THE UNIVERSITY OF BRITISH COLUMBIA

Usability of Security Administration vs. Usability of End-user Security

Panelists:

Mary Ellen Zurko, IBM

Steve Chan, UC Berkley & LBL

Greg Conti, United States Military Academy

Moderator:

Konstantin (Kosta) Beznosov, UBC

same or different?

- Is the notion of usable security for end-users and security administrators the same?
- What are, if any, the differences/similarities in the
  - background
  - training
  - goals
  - constraints
  - tools

  between admins and end-users?
- How do these differences/similarities affect the (perception of) usability of the protection mechanisms and other security tools?

reusing results

- Can the approaches to improving the security usability for end-users be directly applied to security administration?
- To what degree?
- What about vice versa, i.e., admin --> end-user?

where is the borderline?

- With some of the modern-day systems, where users are largely responsible for their own security self-administration, where is the borderline between the end-users and administrators?
- Can it be defined precisely or is it blurred?
  - If the changes you make to the system affect somebody else's security …

to summarize the topics

- same or different?
- reusing results?
- where’s the borderline?

THE UNIVERSITY OF BRITISH COLUMBIA

And now for something completely different …

Mary Ellen Zurko

- leads security architecture and strategy for Workplace, Portal and Collaboration Software at IBM
- introduced User-Centered Security in 1996
- on the steering committee for NSPW, ACSAC, and the International WWW Conference series
- has worked in security since 1986, at The Open Group Research Institute and DEC, as well as IBM

IBM Software Group

Usability of Security: Administrators and Users (and Developers)

Mary Ellen Zurko
IBM Software Group

Lotus software

e business on demand software

Usability Techniques for Administration of Security

- Usability techniques applied to security administrators in research
  - Zurko, Simon, Sanfilippo, IEEE S&P 99
  - Contextual interview
  - Lab study setting authorization policy
- Concentrated on making their (security administration) job easier
- Viewed as a distinct population

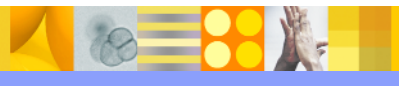
- Other examples in industry
- ACL usability testing in Zurko chapter of Security and Usability book
  - Viewed more as power users within a particular community

How can usability enhance security for administrators and their users?

- "You'll have to do the thinking for both of us, for all of us"
  - Developers, Administrators, and Users
  - If there is no administrator, the developer must substitute

Make the tough choices

- And allow for override down the line
  - Developer to Administrator to User
  - Large granularity and fine granularity
- Earlier in the lifecycle takes more responsibility
  - The later in the lifecycle, the smaller the part of their job is actually to deal with security
  - Not that any of them want to deal with it (unless they're security specialists or evaluators)
- One technique – Policy and Preferences
  - Policies set security relevant defaults for administrative domain
    - Specify whether override is allowed
  - Preferences set user level overrides
  - Developers set policy defaults and provides templates and wizards



And now for something completely different …

Lotus software

Steve Chan

- Lawrence Berkeley National Laboratory and School of Information Management and Systems at UC Berkeley
- master's student in the SIMS program at UC Berkeley
- professional Unix Sys Admin for over a decade
- in LBNL Networking and Security team

School of Information Management & Systems
UNIVERSITY OF CALIFORNIA, BERKELEY

Usable Security for Security Administrators

Presented by
Steve Chan
SIMS, UC Berkeley and Lawrence Berkeley Lab
sychan@sims.berkeley.edu
sychan@lbl.gov

Background

- Most of the examples will be drawn from experience at LBL
  - Lead Admin of PDSF Cluster http://www.nersc.gov/nusers/resources/PDSF/
  - Deploying Production Grid Services at NERSC http://www.nersc.gov/news/nerscnews/NERSCNews_2004_02.pdf
  - Initial personal research into usability and Security Administration tools
- Emphasis on Operational Security from the viewpoint of professional Sys Admins
- Giving away the ending:
  - Usability must be tied to work practices and the work practices of end users are very different from those of security administrators

Security
Personal vs. Collective (local vs. distributed)

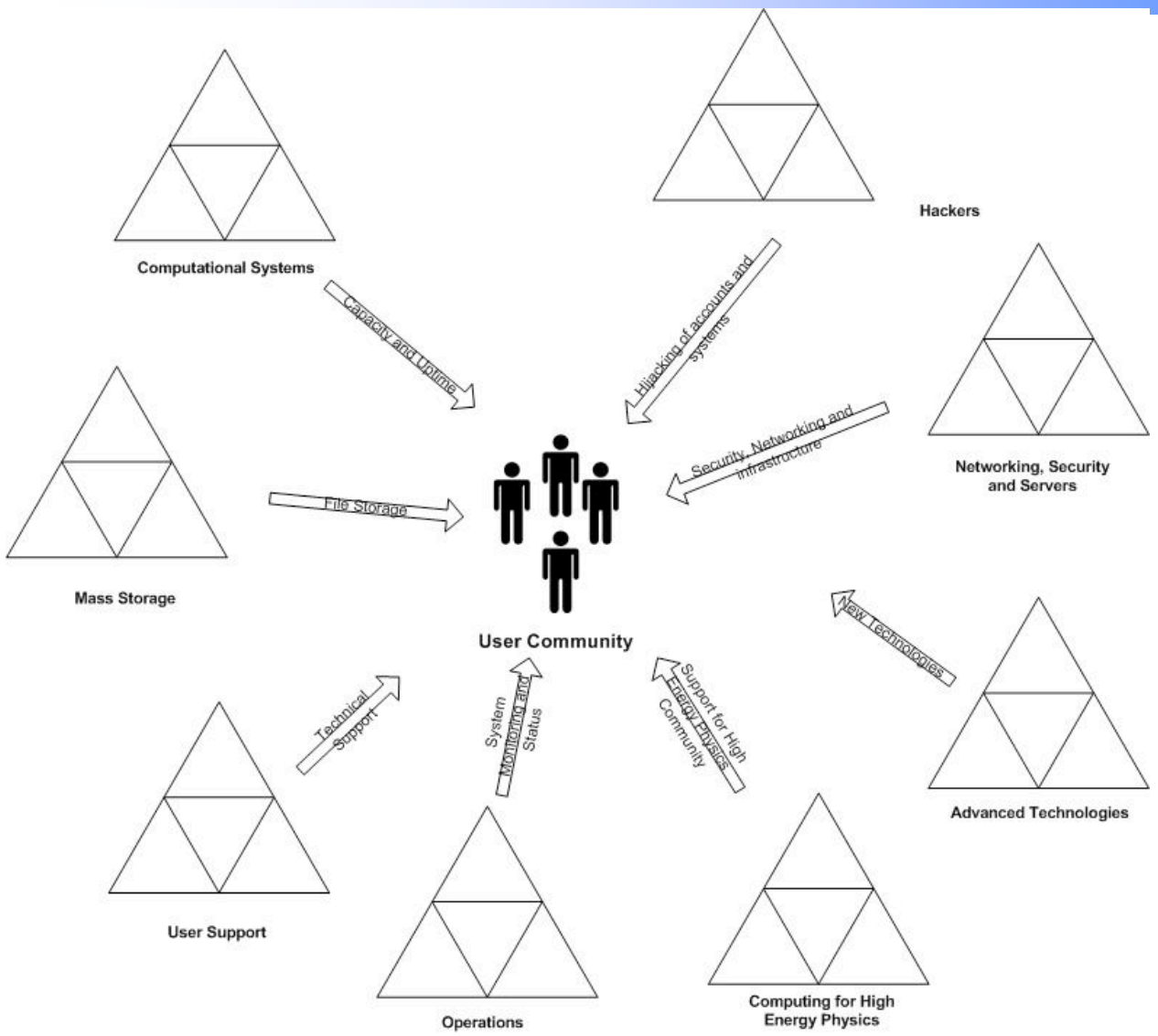
- End Users generally responsible for local security (if that)
- Security Administrators responsible for collective security of distributed systems
  - A single system being compromised may be wedge that opens up multiple systems and sites to compromise
- Different levels of Accountability and Responsibility
  - Security Administrators are explicitly accountable to management, user community, government and many others
  - Security Administrators are highly dependent on cooperation of other groups in IT

Security for Administrators

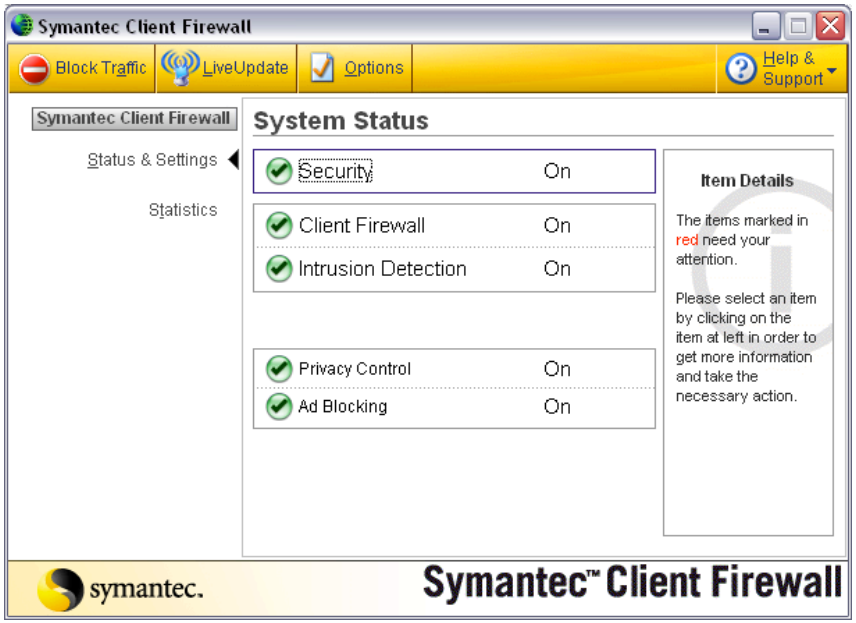
School of Information Management & Systems
UNIVERSITY OF CALIFORNIA, BERKELEY

- Consequences:
  - Negotiation with peer groups and users
  - Centralized policies enforceable across distributed systems
- Security is distributed
  - from border router to internal switches to the files on your disk: defense in depth
- Security is collective
  - Security administration explicitly depends on collaboration with peers at a very technical level, with distributed authority and mutual accountability

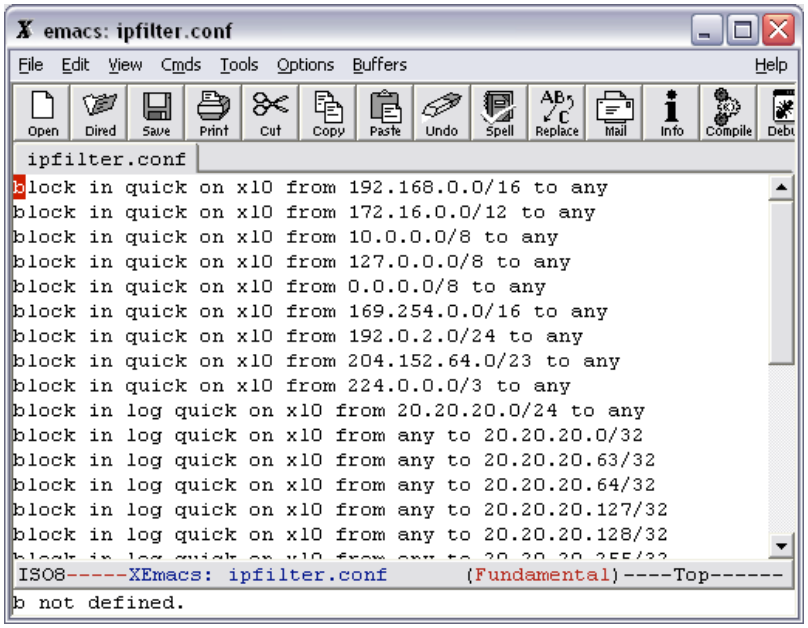
Activity Theoretic Diagram



Security Work Practices



VS.



Different work practices

- Difference in tools reflect different work practices
- Scalability and Flexibility
  - GUIs often don't scale
    - large numbers of machines and applications
    - large quantities of data
  - GUI abstractions often don't match actual work practices
    - Security Administration is a craft, not a science – work practices of any individual security administrator is dependent on their background (network admin, sys admin, developer)
  - Much of operational security work is making routine what was once dynamic
    - Security is an arms race and threats are constantly evolving
    - Constantly evolving threats means constantly evolving detection and countermeasure automation

Summary

- **Usability of tools for Systems Administration is tied to work practices**
  - **At a macro level, Security Administration is collaborative and tools and procedures span multiple groups**
  - **At a micro level, Security Administration tools need the flexibility and scalability that are often abstracted away in GUI tools**
- **Different work practices drive different usability requirements**

And now for something completely different …

Greg Conti

- Assist. Prof. of CS, US Military Academy
- research interests:
  - network security data visualization
  - denial of information attacks
  - secure and usable interface design
  - information warfare
- has worked at a variety of military intelligence assignments specializing in Signals Intelligence
- currently on a DoD Fellowship at Georgia Tech.

Usability of Security Administration vs. Usability of End-user Security: A Clash of Cultures

Gregory Conti
Georgia Tech
conti@acm.org

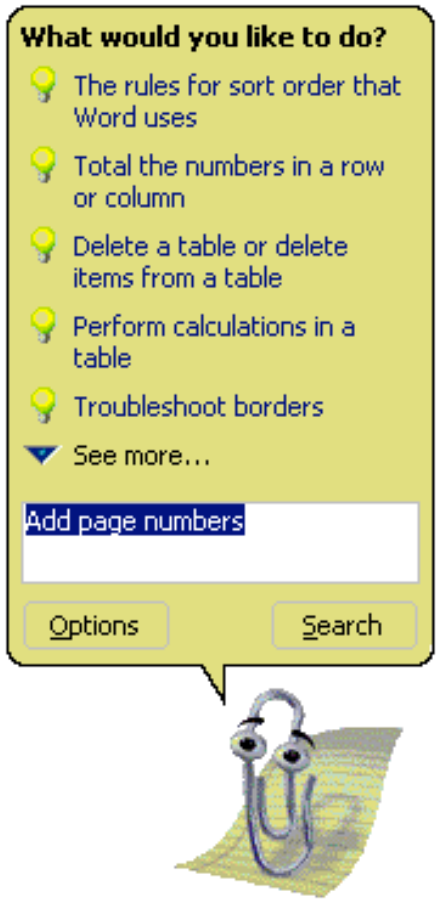
http://daddytypes.com/archive/rtfm_onesie.jpg

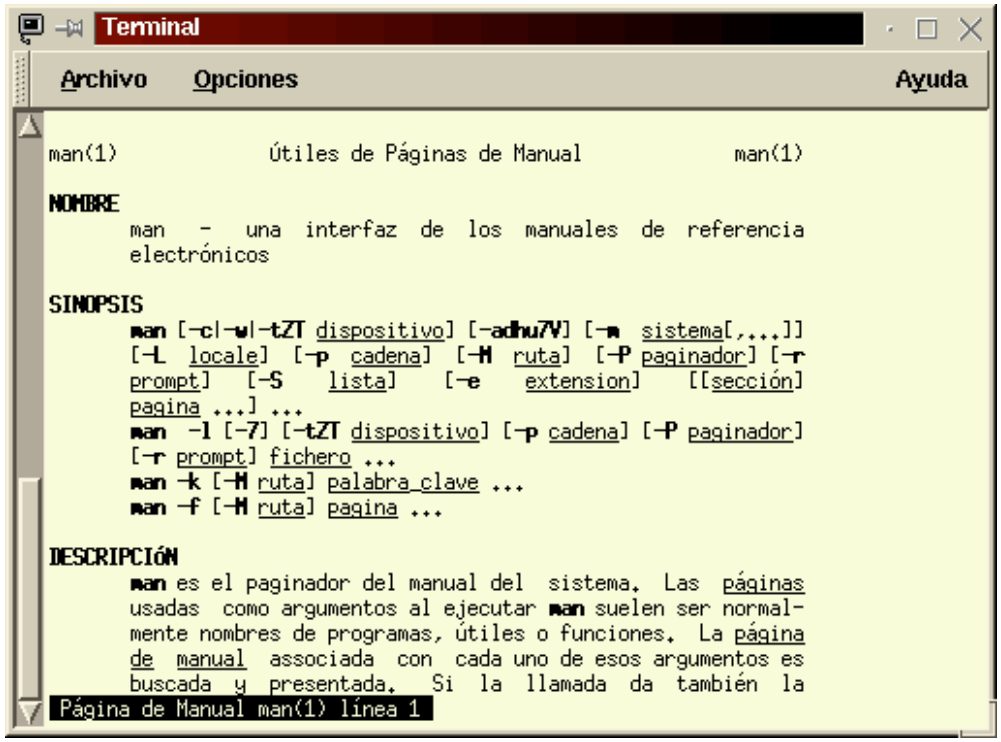
newbie: /n[y]oo´bee/, n.

[very common; orig. from British public-school and military slang variant of ‘new boy’] A Usenet neophyte. This term surfaced in the newsgroup talk.bizarre but is now in wide use (the combination “clueless newbie” is especially common). Criteria for being considered a newbie vary wildly; a person can be called a newbie in one newsgroup while remaining a respected regular in another. The label newbie is sometimes applied as a serious insult to a person who has been around Usenet for a long time but who carefully hides all evidence of having a clue. See B1FF; see also gnubie. Compare chainik, luser.

http://www.catb.org/~esr/jargon/html/frames.html

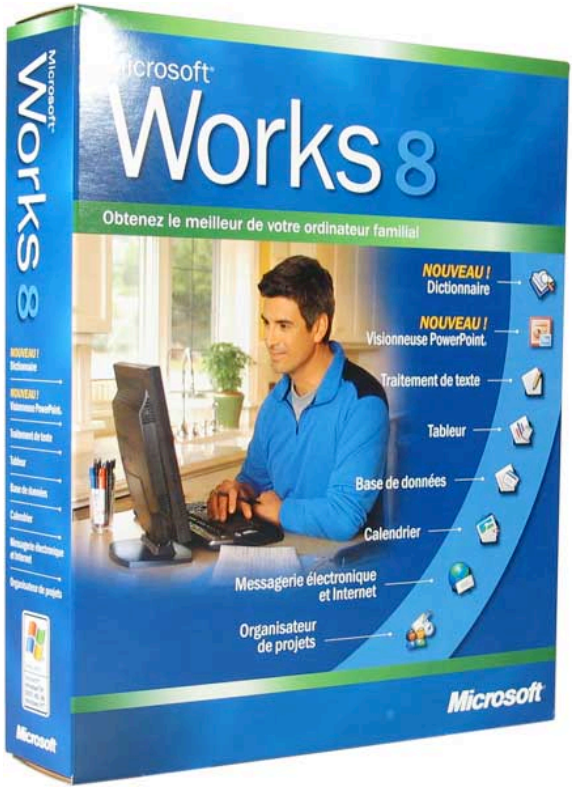
Getting Help…





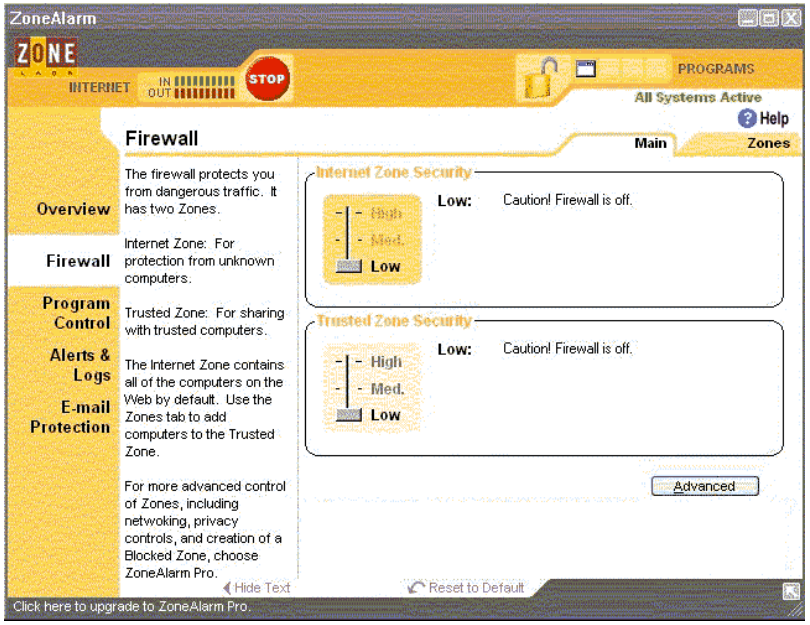
http://www.linuxfocus.org/common/images/man.gif
http://www.microsoft.com/technet/images/prodtechnol/office/office2000/maintain/operate/images/runo2k08.gif

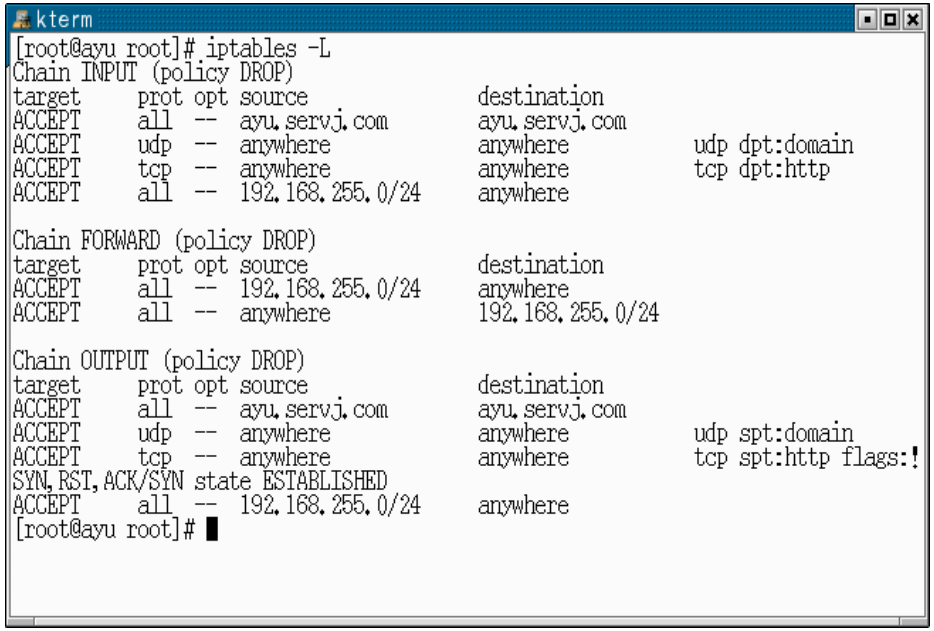
Editing Documents…



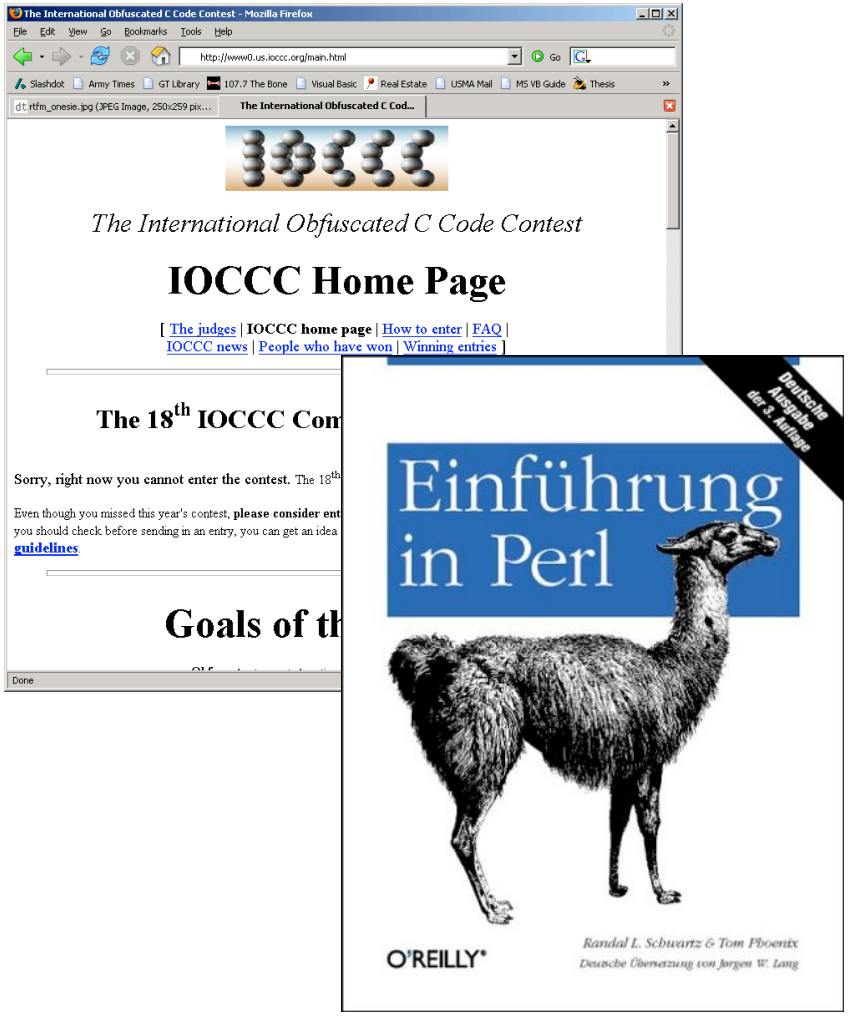

```
Require password to log in to your computer.

Use a screensaver or screenlock that requires a password to access the
computer's desktop.

Use the UNM Portal for file sharing. Avoid Windows file sharing.

Encrypt sensitive files.

Assure privacy of personal information. DO NOT store sensitive personal
information on your UNM computer.


~
~
~
~
~
~
~
~
~
~
"examples.list" 13L, 340C                                    3,9           All
```

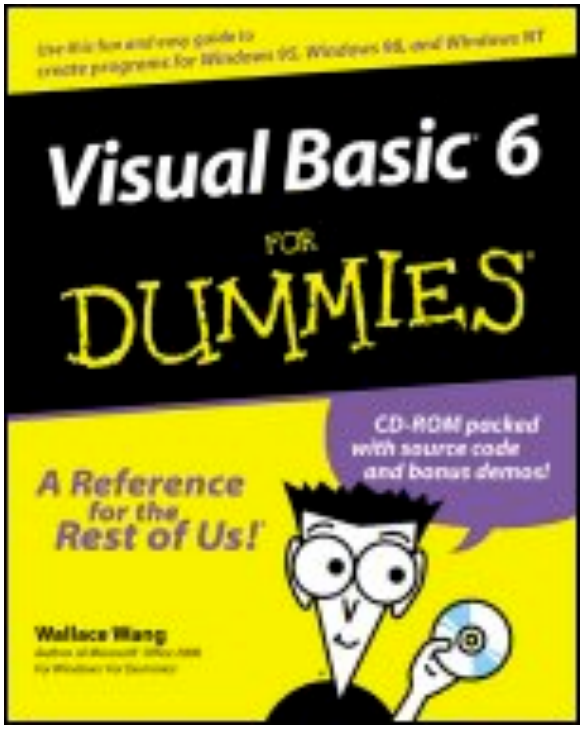
Protecting Their Computer…





Within the Computing Community…





http://www.ioccc.org/

http://www.nnbh.com/base/07/images/0764503707.jpg

http://images-eu.amazon.com/images/P/3897211475.03.LZZZZZZZ.jpg

Great Flame Classics…

- The Spelling flame
- The Bandwidth flame
- The Untrimmed-Quoted-Text flame
- The Clueless-Newbie flame
- The Read-the-Manual flame
- The You?!?-a-Worthwhile-Idea??? flame
- The You-Like-X?!? flame
- The Get-a-Life flame
- The Starry-eyed-Idealist flame
- The Why-Bother? flame
- The Science-Skeptic flame

http://www.robotwisdom.com/net/flamers.html

Crack in One Line of Perl

```
perl -nle 'setpwent;crypt($_,$c)eq$c&&print"$u $_"while($u,$c)=getpwent'
```


Author: Alec Muffett

Several Lines of Perl Can Crack DVD Encryption

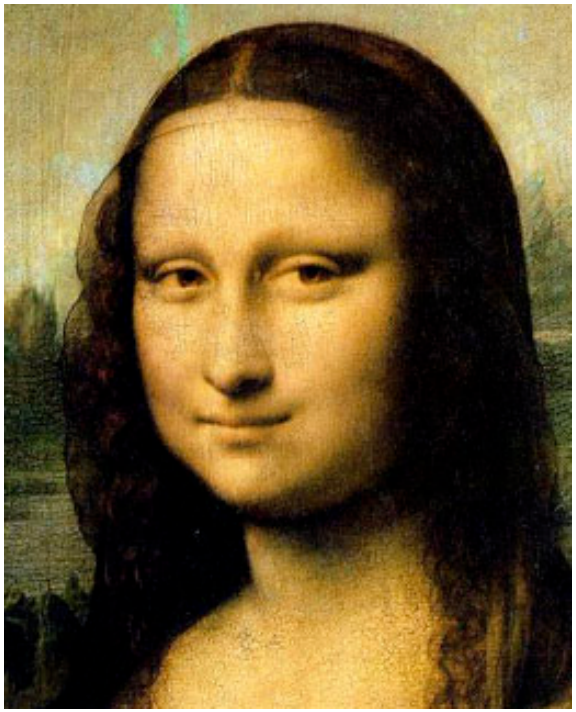
```
#!/usr/bin/perl
# 472-byte qrpff, Keith Winstein and Marc Horowitz <sipb-iap-dvd@mit.edu>
# MPEG 2 PS VOB file -> descrambled output on stdout.
# usage: perl -I <k1>:<k2>:<k3>:<k4>:<k5> qrpff
# where k1..k5 are the title key bytes in least to most-significant order

s''$/=\2048;while(<>){G=29;R=142;if((@a=unqT="C*",_)[20]&48){D=89;_=unqb24,qT,@
b=map{ord qB8,unqb8,qT,_^$a[--D]}@INC;s/...$/1$&/;Q=unqV,qb25,_;H=73;O=$b[4]<<9
|256|$b[3];Q=Q>>8^(P=(E=255)&(Q>>12^Q>>4^Q/8^Q))<<17,O=O>>8^(E&(F=(S=O>>14&7^O)
^S*8^S<<6))<<9,_=(map{U=_%16orE^=R^=110&(S=(unqT,"\xb\ntd\xbz\x14d")[_/16%8]);E
^=(72,@z=(64,72,G^=12*(U-2?0:S&17)),H^=_%64?12:0,@z)[_%8]}(16..271))[_]^((D>>=8
)+=P+(~F&E))for@a[128..$#a]}print+qT,@a}';
```

Authors: Keith Winstein and Marc Horowitz

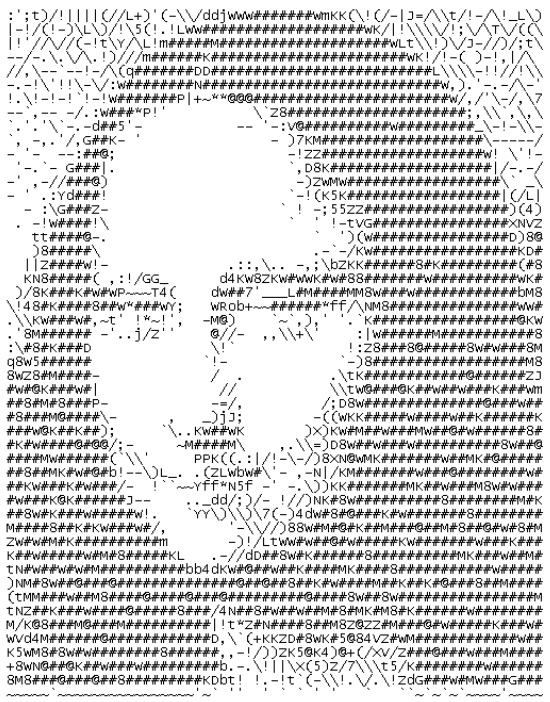
Original source: http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/qrpff.pl

*Note that code above is not complete

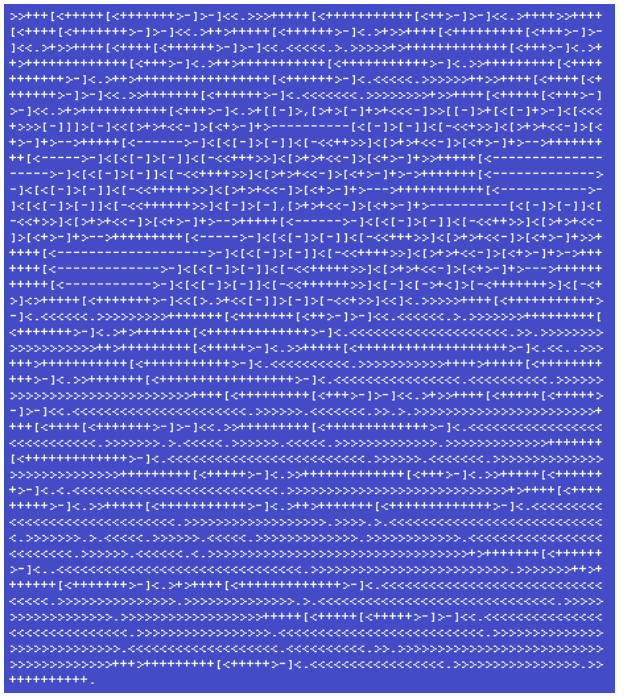
An Art Survey…



A

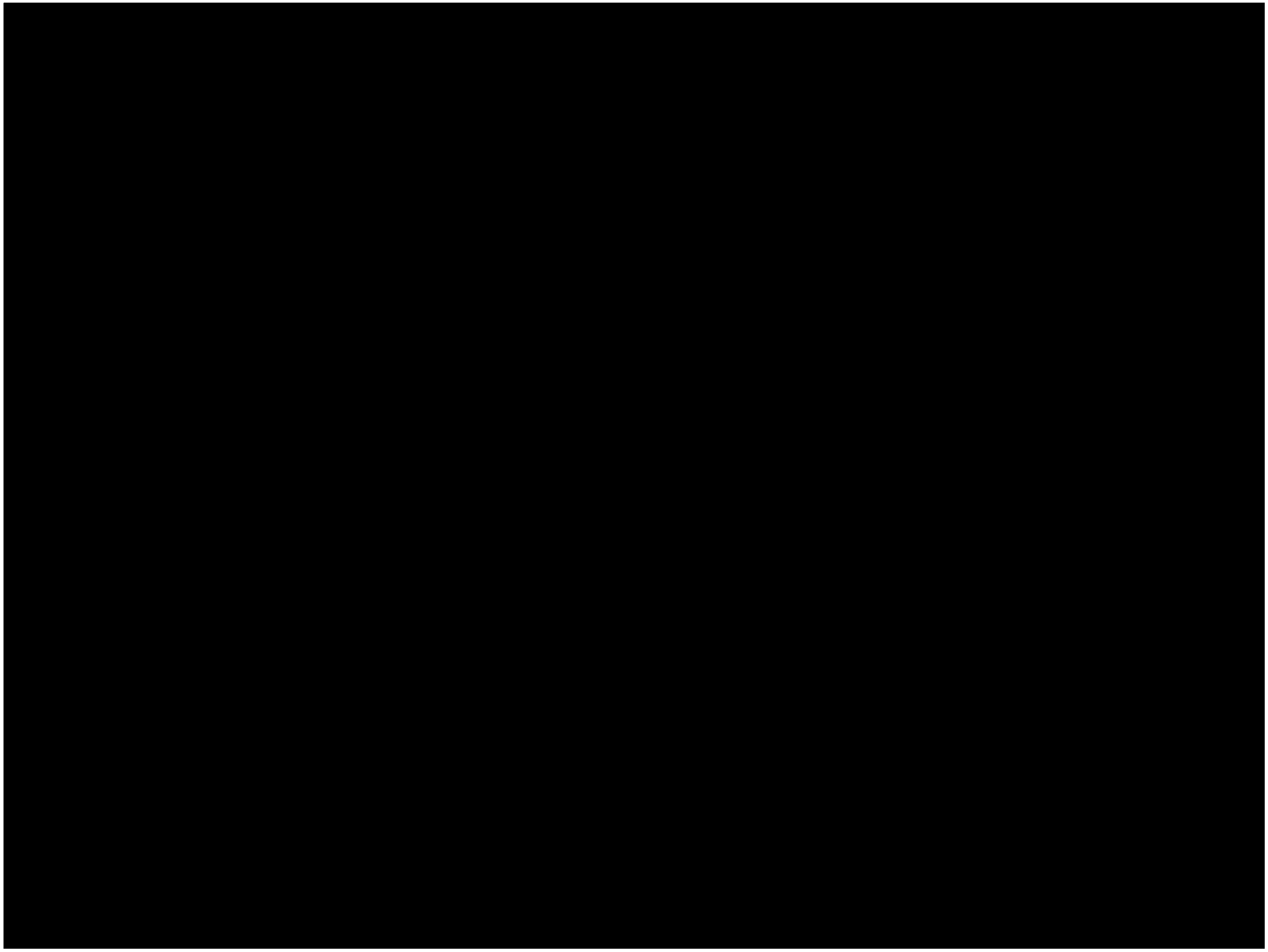


B



C

http://www.clifford.at/cfun/progex/
http://www.muppetlabs.com/~breadbox/bf/
http://www.geocities.com/h2lee/ascii/monalisa.html
http://www.artinvest2000.com/leonardo_gioconda.htm



And now for something completely different …

Q&A