

---

# A cheap and quick way to harden your passwords

By Marc DeBonis

Systems Architect - IS&C/VTMIG

020711

Presented for the members of the VTntug

<http://vtntug.w2k.vt.edu>

---

# Problem with passwords

## ◆ Length matters!

- ✍ The longer the string
  - ✍ Harder to crack
  - ✍ More difficult to remember
    - ✍ Tendency to store somewhere (sticker note, etc)

## ◆ Complexity matters!

- ✍ Ideally we want random alphanumeric
  - ✍ Extremely difficult to remember

# A device called a CueCat

- ◆ Was an attempt to provide a barcode scanner with a unique serial id
- ◆ Company partnered with Radio Shack to include bar codes for each item in the catalog
- ◆ Installed software and hardware device to provide a passthru to keyboard input
- ◆ Software would do a lookup (while recording your transaction) and provide you with a website giving you more information
- ◆ Devices were given out FREE! FREE! FREE!

# How it works

- ◆ Hook up the cuecat between your computer's keyboard ps2 connection and the keyboard
- ◆ Open notepad and scan in a barcode
- ◆ Using my Kroger Card I get a output of
  - ✍ .C2nZC2nZC2nXD2z1C2DWCNnY.fHlc.D3f5Cxz7C4vZE4D7.
  - ✍ This output is uniquely tied to my Kroger card AND to the specific cuecat device
  - ✍ Result is 48 characters long and quite complex

# Making it more complex

- ◆ I would suggest adding a character or two at the beginning of the string
  - ✍ Password now has two “hard” unique components (the barcode and the specific cuecat device)
  - ✍ And a “soft” component, something only you know (the extra characters)
- ◆ Put in two or three barcodes for huge passwords!

# Downsides

- ❖ Using this “ties” you to a location unless you want to cart around the cuecat device. Keyboards don’t like to be constantly unplugged.
- ❖ Losing any piece of the “equation” and you lose the ability to recreate the password string.
- ❖ String generated from the cuecat is a subset of all valid alphanumerics, smaller keyset to attack
- ❖ Still attackable via keystroke recording
- ❖ Using “down level clients” greatly weakens the password string. 9x lowercases and records only first 7 characters which is saved in LM hash


# Other ideas

- ◆ Build a 3x3x3 matrix of barcodes and laminate them in a wallet sized card. Label each barcode with some sort of meme for easy remembrance
- ◆ Build some sort of ps2 switch to allow easy removal of the “collared” cuecat.
- ◆ Any value in un-serializing the cuecat?
  - ✍ Already broke one of them doing this. Doh...

# Links

- ◆ <http://airsoldier.com/~cueecat/>
- ◆ <http://www.beau.lib.la.us/~jmorris/linux/cueecat/>
- ◆ <http://blort.org/cueecat/>
- ◆ <http://osiris.978.org/~brianr/cueecat/>
- ◆ <http://cueecatastrophe.com/>
- ◆ <http://www.ebay.com>

✍ Get them cheap!



---

# A cheap and quick way to harden your passwords

By Marc DeBonis

Systems Architect - IS&C/VTMIG

020711

Presented for the members of the VTntug

<http://vtntug.w2k.vt.edu>

---