Parte 2:

Comprensione

Natura del software
Volontà e macchine
Attacchi mirati e non mirati

Informatica: Dato di fatto

- **Ogni** sistema ha **numerose vulnerabilità** (caratteristiche indesiderate)
- Permettono **uso arbitrario** da parte di **chiunque**

- Non evidenti (ma **ci sono**)
- **Chi** le trova può **sfruttarle**

- Unica tecnologia della storia con questa caratteristica

Esempio: Microsoft (Aprile 2017)

- A ...vulnerability exists in the way that **Microsoft Office and WordPad** parse specially crafted files
- An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
- An attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file

Esempio: Microsoft (Settembre 2017)

- A ...vulnerability exists when **Microsoft .NET Framework** processes untrusted input
- An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
- To exploit the vulnerability, an attacker would first need to convince the user to open a malicious document or application.

Lezione appresa

- **UN** click può essere sufficiente per **perdere il controllo** del proprio dispositivo / dati
  - Senza che ci sia una notifica evidente...
- L'**inganno dell'utente** è una tecnica potentissima e (in questi casi) necessaria
- Utente **crede** di eseguire una certa azione ed in realtà ne sta eseguendo una diversa

Esempio: Apple (Settembre 2017)

`Alert ID: GCSA-17055`

- ...
- Apple ha rilasciato degli aggiornamenti di sicurezza che risolvono alcune vulnerabilita' presenti in vari software.
- Un aggressore remoto potrebbe sfruttare alcune di queste vulnerabilita' per prendere il controllo dei sistemi esposti.
- `Apple iOS`
  `Apple tvOS`
  `Apple watchOS`
  `Apple Safari`
  `Apple Xcode`

Vulnerability: Quante sono?

Computer Security Resource Center

National Vulnerability Database

NIST

National Institute of Standards and Technology

Search Parameters:

- Results Type: Overview
- Search Type: Search Last 3 Years
- Keyword (text search): android

There are **3,229** matching records.
Displaying matches **1** through **20**.

Search Parameters:

- Results Type: Overview
- Search Type: Search Last 3 Years
- Keyword (text search): apple

There are **1,770** matching records.
Displaying matches **1** through **20**.

Quali software?
SAP (Maggio 2016)

Alert (TA16-132A)
Exploitation of SAP Business Applications

Systems Affected
Outdated or misconfigured SAP systems

Overview
Exploitation of the vulnerability gives **unauthenticated remote attackers** **full access** to affected SAP platforms, providing **complete control** of the business information and processes on these systems...

Quali software?
Antivirus (Luglio 2016)

Alert (TA16-187A)

Symantec and Norton Security Products Contain Critical Vulnerabilities

Systems Affected

All Symantec and Norton branded antivirus products

Overview

Exploitation of these vulnerabilities could allow a **remote attacker** to **take control** of an affected system.

Quali software?
Automobili (September 2016)

- From 12 miles away, while the car was moving
- ...remotely slam on the **brakes**, pop the **trunk** and fold in the **side mirror**...
- ...opened the **sunroof**, moved the power **seats**, and switched on the **turn signals**.

Quali software?
Pompe per diabetici (October 2016)

J&J warns diabetic patients: Insulin pump vulnerable to hacking

- ...a **remote attacker** can spoof the meter and **trigger unauthorized insulin injections**...
- ...these attacks could be performed from one to two kilometers away...

Quali software? Pacemakers (August 2017)

465,000 Patients Need Software Updates for Their Hackable Pacemakers, FDA Says

MOTHERBOARD

- The recall has the goal of reducing the risk of hackers taking control of the pacemakers, potentially, harming the patients.

Gli ultimi mesi…

- "KRACK" **Protocollo WiFi**
  - Attaccante può decrittare tutto il traffico della cella in cui si trova
- "Meltdown" e "SPECTRE" **Hardware**
  - Un programma (maligno) può leggere memoria a cui non dovrebbe potere accedere

- **Tutti** i dispositivi degli ultimi anni **vulnerabili**
- **Nessuno** se ne era accorto

"Ho l'antivirus!"

- Rileva **poche** tipologie di attacco
- Quelle poche, inizia a rilevarle con **giorni** o **settimane** di ritardo

Wannacry (Maggio 2017): 30 minuti

150 paesi
100.000 organizzazioni

Attack Focus

- **Mirato**
  1. Scelgo il target
  2. Ispeziono il target e vedo quali exploit posso usare

  - Costoso, Manuale

- **Non mirato**
  1. Tento di iniettare uno stesso exploit su molti target
  2. Vedo quali target ho colpito

  - Economico (costi incrementali irrisori), Automatizzato

"Chi vuoi che attacchi proprio me?"

- Ragionamento **SBAGLIATISSIMO**
  - Posso essere colpito da attacchi **non mirati**
  - Sono **i più comuni**

- Non sono colpito in quanto "Alberto Bartoli"
- Sono colpito in quanto
  - Windows 8.1 versione 6.5.4
  - Adobe Acrobat versione 16.10.23
  - ...
  - Ho account Facebook
  - Ho account Paypal
  - ...

Estate 2017: NON MIRATI

Last month's malware outbreak cost this household company £100 million

Reckitt Benckiser

tripwire

Shipping Company Maersk Says NotPetya Cyberattack Could Cost Up to $300M

tripwire

NotPetya cyber-attack cost TNT at least $300m

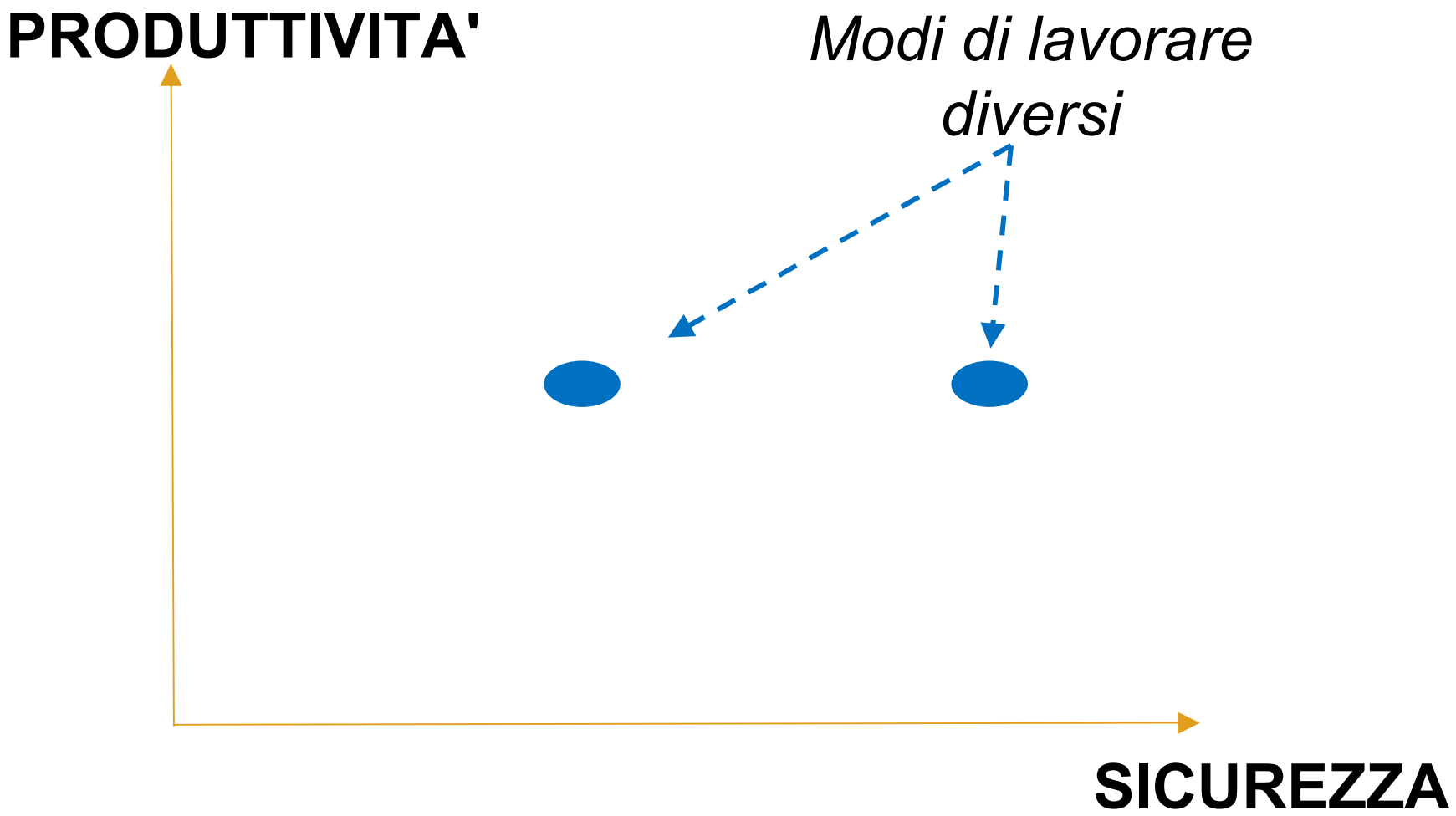
BBC

Processo collettivo

- Non è un evento **puntuale**, responsabilità dei **soli tecnici**
  - Investo X euro
  - Compro, Configuro, Sistemo

- E' un processo **continuo**, responsabilità di **tutti**
  - Vulnerabilità e tecniche di attacco cambiano
  - Software diventano obsoleti
  - Tutti gestiscono informazioni/dispositivi di potenziale valore

Produttività e Sicurezza



Security = Compromesso