We thought we had this stuff figured out back in the 1970s. What went wrong?

Jerome H. Saltzer, MIT
<Saltzer@mit.edu>

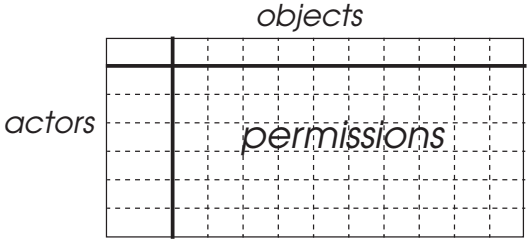
ISSSE 2006

What I'm planning to say…

- What we thought we knew
- What happened next (*PC's and the Internet*)
- What went wrong (*neglect of complete mediation*)
- What happened in UNIX (*buffer overflows*)
- What went wrong (*neglect of complete mediation*)
- Analysis: Why? (*more trouble ahead…*)

Two models

- Discretionary



- Mandatory

Read:

$level_{classification} \leq level_{clearance}$

$hwm \leftarrow \text{MAX}\ (hwm, level_{classification})$

Write:

$level_{classification} \geq level_{hwm}$

(where hwm is a high-water mark)

1278 PROCEEDINGS OF THE IEEE, VOL. 63, NO. 9, SEPTEMBER 1975

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

Invited Paper

Progress report…

√ What we thought we knew

⇒ What happened next
(*PC's and the Internet*)

- What went wrong
(*neglect of complete mediation*)
- What happened in UNIX
(*buffer overflows*)
- What went wrong
(*neglect of complete mediation*)
- Analysis: Why?
(*more trouble ahead…*)

BugTraq Mode: Threaded Go

Expand all | Post message

(Page 1 of 552) 1 2 3 4 5 6 7 8 9 10 11 Next >

- Virex on-access scanning unreliable 2006-02-28
hahn math hu-berlin de
- Mozilla Thunderbird : Multiple Information Disclosure Vulnerabilities 2006-02-28
Renaud Lifchitz (r lifchitz sysdream com)
- [security bulletin] SSRT061118 rev.1 - HP System Management Homepage (SMH) Running on Windows: Remote Unauthorized Access 2006-02-28
security-alert hp com
- (PHP) mb_send_mail security bypass 2006-02-28
ced clerget free fr
- (PHP) imap functions bypass safemode and open_basedir restrictions 2006-02-28
ced clerget free fr
- MyBB 1.3 NewSQL Injection 2006-02-28
o y 6 hotmail com
- QwikiWiki v1.4 XSS Vulnerability 2006-02-28
drdeath_2006 linuxmail org
- EJ3 TOPo - Cross Site Scripting Vulnerability 2006-02-28
mail yunusemreyilmaz com
- FarsiNews 2.5Pro Exploit 2006-02-28
hessamx hessamx net
- Fedex Kinkos Smart Card Authentication Bypass 2006-02-28
Lance James (bugtraq securescience net)

Complete Mediation

Always ask three questions…

1. Authentication:
Who made the request?

2. Integrity:
Has anyone tampered with it?

3. Authorization:
Is this request permitted?

Why was this design principle, which is so fundamental to security, neglected?

Why was this design principle, which is so fundamental to security, neglected?

1. Rapid rise of the PC

2. Rapid rise of the Internet

3. Government interference

next…

√ What we thought we knew

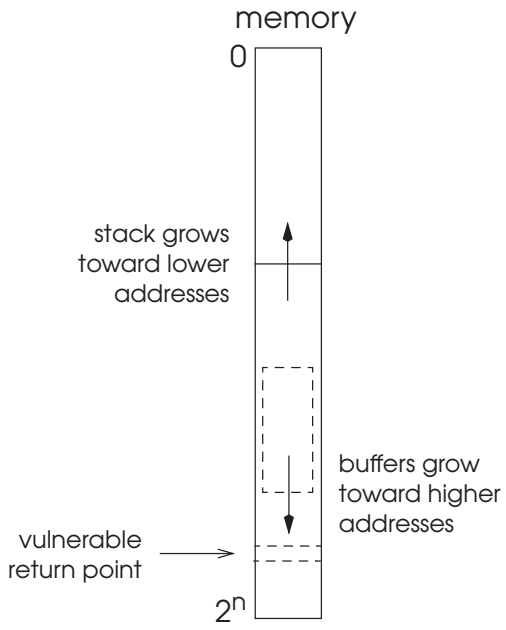
√ What happened next
(*PC's and the Internet*)

√ What went wrong
(*neglect of complete mediation*)

⇒ What happened in UNIX
(*buffer overflows*)

- What went wrong
(*neglect of complete mediation*)
- Analysis: Why?
(*more trouble ahead…*)

Buffer overflow exploitation



next…

√ What we thought we knew

√ What happened next
(*PC's and the Internet*)

√ What went wrong
(*neglect of complete mediation*)

√ What happened in UNIX
(*buffer overflows*)

⇒ What went wrong
(*neglect of complete mediation*)

- Analysis: Why?
(*more trouble ahead…*)

Return instruction:

load *program_counter* **from** *return_point*;

Complete Mediation

Always ask three questions…

1. Authentication:
Who made the request?

2. Integrity:
Has anyone tampered with it?

3. Authorization:
Is this request permitted?

next…

√ What we thought we knew

√ What happened next
(*PC's and the Internet*)

√ What went wrong
(*neglect of complete mediation*)

√ What happened in UNIX
(*buffer overflows*)

√ What went wrong
(*neglect of complete mediation*)

⇒ Analysis: Why?
(*more trouble ahead…*)

The future…

Is security going to improve?

The future…

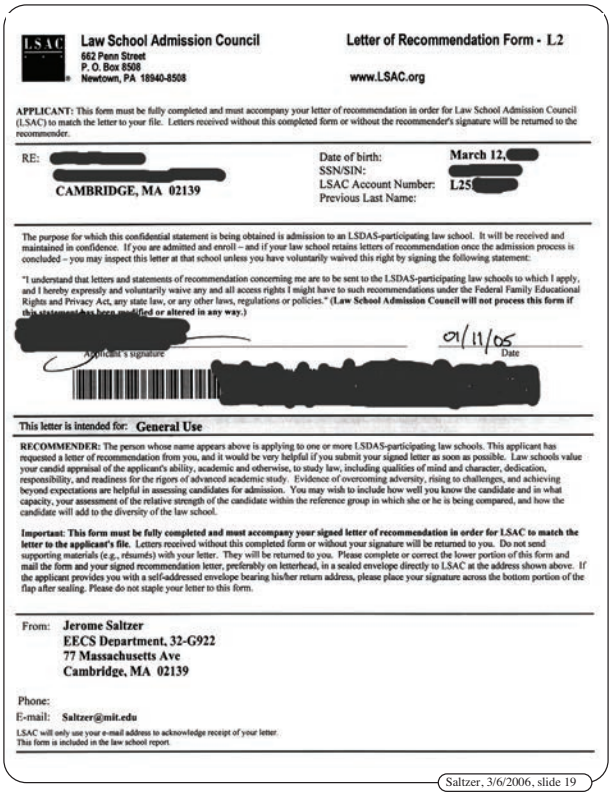
Is security going to improve?

No!

1. Technology change:

   $$\frac{d(technology)}{dt}$$ is too large!

2. Can't keep up with all of the elves.



Law School Admission Council
662 Penn Street
P. O. Box 8508
Newtown, PA 18940-8508

Letter of Recommendation Form - L2

www.LSAC.org

APPLICANT: This form must be fully completed and must accompany your letter of recommendation in order for Law School Admission Council (LSAC) to match the letter to your file. Letters received without this completed form or without the recommender's signature will be returned to the recommender.

RE: [redacted]
[redacted]
CAMBRIDGE, MA 02139

Date of birth: March 12, [redacted]
SSN/SIN: [redacted]
LSAC Account Number: L25[redacted]
Previous Last Name:

The purpose for which this confidential statement is being obtained is admission to an LSDAS-participating law school. It will be received and maintained in confidence. If you are admitted and enroll – and if your law school retains letters of recommendation once the admission process is concluded – you may inspect this letter at that school unless you have voluntarily waived this right by signing the following statement:

"I understand that letters and statements of recommendation concerning me are to be sent to the LSDAS-participating law schools to which I apply, and I hereby expressly and voluntarily waive any and all access rights I might have to such recommendations under the Federal Family Educational Rights and Privacy Act, any state law, or any other laws, regulations or policies." **(Law School Admission Council will not process this form if this statement has been modified or altered in any way.)**

[redacted] 01/11/05
Applicant's signature Date

[redacted]

This letter is intended for: **General Use**

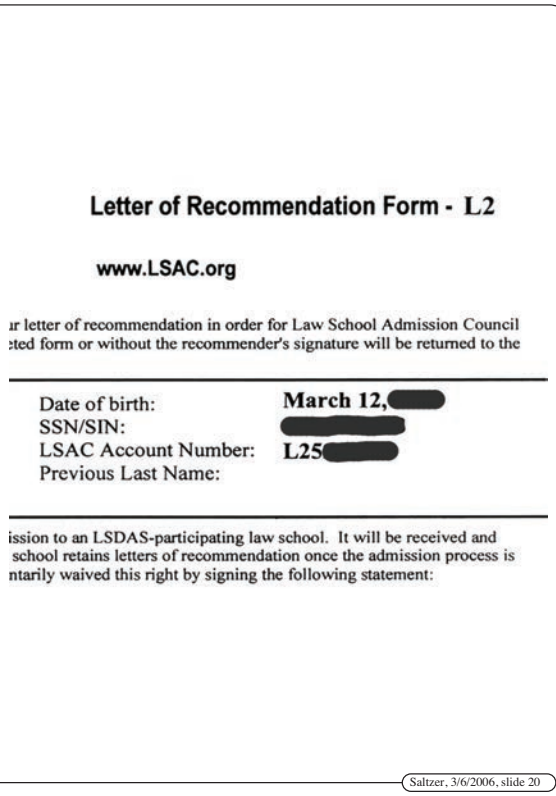
RECOMMENDER: The person whose name appears above is applying to one or more LSDAS-participating law schools. This applicant has requested a letter of recommendation from you, and it would be very helpful if you submit your signed letter as soon as possible. Law schools value your candid appraisal of the applicant's ability, academic and otherwise, to study law, including qualities of mind and character, dedication, responsibility, and readiness for the rigors of advanced academic study. Evidence of overcoming adversity, rising to challenges, and achieving beyond expectations are helpful in assessing candidates for admission. You may wish to include how well you know the candidate and in what capacity, your assessment of the relative strength of the candidate within the reference group in which she or he is being compared, and how the candidate will add to the diversity of the law school.

Important: This form must be fully completed and must accompany your signed letter of recommendation in order for LSAC to match the letter to the applicant's file. Letters received without this completed form or without your signature will be returned to you. Do not send supporting materials (e.g., résumés) with your letter. They will be returned to you. Please complete or correct the lower portion of this form and mail the form and your signed recommendation letter, preferably on letterhead, in a sealed envelope directly to LSAC at the address shown above. If the applicant provides you with a self-addressed envelope bearing his/her return address, please place your signature across the bottom portion of the flap after sealing. Please do not staple your letter to this form.

From: **Jerome Saltzer**
EECS Department, 32-G922
77 Massachusetts Ave
Cambridge, MA 02139

Phone:
E-mail: **Saltzer@mit.edu**

LSAC will only use your e-mail address to acknowledge receipt of your letter.
This form is included in the law school report.



Letter of Recommendation Form - L2

www.LSAC.org

ır letter of recommendation in order for Law School Admission Council
ted form or without the recommender's signature will be returned to the

Date of birth: **March 12,** [redacted]
SSN/SIN: [redacted]
LSAC Account Number: **L25**[redacted]
Previous Last Name:

ission to an LSDAS-participating law school. It will be received and
school retains letters of recommendation once the admission process is
ntarily waived this right by signing the following statement:

The real security challenge:

How do you keep people from doing stupid things?