Vulnerability Assessment and Reverse Engineering

Lecture

10

Introduction to Reverse Engineering

Dr Syed Muhammad Sajjad
Department of Cyber-Security,
Faculty of Computing and Artificial Intelligence,
Air University, Islamabad, Pakistan.

System Re-Engineering

- Re-structuring or re-writing part or all of a legacy system without changing its functionality
- Applicable where some but not all sub-systems of a larger system require frequent maintenance
- Re-engineering involves adding effort to make them easier to maintain
- The system may be re-structured and re-documented

When to Re-Engineer

- When hardware or software support becomes obsolete
- When new ways of accessing are needed

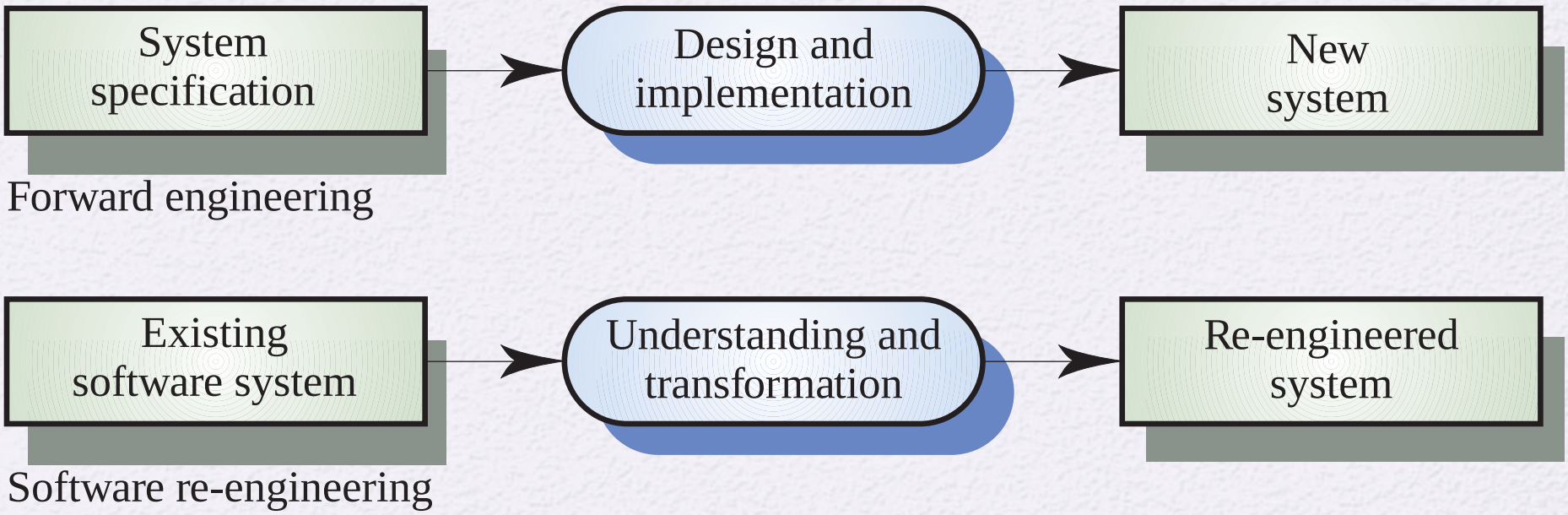
Re-Engineering Advantages

- Reduced risk
  - There is a high risk in new software development
  - There may be development problems, staffing problems and specification problems
- Reduced cost
  - The cost of re-engineering is often significantly less than the costs of developing new software

Business Process Re-Engineering

- Concerned with re-designing business processes to make them more responsive and more efficient
- Often reliant on the introduction of new computer systems to support the revised processes
- May force software re-engineering as the legacy systems are designed to support existing processes

Forward Engineering & Re-Engineering



Forward Engineering & Re-Engineering

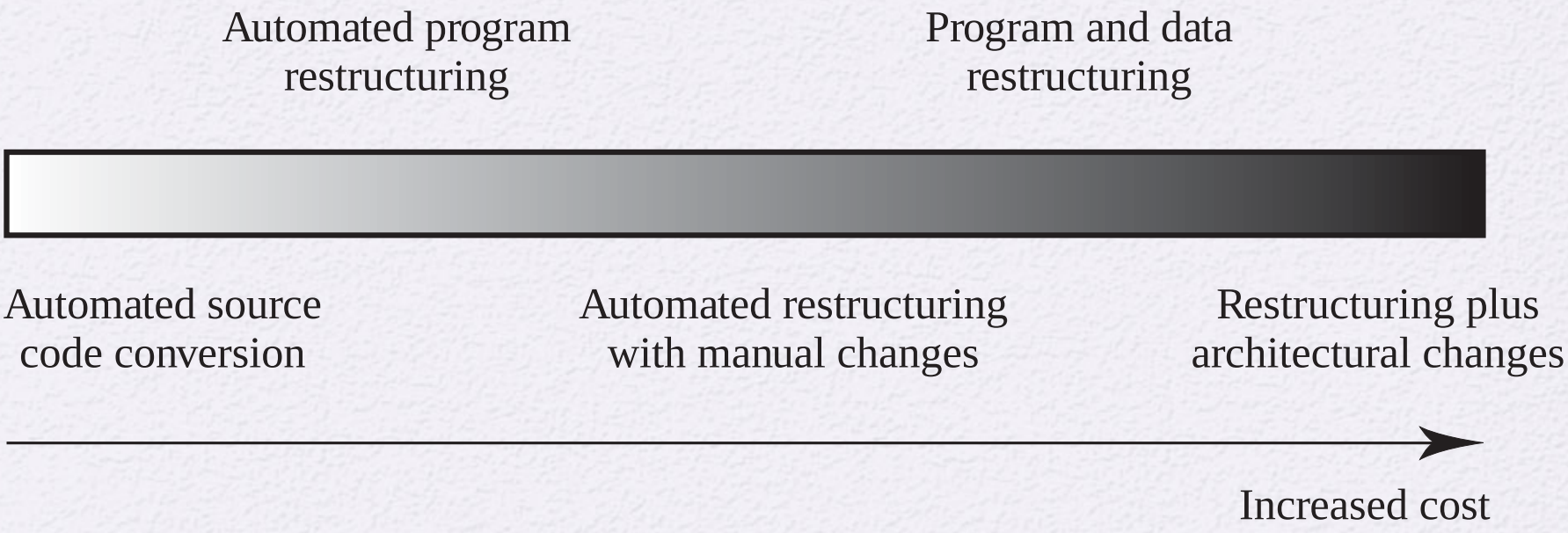
"**Forward engineering** is the traditional process of moving from high-level abstractions and logical, implementation-independent designs to the physical implementation of a system."

[ElliotChikofsky and JamesCross, Reverse Engineering and Design Recovery: A Taxonomy, IEEE Software 7(1):13-17, 1990.]

Re-Engineering Cost Factors

- The *quality* of the software to be re-engineered
- The *tool support* available for re-engineering
- The *extent of the data conversion* which is required
- The availability of *expert staff* for re-engineering

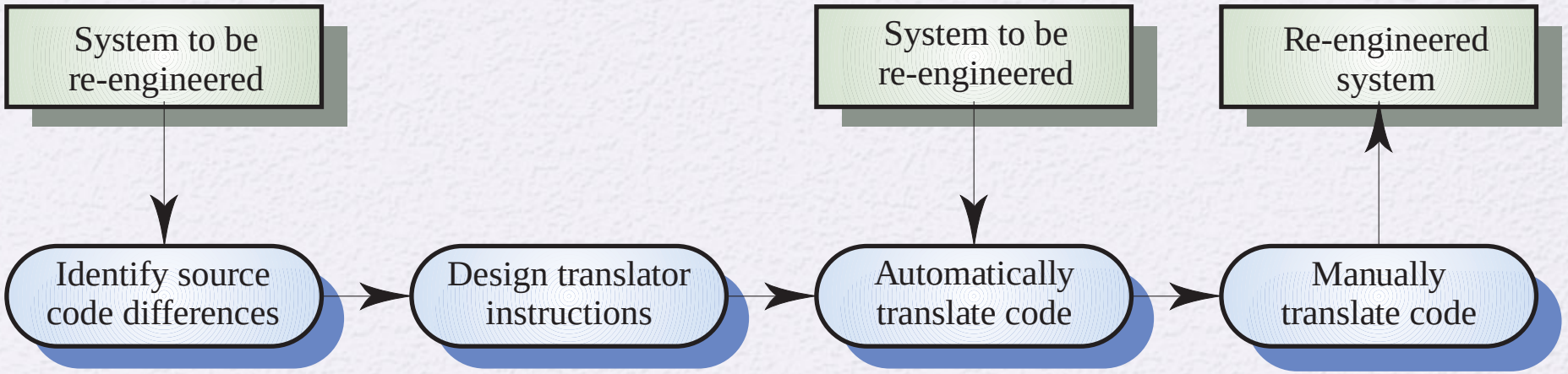
Re-Engineering Approaches



Source Code Translation

- Involves converting the code from one language (or language version) to another e.g. FORTRAN to C
- May be necessary because of:
  - Hardware platform update
  - Staff skill shortages
  - Organisational policy changes
- Only realistic if an automatic translator is available

The Program Translation Process



Reverse Engineering

- Analysing software with a view to understanding its design and specification
- May be part of a re-engineering process but may also be used to re-specify a system for re-implementation
- Builds a program data base and generates information from this
- Program understanding tools (browsers, cross-reference generators, etc.) may be used in this process

Reverse Engineering

- **Reverse engineering** is the process of analysing a subject system with two goals in mind:
  - To identify the system's components and their interrelationships; and
  - To create representations of the system in another form or at a higher level of abstraction

[ElliotChikofsky and JamesCross, Reverse Engineering and Design Recovery: A Taxonomy, IEEE Software 7(1):13-17, 1990.]

Reverse Engineering

- Breaking something down and putting it back together is a process that helps people understand how things were made
- The complex nature of the human anatomy requires people to understand each and every part of the body. How? By dissecting it
- Reverse engineering is a way for us to understand how things were designed, why is it in its state, when it triggers, how it works, and what its purpose is
- In effect, the information is used to redesign and improve for better performance and cost

Reverse Engineering

- Imagine if the Trojan Horse was thoroughly inspected and torn down before it was allowed to enter the gates of a city
- This would probably cause a few dead soldiers outside the gate fighting for the city
- The next time the city is sent another Trojan Horse, archers would know where to point their arrows
- And no dead soldiers this time
- The same is true for malware analysis—by knowing the behaviors of a certain malware through reverse engineering

Reverse Engineering

- the analyst can recommend various safeguards for the network
- Think of it as the Trojan Horse being the malware
- The analyst being the soldier who initially inspected the horse, and
- The city being the network of computers
- In the software security industry, one of the core skills required is reverse engineering
- Every attack, usually in the form of malware, is reversed and analyzed

Reverse Engineering

- The first thing that is usually needed is to clean the network and systems from being compromised
- An analyst determines how the malware installed itself and became persistent
- The analysis provides information about how the malware was able to compromise the system
- With this information, network administrators are able to impose policies to mitigate the attack
- If the malware was able to enter the system because of a user opening an email attachment that contains JavaScript code

Reverse Engineering

- The network administrator would implement the blocking of emails that contain a JavaScript attachment
- Some administrators are even advised to restructure their network infrastructure
- Once a system gets compromised, the attackers may already have got all of the information about the network, and would easily be able to make another wave of the same attack
- Making major changes will greatly help prevent the same attack from happening again

Reverse Engineering

- Part of restructuring the infrastructure is education
- The best way to prevent a system from being compromised is by educating its users about securing information, including their privacy
- Knowing about social engineering and having experience of previous attacks makes users aware of security
- It is important to know how attackers are able to compromise an institution and what damage they can cause
- As a result, security policies are imposed, backups are set up, and continuous learning is implemented