

# Fondamenti di Cybersecurity

*Ozalp Babaoglu*

ALMA MATER STUDIORUM – UNIVERSITÀ 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

© Babaoglu 2001-2022

Cybersecurity

2

## Administrative Information

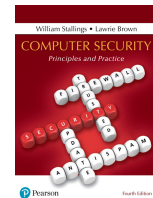
- My Home Page
  - <http://www.cs.unibo.it/babaoglu>
- Course Home Page
  - <http://www.cs.unibo.it/babaoglu/courses/security/>
- Tutor: Davide Berardi
- Schedule:
  - Monday 09.00–11.00 (Aula Magna Chimica)
  - Wednesday 11.00–13.00 (Aula M1)
  - Friday 09.00–11.00 (Aula G1)
- Office Hours: Tuesdays 13.00–15.00 (via Teams)

© Babaoglu 2001-2022

Cybersecurity

3

## Textbooks (recommended)



- *Computer Security: Principles and Practice* (4th Edition), Stallings and Brown, Pearson, 2018



- *Computer Security: Art and Science* (2nd Edition), Matt Bishop, Addison-Wesley, 2018

© Babaoglu 2001-2022

Cybersecurity

4

## What is Cybersecurity?

From the Merriam-Webster dictionary

### cyber adjective

cy·ber | \sī·bər \

#### Definition of cyber

: of, relating to, or involving computers or computer networks (such as the Internet)

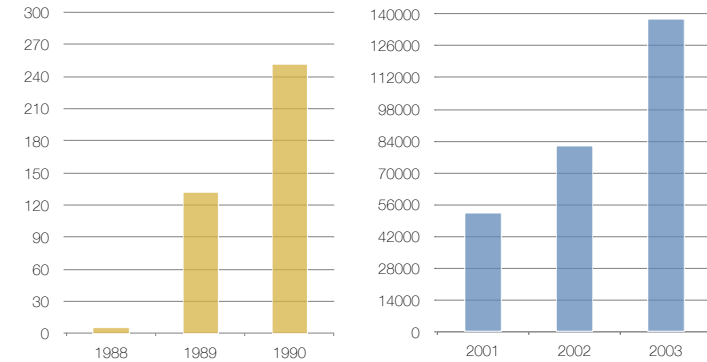
### cybersecurity noun

cy·ber·se·cu·ri·ty | \sī·bər-sī-,kyūr-ə-tē \

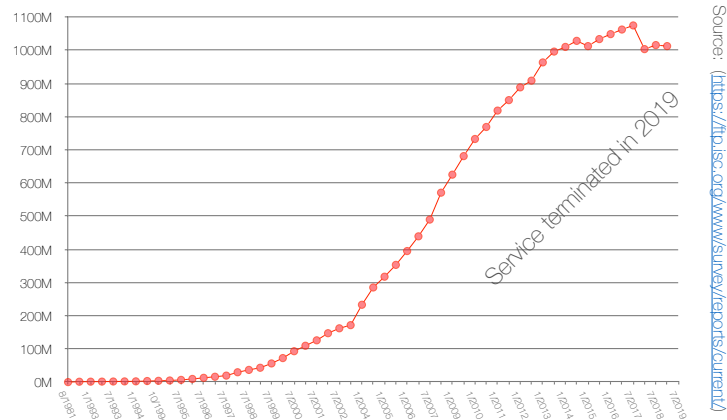
#### Definition of cybersecurity

: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

## Security Incidents Reported to CERT



## Internet Domain Survey Host Count



## (Lack Of) Security in the Media

- New York Times, 5 May 1990 "Computer Intruder Is Put on Probation And Fined \$10,000"
  - On November 2, 1988, Robert Morris had released the first computer worm on the Internet infecting 6,000 Unix machines causing \$10M—100M of damage
- New York Times, 18 August 1996 "Computer Hacker Invades Web Site of the Justice Department"
- New York Times, 14 September 1998 "Hacker Group Commandeers The New York Times Web Site"
- New York Times, 8 February 2000 "Yahoo Blames a Hacker Attack for a Lengthy Service Failure"
  - Popular sites like Yahoo, eBay, Amazon, Netflix, AOL, Altavista, GeoCities, Hotmail taken down

## (Lack Of) Security in the Media

- And countless other incidents that are not publicized for fear of embarrassment
- Yet when a public incident occurs, security experts and antivirus software vendors tend to exaggerate its costs
- Worldwide spending on cybersecurity products and services is estimated to exceed \$1 trillion during 2017–2021

## (Lack Of) Security in the Media

- 3 October 2012: “The peddlers of so-called “scareware” are facing a \$163 million fine from the Federal Trade Commission for misrepresenting that they had conducted scans of consumers’ computers and detected security or privacy issues”



## 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
  - Ransomware
  - Cyber-extortion
  - Cyber-warfare
  - Hacktivism
  - Crypto-jacking
  - Supply-chain attack

## Identity Theft

- New York Times, 5 August 2014
  - A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say
- New York Times, 14 December 2016
  - Yahoo says 1 billion user accounts were hacked
- New York Times, 7 September 2017
  - Equifax says cyberattack may have affected 143 million in the U.S.

## Phishing

- To avoid detection (and being blocked), cyber-criminals now switch their location using free Web hosting providers that automatically generate new domain names
- Google says many phishing sites now only stay online for less than an hour, some are switched every 10 minutes
- Google now finds 300,000 new phishing sites a month

## Ransomware

- Crypto-style ransomware, like CryptoLocker, are malicious programs that encrypt files on a computer and demand a fee before handing over the key to the victim
- The Guardian, 12 May 2017
  - "What is WannaCry ransomware and why is it attacking global computers?" Malicious software has attacked Britain's health service and companies in Spain, Russia, the Ukraine and Taiwan
- The New York Times, 27 June 2019
  - "Another Hacked Florida City Pays a Ransom, This Time for \$460,000"
- ProPublica, 27 August 2019
  - "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks" In recent years, cyber insurance sold by domestic and foreign companies has grown into an estimated \$7 billion to \$8 billion-a-year market in the U.S. alone

## Ransomware

- 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. "Any doofus can be a cybercriminal now," said Sergei A. Pavlovich, a former hacker who served 10 years in prison in his native Belarus for cybercrimes. "The intellectual barrier to entry has gotten extremely low."

## Ransomware

- DarkSide offers what is known as “ransomware as a service,” in which a malware developer charges a user fee to so-called affiliates like Woris, who may not have the technical skills to actually create ransomware but are still capable of breaking into a victim’s computer systems
- DarkSide’s services include providing technical support for hackers, negotiating with targets like the publishing company, processing payments, and devising tailored pressure campaigns through blackmail and other means, such as secondary hacks to crash websites. DarkSide’s user fees operated on a sliding scale: 25 percent for any ransoms less than \$500,000 down to 10 percent for ransoms over \$5 million, according to the computer security firm, FireEye
- Even before the attack on Colonial Pipeline, DarkSide’s business was booming. According to the cybersecurity firm Elliptic, which has studied DarkSide’s Bitcoin wallets, the gang has received about \$15.5 million in Bitcoin since October 2020, with another \$75 million going to affiliates

## 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 as \$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

```

12:31 < > /\ Selling Dumps Track 1 & 2 With Pin /\ Selling Shop Admin US With Big
& Samll Daily Order /\ Selling Serial Camfrog & Paltalk /\ Selling
Software Find Fresh Maillist Perfect /\ Selling Shell C99 /\ Selling Root
/\ ~ I ACCEPT ONLY
12:31 * Chkon msr206 msg now
12:32 < > selling Account SMTP inbox (send to your inbox for test)...also selling US
& UK maillist...selling Host Support Cpanel+Ftp...selling SMTP scanner &
SSH Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY for serious buyer
payment only ( RIPPER ) !!
12:32 < > - Set your timers on , using -> "/timer 0 50 /msg your message here
Enjoy your stay!!
12:32 * Selling Fresh Dumps, Cvv2 & Fullz. USA / CAN / UK / Europe. Spammed &
Hacked Shop Admin. Accepting + +
12:32 * I Can CASHOUT UK Cvv With DOB,
12:32 < > selling Account SMTP inbox (send to your inbox for test)...also selling US
& UK maillist...selling Host Support Cpanel+Ftp...selling SMTP scanner &
SSH Scanner POP3 Scanner SQL scanner & CVV ALL COUNTRY for serious buyer
payment only ( RIPPER ) !!
    
```

## Underground Economy

- Goods and services on an underground economy server
- Source: Symantec Corporation

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	\$0.07-\$100
2	2	Bank account credentials	16%	19%	\$10-\$900
3	3	Email accounts	10%	7%	\$1-\$18
4	13	Attack tools	7%	2%	\$5-\$650
5	4	Email addresses	5%	7%	\$1/MB-\$20/MB
6	7	Credit card dumps	5%	5%	\$0.50-\$120
7	6	Full identities	5%	5%	\$0.50-\$20
8	14	Scam hosting	4%	2%	\$10-\$150
9	5	Shell scripts	4%	6%	\$2-\$7
10	9	Cash-out services	3%	4%	\$200-\$500 or 50%-70% of total value

## 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

## Cyber-Warfare

- New York Times, 26 July 2016
  - “Spy agency consensus grows that Russia hacked D.N.C.” American intelligence agencies have told the White House they now have “high confidence” that the Russian government was behind the theft of emails and documents from the Democratic National Committee
- New York Times, 5 May 2017
  - “Macron campaign says it was target of ‘massive’ hacking attack”

## 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

- 2011 has seen a huge rise in cyber activity that has come to be known 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



## Crypto-Jacking

- Wired, 29 December 2017 *"Crypto-jacking has gotten out of control"*
  - Crypto-jacking, which exploded in popularity this fall, works by embedding a JavaScript component in a website that can leverage a visiting device's processing power to mine a cryptocurrency (usually Monero). Each visitor might only do a tiny bit of mining while they're there, but every user lending some hash power over time can generate real money.

## 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"*
  - The Trump administration acknowledged on Sunday that 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
  - FireEye, a computer security firm first raised the alarm about the Russian campaign after its own systems were also pierced

## Supply-Chain Attack

- NBC News, 3 February 2021 *"More exploitable flaws found in SolarWinds software, says cybersecurity firm"*
  - A cybersecurity company has identified three new "critical" flaws in software produced by SolarWinds, the company that was exploited in what U.S. officials said last year was a massive hack of U.S. government and corporate sites by Russian intelligence. The security company, Trustwave, said it informed SolarWinds about the vulnerabilities, which Trustwave said could have enabled an attacker to compromise the networks of SolarWinds customers



## Supply-Chain Attack

- ARS Technica, 16 February 2021 “*New type of supply-chain attack hit Apple, Microsoft and 33 other companies*”
  - Last week, a researcher demonstrated a new supply-chain attack that executed counterfeit code on networks belonging to some of the biggest companies on the planet, Apple, Microsoft, and Tesla included
  - 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 such as Apple, Microsoft, Tesla, and 33 other companies, Birsan was able to get these 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-recovery × 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” (Auto insurance, 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, never wears out, cannot be attacked with drills or explosives
- Plus, information can be effectively secured 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

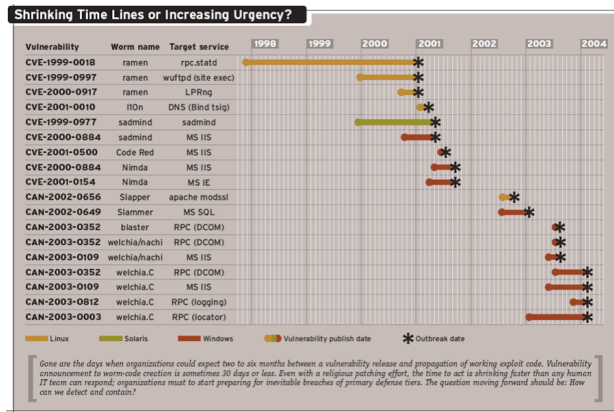
## Overview of Cybersecurity

- 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](http://www.nwc.com)), April 2004

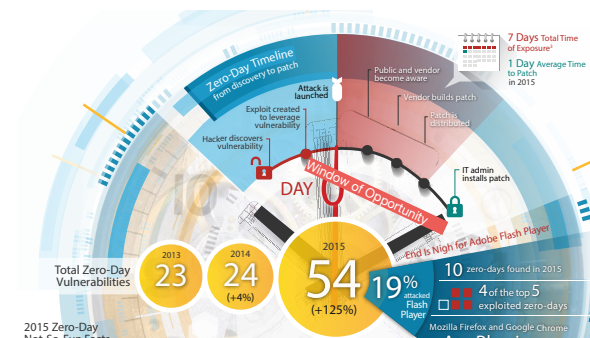
## Zero-Day

- **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 Bourne-Again *SHell*)
- 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 bash+3-025 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='\0 { :; }; echo vulnerable' bash -c "echo I hate colors"  
vulnerable  
I hate colors  
bash-3.2$  
bash-3.2$
```

## 2021 Security Summary

- *Nation-state attacks escalate*
  - The report accused the North Korean regime of conducting "operations against financial institutions and virtual currency exchange houses" to fund its nuclear and missile programs and to keep the country's struggling economy afloat
- *Another nation state made a debut in the on-going SolarWinds cyber security saga*
  - Russia was purportedly behind the massive supply chain hack last December that took aim at high-profile targets like the U.S. Commerce, Treasury, Homeland Security, and Energy departments along with private companies
  - But now Reuters is reporting that Chinese hackers also got in on the game, choosing a different line of attack

## 2021 Security Summary

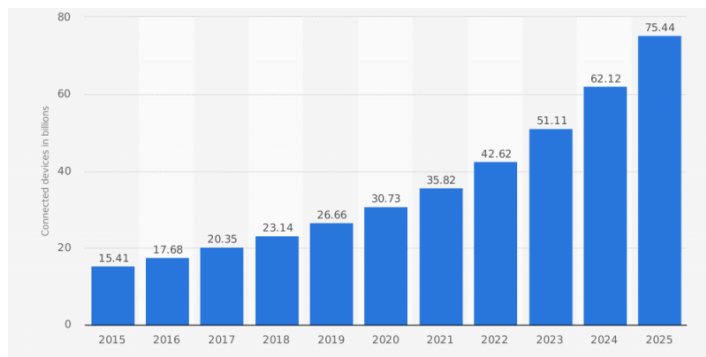
- *Apart from these high-profile examples, Iranian state-based hacking groups hit the radar screen, accused of spying on Iranian citizens around the globe*
  - The so-called Domestic Kitten group, has reportedly been conducting widespread surveillance for the last four years on a target list of about 1,200 individuals using a mobile malware called Furball to carry out its spying
  - The malware is then spread using phishing, Iranian websites, Telegram channels, and malicious SMS messages and can grab call logs, record communications, even steal files
- *Industrial IoT cyber security becoming a nightmare*
  - An incident in early February is a nod to future cyber security disasters as more devices and critical civil infrastructure is connected to the Internet
  - An unknown hacker broke into a water treatment plant in Oldsmar, FL, and took over the controls system to increase the levels of lye in the water to dangerous levels

## 2021 Security Summary

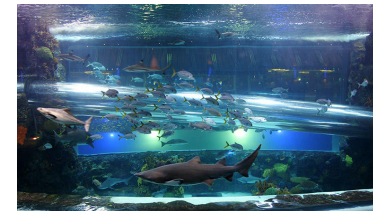
- *Cyber-crime pays*
  - Despite an overall decline in cyber-criminal activity, payments to ransomware gangs surged during 2020
  - According to research from Chainalysis, a blockchain analysis firm, ransomware payments using cryptocurrency spiked 311% in 2020, reaching a total volume of \$350 million

## 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 of 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.

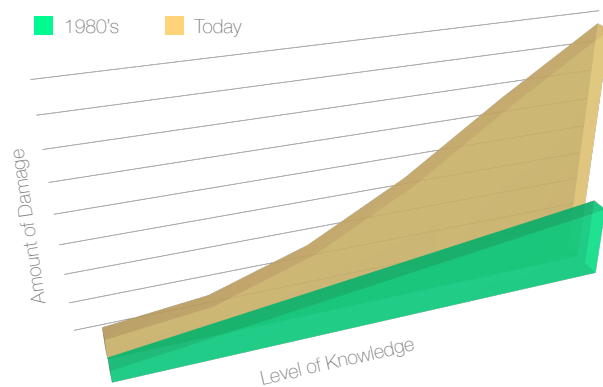
## Internet of Things

- ArsTechnica 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

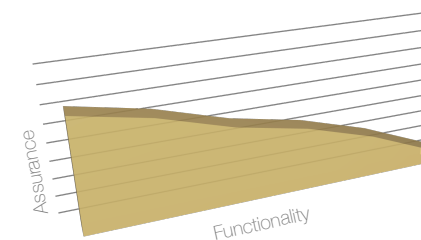
- What do locks, keys, values and the police have to do with cybersecurity?
  - **Locks**: authorization, access control mechanisms
  - **Keys**: authentication required to open a lock
  - **Police**: same as in the real world

## Gold Standard of Cybersecurity

- Any system claiming to be secure must contain mechanisms for
  - **Auth**entication
  - **Auth**orization
  - **Auth**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