

# A hype és ami mögötte van



## EPIC FAIL

Seriously, how the fuck did you manage that?

# Miről lesz szó?

- Áttekintés az elmúlt egy év alapvető infrastruktúrát érintő biztonsági eredményeiből
  - És egy kis múltba révedés
- Gondolatébresztő
  - Hogyan váltak az Internet létrehozásakor meghozott tervezői döntések mára elavulttá
- Néhány demo ;)

# Mit írnak a lapok?

- "Már az SSL-lel védett weboldalakon sincsenek biztonságban az információk" - HWSW
- "Kijátszható a web legelterjedtebb titkosítási módszere" - Index
- "... leáldozott az SSL-lel fedezett banki tranzakcióknak?" - IT café

# Kezdjük az elején

- SSL: Secure Sockets Layer /  
TLS: Transport Layer Security
  - Végponttól végpontig működő
  - ... hitelesítés és titkosítás
  - "Keret" protokoll, amely különböző kriptográfiai algoritmusokat tartalmaz
    - pl.: RSA, AES, SHA-1 stb...
  - Ha ezeket "feltörnék", nagy bajban lennénk!
  - HTTPS, IMAPS, POP3S, stb...

# Kezdjük az elején

- Hitelesítés
  - Tudjuk ki beszél/kihez beszélünk a túloldalon
  - Ezt egy Nagyon Megbízható Szervezet (CA) garantálja
  - És az, hogy nem tudunk hatékonyan faktorizálni :P
- Titkosítás
  - Nem tudják elolvasni amit írunk
- Végponttól-végpontig
  - A köztes állomások nem pofátlankodhatnak bele a kommunikációs csatornába

# HTTPS for dummies

- A böngésző nyit egy kapcsolatot a webservert felé egy megbízhatatlan (Internet-) kapcsolaton
  - Odamegyünk a Moszkva téren egy emberhez
- Kézfogás során felderítik egymás képességeit
  - Do you speak English? Sprechen Sie Deutsch?
- Tanúsítványt cserélnek és ellenőrzik azt
  - Megbízható (pl. államilag kiadott) személyi okmány
- Ha minden rendben van, létrehoznak egy **biztonságos és hiteles** csatornát és lőn

# Ahol bánáhnéhj kerülhet a földre

- A csatorna csakis akkor biztonságos (csak a két fél érti a beszélgetést) és hiteles (a másik fél az, akinek mondja magát), ha a tanusítvány
  - Olyan által van hitelesítve, akiben bízunk (→ a böngészőnk bízik)
    - Rendőr sem fogad el könyvtári tagkártyát
  - A tanúsítandó entitásnak szól
    - vö: valaki másnak a személyi igazolványa

# Mi volt a hírek alapja?

- Moxie Marlinspike és az SSLStrip
- Felhasználói figyelmetlenség
  - Nem figyelünk eléggé a címsorra
  - Különös tekintettel a protokollazonosítóra
  - A pozitív visszacsatolást jobban értékeljük, mint a negatívát
- Az SSL-lel technikai értelemben nincs probléma.

# 2009.

- Még mindig Mr. Marlinspike
- Implementációs problémák
  - A NULL byte lezárja a stringeket (C/C++)
  - Automatizált tanúsítványkiadás
  - Az X.509 tanúsítványok más módon jelzik a karakterláncok hosszát
  - Így tanúsítvány mezőibe került NULL karakter eljuthat a (C-ben/C++-ban írt) böngészőig

# X.509 WTF?

- ITU-T Szabvány többek között a nyilvános kulcsú infrastruktúrák tanúsítványainak formátumára
  - Egyebek: Visszavonási listák, tanúsítási-út ellenőrzési algoritmus stb.
- Hierarchikus, egyirányú CA láncot feltételez
  - Szemben pl. a PGP bizalmi hálójával

# 2009.

- Dan Kaminsky
- További implementációs problémák - X.509
  - MD5 ill. MD2(!) ujjlenyomatok elfogadása
    - Frédéric Muller (2004): Az MD2 "nem egyirányú"
    - 25C3: MD5 lenyomattal rendelkező tanúsítvány hamisítása
  - Nem szabványos tanúsítványok elfogadása és eltérő értelmezése
- Ezek még mindig nem az SSL hibái!

# 2009...

- Chen-Mao-Wang-Zhang: Pretty Bad Proxy
- A proxy nem hitelesíti magát
- A böngésző sokszor automatikusan proxy után kutat
- Az SSL végponttól végpontig tartó biztonságot adna, de ...

# Pretty Bad Proxy

- További implementációs problémák
  - A proxy-k nem hitelesítik magukat, könnyű célpontok stb.
  - A proxy által generált üzenetek titkosítatlanul továbbítódnak
  - A böngészők rosszul valósítják meg a cross-domain policyt
    - A tanúsítványok cache-elődnek
    - Az átirányítás után betöltött oldalak az eredeti domain kontextusában renderelődnek
    - Legtöbb helyen már javítva

# Mi a valódi probléma?

- A felhasználók amúgy is magasról tesznek a tanúsítványokra
- Sokan még mindig elavult böngészőket használnak
- A leggyengébb láncszem messze nem az SSL!
  - Sőt, ez jelenthetné az utolsó védelmi vonalat
  - De a hozzánemértők ügyesen beszélik le használatáról a felhasználókat :P

# Tényleg ez a legnagyobb problémánk?

- Az Internet a "hagyományos" biztonsági szemléletre épült
  - Védjük a "várfalat", a bent lévőkben megbízunk
  - Lásd még: Trójai faló...
- A bejutási küszöb az évek során eltűnt
- Így mindenki kedvére bulizhat a várban :)

# DNS (1983)

- Domain Name System - "Az Internet telefonkönyve"
  - Domain névhez IP cím
  - Hierarchikus felépítés, rekurzív lekérdezések
  - Nagyon régi infrastruktúra
  - Ma már nélkülözhetetlen az internetes szolgáltatások működéséhez
- Gyakrolatilag semmilyen hitelesítést nem valósít meg!

# DNS

- Mindössze egy 16 bites mező (QueryID) akadályozza meg a MitM támadásokat
- 2008. Dan Kaminsky: "Meg kell foltozni az Internetet!"
  - Praktikus támadás a DNS infrastruktúra ellen
  - Bármely domain név eltéríthető
  - Hatalmas titkolózás, végül egy "véletlen" folytán idő előtt nyilvánosságra kerül a módszer
  - AT&T elleni sikeres támadás

# DNS – Hagyományos mérgezés

- Kérdezzük egy névre
- Megpróbálunk gyorsabban válaszolni, mint a legitim NS + eltalálni a QID-t
  - A QID szekvenciális!
  - Az aktuális érték lekérdezhető egy másik névszerveren, vagy lehallgatással
- Ha nyertünk, a válaszuk bent marad a gyorsítótárban TTL-ig
- Megoldás: Legyen véletlenszerű a QID!

# DNS – Kaminsky módszere

- **Rengeteg véletlen kérést intézünk a célpont NS felé**
  - A legitim NS ügysem fog tudni válaszolni
- **A válaszokban csak az authoritative NS-t határozzuk meg – a sajátunkat :)**
- **Megfelelő mennyiségű kérdés esetén jó eséllyel betalálunk**
  - Boldog születésnapot!
- **Miénk a teljes zóna!**

# DNS – A megoldás

- **Jelen: DNS source port randomization**
  - Nem csak a QID, hanem a forrás port is egy véletlen generált érték, ami "hitelesíti" a névszerveret
  - Ideiglenes megoldás, Gigabiten talán ez is kevés!
- **Jövő: DNSSEC**
  - Hitelesített megvalósítás
  - Jelentős fejlesztéseket igényel a globális infrastruktúrában
  - 2010-től a .edu gTLD tervezi megvalósítani
  - A Pentagon szorgalmazza a bevezetést
- **Addig is: SSL a felhasználói oldalon**

# BGP (1994)

- Border Gateway Protocol
  - Autonóm rendszerek (AS) peremrouterei közti információcserére
    - Tipikusan ISP-k között
  - Az alap Internet infrastruktúra kritikus komponense
  - Úthossz-vektor protokoll
  - Nincs hitelesítés!
  - A biztonságot csak az AS-k közti bizalom garantálja
- Lásd még: Szabó István – Hacktivity 2008!

# BGP - Működés

- Útvonalinformációk UPDATE üzenetekben
  - Visszavont útvonalak
  - Elérhető hálózatok
  - Az elérhető hálózatokhoz vezető útvonalak
- A belső szabályrendszernek megfelelő útvonalak használata
- Útvonalak továbbítása a szomszédos csomópontok felé

# BGP – Támadási lehetőségek

- "Fekete lyuk"
  - Elérhetetlen célpontok
- Instabilitás okozása
  - Szakadozó összeköttetések
- Átirányítás
  - Lehallgatás
  - MitM
  - Irányított DoS

# BGP - Támadások

- Jogosulatlan útvonalhírdetés
  - MOAS
- Legrövidebb utakról szóló üzenetek propagálása
- Hálózati torlódás okozása
  - Sok eldobott útvonal
  - A helyreállítás után az eldobott útvonalak pótlása hatalmas BGP forgalmat generál

# BGP – Néhány ”incidens”

- L0pht 1998
  - ”30 perc alatt ledöntjük az Internetet”
- YouTube vs. Pakisztán – 2008
- Kapela-Pilosov – 2008
  - A teljes eltérített forgalmat továbbították a megfelelő helyre, így észrevétlenek maradtak

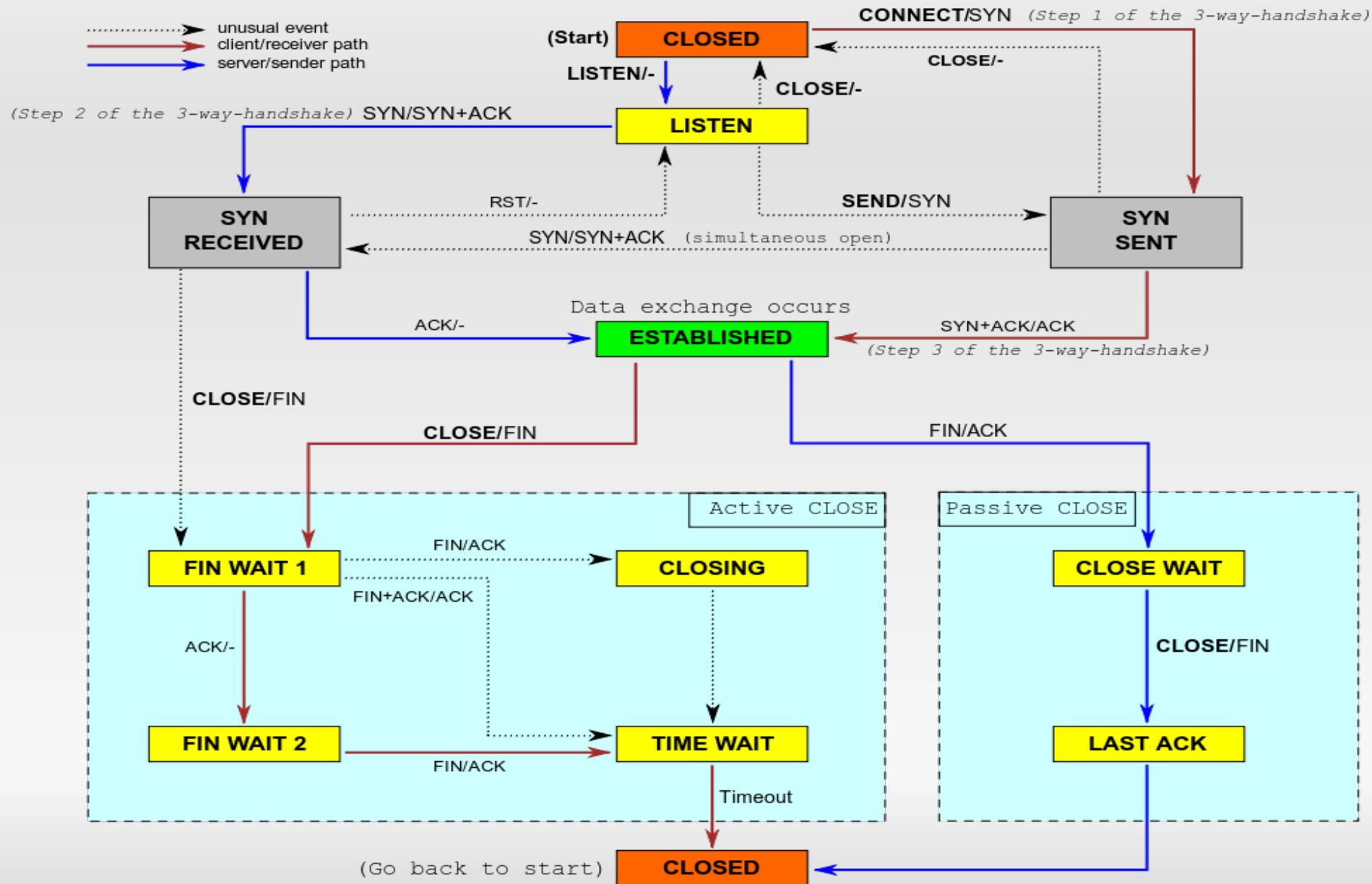
# BGP – Védekezés

- Rész megoldások:
  - Statikus szűrők
    - Naprakész, globális képet igényel a teljes hálózatról!
  - BGP TTL Security Hack (BTSH)
  - TCP MD5(!) Signature Option
  - Az átviteli utak védelmére: IPSec
- A jövő: PKI alapú hitelesítés
  - S-BGP
  - so-BGP

# TCP (1981)

- Transmission Control Protocol
  - Szállítási réteg
  - Állapotokkal rendelkezik
  - Visszaigazolás, sorszámozás, flow control stb...
  - "Három-utas kézfogás"
    - SYN
    - SYN/ACK
    - ACK
  - HTTP, POP, FTP stb.

# TCP állapotdiagram



# TCP – SYN Flood

- Sok SYN-t küldünk
  - Akár hamis IP-ről
- Az áldozat erőforrásokat allokál a kapcsolat számára
- A SYN/ACK-ra már nem küldünk választ
- Az áldozat erőforrásai foglaltak maradnak még egy ideig...
- ... elég SYN esetében elfogynak :(

# TCP – SYN sütik

- Nem helyi erőforrásokat használunk a kapcsolódási kísérlet adatainak nyilvántartására
- Ehelyett a SYN/ACK csomag sorszámába kódoljuk a szükséges információkat
  - Mi határozzuk meg
  - Visszajön az ACK-kal
- Ha egy legitim fél visszaküldi a megfelelő ACK-t, vissza tudjuk állítani a SYN-t

# TCP – Kliens oldali SYN sütik

- Csökkentsük az erőforrásigényt a támadói oldalon is!
- Kódoljuk a kapcsolat adatait a SYN sorszámába
  - Mi választjuk meg
  - Visszajön a SYN/ACK-kal
- A Timestamp mezőt időmérésre használhatjuk
- Minimális erőforrással tarthatunk fenn kapcsolatokat!

# Sockstress – *Faló a várban*

- Jack C. Louis, Robert E. Lee
  - Unicornscan
- Támadáscsoport
  - Miután a kapcsolat kiépült, az áldozat feltételezi, hogy nem akarunk rosszat
- Nyilvánossághozatal (?): 2009. 09. 08.
  - Jó közelítések: Phrack #66, fabs, Steve Gibson...
  - Több hasonló megközelítés létezik
    - **FIN\_WAIT-1**
    - **FIN\_WAIT-2**

# NKiller2 - FIN\_WAIT1

- Ithilgore, Phrack #66
  1. Támadó: Elfogyott a pufferem (ablakméret: 0)
  2. Célpont: Időzítő → Van már helyed?
  3. Támadó: Még nincs, GOTO 1
- A körülfordulási idő növelésével növelhetjük az időzítést

# Sockstress – Megoldás?

- MS09-048
  - Véletlenszerűen dobálunk el kapcsolatokat vész esetén
  - A Windows XP-re nincs folt
- Red Hat
  - Mivel nincs upstream patch kilátásban (!) tűzfalszabályok érvényesítésével lehet védekezni támadás esetén

# Konklúzió?

- Már nem (csak) az atombombáktól kell tartani...
- A drót másik végénél nem biztos, hogy az ül, akire számítunk
- Leginkább a matematikában bízhatunk
  - Titkosítás és hitelesítés FTW!
  - Sajnos sokszor itt is csak a tapasztalat alapján...
- A technológia már megvan a biztonságos kommunikációhoz
  - A Internetet sem lámák építették
  - Minden csak elszántság és idő kérdése...

# Utószó

”Senkiháziak kezében van az IT security szakma” :)

**Köszönjük a figyelmet!**

[buherator@silentsignal.hu](mailto:buherator@silentsignal.hu)  
[vsza@silentsignal.hu](mailto:vsza@silentsignal.hu)

# További olvasnivaló

- <http://www.blackhat.com/presentations/bh-usa-09/MARLINSPIKE/BHUSA09-Marlinspike-DefeatSSL-PAPER1.pdf>
- <http://thoughtcrime.org/papers/null-prefix-attacks.pdf>
- <http://thoughtcrime.org/software/sslstrip/>
- <http://research.microsoft.com/apps/pubs/default.aspx?id=79323>
- <http://www.sockstress.com>
- <http://recurity-labs.com/content/pub/25C3TCPVulnerabilities.pdf>
- <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>
- <http://www.cc.gatech.edu/~dovrolis/Papers/ccr-bgp.pdf>