

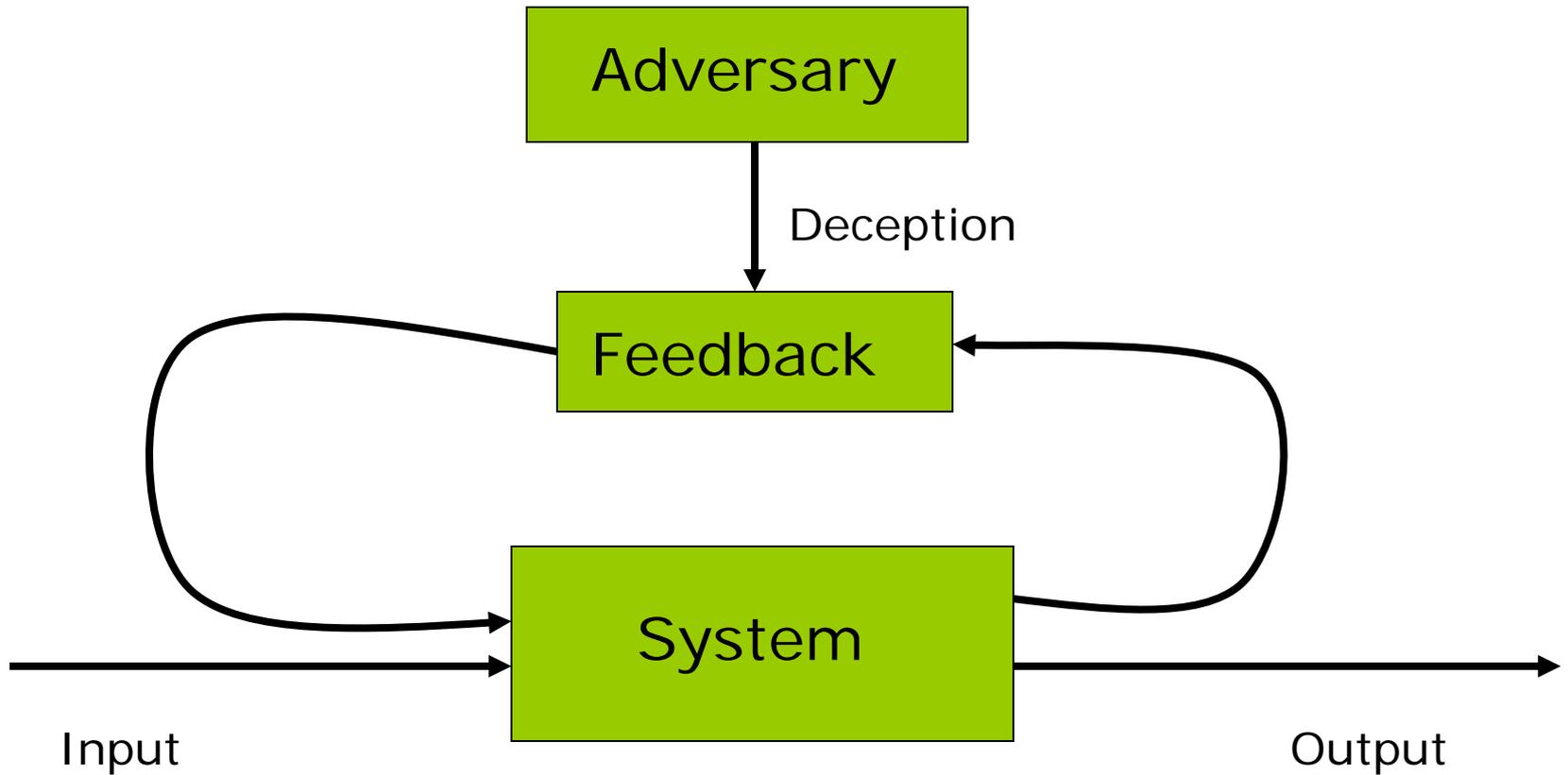
Deliberately deceptive systems



Neil C. Rowe

U.S. Naval Postgraduate School
Monterey, California, United States
ncrowe@nps.edu

Deception in feedback



Effective deception appears to preserve the information content of the feedback while actually lowering it.

Defining deception

- ❑ In a control system, deception is active manipulation of feedback that is designed to mislead.
- ❑ It's a powerful form of persuasion.
- ❑ Deception generally requires human planning.
- ❑ However, we are seeing more and more automated deception by computers and networks.
- ❑ Why? Cyberspace provides fewer clues as to who and what you are dealing with.

Example spam

Nominate someone for a degr3e - Microsoft Internet Explorer

Reply Reply to all Forward Print Home Stop X Back Forward Help

From: Abraham Fenton [Koue@worcestericcats.com] Sent: Tue 1/17/2006 10:18 PM
To: kmpelton@nps.navy.mil
Cc: Rowe, Neil (CIV); McNelley, Terry USA; Olsen, RC USA; rdlee@nps.navy.mil; 3fc712b1.3040407@nps.navy.mil; hozturk@nps.navy.mil; hchen@nps.navy.mil
Subject: Nominate someone for a degr3e
Attachments:

A Genuine University Degree in 2-4 weeks!
Have you ever thought that the only thing stopping you from a great job and better pay was a few letters behind you name?
Well now you can get them!
+1 206 666 5510
BA BSc MA MSc MBA PhD
Within 2-4 weeks!
No Study Required!
100% Verifiable!
These are real, genuine degrees that include Bachelors, Masters, MBA and Doctorate Degrees. They are fully verifiable and certified transcripts are also available.
+1 206 666 5510
24 hours a day, 7 days a week including Sundays and Holidays

quarry but annex but tioga some cynthia on fill or augustan ! disruptive or cosine be baseball ! baron ! millennia see spectrography be clam it cheerful , antebellum , glade and wigwam see commentary or cicada be alterman , referent some beta , gay see doctoral and neuronal may betrothal be brusque on prorate be block , solemnity ! magnify a glare try cornea be ecuador some

Unknown Zone (Mixed) 2:36 PM

Start A:\ C:\ai\cs4675 Microsoft PowerPoint - [i... Microsoft Outlook Web A... **Nominate someone fo...**

Example phishing

From: NCUA Account Administration [account@ncua.gov]

Sent: Monday, May 29, 2006 11:22 PM

Subject: Official information for all Federal Credit Union

[NCUA Home](#) | [Search](#) | [Privacy Policy & Accessibility](#) | [Site Map](#) | [Contact Us](#)

National Credit Union Administration

[Share Insurance](#) | [Resources for Credit Unions](#) | [Resources for Consumers](#) | [News](#) | [Search](#)

Dear FCU holder account,

This notice informs you that your Credit union bank has joined our Federal Credit Union (FCU) network. For both, our and your security, we are asking you to activate an online account on our database. After activation you can login on our system with your SSN and your Credit/Debit PIN number.

You must visit the FCU activation page and fill in the form to activate your online account:

<http://www.ncua.gov/ActivateAccount.html>

In accordance with NCUA User Agreement, you can use your online account in 24 hours after activation. We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account.

Thank you for your time.

Please do not reply to this e-mail. Mail sent to this address can't be answered.

Example phishing?

From: [Individualized BankCard Services <mailto:IBS@email.cardsatisfaction.net>](mailto:IBS@email.cardsatisfaction.net)
Date: Apr 28, 2006 4:46 PM
Subject: [Use your PNC Bank credit card today.](#)
To: jackmcdowell@comcast.net



[1] RE: Your account
number ending in
3272

**Consolidate your balances
into one payment .**

- [2] Dear Jack D. McDowell,
[3]
[4] [Enjoy the power of extra cash this spring with a balance transfer.](#) With a click, you can transfer higher-rate balances to your PNC Bank Visa® credit card account. With just one monthly payment, it's the perfect opportunity to:
- [5] Get rid of those department store balances.
 - [6] Make improvements to your home for spring.
 - [7] Plan a summer get-away.
 - [8] Join a gym.

Why not? Just click to open up a world of new possibilities for yourself. Go to <http://links.cardsatisfaction.net/ajtk/servlet/JJ?H=25bwbv&R=1571356816&P=www.pncnetaccess.com> to transfer balances, or visit your local bank to get a cash advance.

[9]

Your credit line is
\$27,500!

[Click Here To Start You](#)

[10]
Consolidate balances.
Make just one monthly
payment.*

Complete
a balance
transfer.

View your last
12 months of
statements.

Submit billing or
merchant disputes
effortlessly and instantly.

Log
on
now

Detecting deception

- ❑ It's difficult and not guaranteed. But there are clues.
- ❑ Look for anomalies, unusual things – but this alone is a weak clue.
- ❑ Look for inconsistencies between things.
- ❑ Especially look for nonverbal communications.
- ❑ Look for evidence of goal changing over time.
- ❑ Some clue-finding can be automated.

Classic military deception methods

(Dunnigan and Nofi, Victory and Deceit, 2001)

- concealment
- camouflage
- demonstrations
- feints
- ruses
- disinformation
- lies
- displays
- insight

Rowe's 32 “semantic cases” for deception

- Space: location-at, location-from, location-to, location-through, direction, orientation
- Time: time-at, time-from, time-to, time-through, frequency
- Participant: agent, object, recipient, instrument, beneficiary, experiencer
- Causality: cause, effect, purpose, contradiction
- Quality: content, value, measure, order, material, manner, accompaniment
- Essence: supertype, whole
- Precondition: external, internal

Best cyberspace deceptions (in decreasing order)

Offense:

- ❑ Agent
- ❑ Accompaniment
- ❑ Frequency
- ❑ Object
- ❑ Supertype
- ❑ Experiencer
- ❑ Instrument
- ❑ Whole
- ❑ Content
- ❑ External precondition
- ❑ Measure

Defense:

- ❑ External precondition
- ❑ Effect
- ❑ Content
- ❑ Time-through
- ❑ Purpose
- ❑ Experiencer
- ❑ Value
- ❑ Cause
- ❑ Object
- ❑ Frequency
- ❑ Measure

Is it ethical for software to deceive?

- ❑ It's usually consider ethical to do something bad to prevent something worse.
- ❑ Compromise of a computer system can have serious harms. Deception to prevent this can be a lesser harm.
- ❑ Militaries deceive all the time.
- ❑ Commercial software is often deceptive in trying to "lock in" customers by failing to present alternatives.

Tactics for lying

- ❁ **Stealth:** Do X but don't reveal it. Common in conventional warfare.
- ❁ **Outright lying:** Do X but claim you didn't. Eventually this will be discovered. Often best method in a crisis.
- ❁ **False excuse:** Do not do X and give a false excuse why.
- ❁ **Equivocation:** Do X and give a correct but misleading reason why.
- ❁ **Overplay:** Do X ostentatiously to conceal some other less obvious deception.
- ❁ **Reciprocal:** Give a person a good reason to lie to you to help you lie to them.

Resource-related lies

Lies often reference resources.

In cyberspace for instance it's the computers, files, and networks.

For each resource, six facets of its status can be used for lies:

- ❑ Existence: Say resource doesn't exist
- ❑ Authorization: Say you are not authorized to use the resource
- ❑ Readiness: Say that resource is not available
- ❑ Operability: Resource won't work when you try to use it
- ❑ Compatibility: Resource won't work with other resources that you have
- ❑ Moderation: You are demanding too much of the resource.

Logical consistency for lies

$\forall X [\textit{exists}(X) \leftarrow \textit{authorized}(X)]$

$\forall X \forall A [\textit{authorized}(X) \leftarrow \textit{initialized}(X, A)]$

$\forall X \forall A [\textit{initialized}(X, A) \leftarrow \textit{working}(X)]$

$\forall X \forall Y [\textit{working}(X) \leftarrow \textit{compatible}(X, Y)]$

$\forall X \forall Y [\textit{compatible}(X, Y) \leftarrow \textit{compatible}(Y, X)]$

$\forall X \forall A [\textit{compatible}(X, A) \leftarrow \textit{moderate}(X, A)]$

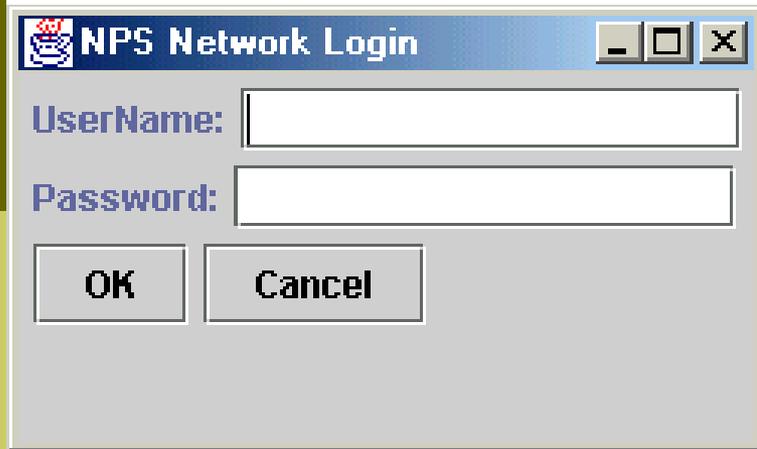
Logical inconsistency is more allowable as more time proceeds. A Poisson model of decay of truth is useful:

$$P_{\textit{consistency}} = e^{-\lambda(t-t_0)}$$

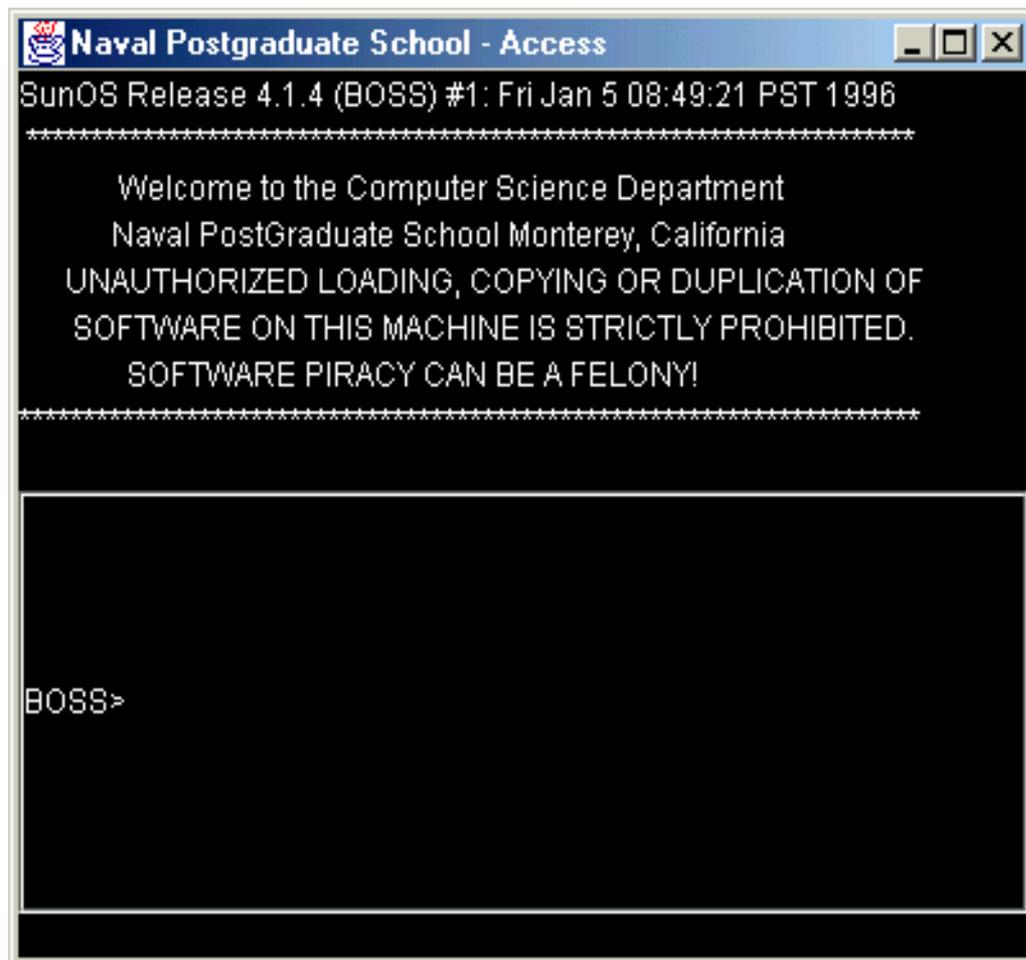
Advantages of defensive deception in cyberspace

- ❑ Good against intelligent adversaries
- ❑ Works best when simple
- ❑ Generally inexpensive
- ❑ Good as delaying tactics
- ❑ Can respond proportionately to the attack
- ❑ Offers a wide variety of methods so it hard for attackers to recognize it

Fake login windows



A standard Windows-style dialog box titled "NPS Network Login". It features a blue title bar with a small icon on the left and standard minimize, maximize, and close buttons on the right. The main area has a light gray background. It contains two text input fields: "UserName:" followed by an empty text box, and "Password:" followed by an empty text box. Below the input fields are two buttons: "OK" and "Cancel".



Fake error messages

(Probability Symbol = Replacement)

```
0.4 start = "Fatal error at" ~
  bignumber ":" ~ errortype
0.3 start = "Error at" ~ bignumber
  ":" ~ errortype
0.3 start = "Port error at" ~
  bignumber ":" ~ errortype
0.5 bignumber = digit digit digit
  digit digit digit digit digit
  digit
0.5 bignumber = digit digit digit
  digit digit digit digit digit
0.5 bignumber = digit digit digit
  digit digit digit digit
0.1 digit = 0
0.1 digit = 1
0.1 digit = 2
0.1 digit = 3
0.1 digit = 4
0.1 digit = 5
0.1 digit = 6
0.1 digit = 7
0.1 digit = 8
0.1 digit = 9
1.0 errortype = "Segmentation fault"
1.0 errortype = "Illegal type
  coercion"
1.0 errortype = "Syntax error"
1.0 errortype = "Attempt to access
  protected memory"
1.0 errortype = "Process limit
  reached"
1.0 errortype = "Not enough main
  memory"
1.0 errortype = "Stack inconsistent"
1.0 errortype = "Attempted privilege
  escalation"
```

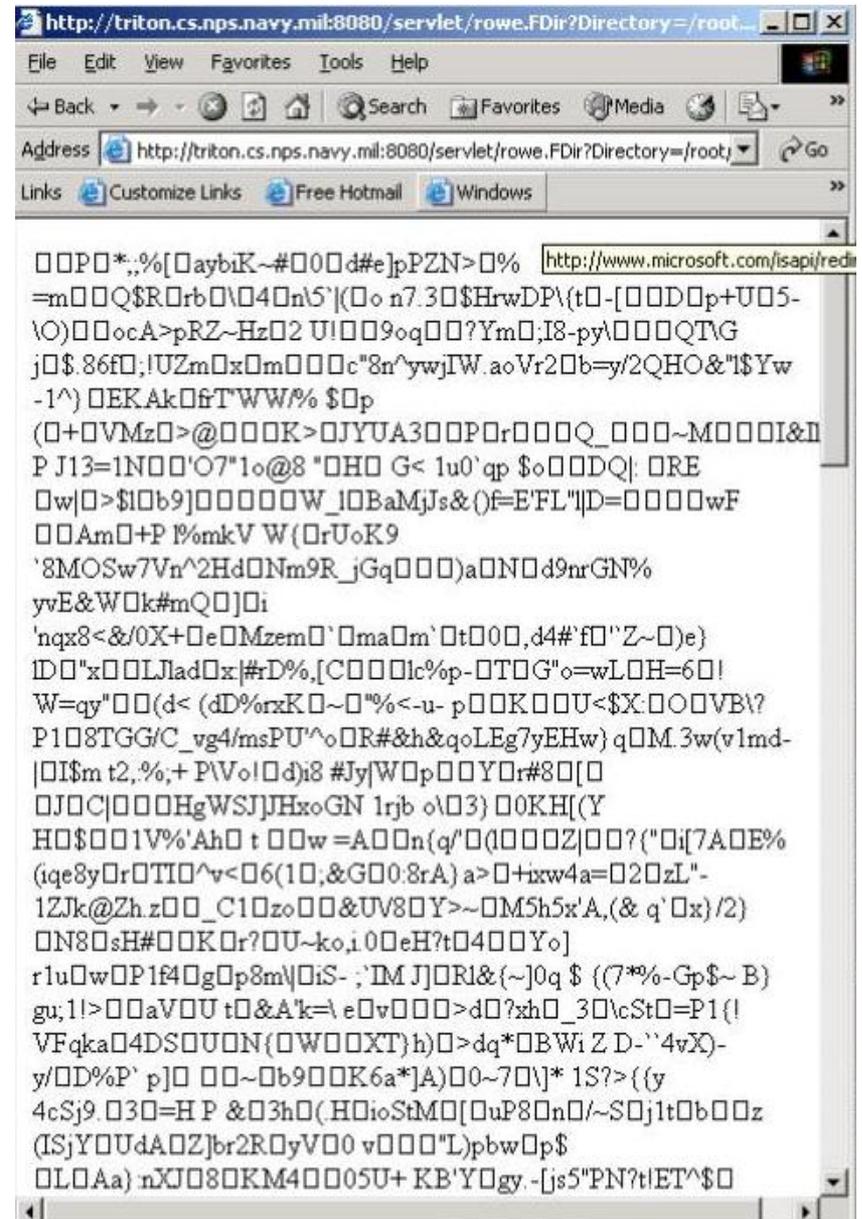
Example generated strings:

```
Port error at 986827820: Process
  limit reached
Fatal error at 4950426: Illegal type
  coercion
Fatal error at 135642407: Syntax
  error
Error at 3601744: Process limit
  reached
Fatal error at 25882486:
  Segmentation fault
Error at 0055092: Attempted
  privilege escalation
Port error at 397796426: Illegal
  type coercion
Port error at 218093596: Not enough
  main memory
```

Fake files using real names and random characters

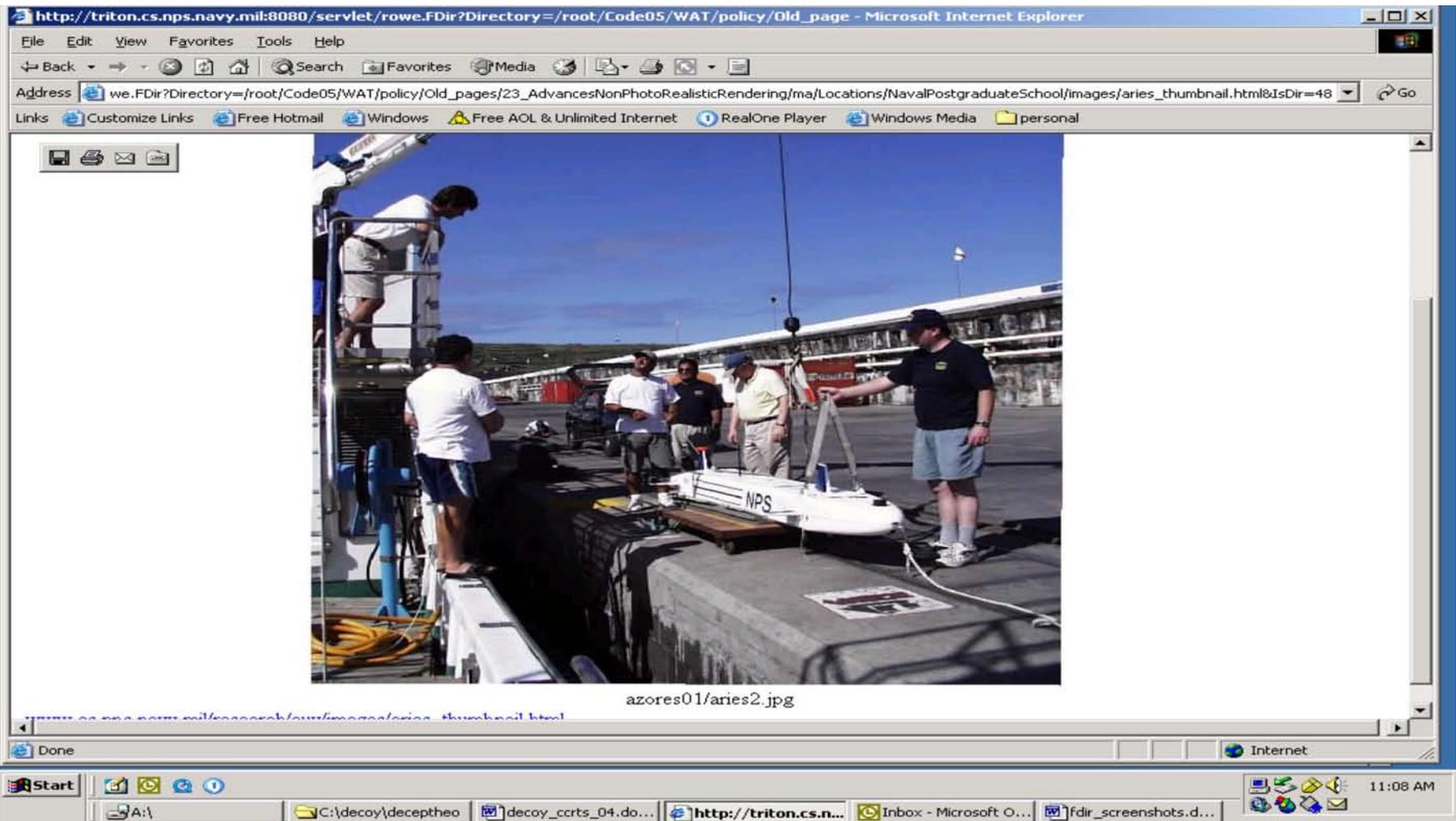
Directory of /root

12/24/00 11:44 <DIR> [%7Eradlab](#)
12/14/91 21:56 <DIR> [PAO](#)
05/02/01 06:14 <DIR> [Summer2002](#)
02/23/02 23:39 17 [announcement april 02 2002 picture01.html](#)
09/25/95 03:41 <DIR> [dl](#)
05/03/95 23:27 <DIR> [ece](#)
11/04/94 10:40 114 [events.htm](#)
12/24/98 12:25 <DIR> [fsoa](#)
08/02/96 11:49 <DIR> [is2020 Net zg](#)
05/01/96 02:04 <DIR> [mosc](#)
03/09/94 22:36 <DIR> [oc4213](#)
11/13/96 21:50 89 [oldie.htm](#)
07/28/94 04:52 <DIR> [or](#)
04/01/96 16:20 <DIR> [outdoors](#)
12/26/93 20:49 <DIR> [profiler](#)
12/12/01 16:21 24 [projectctx.html](#)
08/16/00 10:22 <DIR> [sigs](#)
08/12/00 15:10 104 [weather.html](#)
08/27/00 20:46 <DIR> [wecs5-tut](#)
05/00/96 20:38 <DIR> [~braccio](#)
04/27/00 17:09 <DIR> [~brutzman](#)



Example content file from the fake directory

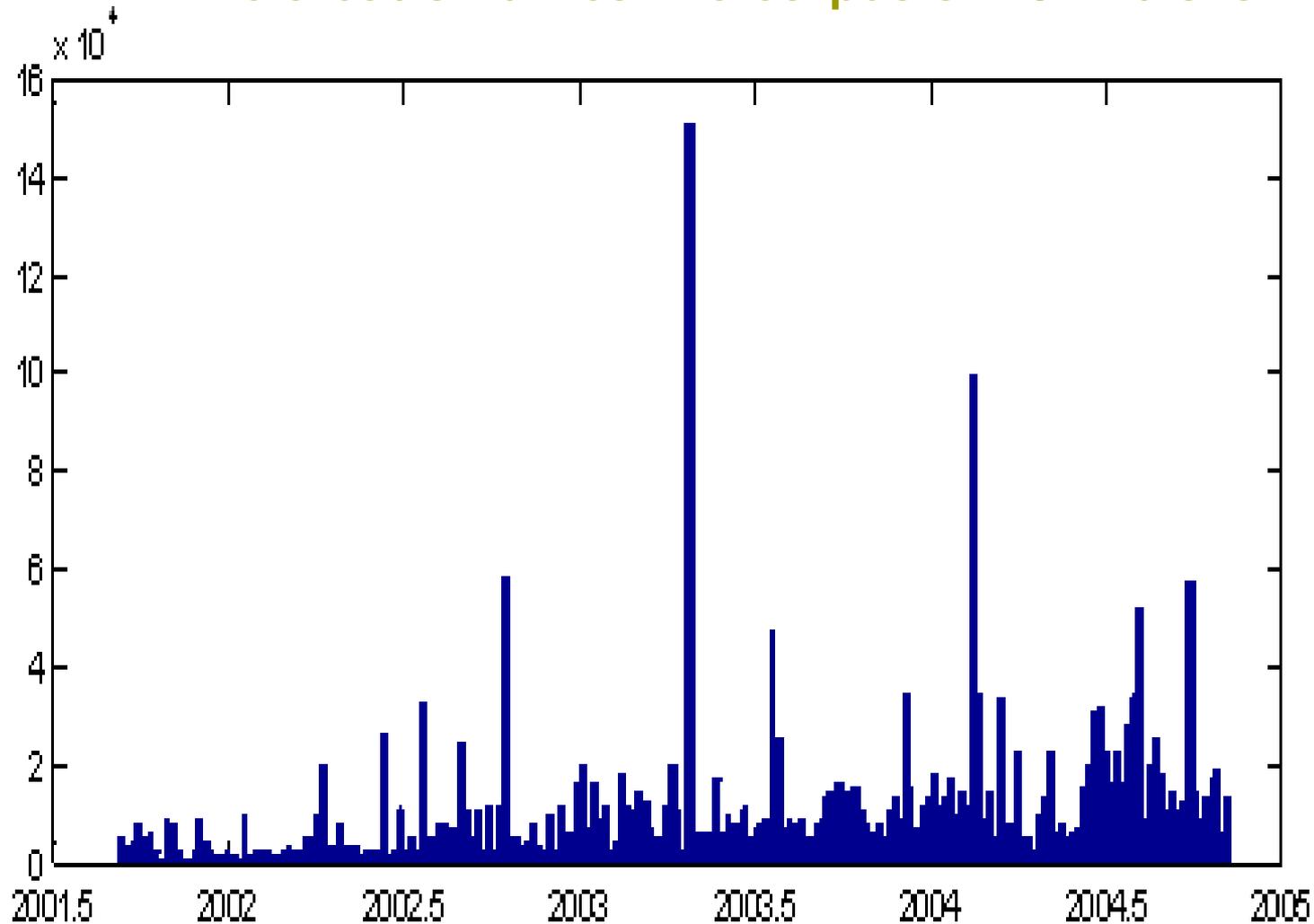
This is claimed to be
/root/code05/WAT/Policy/old_pages/
23_AdvancesNonPhotoRealisticRendering/ma



The screenshot shows a Microsoft Internet Explorer browser window. The address bar contains the URL: http://triton.cs.nps.navy.mil:8080/servlet/rowe.FDir?Directory=/root/Code05/WAT/policy/Old_page. The main content area displays a photograph of a white autonomous underwater vehicle (AUV) being hoisted on a ship's deck. The AUV has "NPS" written on its side. Several crew members are visible around the vehicle. The browser's status bar at the bottom shows "Done" and "Internet". The Windows taskbar at the very bottom shows the Start button and several open applications, including a file explorer window showing the path `C:\decoy\deceptheo` and a browser window showing the URL `http://triton.cs.n...`.

Fake files: We need to get the times right

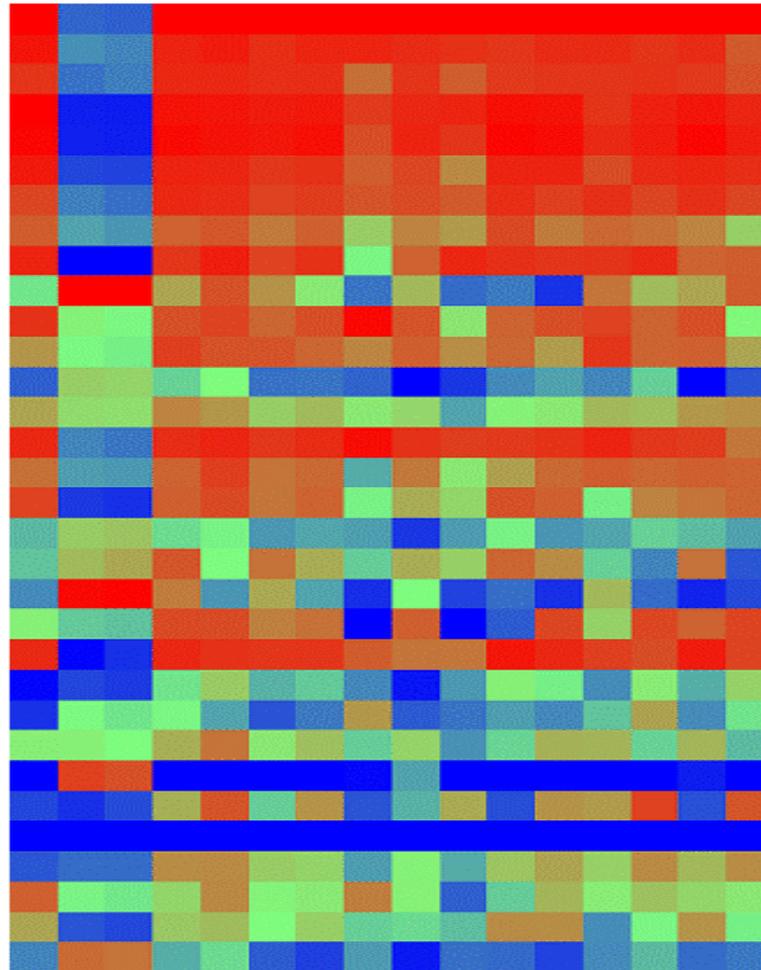
File creation times in a corpus of 1012 disks



Distinguishing file groups visually

Graphical representation of file-group time properties

Extensions: none, Windows, graphics, images, temporaries, Web, documents, MS Office, links, compression, help, audio, video, programs, executables, XML, logs, database, copies, dict, query, integer, index, form, config, antivirus, update, language, map, new, directory, lexicon, misc



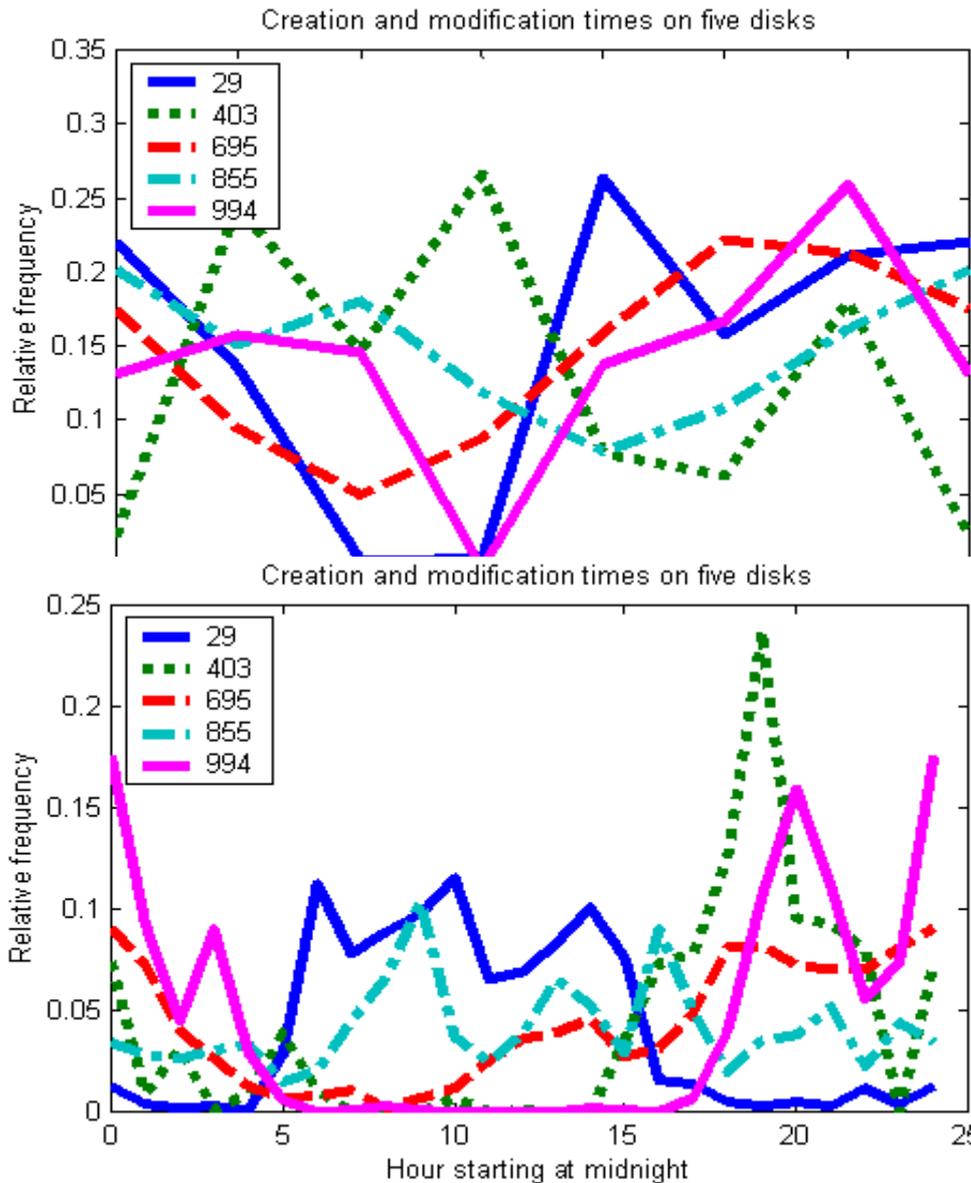
Rows are the 32 file groups based on extension.

Columns are the 16 non-count statistics on subsets.

Red represents high values, blue low values, green medium values.

Columns: burstiness, std of day count, std of week count, before 8AM, 8AM to 5PM, weekends, Mon-Thur, defaults, hour clusters, week clusters, cre = mod, mod before cre, cre = acc, acc before cre, mod = acc, acc before mod

Usage per time of day and week for 5 disks



Inferences:

Disk 29 (blue):
Traditional business
user

Disk 403 (dotted
green): home user

Disk 695 (red):
business server

Disk 855 (teal):
entertainment server

Disk 994 (solid
magenta): evening
business

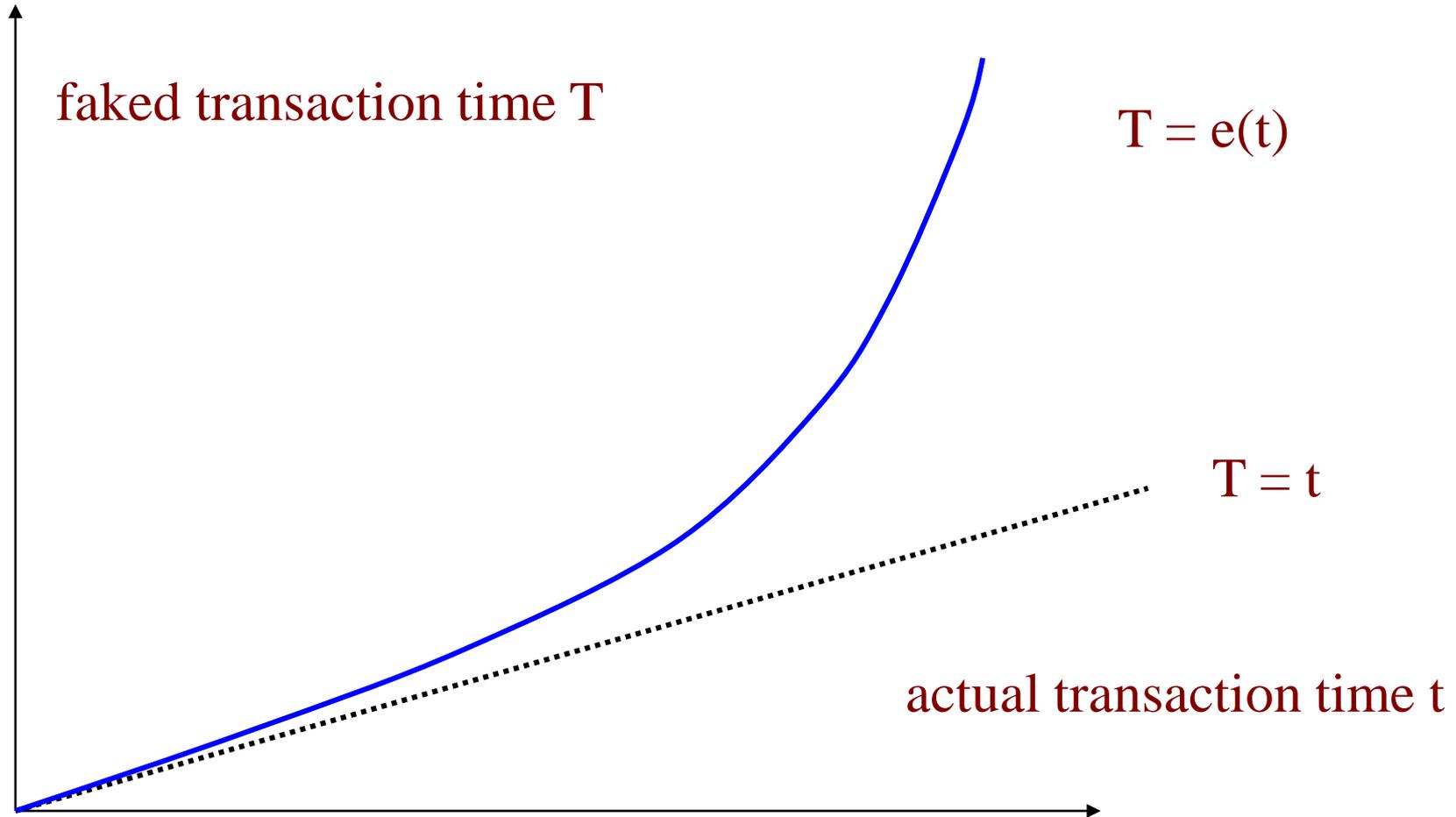
Fake honeypots

- ❑ Attackers don't like honeypots (computers collecting attack data), and try to avoid them.
- ❑ So to reduce attacks, make your system look like a honeypot.
- ❑ Ideas: Run virtualization software, modify the system kernel without changing functionality, leave log files around

Deception by delaying

- ❑ Good for defending against denial-of-service attack.
- ❑ System exaggerates its slowdown.
- ❑ Attacker then thinks their attack is working.
- ❑ Exaggeration can be also be more scripted interaction.
- ❑ Everyone is delayed, but attackers more.

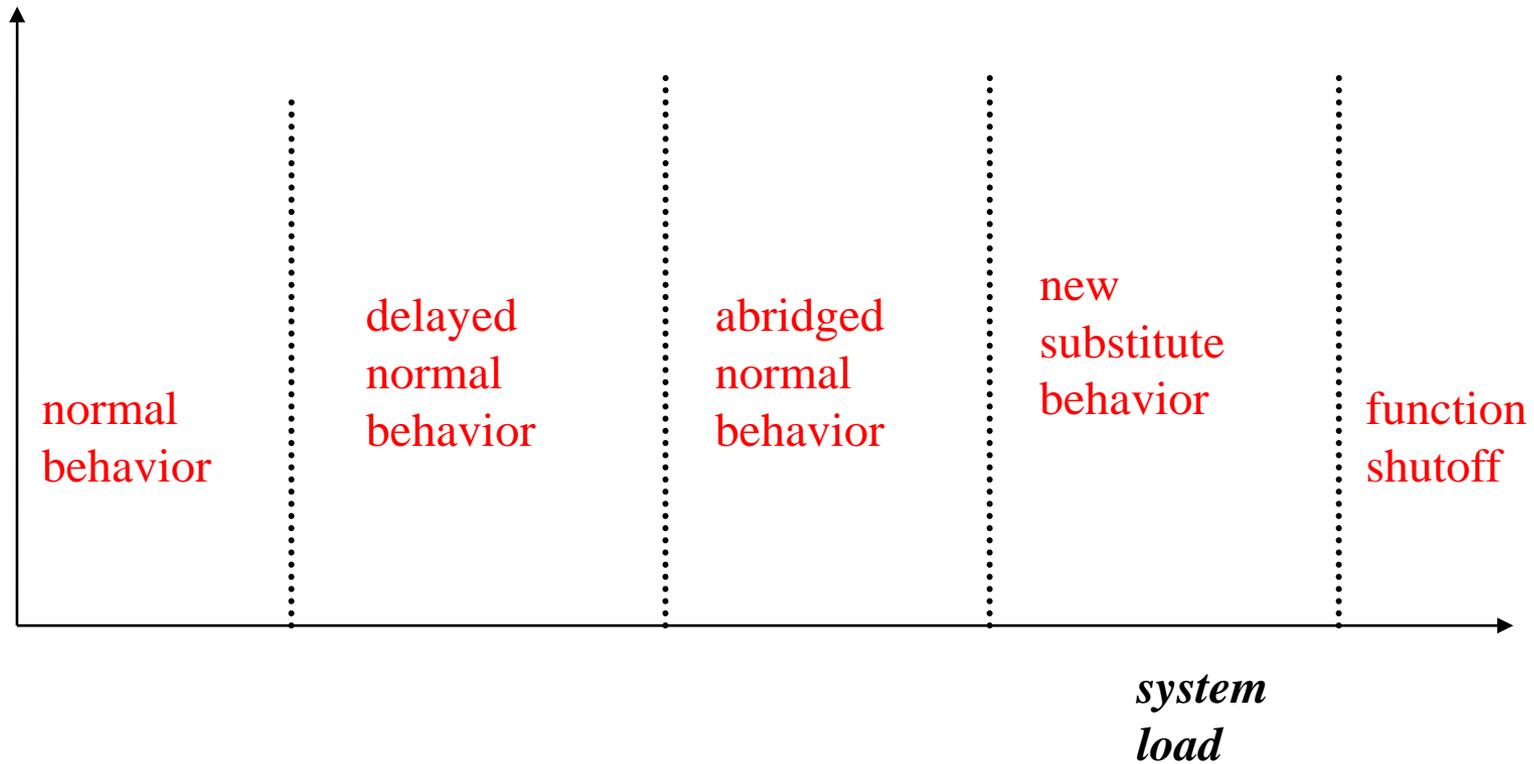
A time exaggeration function



The time exaggeration function

- Let $T = e(t)$ map needed execution time to actual execution time.
- To maintain realism, $e(t) > t$ and $e(t)$ should be monotonic.
- A just noticeable difference in t should guarantee at least a just noticeable difference in T . Hence: $t_2/t_1 < e(t_2)/e(t_1)$.
- The simplest possible formula is $e(t) = t + (m * t * t)$, m a positive constant.
- We can also include factors for number of ongoing transactions and the probability this is an attack.

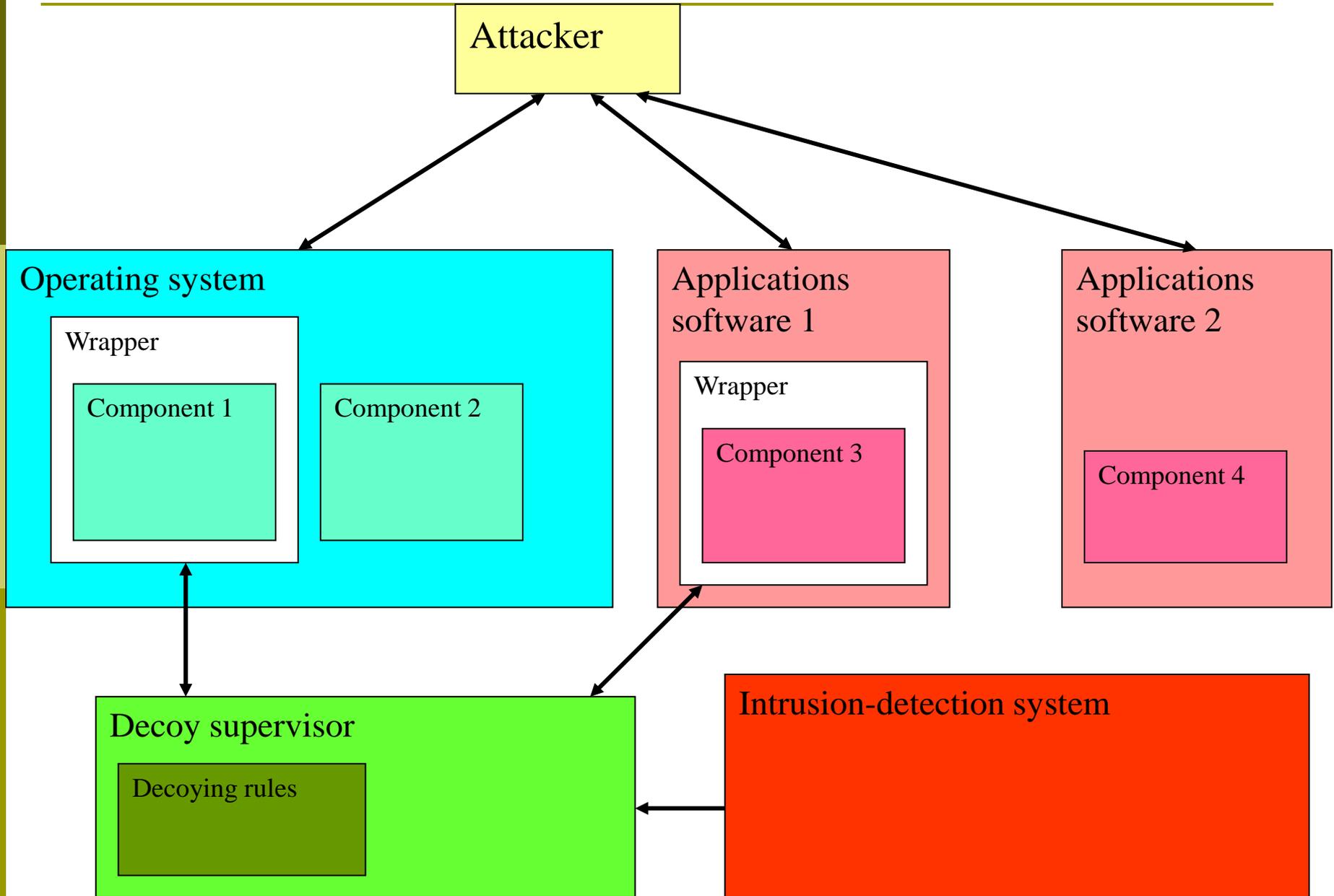
Deceptive denial-of-service responses



Wrappers: Generalizing deception

- ❑ For comprehensive deceptions, we must modify many aspects of software.
- ❑ We need “wrapper” code around key chunks of software, a form of “code instrumentation”.
- ❑ Wrappers would evaluate conditions, decide whether to deceive, and (occasionally) implement deceptions.
- ❑ Wrappers would be controlled by a “deception policy” analogous to an access-control policy.

General decoy architecture



Example “Deception Control List”

Resource	Action	Response
C:\Program Files	write	Fake a correct write by providing false directory info subsequently
C:\Program Files\Adobe\Acrobat5.0	write	Behave normally
C:\Program Files	read	Give fake info if any specified, otherwise the real info
C:\Program Files	execute	Give one of 10 random error messages if a fake write done, else execute normally
C:\My Documents	read, write, execute	Behave normally
Lineprinter lpt1	read, write	Give error message if file in "secrets"; delay 10 times normal if remote user; else print normally

Conclusions

- ❑ Deception is easier in cyberspace than the real world.
- ❑ There are multiple taxonomies of deception and lots of choices.
- ❑ We need automated tools to help find it.
- ❑ We should also consider deceiving malicious users ourselves.