Secure Systems Engineering
(Introduction)

Chester Rebeiro

IIT Madras

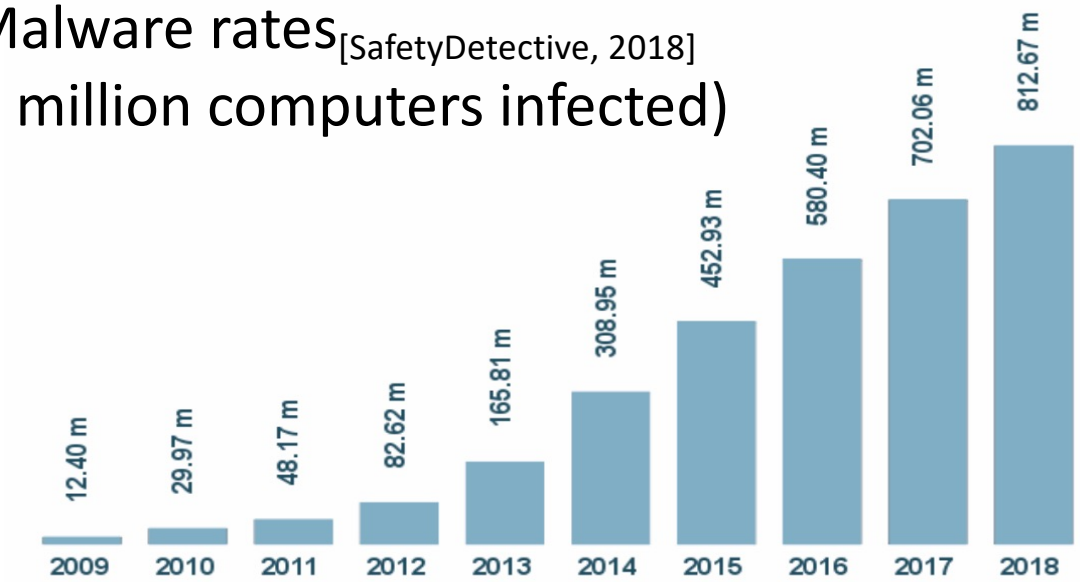
Computer System Protection

Find vulnerability then patch

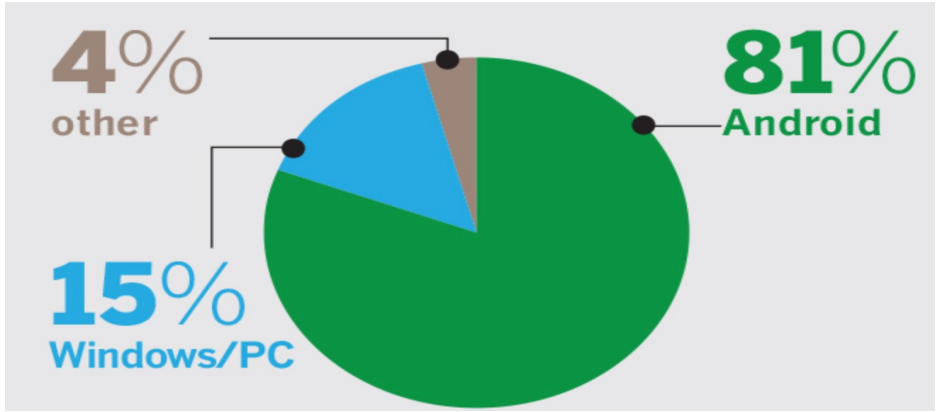
- Attackers find new ways to compromise the system
- Attackers look at security patches, to find the vulnerabilities that have been fixed and attack systems which do not apply patch [Wannacry]
- Every new feature added to the software may be a source of new vulnerabilities

Rise of Malware

Malware rates[SafetyDetective, 2018]
(in million computers infected)



Malware Target Device[NOKIA, 2016]
(rate of increase)



IoT malware samples increased by 3x in 2018-H1[Kaspersky,2018]

Number of New Attack Vectors continuously rising

Where did we go wrong?

Mainframes (1960-1975)

General Electric GE-600 series mainframe computer

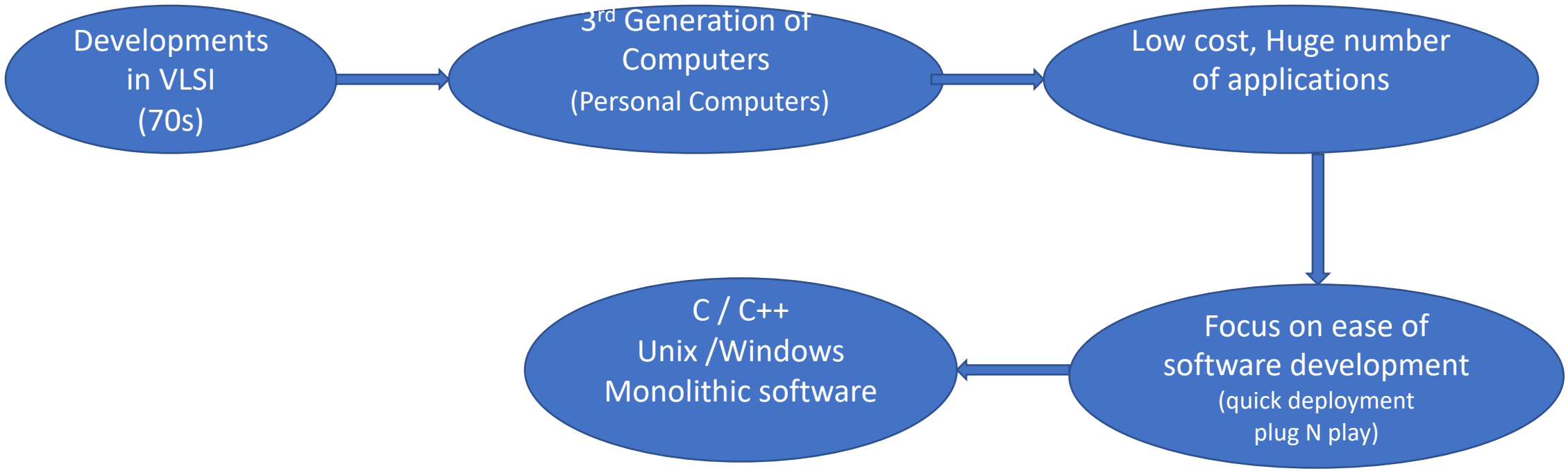
Cost: over USD 1,000,000

Cold war era
Large number of users with conflicting interests ranging from

- Top secret military applications
- Business applications
- Computer games and other leisure applications

“Security the prime concern”

Wind of change



“Security less of a concern”

New Computing Paradigms

Internet
(computers got connected)

IoT
(devices got connected)

Cloud Computing
(computing got offloaded)

- Personal computers not personal anymore
- All of this built over computers that have low security levels.
- Security suddenly became very important criteria

New Computing Paradigms

Internet
(computers got connected)

- Personal computers not personal anymore

ve low security levels.

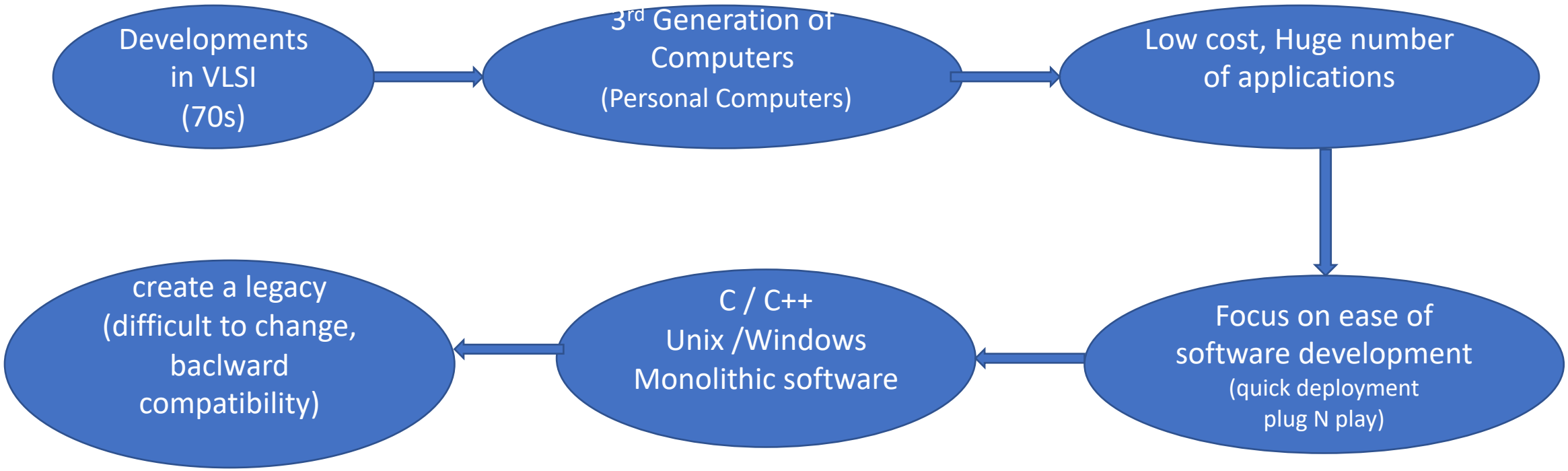
Io
(d

ant criteria

Computers not secure anymore!!!

Cloud Computing
(computing got offloaded)

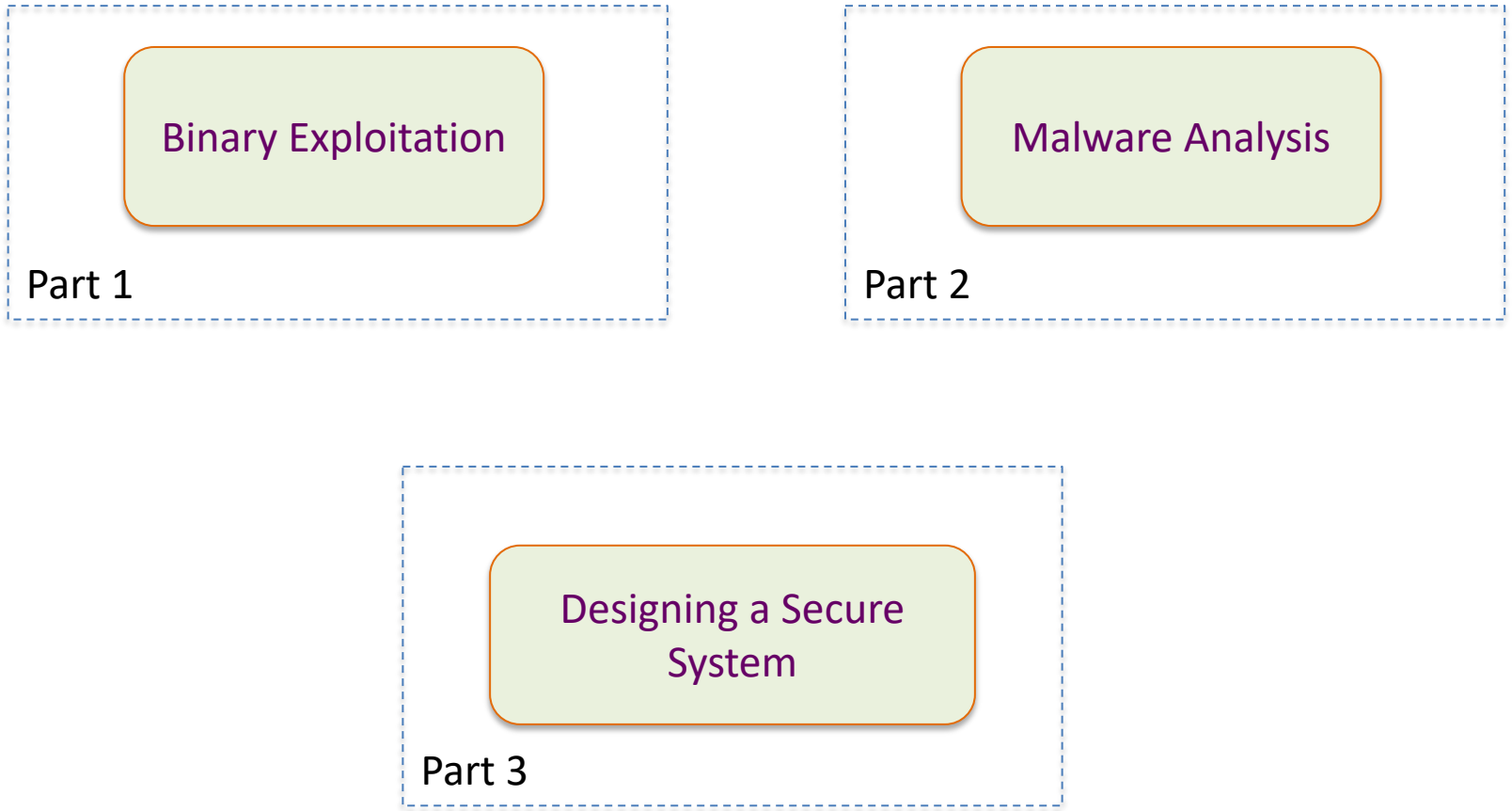
legacy


Developments in VLSI (70s)
3rd Generation of Computers (Personal Computers)
Low cost, Huge number of applications
Focus on ease of software development (quick deployment plug N play)
C / C++ Unix /Windows Monolithic software
create a legacy (difficult to change, baclward compatibility)

Design for Security

DevSecOps

Course Structure



What to expect during this course

- Deep dive into systems:
  - Software
    - Assembly level
    - Compiler and OS level

      (Programming assignments in class and homework)

- Analysis techniques
    - Static, dynamic analysis / symbolic execution
    - Statistical analysis techniques and some ML

      (Programming assignments for homework)

- Reading assignment

Expected Learning Outcomes

- Understand how C and C++ programs really work!
- Understand the internals of malware and other security threats
- Evaluate security measures applied at the hardware, OS, and compiler
- Understand trade offs between performance and security
- Malware families and malware analysis

Grading

Q1. : 20 marks

Q2 : 20 marks

End Semester / Course Project : 20 marks

Assignments : 40 marks

LOGISTICS

Classes will be held from 16th Jan, 2022 in Slot C at CS36 (CSE, IITM)

- Monday : 10:00 - 10:50 AM
- Tuesday : 9:00 - 9:50 AM
- Wednesday : 8:00 - 8:50 AM
- Friday: 12:00 - 12:50 PM (will be used for Lab and Tutorials)

TAS

- Keerthi K (RISE Lab)
- Pallavi Borkar (RISE Lab)
- Reetwik Das (RISE Lab)
- Sai Venkata Krishnan V (RISE Lab)
- Saltanat (RISE Lab)
- Dhiraj Prajapati (RISE Lab)
- Devashish Dewangan (RISE Lab)
- Parkhiya Dixit (RISE Lab)

WEBPAGE

https://sites.google.com/cse.iitm.ac.in/cs6570-2023/

MICROSOFT TEAMS GROUP

6z998qd