

Computer Security

Introduction

Prof. Jean-Noël Colin

jean-noel.colin@unamur.be

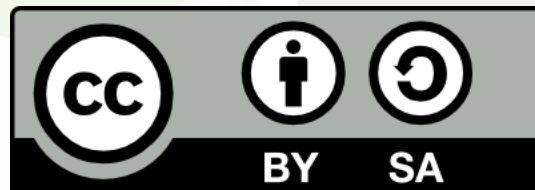
Office #306

University of Namur
Computer science faculty

www.unamur.be



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).



Agenda

- Objectives
- Context
- Issues
- Threats
- Definitions
- Solutions



Objectives

- Raise awareness
- Introduction to security
 - Threats
 - Security criteria
 - Countermeasures
 - Methodology
- Structured approach
- References and pointers

Computer systems are everywhere

- e-everything
 - e-Commerce
 - e-Banking
 - e-Government
 - e-Health
 - e-ntertainment, e-Learning, e-nergy, e-car
 - ...
 - ubiquitous and pervasive computing
 - mobile computing
 - 'smart' computing and devices
 - legal and regulatory context

Computer systems are getting more and more complex

- Trinity of trouble (G. Mc Graw)
 - Connectivity
 - larger and larger number and diversity of connected devices and communication means
 - increase in targets and attack vectors
 - no need of physical access to target
 - Extensibility
 - build by assembly and reuse
 - how to assess security of building blocks ?
 - Complexity
 - hardware and software architectures get more and more complex
 - how to assess the overall level of security ?

Mobile and open systems

- Mobility
 - users
 - devices
- Open and inter-connected environments
 - business integration, SOA...
 - multi-party computing
- Security of User-provided content (Web 2.0)
 - reliable? secure?
- Fast developing threats
 - Beyond script kiddies, criminal organizations, governments, industrials
 - targeted

Mobile and open systems



Mobile and open systems



Legal and regulatory constraints

- Just to mention a few

- Privacy

- European General Data Protection Regulation (May 2018)
 - Taking over from belgian law (Dec. 8th, 1992), European directive 95/46
 - general principles : accountability, fair and lawful processing, purpose limitation and specification, minimal storage term, transparency (consent), data quality, security, data minimisation, special categories of data
 - HIPAA – Health Insurance Portability and Accountability Act (1996)
 - COPPA – Children’s Online Privacy Protection Act
 - Sarbanes-Oxley (SOX) 2002







Consequences of a security breach

- Would you report a security breach ?
 - many incidents not reported, because organizations
 - didn't detect
 - do not want to reveal their weaknesses
 - are not prepared or equipped to deal with the crisis
 - do not trust the authorities
 - in some cases, a legal obligation

Consequences of a security breach

- business continuity
- information security, IPR
- financial
- reputation
- trust of shareholders/customers/users
- compliance (privacy ...)
- hardware and infrastructure security
- loss of data can lead to the end of the organization

Just a few examples

 <p>SEP 07 BY DANNY BRADBURY 0</p> <p>Dark web sites could be exposed by routine slip-up</p>	 <p>SEP 06 BY LISA VAAS 0</p> <p>Mobile spyware maker mSpy leaks millions of records – AGAIN</p>	 <p>SEP 06 BY DANNY BRADBURY 1</p> <p>Social Security numbers exposed on US government transparency site</p>
 <p>SEP 06 BY JOHN E DUNN 1</p> <p>Thousands of unsecured 3D printers discovered online</p>	 <p>SEP 06 BY LISA VAAS 4</p> <p>Ungagged Google warns users about FBI accessing their accounts</p>	 <p>SEP 05 BY PAUL DUCKLIN 4</p> <p>MEGA secure upload service gets its Chrome extension hacked</p>

Just a few examples

LATEST NEWS

Sep 10, 2018



No.1 Adware Removal Tool On Apple App Store Caught Spying On Mac Users

A highly popular top-tier app in Apple's Mac App Store that's designed to protect its users from adware and malware threats has been, ironically, found surreptitiously stealing their browsing history without their consent, and sending it to a server in China. What's more concerning? Even after ...

[Read More](#)



British Airways Hacked – 380,000 Payment Cards Compromised

British Airways, who describes itself as "The World's Favorite Airline," has confirmed a data breach that exposed personal details and credit-card numbers of up to 380,000 customers and lasted for more than two weeks. So who exactly are victims? In a statement released by British Airways on ...

[Read More](#)



U.S. Charges North Korean Spy Over WannaCry and Sony Pictures Hack

The U.S. Department of Justice announces criminal charges against a North Korean government spy in connection with the 2017 global WannaCry ransomware attack and the 2014 Sony Pictures Entertainment hack. According to multiple government officials cited by the NY Times who are familiar with the ...

[Read More](#)



Just a few examples

Apple gets cored: 90GB of 'secure files' stolen by high schooler

17 AUG 2018 12

Apple, Law & order, Organisations, Security threats



Just a few examples

Chinese hotel chain's customer data
on Dark Web – 500M records for
\$50K

30 AUG 2018 0



Just a few examples

Pacemaker hack can deliver deadly 830-volt jolt

Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination

By Jeremy Kirk

IDG News Service | Oct 17, 2012 1:40 AM PT

RELATED TOPICS

[Network Security](#)

[Security](#)

Pacemakers from several manufacturers can be commanded to deliver a deadly, 830-volt shock from someone on a laptop up to 50 feet away, the result of poor software programming by medical device companies.

RELATED

[Top hacker dies days before scheduled Black Hat talk](#)

[Wireless medical devices face myriad security concerns](#)

[InfoSec community mourns the loss of well-known hacker Barnaby Jack](#)

[on IDG Answers](#) ➔

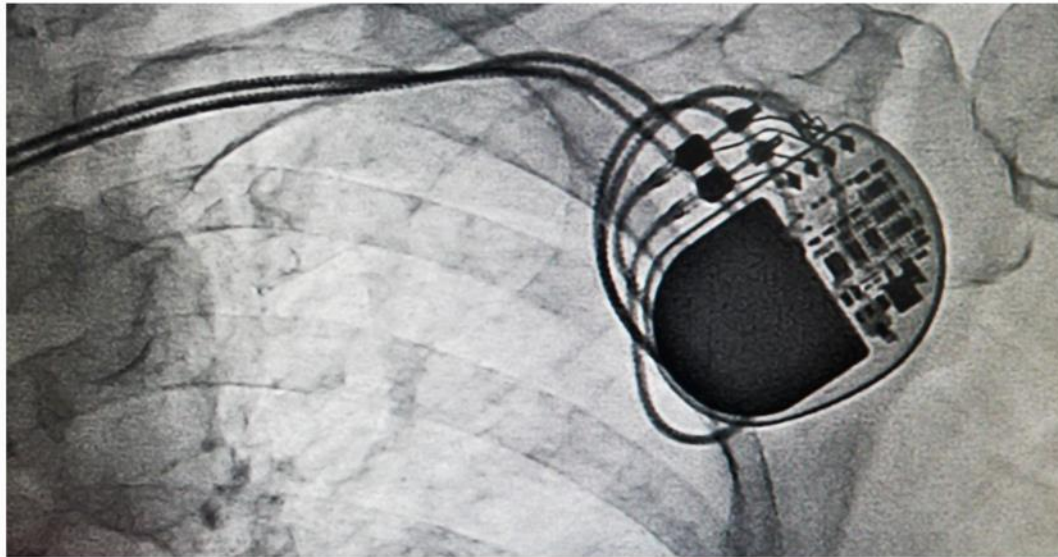
[How can wireless carriers detect if you are tethering your device?](#)

Just a few examples

Pacemaker controllers still vulnerable 18 months after flaws reported

14 AUG 2018 0

Black Hat, IoT, Security events, Security threats, Vulnerability



Just a few examples

Healthcare IT News

TOP

When medical devices get hacked, hospitals often don't know it

The threat to medical devices is real and happening now – and it's a patient safety issue, much more than one of HIPAA compliance.

By [Jessica Davis](#) | May 11, 2018 | 09:54 AM



Just a few examples

Krebs on Security

In-depth security news and investigation

24 Hackers Breached Virginia Bank Twice in Eight Months, Stole \$2.4M

JUL 18

Hackers used phishing emails to break into a Virginia bank in two separate cyber intrusions over an eight-month period, making off with more than \$2.4 million total. Now the financial institution is suing its insurance provider for refusing to fully cover the losses.

According to a lawsuit filed last month in the Western District of Virginia, the first heist took place in late May 2016, after an employee at **The National Bank of Blacksburg** fell victim to a targeted phishing email.

Just a few examples

1. The Mirai Botnet (aka Dyn Attack)

Back in October of 2016, [the largest DDoS attack ever was launched on service provider Dyn](#) using an IoT botnet. This led to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware. These devices were things like digital cameras and DVR players.

Much of the embedded firmware running connected devices is insecure and highly vulnerable, leaving an indeterminate number of critical systems at risk.

[CLICK TO TWEET](#) 

Just a few examples



August 25, 2017



Hacking IoT Devices: How to Create a Botnet of Refrigerators

DDoS attacks that use botnets made of IoT devices are not just possible—they're happening.

You see threat lists and news articles that mention the Internet of Things (IoT) getting hacked as a major concern all the time. But what does that mean?

To many people, the entire concept is an abstraction. Some folks still see hacking through a 90's movie lens where the hacker smashes keys and says stuff like, "I'm tapping into the mainframe." So, envisioning a scenario where someone could hack a thermostat and do much more than turn on your heat is kind of difficult.

Just a few examples

THE  TIMES

Hackers could take control of cars and kill millions, ministers warned

Andrew Ellson,
Consumer Affairs Correspondent

November 20 2017, 12:01am,
The Times

Law

Education

Investment

Crime

Politics



Carmakers must fix vulnerabilities in motor technology, one of the world's experts in vehicle software has said
PA

Modern cars are an “open door” to hackers, inviting hostile states to use Britain's roads as a weapon against citizens, ministers have been warned.

Deaths are inevitable within five years if carmakers do not fix vulnerabilities in technology, one of the world's experts in vehicle software has said.

Just a few examples

Forbes

Billionaires

Innovation

Leadership

Money

Consumer

Industry

save points.

Delta Deduplication.

49,674 views | Mar 16, 2018, 06:00am

Russia Hacks Into U.S. Power Plants, But Nuclear Reactors Should Be Impervious



James Conca Contributor ⓘ

Energy

I write about nuclear, energy and the environment

Just a few examples



The screenshot shows the top section of The Guardian's website. At the top left is a black button that says "Support The Guardian". To its right are links for "Subscribe", "Find a job", "Sign in / Register", and a "Search" dropdown. On the right side of the top bar is the "International edition" link with a dropdown arrow. Below this is a navigation bar with categories: "News" (underlined in red), "Opinion", "Sport", "Culture", "Lifestyle", and "More" with a dropdown arrow. The main masthead "The Guardian" is on the right. Below the navigation bar is a horizontal menu with various news sections: "World", "UK", "Science", "Cities", "Global development", "Football", "Tech", "Business", "Environment", and "Obituaries". The "Tech" section is highlighted. The main content area features a "Malware" sub-header in red, followed by a large red headline: "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017". Below the headline is a short paragraph: "Most first encountered ransomware after an outbreak shut down hospital computers and diverted ambulances this year. Is it here to stay?". To the right of the article is an advertisement box titled "Advertisement" with the text "Ad closed by Google". It contains a blue button labeled "Report this ad" and a link "Why this ad? |>".

Support The Guardian

Subscribe Find a job Sign in / Register Search

International edition

News Opinion Sport Culture Lifestyle More

The Guardian

World UK Science Cities Global development Football Tech Business Environment Obituaries

Malware

WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Most first encountered ransomware after an outbreak shut down hospital computers and diverted ambulances this year. Is it here to stay?

Advertisement

Ad closed by Google

Report this ad

Why this ad? |>

Just a few examples

CYBERSECURITY

[TECH](#)[MOBILE](#)[SOCIAL MEDIA](#)[ENTERPRISE](#)[CYBERSECURITY](#)[TECH GUIDE](#)

Turkish 'hacktivists' take over social media accounts of US journalists

- "Hacktivists" are activists that use various hacking methods to spread their political viewpoints, usually by breaking into social media accounts of prominent individuals or attacking prominent websites.
- Reporters from Fox News, Bloomberg and The New York Times had social media accounts co-opted in the attacks over the past two weeks, according to research by cybersecurity company CrowdStrike.

Kate Fazzini

Published 1:57 PM ET Fri, 24 Aug 2018 | Updated 4:13 PM ET Fri, 24 Aug 2018



Just a few examples

Huawei and ZTE banned from selling 5G equipment to Australia

- China's Huawei and ZTE have been banned from providing 5G technology equipment to Australia, citing national security concerns.
- Huawei said the move was "extremely disappointing."
- Australia's government did not name the Chinese firms, but said companies with "extrajudicial directions from a foreign government" may not adequately protect a mobile network.

Arjun Kharpal | [@ArjunKharpal](#)

Published 4:00 AM ET Thu, 23 Aug 2018 | Updated 4:59 AM ET Thu, 23 Aug 2018



Just a few examples

- Beyond attacks
 - failure (hardware, software, human)
 - natural disaster (flooding, fire, earthquake)
 - sabotage, terrorism ...



Some attacks

- Infrastructure
 - (Distributed) Denial of Service – (D) DoS
 - DNS attacks
 - cache poisoning
 - compromised DNS server
 - spoofing
 - routing attack
 - sub-optimal routing
 - congestion
 - network partitioning
 - load/path overload

Some attacks

- Software
 - code injection
 - data encoding
 - error handling
 - weak crypto mechanisms or bad implementation
 - bad configuration
 - ...
- Any part of the information system can be the target

Information security

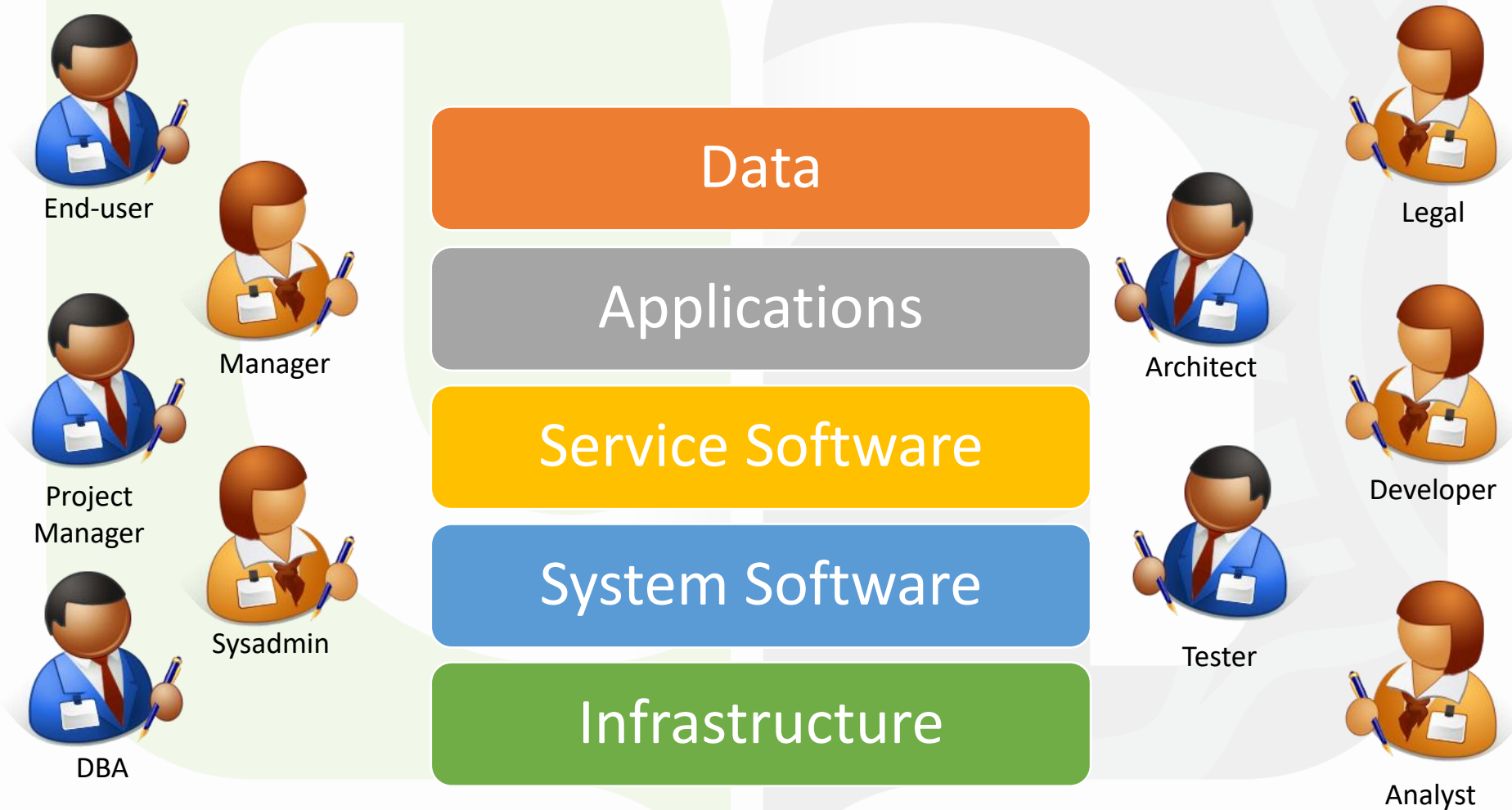
- Security is not a monolithic property, but is the aggregation of independent objectives defined by
 - criteria
 - level
- Security triad
 - [Confidentiality] property that information is not made available or disclosed to unauthorized individuals, entities or processes (when stored, exchanged or processed)
 - [Integrity] property of accuracy and completeness (when stored, exchanged or processed)
 - [Availability] property of being accessible and usable upon demand by an authorized entity
- Often completed with
 - [Traceability (auditability, proof)] ability to trace an event back to its origin

Information security

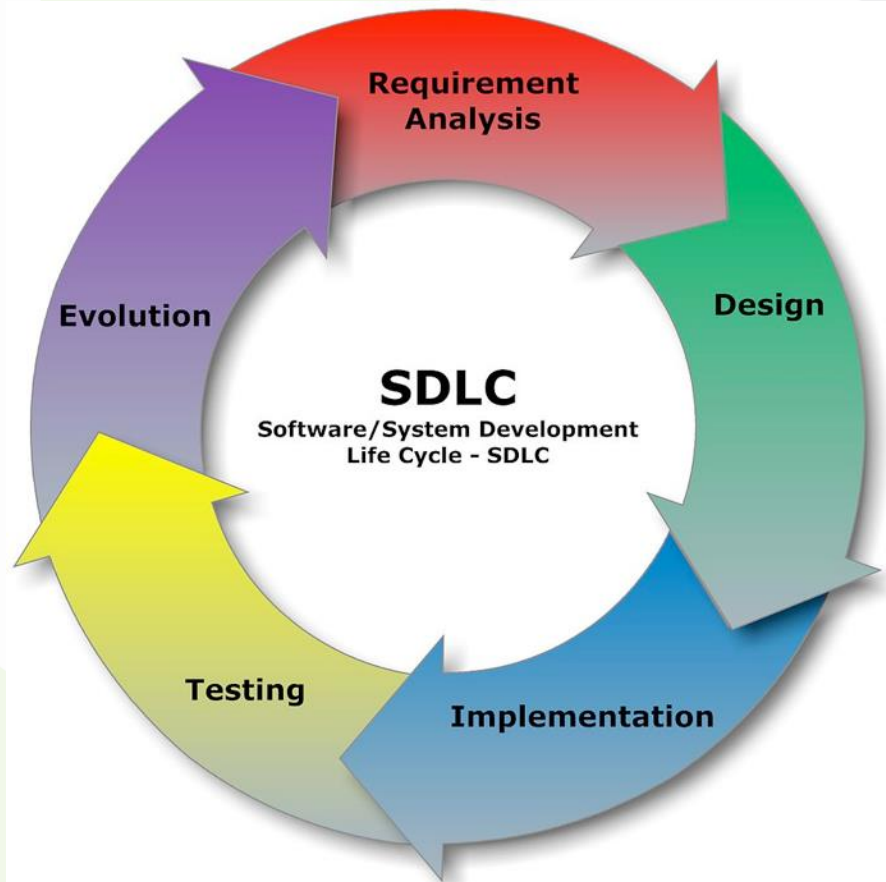
- Some other criteria

- [Authenticity] property that an entity is what it claims to be
- [Non-repudiation] ability to prove the occurrence of a claimed event or action and its originating entities
- [Reliability] property of consistent intended behaviour and results

Information system: layered approach



Information System Lifecycle



Improving security

- A structured approach
 - integrated: technical is not enough: management and legal have to be there
 - in depth: one line of defense is not enough! secure each layer
 - continuous
- When to act ? 3 lines of defense
 - Before incident... prevention
 - avoid vulnerabilities
 - During incident... detection
 - detect and notify incidents
 - After incident... recovery
 - restore system to operational state

Improving security

- Examples of security measures
 - Software development
 - security requirement engineering
 - threat modeling
 - secure programming
 - static analysis
 - ...
 - Infrastructure
 - security technologies
 - patches, updates
 - documentation, procedures
 - ...
 - Awareness raising and training
- Not all security measures are technical!

“Distrust and caution are the parents of security”

Benjamin Franklin