Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia

M. Stanek / M. Rjaško

2013

KPMG
cutting through complexity™

KRYPTOLÓGIA

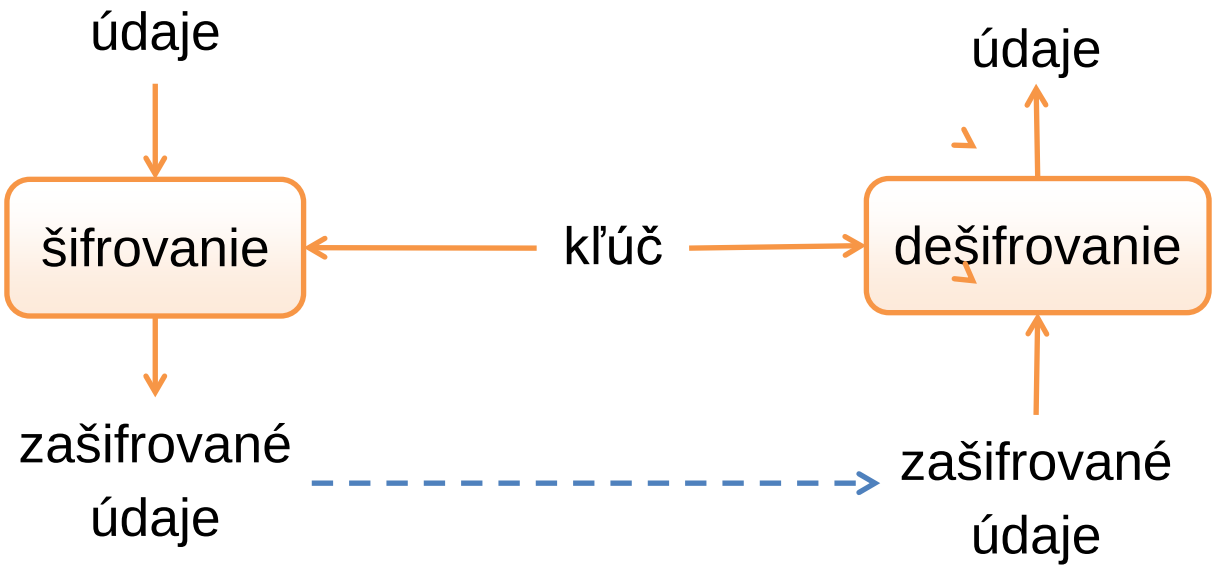
Martin Stanek

Úvod

- Kryptografické konštrukcie, kryptoanalýza
- Symetrické a asymetrické šifrovanie
- Hašovacie funkcie a autentizačné kódy správ
- Digitálne podpisy
- Protokoly
- Heslá a kryptografické kľúče
- Infraštruktúra verejných kľúčov
- Zraniteľnosti a kryptografia
- Štandardy a legislatíva

Symetrické šifrovanie

- Dôvernosť údajov
- Šifrovanie aj dešifrovanie využíva rovnaký kľúč



Symetrické šifrovanie 2

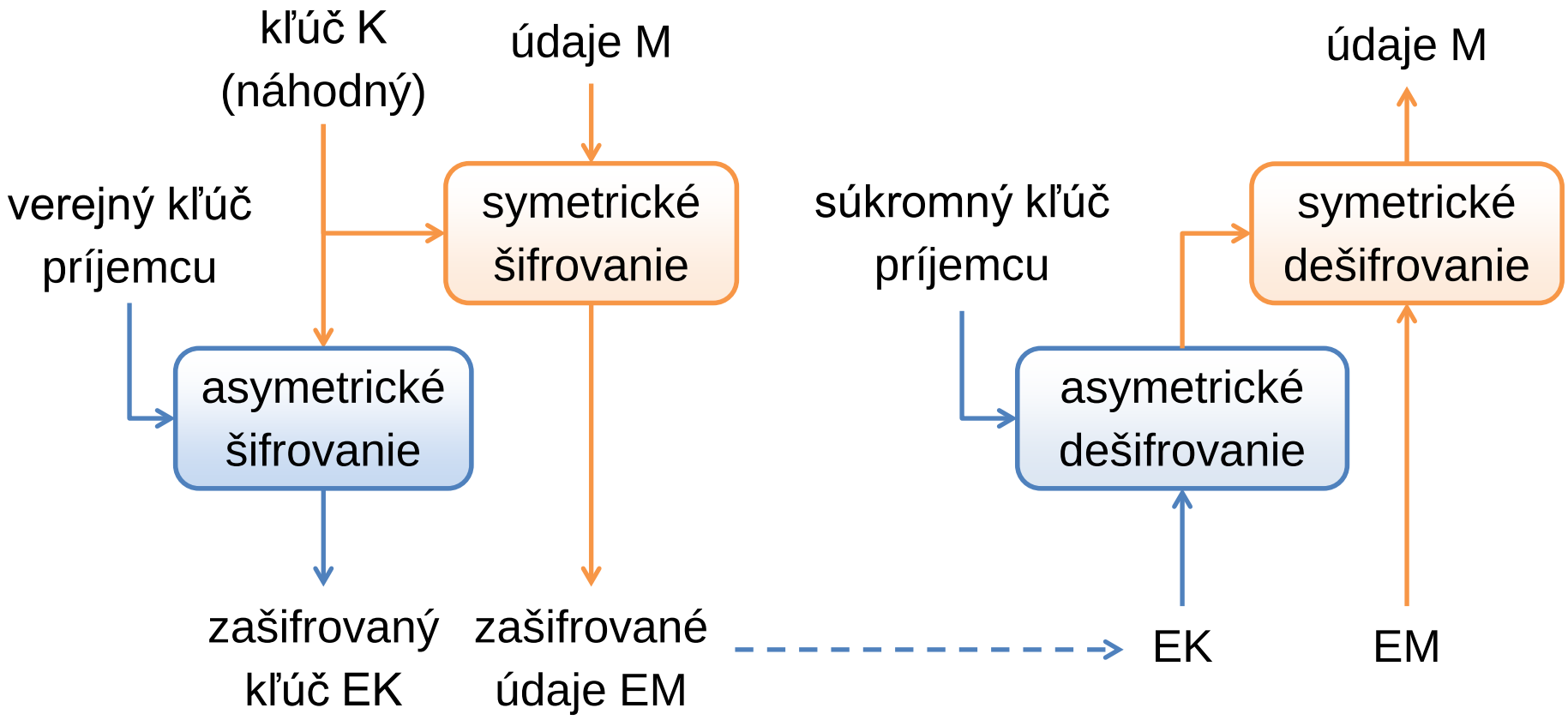
- Kľúč: obvykle náhodne volený reťazec bitov
- Dĺžka kľúča a útok úplným preberaním
- Najpoužívanejšie algoritmy (blokové šifry): AES, 3DES
- Varianty AES: AES-128, AES-192, AES-256
- Vysoká priepustnosť
- Hardvérová podpora v novších CPU

Asymetrické šifrovanie

- Dvojica kľúčov: verejný a súkromný
- Šifrovanie s verejným kľúčom (ktokoľvek vie šifrovať)
- Dešifrovanie so súkromným kľúčom
- Bezpečnosť sa opiera o zložitosť matematických problémov
- Najpoužívanejší systém: RSA (problém faktorizácie)
- Ekvivalentná dĺžka kľúča:
  - NIST SP 800-57: 3072 bitov RSA ~ 128 bitov symetrického kľúča

Hybridné šifrovanie

- Kombinácia asymetrického a symetrického šifrovania



Symetrické vs. asymetrické šifrovanie

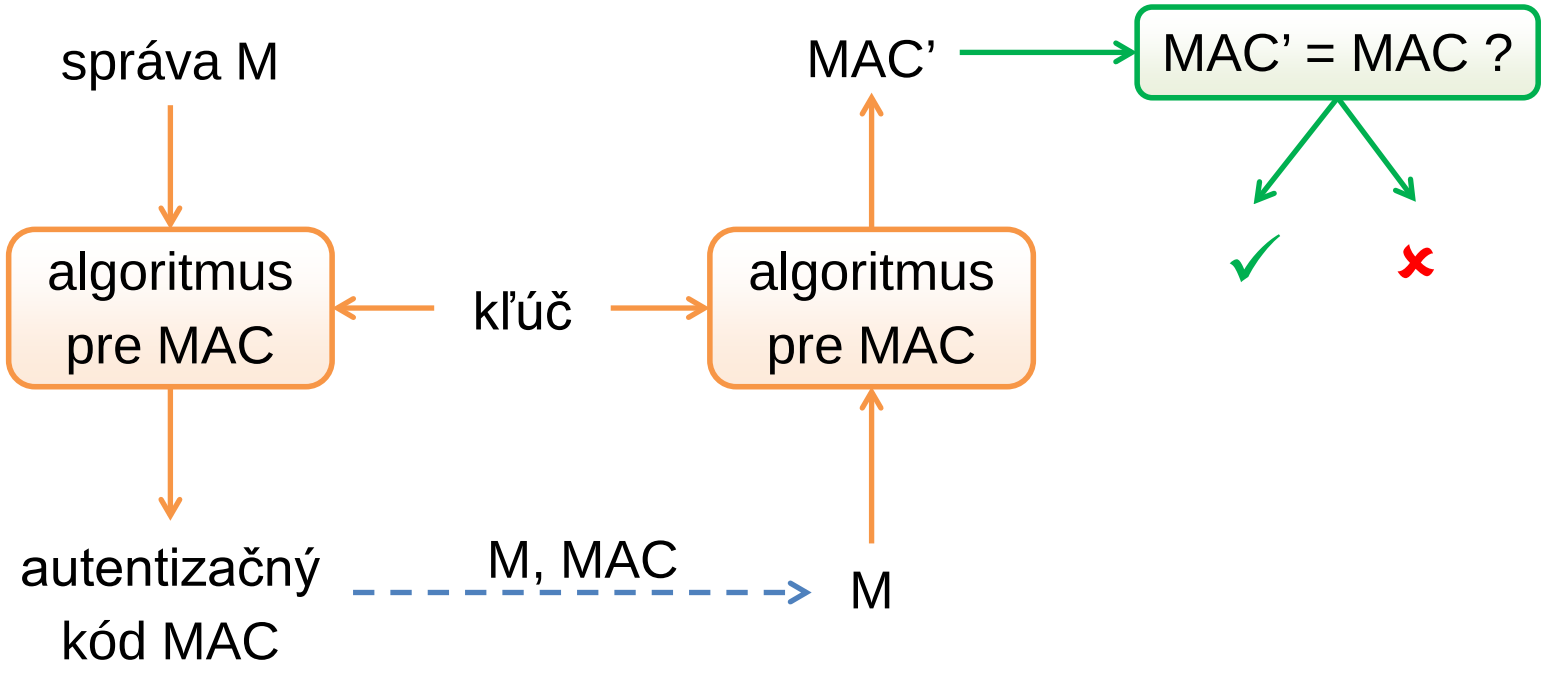
	Symetrické šifrovanie	Asymetrické šifrovanie
Primárne použitie	dôvernosť údajov ľubovoľného rozsahu	dôvernosť krátkych dát (typicky napr. kľúče pre symetrické šifrovanie)
Komunikácia	1:1 – obvykle dvaja účastníci	N:1 – ľubovoľný počet odosielateľov (šifrovací kľúč je verejný), jeden príjemca (súkromný dešifrovací kľúč)
Efektívnosť	rýchle šifrovanie aj dešifrovanie	pomalé šifrovanie aj dešifrovanie
Dĺžka kľúčov	obvykle 112 až 256 bitov (náhodný reťazec bitov)	v závislosti na konkrétnom algoritme, niekoľko sto až niekoľko tisíc bitov

Hašovacie funkcie

- Transformácia vstupu na odtlačok fixnej dĺžky
- Najpoužívanejšie: SHA-1 (160 bitov), SHA-256
- Žiadny kľúč
- Zabezpečenie integrity dát
- Detekcia *náhodnej/neúmyselnej* zmeny dát
- Očakávané vlastnosti:
  - Odolnosť vzoru (jednosmernosť)
  - Odolnosť voči kolíziám

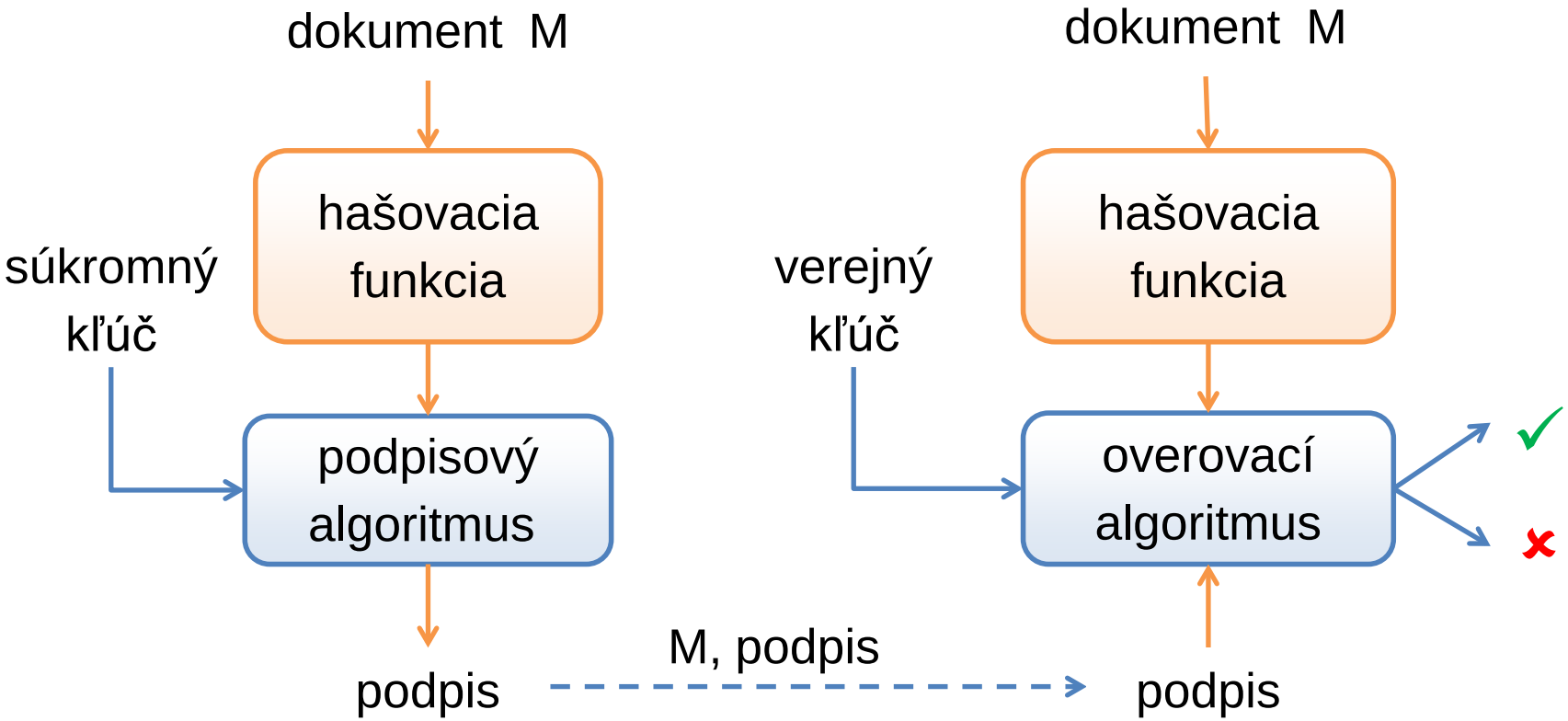
Autentizačné kódy správ

- Symetrický kľúč (odosielateľ a príjemca)
- Integrita a autentickosť dát
- Najznámejšia konštrukcia: HMAC (z hašovacích funkcií)



Schémy digitálnych podpisov

- Asymetrická konštrukcia (verejný a súkromný kľúč)
- Integrita a autentickosť dát
- Najznámejšie konštrukcie: RSA, DSA, ECDSA



Porovnanie

	Hašovacie funkcie	Autentizačné kódy	Digitálne podpisy
Integrita	áno	áno	áno
Autentickosť	nie	áno	áno
Nepopierateľnosť autorstva	nie	nie	áno
Kľúče	žiadne	symetrické	asymetrický pár kľúčov
Efektívnosť	rýchle	rýchle	pomalé
Typická aplikácia	kontrola integrity statických dát	autentickosť jednotlivých paketov v sieti	autentickosť dokumentov

Protokoly

- Protokoly pre autentizáciu a dohodnutie kľúčov
- Najznámejšie: SSL/TLS, IPSec, SSH a pod.
- Viaceré varianty – algoritmy, spôsoby autentizácie
- Prostriedky autentizácie účastníka protokolu:
  - Zdieľaná tajná informácia (heslo/kľúč)
  - Znalosť súkromného kľúča k verejnému kľúču uvedenom v certifikáte

Základné charakteristiky TLS (SSL)

Autentizácia servera	povinná (znalosť súkromného kľúča k verejnému kľúču z certifikátu)
Autentizácia klienta	voliteľná (málokedy používané, obvykle riešené po vytvorení TLS spojenia)
Distribúcia kľúčov	viaceré protokoly (odvodenie kľúčov pre šifrovanie a autentizačné kódy)
Dôvernosť	symetrické šifrovanie (podpora rôznych algoritmov a módov)
Autentickosť	autentizačné kódy (podpora rôznych algoritmov)
Úprava aplikácie	zvyčajne potrebné v aplikácii špecificky inicializovať komunikačný kanál

Kryptografické kľúče

- Správa kľúčov (ako – algoritmy a postupy)
  - Generovanie
  - Distribúcia
  - Ukladanie a prístup
  - Ničenie kľúčov
  - Postupy pri kompromitácii kľúčov
- Dĺžka kľúčov – nutná ale nepostačujúca podmienka bezpečnosti

Útok prehľadávaním priestoru kľúčov

Čas útoku	Individuálny útočník 1 procesor	Stredne veľká firma 500 procesorov	Príjmy SR za 1 rok (53,8 mil. procesorov)
1 minúta	33,7	42,6	59,3
1 hodina	39,6	48,5	65,2
1 deň	44,1	53,1	69,8
30 dní	49,1	58,0	74,7
1 rok	52,7	61,6	78,3
100 rokov	59,3	68,3	85,0

- Ilustračný príklad pre konkrétny procesor (i7-2600)

Infraštruktúra verejných kľúčov

- Certifikačná autorita
- Certifikát verejného kľúča:
  - Sériové číslo
  - Identifikácia subjektu
  - Verejný kľúč (vrátane identifikácie algoritmu)
  - Účel použitia (podpisová schéma, šifrovanie a pod.)
  - Interval platnosti
  - ... <ďalšie údaje: SAN, URL pre CRL/OCSP atď.>
  - Podpis CA
- Overenie certifikátu
- Zneplatňovanie certifikátov
- Dôvera v CA

Heslá

- Bezpečnosť
  - Dĺžka a „náhodnosť“ hesla
  - Spôsob prenosu hesla a jeho overenia
  - Spôsob uloženia hesla používateľom
  - Spôsob uloženia hesla serverom
  - Iné parametre:
    - Doba platnosti hesla
    - Počet
- Odvádzanie symetrických kľúčov z hesiel

Náhodnosť používateľských hesiel

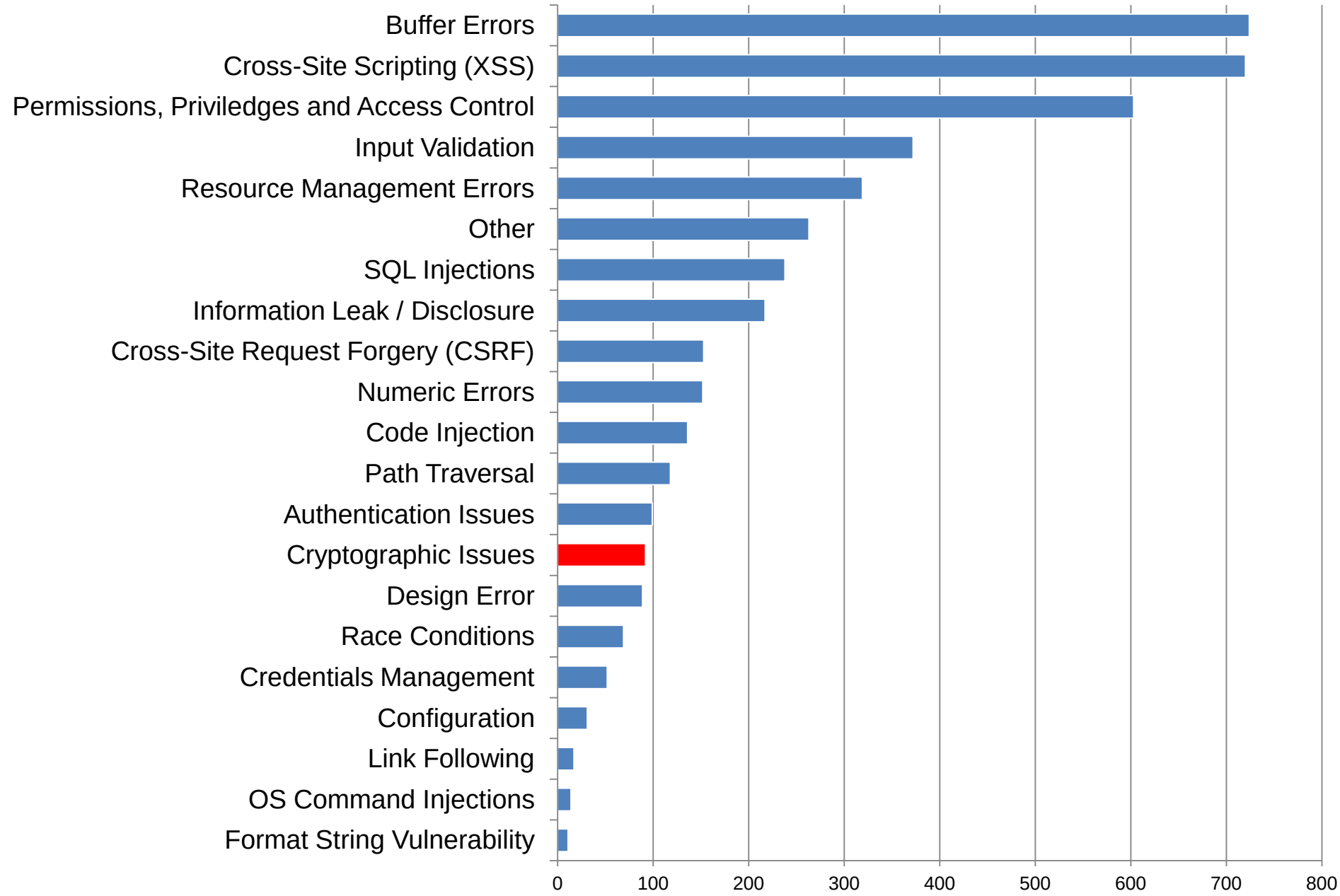
Dĺžka hesla	PIN (10 znaková abeceda)	Všeobecné heslá (94 znaková abeceda)
4	9	10
8	13	18
10	15	21
16	21	30
22	27	38

- Príklad: 2012, LinkedIn, 6,5 mil. používateľských účtov
- 4 hodiny + slovníkový útok → cca. 900 tisíc hesiel
- Pokračovanie slovníkového útoku → cca. 2 mil. hesiel

Kryptografia a zraniteľnosti

- NIST: NVD (National Vulnerability Database)
  - SW zraniteľnosti a ich klasifikácia (typ, závažnosť a pod.)
- Najčastejšie zraniteľnosti v „Cryptographic Issues“:
  - použitie nekvalitného zdroja náhodnosti pri generovaní kľúčov,
  - nedostatočná (neúplná) kontrola certifikátov,
  - nekorektná implementácia kryptografických algoritmov alebo protokolov,
  - fixné heslá servisných účtov alebo heslá odvodené z verejne známych údajov

Počty zraniteľností publikovaných v roku 2012 podľa NVD



Štandardy

- Kryptografické algoritmy (šifry, podpisové schémy, hašovacie funkcie)
  - Primárne NIST, široká akceptácia
- Protokoly
  - Zvyčajne RFC
- Štandardy v IB riešia kryptografiu len okrajovo
- ISO/IEC 27000:
  - Politika používania kryptografických opatrení
  - Riadenie kľúčov
- ISO/IEC 15408 (Common Criteria):
  - Správa kryptografických kľúčov
  - Prevádzka kryptografie

FIPS PUB 140-2

- Security Requirements for Cryptographic Modules
- 4 bezpečnostné úrovne
- Oblasti: špecifikácia modulu, role, služby, autentizácia, fyzická bezpečnosť modulu, samotestovanie, správa kľúčov, elektromagnetické vyžarovanie a ďalšie
- Certifikované moduly v roku 2012
  - 68 osvedčení na úrovni 1, 95 na úrovni 2, 37 na úrovni 3 a žiadne na úrovni 4
- Certifikácia nie je zárukou bezpečnosti
  - Príklad: certifikované USB kľúče

Legislatíva SR

- Výnos Ministerstva financií SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (časť Technické štandardy):
  - IPSec, SSL alebo TLS, S/MIME
  - Zmienky o ďalších konštrukciách ... bez konkrétnych detailov
- Zákon č. 215/2002 o elektronickom podpise
  - Bez technických podrobností
  - Vyhlášky NBÚ SR, najmä č. 135/2009 (formáty, algoritmy a pod.)
- Zákon č. 215/2004 o ochrane utajovaných skutočností
  - Šifrová ochrana informácií
  - Podrobnosti sú utajovanou skutočnosťou

Odporúčania

- ✓ Používajte štandardné kryptografické algoritmy, schémy a protokoly
- ✓ Používajte dostatočné dĺžky kľúčov
- ✓ Pravidelne meňte kľúče a heslá
- ✓ Dbajte na kvalitné generovanie kľúčov a voľbu hesiel
- ✓ Majte premyslené, čo robiť po kompromitácii kľúčov alebo hesiel
- ✓ Ak môžete, použite certifikované riešenia
- ✓ Poznajte konfiguračné možnosti kryptografických riešení a ich bezpečnostné dopady
- ✓ Dôsledne overujte certifikáty verejných kľúčov
- ✓ Koreňové certifikáty získajte dôveryhodným spôsobom

Varovania

- Kryptografia nie je miesto na kreativitu a ad-hoc riešenia
- Dlhodobo nezmenené kľúče považujte za prezradené
- Šifrovanie nezabezpečuje integritu ani autentickosť údajov
- Autentizačné kódy ani digitálne podpisy nezabezpečujú dôvernosť
- Obvykle je heslo najslabším „kľúčom“ v systéme
- Samopodpísaný certifikát nehovorí nič o autentickosti verejného kľúča
- Certifikácia nie je náhradou bezpečného používania
- Kryptografia nenahradí iné organizačné a technické bezpečnostné opatrenia

Ďakujem za pozornosť