě.
  - Opatření na ochranu soukromí obecně upravují způsob, jakým je povolen přístup k osobním údajům a jejich prohlížení, včetně způsobu ukládání údajů a jejich využití, např. můžeme určit
    - Kdo je může znát (čist, vidět, …)
    - Kdo s nimi může nakládat
    - Pro jaké účely je může využit
    - Komu je mohou poskytnout
    - …
- **Bezpečnost** – safety x security – často chápána jako synonyma, ale
  - Bezpečnost = safety - obecně označuje stav, kdy je člověk chráněn před újmou, nebezpečím nebo rizikem. Zahrnuje fyzickou pohodu, zdraví a nepřítomnost nebezpečí.
  - Bezpečnost / zabezpečení = security - obvykle označuje opatření přijatá na ochranu před potenciálními hrozbami, včetně neoprávněného přístupu, trestné činnosti nebo jiných škodlivých aktivit.

Účastníci (role)

- **Alice a Bob** – jsou legitimní (good guys) subjekty (osoby, procesy, počítače,…), označení poprvé použil Ron Rivest 1978
- Eve, Mallory, Oscar, Trudy – nelegitimní subjekt (bad guy), obecně útočník
  - **Odesílatel** (sender) je entita (někdo nebo něco), která legitimně zasílá zprávu (budeme je označovat Alice, A).
  - **Příjemce** (reciever) je entita (někdo nebo něco), která zprávu legitimně přijímá (budeme je označovat Bob, B),
  - **Útočník** (intruder, eavesdropper, adversary, opponent atd.) je entita, která není ani odesílatelem ani příjemcem zprávy, a která se pokouší prorazit bezpečnostní mechanismus zabezpečující komunikaci mezi A a B (ozn. E, M apod.).
    - Kdo může být útočníkem (nepřítelem)? Různé typy útočníků (Organised crime, Terrorists, Amateurs, „Script kiddies“, Crackers, „Cyberwarriors„ …)

Účastníci (role)



http://xkcd.com/177/

Příklad CIA (1)

- Alice provozuje Alice’s Online Bank (AOB)
- Jaké jsou Aliciny požadavky na bezpečnost?
- Pokud Bob je zákazníkem AOB, jaké jsou jeho o bezpečnostní požadavky?
- V čem jsou požadavky Alice a Boba stejné? V čem se liší?
- A jak se na to dívá Oscar?

Příklad (2)

- C - AOB musí např. zabránit Oscarovi zjistit zůstatek na Bobově účtu
- I - Oscar nesmí mít možnost změnit Bobův zůstatek na účtu. Také Bob nesmí být schopen nesprávně měnit zůstatek na vlastním účtu
- A - AOB musí poskytovat informace vždy, když je to potřeba. A Alice musí být schopna provést transakci - pokud ne, může s podnikáním skončit.

Příklad (3)

- Jak „pozná“ Bobův počítač, že „Bob“ je opravdu Bob a ne Oscar?
- Bob se **autentizuje** heslem, heslo musí být ověřeno
  - Řešeno pomocí **bezpečnostních kryptografických mechanismů**
- Bezpečnostní problémy s hesly
- Existuje nějaká alternativa k heslům?

Příklad (4)

- Když se Bob naloguje do AOB, jak AOB pozná, že „Bob” je opravdu Bob?
  - Opět je Bobovo heslo ověřeno, ale
  - na rozdíl od předchozího případu, přidávají se problémy se **zabezpečením sítě**.
- Kriticky důležité jsou protokoly
  - „Jednoduché“ autentizační protokoly
  - „Real-world“ protokoly (SSH, SSL, IPSec, Kerberos, WPA,…)

Příklad (5)

- Jakmile Bob je ověřen AOB, pak AOB musí omezit Bobovy akce
  - Bob si nemůže zobrazit informace o účtu dalšího subjektu
  - Bob nemůže instalovat nový software, atd.
- Prosazování těchto omezení zajistí **autorizace**
- **Řízení přístupu** zahrnuje jak autentizaci a autorizaci
  - Autentizace (hesla, biometriky, …)
  - Autorizace (Access Control Lists/Capabilities, Multilevel security (MLS), firewally, IDS)

Bezpečnostní incident

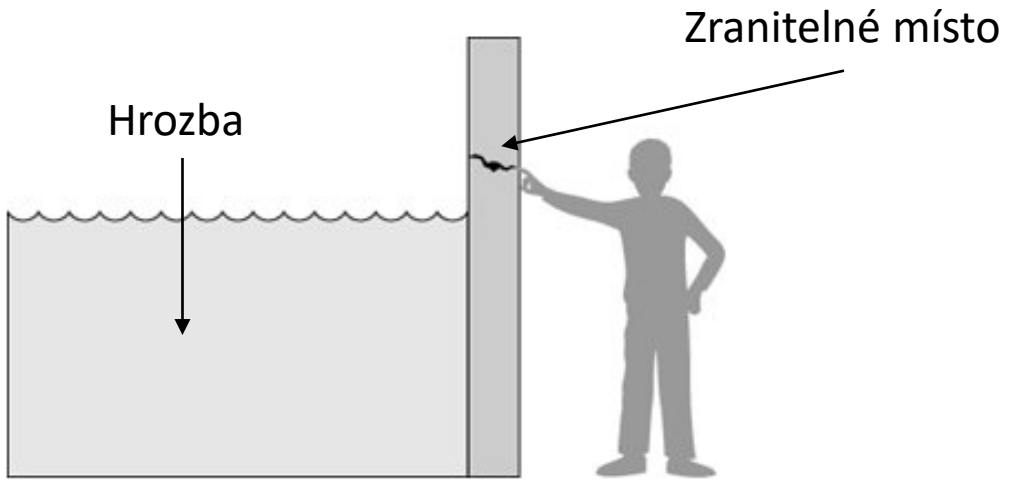
- **Bezpečnostním incidentem** rozumíme:
  - buďto úmyslné využití zranitelného místa ke způsobení škod/ztrát na tzv. aktivech
    - **útok** (attack) vyžaduje aktivního protivníka, má implicitní pojetí „záměru, úmyslu“
  - nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech
    - zhroucení serveru, které způsobí ztrátu dostupnosti, nemusí nutně být úmyslný útok.
- **Dopad** (impact) – důsledek incidentu, rozsah škod
- Bezpečnostní incident tedy představuje narušení bezpečnosti ICT a bezpečnostních pravidel (bezpečnostní politiky). Může jít např. o:
  - vydávání se za jinou oprávněnou osobu a zneužívání jejích privilegií,
  - neoprávněné zvýšení svých privilegií přístupu k informacím,
  - pokažení funkcionality softwaru doplněním skrytých funkcí,
  - zařazení se jako skrytého mezičlánku v konverzaci jiných subjektů,
  - požár, potopa,
  - Denial of Service (DoS – odepření služby), Distributed Denial of Service (DDoS – distribuované odepření služby – např. červ CodeRed).

Zranitelnost

- **Zranitelné místo** (vulnerability) je slabina systému využitelná ke způsobení škod nebo ztrát útokem. Vyskytuje se:
  - ve fyzickém uspořádání,
  - v organizačních schématech,
  - v administrativních opatřeních,
  - v logických a technických opatřeních,
  - v personální politice, správě nebo managementu organizace,
  - lidský faktor,
  - Např. server neautentizuje své uživatele, Konkrétní systém může být například zranitelný vůči neoprávněné manipulaci s daty, protože systém před povolením přístupu k datům neověřuje identitu uživatele.
- Příčiny
  - chyby v analýze, návrhu, implementaci,
  - složitost software,
  - existence skrytých (postranních) kanálů http://cs.wikipedia.org/wiki/%C3%9Atok_postrann%C3%ADm_kan%C3%A1lem ,
  - …

Hrozba

- **Hrozba** (threat) – potenciální možnost (soubor okolností) využití zranitelného místa k útoku (ke způsobení škody, ke zničení aktiv, …)
  - Charakteristiky hrozeb – zdroj (vnější, vnitřní), motivace (finanční zisk, průmyslová špionáž, …), frekvence
  - Hlídáme (kontrolujeme) slabá místa, jako prevenci útoku a zablokování (eliminaci) hrozeb.



http://ptgmedia.pearsoncmg.com/images/9780132789462/samplepages/0132789469.pdf

Riziko

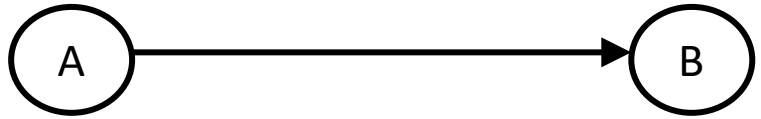
- **Riziko** (risk) – existence hrozby představuje riziko - pravděpodobnost využití zranitelného místa
  - Riziko – je funkcí pravděpodobnosti výskytu incidentu a způsobené škody
- Posouzení rizik zahrnuje následující kroky:
  1. charakterizace systému
  2. identifikace hrozeb
  3. identifikace zranitelností
  4. analýza kontrol (kontrolních mechanismů)
  5. určení pravděpodobnosti (využití zranitelnosti)
  6. analýza dopadu
  7. stanovení rizika
  8. kontrolní doporučení
  9. dokumentace výsledků

Bezpečnostní politika

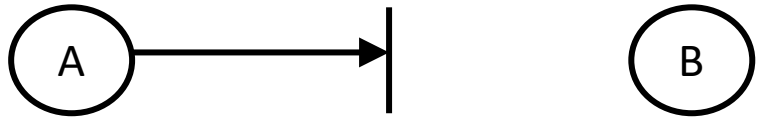
- Všeobecná bezpečnostní politika organizace - souhrn zásad a předpisů definujících způsob zabezpečení organizace od fyzické ostrahy, přes ochranu profesních zájmů až po ochranu soukromí a lidských práv.
- **Bezpečnostní politika ICT** organizace se zabývá výběrem bezpečnostních zásad a předpisů, které obecně definují bezpečné používání informačních zdrojů v rámci organizace **nezávisle** na konkrétně použitých informačních technologiích. Je to prohlášení o tom, co je, a není dovoleno.
- **Systémová bezpečnostní politika ICT**
  - určuje detaily konkrétních norem a předpisů, které definují způsob správy, ochrany a distribuce informací v rámci organizace.
  - Specifikuje bezpečnostní opatření a způsob jejich implementace.
  - Určuje způsob použití těchto opatření, přičemž jsou respektovány použité ICT.
- https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/bis_1ed.pdf kapitola 2.2

Útoky (1)

- Bezpečnostní incident – úmyslná nebo neúmyslná akce s vedoucí ke škodě na aktivech.
- Normální tok informace*:*

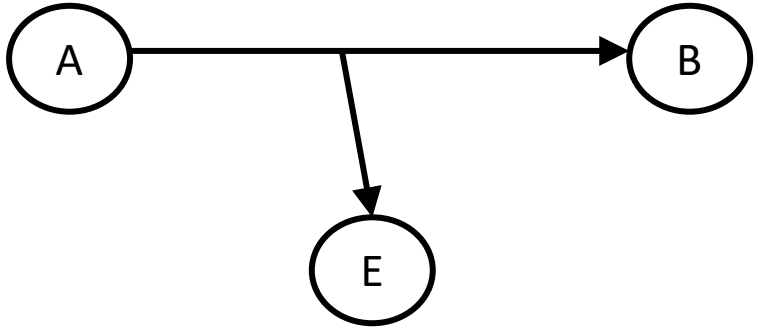


- **Útok přerušením** (interruption): jedná se o útok na dostupnost (zničení hardware, přerušení komunikační linky, znepřístupnění souborů, porucha hardware, …)

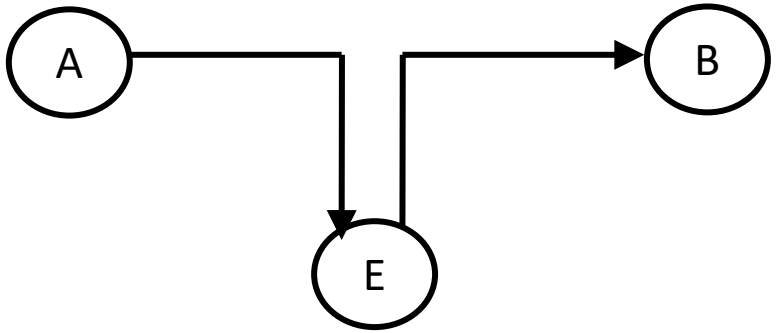


Útoky (2)

- **Zachycení zprávy, odposlech** (interception): útok na utajení; neautorizovaný subjekt E (útočníkem může být program, počítač, člověk) odposlouchává, nedovoleně kopíruje data,…

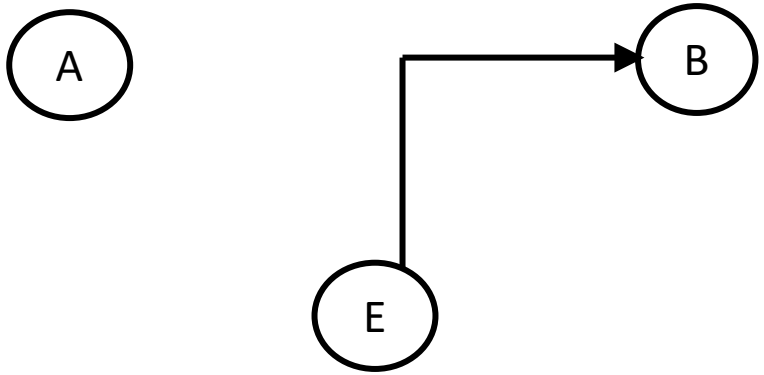


- **Modifikace** (modification) je útok na integritu dat; neautorizovaný subjekt *E* změní hodnoty dat, funkčnost programu, obsah zprávy posílané po síti, …



Útoky (3)

- **Přidání hodnoty**, „padělání“ (fabrication) je útok na autenticitu, integritu; neautorizovaný subjekt E vloží nějaký „padělek“ do systému (vložení podvržené zprávy, přidání záznamů k souboru, …).



Útoky (4)

- **Pasivní útoky** (odposlechem, monitorováním):
  - zveřejnění obsahu zprávy (chceme tedy zabránit útočníkovi aby se dověděl o obsahu přenosu),
  - sledování provozu (traffic analysis) – útočník může sledovat polohu a identitu komunikujících subjektů, frekvenci a délku vyměňovaných zpráv, což umožní odhadnout povahu komunikace.
  - Ochrana: prevence (detekce odposlechu je obtížná).
- **Aktivní útoky** (přerušením, změnou a přidáním hodnoty):
  - maškaráda (masquerade) (entita se vydává za jinou),
  - zachycení (replay),
  - modifikace zprávy,
  - odepření služby (denial of service).

Bezpečnostní mechanismy (1)

- **Bezpečnostní mechanismy** – implementují (zajišťují) bezpeč. funkce. Jsou to mechanismy navržené tak, aby detekovaly útoky, zabraňovaly jim, ev. pomohly zotavení se z útoků:
  - je jich mnoho, mohou mít charakter fyzického opatření (UPS, …), administrativní akce (školení, …), může jimi být technické zařízení nebo logický nástroj (algoritmus),
  - Obecně
    - kryptografie,
    - softwarová kontrola,
    - kontrola hardware,
    - fyzická kontrola,
    - politiky a procesy (metodika)

Bezpečnostní mechanismy (2)

- Pro mnoho bezpečnostních mechanizmů jsou základem **kryptografické techniky** (návrh, používání a jejich management)
  - Ochrana dat tím, že budou pro útočníka nečitelná
  - Ověřování uživatelů pomocí digitálních podpisů
  - Ověřování transakce pomocí kryptografických protokolů
  - Zajištění integrity uložených dat
  - …

Bezpečnostní mechanismy (3)

- Softwarová kontrola
  - Hesla a jiné formy řízení přístupu
  - OS - oddělování akcí uživatelů od ostatních akcí
  - Antiviry pro odhalení některých druhů malwaru
  - Osobní firewally
- Kontrola hardwarová (myšleno ne ochrana samotného hardwaru, ale použití samostatného hardwaru pro ochranu systému jako celku)
  - Čtečky otisků prstů
  - Chytré tokeny
  - Firewally
  - IDS, systémy detekce průniku
- Fyzická kontrola (ochrana hardwaru samotného, stejně jako fyzická ochrana přístupu k aktivům)
  - Zámky
  - Strážní služba
  - IPS, ...
- Politiky a procesy (netechnické prostředky ochrany)
  - Politika o nakládání s hesly
  - Výcvik v osvědčených postupech, bezpečnostní vzdělávání

Metody obrany

- Jak se můžeme bránit?
  - **Prevence útoku**
  - **Odradit útočníka**: učinit útok těžší nebo dražší
  - **Odvést pozornost**: učinit věci pro útočníka méně atraktivními
  - **Detekovat útok**: Detekce nadcházejícího nebo již uskutečněného útoku
  - **Zotavení se z útoku**
- Absolutní prevence útoků zajistitelná není
- Typická ochrana (hlavně před aktivními formami útoků) je založena na **detekci útoků a na následné obnově činnosti**

Pár úvah na konec úvodu (1)

- Perfektní bezpečnost je sice teoreticky možná, není však prakticky využitelná. Na každý nejlepší bezpečnostní mechanismus lze útočit hrubou silou.
- Každý použitý bezpečnostní mechanismus musí být akceptovatelný uživatelskou komunitou.
- Bezpečnost není stav, ale PROCES.
- Bezpečnost netkví v nakoupené technice, ale v jejím správném používání.
- Princip nejjednoduššího útoku
  - „Systém je tak bezpečný, jak je bezpečný jeho nejslabší článek. A lidé jsou nejslabší článek.“ Bruce Schneier, Secrets and Lies, 2000
  - Abychom byli schopni vybudovat bezpečný systém, musíme myslet jako útočník
- Princip adekvátní ochrany
  - Nemá smysl utratit $100,000 na ochranu systému, jehož hodnota je jen $1,000.

Pár úvah na konec úvodu (2)

- „Only amateurs attack machines; professionals target people. And any solutions will have to target the people problem…“ Bruce Schneier, Crypto-gram, 15 Oct 2000
- „Many systems fail because their designers protect the wrong things or protect the right things in the wrong way.“ Ross Anderson, Security Engineering, 2008
- „Without usable systems, the security and privacy simply disappears as people defeat the processes in order to get their work done … The more secure you make something, the less secure it becomes.“
  - Why? Because when security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security. Hence the prevalence of doors propped open by bricks and wastebaskets, of passwords pasted on the fronts of monitors or hidden under the keyboard or in the drawer, of home keys hidden under the mat or above the doorframe or under fake rocks that can be purchased for this purpose ... The strongest locks in the world do not deter the clever social engineer. Don Norman, When Security Gets in the Way, 2010

Úvod (2)

- Neexistují techniky návrhu a implementace zabezpečení, které by systematicky vylučovaly všechny bezpečnostní chyby a zabraňovaly všem neoprávněným činnostem. Proto existuje soubor široce dohodnutých zásad, kterými se řídíme při vývoji bezpečnostních mechanismů.
  - **Economy of mechanism** - bezpečnostních opatření obsažená v hardwaru i softwaru by měla být co nejjednodušší a nejmenší.
  - **Fail-safe defaults** - výchozí situací je omezený přístup a schéma ochrany určuje podmínky, za kterých je přístup povolen.
  - **Complete mediation** - každý přístup musí být v rámci mechanismu kontroly přístupu zkontrolován. Systémy by se neměly spoléhat na rozhodnutí o přístupu získaná z mezipaměti.
  - **Open design** znamená, že návrh bezpečnostního mechanismu by měl být otevřený. Např. dílčí algoritmy pak mohou být přezkoumány mnoha odborníky, a uživatelé jim proto mohou velmi důvěřovat.
  - **Separation of privilege**- obecně se jedná o oddělení uživatelů a procesů na základě různých úrovní důvěryhodnosti, potřeb a požadavků na oprávnění.
  - **Least privilege** - každý proces a každý uživatel systému by měl pracovat s nejmenší sadou oprávnění nezbytných k provedení úkolu. Dobrým příkladem použití tohoto principu je řízení přístupu na základě rolí. Jakýkoli systém řízení přístupu by měl každému subjektu umožňovat pouze oprávnění, pro která je autorizován.

Úvod (3)

- **Least common mechanism** - design by měl minimalizovat funkce sdílené různými uživateli a poskytovat vzájemné zabezpečení.
- **Psychological acceptability** - bezpečnostní mechanismy by neměly nepřiměřeně zasahovat do práce uživatelů, být rušivé nebo zatěžující.
- **Isolation** - veřejně přístupné systémy by měly být izolovány od kritických zdrojů (data, procesy atd.). Dále by měly být procesy a soubory jednotlivých uživatelů navzájem izolovány, kromě případů, kdy je to výslovně požadováno. A konečně, bezpečnostní mechanismy by měly být izolované ve smyslu zabránění přístupu k těmto mechanismům.
- **Encapsulation** - zapouzdření je specifickou formu izolace v OOP, kdy jsou data zvenčí přístupná jen prostřednictvím metod. Dále se se zapouzdřením potkáváme u počítačových sítí.
- **Modularity** - v kontextu zabezpečení odkazuje jak na vývoj bezpečnostních funkcí jako samostatných chráněných modulů, tak na použití modulární architektury pro návrh a implementaci mechanismu.
- **Layering** - vrstvením se rozumí použití více překrývajících se ochranných přístupů zaměřených na lidi, technologie a provozní aspekty informačních systémů.
- **Least astonishment** - programové nebo uživatelské rozhraní by mělo vždy reagovat způsobem, který uživatele nejméně pravděpodobně překvapí.

Protokoly (1)

- Bezpečnostní protokol je v podstatě komunikační protokol (dohodnutá posloupnost akcí prováděných dvěma nebo více komunikujícími entitami za účelem dosažení nějakého vzájemně žádoucího cíle), který využívá (kryptografické) techniky umožňující komunikujícím entitám dosáhnout bezpečnostního cíle.
- Kryptografické protokoly obvykle využívají jeden nebo více kryptografických primitiv a / nebo schémat.
  - Příkladem může být přenos čísla kreditní karty od Boba na webovou stránku Alicina e-shopu.
  - Takový protokol může zahrnovat schéma digitálního podpisu (pak Bob ví, že komunikuje s Alicí) a formu šifrování (aby se zajistilo, že při přenosu nebudou zachyceny údaje o Bobově kreditní kartě).
- Šifrovací algoritmy, podepisovací algoritmy a hashovací funkce jsou základem bezpečnostních protokolů.

Protokoly (2)

- Obecné protokoly
  - Key agreement - Protokol dohody na klíči umožňuje dvěma stranám dohodnout se na sdíleném tajném klíči. Autentizace je založená na dvojici veřejný a soukromý klíč. Důležitý rozdíl je mezi přenosem klíčů, kde jedna strana generuje klíč a odešle jej druhé, a dohodou o klíčích, kde žádná ze stran nemá úplnou kontrolu nad procesem generování klíčů.
  - Identification and Authentication Protocols - protokoly pro identifikaci (1:N) a autentizaci (1:1) uživatelů
  - …
- Specifické protokoly
  - TLS byl navržen tak, aby zabezpečoval komunikaci mezi prohlížečem a webovou stránkou
  - SSH 10 - používá se např. k zajištění zabezpečeného kanálu mezi dvěma počítači v síti pro aplikace, jako je přenos souborů
  - IPSec - (Internet Protocol SECurity) je komplexní soubor protokolů na síťové vrstvě, který nabízí tunelování, šifrování a autentizaci
  - Kerberos – protokol, umožňuje klientovi autentizaci vůči více službám. Kerberos poskytuje centralizovaný ověřovací server, jehož funkcí je ověřovat uživatele vůči serverům a servery vůči uživatelům
  - …
- Aplikačně specifické protokoly
  - WEP/WPA - Protokoly WEP / WPA se používají k ochraně komunikace v bezdrátových sítích
  - UMTS/LTE - Protokoly GSM, UMTS a LTE jsou určeny k zabezpečení komunikace mezi mobilním telefonem a základnovou stanicí operátora
  - Bluetooth - Bluetooth je technologie pro bezpečnou výměnu dat na krátké vzdálenosti
  - ZigBee je standard rádiové komunikace provozovaný hlavně při nižším výkonu a dosahu než Bluetooth
  - …

Kryptografie a počítačová bezpečnost

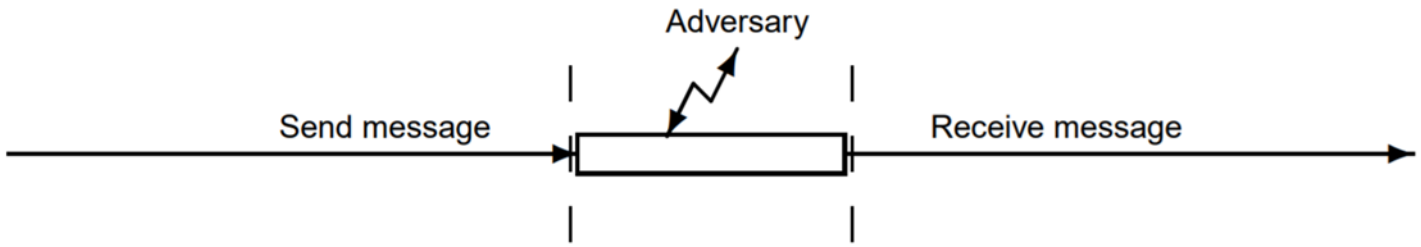
Úvod do kryptografie

Literatura

- Chapter 1, Stallings, W.: Cryptography and Network Security

Proč kryptografie?

- Kryptografie se zabývá vývojem algoritmů, které mohou být použity k:
  - utajení zpráv (jejich obsahu, ne existence),
  - autentizaci - zjistitelnost původu zprávy, bezpečná identifikace subjektu, který
    - informaci vytvořil,
    - přijímá ji,
    - který s ní operuje,
  - kontrole integrity - informaci může modifikovat / generovat jen autorizovaný subjekt,
  - k zajištění nepopiratelnosti
    - příjmu,
    - doručení,
    - původu citlivé informace.



Kryptologie

- **Kryptologie** je věda o utajování informace, stojící na pomezí matematiky a informatiky, s větším přesahem do matematiky, zejména v oblasti teorie čísel a algebry. Součástí kryptologie je:
  - **Kryptografie** je „umění“ a věda o převedení informace do podoby, ve které je obsah informace skrytý, utajený (a to i tehdy, pokud je tato nečitelná informace prozrazena třetí straně). Je to tedy věda o šifrování dat za pomoci matematických metod (ale nejen o tomto).
  - **Kryptoanalýza** je umění a věda o prolomení skryté informace (šifry nebo klíče), zabývá se odolností kryptografického systému.
- Proč? Kryptografie je základem mnoha technologických řešení problémů počítačové bezpečnosti, tedy kryptografických bezpečnostních mechanismů.

Kryptografický systém (1)

- **Kryptografický systém** je pětice {M, C, K, E, D}, kde:
  - symbolem M označujeme tzv. prostor otevřených textů, což je konečná množina prvků, kterým se říká **otevřený** (srozumitelný) **text** (zpráva) (angl. plaintext),
  - symbolem C označujeme tzv. prostor šifrových textů. C je konečná množina prvků nazývaných **šifrový text** (ciphertext),
  - K je konečná množina možných klíčů, tzv. prostor klíčů, jejímž prvkem je **klíč** (key),

Kryptografický systém (2)

- E je množina šifrovacích funkcí (algoritmů, pravidel). **Šifrováním** (encryption, enciphering) nazýváme proces, kterým z otevřeného textu získáme jeho šifrový text,
- D je množina dešifrovacích funkcí (algoritmů, pravidel). **Dešifrováním** (decryption, deciphering) nazýváme proces, kterým z šifrového textu získáme otevřený text.

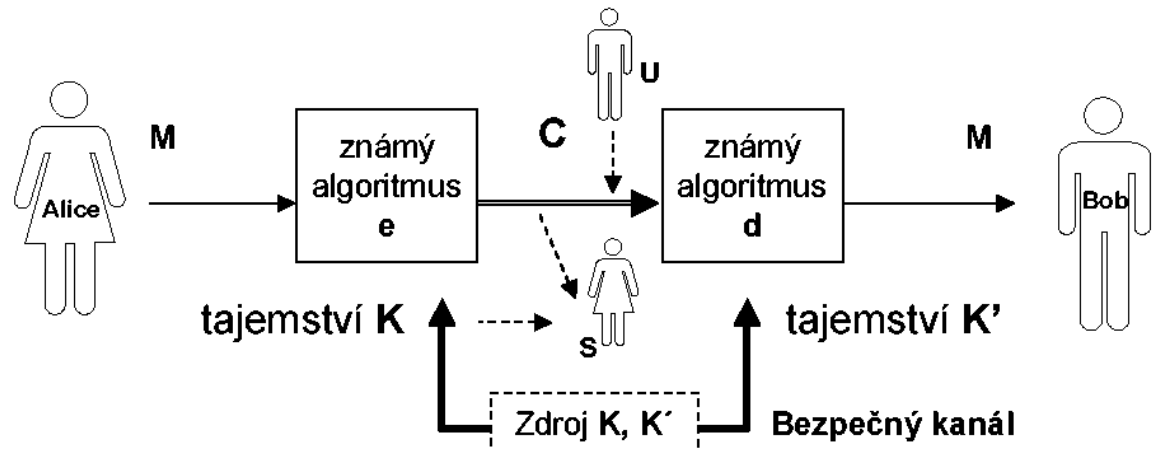
Abeceda

- **Přípustná abeceda** je konečná množina prvků, ze kterých se skládá otevřený i šifrový text. Přípustná abeceda se může pro otevřený text a šifrový text lišit:
  - otevřená abeceda (OA), šifrová abeceda (ŠA),
    - např. anglická abeceda bez mezery (AAbM),
    - anglická abeceda s mezerou,
    - {0,1},
    - ...

Kryptografický systém

- Platí:
  - Pro $\forall k \in K$ existuje šifrovací algoritmus (funkce) $e_k \in E$ a jemu odpovídající dešifrovací alg. $d_k \in D$.
  - Každá $e_k : m \rightarrow c$ a $d_k : c \rightarrow m$, $k \in K$ jsou funkce, pro které platí tzv. **correctness condition**
    - $d_k(e_k(m)) = m$, pro $\forall m \in M, \forall k \in K$.
  - Klíč pro šifrování *k* nemusí být totožný s klíčem pro dešifrování *k'*, pak hovoříme o dvojici klíčů ($k \neq k'$).

Kryptografický systém



- K = K' ~ symetrická kryptografie, SK
  - tajný klíč K
- K ≠ K' ~ asymetrická kryptografie, ASK
  - veřejný klíč, K = K_V, soukromý klíč, K'= K_S

Proprietární algoritmy

- V minulosti se používaly tzv. **proprietární algoritmy**, kdy se utajoval princip algoritmu. Nevýhody:
  - každá skupina, která si chce předávat informace, musí mít svůj vlastní algoritmus,
  - prozrazení algoritmu může zkompromitovat všechny zprávy jím zašifrované,
  - jelikož algoritmy musejí zůstat tajné, není možné, aby mezinárodní kryptologická komunita ověřila jejich odolnost proti kryptoanalýze a utajení rovněž neumožní proces standardizace takovýchto algoritmů.
- Nyní používané algoritmy jsou veřejně známé!

Kerckhoffsův princip

- R. 1883 formuloval Auguste Kerckhoffs první principy kryptografického inženýrství: **„Bezpečnost šifrovacího systému nesmí záviset na utajení algoritmu, ale na utajení klíče“**
- Moderní kryptografie zpravidla používá algoritmy závislé na klíči (tzv. ***Kerckhoffsův princip***). Tj. kryptografické algoritmy **jsou veřejně publikovány** a jejich znalost nesmí kryptoanalytikovi pomoci ve snaze překonat utajení - to musí být plně závislé na klíči (který kryptoanalytik nezná).
- Bezpečnost jakéhokoliv šifrovacího algoritmu (používajícího klíč) spočívá v počtu možných klíčů (u hašovacích funkcí nikoliv, jiný princip).

Útok hrubou silou

	Velikost abecedy	Délka klíče	Velikost stavového prostoru	Doba útoku hrubou silou při 1 µs/1 test
PIN	10	4	10^4	0,01 s
6 písmen (VELKÁ)	26	6	$3{,}01 \times 10^8$	301 s
6 písmen / cifer	62	6	$5{,}7 \times 10^{11}$	15 hod.
heslo (Unix)	96	8	$7{,}21 \times 10^{15}$	229 roků
klíč DES	2	56	$7{,}21 \times 10^{16}$	2285 roků
klíč 128 bitů	2	128	$3{,}4 \times 10^{38}$	10^{16} ess
klíč 512 bitů	2	512	$1{,}34 \times 10^{154}$	4×10^{129} ess

ess – doba existence sluneční soustavy, cca 10^9 let, 10^{16} ess = 10^{25} let

Key size (bits)	**Number of alternative keys**	**Time required at 1 decryption/µs**	**Time required at 10^6 decryption/µs**
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^6 years