# 1. Jak a proč posílat SPAM

## Definice

- SPAM je hromadná nevyžádaná pošta
- např. využití botnetů pro rozesílání spamu

## Důvody

- nekalé obchodní praktiky
- podvodné zvyšování provozu webu (uměle vygenerované odkazy na web)
- pro podvody
  - phishing
  - krádež identity
  - získávání hesel, autentizačních informací

## Wiki

http://cs.wikipedia.org/wiki/Spam

# 2. Jak a proč udělat phishing útok

## Definice

- PHISHING je nalákání na podvodný web za účelem získání osobních dat, technika sociálního inženýrství
- např. předstírání, že e-mail nebo zpráva pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů nebo IT administrátorů

## Důvody

- získání osobních dat
- krádež finančních prostředků z bankovních účtů

## Wiki

http://cs.wikipedia.org/wiki/Phishing

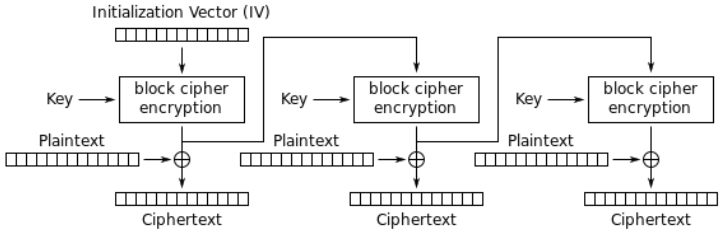
# 3. Který typ blokové šifry se dá použít jako PRNG

## OFB – Output Feedback

- synchronní proudová šifra

## Wiki

http://cs.wikipedia.org/wiki/Proudov%C3%A1_%C5%A1ifra#Synchronn.C3.AD_proudov.C3.A9_.C5.A1ifry




Output Feedback (OFB) mode encryption

## 4. Zabezpečení proti odcizení dat při ztrátě telefonu

- **screen lock** (passcode, PIN, gesto, rozpoznání obličeje, hlas, kombinace)
- **vzdálené smazání obsahu zařízení** (Remote Wipe)
- **lokální smazání obsahu zařízení** (Local Wipe)
- **lokalizace** (GPS, WiFi, BT)
- **šifrování zařízení**
- **neprovádět root/jailbreak**
- **Android – vypnutí ADB**
- **iOS – změna výchozích přihlašovacích údajů po jailbreaku**

## 5. Typy modifikace malware proti odhalení (např. šifrování)

### Obfuskace - vyhýbání se odhalení, skrývání

- **polymorfní** - mutace kódu, ale funkcionalita se nemění. Kód se při každém spuštění změní, funkcionalita zůstává stejná.
- **oligomorfní** - mutace kódu změnou několika částí na předdefinované alternativy. Pouze stovky různých kódů.
- **metamorfní** - vytváření naprosto odlišných logických ekvivalentů. Překlad do přechodné representace, úprava representace, opětovný překlad do binárního kódu.
- **šifrování** - tělo kódu je šifrováno, připojen dešifrovací mechanismus. Šifrování není morfismus!

### Techniky

- **dead-code insertion** (NOP)
- **transposice kódu**
- **výměna registrů** - náhodné přehození registrů v každém replikačním cyklu
- **subroutine reordering** - změna pořadí funkcí
- **substituce instrukcí** za ekvivalenty (MOV za PUSH/POP)
- **integrace do kódu** - kód je dekompilován, malware vložen dovnitř a celkový kód znovu zkompilován

## 6. Hrozby, aktiva, bezpečnostní funkce (státnicová otázka)

### Hrozby

Taková vlastnost prostředí, která může způsobit narušení bezpečnosti (bezpečnostní incident), pokud dostane příležitost.

- **neúmyslná (nealgoritmická, pravděpodobnostní)**
  - živelné události (požár, výpadek proudu, záplava)
  - poruchy zařízení
  - chyby v software
  - selhání osob (omyly)
- **úmyslná (algoritmická)**
  - cílem nejsou data
    - krádež HW a médií
    - úmyslné poškození, zničení zařízení
    - neoprávněné využívání HW
    - založený požár, bomba

    - cílem jsou data
        - krádež SW
        - krádež dat (prodej, zneužití dat, průmyslová špionáž)
        - neoprávněná manipulace s daty (modifikace, zničení)
    - škodlivé programy
        - viry, červi, logické bomby, trojské koně

### Aktiva

Složky informačního systému, které mají nějakou hodnotu.

- HW (servery, HDD, switche), SW (aplikace, OS, bezpečnostní komponenty), důvěrné informace (celkově data), ale i osoby (zaměstnanci)

### Bezpečnostní funkce

- **důvěrnost** – prevence proti neautorizovanému odhalení informace
- **integrita** – prevence proti neautorizované modifikaci informace
- **dostupnost** – prevence proti neautorizovanému odmítnutí informace nebo zdrojů
- **účtovatelnost** – identifikace a monitorování důležitých událostí, sledování činnosti
- **bezpečnost přenosu dat** – důvěrnost, integrita, nepopiratelnost
- **audit x nemožnost sledování**
- **autentizace x anonymita a pseudonymita**

### Bezpečnostní opatření

- redukují pravděpodobnost vzniku bezpečnostního incidentu (omezují zranitelná místa)
- bariéra mezi hrozbami a aktivy
- **omezující bezpečnostní opatření**
    - minimalizace ztrát vzniklých útokem (odhalení nebo odvrácení útoku)
    - maximalizace zotavení po útoku
- **preventivní bezpečnostní opatření**
    - snížení pravděpodobnosti útoku
    - zvýšení nákladů na útok pro útočníka (cena vyšší než zisk)
        - pravděpodobnost a dopad odhalení
        - náklady na útok
        - čas potřebný k útoku

### Zranitelná místa

Slabiny v informačním systému, které mohou být využity pro provedení útoku (bezpečnostního incidentu).

## 7. Popsat útok na PEAP

1. Rogue AP (hostapd)
2. Vlastní radius server (freeradius-wpe)
3. Deautentizace klienta (aireplay-ng)
4. Crack challenge (asleap)

## 8. Popsat útok na WPA/WPA2

### TKIP útok (WPA)

1. Využití slabiny algoritmu Michael – TKIP v případě detekce 2 rámců, které neprošly testem integrity, blokuje provoz po dobu 60s – proběhne restart sítě, generování nových klíčů a nová autentifikace
2. Selhání MIC (Message Integrity Check)
3. Útočník sleduje odpověď, čeká 60s, aby se vyhnul protiopatřením MIC
4. Pomocí mechanismu 1bit/minuta dekóduje paket (ARP za 15 minut)
5. Snaží se paket vložit klientovi

### Shrnutí útoku

- nedochází ke kompromitaci TKIP klíčů
- útok postihuje režim PSK i 802.1x
- dokáže odhalit 1bit/minutu
- je schopný dešifrovat pouze TKIP rámce od AP

### Obrana

- použít AES-CCMP (Counter Mode with CBC) – používá WPA2 – považován za bezpečný

## 9. Proč se SSID hiding a MAC filtering nepovažuje za zabezpečení

- Útočník může zachytit paket s MAC adresou a nastavit svou kartu na tuto adresu.
- V případě SSID hiding se síť neukazuje pouze v seznamu dostupných sítí, ale je možno SSID zjistit odchycením komunikace na síti.

## 10. Faktory autentizace (heslo, klíč, biometrika)

### Faktor znalosti

Autentizace na základě toho, **co uživatel zná** (heslo).

- **výhody**: nejsnazší, nejlevnější řešení, nevyžaduje zvláštní HW ani SW, universální
- **nevýhody:** nutnost zapamatovat si heslo, často používáno jedno heslo pro více účtů, obecně nižší bezpečnost, pokud není heslo silné

### Faktor vlastnictví

Autentizace na základě toho, **co uživatel má** (certifikát na USB tokenu, čipové kartě, klíč).

- **výhody**: složitější získání (pro útočníka), automaticky šifrovaný přenos
- **nevýhody:** obtížnější implementace, vyšší cena, nižší flexibilita

### Faktor neměnné charakteristiky

Autentizace na základě toho, **čím uživatel je** (biometrická charakteristika). Lze zavést i čtvrtý **Faktor dovednosti** (**co člověk umí** – podpis a jiné dynamické biometrické charakteristiky).

- **výhody**: teoreticky nejvyšší bezpečnost, složité získání
- **nevýhody:** vysoká cena některých systémů, složité specializované systémy

## 11. Cookies

### httpOnly

- použito pouze při zasílání http nebo https dotazů, čímž je zamezen přístup jiným API (např JavaScript)
- omezení snižuje hrozbu odcizení cookie pomocí XSS (ale neeliminuje zcela)
- pouze session-management cookies

### Secure

- povolený atribut secure a je použito pouze při https, což zajišťuje, že je cookie při přenosu od klienta na server vždy zašifrováno
- odolnější proti odposlechu

### Session

- vytvářené v dočasné paměti pro uživatelovu relaci na webu
- vytvářeno, pokud není zadán interval validity nebo datum vypršení cookie
- prohlížeče by při ukončení činnosti měli session cookies vymazat

### Persistent

- pevně nastavené datum vypršení cookie nebo interval validity
- persistentní cookie je zasíláno pokaždé, když se uživatel připojí na daný server (web)
- ukládá např. informace o tom, jak se uživatel na web dostal

## 12. Podmínky nerozluštitelnosti Vernamovy šifry

- klíč je alespoň tak dlouhý jako všechny šifrované zprávy
- klíč není nikdy použit znovu
- klíč je zvolen opravdu náhodně

## 13. Co je Tamper Evidence + příklad

- mechanismus, který při neoprávněném zacházení zanechává důkaz
- například: pečeť (vosková na dopise, na elektroměru), holografické nálepky, ale také elektronické podpisy apod.