Closing workshop

Jim Manico and Johan Peeters

@SecAppDev

https://groups.google.com/group/secappdevorg
Overview

• New things learned
• Things to avoid
• Puzzles
• Monday
New things learned

Single most important new thing learned
  Reflection (3’)
  Max 7 words

Understand items on the list
  Clarification
  Where was this discussed?
  Why is this important?
RC4 has security problems too. Complexity is the enemy of sec. Always foresee algorithm, agility in your code.

Companies deal with security like pollution.

David vs. Goliath.

Not only what, but also how security depends on the weakest link.

Pick your battles, go step by step.

Safe password manage is hard.

Be paranoid while coding.

GCM mode is hard to implement correctly.
Things to avoid

Single most instructive mistake
  Reflection (3’)
  Max 7 words

Understand items on the list
  Clarification
  Why is this important?
Things to avoid

- Implementing solutions without explicit threat model
- Working alone
- Avoid assuming your passwords will not be exposed
- Forgetting the end user might be the weakest link
- Crypto complacency
- Leaving unencrypted data on a mobile device
- Forgetting the social part
- Giving unanalyzed code review reports to developers
- Avoid forgetting the master password to your password vault
- Avoid making it too complex
- Input sanitization with a character blacklist
- Build your own security protocol
Puzzles (15’)

• The intuitive thing should be the secure thing
• Secure framework defaults for developers
• How to securely store passwords
• **What is the incentive to write secure code**
• Desire to learn more about threat modeling
• Taking the threat to the economics
• Money/Time/Quality Tradeoff
• How to get developers to use crypto correctly
• What are the architectural level principles to build secure systems
• What are the good libraries I should be using for security?
• What are good functionalities that should use?
• Secure Frameworks needed
On Monday, I will...

Groups of 4
  present candidates (5’)
  vote
  prepare pitch (5’)
Present an action for Monday (30”)
  ask for clarification (5’)
Discuss
Thank you

@SecAppDev
http://secappdev.org
https://groups.google.com/group/secappdevorg