

```

/* reverse tables */

#define RT1
V1S1,F4,A7,50) V1E,41,65,53) V1A,1,F,A4,C0) V1M,
V1B,AB,0B,CB) V1F,9D,45,F1) V1AC,FA,5A,AA) V1D,
V1G,3D,FA,55) V1AD,76,6D,F0) V1R,CC,76,91) V1H,
V1F,E5,D7,FC) V1CS,2ACB,D7) V1G,35,4A,80) V1M,
V1E,B1,5A,49) V1S,BA,1B,67) V1N,EA,0E,9E) V1R,
V1C3,2F,75,02) V1B,4C,F0,12) V1D,46,97,AA) V1E,
V1D,8F,5F,E7) V1S,92,9C,95) V1B,6D,7A,BD) V1D,
V1D,1E,83,2D) V1S,74,31,D3) V1R,99,69,2D) V1F,
V1S,C2,89,6A) V1F,4E,79,79) V1R,58,3E,6B) V1R,
V1E,B1,4F,6B) V1R,4A,AD,17) V1C,2,0AC,06) V1S,
V1S,DF,4A,19) V1S,1A,31,31) V1R,31,2A,6D) V1B,
V1B1,64,77,ED) V1B1,6B,AE,84) V1E,42,AB,8C)
V1G,48,68,58) V1B,F,45,FD,19) V1B,DE,6E,6E)
V1AB,73,DX,23) V1Z,4B,02,E2) V1S,1F,8F,57)
V1E,EB,78,07) V1F,BS,C2,03) V1B,C3,1E,78)
V130,28,87,F2) V1Z,EF,AS,B2) V1D,0,0A,0A)
V1R,ACE,1C,2B) V1A,79,B4,92) V1S,07,23,F7)
V165,DA,F4,CD) V1G,05,DE,D5) V1D,18,62,1B)
V134,3E,53,9D) V1A,3F,55,AD) V1S,4A,E1,7E)
V1B,83,EC,39) V1B,66,EF,AA) V1S,71,59,2E)
V1E,1,8A,F9) V1G,DD,3E,05,4E)
V1B,5A,AD,E5) V1F,CA,07)
V119,9B,ED,94) V1G,8D,E8) V1E,66,3D,33)
V1B,0E,8,42,DD) V1G,82,82) V1B,0,2,2C)
V1A,7C,04,47) V1C,42,0F,E) V1E,0,3,3D)
V1D9,8D,86,83) V1Z,2B,ED,4) V1D,1,0,0)
V1D,0E,FF,F0) V1F,85,3E,5E) V1D,1E,05,1E)
V1D,0F,D9,64) V1E,5C,A6,21) V1D,5H,4A,01)
V1C,0A,67,B1) V1Z,57,E7,0F) V1E,EE,9E,1D)
V1R,C0,C5,4F) V1G,DC,0A,2) V1A,77,4E,0E)
V1E,93,BA,0A) V1C,0A,2A,E5) V1C,51,00,4)
V1E,09,DD,0E) V1Z,8B,C7,AD) V1Z,D6,3E,9A)
V1G,71,19,85) V1F,75,07,42) V1E,99,DD,00)
V1F,01,26,8F) V1C,2,2,2,2) V1A,66,30,33)
V1B,43,29,76) V1E,43,C6,4C) V1B,ED,0D,0A)
V1D7,11,DC,CA) V1E,64,8S,10) V1D,37,34,99)
V1E,4A,24,7D) V1Z,EB,38,F4) V1E,19,18,1D)
V1D,9E,3F,4B) V1C,B2,3D,F4) V1D,66,52,2C)
V1D,E3,16,6C) V1A,70,B9,99) V1I,34,48,0A)
V1A,FC,8C,C4) V1A,0,F,1A) V1E,7D,7C,2C)
V1B,74,9,4E,C7) V1D9,38,D1,C1) V1C,CA,AD,0E)
V1A6,F5,31,CF) V1A5,7A,DE,3B) V1A,07,8E,
V1C,3A,9D,E4) V1S,71,87,0D) V1E,45,0E,4E)
V1E,8D,1A,C9) V1R,DA,B9,E4) V1E,89,F8,00)
V1E,5D,8D,8E) V1B,9,8D,7D) V1F,DA,DA,0E)
V1C,AE,89,3D) V1D,18,7D,A7) V1E,9C,83,00)
V1C,D,26,78,09) V1E,89,18,F9) V1C,WA,B7,00)
V1E,95,8E,65) V1A,FE,EA,7E) V1D,1A,CF,0E)
V1A,B1,9B,D9) V1A,07,35,CB) V1E,8,0E,0E)
V1I,A9,ED,AF) V1A,1E,31,31) V1C,AA,9E,0E)
V174,4E,BC,3D) V1C,81,CA,A0) V1D,9D,0E,0E)
V1F,04,98,4A) V1L,EC,DA,F7) V1F,0D,0E,0E)
V176,4D,T6,8D) V1A3,6F,B0,4D) V1C,AA,4E,0E)
V1E,D1,B5,E3) V1C,6A,84,16) V1C,1N,1F,0E)
V1D,SE,EA,04) V1D,3C,35,5D) V1A,4E,9E,0E)
V1B3,67,1D,5A) V1D,DE,DD,5A) V1E,0,0E,0E)
V1A,D7,01,83) V1Z,41,0C,2A) V1S,4E,7A,0E)
V1C,A9,77,ED) V1Z,61,C9,5A) V1E,1,0E,0E)
V1C,DD,DF,59) V1S,77,7A,31) V1A,1A,0E,0E)
V1B3,F7,CD,EA) V1S,FD,A1,2B) V1D,3D,0E,0E)
V1C,A7,F3,81) V1B,68,C4,82) V1D,79,0E,0E)
V1E,1D,C3,72) V1E,E2,25,0E) V1E,42,0E,0E)
V139,AS,01,71) V1E,DC,B1,DE) V1D,2D,0E,0E)
V17B,CB,84,61) V1S,32,E6,70) V1E,0E,0E,0E)

```

```

#define V(a,b,c,d) static const unsigned RT1[256] = {
}
#define V(a,b,c,d) static const unsigned RT2[256] = {
}
#define V(a,b,c,d) static const unsigned RT3[256] = {
}
#define V(a,b,c,d) static const unsigned RT4[256] = {
}

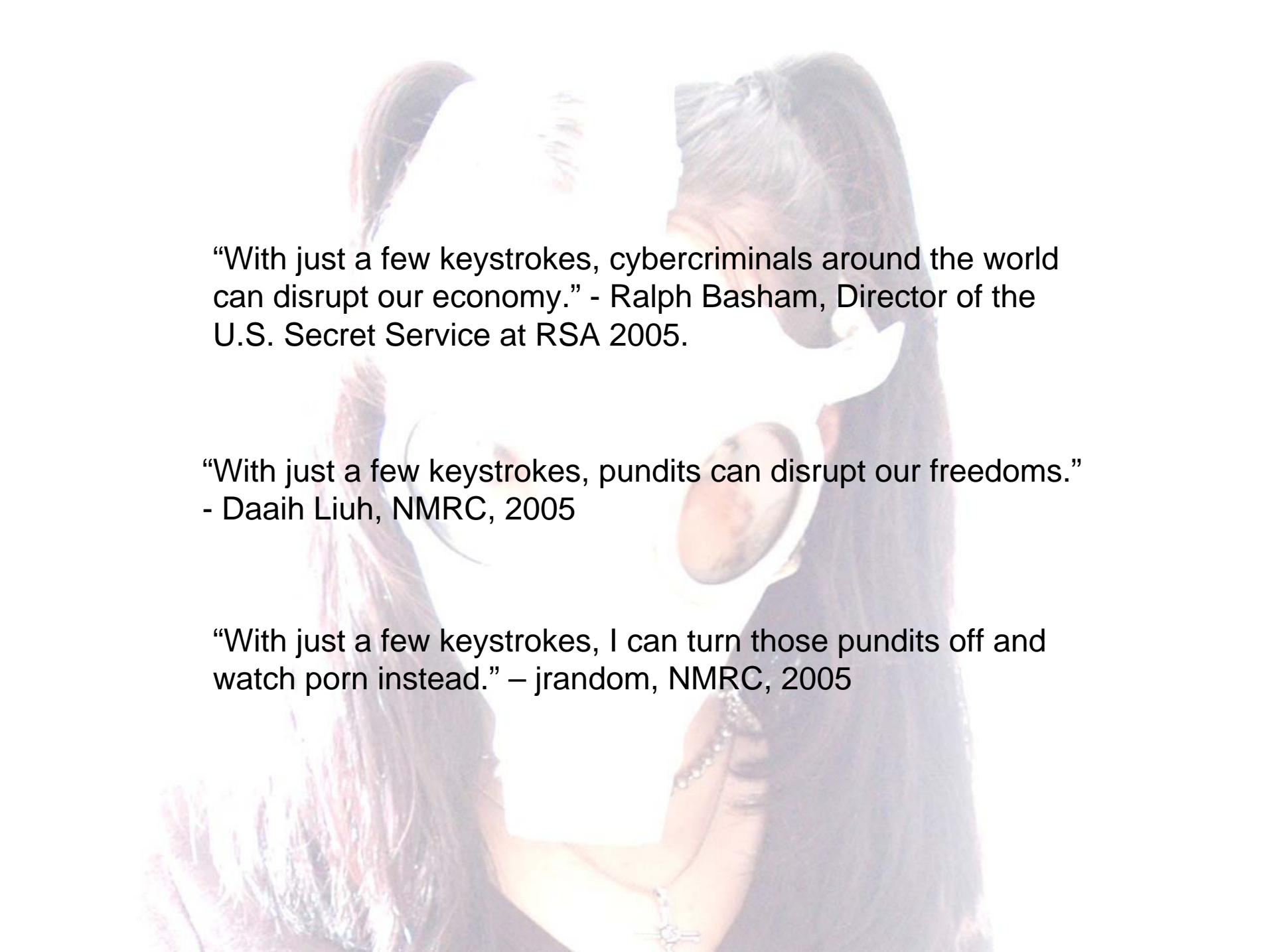
/* named constants */
static const unsigned RT1[256] = {
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
0x01000000, 0x00000000, 0x00000000, 0x00000000,
}

```

The NMRC Warez 2005 Extravaganza

DefCon 2005
nomad mobile research centre





“With just a few keystrokes, cybercriminals around the world can disrupt our economy.” - Ralph Basham, Director of the U.S. Secret Service at RSA 2005.

“With just a few keystrokes, pundits can disrupt our freedoms.”
- Daaih Liuh, NMRC, 2005

“With just a few keystrokes, I can turn those pundits off and watch porn instead.” – jrandom, NMRC, 2005

Who We Are



```
/* reverse tables */
#define RT1
V151.F4.A7.50) V17E.41.65.53) V17A.17.A4.C0) V18A.
V18B.AB.0B.CE) V11F.9D.45.F1) V1AC.FA.5A.A6) V1B0.
V1D.0.3D.FA.55) V1AD.76.6D.F0) V1B8.CC.76.91) V1C0.
V1F.E5.D7.FC) V1CS.2ACB.D7) V1Q.6.35.94.80) V1R0.
V1DE.B1.5A.49) V1D5.BA.1B.67) V1F5.EA.0E.98) V1G0.
V1K3.2F.75.02) V1R1.4C.F0.12) V1B2.46.97.A3) V1B3.
V1Q3.8F.5F.E7) V1S.92.9C.95) V1BF.6D.7A.B3) V1C1.
V1D1.BE.83.2D) V1S8.74.31.D3) V199.E0.69.20) V1A0.
V175.C2.89.6A) V1F4.8E.79.78) V1W.58.3E.6B) V1X0.
V1EB.E1.4F.66) V1P0.8A.AD.17) V1CS.20.AC.06) V1D0.
V1S3.DF.43.19) V1E5.1A.91.82) V1B5.51.2A.60) V1C2.
V1B1.64.77.E0) V1B1.6B.AE.84) V1E4.42.A0.82) V1F5.
V170.48.68.58) V1BF.45.FD.19) V1B4.0E.6C.7A) V1C3.
V1AB.73.DX.23) V1Z.4B.02.E2) V1E3.1F.8F.57) V1F0.
V1E1.EB.28.07) V1D1.B5.C2.03) V1B6.C1.7E.92) V1C4.
V130.24.87.F2) V1D3.FF.A5.B2) V1O2.0.6A.0A) V1A1.
V18A.CE.1C.2B) V1A7.79.B4.92) V1E1.07.72.F9) V1C5.
V165.DA.F4.CD) V1O6.05.BE.D5) V1D1.38.62.18) V1C6.
V134.3E.53.9D) V1A2.F3.55.A0) V1E3.8A.E1.20) V1C7.
V1B8.83.EC.39) V14B.60.EF.AA) V13E.71.91.06) V1C8.
V1B6.21.8A.F9) V1P6.DD.06.8D) V1DD.18.05.AE) V1C9.
V191.54.1D.E5) V1F1.C4.5D.03) V1A8.06.04.82) V1D1.
V112.9B.FD.24) V1D6.BDE.97.97) V1B5.40.83.2E) V1C0.
V1B0.E8.42.BD) V1Q7.82.8B.80) V1E7.19.4E.49) V1C1.
V1A1.7C.04.47) V17C.42.0F.E9) V1E8.24.1E.C0) V1C2.
V1O9.80.86.83) V132.2B.ED.48) V11E.11.70.42) V1C3.
V1FD.0E.FF.F0) V1Q7.85.3E.56) V1D1.AE.05.1B) V1C4.
V1D4.0F.D9.64) V168.5C.A6.21) V1D5.5H.4A.01) V1C5.
V1O0.0A.67.B1) V1Q3.57.E7.0F) V1B4.EE.96.00) V1C6.
V1R0.C0.C5.4F) V1G1.DC.0.A2) V1SA.F7.40.9E) V1C7.
V1E2.93.BA.0A) V1C0.A0.2A.E5) V13C.51.E0.43) V1C8.
V1OE.09.0D.0E) V1F2.8B.C7.AD) V1ZD.D6.4E.8A) V1C9.
V1G7.F1.19.85) V1AF.75.07.4C) V1E2.99.DD.0E) V1CA.
V1F7.01.26.8F) V1CC.22.FD.C3) V144.66.90.C5) V1CB.
V1B8.43.29.76) V1CB.23.C6.4C) V1B9.ED.F0.0A) V1CC.
V1D7.31.DC.CA) V1B2.63.85.10) V1D3.87.54.99) V1CD.
V185.4A.24.7D) V1Z2.BB.3E.F4) V1AE.F9.8E.1D) V1CE.
V1D.9E.2F.4B) V1DC.B2.3D.F4) V1RD.86.52.CE) V1CF.
V1D2.E3.16.6C) V1A9.7D.B9.94) V1E7.8E.9E.97) V1CG.
V1A8.FC.8C.C4) V1A0.F0.3F.1E) V18C.C4.8E.8E) V1CH.
V1B7.49.4E.C7) V1D9.38.D1.C1) V18C.C4.8E.8E) V1CI.
V1A6.F5.81.CF) V1AS.7A1E.37) V144.70.8E.8E) V1CJ.
V1C2.3A.9D.E9) V1S0.78.97.0E) V18A.53.9E.9E) V1CK.
V1F6.8D.1A.C9) V1P0.D4.B9.E4) V18B.70.80.7D) V1CL.
V1F9.5D.80.EB) V1B9.20.80.7D) V18B.70.80.7D) V1CM.
V1C3.AC.89.3D) V110.18.D0.A7) V18A.53.9E.9E) V1CN.
V1CD.26.78.09) V1E6.59.18.F9) V1E3.8A.D0.8E) V1CO.
V1E6.95.8E.65) V1AA.F1.E6.7E) V11A8.CF.8E.8E) V1CP.
V1BA.E7.9E.D9) V1A4.07.3E.CB) V1E3.8A.D0.8E) V1CQ.
V131.A9.E2.A7) V1D4.1E.33.31) V1C4.A1.9E.8E) V1CR.
V174.4E.BC.3D) V1FC.81.CA.A0) V1B0.90.8E.8E) V1CS.
V1F1.04.98.4A) V141.EC.DA.FD) V11F.CD.8E.8E) V1CT.
V176.4D.D6.8D) V143.EF.B0.4D) V1C0.AA.9E.8E) V1CU.
V19E.D1.B5.E3) V1FC.6A.84.16) V1C1.NE.1F.8E) V1CV.
V1B0.SE.EA.04) V1D1.8C.85.5D) V1A4.8E.8E.8E) V1CW.
V1B3.67.1D.5A) V1D2.DE.D0.5A) V1E9.10.6E.8E) V1CX.
V19A.D7.61.8A) V1Z7.81.8C.7A) V1S0.8E.8E.8E) V1CY.
V1C3.A9.77.EB) V1B7.61.C9.5A) V181.D7.8E.8E) V1CZ.
V19C.DD.DF.59) V1S5.F7.7A.91) V1A1.1A.8E.8E) V1D0.
V1B3.F7.CD.EA) V1SF.FD.A1.5B) V1D1.8E.8E.8E) V1D1.
V1CA.A7.F7.81) V1B9.68.C4.8E) V138.79.8E.8E) V1D2.
V16.1D.C3.72) V1E0.E2.25.C2) V1E2.AE.8E.8E) V1D3.
V139.A8.01.71) V1O8.0C.B3.DE) V1D8.20.8E.8E) V1D4.
V17B.CB.84.64) V1D5.32.E6.70) V1A8.0E.8E.8E) V1D5.
```

On To The Warez....



Updated Ncrypt

- New features and bug fixes
 - Includes Todd MacDermind's nrm, a drop-in replacement for rm for secure file erasure
 - More features for script integration (the users demanded it!)

Stronghold

- For Windows 2000, XP, 2003
- Locks down the box
 - Implements the NIST standards for securing Windows
- Rollback feature
- GPL, and it's freeware, feel the love

Stronghold Analyzer

- For Windows 2000, XP, 2003
- Like Stronghold, it uses NIST standards for securing Windows
- Shows security holes that exist in Windows that Stronghold will secure
- GPL, and it's freeware, feel even more love

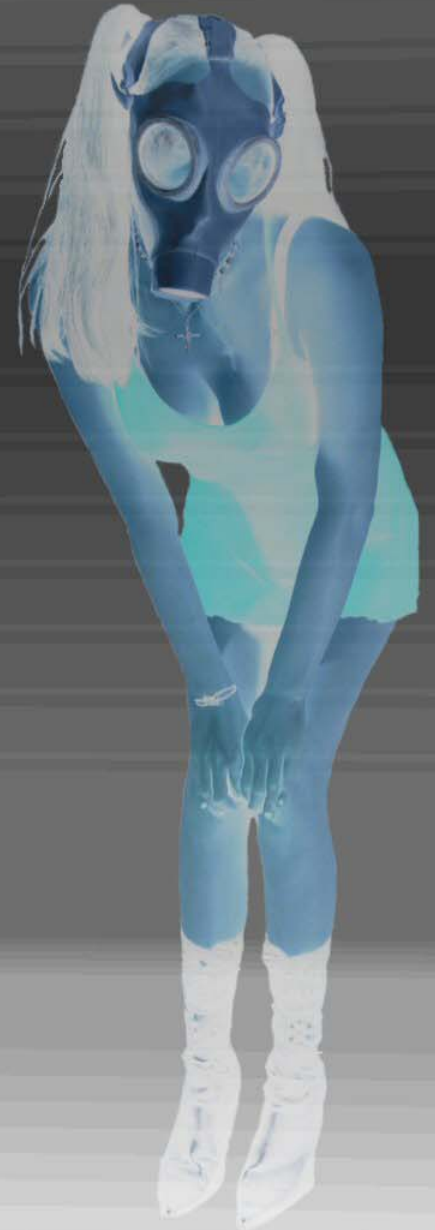
Stronghold / Stronghold Analyzer Demo



SPA

- SPA is Single Packet Authentication, a single packet that can authenticate a user to a system
- It is a protocol for allowing a remote user to authenticate securely on a “closed” system (limited or no open services)
- Uses GPG to sign/encrypt a message to a sniffing server in a single TCP, UDP, or ICMP packet
- Work across NAT
- Free

SPA Demo



NPC

- NPC is Nearly Perfect Crypto. Seriously....
- It includes a utility for creating large one time pads (using the PRNG ISAAC)
- Fast, simple and quick
- If you can manage the key exchange, it is nearly the most perfect and unbreakable crypto you can get (one time pads are considered the ultimate crypto)
 - Key management is a bitch, and may render this impractical for modern humans

NPC Demo



Q & A

- We will spank audience members during the Q & A
- You must sign our Ass Release Form before you can be spanked
- You may choose any NMRC member to spank you
- If you do not choose a particular NMRC hacker to spank you, the NMRC hacker answering the question will spank you while giving the answer





FIN, Biatchez

Images © 2005 NMRC
www.nmrc.org