Тенденции развития технологий защиты и анализа программного кода

Тихонов А.Ю.

- Цель доклада – очертить круг вопросов для организации обсуждения вообще и на данной секции в частности

«хакерские» конференции

- PHDays
- ZeroNights
- recon (recon.cn)
- black hat briefings (есть версия специально для федеральных служб США). Июль 2013 - выступление директора АНБ
- DEF CON

Круг вопросов:

- Поиск уязвимостей – пентестинг (penetration testing – тестирование на проникновение)
- Поиск уязвимостей – анализ ПО
- Анализ вредоносного кода
- Защита от анализа
- Разработка инструментария для вышеперечисленного

На фоне академических работ – уровень крайне низкий даже для зарубежных конференций

«академические» конференции

- USENIX
- Conference on Software Engineering
- Network and Distributed System Security Symposium
- IEEE Security and Privacy Symposium
- Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)
- Programming Language Design and Implementation (PLDI)
- International Symposium on Software Testing and Analysis (ISSTA)
- …

«академические» проекты

- Klee (http://***klee***.*llvm.org*) – Stanford Univ.
- BitBlaze (http://bitblaze.cs.berkeley.edu) – Berkeley Univ.
- BAP (http://www.cylab.cmu.edu) – CyLab: Carnegie Mellon Univ. (RnD-лаборатория АНБ – одна из 50+). На базе BAP - Mayhem
- S2E (http://dslab.epfl.ch/proj/s2e)
- Sage – Microsoft (http://research.microsoft.com/en-us/um/people/pg/)

SMT-солверы:

- STP (https://sites.google.com/site/stpfastprover/)
- Z3 (http://z3.codeplex.com/)
- Boolector (http://fmv.jku.at/boolector/)
- …

Две стратегии решения задачи поиска дефектов/уязв.:

1. «выявление всех ошибок» - формальная верификация: построить формальную модель корректного (безопасного) поведения программы и формально доказать соответствие программной реализации и модели. Работающих подходов нет, поэтому другая стратегия:

2. «выявление каких-нибудь ошибок» - самые разные подходы, развитие которых когда-нибудь должно привести к решению в формулировке 1

Сложность и стоимость задачи верификации (1)

- единственное известное на данный момент формально верифицированное на отсутствие ошибок (не уязвимостей!) микроядро – ОС L4.
- Исполнитель работы – одно из подразделений NICTA Group. По окончании работы подразделение было сразу же поглощено фирмой General Dynamics.
- При верификации математически доказано соответствие реализации модели и отсутствие ряда классов ошибок, таких как взаимоблокировки, переполнение буфера, вечные циклы, использование неинициализированных переменных.
- Размер верифицированного кода составил **8700** строк СИ-кода и 600 строк ассемблера. Количество составленных и доказанных теорем превышает **200000**, при этом выявлено 144 программных дефекта.
- Стоимость проекта составила порядка $87млн, продолжительность проекта – 7 лет, трудоемкость – 25 человеко-лет.

- [seL4: Formal Verification of an OS Kernel/Gervin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harwey Tuch, Simon Winwood/NICTA, UNSW, Open Kernel Labs, ANU/22nd ACM Symposium on Operating System Principles, October 2009]

Carnegie Mellon University
CyLab

Search | Portal Login

RESEARCH | EDUCATION | PARTNERSHIP | OUTREACH | NEWS & EVENTS | ABOUT CYLAB | QUICK LINKS

ABOUT CyLab

CARNEGIE MELLON CYLAB is a bold and visionary effort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy, and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cybercitizens of all ages.

Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves more than 50 faculty and 100 graduate students from more than six different departments and schools.

CyLab provides technology resources and expertise in four areas:

1. **Technology transfer to and from the public sector**
2. **Technology transfer to and from the private sector**
3. **Development of Information Assurance professionals**
4. **National awareness programs and tools**

FAST facts

CyLab was founded in 2003 and is one of the largest university-based cybersecurity research and education centers in the U.S. Here are some quick facts - CyLab is:

- A National Science Foundation (NSF) CyberTrust Center
- Affiliated with CERT, at the Software Engineering Institute
- A key partner in NSF-funded Center for Team Research in Ubiquitous Secure Technology
- A National Security Agency (NSA) Center of Academic Excellence in Information Assurance Education and a Center for Academic Excellence in Research

CyLab Researchers Work To Make Commercial Technologies Secure For Defense Department

posted by Nichole Dwyer
November 11, 2013

Researchers from Carnegie Mellon University CyLab and the University of Pennsylvania have received a four-year, $3.9 million grant from the Defense Advanced Research Projects Agency (DARPA) to improve the security of commercial technologies used by the military.

Researchers from Carnegie Mellon University CyLab and the University of Pennsylvania have received a four-year, $3.9 million grant from the Defense Advanced Research Projects Agency (DARPA) to improve the security of commercial technologies used by the military.

"We are studying how to improve the security for commercial-off-the-shelf (COTS) technology that remains vulnerable to attack from latent vulnerabilities or hidden malicious codes," said CyLab researcher **David Brumley**, the Gerard G. Elia Career Development Professor in the Department of Electrical and Computer Engineering. Brumley is widely regarded for his cutting-edge contributions to addressing the challenges associated with malware.

Brumley along with CyLab Director **Virgil Gligor**, a CMU professor of electrical and computer engineering, will analyze each COTS system, such as wireless routers and printers, and make certain they are malice-free.

"COTS consists of complex stacks where a weakness at any level can endanger the entire system," said Brumley, a faculty adviser for CMU's award-winning "Capture the Flag" team. "Capture the Flag" is a computer security game in which each team competes to find a key source of information by solving challenging problems.

The COTS technology challenge is important to the Defense Department because it buys and uses commercial technologies for everything from information technologies to retrofitting the F-15E Fighter with new digital video recording equipment.

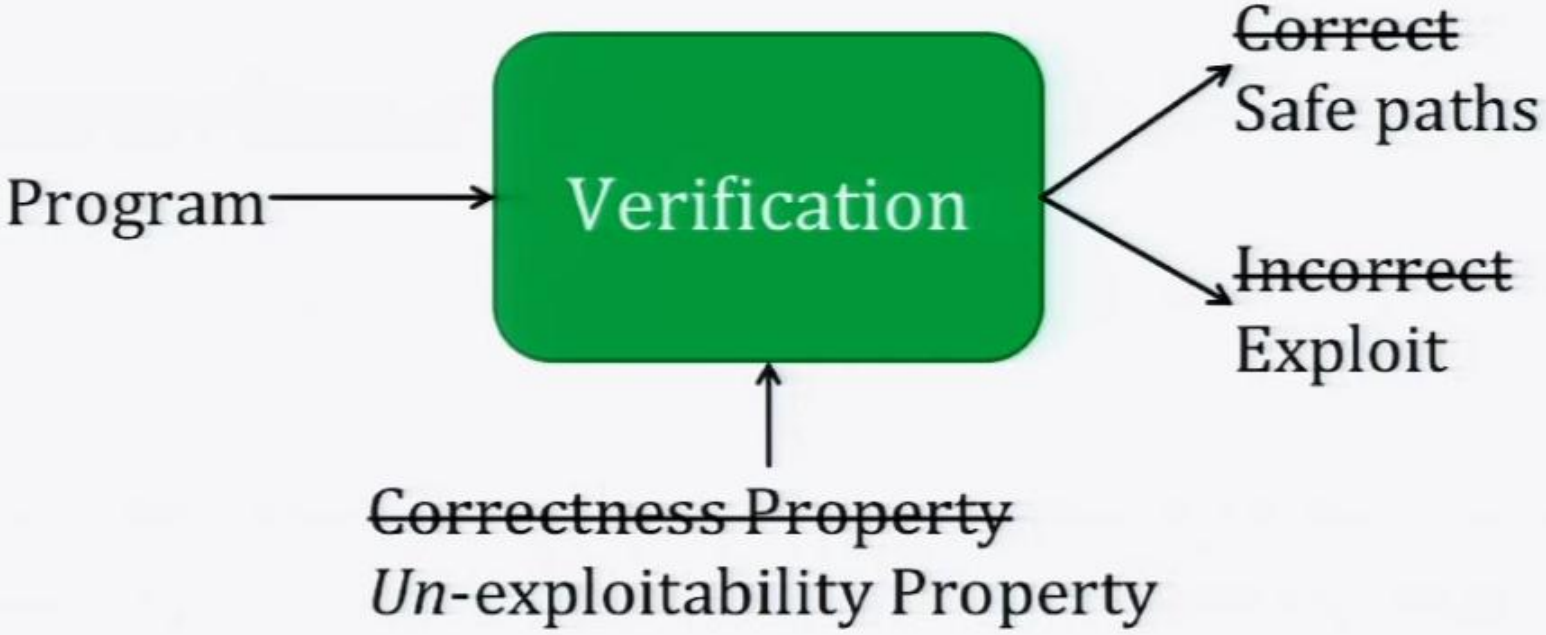
CMU researchers report that plugging such devices into the network can significantly harm overall security.

Funding:

Core Security
DARPA
Google
Lockheed Martin
Northrop Grumman
NSA
NSF
SEI

Carnegie Mellon University
CyLab

Verification, but with a twist



Carnegie Mellon University
CyLab

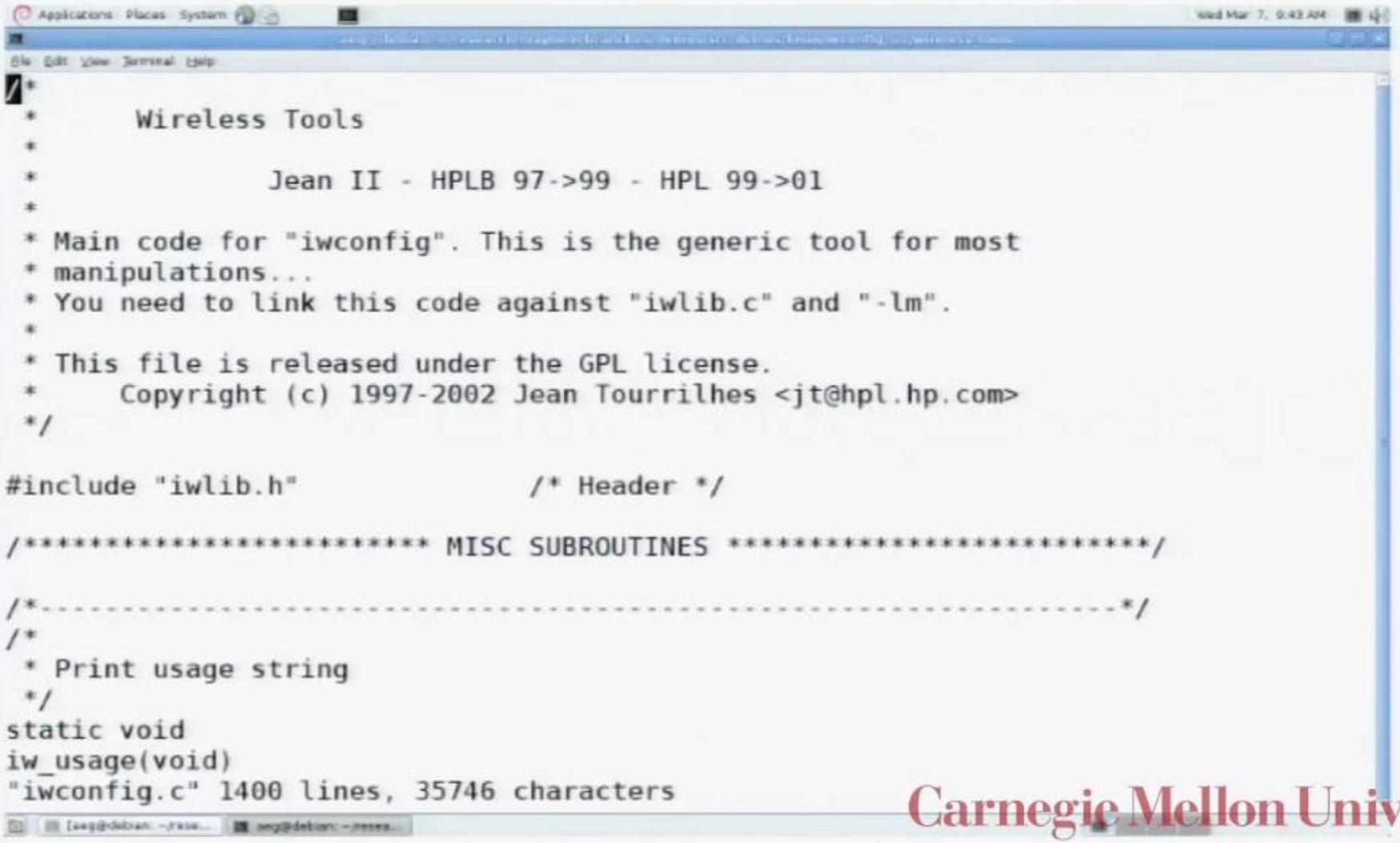
Automatic Exploit Generation with Mayhem

March 7, 2012

Carnegie Mellon University
CyLab

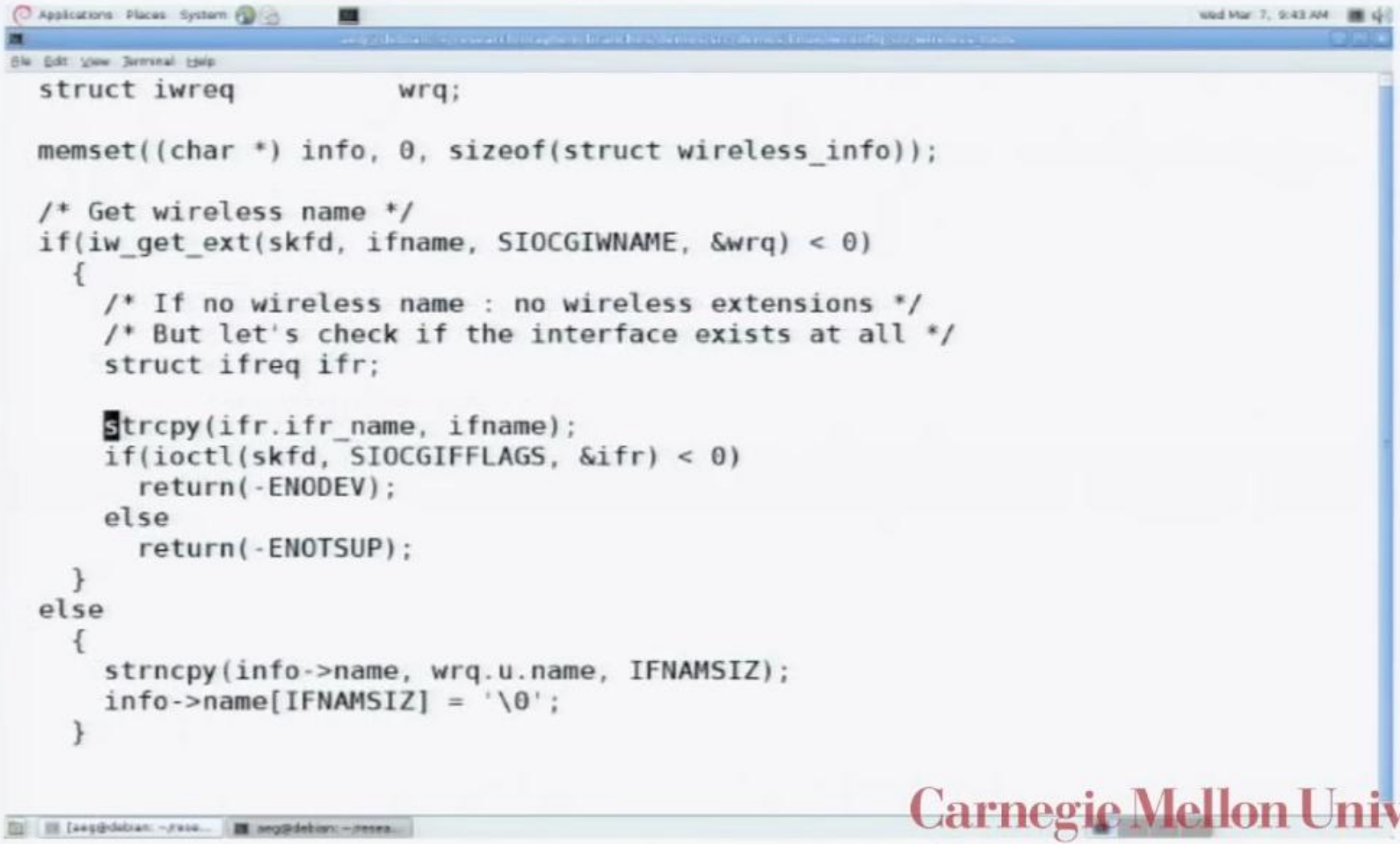
Carnegie Mellon University

CyLab



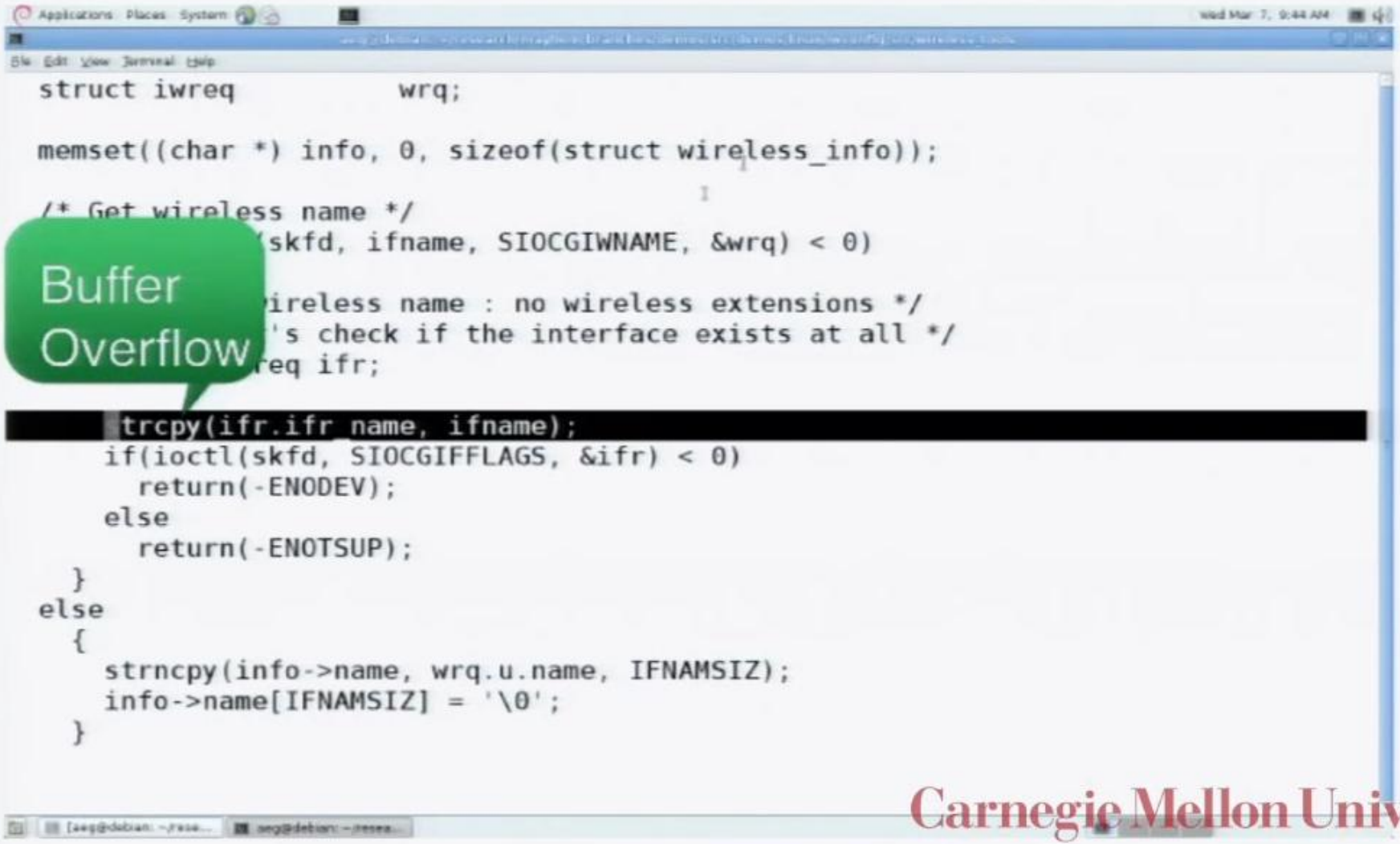
Carnegie Mellon University

CyLab



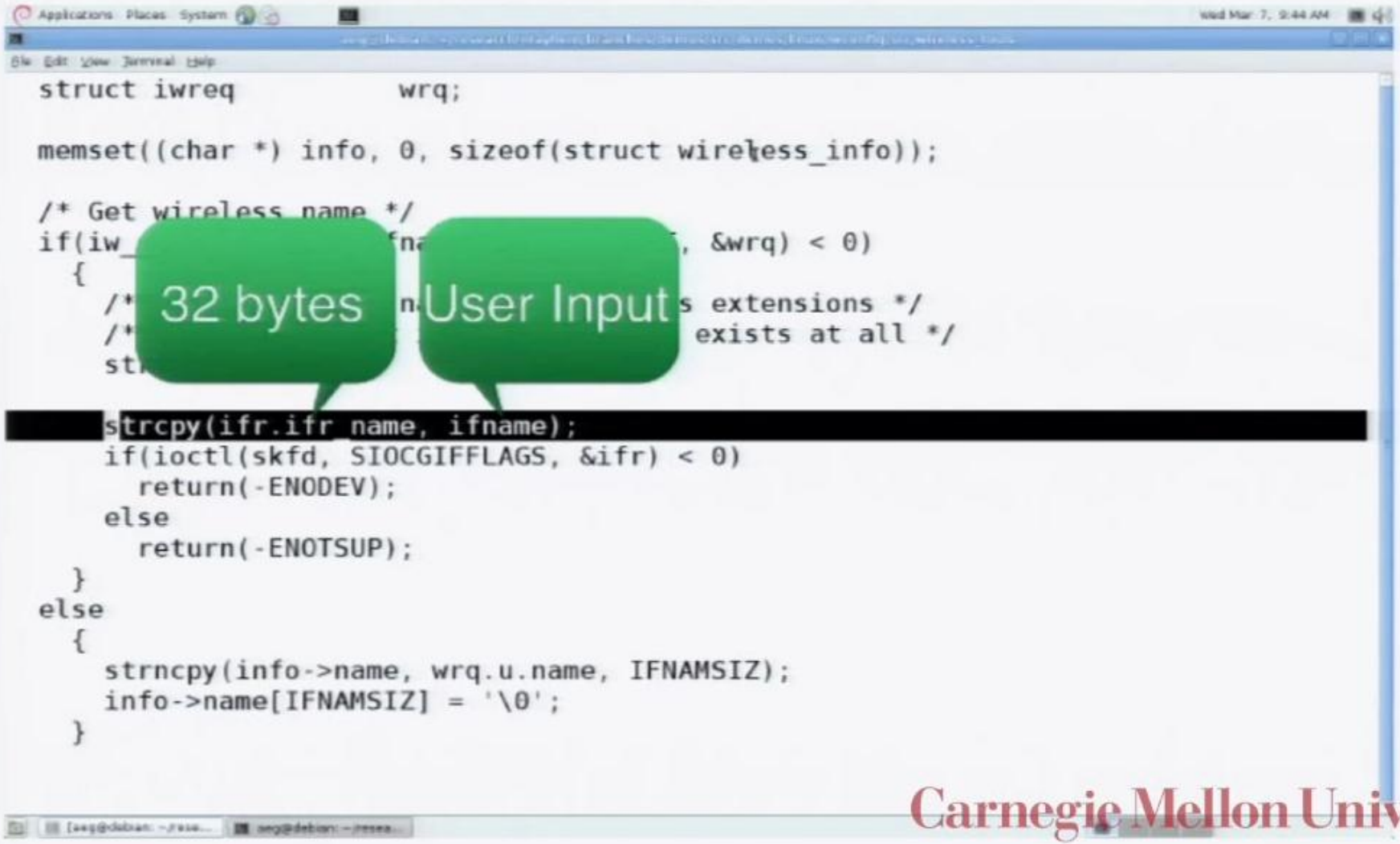
Carnegie Mellon University

CyLab



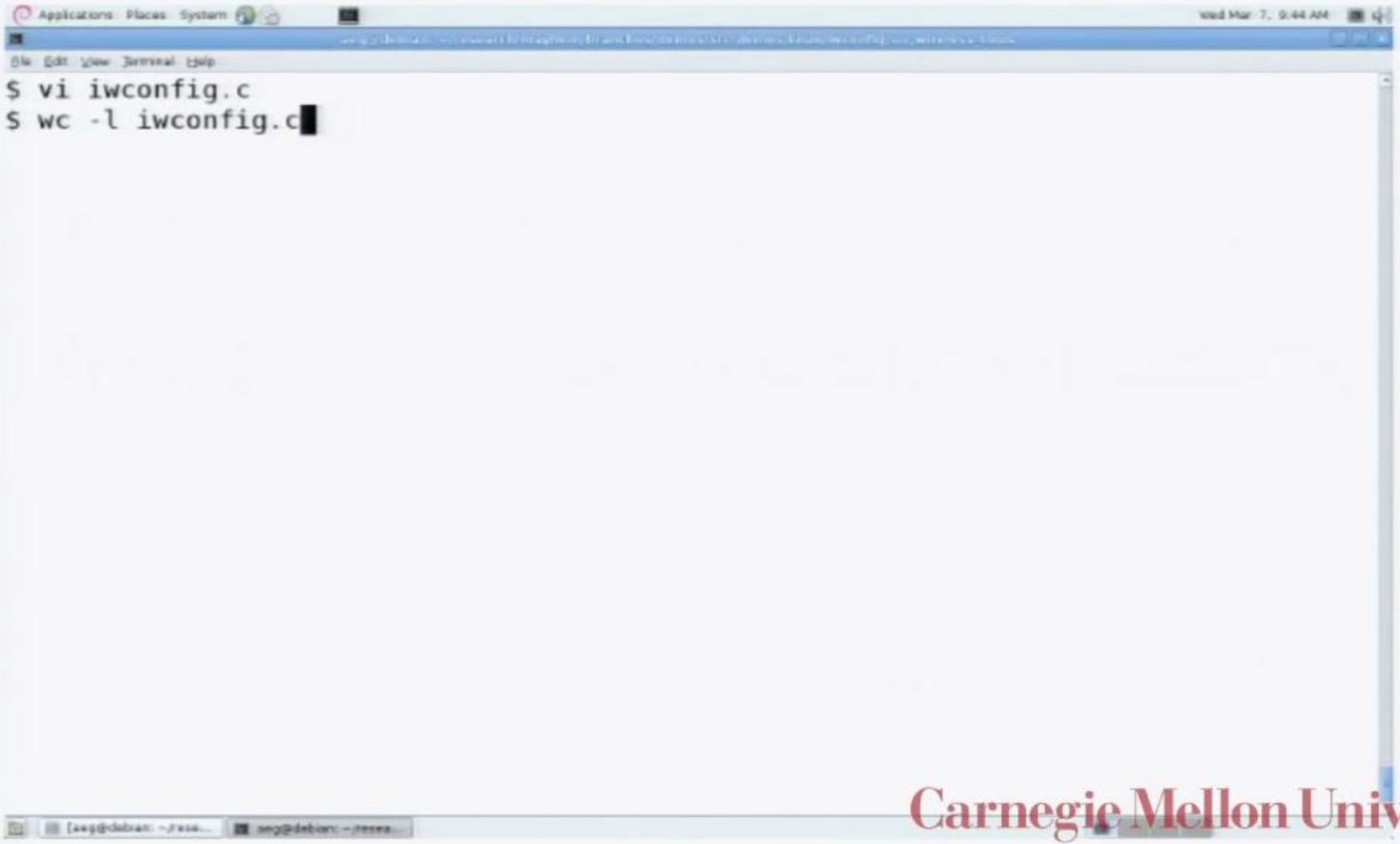
Carnegie Mellon University

CyLab



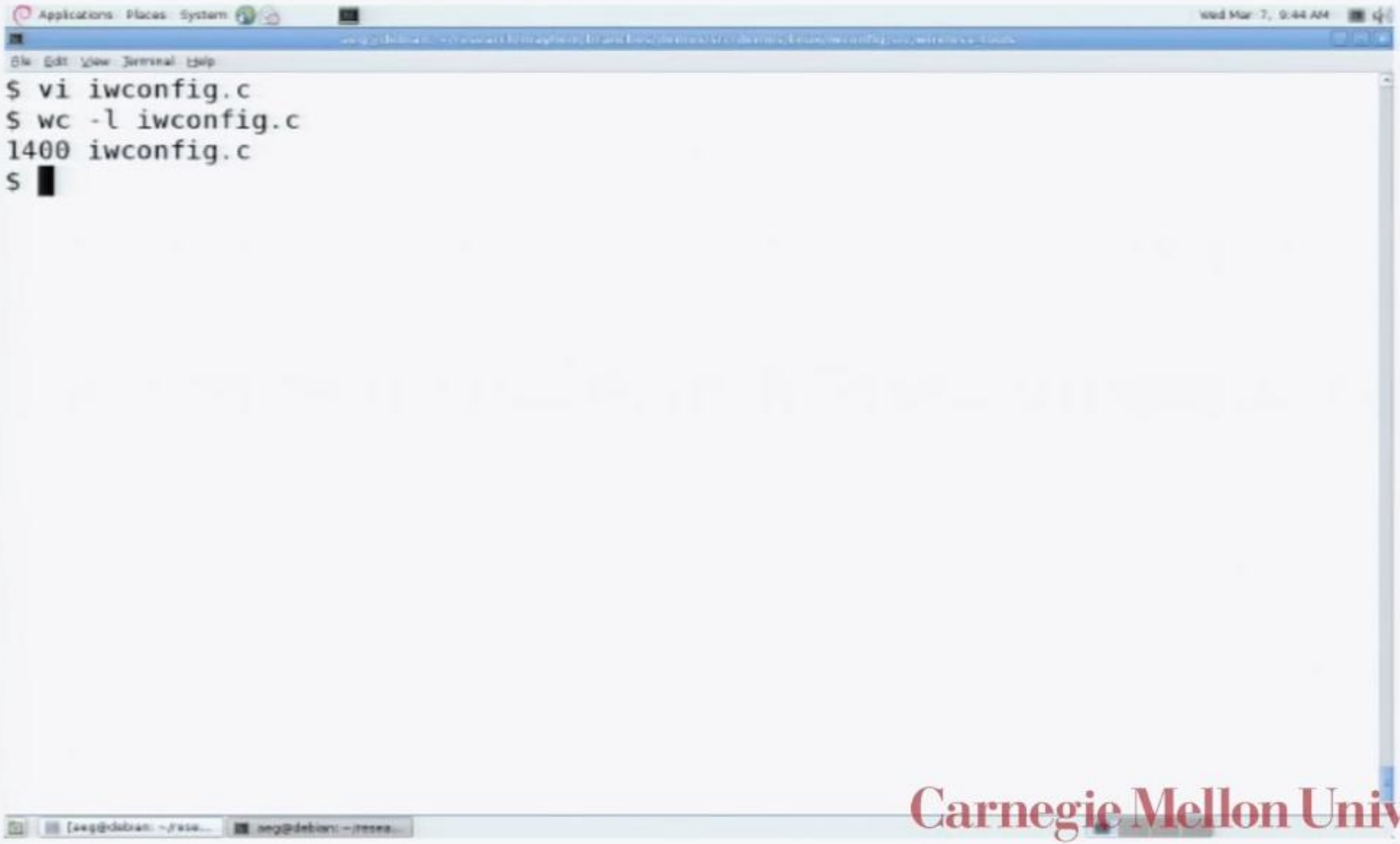
Carnegie Mellon University

CyLab



Carnegie Mellon University

CyLab



Carnegie Mellon University

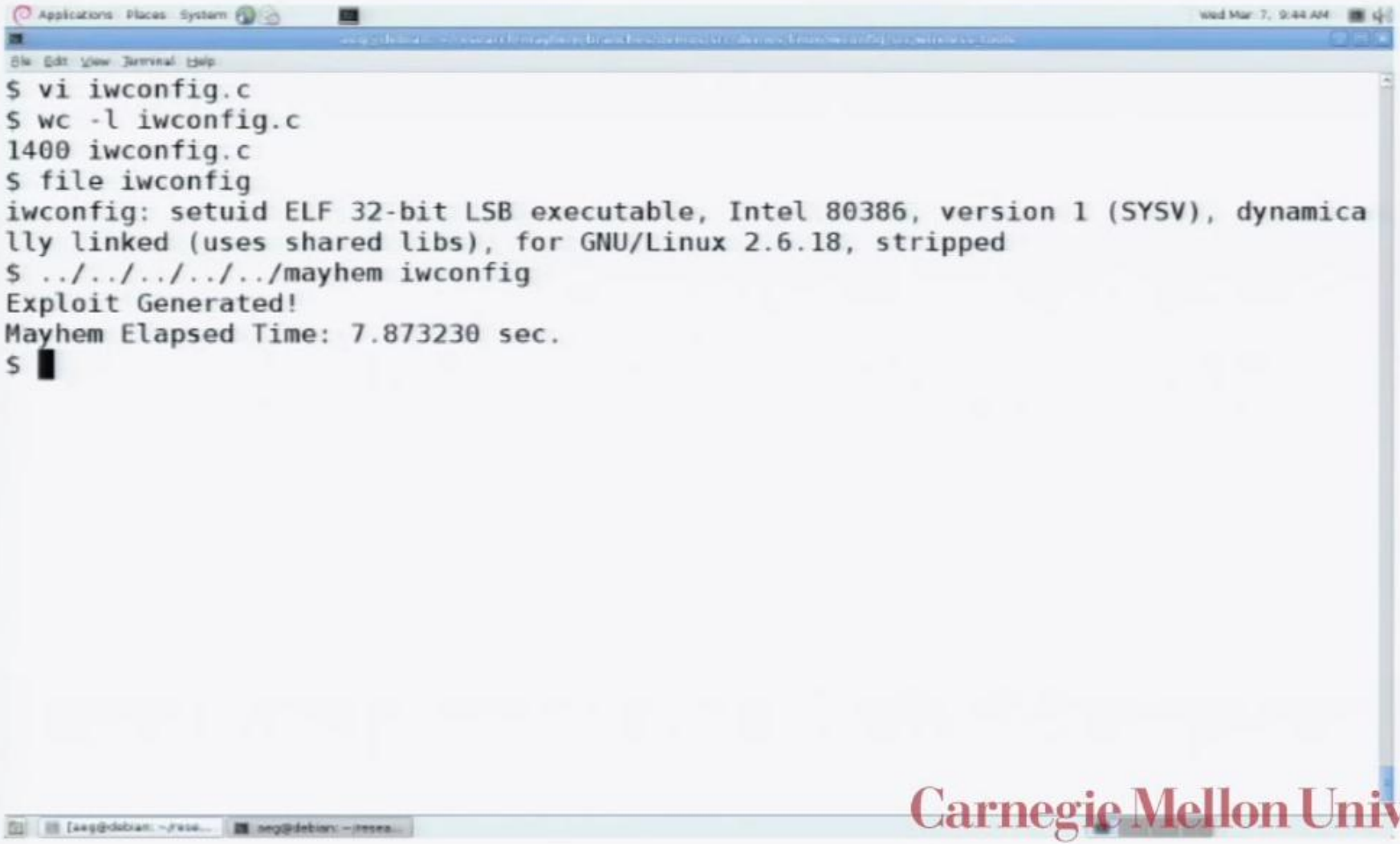
CyLab

Carnegie Mellon University

CyLab

Carnegie Mellon University

CyLab

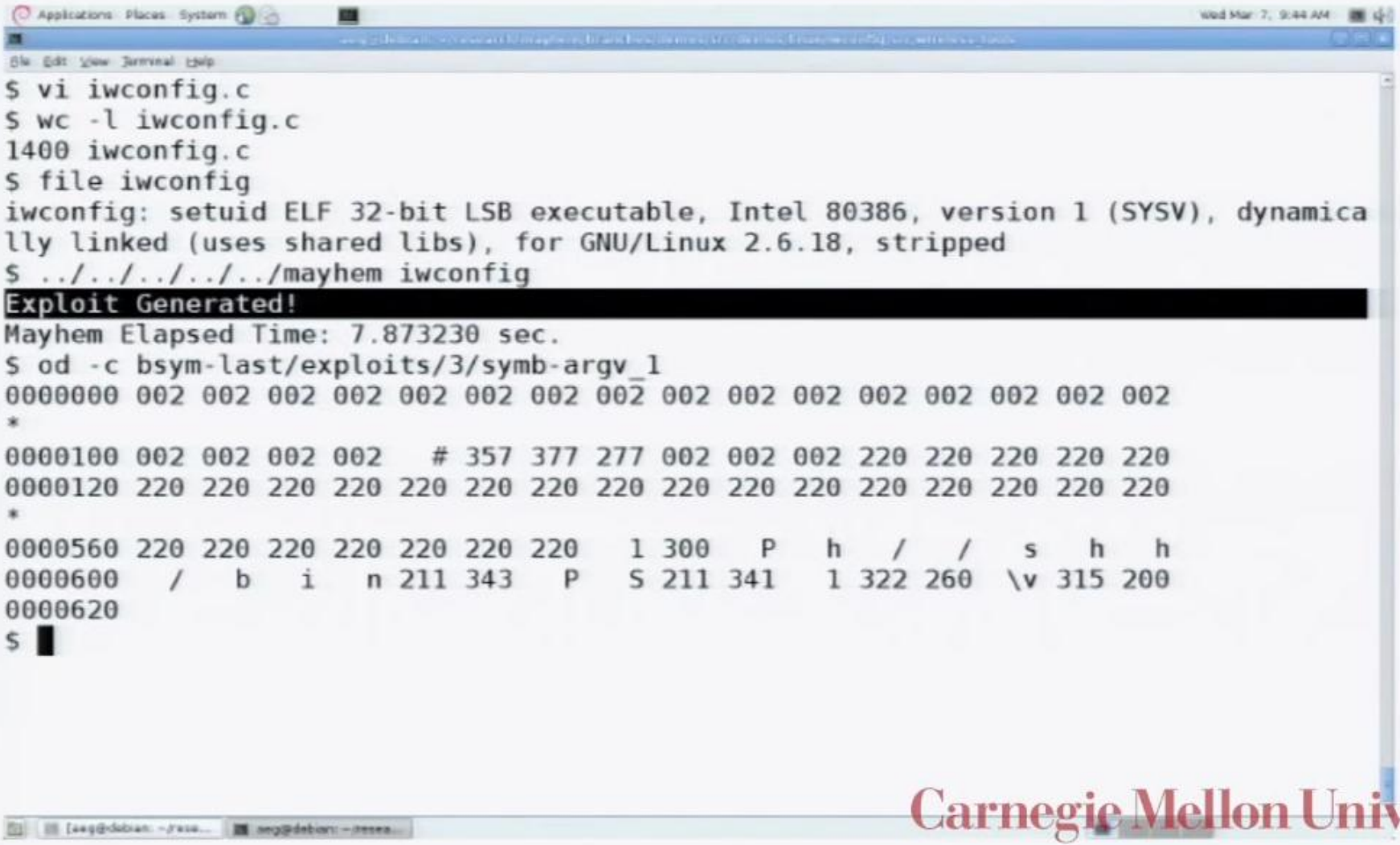


Carnegie Mellon University

CyLab

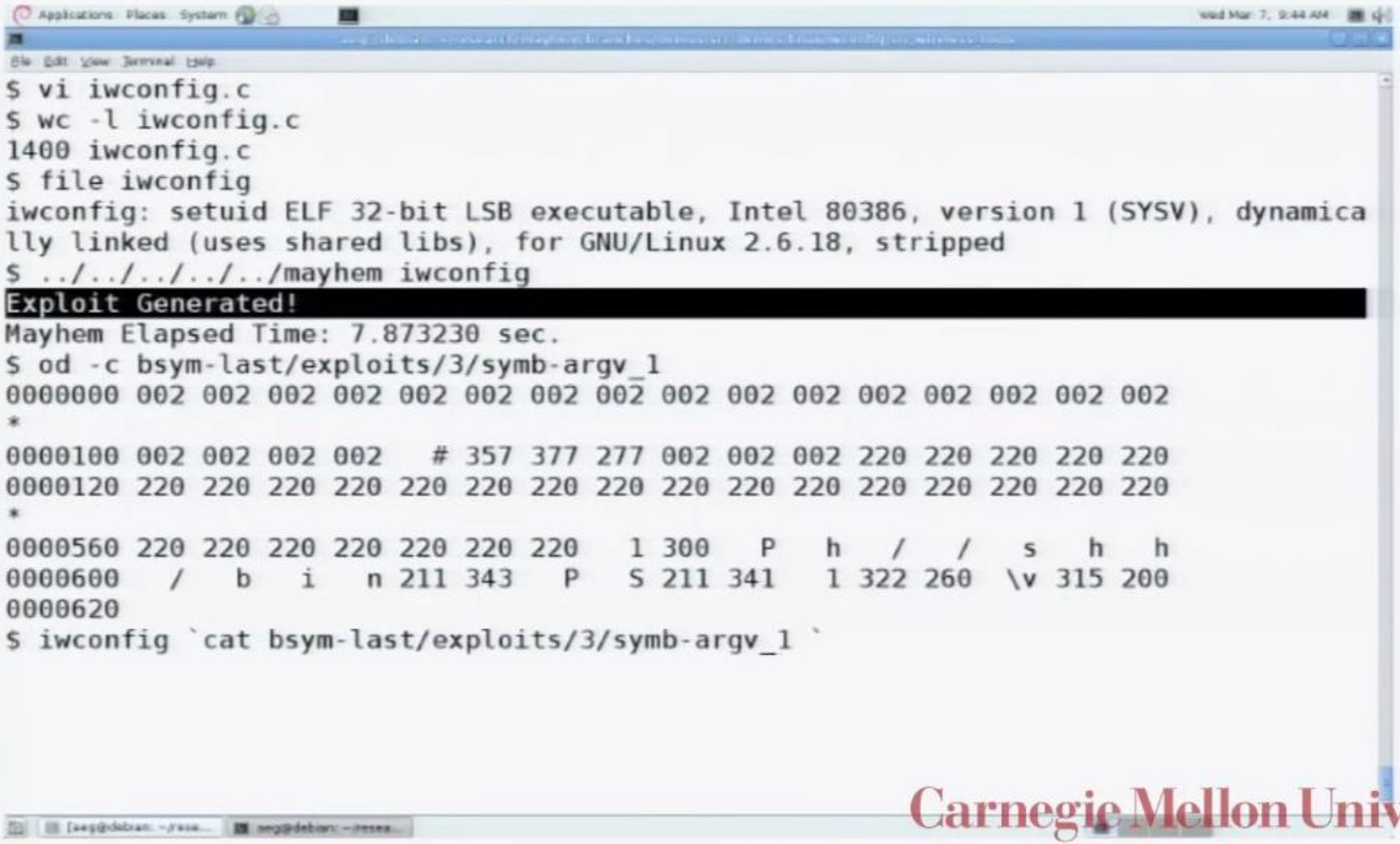
Carnegie Mellon University

CyLab



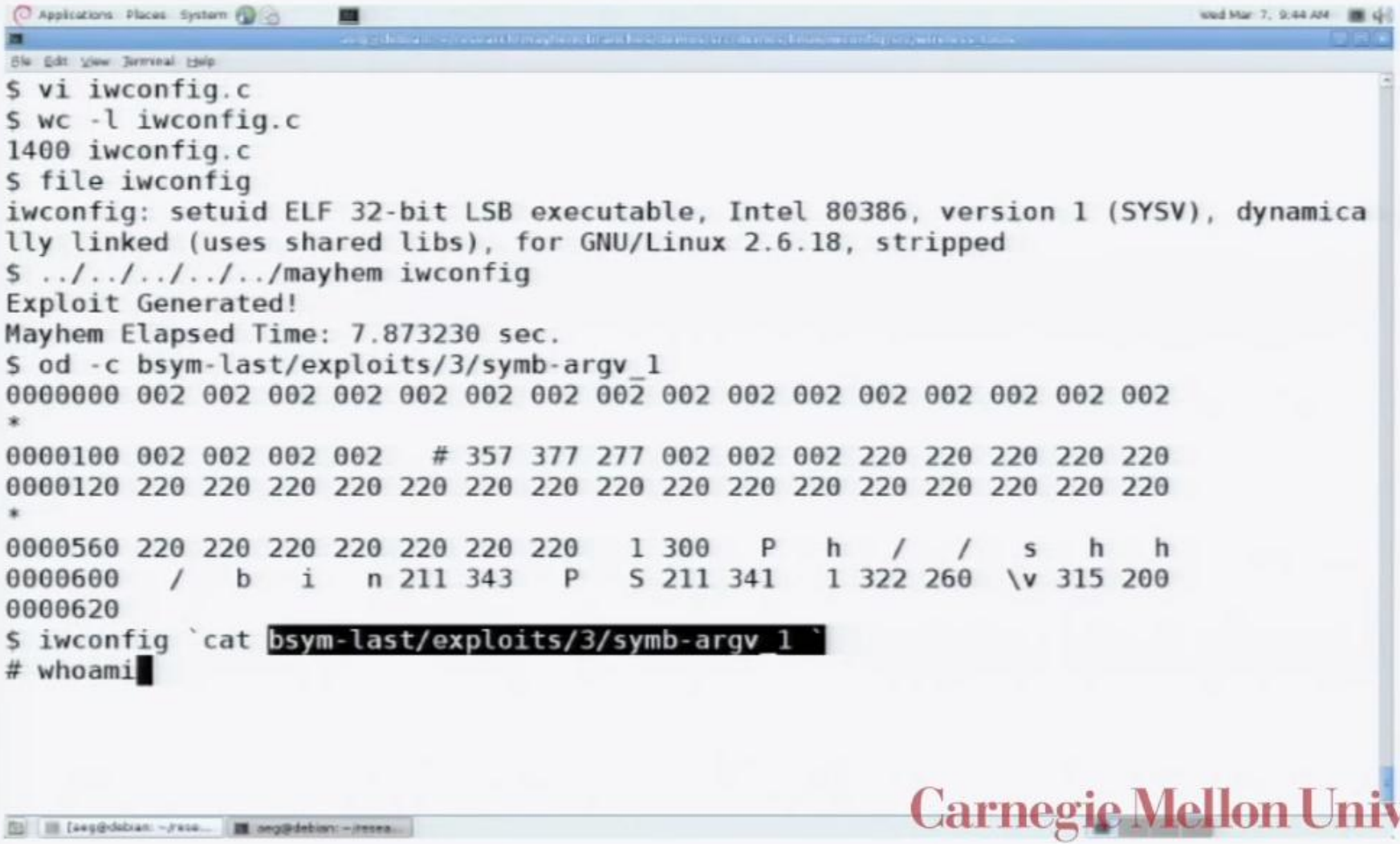
Carnegie Mellon University

CyLab



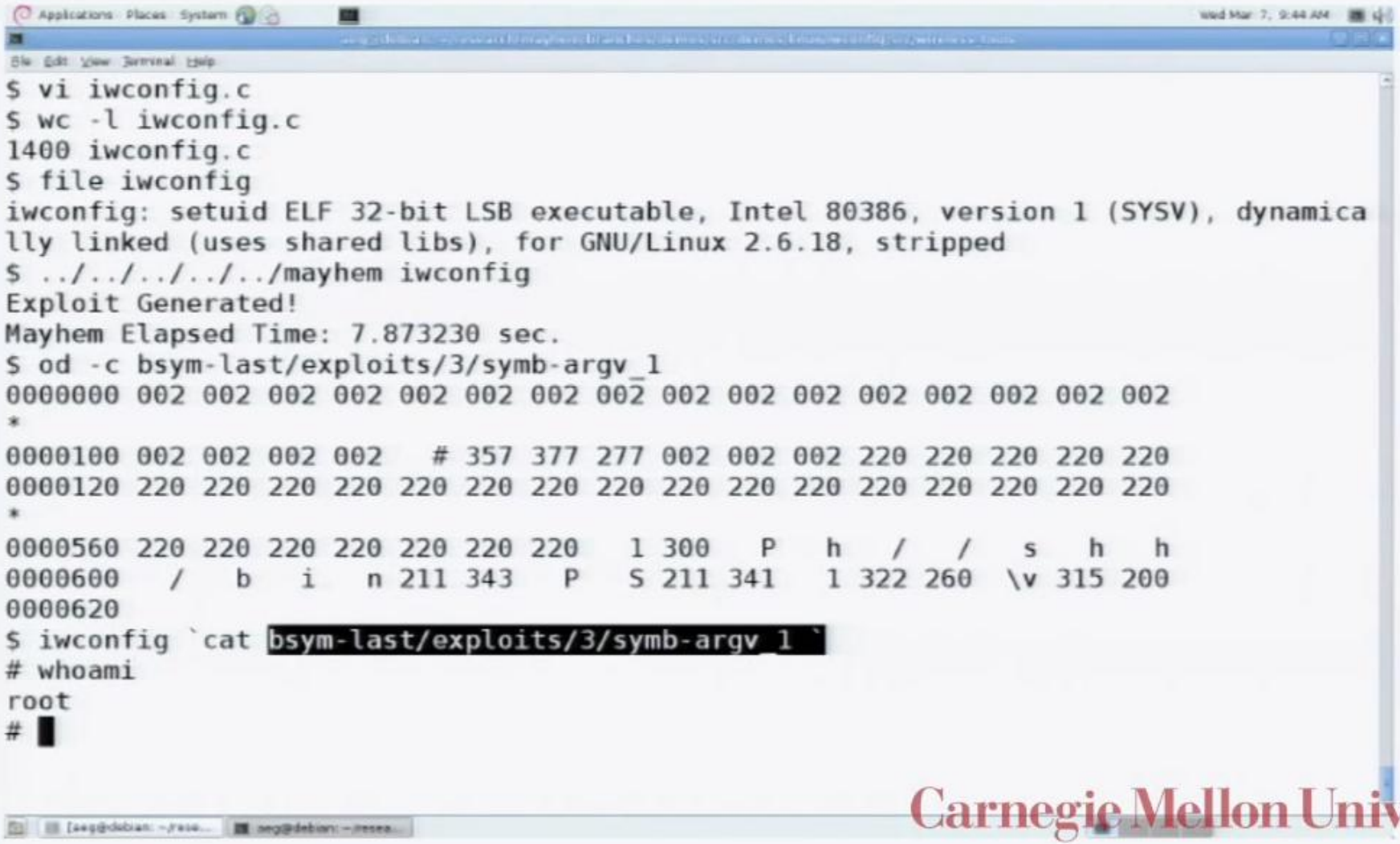
Carnegie Mellon University

CyLab



Carnegie Mellon University

CyLab



Carnegie Mellon University

CyLab

Evil David

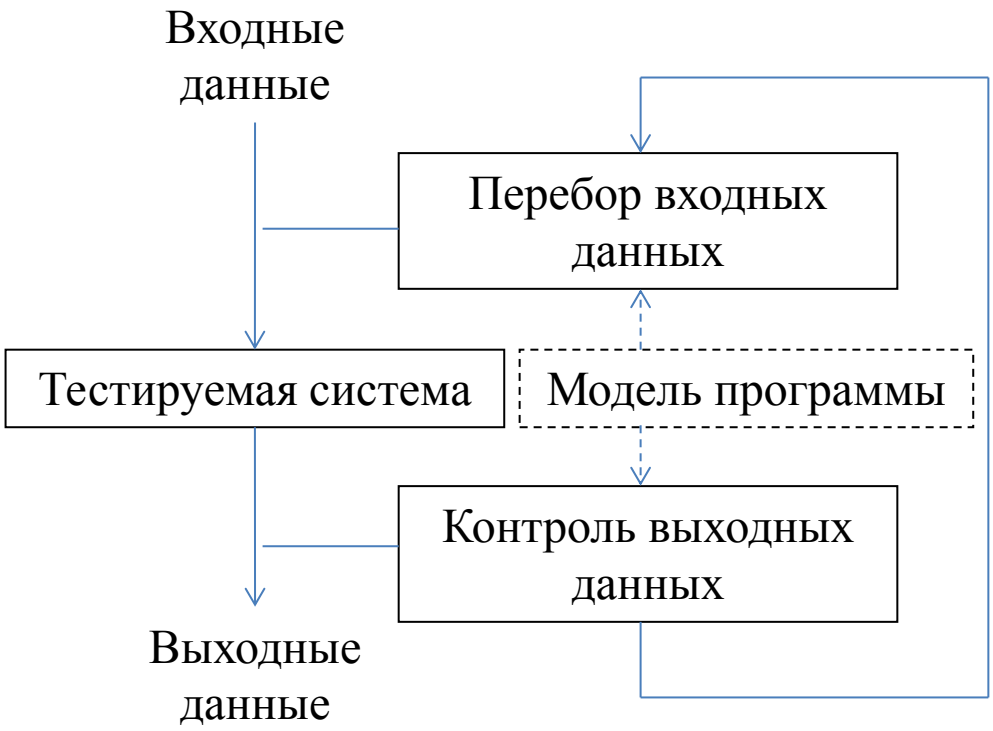
We owned the machine in seconds

Carnegie Mellon University
CyLab

real world exploit generation
a brief history

2005	Automatic Discovery of API-Level Exploits [Ganapathy et al, Conference on Software Engineering]
2008	Automatic Patch-Based Exploit Generation [Brumley et al, IEEE Security and Privacy Symposium]
2010	Automatic Generation of Control Flow Hijack Exploits for Commodity Software [Heelan, MS Thesis]
2011	Automatic Exploit Generation [Avgerinos et al, Network and Distributed System Security Symposium]
2011	Q: Exploit Hardening Made Easy [Schwartz et al, USENIX Security Symposium]
2012	Unleashing Mayhem on Binary Code [Cha et al, IEEE Security and Privacy Symposium]

фаззинг



Каким образом перебирать входные данные? Даже для небольших программ длина входных данных может не иметь ограничений.

При длине входных данных **N** количество возможных значений входных данных $\mathbf{2^N}$

2 подхода:

- Неуправляемый фаззинг : программа – черный ящик, тотальный перебор входов
- Управляемый фаззинг: программа – белый ящик, подбор входов на основе ее свойств (модели)

Что является критерием некорректности работы программы (выходных данных)?

2 подхода:

- Критерий – падение программы
- Критерий – на основе модели

- Что является результатом фаззинга?
- Ровно то, что искали – входные данные, приводящие к нарушению работы программы.
- Это не та уязвимость, посредством которой можно получить контроль над программой.
- Условия контроля (эксплуатабельности) – контролируемая перезапись чувствительных данных, например ключей шифрования, либо внедрение кода.
- А вот «закладка» обнаружена не будет – нет нарушения работы программы

Два вопроса:

1. Какова вероятность что найденная фаззингом уязвимость будет удовлетворять условиям эксплуатабельности?
2. Как найти входные данные, удовлетворяющие этим условиям, зная условия нарушения работы программы?

Какова вероятность?

Charlie Miller, Juan Caballero, Noah M. Johnson, Min Gyung Kang, Stephen McCamant, Pongsin Poosankam, and Dawn Song. *Crash analysis with BitBlaze.* In BlackHat 2010, Las Vegas, NV, July 2010:

- эксплуатабельные уязвимости обнаруживаются в одном из сотен тысяч случаев падения программной системы, тестируемой с помощью фаззинга
- При эксплуатации систем фаззинга на кластерах в течение суток наблюдаются сотни тысяч падений

Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert and David Brumley. *Unleashing Mayhem on Binary Code*. In Proceedings of the 33rd IEEE Symposium on Security and Privacy, May 2012):

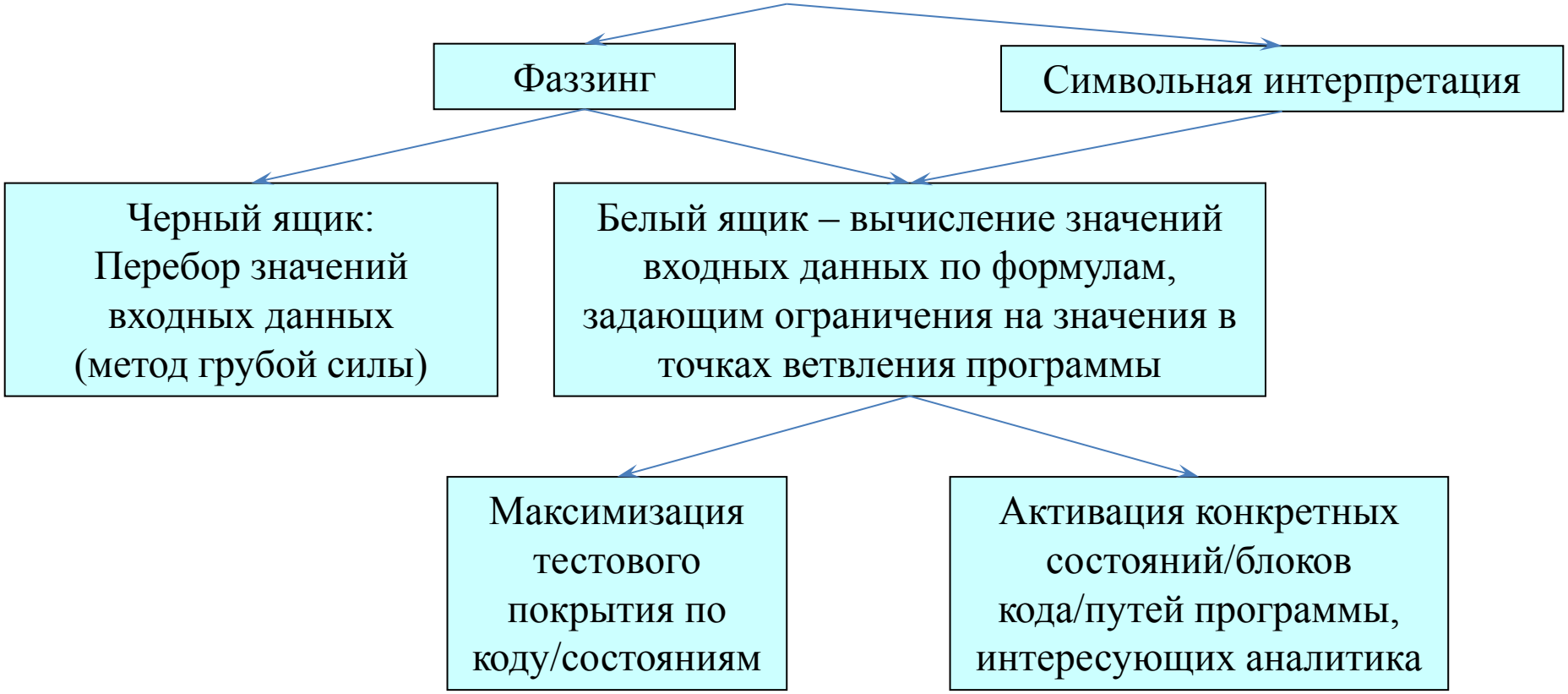
- время поиска уязвимостей для «простых» программ составляет в среднем несколько сотен секунд

Как искать?

- Ручной анализ – непродуктивен: большое число выявляемых падений при малой вероятности встретить эксплуатабельную уязвимость.

- Символьная интерпретация. Довольно сложная для реализации технология.

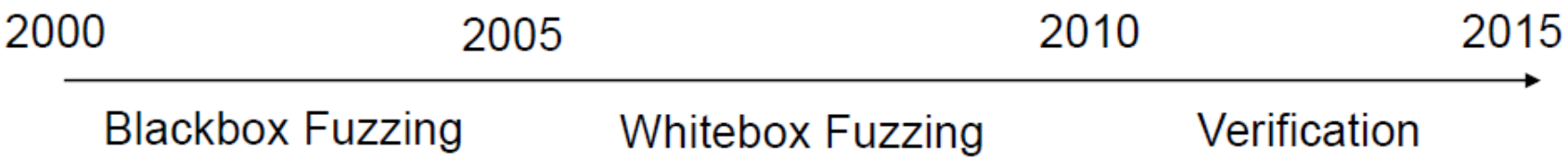
Подходы



Демонстрация проблемы на примере работ Microsoft:

- Фаззинг ч.я. на кластере – сотни тысяч падений в сутки.
- Как определить причину ошибки?
- Как определить критичность (т.е. является ли ошибка уязвимостью)?
- !exploitable: примерно 50% ответов - «не знаю»

В результате – переход от фаззинга ч.я. к символьной интерпретации - SAGE


2000
2005
2010
2015
Blackbox Fuzzing
Whitebox Fuzzing
Verification

SAGE (Scalable Automated Guided Execution)

- Generational search introduced in SAGE
- Performs symbolic execution of x86 execution traces
  - Builds on Nirvana, iDNA and TruScan for x86 analysis
  - Don't care about language or build process
  - Easy to test new applications, no interference possible
- Can analyse any file-reading Windows applications
- Several optimizations to handle huge execution traces
  - Constraint caching and common subexpression elimination
  - Unrelated constraint optimization
  - Constraint subsumption for constraints from input-bound loops
  - "Flip-count" limit (to prevent endless loop expansions)

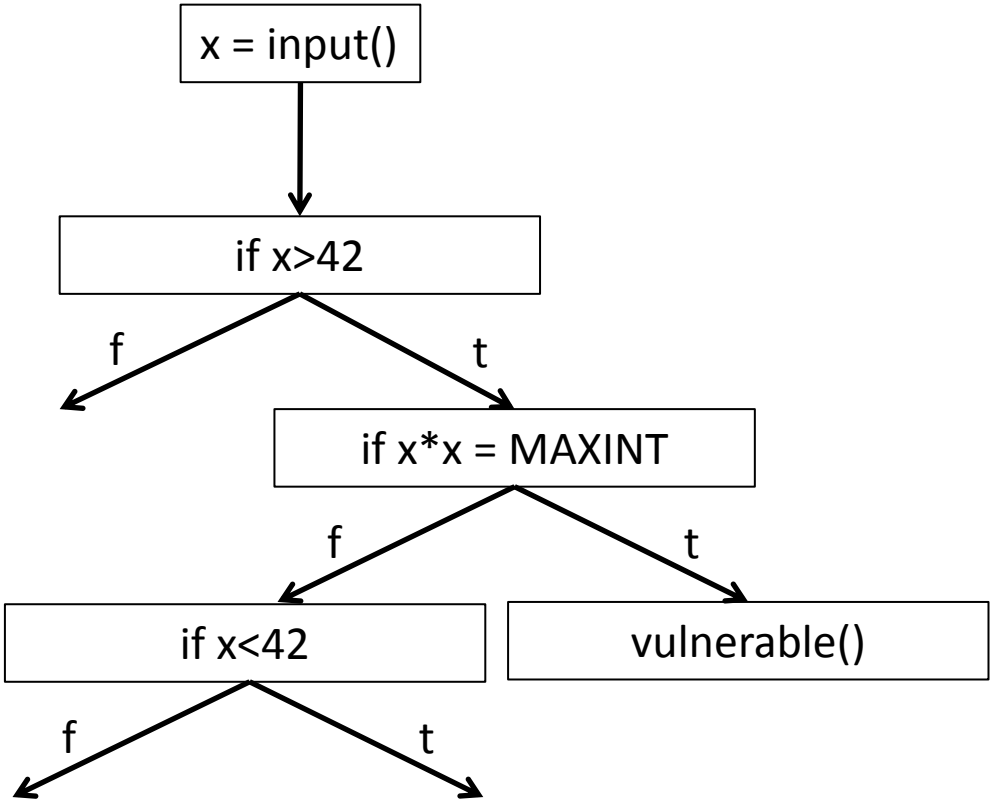
SAGE

- Эксплуатируется с 2007 года на нескольких сотнях компьютеров в режиме 24/7
- Анализ бинарного кода по трассе с использованием символьной интерпретации
- Критерии дефектов – нарушение структуры обрабатываемых файлов
- В качестве SMT-решателя используется Z3
- Более 1/3 всех выявленных при тестировании ошибок в Windows7 найдено с помощью Sage, причем Sage применяется после всех остальных средств тестирования (анализ исходных текстов, фаззинг ч.я., …)

- С 2010г. все результаты применения Sage поступают в единое облачное хранилище – Sagan
- С одной машины Sage в неделю более 300Gb выхода (*несколько сотен машин)

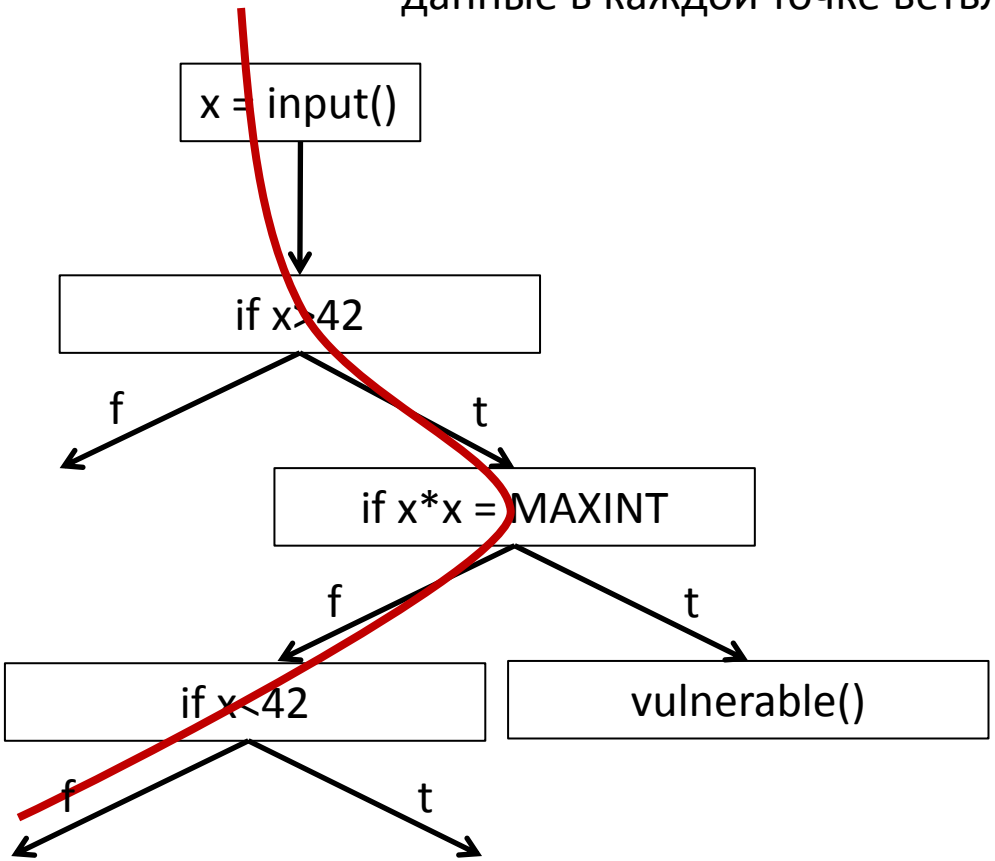
- На данный момент наработка системы – более 400 машино-лет

Суть технологии символьной интерпретации



Суть технологии символьной интерпретации

Построение системы SMT[1]-уравнений, описывающих ограничения на входные данные в каждой точке ветвления программы



x может быть любым

(x > 42)

(x > 42) Λ (x*x != MAXINT)

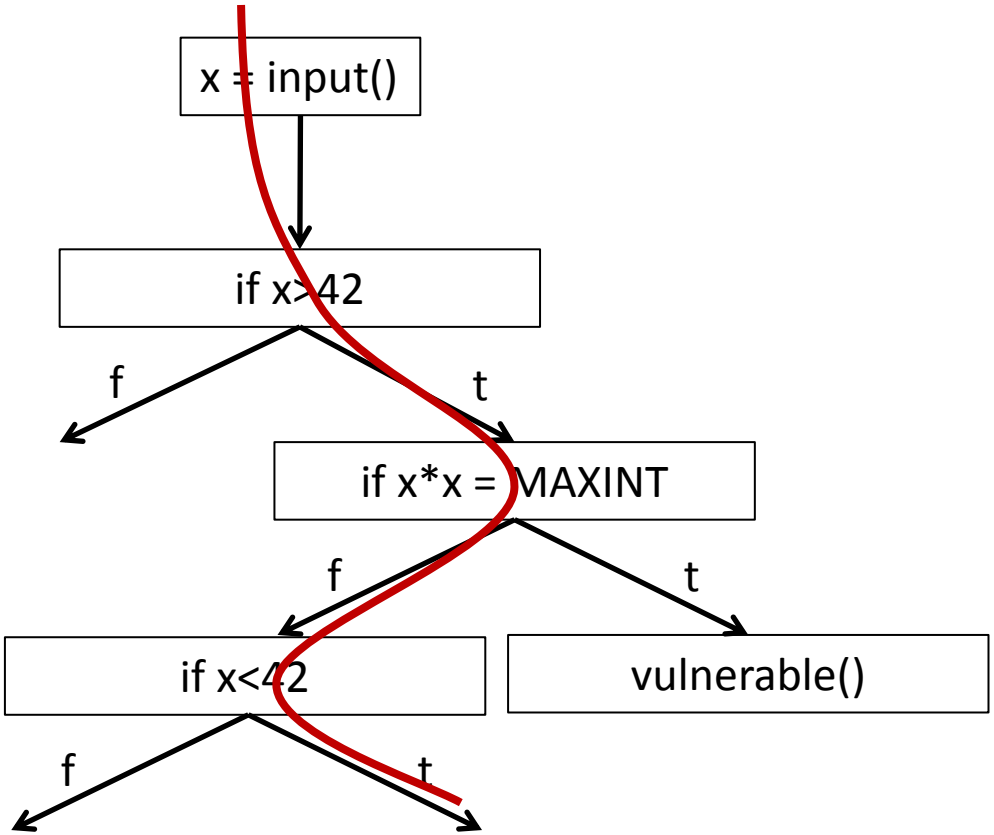
(x > 42) Λ (x*x != MAXINT) Λ !(x<42)

SMT Solver:
Уравнение разрешимо?
x=43

Если уравнение разрешимо – решением являются конкретные значения входных данных, удовлетворяющие заданным ограничениям.

1) SMT- задача разрешимости для логических формул (Satisfiability Modulo Theories) – обобщение задачи выполнимости булевых формул BSAT (Boolean satisfiability problem). В случае КНФ – NP-полная.

Суть технологии символьной интерпретации



x может быть любым

(x > 42)

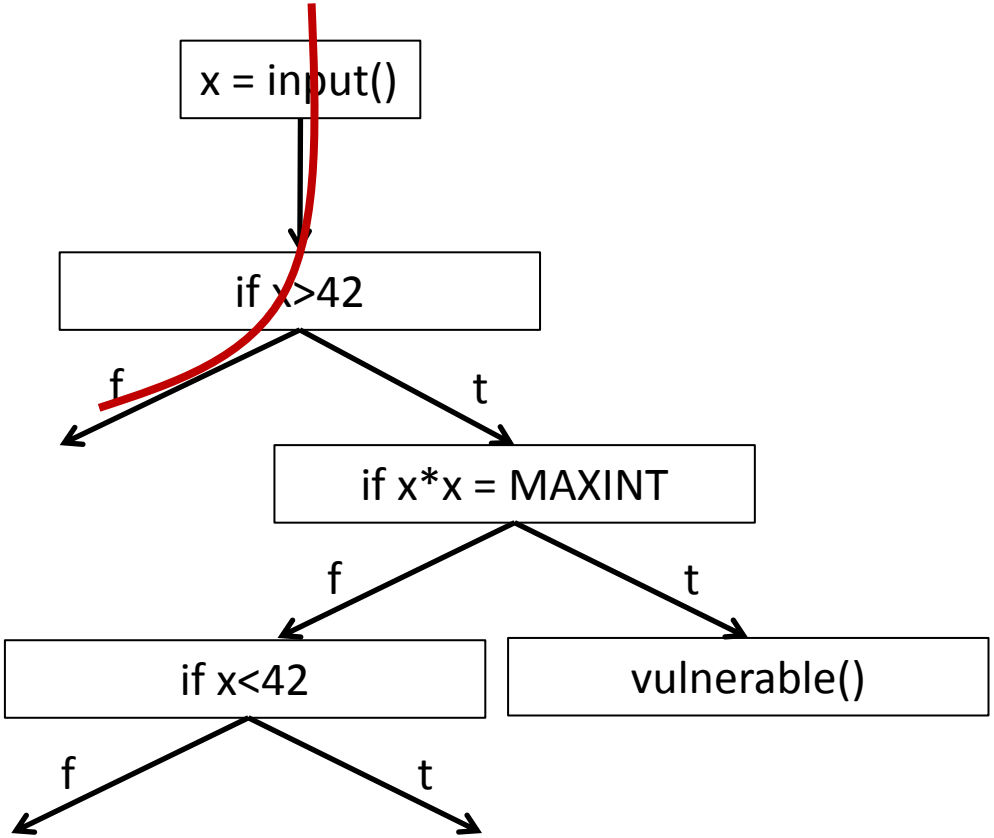
(x > 42) Λ (x*x != MAXINT)

(x > 42) Λ (x*x != MAXINT) Λ (x<42)

SMT Solver:
Уравнение разрешимо?
UNSAT – недостижимый код

Суть технологии символьной интерпретации

Тотальный перебор путей: генерация всех возможных комбинаций SMT-уравнений с инвертированными условиями

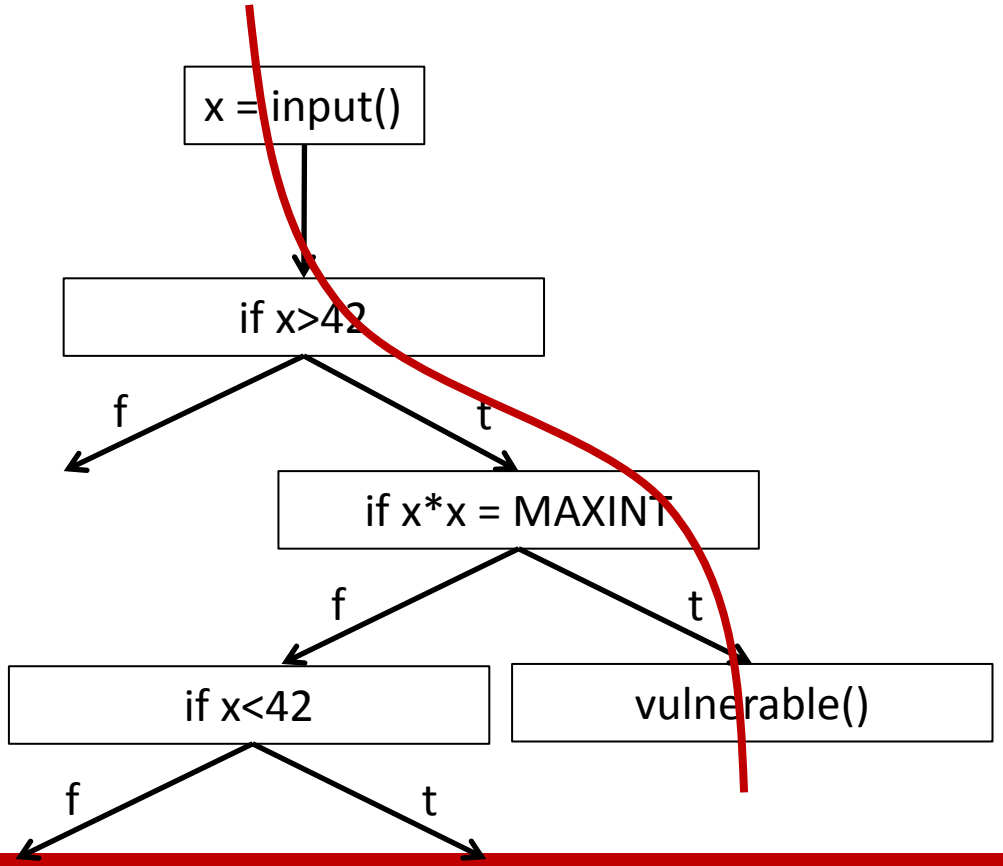


x может быть любым

¬(x > 42)

Суть технологии символьной интерпретации

Проверка свойств эксплуатабельности



x может быть любым

(x > 42)

(x > 42) Λ (x*x = MAXINT)

Критерий на эксплуатабельность:

(x > 42) Λ (x*x = MAXINT) Λ exploitable

Критерий эксплуатабельности (один из): EIP зависит от контролируемого входа программы

Варианты:

1. Измененный EIP указывает на shell-код, полученный со входа программы
2. В стеке формируется последовательность адресов возврата и параметров служебных функций, формирующих требуемую атакующему функциональность (ROP – Rerurn-Oriented Programming)

Две стратегии трансформации SMT-формулы:

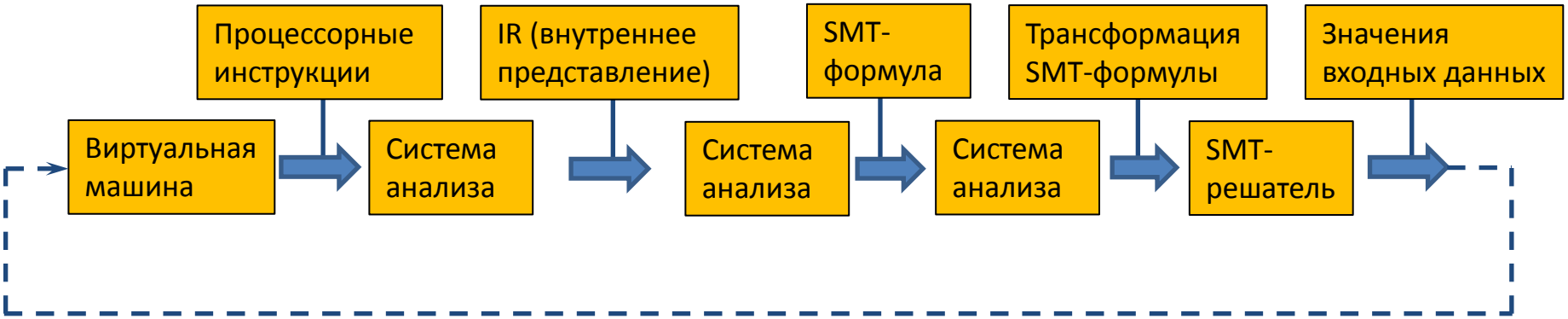
- ПОИСК ЗАКЛАДОК: «тотальный перебор путей» - генерация всех возможных комбинаций инвертирования условий, составляющих SMT-формулу
- ПОИСК УЯЗВИМОСТЕЙ: нахождение траектории до конкретного состояния, для которого можно описать критерий (расширение SMT-формулы критериями на искомые аналитиком состояния). При поиске уязвимостей – критерии на уязвимые состояния.

Две стратегии перебора путей:

- Обход в ширину.
  Проблема – «полезные» точки траектории могут находиться далеко от вершины. Количество траекторий растет экспоненциально от числа ветвлений – можем не дойти до нужной точки
- Обход ближайших веток относительно первоначальной траектории (определяется трассой)

Задачи символьной интерпретации

- Базовая схема процесса символьной интерпретации

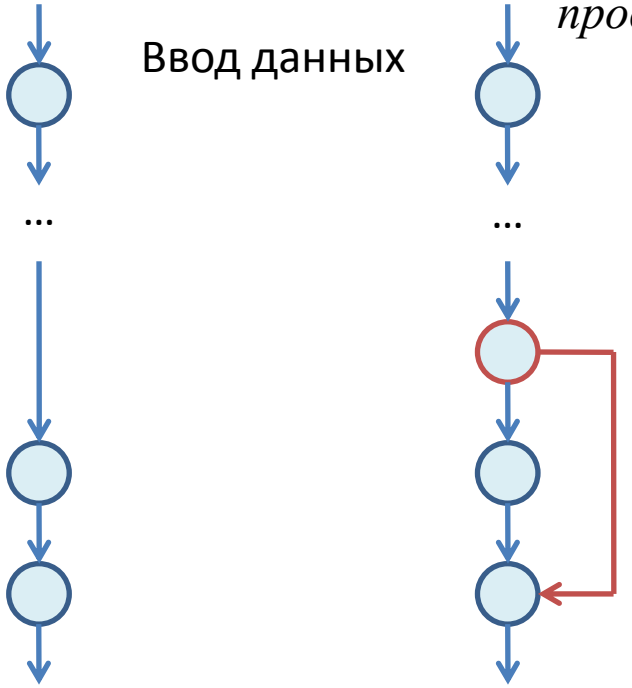


Пример использования символического анализа: BitBlaze, APEG

BitBlaze - Binary Analysis for Computer Security (Berkeley)
Automatic Patch-Based Exploit Generation (Carnegie Mellon, Berkeley, Pittsburg University)

P – исходная программа

P' – получена из P путем добавления дополнительных проверок на корректность входных данных



Идея: сравниваем P и P', находим добавленные проверки

Гипотеза: это проверка корректности входных данных

Решение: с учетом зависимостей по данным ищем пути в P', ведущие от ввода данных до добавленной проверки

Например, снимаем трассу, в которой срабатывает одна из веток такого условия – считаем ее «корректной», а не сработавшую – «обработкой ошибки»

Если такие пути есть – строится формула, описывающая ограничения на входные данные, ее решение определяет значение входные данных, при которых срабатывает ветка «обработки ошибки»

Основные направления развития технологий (1)

Развитие технологий анализа

- Как контролировать работу вычислительной системы (симуляторы, трассировка, поддержка символьных вычислений и taint-анализа). Симуляторы, песочницы, honeypot’ы, DBI (Dynamic Binary Instrumentation). Современные возможности – несколько суток контроля вычислительной системы с малым замедлением и возможностью воспроизведения работы системы в пошаговом режиме
- Как анализировать зависимости между инструкциями (слайсинг, taint-анализ)
- Как генерировать систему SMT-уравнений по программному коду
- Как описывать уязвимые состояния в SMT
- Как эффективно решать систему SMT-уравнений. Распараллеливание. International SAT/SMT Summer School (ежегодно с 2011г. – первая в MIT)
- Генерация критериев на дефектные и уязвимые состояния – применение знаний о спецификации функций, типов (форматов) данных. Отсюда – работы по темам «specification mining», восстановление форматов данных по программному коду
- Контроль потоков данных (taint-анализ) в режиме реального времени для поиска нарушений правил доступа к данным. Вплоть до контроля на аппаратном уровне.

Основные направления развития технологий (2)

Противодействие технологиям анализа:

- Противодействие симуляторам (в идеале - под симулятором программа работает не так, как в обычной неконтролируемой среде).
- Противодействие анализу зависимостей – обфускация.
- Противодействие поиску уязвимостей и уменьшение времени, в течение которого знание уязвимости актуально, до десятков секунд – динамическая обфускация. Обфускация как часть SDLC. Пример – Collberg - RPC
- Противодействие SMT-решателям. Пример - противодействие символьной интерпретации при поиске закладок: *Linear Obfuscation to Combat Symbolic Execution. Zhi Wang, Jiang Ming, Chunfu Jia, Debin Gao (совместно Китай, США, Сингапур)*.
  Цель работы – затруднить вычисление условия активации закладки. Из аннотации к работе: «*Trigger-based code (malicious in many cases, but not necessarily) only executes when specific inputs are received. Symbolic execution has been one of the most powerful techniques in discovering such malicious code and analyzing the trigger condition. We propose a novel automatic malware obfuscation technique to make analysis based on symbolic execution difficult. … Evaluation shows that applying symbolic execution to the obfuscated code is inefficient in finding the trigger condition.*»

А что у нас?

- Осознание проблемы
  ruscrypto – как площадка для обсуждения
  сборник публикаций
- Образовательная база
  ФГОС по специальности 090301 (Компьютерная безопасность)
- Исследовательские коллективы и проекты
- Методы и средства

Спасибо за внимание!

«кадры решают всё»

США:

- программа NICE (National Initiative for Cybersecurity Education): в обеспечении задействован практически весь государственный аппарат, в особенности спецслужбы. Выделена 31 специализация в области подготовки специалистов по компьютерной безопасности.
- NSA и DHS: совместная программа финансирования академических исследований: National Centers of Academic Excellence in Information Assurance: только исследовательских центров в крупных университетах - более 50

Cybersecurity is a National Concern

Your help is critical to defining the Nation's cybersecurity workforce!

Effective cybersecurity management is essential to protecting our nation's technology infrastructure. The professionals accountable for this protection constitute a critical workforce. Until now, there has been little consistency in terms of how cybersecurity work is defined and categorized, who is responsible for the work, and what skill sets are needed to perform successfully. Even within organizations, individuals performing cybersecurity work are difficult to identify, locate, and quantify. As a nation, we must establish consistency in how the cybersecurity workforce is defined and classified.

With the direct engagement of over 20 Federal departments and agencies, and numerous public and private organizations, the National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (the Framework) to define cybersecurity work and lay a foundation for cybersecurity workforce efforts. The Framework provides a common language and taxonomy and defines specialty areas, knowledge, skills, and abilities (KSAs), and codifies talent.

This how-to guide explains what the Framework is, and why you need to not only be aware of the Framework, but also adopt it according to your organization's needs. Explore the guide using the Navigation Bar and by clicking on other links.

Along with representatives from departments and agencies listed on the right, I would like to be among the first to thank you for your support.

Ernest McDuffie

Ernest McDuffie, National Institute for Standards & Technology

The following organizations participated in the development of the Framework, among others:

- Department of State
- Department of Education
- Department of Labor
- Office of Management and Budget
- Office of Personnel Management
- Department of Defense
- Department of Justice
- Information Sciences & Technologies
- Department of Homeland Security
- Central Intelligence Agency
- Defense Intelligence Agency
- Director of National Intelligence
- Federal Bureau of Investigation
- National Security Agency
- National Science Foundation
- Department of Defense National Counterintelligence Executive
- Federal Chief Information Officers Council

"As a nation, we must establish consistency in how the cybersecurity workforce is defined and classified."

What are the 31 Specialty Areas?

Each specialty area represents an area of concentrated work, or function, within cybersecurity. The Framework provides the typical tasks and knowledge, skills and abilities (KSAs) within each specialty area.

Securely Provision

- Systems Requirements Planning
- Systems Development
- Software Assurance and Security Engineering
- Systems Security Architecture
- Test and Evaluation
- Technology Research and Development
- Information Assurance (IA) Compliance

Operate and Maintain

- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management

Collect and Operate

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Protect and Defend

- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Analysis
- Computer Network Defense (CND) Infrastructure Support

Investigate

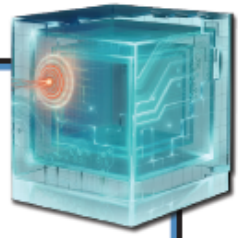
- Investigation
- Digital Forensics

Analyze

- Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence

Oversight and Development

- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development
- Information Systems Security Operations (ISSO)
- Security Program Management (Chief Information Security Officer [CISO])



SECURELY PROVISION

TECHNOLOGY RESEARCH AND DEVELOPMENT

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

TASK | KSA

ID	Statement	Competency
1054	Knowledge of hardware reverse engineering techniques	Vulnerabilities Assessment
1055	Knowledge of middleware	Software Development
1056	Knowledge of operations security	Public Safety and Security
1059	Knowledge of networking protocols	Infrastructure Design
1061	Knowledge of the lifecycle process	Systems Life Cycle
1062	Knowledge of software reverse engineering techniques	Vulnerabilities Assessment
1063	Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications)	Operating Systems
1064	Knowledge of Extensible Markup Language (XML) schemas	Infrastructure Design
1066	Skill in utilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (penetration and testing)	Vulnerabilities Assessment
1067	Skill in utilizing network analysis tools to identify software communications vulnerabilities	Vulnerabilities Assessment
1072	Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Information Systems/Network Security

NEXT PAGE | PREVIOUS PAGE

Information Assurance (IA) Compliance | Software Assurance and Security Engineering | Systems Security Architecture | Technology Research and Development | Systems Requirements Planning | Test and Evaluation | Systems Development

Home | Using This Document | Sample Job Titles | Securely Provision | Operate and Maintain | Protect and Defend | Investigate | Collect and Operate | Analyze | Oversight and Development

Information Assurance

- About IA at NSA
- IA Client and Partner Support
- IA News
- IA Events
- IA Mitigation Guidance
- IA Academic Outreach
- National Centers of Academic Excellence in IA Education
  - Colloquium
  - Institutions
  - SEAL Program
- IA Courseware Evaluation Program
- Student Opportunities
- IA Business and Research
- IA Programs
- IA Careers
- Contact Information

SEARCH

National Centers of Academic Excellence in IA Research (CAE/R) Criteria for Measurement

The goal of the CAE-R program is to increase our understanding of robust IA technology, policy, and practices that will enable our Nation to effectively prevent or respond to a catastrophic cyber event. This program will significantly contribute to the advancement of state-of-the-art IA knowledge and practice. Applicants for CAE/R must meet the Carnegie Foundation's classifications of Research University/Very High (RU/VH), Research University/ High (RU/H) or Doctoral Research University (DRU) or the equivalent is eligible to apply.

Applications must be submitted electronically via the on-line application process. Applications are assessed against a specific set of criteria (PDF attached). Applicants must clearly demonstrate how they meet each of the criteria. Minimum requirements for each of the criteria must be met to obtain designation. Successful applicants are designated as a CAE/R for a period of five academic years, after which they must successfully reapply to retain the designation. The criteria are reviewed annually and strengthened as appropriate to keep pace with the evolving nature of IA/Cybersecurity. (Designation as a National Center of Academic Excellence in IA Research does not carry a commitment of funding from the National Security Agency nor from the Department of Homeland Security.)

The vision for the CAE-R Program is to establish a process that will:

- Recognize schools with programs that integrate research activities into the curriculum and into the classroom.
- Provide NSA, DHS, and other Federal agencies with insight into academic IA programs (with their reach into industry) that can support advanced academic, research, and development capabilities.
- Serve as a potential source and facilitator for government–academic researcher exchanges.
- Present opportunities for IA research centers to drill deeper into much-needed solutions for securing critical information systems and networks.

CAE-R Program Requirements: There are six foundational criteria for establishing CAE-Research:

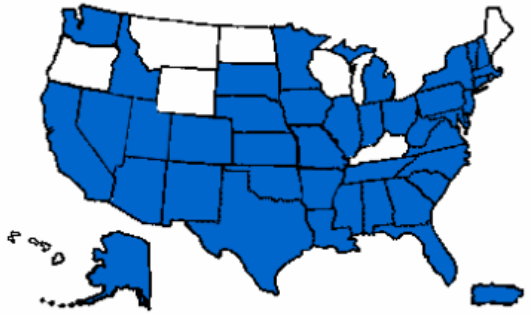
Information Assurance

- About IA at NSA
- IA Client and Partner Support
- IA News
- IA Events
- IA Mitigation Guidance
- IA Academic Outreach
- National Centers of Academic Excellence in IA Education
  - CAE/IAE Program Criteria
  - CAE-R Program Criteria
  - Colloquium
  - Institutions
  - SEAL Program
  - Applying
  - FAQs
- IA Courseware Evaluation Program
- Student Opportunities
- IA Business and Research
- IA Programs
- IA Careers
- Contact Information

SEARCH

Centers of Academic Excellence Institutions

Select a state from the map or from the list below.



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

CAE/2Y - National Centers of Academic Excellence in Information Assurance 2-Year Education

CAE/IAE- National Centers of Academic Excellence in Information Assurance Education

CAE/R - National Centers of Academic Excellence in Information Assurance Research

Alabama	
Auburn University	CAE/IAE, CAE/R
Jacksonville State University	CAE/IAE
Tuskegee University	CAE/IAE
Snead State Community College	CAE/2Y
The University of Alabama at Birmingham	CAE/R
University of Alabama Huntsville	CAE/IEA

Carnegie Mellon University
CyLab

Search | Portal Login

RESEARCH | EDUCATION | PARTNERSHIP | OUTREACH | NEWS & EVENTS | ABOUT CYLAB | QUICK LINKS

ABOUT CyLab

CARNEGIE MELLON CYLAB is a bold and visionary effort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy, and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cybercitizens of all ages.

Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves more than 50 faculty and 100 graduate students from more than six different departments and schools.

CyLab provides technology resources and expertise in four areas:

1. **Technology transfer to and from the public sector**
2. **Technology transfer to and from the private sector**
3. **Development of Information Assurance professionals**
4. **National awareness programs and tools**

FAST facts

CyLab was founded in 2003 and is one of the largest university-based cybersecurity research and education centers in the U.S. Here are some quick facts - CyLab is:

- A National Science Foundation (NSF) CyberTrust Center
- Affiliated with CERT, at the Software Engineering Institute
- A key partner in NSF-funded Center for Team Research in Ubiquitous Secure Technology
- A National Security Agency (NSA) Center of Academic Excellence in Information Assurance Education and a Center for Academic Excellence in Research