Säkerhetsbrister & intrång

Internetdagarna 2001

© Anders Ingeborn 08-662 10 70 www.ixsecurity.com

Vem är Anders Ingeborn?

- Civilingenjör Datateknik KTH
- iXsecurity
- Frilansskribent
- Föredragshållare

© Anders Ingeborn 08-662 10 70 www.ixsecurity.com

Innehåll

- Tekniska säkerhetsbrister
- Trender
- Erfarenheter från säkerhetsgranskningar
- Tips för att skydda sig

Code Red

- Juli 2001 375.000 infekterade webbservrar
- Inslag på SVT 31 juli
  - ”slå ut hela internet”
- Många stora tidningsrubriker

Vad var felet, rent tekniskt?

- Minnesöverskrivning
- ”Buffer overflow”
  - Minneskopiering
  - Formatsträngar
- Skickar maskinkodsinstruktioner
- Servern exekverar dessa!

Var ligger felet?

- Mellan teori och praktik
- Inte direkt ett designfel i webbservern
  - Möjligen av datorarkitekturen
- Snarare implementationsfel
  - Slarvig programmering
  - Ingen bra minneshantering
  - Otillräcklig kvalitetskontroll

Trender

- Minnesöverskrivning
  - Vanligaste typen av brist i 10 år!
    - Oregon Institute of Technology -99
  - Ökad komplexitet i applikationer
    - Svårare att överblicka och granska
- Maskar
  - Morris Worm 1988, 10% av internet
  - CodeRed, Nimda...

Hur kan man skydda sig?

- Blockera symptom (enklast)
  - Trafik på okända portar etc.
- Filter framför webbserver (lite svårare)
  - Tillåt ingen maskinkod
  - Endast fördefinierade webbsidor
- Granska kod (svårt)
  - Öppen källkod? Tid? Kunskap?

Blockera symptom?

- Brist i form av minnesöverskrivning
  - Angrepp in över port 443/tcp
  - Maskinkodsinstruktionerna öppnar kommandoskal på port 31337/tcp
  - Förhindra angriparen att ansluta!
- Men se upp!
  - Webbservern kanske får ansluta sig tillbaka till angriparen!

Räcker det inte så?

- Port 443 in och ingen ut...
- Angripa med enbart ASCII-kod
- Byta ut en tillåten webbsida
  - .asp, .jsp, .php, .cgi, .exe, eller .dll?
- Utnyttja befintlig TCP-session
  - Komma undan många IDS

Filter framför webbservern?

- Ingen maskinkod
  - Vissa maskinkodsinstruktioners bytevärden är giltiga ASCII-tecken
- Endast fördefinierade webbsidor
  - GET /webbsida.html HTTP/1.1
  - GET /#\,?-ä¨C´´,¤]`_ss1}&£:
  - Kontrollera alla fält i HTTP-huvudet
    - Till exempel ”Host: ´,¤]`_ss1}”

Se upp!

- Erfarenhet från 2001
- Vissa filter har egna problem
  - Unicode
  - Luras att släppa igenom trafik!
- Falsk trygghet?
  - Underlåtit att säkra systemen bakom

Gäller det bara vanliga webbservrar?

- Nej, även PKI-system
- Ger ut certifikat till alla och envar
- OCSP-tjänst över HTTP
  - Minnesöverskrivning?
  - Privat nyckel för signering av svar klartext på hårddisk?

Andra brister i PKI-system?

- Det stod ju att det var säkert?
  - ”RSA med 1024 bitars nycklar”
- RSA bra algoritm
  - Om man använder den rätt
- Leverantören implementerat själv?
- Följer standard?
- Vilken version?

Följer standard?

- Attack mot ”ren RSA”
  - Generera falska RSA-signaturer
- Faktorisera checksummorna för ett visst meddelande
- Lyckas lura tjänsten att signara delarna var för sig
- Multiplicera ihop signaturerna
- Motmedel: utfyllnad enligt PKCS#1 v1.5

Vilken version?

- Kryptera meddelanden med publik nyckel
- Orakel som dekrypterar och svarar om
  - Vettig PKCS#1 v1.5-padding?
  - Vettigt meddelande?
- Attack som liknar ”intervallhalvering”
  - utesluta sig fram till klartextmeddelandet
  - kräver cirka 1 miljon frågor
- Motmedel: utfyllnad enligt PKCS#1 v2.0

Slutsats

- Algoritmen RSA är bra
  - Det är svårt att faktorisera stora tal
- En produkt är inte nödvändigtvis bra..
  - ..för att det står RSA utanpå
  - Den måste användas på rätt sätt

Mer om kryptering

- RadioLAN enligt IEEE 802.11b
- #1 Nätnamn
  - skickas i klartext
- #2 Spärrlista MAC-adresser
  - skickas i klartext, enkelt byta sin egen
- #3 Kryptering enligt WEP

Nyckellängd och entropi

- Nyckellängd: 64 bitar
  - 2^64 är ett stort tal
- Osäkerheten, ”entropin”, är lägre
  - 24 bitar i klartext, 40 bitar kvar
  - 40b / 8b per bokstav i ett lösenord = 5
  - A-Z a-z 0-9 ”utnyttjar” inte alla 8 bitar
    - Snarare 6 bitar, eller 2^30

RC4 precis som RSA

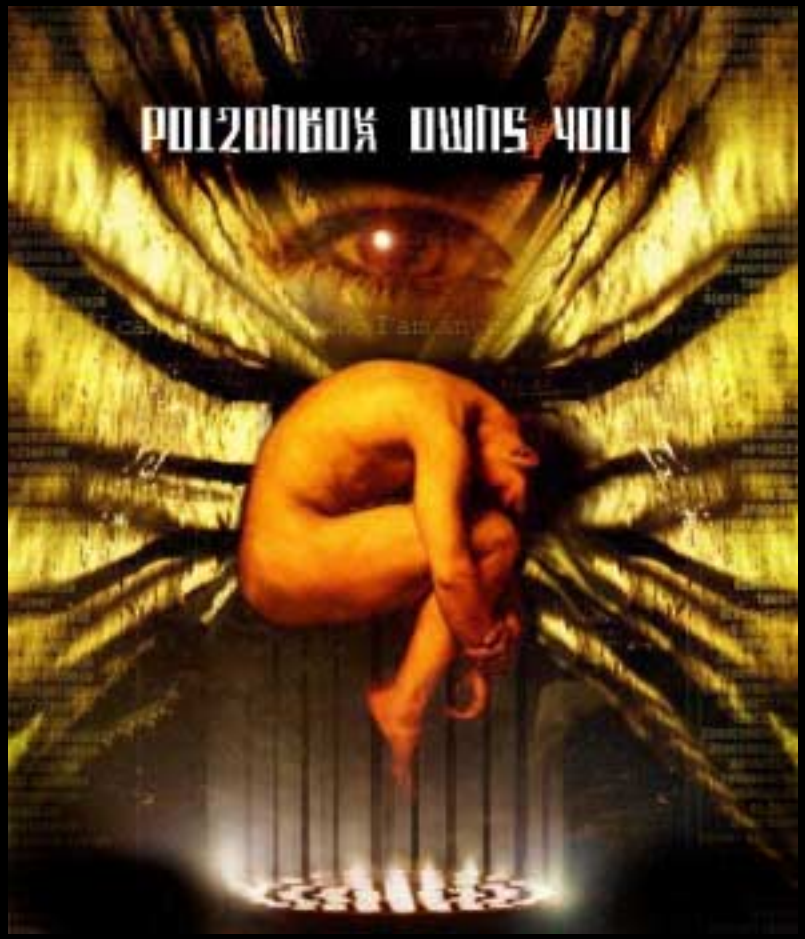
- RC4 ”skapligt bra” krypteringsalgoritm
- Om man använder den ”rätt”
  - Relativt få nyckelbitar ger flertal bitar i början av slumpströmmen
  - Slumpströmmen möjlig identifiera eftersom nätverkstrafik är förutsägbar
  - Möjlig gå bakvägen och beräkna nyckelbitar från inledande slumpström
  - Ännu enklare om en del av nyckeln är känd

Vadå använder RC4 rätt?

- Kastar inledande slumpström
- Inte tillåter en del av nyckeln vara känd
  - RC4(Hash(IV | lösenord))(data)
- Hur gjorde man i WEP?
  - Använder bara inledande sekvenser
  - 24 bitar av den nyckeln i klartext

Oj, så jobbigt

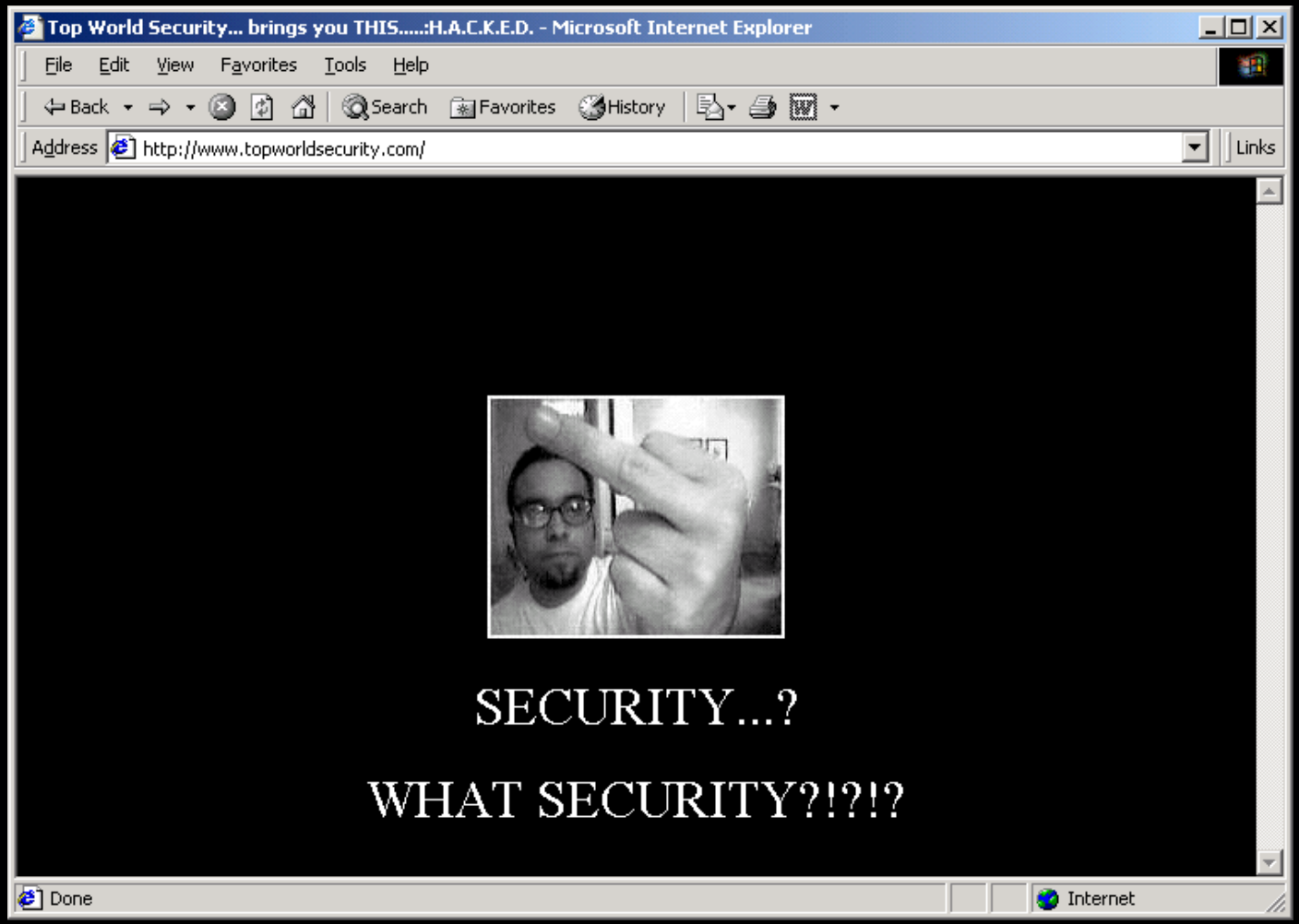
Det händer nog inte oss...



Alla och alla med hög profil

- Spontana angrepp mot alla
  - Grannarna, de närmaste
  - Breda sökningar
    - Många IP-adresser få brister
- Angrepp mot alla med hög profil
  - Microsoft drygt 15 gånger i vår/sommar
  - Företag med ”security” eller ”police”
  - Yahoo! News

www.topworldsecurity.com




BW Online | September 20, 2001 | Yahoo! News Hacked - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.businessweek.com/technology/content/sep2001/tc20010920_4498.htm
Links
BusinessWeek online
Search
e.biz
BW MAGAZINE
DAILY BRIEFING
INVESTING
GLOBAL BUSINESS
TECHNOLOGY
SMALL BUSINESS
B-SCHO
SEPTEMBER 20, 2001
TECHNOLOGY
SECURITY FOCUS
Yahoo! News Hacked
Hacker tinkers with news stories undetected
In a development that exposes grave risks of news manipulation in a time of crisis, a hacker demonstrated Tuesday that he could rewrite the text of Yahoo! News articles at will, apparently using nothing more than a web browser and an easily-obtained Internet address.
Yahoo! News, which learned of the hack from SecurityFocus, says it has closed the security hole that allowed 20-year-old hacker Adrian Lamo to access the portal's web-based production tools Tuesday morning, and modify an August 23rd news story about Dmitry Sklyarov, a Russian computer programmer facing federal criminal charges under the controversial Digital Millennium Copyright Act (DMCA).
Recent Tech Features
Tech Special Reports
Microsoft Watch
E.Biz
Product Reviews
Internet Security
Science & Health
Tech Columns
COLUMNS
FORUMS & CHATS
NEWSLETTERS
PERSONAL FINANCE
SEARCH & BROWSE
SPECIAL REPORTS
TOOLS & SCOREBOARDS
VIDEO VIEWS
How can you use software to launch a service business?
Sponsored by IBM
Provided By
SecurityFocus
Printer-Friendly Version
E-Mail This Story
RELATED ITEMS
Variables.nocolonstrap Archive
Internet

Hur går ett angrepp till?

- Leta efter svag punkt!
  - Kända brister
  - Breda sökningar
  - Tålamod
- Skapa en plattform för nya angrepp!
  - Kommandoskal
  - Grafisk fjärradministration
  - Avlyssning

Vanligt på svenska företag

- Senaste version av ”huvudwebbserver”
- Senaste version av känt UNIX-OS
- Alla säkerhetsuppdateringar
- I princip inga onödiga tjänster
- Bortglömd MS-IIS 4.0 ett närliggande segment, labbnät, testnät etc.
  - Administratör på en eftermiddag
  - Plattform för angrepp

Vanlig situation #2

- Webbserver på hotell
  - Webbmail själv, t.ex. OWA
  - Lämnar ut addressboken
- Ingen spärr för antal felaktiga inloggningsförsök mot webbmail
- Exponera webbserverbrister inne på webbmail
- Plattform för attack mot interna system
  - Även från DMZ

Vanlig situation #3

- Distansarbetsplats i bredbandshem
  - Angrepp mot ”vanlig” dator enklare
- Plocka ut användaruppgifter
  - Anslut själv!
- Nu börjar nästa föredrag...

Frågor

- Nu direkt
- När som helst under konferensen
- Via e-post: ingeborn@ixsecurity.com