Bezpečnost routeru

Pavel Bašta • pavel.basta@nic.cz • 15.04.2013

Osnova

- Různé vektory útoků
  - Vzdálená správa
  - Chyba ve výchozí konfiguraci
  - Chyba v kódu
  - Nejčastější útoky na lokální sítě (IPv4, IPv6)
  - Útoky na Wi-Fi

Kali Linux

- Dříve BackTrack
- Specializovaná linuxová live distribuce pro penetrační testování
- Velké množství nástrojů pro testování bezpečnosti
- www.kali.org

Vzdálená správa

- Brutte-force útoky na rozhraní vzdálené zprávy
  - Chyba uživatelů
  - Příliš jednoduchá/výchozí hesla
- SOHO pharming
  - Cca od 12/2013
  - Změna DNS serverů
  - Především Evropa a Asie
  - Zyxel (zranitelnost ROM-0(stažení konf.souboru a získání jména a hesla), D-Link, Micronet, Tenda, TP-Link (CSRF) a další.
  - Použito již ve dvou kampaních proti SoHo routerům

Vzdálená správa

- Obrana
  - Změnit výchozí jména a hesla
  - Vyhnout se triviálním heslům
  - Pokud to není nutné, vůbec nevystavovat konfigurační rozhraní do internetu

Chyba ve výchozí konfiguraci

- Obvykle chyba ve výchozím nastavení některé služby
- ASUS
  - Umožňuje připojení USB disků
  - V průvodci spuštění FTP přístupu k těmto diskům je jako výchozí možnost „limitless access rights.“
  - Ale i další volba, tedy „limited access rights“ umožňuje automatické zvolení jména a hesla „Family“
  - Seznam IP se špatně nakonfigurovanými routery ke stažení na serveru pastebin.com

Chyba ve výchozí konfiguraci

- Obrana
  - Nepoužívané služby vypnout
  - Služby konfigurovat s rozvahou
  - Penetrační testy :-)
  - Sledovat stránky výrobce

Chyby v kódu

- Chyby v implementaci rozhraní pro vzdálený přístup (XSS, CSRF, SQLi, atd)
- Linksys
  - Worm TheMoon
  - CGI skripty umožňující obejít přihlašovací jméno a heslo a spustit vlastní kód
  - Exploity pro zranitelné cgi skripty jsou známé
    - http://www.exploit-db.com/exploits/31683/

Chyby v kódu

- Chyby v implementaci síťových protokolů
- CISCO
  - NTP, DHCP, Internet Key Exchange protocol, NAT, PPTP, VPN, TCP input, IPv6 a další zranitelnosti
  - Obvykle denial-of-service, ale i možnost obejít přihlášení
- Obrana
  - Omezit běžící služby pouze na používané
  - Pokud to není nutné, vůbec nevystavovat konfigurační rozhraní do internetu
  - Sledovat nové verze a opravy firmware/software

Nejčastější útoky na lokální sítě (IPv4)

- Odposlouchávání bylo dříve snadné
  - Nepřepínaný ethernet
  - HUB, BNC
  - Data dorazila na všechny počítače v LAN
  - Standardně síťová karta poslouchá jen data pro její MAC adresu
  - Stačilo přepnout kartu do promiskuitního módu a poslouchat vše
  - Pasivní sniffing

Nejčastější útoky na lokální sítě (IPv4)

- Dnes přepínaný ethernet
  - Switch
  - Posílá data na port, kde je konkrétní MAC adresa
  - Informace o MAC vs. Port si ukládá do CAM (Content Addressable Memory) tabulky
  - Útoky aktivně ovlivňují síťové prvky, nebo protokol ARP
  - Aktivní sniffing

Nejčastější útoky na lokální sítě (IPv4)

- Programy pro odchytávání síťové komunikace
  - Ethereal
  - Wireshark
  - MS Network monitor
  - Tcpdump

Nejčastější útoky na lokální sítě (IPv4)

- Jak tedy odposlouchávat na přepínaném ethernetu
- Útokem na CAM tabulku
  - Co se stane, když se zaplní CAM tabulka?
  - Switch se začne chovat jako HUB a co nemá v CAM tabulce začne posílat na všechny své porty
  - Útočník tedy potřebuje zaplnit tabulku CAM
  - Nástroje macof, Yersinia

Nejčastější útoky na lokální sítě (IPv4)

- Jak tedy odposlouchávat na přepínaném ethernetu
- Útokem na CAM tabulku
  - Co se stane, když se zaplní CAM tabulka?
  - Switch se začne chovat jako HUB a co nemá v CAM tabulce začne posílat na všechny své porty
  - Útočník tedy potřebuje zaplnit tabulku CAM
  - Nástroje macof, Yersinia

Nejčastější útoky na lokální sítě (IPv4)

- Obrana proti zaplnění CAM na switchi
  - Port-security
    - Na daném portu povolím jen určité množství MAC, pokud se objeví další zařízení, spustí se administrátorem definovaná akce
- Otrava ARP Cache
  - Chci-li komunikovat po lokální síti, musím znát MAC cílového stroje (protokol ARP)
    - ARP slouží k překladu IP na MAC adresy

Nejčastější útoky na lokální sítě (IPv4)

Dotaz:

Adresová část	Datová část	
MAC adresa	IP adresa	MAC adresa
FF:FF:FF:FF:FF:FF	IP adr. cílového PC	00:00:00:00:00:00
Vaše MAC adresa	vaše IP adresa	vaše MAC adresa

Odpověď

Adresová část	Datová část	
MAC adresa	IP adresa	MAC adresa
Vaše MAC adresa	Vaše IP adresa	vaše MAC adresa
MAC adresa cílového PC	IP adr.cílového PC	MAC adr.cílového PC

Nejčastější útoky na lokální sítě (IPv4)

- ARP request
  - Požadavek na nalezení počítače, který má konkrétní IP
  - Posílá se na adresu broadcastu, takže ji obdrží všechna zařízení v dané LAN
- Počítač, který má danou IP jediný odpoví zpět
- Informace o propojení MAC a IP se dočasně uloží na PC

- Pokud už má záznam pro danou IP, pak si ARP protokol nehlídá, zda o data žádal
- Mohu tedy jako útočník poslat paket oběti, ve kterém nastavím jako MAC výchozí brány svou MAC adresu a zároveň bráně pošlu informaci, že k IP oběti patří moje MAC adresa

Nejčastější útoky na lokální sítě (IPv4)

- Tím vstoupím do komunikace mezi bránou a obětí jako prostředník, po přečtení dat pak posílám pakety již na správné MAC adresy
- Obrana
  - Individuální
    - DecaffeinatID0.09 http://www.irongeek.com/i.php?page=security/decaffeinatid-simp
      - Upozorní na změnu GW
    - arp -s IPMAC – statické přidání, dělá se někdy na konferencích (obzlášť na těch o hackingu:-))
    - XARP (Win i Linux)

Nejčastější útoky na lokální sítě (IPv4)

- LINUX
  - ARP Watch

    Lze nasadit i v síti, umí poslat zprávu adminovi
- Cisco switche
  - DHCP Snooping
    - Vytváří tabulku s IP, MAC adresou, port switche, vlan...
  - Dynamic ARP inspection
    - Používá tabulku vytvořenou DHCP Snooping funkcí ke kontrole, zda z daného portu mohla přijít konkrétní kombinace IP a MAC

Nejčastější útoky na lokální sítě(IPv6)

- IPv6 – délka 128 bitů, zapisuje se jako osm skupin po čtyřech hexadecimálních číslicích

  (2001:0718:1c01:0016:0214:22ff:fec9:0ca5)

- Zkrácený zápis
  - Nuly z leva lze vynechat fe80:0000:0000:0000:0202:b3ff:fe1e:8329 se zkráceně zapíše jako fe80:0:0:0:202:b3ff:fe1e:8329
  - následné skupiny nul lze nahradit dvojitou dvojtečkou "::", neboli fe80:0:0:0:202:b3ff:fe1e:8329 je také fe80::202:b3ff:fe1e:8329

Nejčastější útoky na lokální sítě(IPv6)

- Problémy:
  - IPv6 Již funguje i pokud jej v síti nemáte → tunneling → možné obcházení pravidel FW (Facebook) → možný útok na aplikace podporující IPv6 přes tunel
  - Hlavička má kvůli rychlejšímu routování jen 40 bytů → extension headers(EH) → možno libovolně řetězit, nesou další informace, např druh transportního protokolu → každá hlavička odkazuje na další hlavičku → propuštění paketu firewallem, buffer overflow, pád zařízení...

Nejčastější útoky na lokální sítě(IPv6)

- Neighbor Discovery Protocol (NDP)
  - Nahrazuje některé protokoly z IPv4, mimo jiné ARP a DHCP
  - Postup připojování hosta do sítě:
    - Host si pomocí vybrané procedury vytvoří ID rozhraní
    - Host si vytvoří linkovou lokální IP tak, že k prefixu FE80::/10 přidá vytvořené ID rozhraní
    - Host pošle dotaz Router Solicitation
    - Pokud je v síti router, odpoví zprávou Router Advertisement (RA), ta obsahuje:
      - Oznamovaný prefix
      - Router Lifetime – čas po který bude daný router figurovat jako výchozí brána
      - Další parametry, jako je MTU

Nejčastější útoky na lokální sítě(IPv6)

- Host si vytvoří ze zaslaného prefixu a ID rozhraní unikátní globální IPv6 adresu
- Pokud je LifeTime routeru větší než nula, pak si jeho IPv6 zařadí do seznamu výchozích bran

– Problém falešného RA

- Útočník zachytí a zmanipuluje RA z routeru
- Změní LifeTime na nulu, tak si oběť odstraní současnou GW ze seznamu
- Vytvoří vlastní RA, data tak budou téci z oběti přes jeho PC

– RA flooding

- útočník zaplaví LAN router advertisement, každý paket obsahuje 17 prefixu a rout, zatíží to procesor
- Zranitelné jsou: Windows a win servery, Juniper, Free/Net/opn-bsd - dle verze, OS X, Android, iOS

Nejčastější útoky na lokální sítě(IPv6)

- Myslete na to, že IPv6 už v síti máte (tunneling)
- OS který umí IPv6 si automaticky nastaví link local adresy, pak je možný přístup na port např. SSH po místní síti (zapomíná se na FW pro IPv6)
- Při nasazování můžete použít tyto nástroje pro otestování odolnosti sítě:
  - THC IPv6 attack toolkit (thc.org/thc-ipv6/)
  - SI6 Networks IPv6 Toolkit (www.si6networks.com/tools/ipv6toolkit)
    - fake_router26 – Rogue RA
    - kill_router6 – odstranění záznamu pro default gateway
    - flood_router6 – RA flooding

Nejčastější útoky na wi-fi sítě

- Bezdrátové sítě
- Používá bezlicenční pásmo
- Signál není vázán na fyzické médium, nemáme tedy kontrolu nad jeho šířením
- Provozní zprávy nejsou šifrovány (management a control frames)

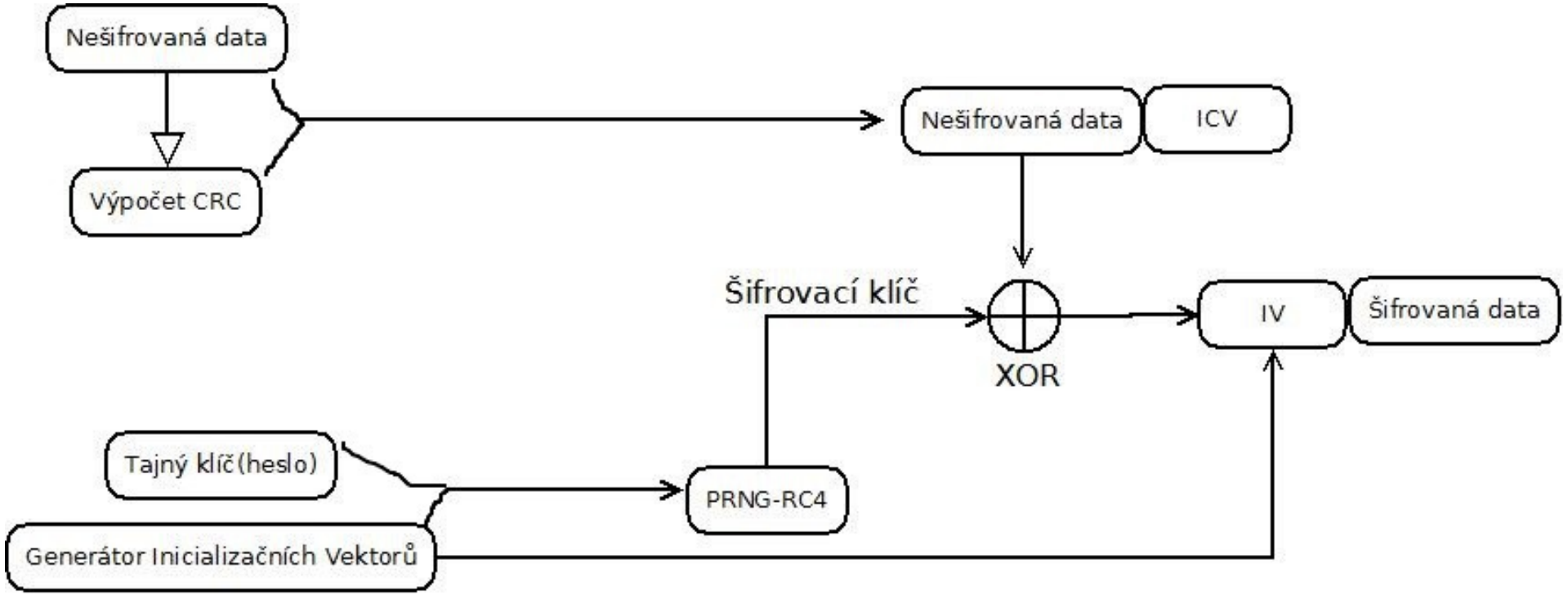
Nejčastější útoky na wi-fi sítě

- Filtrování MAC adres
  - MAC si zjistím a nastavím
- Skrývání SSID sítě
  - Klient ji při připojování prozradí, stačí jej tedy z wifi vyhodit
- WEP
  - Velmi rychlé prolomení
- WPA-PSK se slabým heslem
  - Slabé klíče možno prolomit pomocí slovníkového útoku

Nejčastější útoky na wi-fi sítě (WEP)

- 64 ,128 nebo 256 bit klíč
- Tajný (a sdílený) klíč + měnící se IV (Initialization vector) klíč generovaný vysílací stranou
- IV má vždy 24 bitů, zbytek je pro uživatelský klíč
- IV se posílá v nešifrované podobě v záhlaví rámce

Nejčastější útoky na wi-fi sítě (WEP)



Nejčastější útoky na wi-fi sítě (WEP)

- Šifra RC4 měla zabezpečit jedinečnost vzniklých šifrovacích klíčů
- Problém → Tajný klíč se nemění, náhodnost závisí jen od IV
- Délka IV jen 24 bit → 16,8 miliónu kombinací → dochází k opakování šifrovacích klíčů
- Při nachytání dostatečného množství zašifrovaných dotazů (cca 50 000 a více) lze WEP klíč získat aplikováním matematických a statistických metod

Nejčastější útoky na wi-fi sítě (WEP)

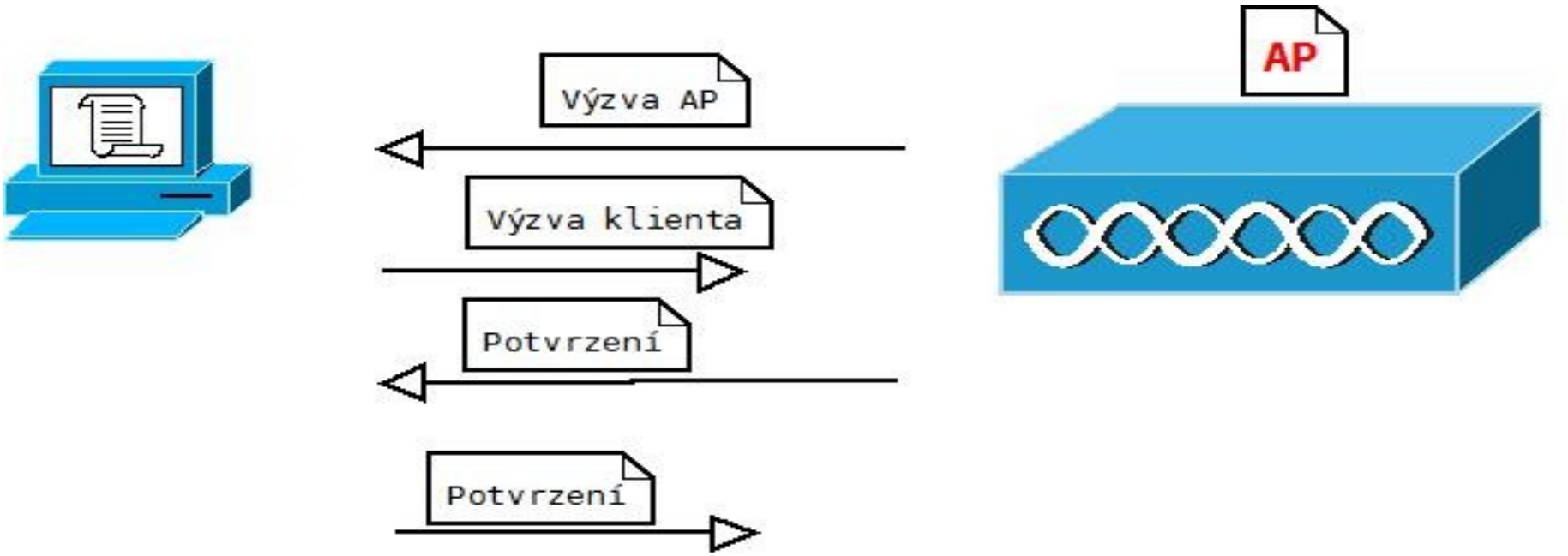
- Při útoku se zachytávají zašifrované ARP dotazy
  - Při velkém provozu je lze nachytat i pasivním odposlechem
  - Lze je snadno rozeznat dle velikosti
  - Lze snadno vynutit jejich opakování
- Opakovaným zasíláním ARP dotazů směrem k AP se vygeneruje potřebný počet rámců (a IV)

Nejčastější útoky na wi-fi sítě (WPA)

- Klienti sdílí stejný klíč pro přístup do sítě
- Každý klient má stejný 256bit PMK (Pairwise Master Key) klíč pro přístup k síti
- Každý klient má svůj jedinečný PTK (Pairwise Transient Key) klíč
- PMK generován pomocí funkce PBKDF2 (RFC2898)
  - Hash funkce SHA1-HMAC (RFC3174,RFC2104)
  - PMK = PBKDF2(heslo, SSID, Počet iterací (brzda) = 4096, délka klíče = 256)

Nejčastější útoky na wi-fi sítě (WPA)

- PTK klíč se vygeneruje po úspěšném připojení pomocí PMK
- Proces generování PTK



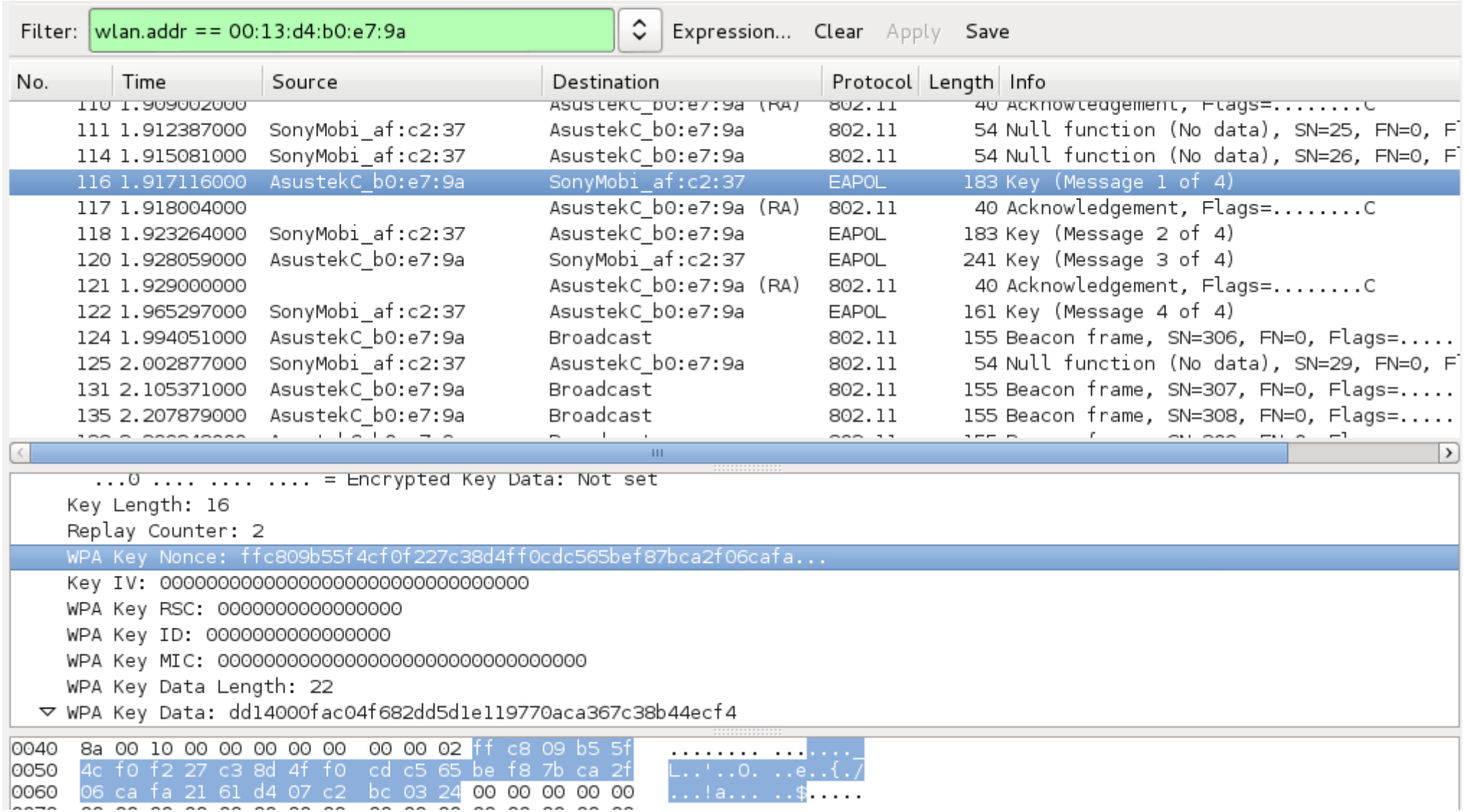
Nejčastější útoky na wi-fi sítě (WPA)

- PTK se vygeneruje z PMK, MAC klienta, MAC AP, výzvy klienta a výzvy AP
- Pokud špatný PMK, pak handshake skončí hned po prvním kroku
- Z PTK se odvodí klíče pro šifrování a kontrolní součty
- Heslo WPA-PSK jde prolomit jen slovníkovým útokem, je brzděn nutností 4096x generovat hash pro PMK
- Při dobře zvoleném hesle neprolomitelný v použitelném čase

Nejčastější útoky na wi-fi sítě (WPA)

- Pozor na výchozí SSID → Rainbow tables
- Pozor na riziko hotelů a dalších veřejných sítí s WPA!
  - Každý kdo zná sdílené heslo pro přístup k síti již může stejně jako u WEP číst vše, co posíláte
  - Musí pouze získat kompletní 4-way handshake
  - Aby toho dosáhl u již připojeného uživatele, stačí mu jej „vykopnout“ ze sítě, počítač se pak musí přihlásit a znovu získat PTK

Nejčastější útoky na wi-fi sítě (WPA)



Nejčastější útoky na wi-fi sítě (WPA)

- WPS (Wi-Fi Protected Setup)
  - Router nakonfiguruje v OS heslo pro přístup k WPA-PSK síti automaticky
  - Uživatel pouze zadá 8místný kód, který je někde na „krabičce“
  - Díky chybě implementace se potvrzuje každá polovina hesla zvlášť
  - Útočník tedy nehádá 10^8 kombinací, ale 10^4 + 10^4 = 20 000 kombinací
  - Ve skutečnosti ještě méně, protože 8 číslo v PIN je kontrolní součet
  - Nástroj reaver

Nejčastější útoky na wi-fi sítě

- Falešné AP
  - Připravím AP se stejným názvem, po připojení na něj se zobrazuje formulář s žádostí o zadání jména hesla
  - Pak vyhazuji klienty, dokud se někdo nechytí
- Pozor na chyby v ovladačích wifi karet
- Hole196
  - Chyba by design na všech WPA a WPA2 sítích
    - GTK (Group Temporal Key) pro broadcast a multicast
    - GTK je společné pro všechny klienty jednoho AP
    - Útok vyžaduje přihlášení do sítě
  - Umožňuje dešifrovat zprávy ostatních klientů (proto má smysl jen v 802.1X, i když zranitelné jsou i WPA-PSK), jedním směrem lze obejít také AP isolation mode
- VOIP

Nejčastější útoky na wi-fi sítě (WEP)

- Obrana
- Ve vaší síti
  - Nepoužívejte WEP
  - Pokud potřebujete WPA-PSK, použijte heslo s vysokou entropií
  - Ideálně používejte 802.1X pro autentizaci
  - Zapněte AP isolation mode
- Na cestách
  - Používejte vlastní šifrování
    - VPN
    - SSH Tunneling

Kde najít více

- http://www.csirt.cz/news/security/
  - Novinky z bezpečnosti zaměřené na ČR
- http://www.root.cz
  - Každé pondělí „Postřehy z bezpečnosti“
  - Souhrn událostí na poli bezpečnosti z posledního týdne
- http://www.soom.cz/
  - Český server o hackingu
- http://www.kyberbezpecnost.cz/

Kde najít více

- https://bettercrypto.org/
  - Návody na lepší zabezpečení různých síťových služeb
- http://securityaffairs.co/wordpress/
- http://thehackernews.com/
- https://isc.sans.edu/
- http://www.govcert.cz/cs/informacni-servis/zraniteln

Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz