"Hopefully you'll be able to catch up"

1 Intro

Software eng security can theoreticly be achieved by following the pillars:

- risk mgnt
- touchpoints
- knowledge

1.1 Touchpoints

There are 7 main touchpoints that follow the software creation:

- Code review
- Arch risk analysis
- Pentesting
- Risk-based sec testing
- abuse (misuse)
- Security requirements
- Security operations

SDL (sec dev lifecycle) has the following steps:

- Training
  You need to keep updated with all the news because every 4 years most of the information is obsolete.
  - Core Security Training Security knowledge is lacking in general
    Historically not taught in universities
    Barely taught in universities now
    The attackers are getting smarter every day, security is a moving target
    Annual training is necessary
    Need to cover all the topics in the SDL

- Requirements (organisation requirements)
  - Establish Security Requirements Assign a security champion.
    Assign a privacy advisor (external to team).
    Assign a privacy lead (internal to team).

- Create quality Gates/Bugs bars Define and document a bug bar for sec and privacy.
  Classification of what are moderate, important , or critical sec and privacy bug types.
  User to set priority for fixing and to determine if the product can ship
  Ensure that bug reporting tools can track security and privacy issues and that a database can be queried dynamically for all security bugs at any time
- Security and privacy risk assessment
  Start a security plan. Identify timing and resources for SDL steps, such as:
  * Team training
  * Threat modeling
  * Security push
  * Final security review

  Security Risk Assessment:
  * Identify specific functional areas that need special review

  Privacy Risk Assessment:
  * Stores personally identifiable information (PII) on the user's computer or transfers it from the user's computer (P1)
  * Provides an experience that targets children or is attractive to children (P1)
  * Continuously monitors the user (P1)
  * Installs new software or changes file type associations, home page, or search page (P1)
  * Transfers anonymous data (P2)
  * None of the above (P3)

- Design
  This step works as a cycle:
  - Design Requirements
  - Threat modeling
  - Attack surface Analysis/reduction

1.1.1 Design Requirements

Design Principles

- Least privilege
- Compartmentalization
- Validate/Sanitize external input to the system
- Log/audit system and data access
- Reuse sec components and libs
- secure the weakest link

Specifications

- Secure architecture
- Identification of sec critical components
- Secure functional requirements
- Security failures

Attack surface Analysis/reduction It is impossible to stop all the attacks since depending on the time and money invested anything is possible. The idea is to reduce the attackers surface.
This surface has 3 dimensions:

- target / enablers
- channels and protocols
- access rights

One of the tools used to deal with this is ASA(attack surf analyzer)

2 Security Usability

2.1 Why security fails ?

- User doesn't consider security as a main task
- The background of users
- Bad knowledge of the system by the users and therefore don't associate the risks.(unique password, and anything lowering the sec layer)
- Professionals can also be blamed if the design of the system doesn't allow users to easily implement the secure requirements.

2.2 Importance

You must be really aware of the weakest link of your systems, usually the humans are the weakest link, because they are potential victims of phishing, ...
The design must be easy but secure.

2.3 Guidelines

The guidelines for best usability are the following ones:

- easy to learn (easy use every time the users has to interact, if too hard users won't comeback.)
- efficiency to use
- easy to remember
- less error prone (able to adapt if users do stuff unexpected)
- likeable

2.4 Security Usability

Usability qualities(usual solution are passwords, that is why there is so much emphasis on this subject) + security = happy people 3 papers to read.

3 Passwords

Can people remember 56 bit passwords ? (12 English letters)

3.1 How to store data in human brain ?

We can see our brain as an hard drive, the difference is that we forget things after a long period of time if we don't recall it regularly.
According to famous cryptographers, humans aren't build to remember proper keys.

3.2 So how to remember passwords

We have to go through spaced repetition:
Paste it many times in your brain and then enter a period of copy/paste period.
One technique used is adding a verification number that would be delayed every time the user would fail the password. There is an interesting paper to read to train the user's memory for their master password (for a password manager)