Managing the Development of Secure Systems

Chapter 25 of “security engineering” by Ross Anderson

PRESENTED BY : ROSE BADER

SECURITY is an organizational PROCESS not a destination

If so then what is a SECURE system ?

What will we be talking about ?

- Managing a Security Project
- Security Requirements Engineering
- Risk Management
- Methodology

A Tale of Three Siblings

Security Requirements Engineering

"Security requirements engineering is often the most critical task of managing secure system development, and can also be the hardest"

1

Managing Project Requirements

2

Parallelizing the Process

3

Managing Requirements Evolution

Managing Project Requirements

Building things from scratch is an accident-prone business

The millennium bug gives another useful data point, which many writers on software engineering still have to digest.

So the requirements engineer needs to acquire a deep knowledge of the application as well as of the people who might attack it and the kind of tools they might use.

Human nature doesn't change much. Historical parallels will also make it much easier for you to sell your proposal to your client's board of directors.

You will likely find that a security requirements specification for a new project requires iteration, so it's more likely to be spiral model than waterfall model.

Security Requirements Engineering

"Security requirements engineering is often the most critical task of managing secure system development, and can also be the hardest"

1. Managing Project Requirements

2. Parallelizing the Process

3. Managing Requirements Evolution

Parallelizing the Process

An interesting question here is how to brainstorm a specification by just trying to think of all the things that could go wrong.

There is also an interesting analogy with the world of software testing where it is more cost efficient to test in parallel rather than series

If your target system is something novel, then instead of paying a single consultant to think about it for twenty days, consider getting fifteen people with diverse backgrounds to think about it for a day each.

People will naturally think of the problems that might make their own lives difficult, and will care less about things that inconvenience others.

Risk Management

“The purpose of business is profit, and profit is the reward for risk”

- Where the science is unknown or inconclusive, people are free to project all sorts of fears and prejudices
- Mitigating and managing the tensions between employees’ duty to maximize shareholder utility, and their natural tendency to maximize their own personal utility instead.
- As a result we see the growing use of stock options and bonus schemes to try to align employees’ interests with shareholders’.

Methodology

Top-Down Design
(waterfall model)

Iterative Design
(spiral model)

Top-Down Design

- At the first two steps in this chain there is feedback on whether we're building the right system (*validation*)
- At the next two on whether we're building it right (*verification*)
- It may increase cost transparency
- It's compatible with a wide range of tools.
- Where it can be made to work, it's often the best approach

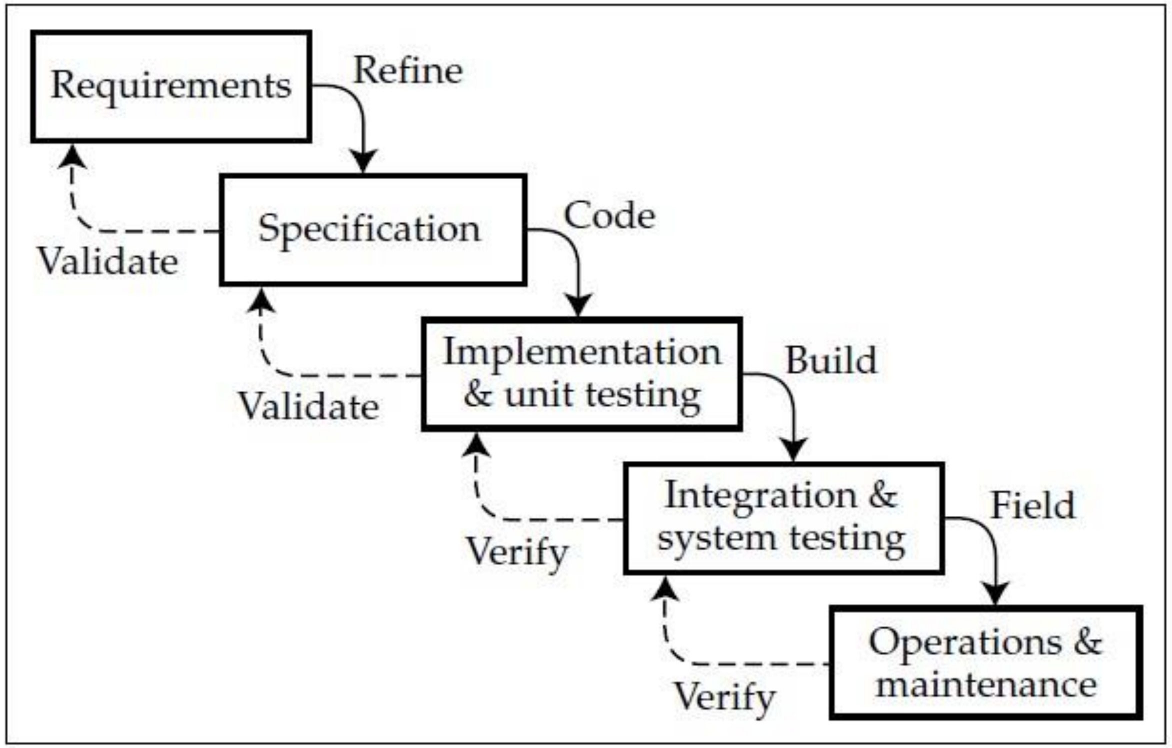


Figure 25.1: The waterfall model

Iterative Design

- When we're starting from an existing product which we want to improve.
- The requirements aren't understood yet by the customer, and a prototype is necessary
- The technology may be changing
- The environment could be changing
- A critical part of the project may involve the design of a human-computer interface

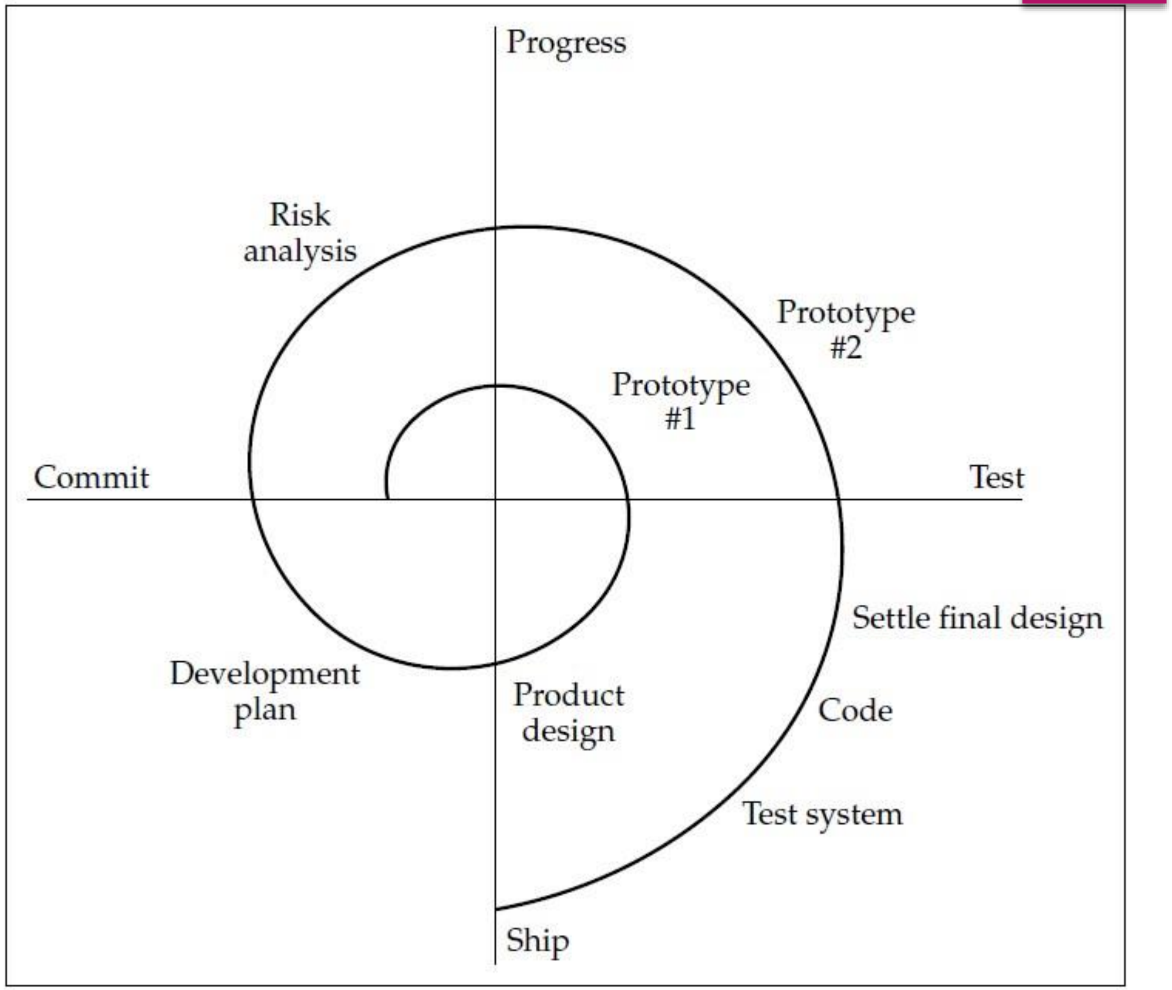


Figure 25.2: The spiral model

Organizational Issues

The Complacency Cycle and the Risk Thermostat

Interaction with Reliability

Solving the Wrong Problem

Incompetent and Inexperienced Security Managers

Moral Hazard

The Complacency Cycle and the Risk Thermostat

- Seat belts make drivers feel safer, so they drive faster in order to bring their perceived risk back up to its previous level.

Interaction with Reliability

- A high false alarm rate for many of the protection mechanisms at once, tempts staff: when they see that errors aren’t spotted they conclude that theft won’t be either

- Investment in software quality will reduce the incidence of computer security problems, regardless of whether security was a target of the quality program or not

Solving the Wrong Problem

- It’s not easy to sell a typical company’s board of directors on the need for proper defenses against insider attack, as this impugns the integrity and reliability of the staff who report to them.

- I would be cautious about this strategy because protection mechanisms without clear justifications are likely to be eroded under operational pressure — especially if they are seen as bureaucratic impositions.

Moral Hazard

- A company can leave itself open to staff who defraud it knowing that a prosecution would be too embarrassing.

- Another common incentive failure occurs when one part of an organization takes the credit for the profit generated by some activity, while another part picks up the bills when things go wrong.

Incompetent and Inexperienced Security Managers

- If you want to get to be the CEO you’ll have to spend maybe 20 or 30 years in the company without offending too many people.

- It’s hardly surprising that the average tenure of computer security managers at U.S. government agencies is only seven months

Managing Requirements Evolution

Bug Fixing

Control Tuning and Corporate Governance

Evolving Environments and the Tragedy of the Commons

Organizational Change

Bug Fixes

01

First, you need to be sure that you learn of vulnerabilities as soon as you can

02

Second, you need to be able to respond appropriately.

03

Third, you need to be able to distribute the patch to your customers rapidly. So it needs to be planned in advance.

Control Tuning and Corporate Governance

- It’s also a good idea to have good channels of communication to your internal audit department. But it’s not a good idea to rely on them completely for feedback. Usually the people who know most about how to break the system are the ordinary staff who actually use it. Ask them.

Evolving Environments and the Tragedy of the Commons

- Even very basic mechanisms such as authentication protocols had to be redesigned once they started to be used by systems where the main threat was internal rather than external.

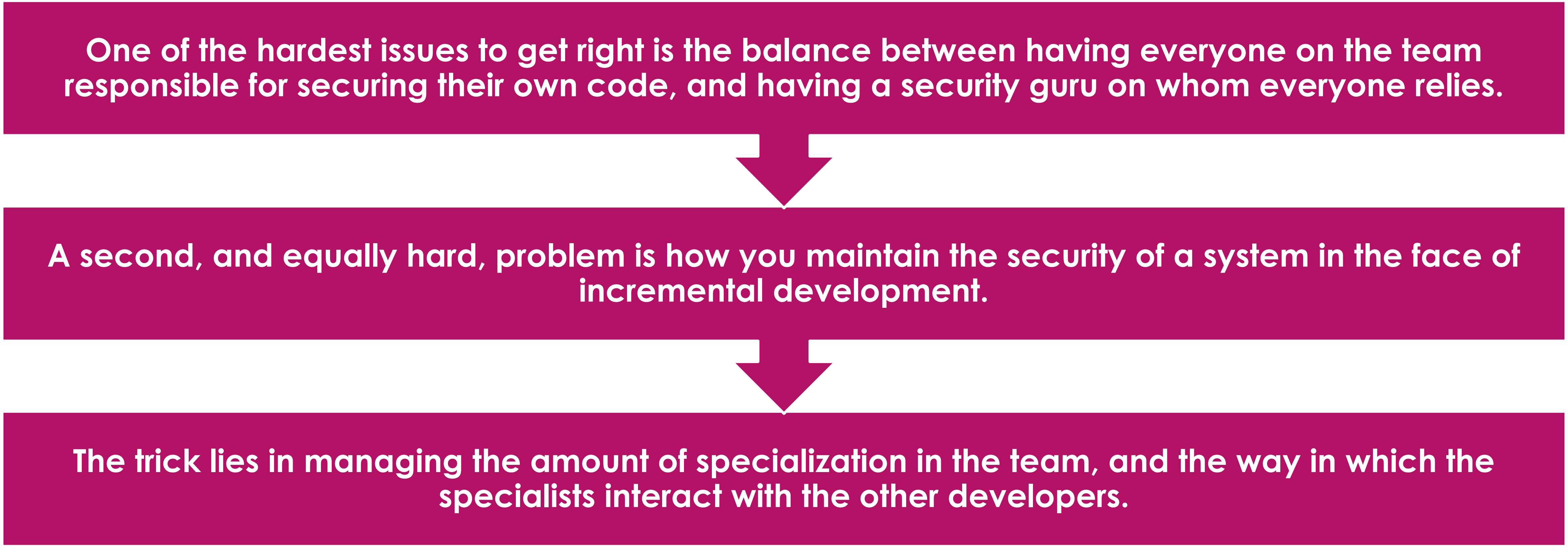
Organizational Change

- Organizational issues are not just a contributory factor in security failure, as with the loss of organizational memory and the lack of community mechanisms for monitoring changing threat environments. They can often be a primary cause

Back to Risk Management

- How much to spend on protection against what.
- *Annual loss expectancy* (ALE)
- Insurance as a solution for large but unlikely risks

Managing the Team



One of the hardest issues to get right is the balance between having everyone on the team responsible for securing their own code, and having a security guru on whom everyone relies.

A second, and equally hard, problem is how you maintain the security of a system in the face of incremental development.

The trick lies in managing the amount of specialization in the team, and the way in which the specialists interact with the other developers.

A Tale of Three Supermarkets

- **Objective:** Lowering the costs of the salaries of the checkout and security staff, and the stock shrinkage due to theft.
- **Solutions:**
  - RFID
  - Persecution
  - Self-service scanning
- **Moral of the story:** sometimes less is more

A Tale of Three Supermarkets

	Solution	What’s the gain?	Problems
South African supermarket	RFID	• Cut staff numbers • Made theft harder	• Large and ugly special trolley • RF tags costs • RF tags are hard to read reliably
European supermarket	Persecution	• Cut down in shoplifting	• Diverting effort from marketing lead to stock price slide
Waitrose supermarket	Self-service scanning	• Lets you exclude known shoplifters • Helps market the store card • Trusting removes motive for cheating	

SECURITY is an organizational PROCESS not a destination

Thank you for listening