Active Content:

Really Neat Technology
or
Impending Disaster?

Charlie Kaufman
Iris Associates
charlie_kaufman@iris.com

I come bearing bad news...

- The world’s computing and communications infrastructure is a security disaster waiting to happen
- It’s getting worse every year
- The mystery is why it has worked for as long as it has

How Bad Is It?

- Most computers are connected (directly or indirectly) to the Internet
- Most computers have easily exploitable security flaws - many are widely known
- The world has come to rely on cheap reliable connectivity

On the Plus Side...

- 90’s were the decade of the Internet
- Global connectivity available to the masses
- Easy to use and configure
- It looks great! - Animated graphics and rich text everywhere
- Transformed how we work and how we play

What’s Active Content?

- Downloading or receiving as email procedural data instead of interpreted data
  - I send you a program and you run it to get my message
  - The running program may be able to do other things with your rights
- One of many security problems, but the hardest to fix

Examples:

- Java, Javascript, ActiveX on web pages
- HTML based email containing same
- Binary Executables, Shell scripts, advanced data formats downloadable or sent as attachments

Inherently Limited Protection

- Virus Scanners
- Firewalls
- Telling users to avoid active content
- Having the FBI track down attackers
- Using a different platform from most other users

Warning Message:

From: <someone you never heard of>
Subject: Virus Safety in the New Millenium
To: <large distribution list>

<<<motivational threatening language removed>>>

Follow these simple precautions to minimize your chances of falling victim to these malicious programs.

1. Never click, open, save, or run executable email attachments. Ever. (Even if your Mom sent it to you.)

If this sounds stringent, it is. Modern computer viruses infest email address books and email themselves to everyone on your list. Your Mom's computer could (potentially) be sending a copy of the virus to everyone in her address book -- including you. Be careful - don't take risks.

<<<more good advice removed>>>

Another Message...

From: <someone else you never heard of>
Date: Tue, 3 Apr 2001 17:25:07
To: <big distribution list>
Subject: Food/Vending Services Survey

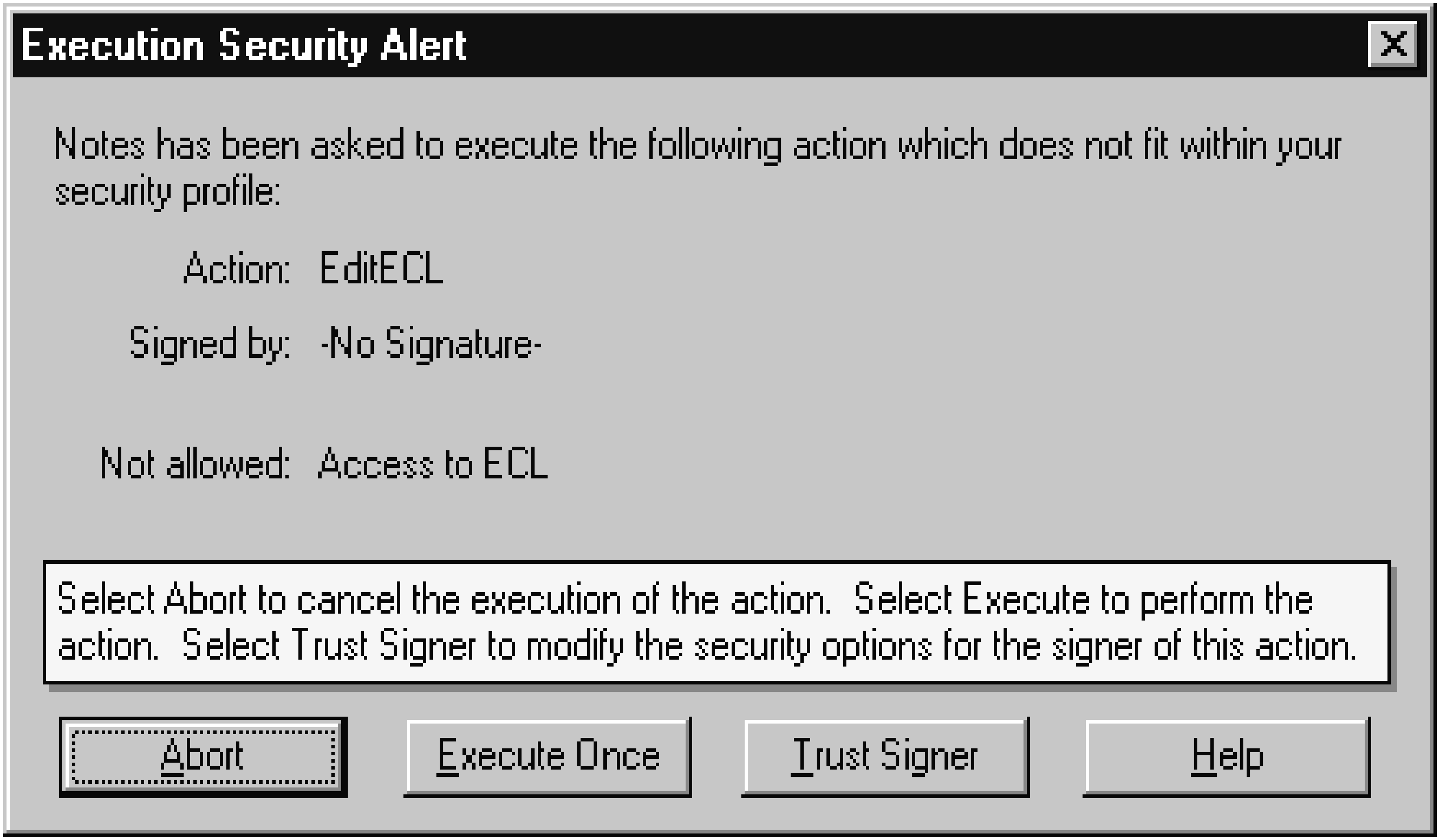
Please take a moment to complete the attached survey.
These surveys are designed to measure your satisfaction
with our site services groups.

To run the survey simply double click on the icon beneath
this message. When the first screens appear simply click
on "ok" until the run window opens and the survey appears.

Thank you for your cooperation and support.

>>>>Attachment is an executeable file<<<<

Warnings...



Execution Security Alert

Notes has been asked to execute the following action which does not fit within your security profile:

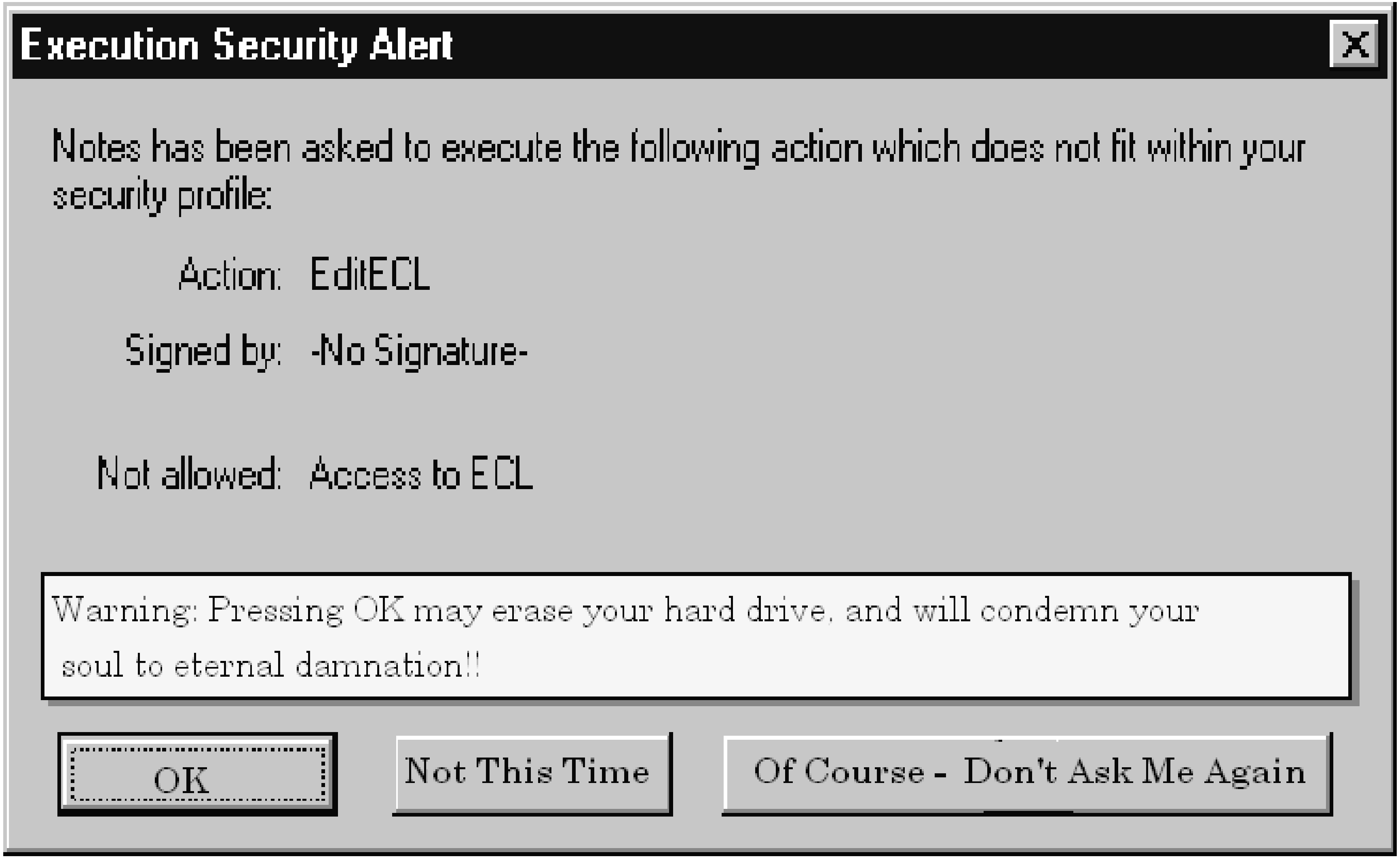
Action: EditECL

Signed by: -No Signature-

Not allowed: Access to ECL

Select Abort to cancel the execution of the action. Select Execute to perform the action. Select Trust Signer to modify the security options for the signer of this action.

Might as well say...



Execution Security Alert

Notes has been asked to execute the following action which does not fit within your security profile:

Action: EditECL

Signed by: -No Signature-

Not allowed: Access to ECL

Warning: Pressing OK may erase your hard drive, and will condemn your soul to eternal damnation!!

Things you can’t do safely...

- Browse a random web site
- Expand an auto-expanding ‘zip’ file
- Display non-text files (.ps, .pdf, .doc, …)
- Read Microsoft’s Kerberos spec
- Find out about the 50ways to use Zip Disks

And if you mess up once...

- Attacker could take control of your workstation
- With keystroke log, get your passwords
- Send email from you; read your email
- Access any files you have rights to access
- Install viruses in any executables you have rights to access

How did we get here?

- Problem was always there
- “Orange Book” tried to address it in the 1970’s
- Micro-Kernel and secure workstation (CMW) projects tried to address it in the 1980’s
- Threat never materialized, and was forgotten
- World conquered by DOS

Meanwhile, the threat grew

- Internet: everybody + anonymity
- Naïve users
- Demise of OS security
  - Resulting in loss of discipline for application developers
  - Applications invade the OS for performance and ease of installation

Three Milestones in the History of Computer Security

- MULTIX
- Unix
- DOS
  - Steve Crocker

Components of a Solution

- **Sandboxes -** running programs without the full run of the machine
- **Digital signatures on code -** know where it’s coming from, and decide rights on that basis
- **Make less use of general purpose procedures when special purpose ones will do**

Sandboxes

- Old idea, new name: run a program with limited privileges
- Timesharing in the 60’s: run a program with the privileges of the user
- Needed now: run a program with even fewer privileges than its invoker
- Java implements the concept within an application

Limitations of Sandboxes

- Bugs allow code to “escape”
- Sometimes a legitimate need for some privileges
  - Saving state
  - Accessing remote resources
- Sharing a sandbox is dangerous
- Users can’t make good decisions about overrides

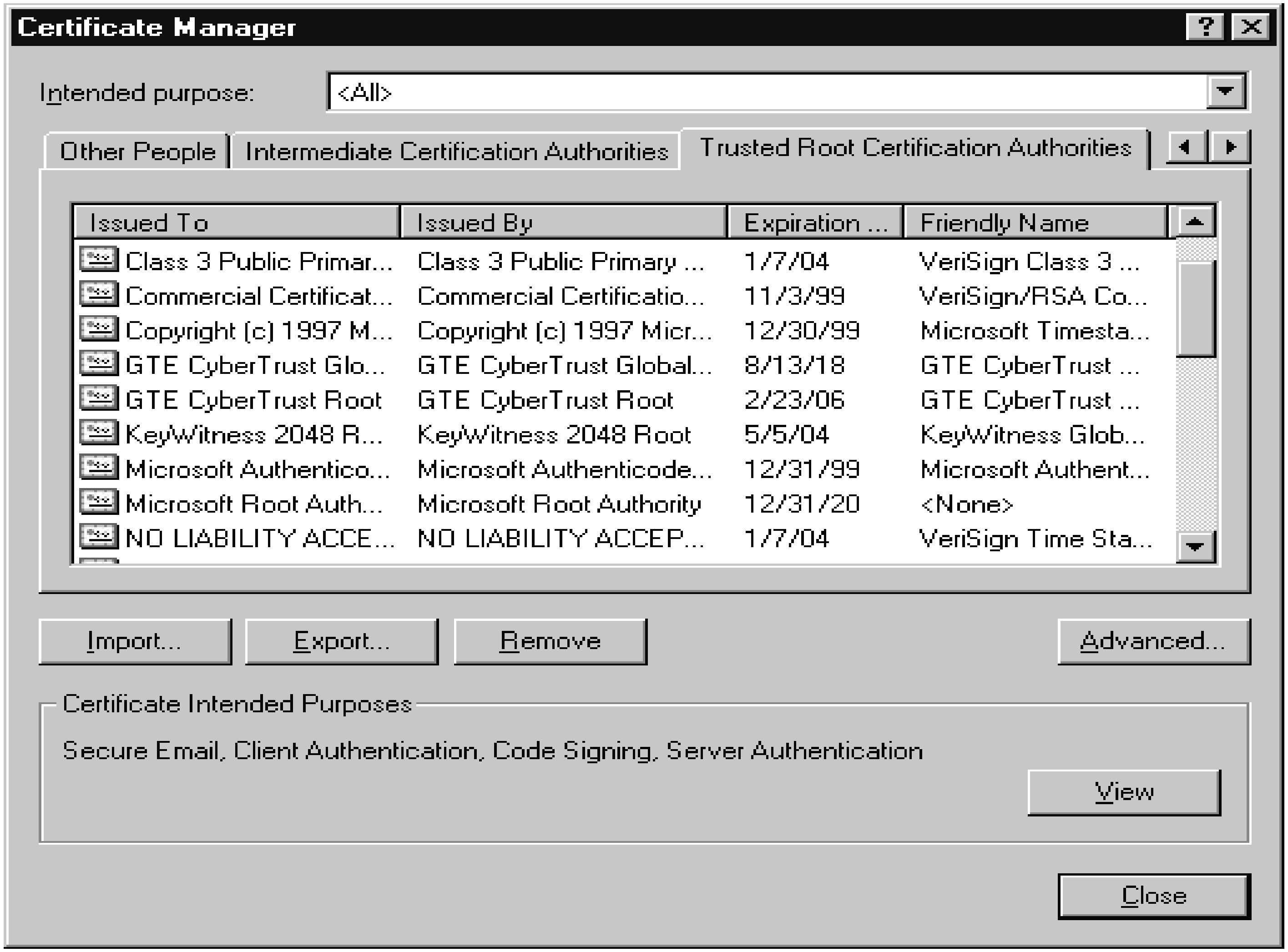
Signed Programs

- Digital Signatures and Public Key Infrastructure allow the signing of executables and reliable identification of sources
- Configuring trusted signers can result in security comparable to a file system

Limitations of Signed Programs

- A lot can go wrong
  - Configuration of trust anchors or trusted signers could be wrong
  - PKI providers can make mistakes
  - Signed programs can have bugs
  - Signed programs can contain viruses
  - Users will want to run programs from other sources

Default Trusted CA's in IE



Certificate Manager
Other People
Intermediate Certification Authorities
Trusted Root Certification Authorities
Import...
Export...
Remove
Advanced...
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiration ...	Friendly Name
Class 3 Public Primar...	Class 3 Public Primary ...	1/7/04	VeriSign Class 3 ...
Commercial Certificat...	Commercial Certificatio...	11/3/99	VeriSign/RSA Co...
Copyright (c) 1997 M...	Copyright (c) 1997 Micr...	12/30/99	Microsoft Timesta...
GTE CyberTrust Glo...	GTE CyberTrust Global...	8/13/18	GTE CyberTrust ...
GTE CyberTrust Root	GTE CyberTrust Root	2/23/06	GTE CyberTrust ...
KeyWitness 2048 R...	KeyWitness 2048 Root	5/5/04	KeyWitness Glob...
Microsoft Authentico...	Microsoft Authenticode...	12/31/99	Microsoft Authent...
Microsoft Root Auth...	Microsoft Root Authority	12/31/20	<None>
NO LIABILITY ACCE...	NO LIABILITY ACCEP...	1/7/04	VeriSign Time Sta...

Certificate Intended Purposes

Secure Email, Client Authentication, Code Signing, Server Authentication

Limit use of Active Content

- IRS now distributes forms as .PDF files
- Standard formats for animations, surveys, RSVP messages, display-only documents

Special Problems with “Terminals”

- It started with programmable function keys on “dumb” terminals
- <esc> FK3 <data> <esc>
  - Suppress display; if the user presses function key #3 in the future, send <data>
- <esc> FR3 <esc>
  - Suppress display; act as though function key #3 was pressed

Special Problems with "Terminals"

- If someone displays a file that ends with: <esc> KF3 rm *.* <cr> <esc>, bad things happen
- Fix was to have function keys return fixed sequences and applications all apply translations

Browsers as the Ultimate "Terminal"

- Browsers accept for "display" rich text HTML that can include links to other URLs
  - Display of even cached or local documents can be monitored via URL references
  - Scripting is like programmable function keys
  - Browsers and servers try to prevent "cross-site" scripting, but it's hard

The new “function keys”

- If I put script or even HREFs in a message you display through a web site, you will send my commands back to that web site
- Servers may filter out scripts… will they notice this one?

-
  ```
  <IMG SRC="j&#x41;vascript:alert
  ('Javascript is executed')">
  ```

Glimmers of Hope

- The attackers are getting faster and more reliable
- The software industry is becoming quicker to respond to attacks with patches
- Some users consider it a matter of “geek pride” to secure their systems

What we need most

- Operating systems that protect themselves from applications, and applications from one another
  - Levels of privilege, with the highest almost never needed

What we need most

- User mode should be low privilege even if user is trusted
  - Protect system utilities
  - Run software from read-only partitions
  - Make user “su” for higher privileges
- Partition a user’s activities from one another
  - Separate virtual browser per web site
  - Separate virtual file system per application

What we need most

- Well behaved applications
  - A word processor doesn’t need unmediated access to the file system or the network
  - Structure in the OS could avoid the need for privilege even to install most software
  - Less application integration

What we need most

- Backup and restore utilities
  - Separation of code and data
  - Separation of applications and OS
  - Logs of all changes
  - Selective and complete recovery
  - Mediated by a protected OS immune to most attacks

What can individuals do?

- Do what you can to protect yourself
  - Learn what is dangerous
  - Complain when it’s hard
  - Favor software that does a better job
- Make others aware of the risks