CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenture

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DiGi ONE
the leading digital company

ICT CYBER CONSULTING

Weaknesses

Enrico Russo

Andrea Valenza

Università di Genova

enrico.russo@unige.it

andrea.valenza@dibris.unige.it

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline

- Confused Deputy
  - SetUID/SetGID
- Race Conditions
  - TOCTOU Race Conditions

© CINI – 2020

Outline

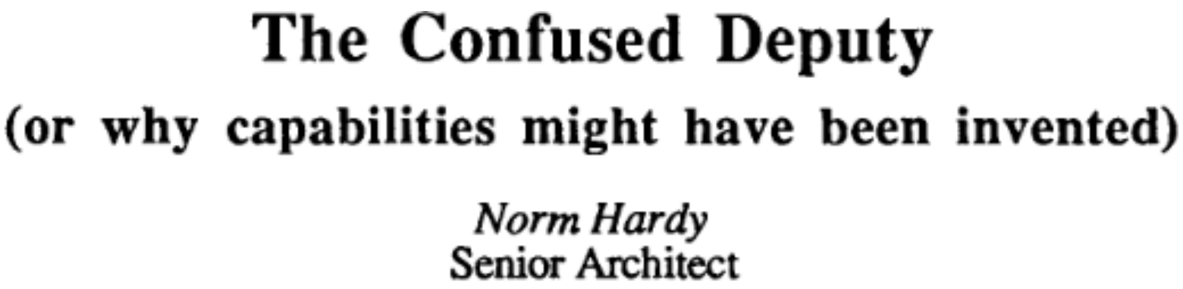
- Confused Deputy
  - SetUID/SetGID
- Race Conditions
  - TOCTOU Race Conditions

© CINI – 2020

Confused Deputy

- A specific type of Privilege escalation
- Exploits the Access Control List (ACL) model
  - Capability based systems are not affected

Original example



The Confused Deputy

(or why capabilities might have been invented)

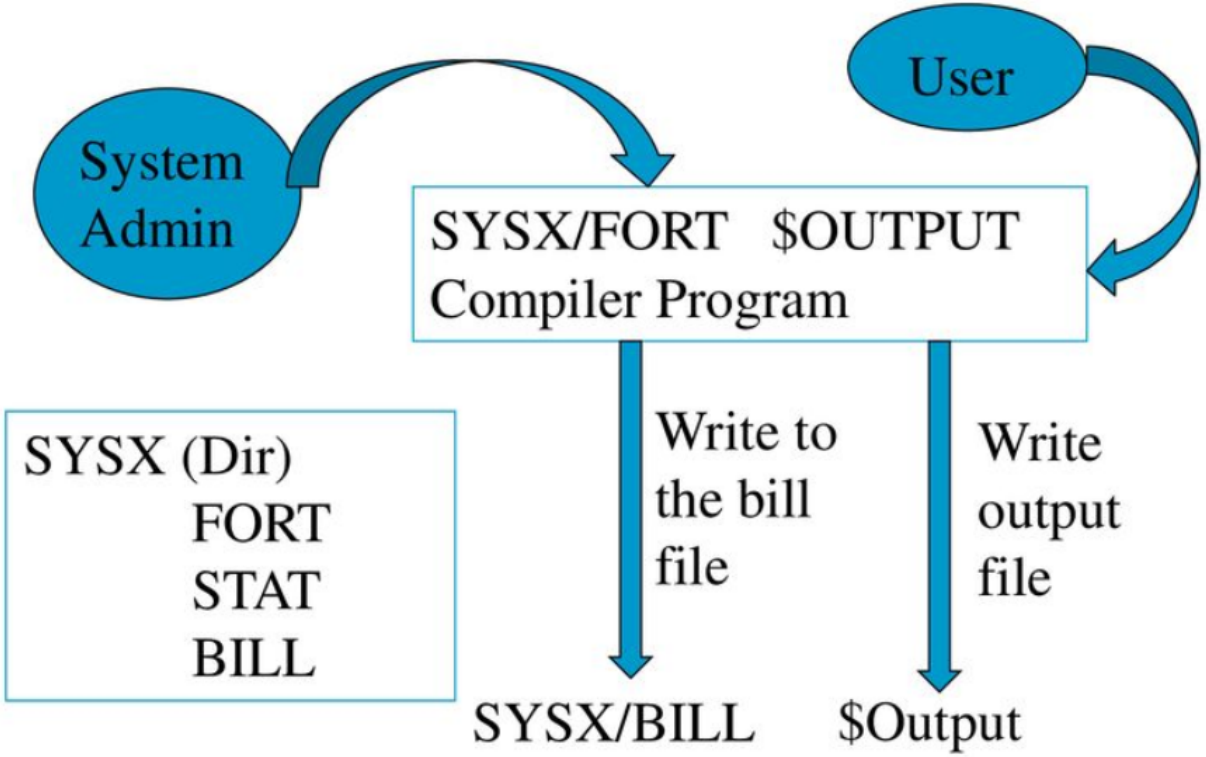
Norm Hardy
Senior Architect

https://zoo.cs.yale.edu/classes/cs422/2010/bib/hardy88confused.pdf

Original example

- A program provides compilation services to other programs
- The compiler service is pay-per-use: the compiler service stores billing information a BILL file
- Only the program has access to BILL.

Original example

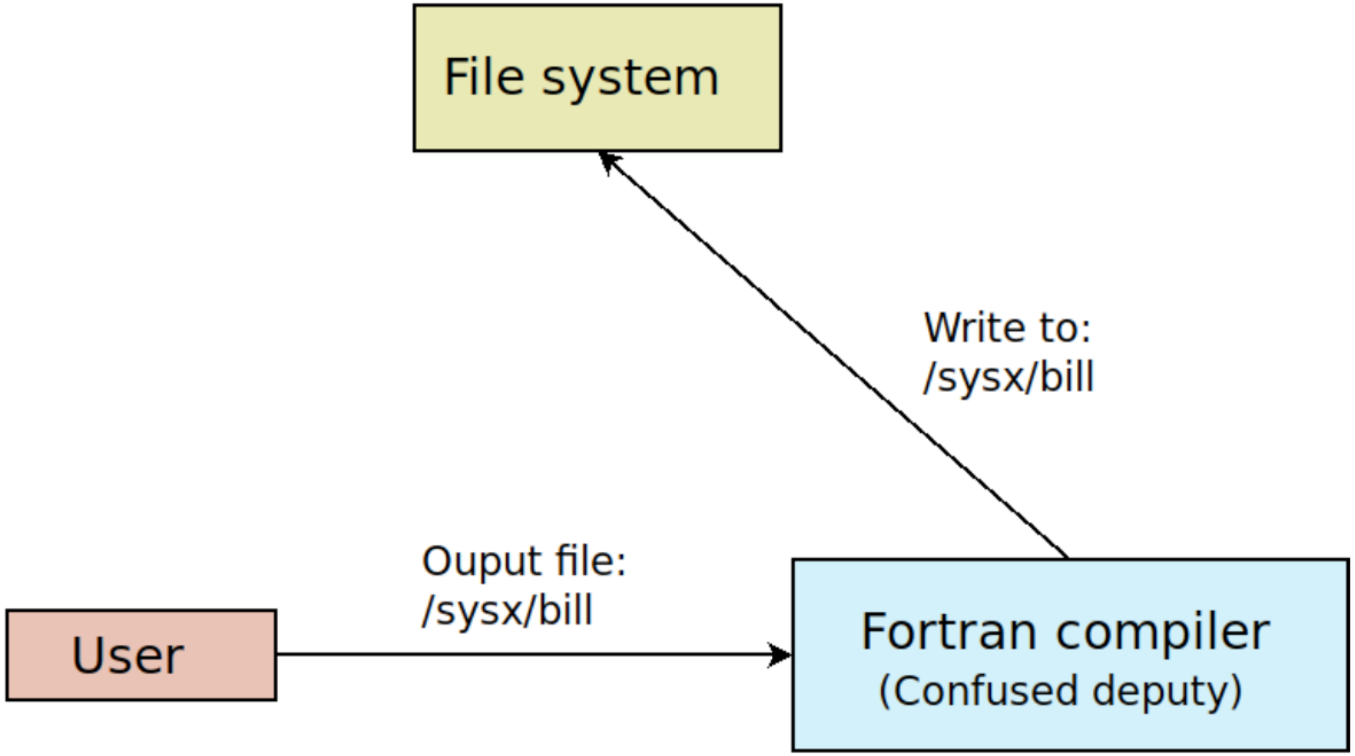


Original example

- Clients can compile and set the output file name
- A malicious client calls the output BILL
- Clients cannot open BILL, but the program can
- The program overwrites the BILL file with the compilation output

© CINI – 2020

Original example



Protection against Confused Deputy

- Use capability based systems
  - Access Control List based systems are ineffective

Outline

- Confused Deputy
  - SetUID/SetGID
- Race Conditions
  - TOCTOU Race Conditions

SetUID/SetGID

- Open SetUID programs let users run as the owner
- If the program is vulnerable, users can run arbitrary commands as the owner
- The program should only offer the right capabilities
  - E.g., only running predefined commands

Outline

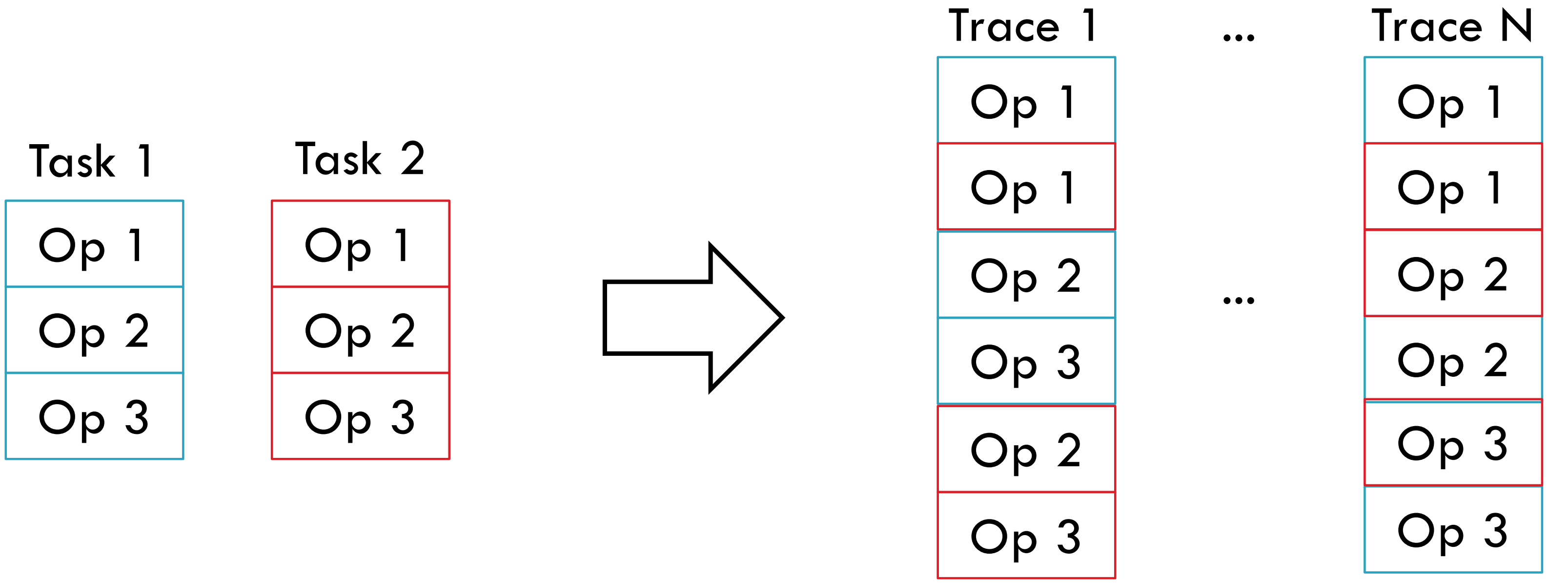
- Confused Deputy
  - SetUID/SetGID
- Race Conditions
  - TOCTOU Race Conditions

© CINI – 2020

Race Conditions

- Concurrency
  - Execution of multiple control flows (e.g., threads)
  - Can lead to non-deterministic behavior
- Race conditions
  - Software can change the intended instruction order
    - E.g., two processes try to write the same file

Race Conditions



Task 1

Op 1

Op 2

Op 3

Task 2

Op 1

Op 2

Op 3

Trace 1

Op 1

Op 1

Op 2

Op 3

Op 2

Op 3

…

…

Trace N

Op 1

Op 1

Op 2

Op 2

Op 3

Op 3

One of the N traces at random
(depending on the scheduler)

Properties for race conditions

- Concurrency property
  - Two (or more) concurrent control flows
- Shared object property
  - Concurrent control flows access a shared *race object*
- Change state property
  - At least one flow alters the state of the *race object*

© CINI – 2020

Race window

- Code segment that accesses the race object in an insecure way
  - Also called *critical section*
- Traditional approach
  - Never overlap critical sections (mutual exclusion)
  - Synchronization primitives (SP)
- Misusing SPs may lead to deadlock

© CINI – 2020

Outline

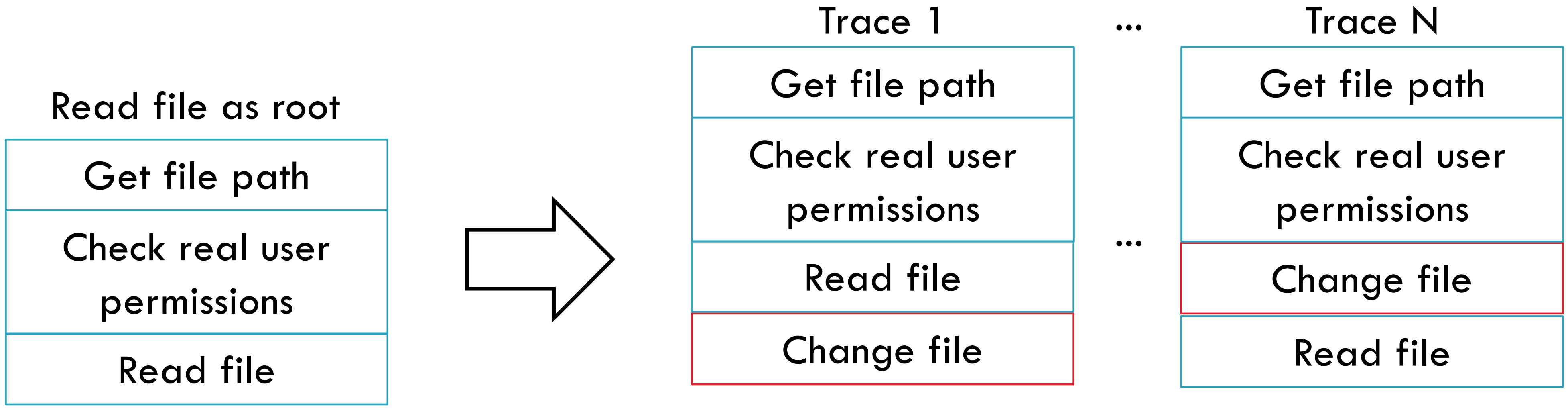
- Confused Deputy
  - SetUID/SetGID
- Race Conditions
  - Time of Check, Time of Use

Time of Check, Time of Use

- Creates a race window by
  - First *checking* the race object
  - Then *using* the race object
- Concurrent operations can fit between checking and using

© CINI – 2020

Time of Check, Time of Use



Read file as root

- Get file path
- Check real user permissions
- Read file

Trace 1

- Get file path
- Check real user permissions
- Read file
- Change file

…

…

Trace N

- Get file path
- Check real user permissions
- Change file
- Read file

Run multiple times concurrently to get the trace you want (i.e., the one that triggers the vulnerability)

TOCTOU

- How can I change a file? “Get file path” passed already
  - Create a symbolic link to a valid file A
  - Make the program read the symbolic link path
  - Change the symbolic link to point to file B
  - The program returns the content of file B

Weaknesses

Enrico Russo

Andrea Valenza

Università di Genova

enrico.russo@unige.it

andrea.valenza@dibris.unige.it

https://cybersecnatlab.it

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenture

aizoOn
AUSTRALIA
EUROPE
USA
TECHNOLOGY CONSULTING

B5

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DaTa
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DiGi ONE
the leading digital company

ICT CYBER CONSULTING