Protezione e Sicurezza nei Sistemi Operativi: Introduction

Ozalp Babaoglu

ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA

Objectives

- Outline the security landscape in a modern interconnected world
- Define the goals and limitations for security in a "cyber" setting
- Understand the current impediments for achieving "absolute" security
- Illustrate the *theory*, *techniques* and *tools* for making computing systems *more* secure
- Understand how to specify, implement and reason about the correctness of security requirements
- Outline some general design principles for security
- Introduce symmetric and asymmetric cryptography as powerful technologies for implementing security

Administrative Information

- My Home Page
  - http://www.cs.unibo.it/babaoglu
- Office: Mura Anteo Zamboni 7, Room 104
- Office Hours: Thursdays 13.00 –15.00 (or via Teams)

Changing Face of Attackers

- Shift from large, multipurpose attacks on the network perimeter towards smaller, more targeted attacks to servers and desktop computers
- Shift from "hacking" towards more overt activity, designed to destabilize and disrupt targeted organizations and countries
- The "lone teen hacker" that once dominated the public imagination has been supplanted by well-organized networks of criminals and government-funded organizations with vast computing resources

Changing Face of Attackers

- Today, most attacks fall into one of the following classes:
  - Identity theft
  - Phishing
  - Denial-of-service
  - Ransomeware
  - Cyber-extortion
  - Cyber-warfare
  - Hacktivism
  - Crypto-jacking
  - Supply-chain attack

Cyber-Extortion

- Ransomeware and Denial-of-Service attacks are the most common vectors for carrying out cyber-extortion
- Crypto-style ransomeware, like CryptoLocker, are malicious programs that encrypt files on a computer and demand a fee before handing over the key to the victim

Ransomeware

- The New York Times, 8 May 2021
  - "Cyberattack Forces a Shutdown of a Top U.S. Pipeline" One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks
- The New York Times, 29 May 2021
  - "Secret Chats Show How Cybergang Became a Ransomware Powerhouse" As the ransomware industry exploded, a Russian-speaking outfit called DarkSide offered would-be computer crooks not just the tools, but also customer support

Cyber-Extortion

- During 2015, there were more than 8 million Denial-of-Service (DoS) attacks per month world-wide on the average
- Wired, 28 November 2016
  - "*San Francisco's transit hack could've been way worse and cities must be prepared*" This weekend, San Francisco's public transit system wouldn't take the riders' money — someone had attacked Muni's computer system and was demanding a ransom

Cyber-Extortion

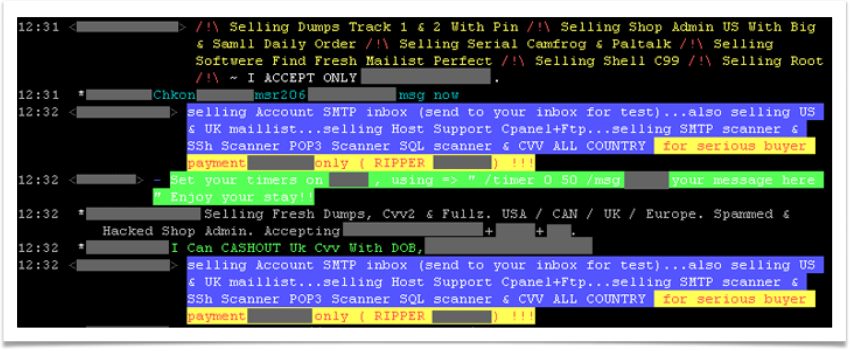
- Most DoS attacks originate at zombie computers and serve to carry out cyber-extortion
- *Zombie*: a compromised computer (infected by malware, virus, trojan horses, etc.) that is used to perform malicious tasks without the knowledge of its owner
  - Denial of Service
  - SPAM
- *Botnet*: a network of zombies remotely controlled by an attacker

"Zombies" and "Botnets"

- In 2013, it was estimated that there were 2.3 million zombie computers worldwide
- Botnets-for-hire were implicated in roughly 40% of all DoS attacks in 2015
- In 2015, the average cost of "renting" a botnet for a DoS attack was less than $1,000 per day
- In 2015, the average cost of a DoS attack to an organization was as high has $40,000 per hour
- 12 October 2020: "Microsoft took action against the *Trickbot botnet*, disrupting one of the world's most persistent malware operations. Trickbot was first spotted in 2016 and over the years, Trickbot's operators were able to build a massive botnet and evolve it into a modular form available for *malware-as-a-service*."

Underground Economy

- Advertisements for goods and services on an underground economy server



Cyber-Warfare

- In 2009, then US Defense Secretary Robert Gates declared cyberspace to be the "fifth domain" of military operations, alongside land, sea, air and space
- USCybercom went fully operational in October 2010 currently headed by General Paul M. Nakasone
- The US currently deploys 6,200 "cyber soldiers"
- Cyber has become the weapon of choice for many countries like North Korea, Russia, China and Iran to steal, disrupt and threaten

Age of Stuxnet, DuQu, Flame, Regin

- New York Times, 25 September 2010
  - "*Iran Fights Malware Attacking Computers*" The Iranian government agency that runs the country's nuclear facilities, including those the West suspects are part of a weapons program, has reported that its engineers are trying to protect their facilities from a sophisticated computer worm that has infected industrial plants across Iran
- New York Times, 11 April 2021
  - "*Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage*" A power failure that appeared to have been caused by a deliberately planned explosion struck Iran's Natanz uranium enrichment site on Sunday, in what Iranian officials called an act of sabotage that they suggested had been carried out by Israel.

Hacktivism

- In recent years we have witnessed a huge rise in cyber activity that has come to be know as "hacktivism" — political, social activism through hacking
- Groups like *LulzSec*, *Anonymous* and *The Syrian Electronic Army* have targeted governments and corporations through highly publicized attacks directed at
  - United States Senate
  - CIA
  - Citibank
  - MasterCard
  - PayPal
  - Sony Corporation (by North Korea in retaliation to the 2014 film *Interview*)

Hacktivism

Anonymous Twitter Feed

Cryptojacking

- *Cryptojacking* is the act of exploiting a computer to mine cryptocurrencies (usually Monero), often through websites running JavaScript, against the user's will or while the user is unaware
- Wired, 29 December 2017 "*Cryptojacking has gotten out of control*"
- Ars Technica, January 2018 "*YouTube advertisements contain JavaScript code that mines cryptocurrency*"

Supply-Chain Attack

- In search of potential attack entry points, threat actors have shifted their strategies to locate vulnerable organizations that are one step away from their main target
- A ***supply-chain attack*** targets service providers, business partners or other organizations trusted by the primary target

Supply-Chain Attack

- NYT, 13 December 2020 "*Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*"
  - Hackers acting on behalf of a foreign government — almost certainly a Russian intelligence agency — broke into a range of key government networks, including in the Treasury and Commerce Departments, and had free access to their email systems

Supply-Chain Attack

- ARS Technica, 16 February 2021 "*New type of supply-chain attack hit Apple, Microsoft, Tesla and 33 other companies*"
  - The so-called ***dependency confusion*** or ***namespace confusion attack*** starts by placing malicious code in an official public repository such as NPM (JavaScript), PyPI (Python), or RubyGems. By giving the submissions the same package name as dependencies used by companies, hackers were able to get companies to automatically download and install the counterfeit code

Security in Context

- Security has to be custom tailored to individual needs, much like a suit or a dental prothesis
- There is no “one-size-fits-all” solution
- Security is a complex and extensive area that permeates all levels of computing systems including their physical environment
- Hardware-OS-Application-Network-Operator
- And like security in any other context, computer security is as strong as its weakest link

Cyber Systems

- Cybersecurity does not concern the security of individual computers but that of ***Cyber Systems***
- Cyber Systems integrate
  - computers,
  - communications, and
  - people (as users and as operators)

Cyber Systems

- These systems are increasingly pervasive in everyday life
  - Internet
  - Mobile and land-line telephone systems
  - Electrical power grid
  - Banking and finance
  - E-Commerce
  - Transportation
  - Automobiles (self-driving or not)
- Yet they are not ***trustworthy***

Cyber Systems: Software Characteristics

- Substantial *legacy* content
  - Documentation missing or incomplete
  - Difficult to modify or port
- Grows by accretion and agglomeration
  - No master plan or architect
  - Nobody understands how/why the system works
- Uses *commercial off the shelf* (COTS) components and software
  - COTS leverage huge economies of scale, allow interoperability and reduce time-to-market but inherit lack of trustworthiness

Trustworthiness

- A cyber system is *trustworthy* when it works correctly despite
  - Malicious/hostile attacks
  - Design and implementation errors (bugs)
  - Human user and operator errors
  - Environmental disruptions

(in increasing order of frequency)

- Holistic and multidimensional problem
  - Property of system, not just components
  - Involves many interacting sub-properties

Trustworthiness

- Trustworthiness is an example of a *nonfunctional* requirement
- ***Functional*** requirements specify *what* a system is supposed to do: inputs produce correct outputs
- ***Nonfunctional*** requirements define *how* a system is supposed to be
- Also known as *qualities of service* (QoS) of a system
  - Scalability
  - Performance
  - Efficiency
  - Operability
  - Interoperability
  - Testability

Trustworthiness

- By their nature, attacks/errors/bugs are unpredictable and cannot be formalized; to do so would rule out possible scenarios
- Trustworthiness cannot be added to an existing system as an afterthought

Security in the (non-cyber) Real World

- Security in the real world is based on three concepts
  - Value
  - Locks
  - Punishment
- Bad guys who break in are caught and punished often enough to make crime unattractive
- Ability to punish implies existence of a “police” force and a judiciary
- Locks should add minimum interference to life

Security in the (non-cyber) Real World

- All locks are not the same
  - Different keys
  - Different strengths
  - Environment dependent
- Individual security needs are based on individual perception
- Pay for what you believe you need
- Locks do not provide absolute security but prevent casual intrusion by raising the threshold of for a break-in

Security in the (non-cyber) Real World

- Perfect defense against theft: put all of your personal valuables in a safe deposit box
- Problem: expensive and inconvenient
- Practical security balances *cost-of-protection* and *cost-of-loss* = (cost-of-replacement × probability-of-loss)
- If *cost-of-protection* is higher than the *cost-of-loss*, it is better to accept loss as "cost of doing business" (Insurance companies, Banks, credit card companies do this all the time)

Cybersecurity

- Cybersecurity is ***not*** about securing physical objects (computers) but the ***services*** they provide and the ***information*** contained within them
- And information is cheap to replace (if we have a backup), never wears out, cannot be attacked with drills or explosives

Why Trustworthy Cyber Systems do not Exist?

- Even if we can replace/restore the bits that constitute information, it may be impossible to undo the damage done by its compromise
- Think of credit card numbers, passwords, bank accounts numbers
- Or trade secrets of a corporation
- Or military secrets

Why Trustworthy Cyber Systems do not Exist?

- Information can be effectively secured by making it unintelligible through *cryptography*
- Thus, we might be tempted to conclude "since cryptography can be nearly perfect, so can cybersecurity"
- This reasoning is flawed for several reasons

Why Trustworthy Cyber Systems do not Exist?

- Most security problems are due to buggy code
  - Even cryptographic modules can contain bugs
- Security is complex and difficult to get right and set up correctly
- Security is a pain and gets in the way of doing things
- Since the value of additional security is difficult to appreciate, people often prefer to buy features over security
- Software and system markets dominated by commercial off-the-shelf (COTS) components

Why Trustworthy Cyber Systems do not Exist?

- Patent restrictions
- Government regulations (restrictions on export of cryptography technologies)
- Reliance on existing communication infrastructures (Internet)
- Everything is interconnected
  - Telephone and power companies use Internet technology
  - Their operational systems are linked to their corporate systems, which are linked to the Internet
  - And the Internet requires power, and is largely built on top of Telephone circuits

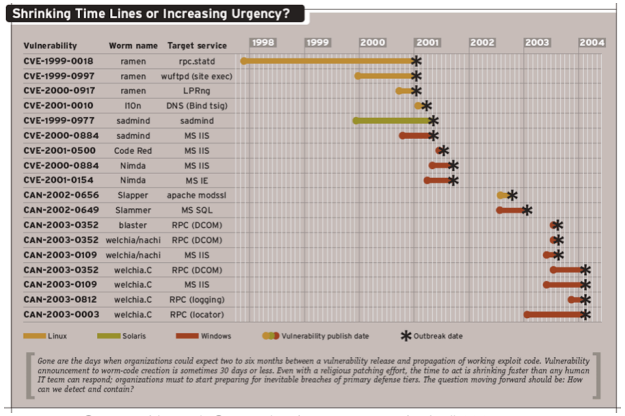
Overview of Cybersecurity

- Like any system, we can study cybersecurity with respect to
  - ***Specification***: What is it supposed to do?
  - ***Implementation***: How does it do it?
  - ***Correctness***: Does it really work?
- In cybersecurity, these are called
  - ***Policy*** (Specification)
  - ***Mechanism*** (Implementation)
  - ***Assurance*** (Correctness)

Definitions

- *Vulnerability*: A weakness that can be exploited to cause damage
- *Attack*: A method of exploiting a vulnerability
- *Threat*: A motivated, capable adversary that mounts an attack
- Strategies:
  - Identify and fix each vulnerability (usually due to bugs)
  - Identify attacks and eliminate those vulnerabilities that those attacks exploit

Shrinking Vulnerability-to-Attack Time



Source: Network Computing (www.nwc.com), April 2004

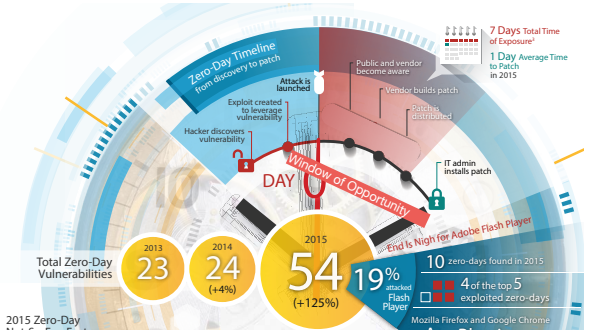
Zero-Day

- *Zero-day vulnerability*: A vulnerability that is unknown to those who should be interested in mitigating it
- *Window of Opportunity*: Time from when a software exploit first becomes active to the time when a patch is released by the affected vendor and applied to the affected system
- *Zero-day attack*: an attack that occurs during the window of opportunity
- In 2005, the average length of a window of opportunity was 54 days
- In 2014, the average length of a window of opportunity had grown to almost 12 months

Google Project Zero

- Project Zero announced in 2014, is a team of security analysts employed by Google tasked with finding zero-day vulnerabilities
- The team's focus is not just on finding bugs and novel attacks, but also on researching and publicly documenting how such flaws could be exploited in practice
- Bugs found by the Project Zero team are reported to the manufacturer and only made publicly visible once a patch has been released or if 90 days have passed without a patch being released

Zero-Day Timeline



Notable Zero-Day Vulnerabilities — Heartbleed

- Disclosed in April 2014
- Vulnerability in the OpenSSL implementation of the Transport Layer Security (TLS) protocol
- Introduced in 2011 and deployed in millions of web servers
- OpenSSL 1.0.1g released on 7 April 2014 fixes the bug
- Yet hundreds of thousand servers still remain vulnerable

Notable Zero-Day Vulnerabilities — Shellshock

- Disclosed on 25 September 2014
- Vulnerability in the Unix command line interpreter *bash* (GNU *B*ourne-*A*gain *SH*ell)
- Has been around since 1989 and deployed in millions of devices running Unix, Linux, Mac OSX
- Apple patch of 29 September 2014 fixes Mac OSX bash

Zero-Day Vulnerabilities — Shellshock

National Cyber Awareness System

Vulnerability Summary for CVE-2014-7169

Original release date: 09/24/2014

Last revised: 09/25/2014

Source: US-CERT/NIST

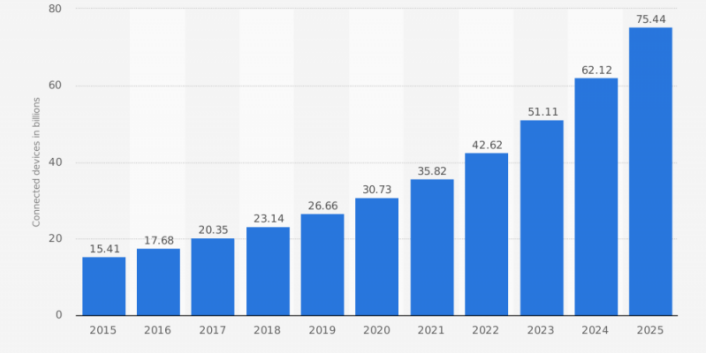
Overview

GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.

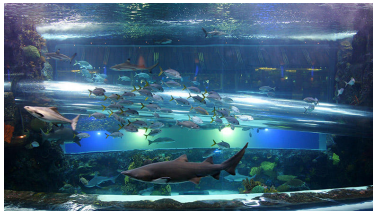
```
bash-3.2$
bash-3.2$
bash-3.2$ bash --version
GNU bash, version 3.2.51(1)-release (x86_64-apple-darwin13)
Copyright (C) 2007 Free Software Foundation, Inc.
bash-3.2$
bash-3.2$
bash-3.2$ env COLOR='() { :;}; echo vulnerable' bash -c "echo I hate colors"
vulnerable
I hate colors
bash-3.2$
bash-3.2$
```

Internet of Things

- IoT connected devices installed base worldwide



Internet of Things



- mashable.com, 15 April 2018 "*Hackers exploit casino's smart thermometer to steal database info*"
  - CEO of cybersecurity company Darktrace, revealed that a casino fell victim to hackers thanks to a smart thermometer it was using to monitor the water in an aquarium they had installed in the lobby. The hackers managed to find and steal information from the casino's high-roller database through the thermometer.

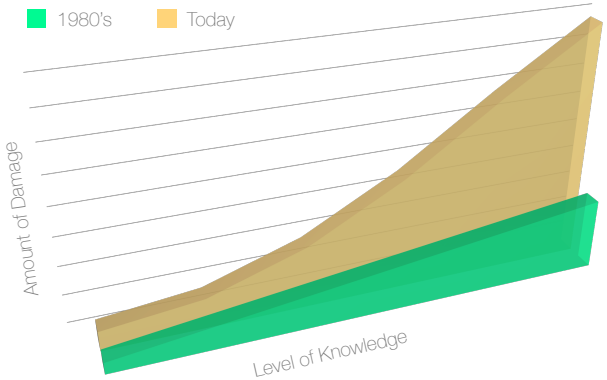
Internet of Things

- Ars Technica 11 December 2018, "A 100,000-router botnet is feeding on a 5-year-old UPnP bug in Broadcom chips"
  - A recently discovered botnet has taken control of an eye-popping 100,000 home and small-office routers made from a range of manufacturers, mainly by exploiting a critical vulnerability that has remained unaddressed on infected devices more than five years after it came to light

Knowledge vs Damage

- Severity of a threat is a function of the resources available for the attack
  - *Knowledge* is a resource
  - Money can buy anything, including knowledge
  - Easy access to "packaged" knowledge (*vulnerability scanners* such as *SATAN*, *nmap*, *Nessus*, *SARA*) results in a discontinuity between the knowledge necessary to mount a particular attack and the severity of the resulting damage

Knowledge vs Damage



Google Hacking

- International Herald Tribune, 28 September 2006. "*Hacking made easy: 'Secret' data just a Google search away*"
  - One widespread vulnerability can be exploited through a practice that has come to be known as Google hacking. These hacks require no special tools and little skill. All that is needed is a Web-connected PC and a few keywords to look for, like "filetype:sqlpassword" or "index.of.password."

Cybersecurity Policies

- *Cyber system security* is responsible for controlling
  - *Confidentiality* (secrecy): controlling who gets to read information
  - *Integrity*: controlling how information changes or resources are used
  - *Availability*: providing prompt access to information and resources
- Known as the *CIA triad*
- We often add a fourth requirement
  - *Accountability*: knowing who has had access to information or resources

Cybersecurity Policies

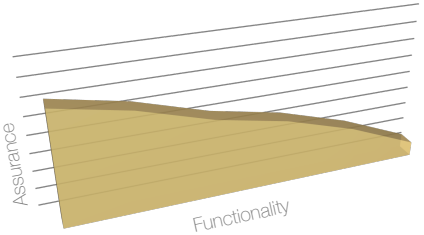
- What do locks, keys, values and the police have to do with cybersecurity?
  - *Locks*: authorization, access control mechanisms
  - *Keys*: authentication required to open a lock
  - *Police*: same as in the real world

Gold Standard of Cybersecurity

- Any system claiming to be secure must contain mechanisms for
  - ***Au***thentication
  - ***Au***thorization
  - ***Au***diting

Assurance vs Functionality

- *Assurance* is an attribute of a cyber system that provides grounds for having confidence that the system is trustworthy
- Increased functionality implies increased complexity and complexity is the worst enemy of security



Some Design Principles

- Fundamental design principles to promote higher assurance
  - Open design
  - Economy of mechanism
  - Fail-safe defaults
  - Complete mediation
  - Least privilege

Open Design

- Security of a mechanism should not depend on attacker's ignorance of how the mechanism works or how it is built
  - No "security through obscurity"
  - Makes security harder but is necessary for increased assurance

Economy of Mechanism

- Small and simple mechanisms whenever possible
  - fewer possibilities exist for errors
  - checking and testing process is less complex, because fewer components and cases need to be tested
  - fewer (wrong) assumptions
- Complex mechanisms often make assumptions about the system and environment in which they run
  - Security problems may derive from incorrect assumptions (for instance, badly formed messages)
  - Interfaces to other modules are particularly suspect

Fail-safe Defaults

- By *default*, subjects should have no access privileges over any object
- (Limited) access to selected objects should be granted *explicitly*
- Typically enforced by the *access control* mechanisms of a cyber system

Complete Mediation

- It should not be possible to access objects directly
- All accesses should be *mediated* by the system (typically through a reference monitor in the operating system)

Least Privilege

- Every subject should operate using the *minimum* set of privileges (access rights) that are necessary to perform its task
  - Limits damage that can result from an accident or error
  - Limits number of privileged programs
  - Helps in debugging
  - Increases assurance
  - Allows isolation of critical subsystems
- *Least Privilege* enforced through a *reference monitor* that implements *complete mediation* — every access to every object is checked