

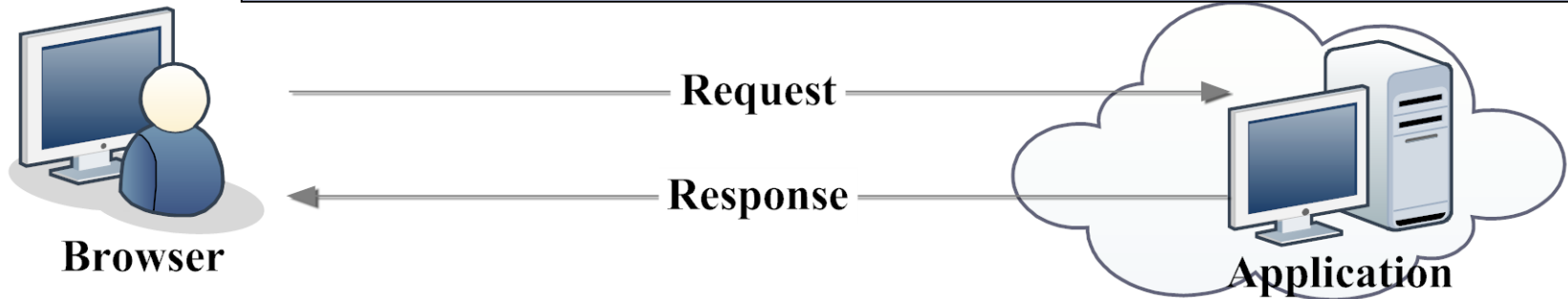
CS 6431

Security Issues in Web Applications

Vitaly Shmatikov

User Input Validation

[Bisht et al. "NoTamper: Automatic Blackbox Detection of Parameter Tampering Opportunities in Web Applications". CCS 2010]



- ◆ Web applications need to reject invalid inputs
 - "Credit card number should be 15 or 16 digits"
 - "Expiration date in the past is not valid"
- ◆ Traditionally done at the server
 - Round-trip communication, increased load
- ◆ Better idea (?): do it in the browser using **client-side JavaScript code**

Client-Side Validation

[Bisht et al.]

Checkout

1 Kitchenaid 5-Quart Mixer, Red (\$399.99)

1 All-Clad Copper Core 14-Piece Set (\$1,999.95)

Credit Card : ✓ 1234-5678-9012-3456
7890-1234-5678-9012

Delivery Instructions

Submit

```
onSubmit=  
  validateCard();  
  validateQuantities();
```

Validation Ok?

Yes

No

send inputs
to server

reject
inputs

Problem: Client Is Untrusted

[Bisht et al.]

Checkout

Checkout

Kitchenaid 5-Quart Mixer, Red (\$399.99)

All-Clad Copper Core 14-Piece Set (\$1,999.95)

Credit Card : ✓ 1234-5678-9012-3456
7890-1234-5678-9012

Delivery Instructions

Submit

Previously rejected values sent to server

Inputs must be re-validated at server!

Online Shopping

[Bisht et al.]

Checkout

CodeMicro.com

-4 Kitchenaid 5-Quart Mixer, Red (\$399.99)

1 All-Clad Copper Core 14-Piece Set (\$1,999.95)

Total Price: 399.95

Credit Card : ✓ 1234-5678-9012-3456
7890-1234-5678-9012

Delivery Instructions

Submit

Client-side constraints:

$$\left. \begin{array}{l} \text{quantity1} \geq 0 \\ \text{quantity2} \geq 0 \end{array} \right\}$$

Server-side code:

$$\text{total} = \text{quantity1} * \text{price1} + \text{quantity2} * \text{price2}$$

Vulnerability: malicious client submits negative quantities for unlimited shopping rebates

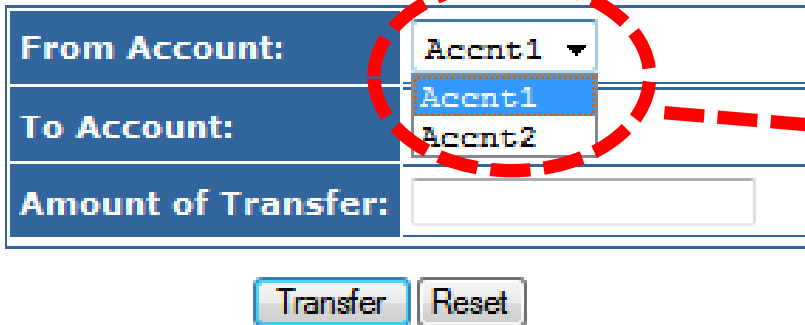
Two items in cart: price1 = \$100, price2 = \$500

quantity1 = -4, quantity2 = 1, total = \$100 (rebate of \$400 on price2)

Online Banking

[Bisht et al.]

Transfer Funds



The screenshot shows a web form titled "Transfer Funds". It has three main input fields: "From Account:", "To Account:", and "Amount of Transfer:". The "From Account:" field is a dropdown menu currently showing "Acct1". A red dashed circle highlights the dropdown menu, and a red dashed arrow points from it towards the text on the right. Below the form are two buttons: "Transfer" and "Reset".

SelfReliance.com

Client-side constraints:

from IN (Acct1, Acct2)

to IN (Acct1, Acct2)

Server-side code:

transfer money from → to

Vulnerability: malicious client submits arbitrary account numbers for unauthorized money transfers

IT Support

[Bisht et al.]

OpenIT - Editing

Editing Employee

First Name: Alice

Last Name:

Middle Initial:

Group: Guests

Password:

Notes:

Submit

Hidden Field

userId == 96 (hidden field)

Client-side constraints:

`userId == 96` (hidden field)

Server-side code:

Update profile with id 96
with new details

Vulnerability: update arbitrary account

Inject a cross-site scripting (XSS) payload in admin account,
cookies stolen every time admin logged in

Content Management

[Bisht et al.]

The screenshot shows a web registration page for 'DCP PORTAL Content Management System'. The page header includes the site logo, a 'RATED #1 IN WEB' badge, and the date '12 October 2011 Web'. Below the header is a navigation bar with a search box, a 'Contents' dropdown menu, and links for 'Links' and 'D'. On the left side, there is a sidebar menu with options for 'News', 'Announcements', and 'Member Area'. The 'Member Area' section contains a registration form with fields for 'Username', 'Password', 'Remember Me!' (checked), 'Sex' (radio buttons for 'Male' and 'Female'), and 'Name'. A 'Login' button is also visible.

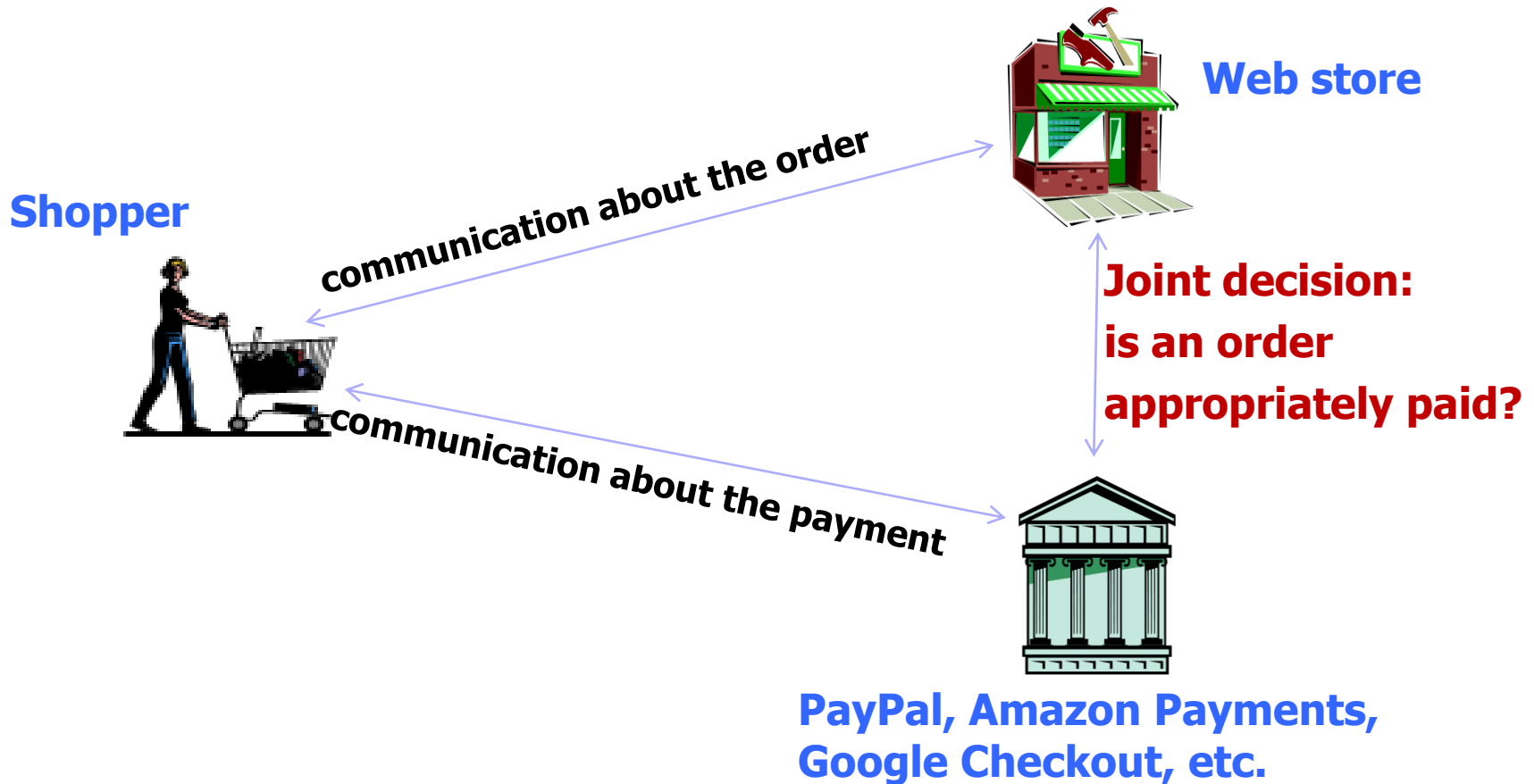
Server-side code:

```
privilege = non-admin;  
if ( _COOKIE['make_install_prn']  
    == 1 )  
    privilege = admin;
```

Vulnerability: malicious client sets make_install_prn cookie,
creates fake admin account

Cashier-as-a-Service

[Wang et al. "How to Shop for Free Online: Security Analysis of Cashier-as-a-Service Based Web Stores". Oakland 2011]



noCommerce + Amazon Simple Pay

[Wang et al.]

◆ Anyone can register an Amazon seller account, so can Chuck

- Purchase a \$25 MasterCard gift card by cash, register under a fake address and phone number
- Create seller accounts in PayPal, Amazon and Google using the card

◆ Chuck's trick

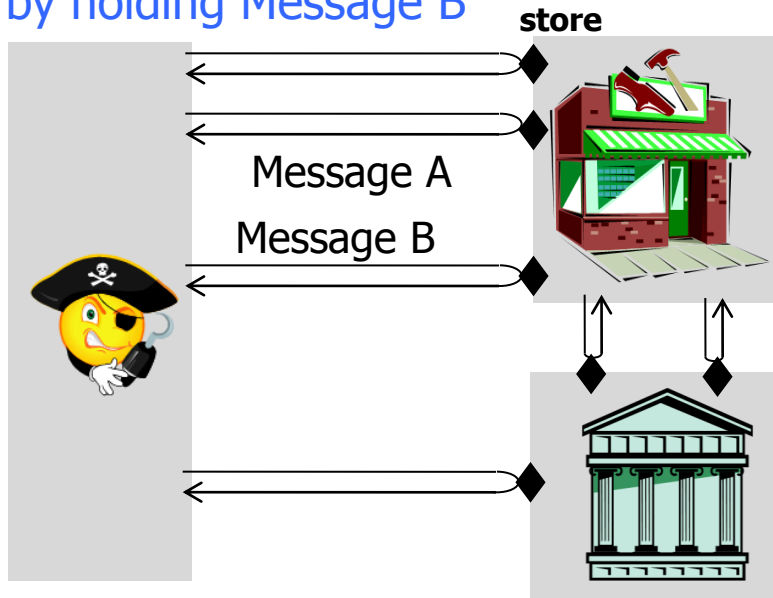
- Check out from Jeff, but pay to "Mark" (Chuck himself)
- Amazon tells Jeff that payment has been successful
- Jeff is confused, ships product



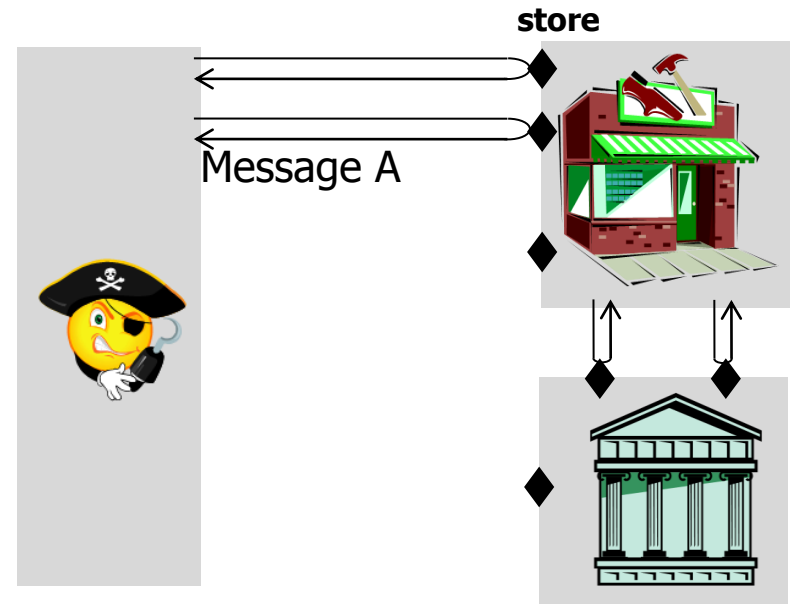
Interspire + PayPal Express

[Wang et al.]

Session 1: pay for a cheap order (**orderID1**), but prevent the merchant from finalizing it by holding Message B



Session 2: place an expensive order (**orderID2**), but skip the payment step



Message A redirects to `store.com/finalizeOrder?[orderID1]store`

Message A redirects to `store.com/finalizeOrder?[orderID2]store`

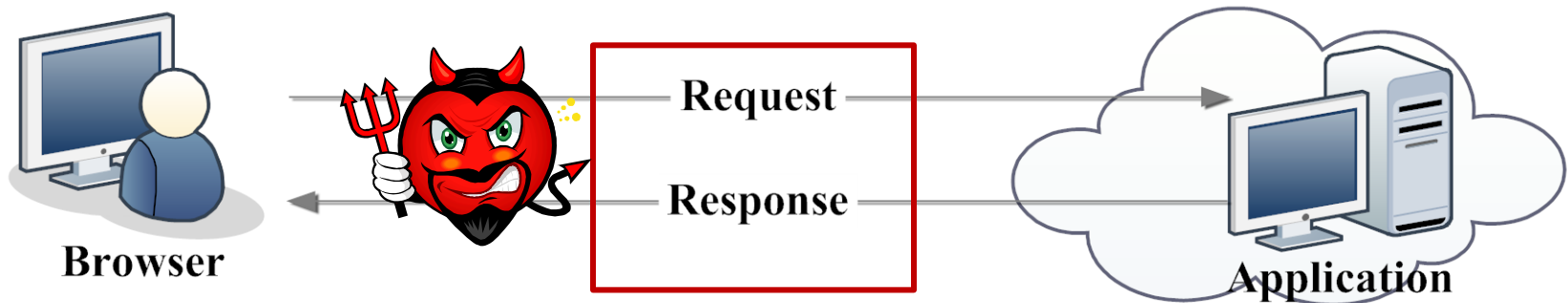
Message B calls `store.com/finalizeOrder?[orderID1]store`

`[orderID2]store`

Expensive order is checked out but the cheap one is paid!

Side-Channel Leaks

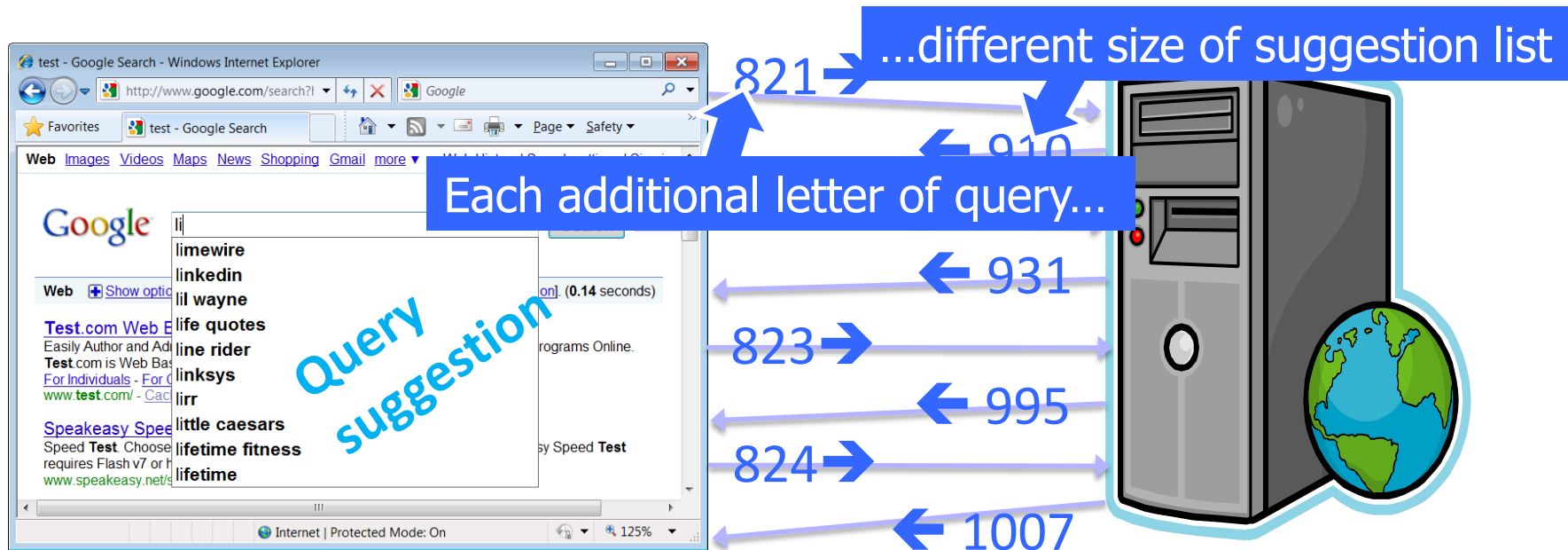
[Chen et al. "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow". Oakland 2010]



encrypted!
privacy problems solved?

Attacker can still see the number of packets,
size of each packet, time between packets...

- ◆ Search using encrypted Wi-Fi (WPA / WPA2)
- ◆ Example: user types "l-i-s-t" on his laptop...



Attacker's effort linear in the size of query

Consequence: any eavesdropper knows our search queries

Online Medical Application

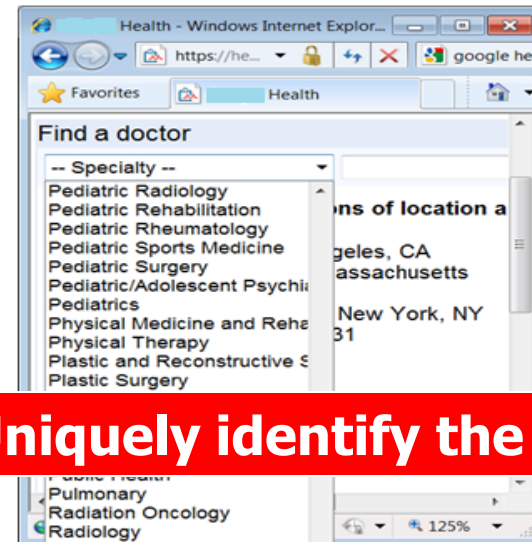
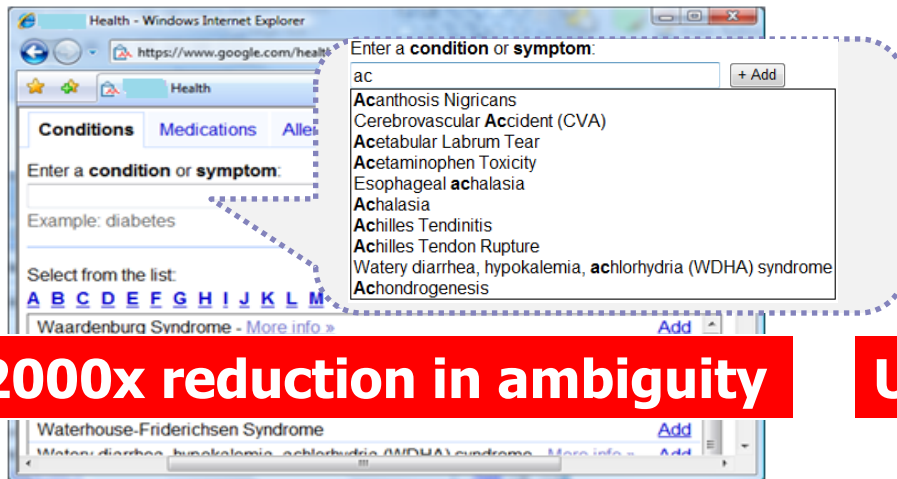
[Chen et al.]

◆ Entering health records

- By typing – auto-suggestion
- By mouse – a tree structure of elements

◆ Finding a doctor

- Dropdown list



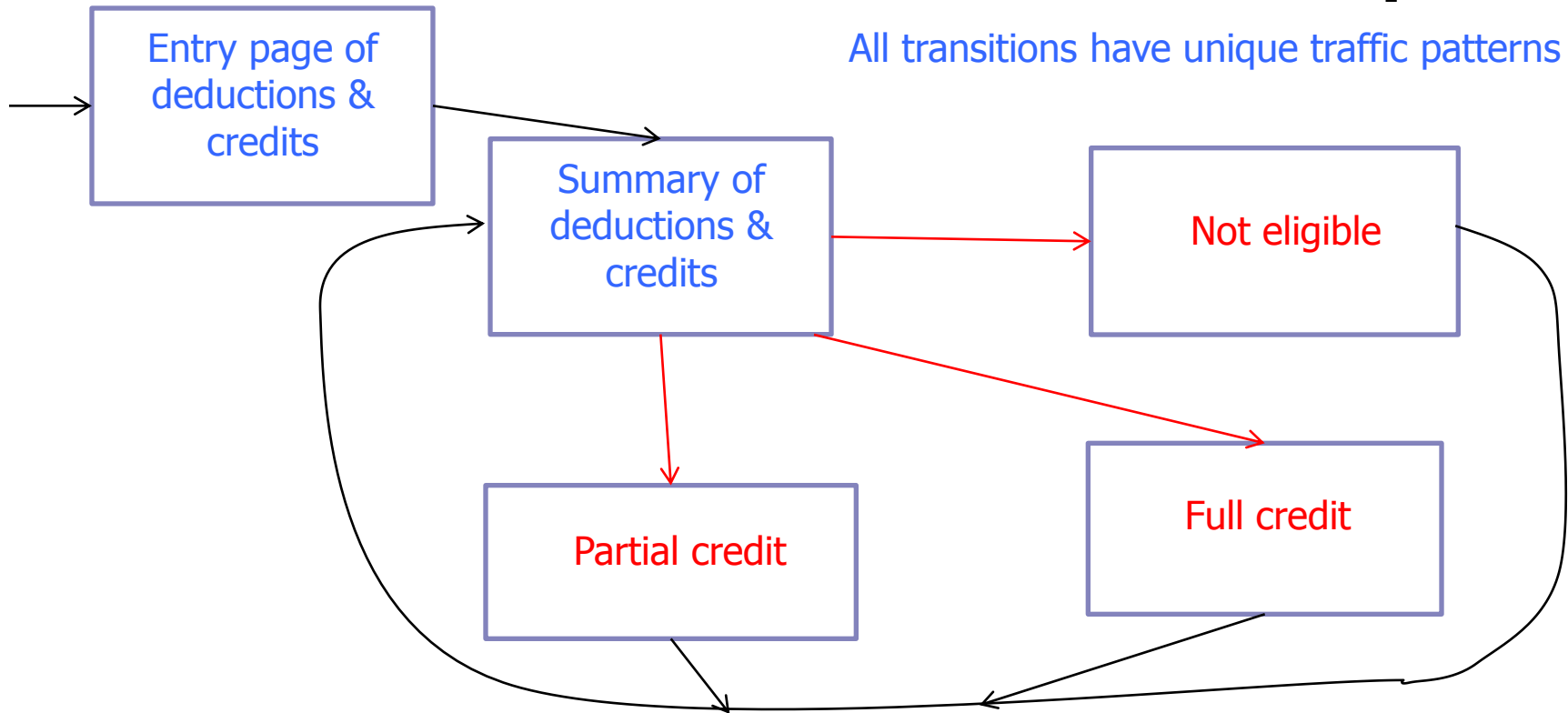
Tax Preparation Application

[Chen et al.]

- ◆ Wizard-style questionnaire
 - Tailor the questions based on previous inputs
- ◆ Which forms you work on reveal filing status, big medical bills, **adjusted gross income...**
- ◆ Knowing the state machine of the application the eavesdropper can infer sensitive information
 - Especially by combining information learned from multiple state machines

Child Credit State Machine

[Chen et al.]



Consult the IRS instruction:

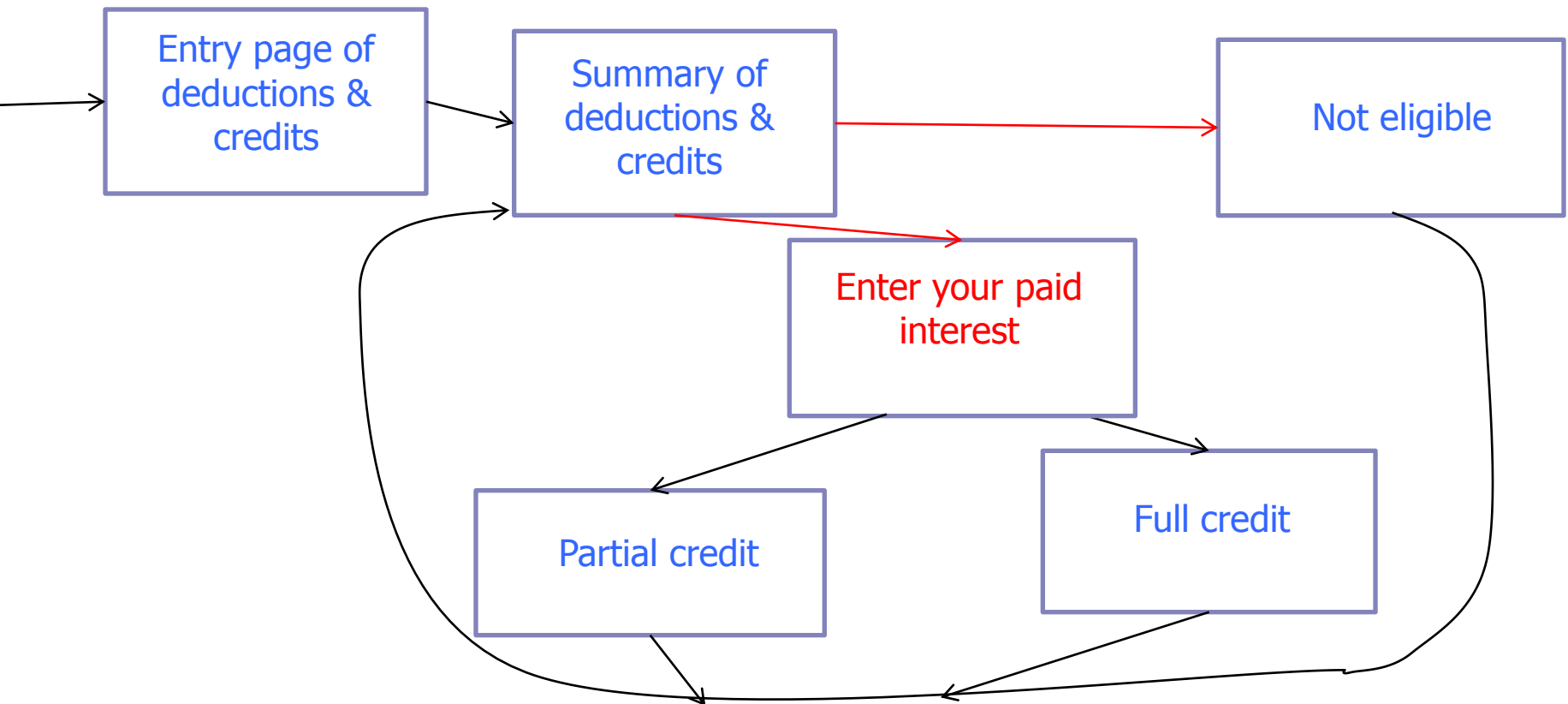
\$1000 for each child

Phase-out starting from \$110,000. For every \$1000 income, lose \$50 credit.

Student Loan Interest State Machine

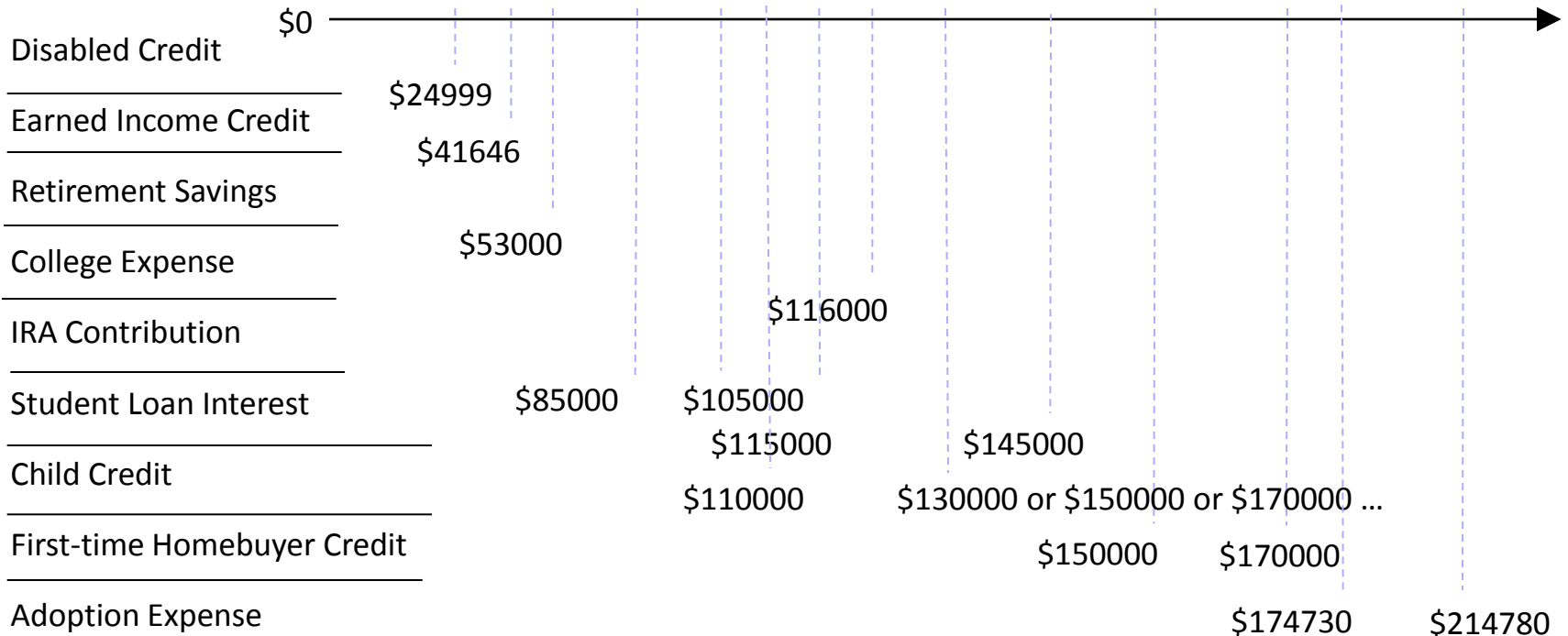
[Chen et al.]

Even worse, most decision procedures for credits/deductions have **asymmetric paths**: eligible – more questions, not eligible – no more questions



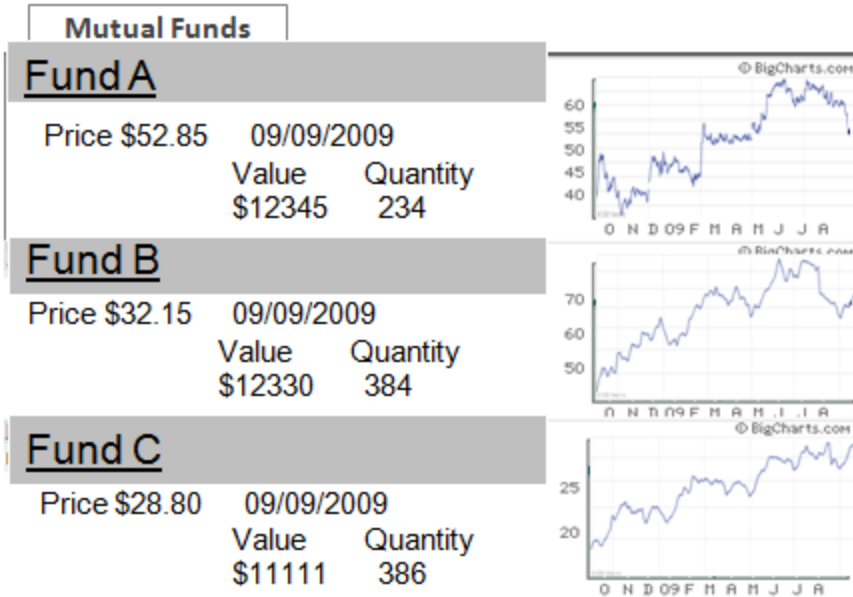
Some Identifiable AGI Thresholds

[Chen et al.]



Online Investments

[Chen et al.]

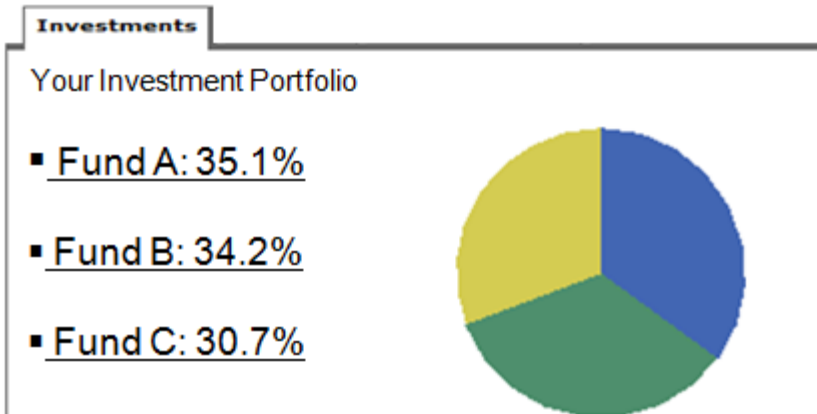


Which funds you invest in?

- ◆ Each price history curve is a GIF image from MarketWatch
 - Anyone in the world can get them from this website
- ◆ Just compare the image sizes!

Your investment allocation?

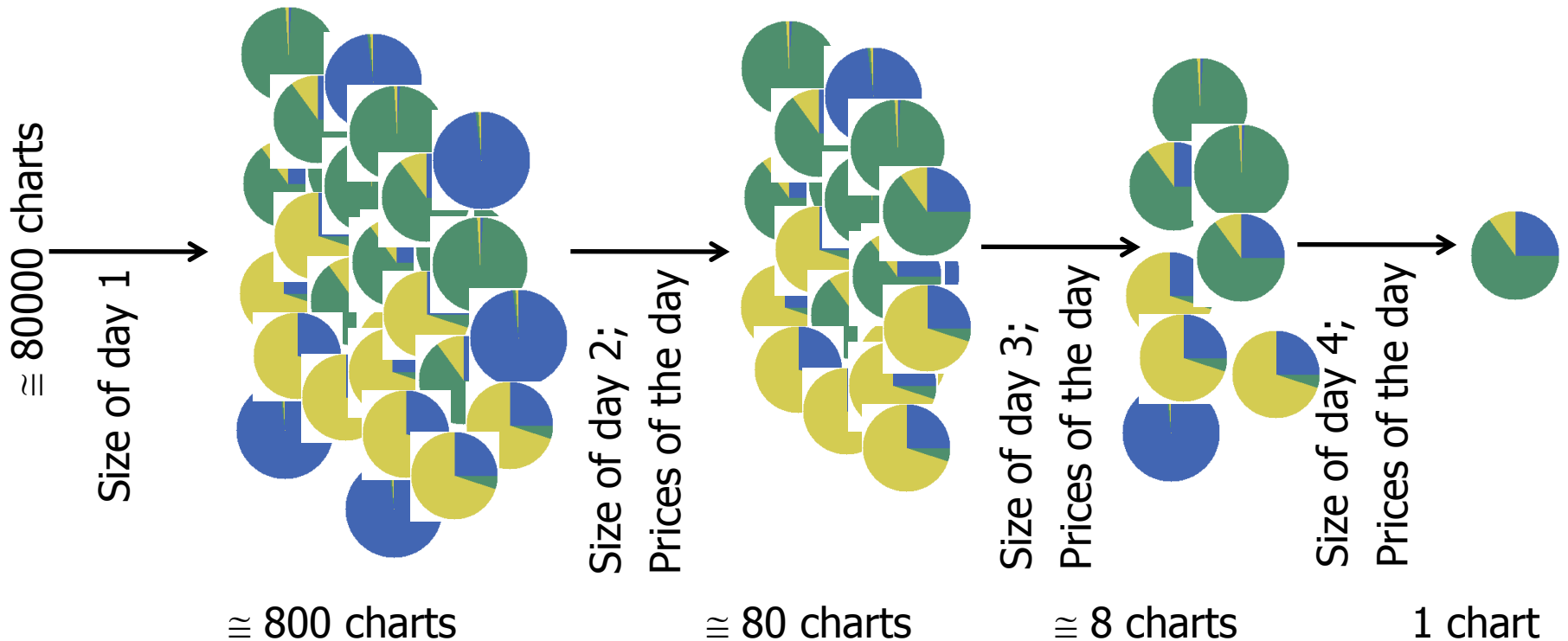
- ◆ Can see the size of the pie chart, but hundreds of pie charts have the same image...



Change Over Time Is Revealing!

[Chen et al.]

Financial institution updates your pie chart every day after market close.
Mutual fund prices are public knowledge.



Rounding? Padding?

[Chen et al.]

- ◆ Still have the asymmetric path problem
- ◆ Google's responses are compressed, destination networks may or may not uncompress responses
 - For example, Microsoft gateways uncompress and inspect Web traffic, but university does not
 - Round before compression – university still sees distinguishable sizes; after compression – Microsoft does
- ◆ Random padding is not appropriate
 - If user checks several times, repeated random padding of the same responses quickly degrades effectiveness
 - Images come from MarketWatch, not site itself

Trends in Software Design

[Jana and Shmatikov. "Memento: Learning Secrets from Process Footprints". Oakland 2012]

- ◆ Applications rely on OS abstractions to improve their safety and reliability
 - "Process", "User"
- ◆ Case study: Web browsers



Unintended Consequences

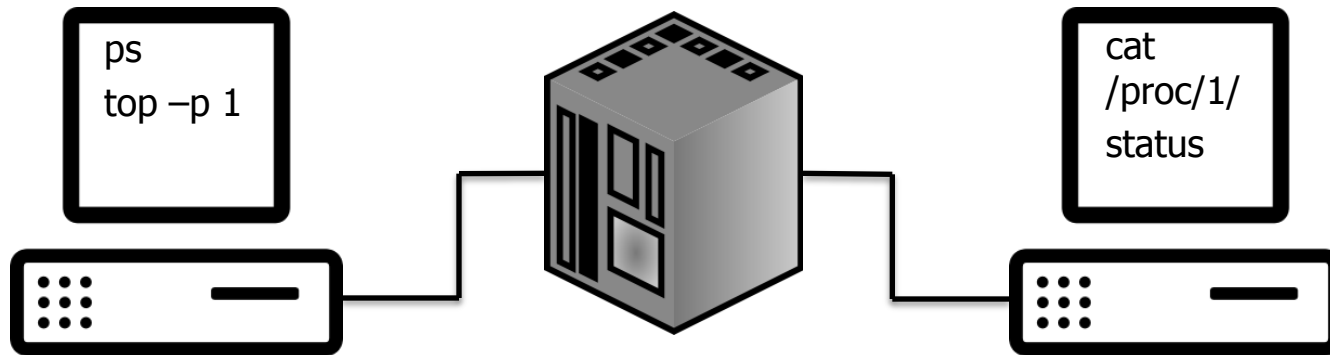
Good

- Better isolation
- Better reliability
 - Others not affected if one process crashes
- Better safety

Bad

Leaks more info to concurrent processes

ProcFS in Multi-User OS



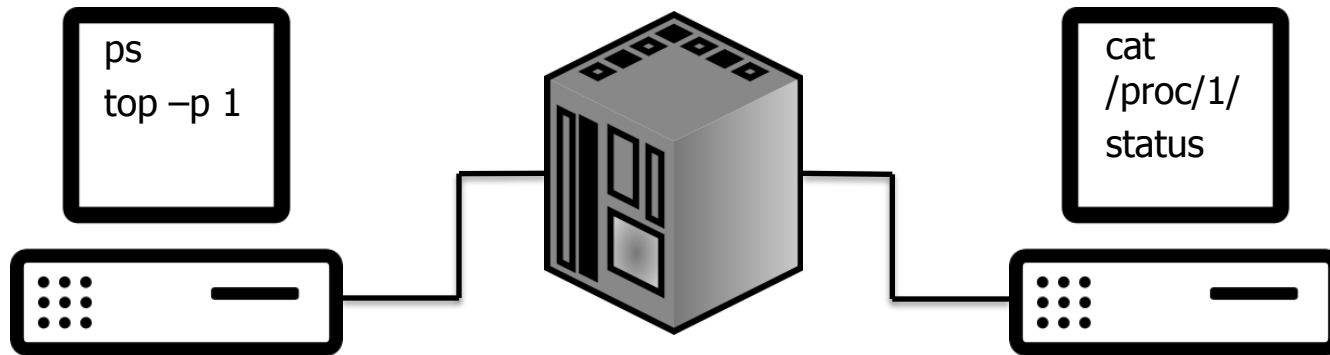
↑
Tom Killian
"Processes as Files"
(1984)

Introduced in the 1980s

"Noone Uses Multi-User OS Anymore"

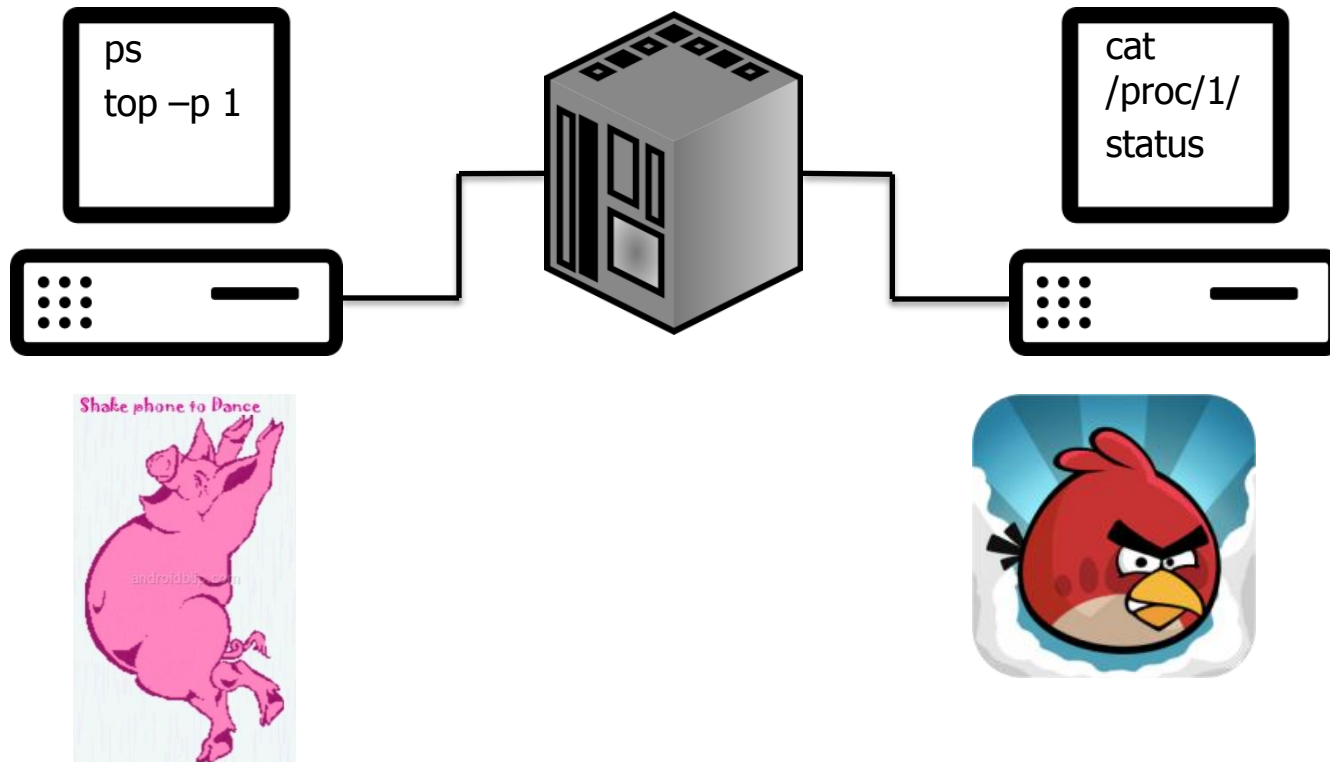


Multi-User Isolation



UNIX multi-users in the 1980s

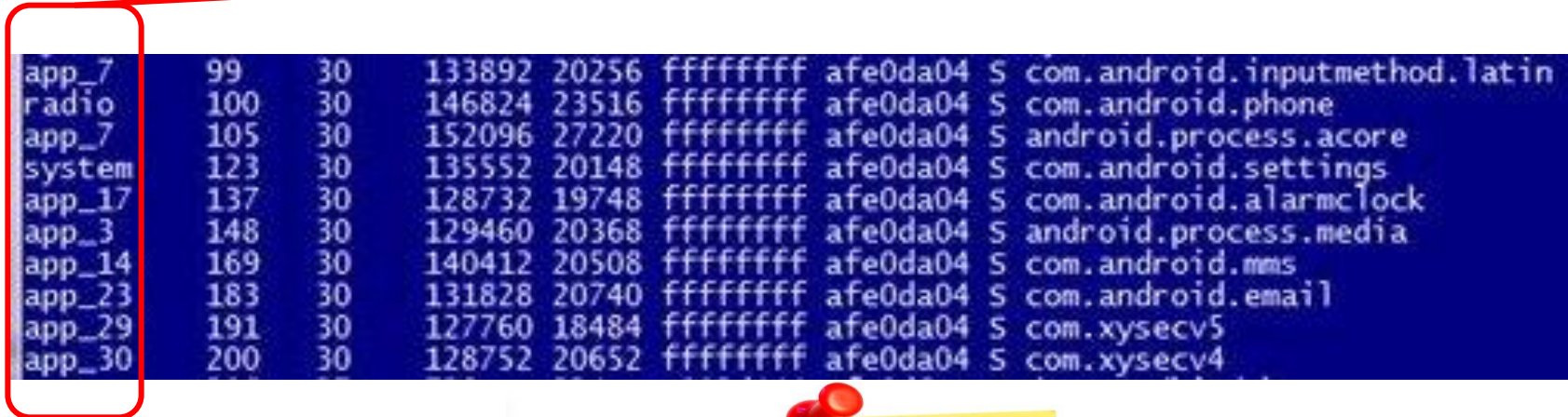
Android Sandboxing



Android "multi-users" today

Android Apps as "Users"

- Different apps run as different **users**



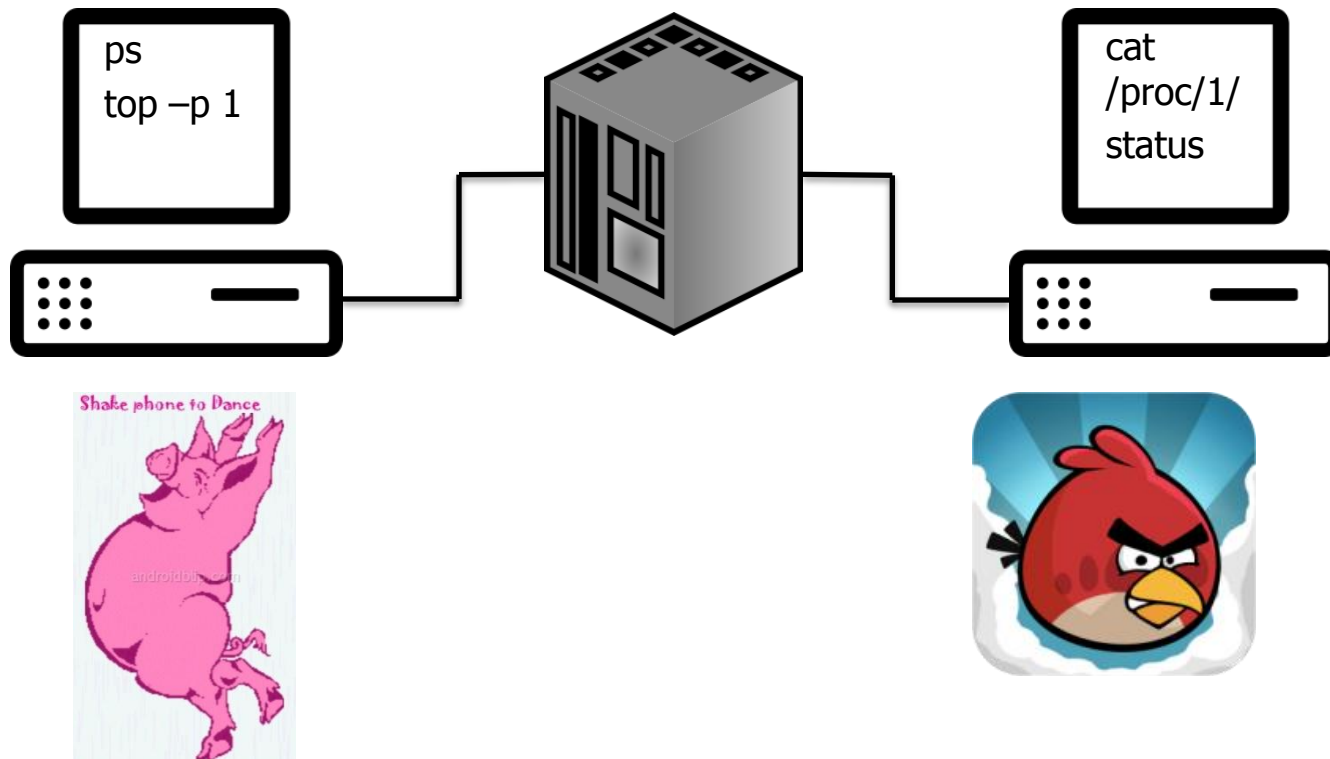
app_7	99	30	133892	20256	ffffffff	afe0da04	S	com.android.inputmethod.latin
radio	100	30	146824	23516	ffffffff	afe0da04	S	com.android.phone
app_7	105	30	152096	27220	ffffffff	afe0da04	S	android.process.acore
system	123	30	135552	20148	ffffffff	afe0da04	S	com.android.settings
app_17	137	30	128732	19748	ffffffff	afe0da04	S	com.android.alarmclock
app_3	148	30	129460	20368	ffffffff	afe0da04	S	android.process.media
app_14	169	30	140412	20508	ffffffff	afe0da04	S	com.android.mms
app_23	183	30	131828	20740	ffffffff	afe0da04	S	com.android.email
app_29	191	30	127760	18484	ffffffff	afe0da04	S	com.xysecv5
app_30	200	30	128752	20652	ffffffff	afe0da04	S	com.xysecv4



Android uses OS
"user" abstraction
to isolate applications

ProcFS Did Not Go Away

ProcFS API is still unchanged!



Android "multi-users" today

This Is Not Just About Android

© 2010 Google Inc. All rights reserved. Google, the Google logo, Android, the Android logo, and "Did you know?" are trademarks of Google Inc. in the U.S. and other countries.



What Can Be Learned from ProcFS?

◆ No permissions needed to read any world-readable file in ProcFS ...

- IP addresses of network connections ← WTF?!

- Value of stack pointer ← "Peeping Tom" attacks

- Various statistics

- Packet counters

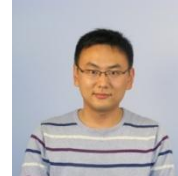
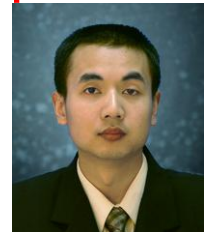
- Number of context switches / CPU scheduling statistics

- Memory usage

TCP sequence number inference

Keystroke sniffing

"Memento" attacks



Putting Memory Streams Together

Photograph Sparks Murder Investigation
Motel Customer Disappears; Leaves Suspicious Photograph, Gun, Documents and Questions

By SEAN O'NEARA
GILLETTE STAFF WRITER

Municipal police initiated a murder investigation Wednesday based on evidence found in a local motel room, which include what police are describing as a photograph of a dead body. "We can't identify the body or we can't identify the body or we're confident that some sort of foul play is involved," said Police Chief Joel Warren. "We're trying to piece together what happened."

Police were called in on Monday after cleaning staff at the Discount Inn reported finding suspicious items in one of the rooms. The man who had been staying in the room, identified by police as Leonard Shelby, formerly of San Francisco, California, had not been seen by local and state authorities.

While searching the room, police found "dozens" of photographs of people and vehicles, an unregistered handgun, and a large quantity of documents, many of them burned or in fragments, Warren said.

Little is known about Shelby himself, but a man by the same name was reported missing from a Bay-area psychiatric facility in September of 1998. Burt Hadley, manager at the Discount Inn, who had contact with Shelby on several occasions, said he was "polite, but weird, forgetful."

Warren said that local police have been questioning local residents to establish if they had any contact with Shelby. He also said that they are hard at work trying to put a name to their possible victim. "The documents [recovered] from Shelby's room suggest some type of revenge killing. So we think the victim's name or picture may be found in the other materials."

SPECIAL FEATURES

- IFC Interview with Writer/Director Christopher Nolan
- Theatrical Trailer and TV Spot
- "Following" Trailer
- Tattoo Gallery
- Director & Cast Biographies
- Interactive Motion Menus
- Scene Selections
- Memento Website

COLUMBIA TRISTAR HOME ENTERTAINMENT PRESENTS A SUMMIT ENTERTAINMENT / TEAM TODD FILM
GUY PEARCE CARRIE ANNE MOSS JOE PANTOLIANO MEMENTO DAVID JULYAN GINNY EVANS DODDY DORN
CASTING BY PATTI PODESTA COSTUME DESIGNER JIMMY HALLYL PRODUCED BY JENNIFER TODD SUZANNE TODD
SCREENPLAY BY JONATHAN LINDOFF DIRECTED BY CHRISTOPHER NOLAN

Running Time Approx. 113 Minutes
10202 W. Washington Blvd., Culver City, California 90232-3195

06598
DVD

MEMENTO

SOME MEMORIES ARE BEST FORGOTTEN

Labels: SAINT, THE FACTS, LOVE, HEY LEONARD, VICTIM, FRIEND, Do not trust her, MEMENTO, SADIST, ALLY, LIAR, FAKER, USER, GUY PEARCE, MARKO, DADD, DADD, WHITE 5'7, 6'2" BLONDE, MUTE/REST INN ON 5th ST, ROOM 6, TEDDY, PUT HIM ONT R/D, OR JUST PUT NATALIE ON HIM, 414 BUNTS.

Memprint: Stream of Memory Usage

10568 KB

15976 KB

49380 KB

65948 KB

11632 KB

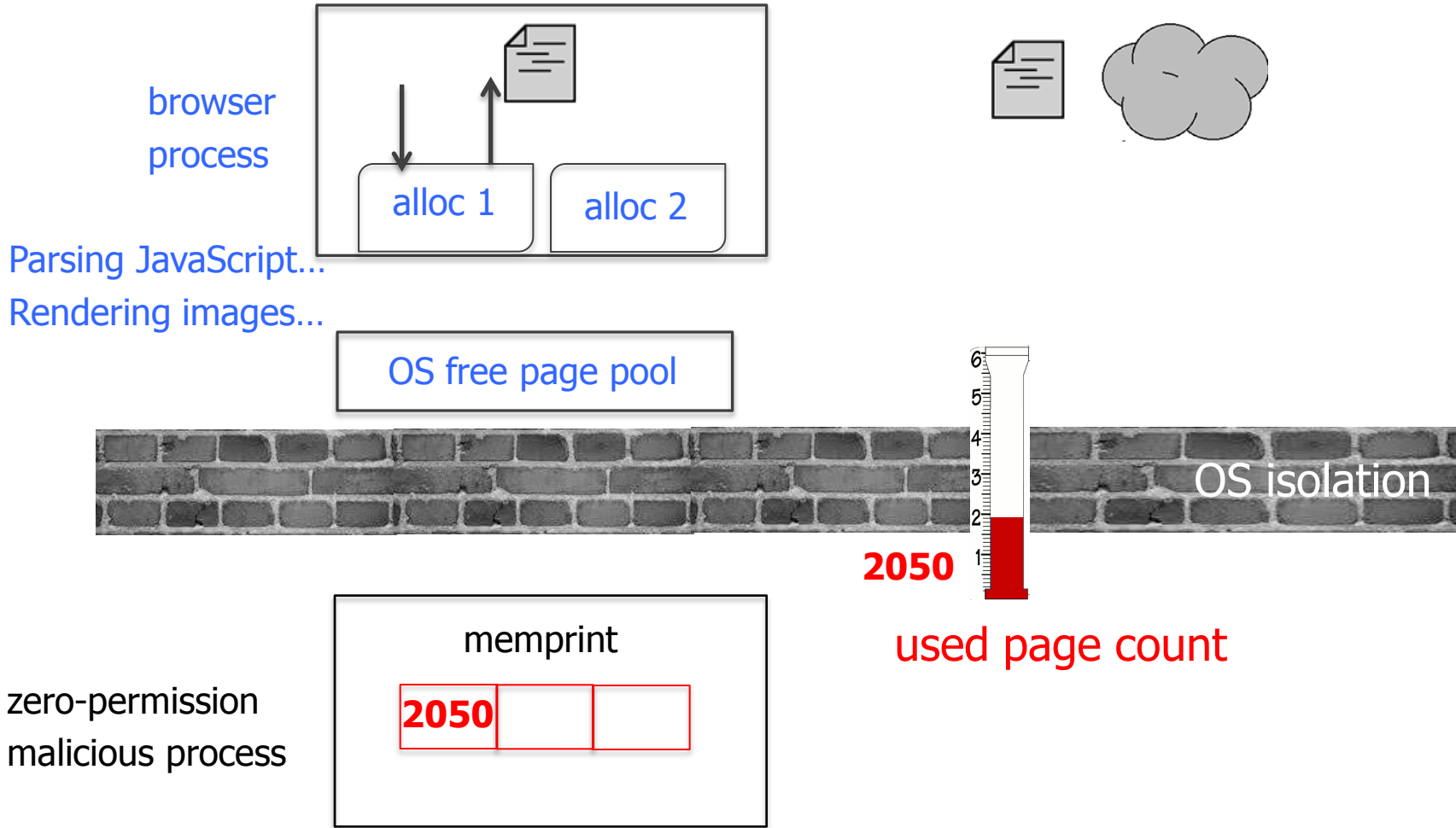
48996 KB

60280 KB

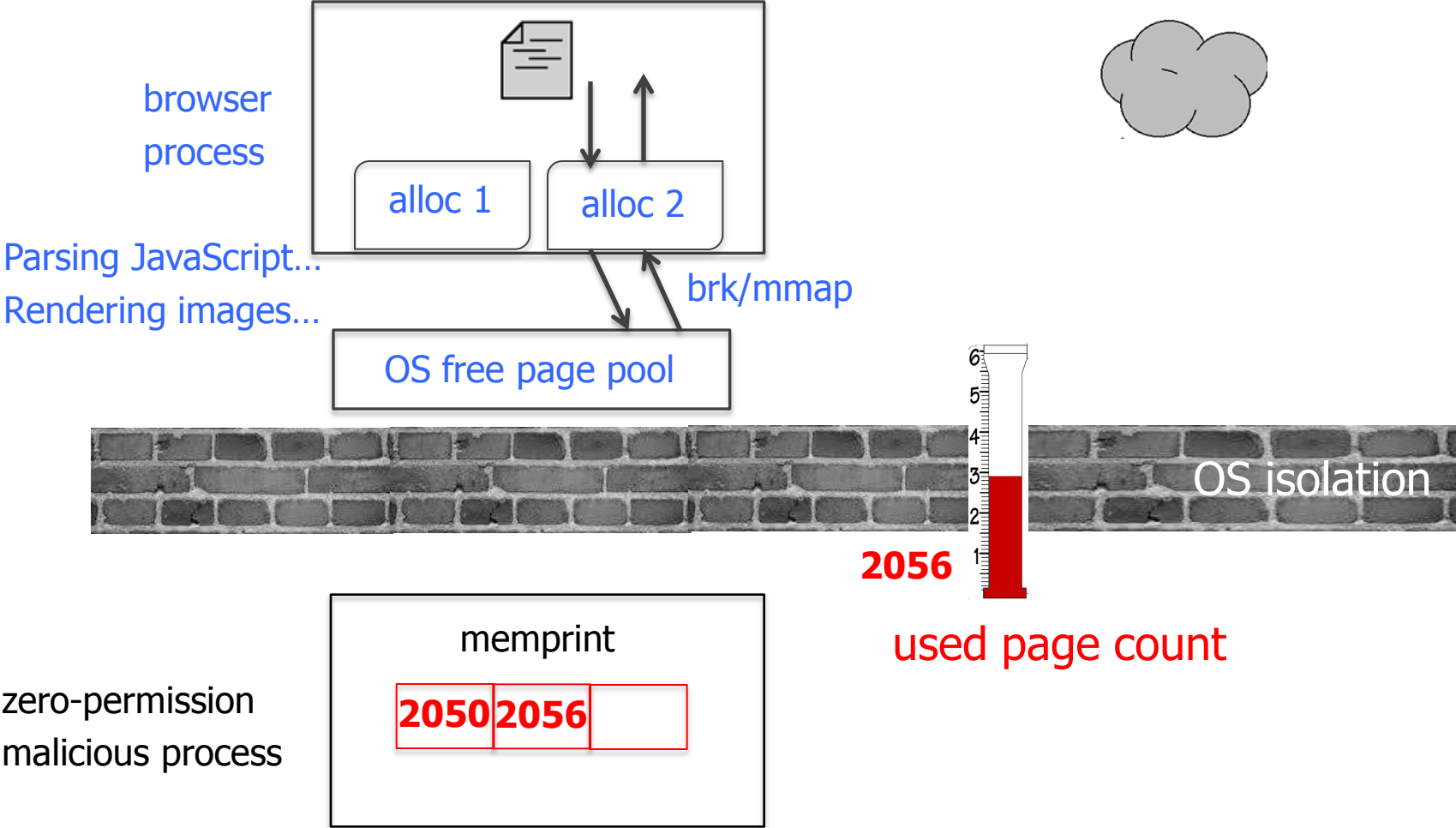
60820 KB

59548 KB

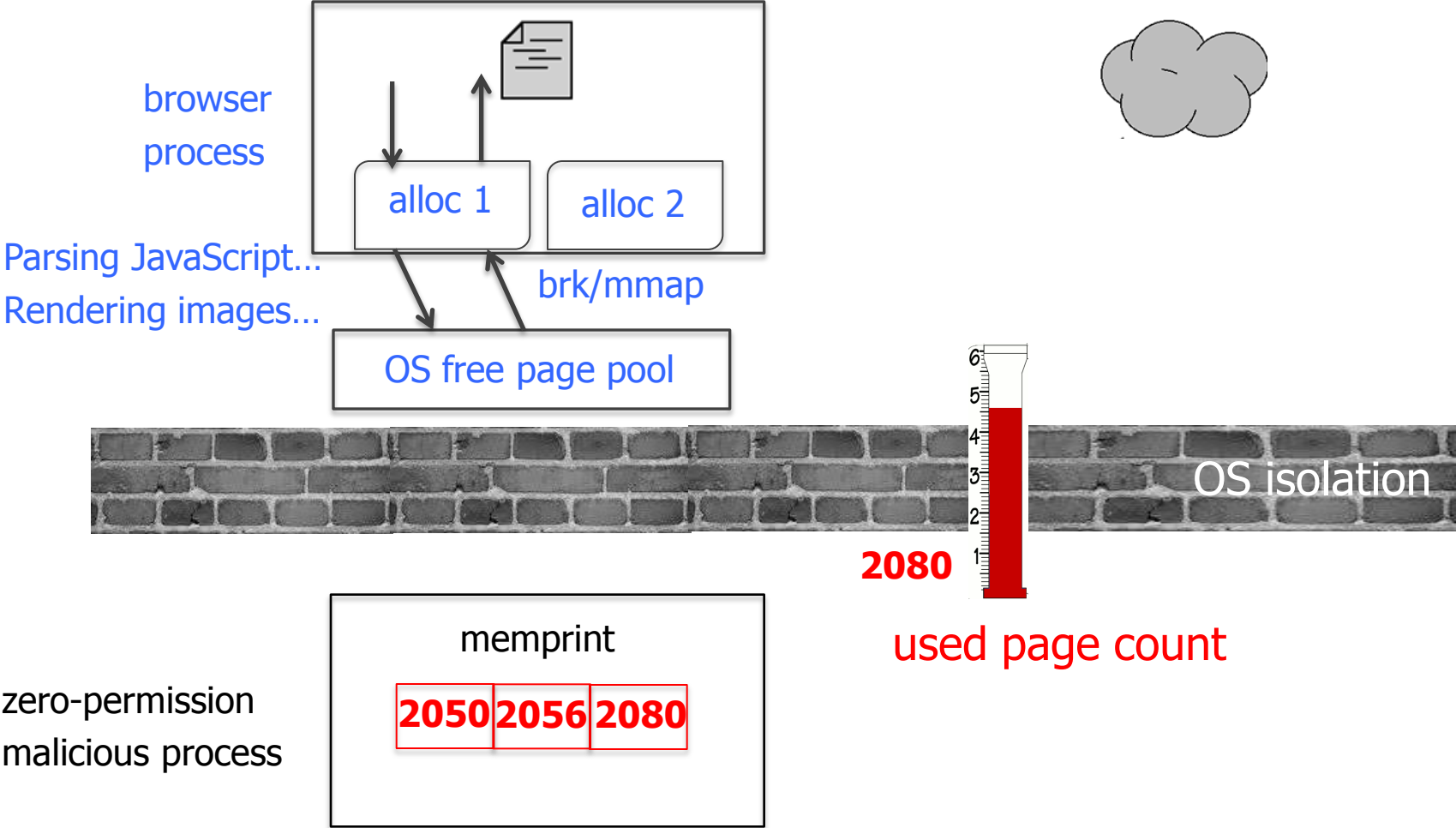
Sniffing Memory Footprints



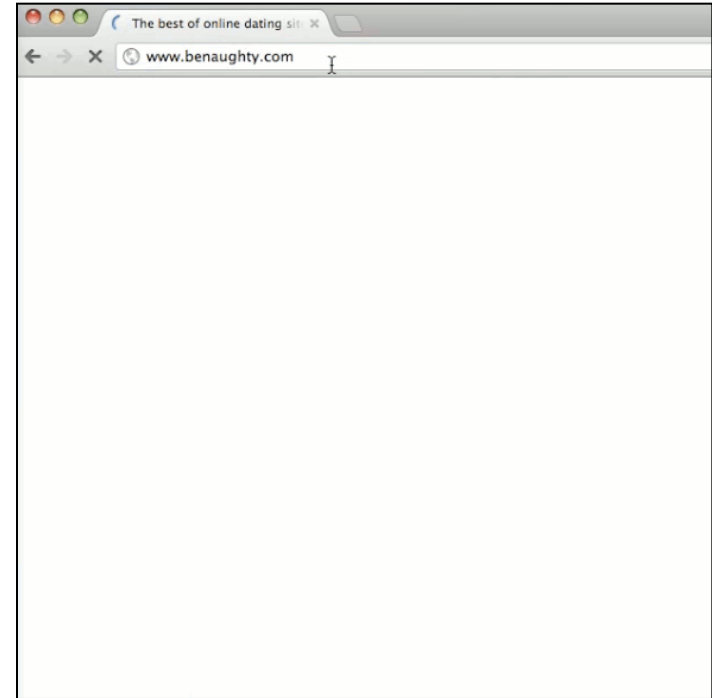
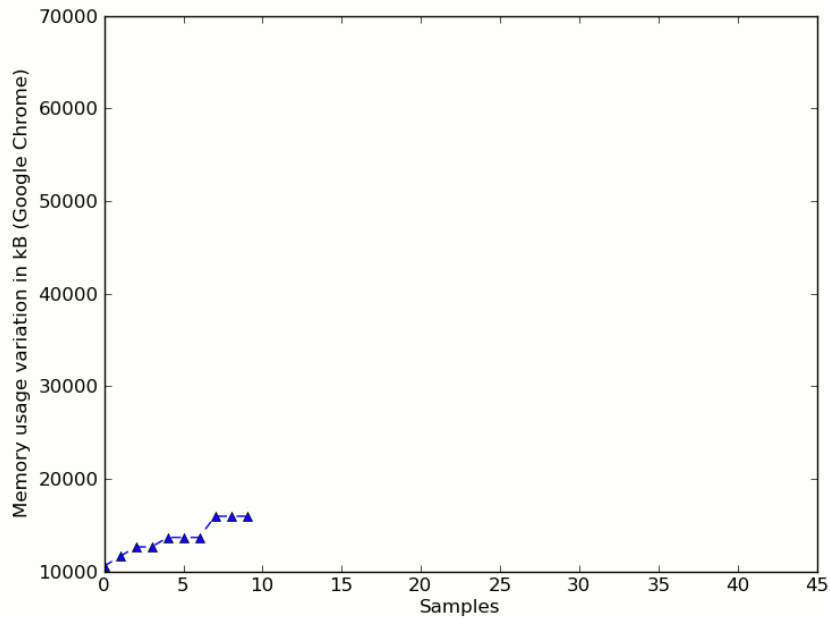
Sniffing Memory Footprints



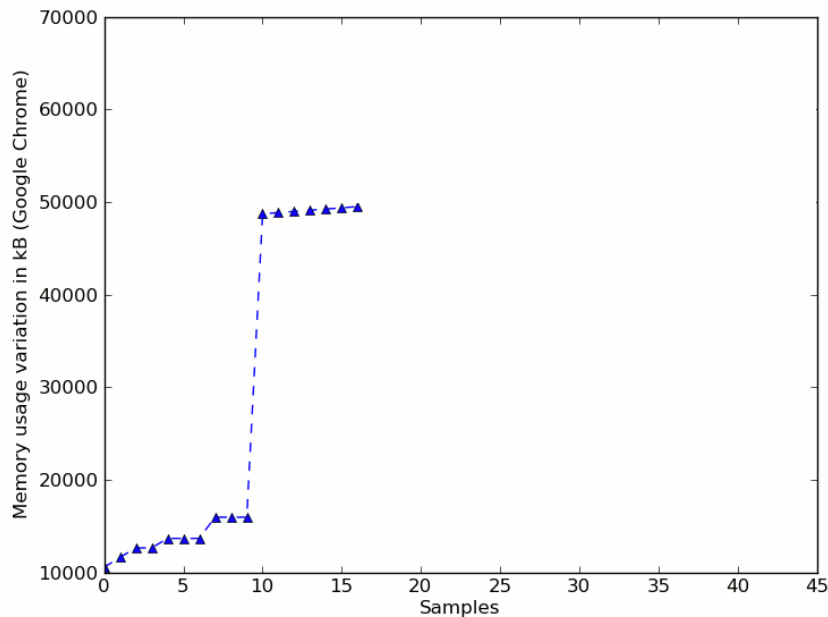
Sniffing Memory Footprints



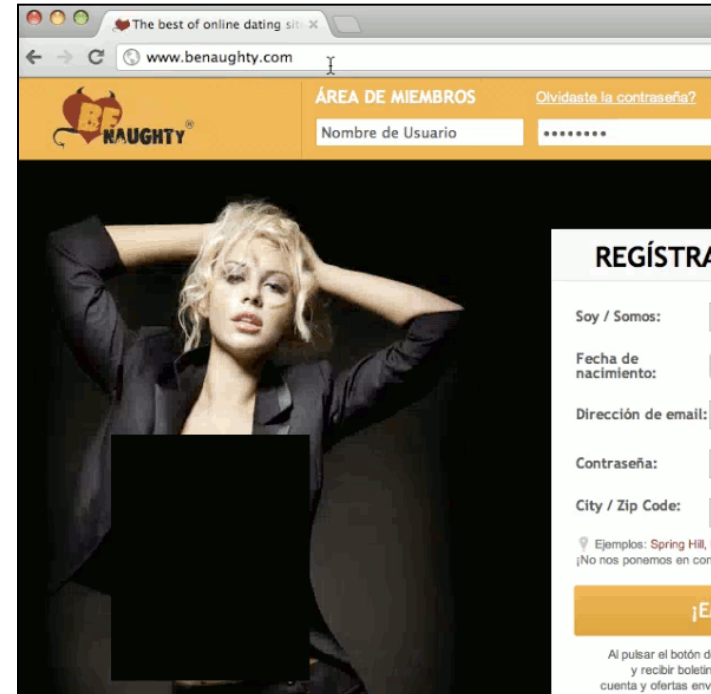
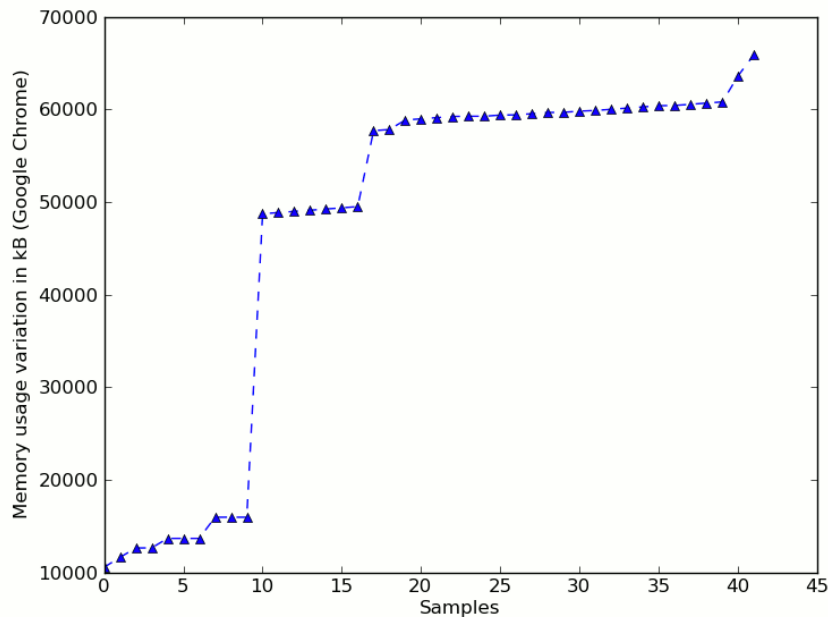
Loading BeNaughty.com in Chrome



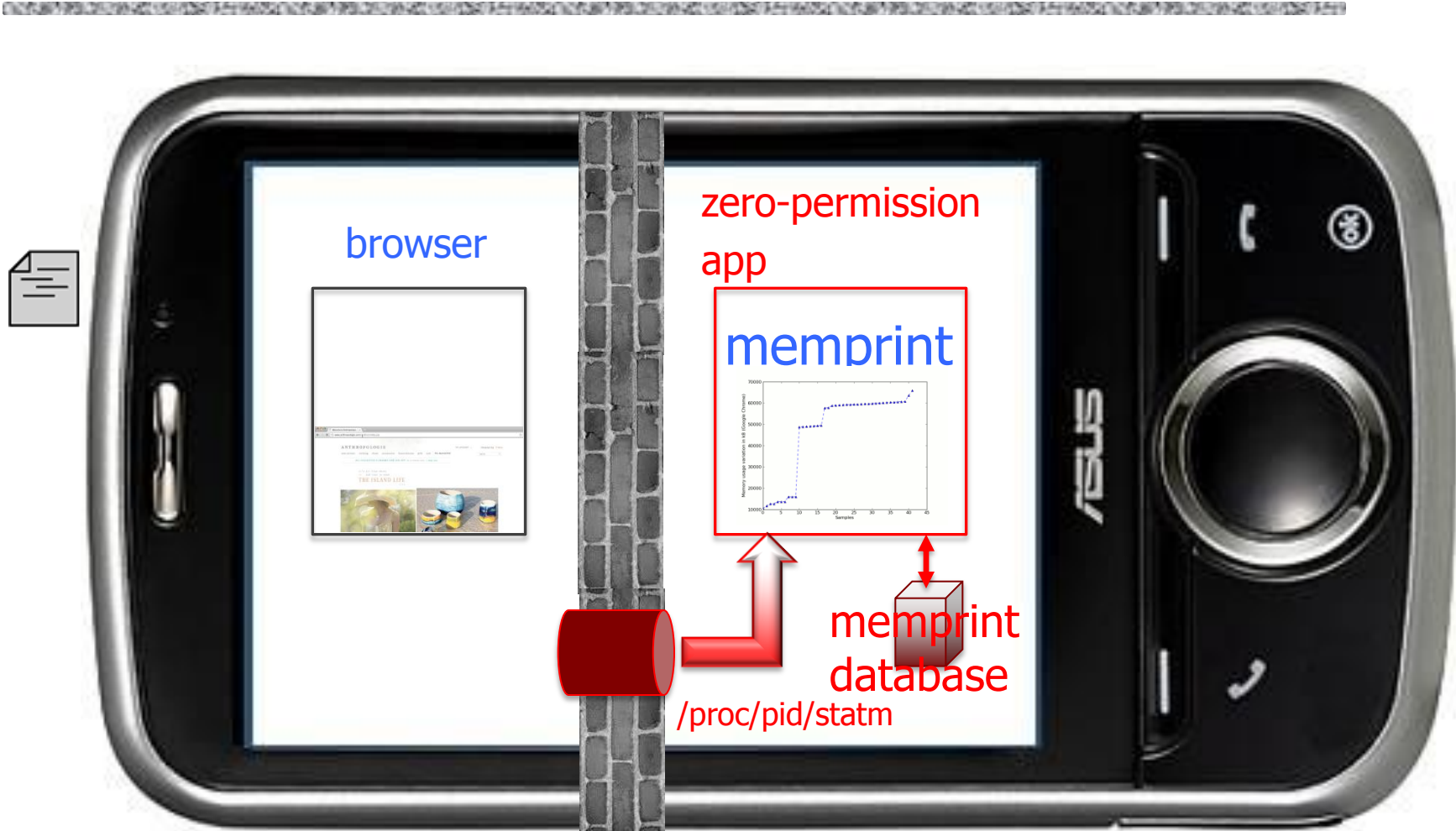
Loading BeNaughty.com in Chrome



Loading BeNaughty.com in Chrome



Full Attack

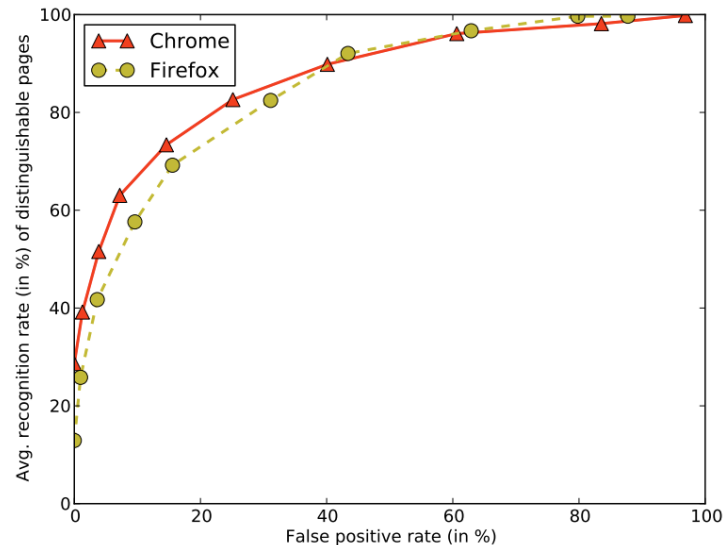


OS isolation

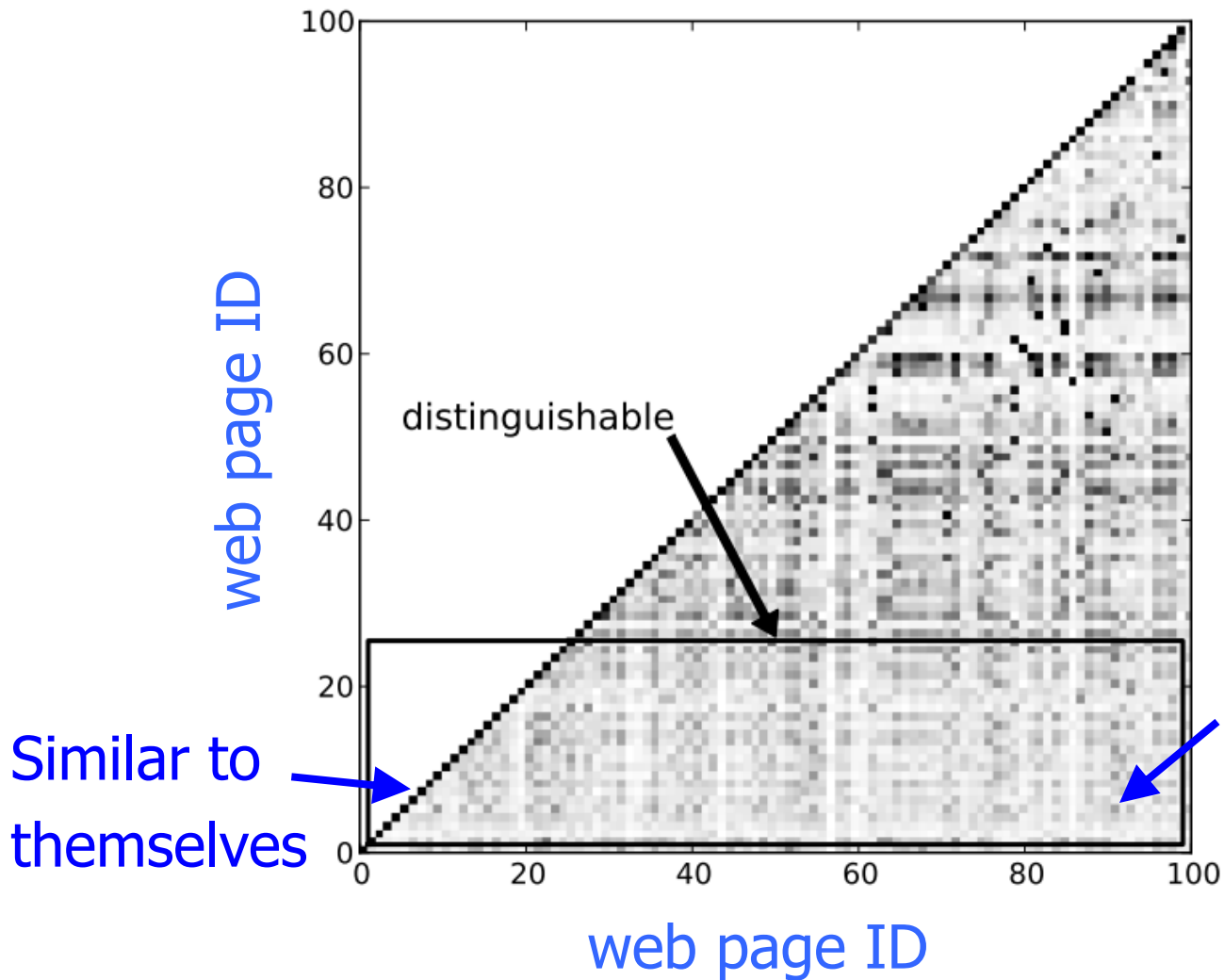
Why the Attack Works

- ◆ Memprints are **unique** - for up to 43% of Alexa top 100,000 pages
 - Can tune recognition to achieve zero false positives
- ◆ Memprints are **stable** across repeated visits to the same page

memprints are
OS/browser-
dependent but
machine-
independent



Cross-Page Similarity



similarity =
Jaccard index
of memprints

Other Privacy Leaks

- ◆ Fine-grained memory dynamics reveal membership in dating sites, interest in medical conditions, etc.
- ◆ Dynamics of CPU scheduling reveal individual keystrokes
- ◆ General problem: **fine-grained resource usage statistics are correlated with secrets**
 - These statistics are visible across isolation boundary
 - Their dynamics are a high-bandwidth side channel