Implementing Cryptography: Good Theory vs. Bad Practice

Viet Pham
Information Security Group, Department of Mathematics
Royal Holloway, University of London

Outline

- News report
- What is cryptography?
- Why is it ever implemented?
- Why are there problems?
- Where do they affect in the systems?
- What could possibly happen?
- What to do and not to do?

News report

- Padding oracle attack on ASP.NET

threatpost
The Kaspersky Lab Security News Service

Wednesday, March 7th, 2012

Google™ Custom Sear Search

Newsletter Sign-up

Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government | Hacks | Malware
Microsoft | Mobile Security | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security

Home › Cryptography ›

September 13, 2010, 7:58AM

'Padding Oracle' Crypto Attack Affects Millions of ASP.NET Apps

by Dennis Fisher
Follow @DennisF

Share Like 159 +1 0

38 Comments

A pair of security researchers have implemented an attack that exploits the way that ASP.NET Web applications handle encrypted session cookies, a weakness that could enable an attacker to hijack users' online banking sessions and cause other severe problems in vulnerable applications. Experts say that the bug, which will be discussed in detail at the Ekoparty conference in Argentina this week, affects millions of Web applications.

Today's Most Popular

- Indictments Reveal Anonymous's Mix Of Greed, Ideology
- An End to Offensive Security Research? Unlikely
- Report: FEDS Arrest Top LulzSec Members
- Attackers Target CVE-2012-0754 Adobe Flash Bug
- US Judge Postpones Death Sentence For Ghost Click Machines

News report

- Bytes recovery attack (chopchop) on WEP and then on WPA TKIP

HOME › NEWS › SECURITY

New attack cracks WPA Wi-Fi encryption in just a minute

By Jose Vilches
August 27, 2009, 1:09 PM EST

9 Like 6 +1 0 Tweet 3

Encryption systems used by wireless routers have had a long history of security problems. The Wired Equivalent Privacy (WEP) system was cracked and rendered effectively pointless within a few years of its introduction in 1997. Now, it looks like its WPA successor may soon suffer the same fate, with a pair of Japanese researchers developing a way to break it in just one minute.

Wi Fi™ The Standard for Wireless Fidelity.

The attack builds on the so-called "Becks-Tews method" unveiled last year by researchers Martin Beck and Erik Tews. However, that method worked on a smaller range of WPA devices and took between 12 and 15 minutes to carry out. Both attacks work on WPA systems that use the Temporal Key Integrity Protocol (TKIP) algorithm. They aren't key-recovery attacks -- but give hackers a way to read encrypted traffic sent between computers and certain types of routers that use the outdated encryption system.

The Wi-Fi Alliance has required since 2006 that Wi-Fi-certified products support WPA 2, a much more powerful encryption system that is not vulnerable to these attacks, but users have been slow to upgrade.

TechSpot on Follow

Most Popular

News report

- Padding oracle attacks on Datagram TLS (NDSS' 11):
  - Flaws in RFCs: Mac-then-pad-then-encrypt
  - Flaws in implementations: did not follow RFCs
- Attacks on GPG (2004):
  - Did not choose private key in the right way
  - Implementations reuse key
- Attacks on Kerberos v.4 (2004):
  - Encryption was not authenticated
- Attacks on bad random number generators, e.g., Netscape (1996)

News report

- Attacks on leap-of-faith authentication

- BIG question:
  - why are all these happening, and what are we going to do?

What is (modern?) cryptography?

- The practice and studies of an (expanding) set of mathematical techniques toward achieving certain security objectives, such as confidentiality, integrity, non-repudiation, etc.

What is (modern?) cryptography?

- The practice and studies of an (expanding) set of mathematical techniques toward achieving certain security objectives, such as confidentiality, integrity, non-repudiation, etc.
- What is so special about this definition?

What is (modern?) cryptography?

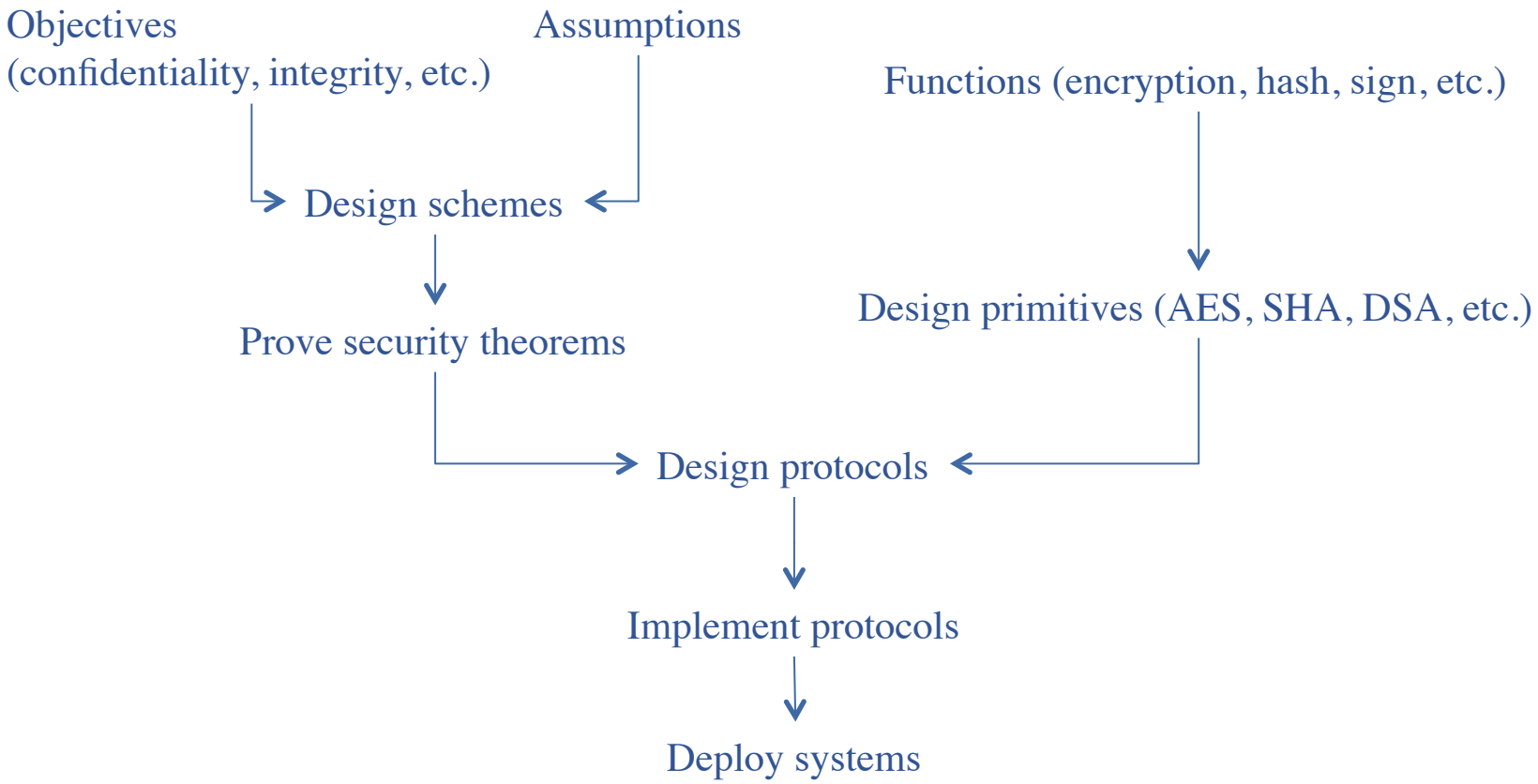
- The practice and studies of an (expanding) set of mathematical techniques toward achieving certain security objectives, such as confidentiality, integrity, non-repudiation, etc.
- What is so special about this definition?
  - Three important keywords: “mathematical”, “techniques”, and “toward”

Why is cryptography being extensively implemented?

- Mathematical: proven secure or mathematically reasoned to be secured
  - Provides security services that could otherwise be impossible without
  - A system is only secure until an attack is found

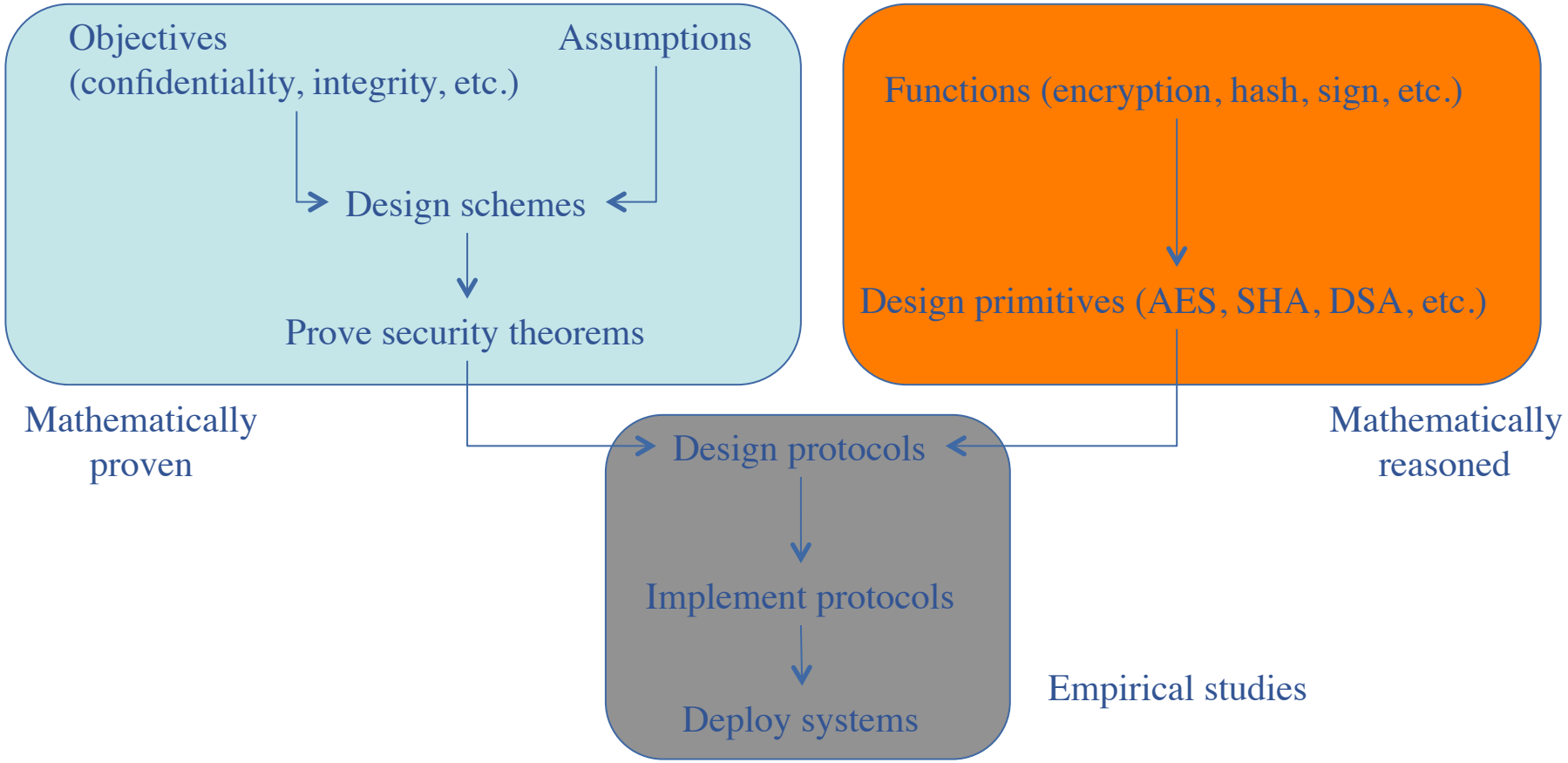
Why are there problems?

- Revisit how system is being created:



Why are there problems?

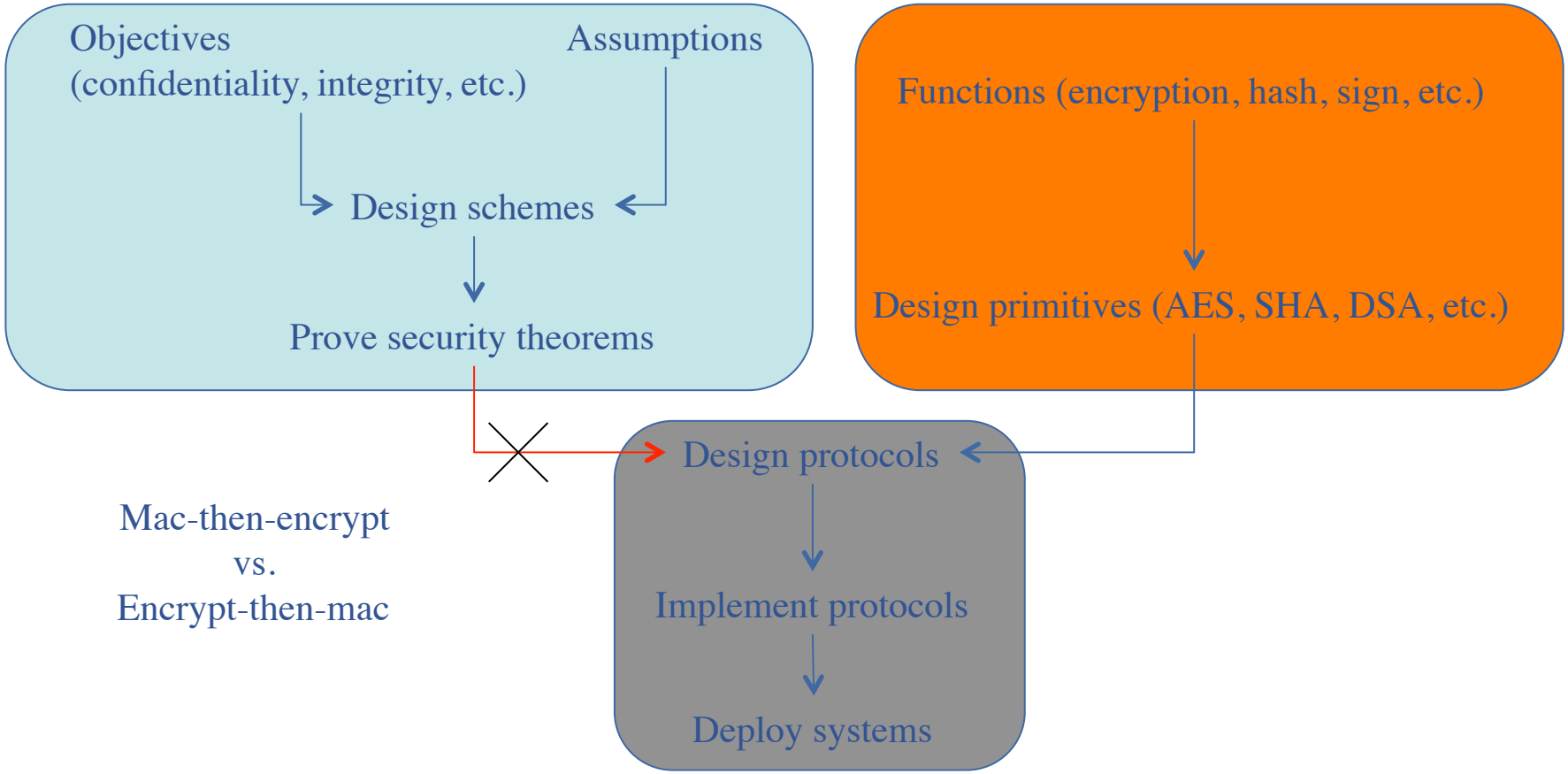
- Cryptography is about **techniques**, not readily useable systems



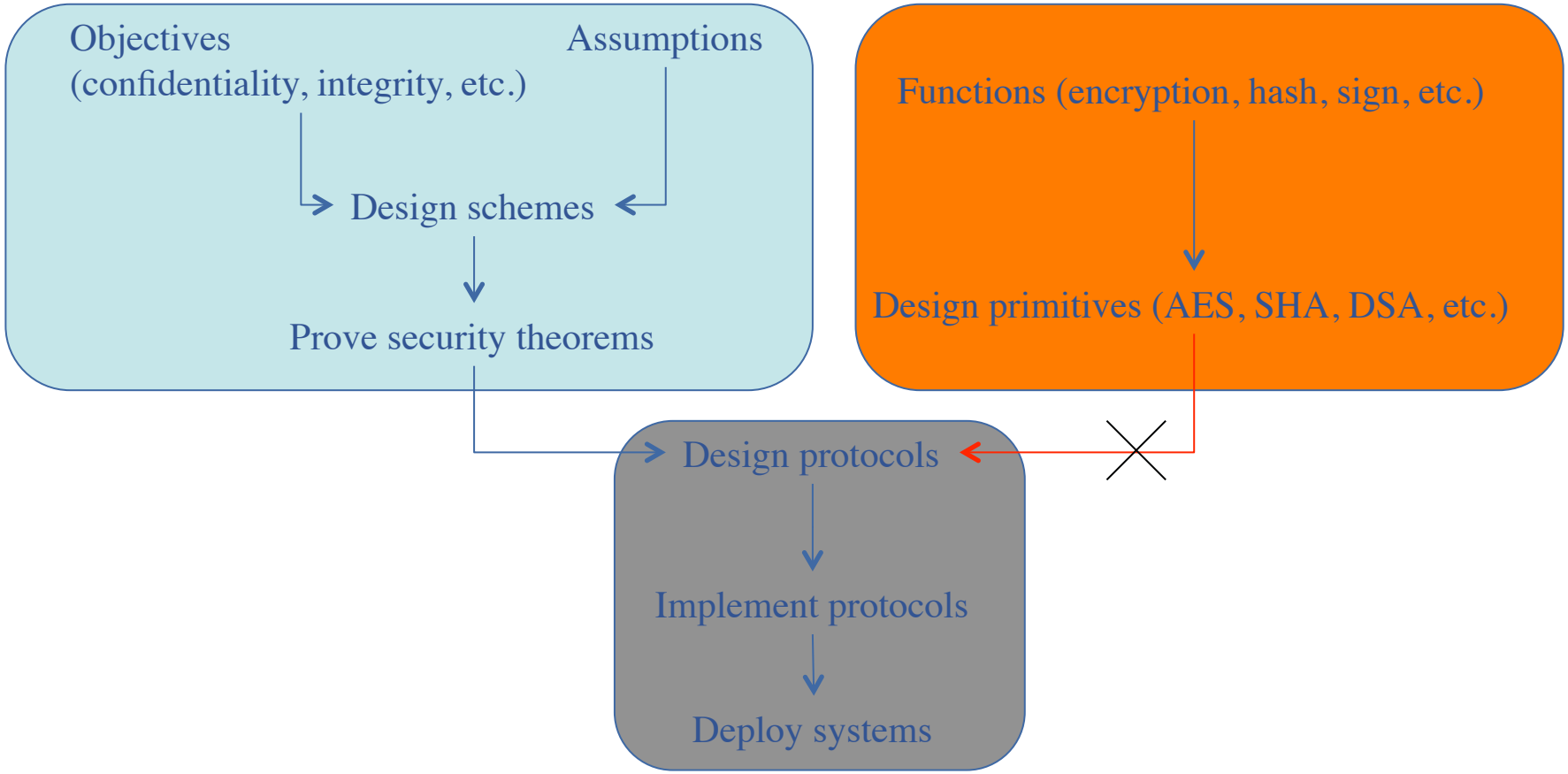
Why are there problems

- Cryptography implementers are often not cryptographers themselves
  - Overestimate the power of cryptography:
    - *"I don't see a reason to have a x of about the same size as the p. It should be sufficient to have one about the size of q or the later used k plus a large safety margin. Decryption will be much faster with such an x."* – comments in GPG source code
  - Lack of theoretical knowledge (e.g., cryptography, formal method) to verify the security of the implementations
  - Use of "look-like secure" components: Mac-then-encrypt, bad random generators, etc.
- Protocol specifications are sometimes too complicated

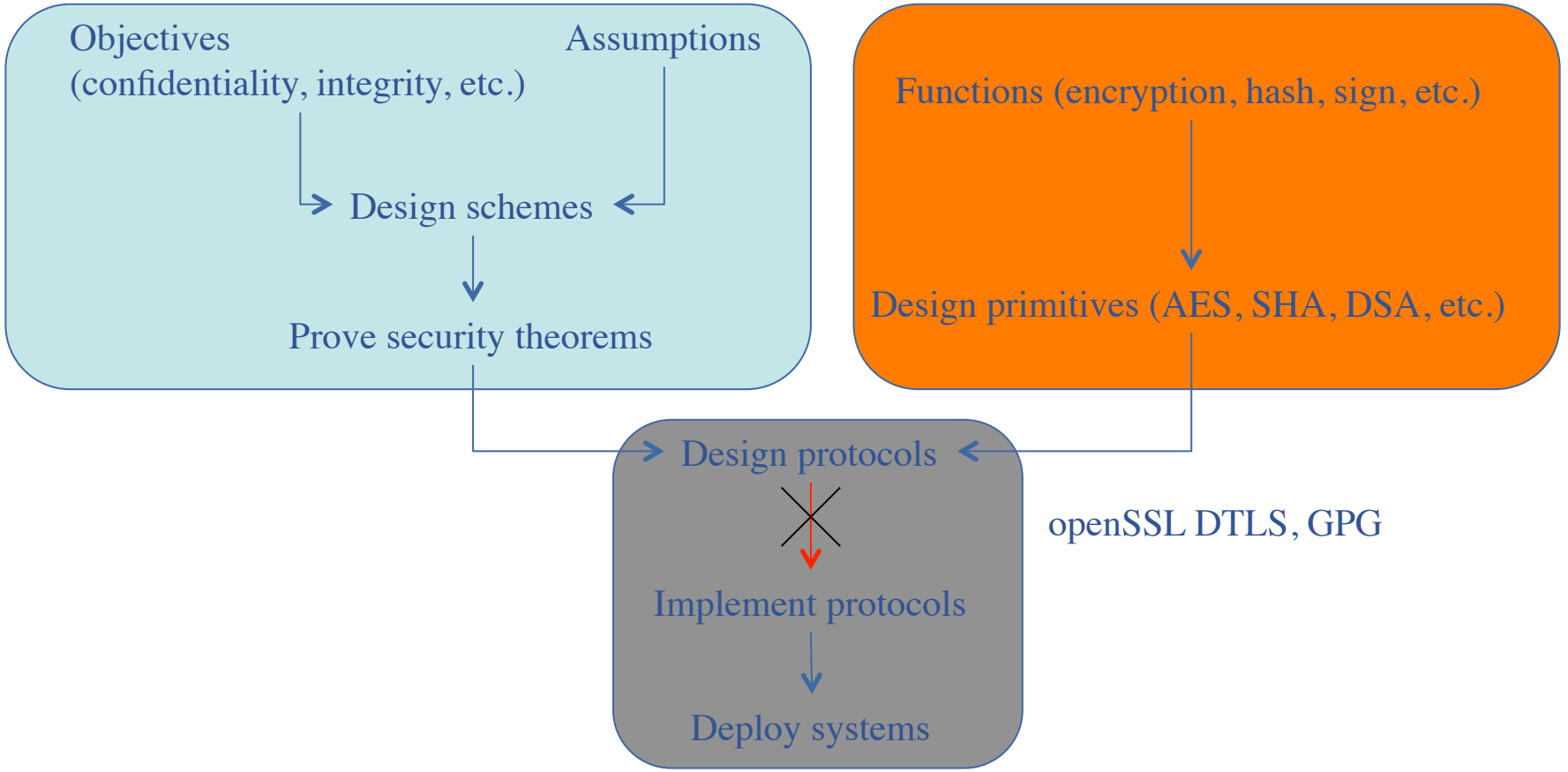
Where do problems happen?



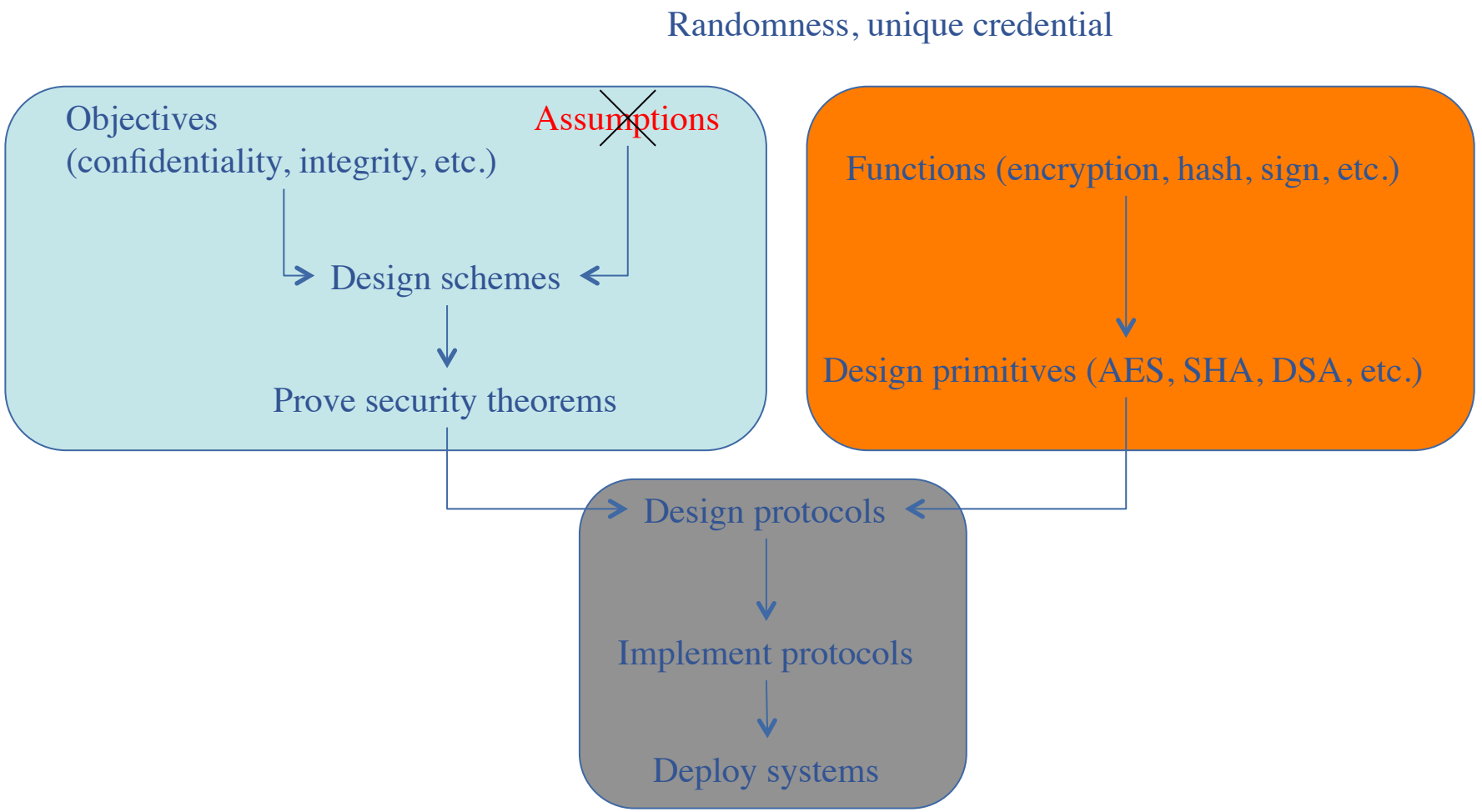
Where do problems happen?



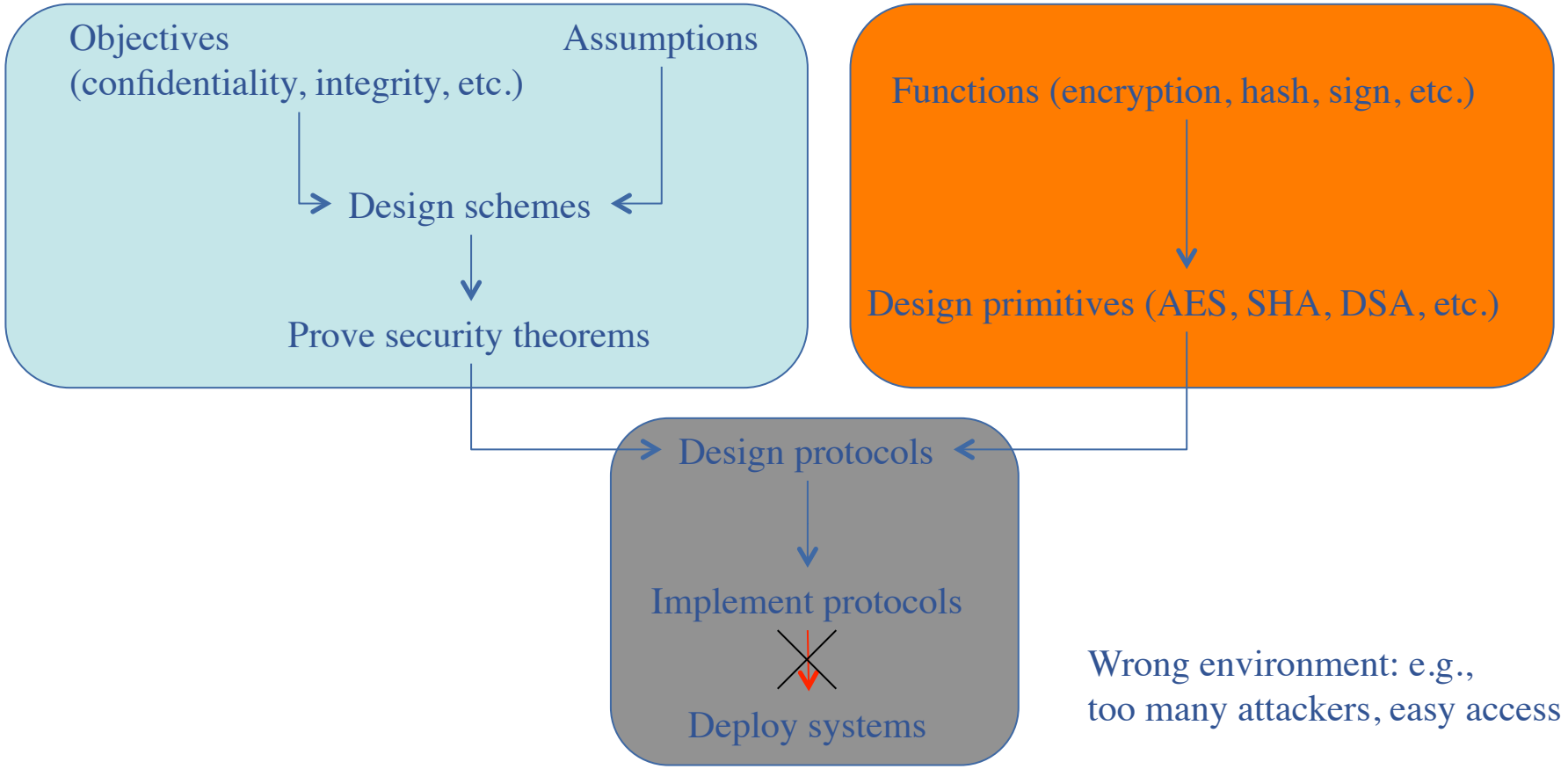
Where do problems happen?



Where do problems happen?



Where do problems happen?



Wrong environment: e.g.,
too many attackers, easy access

What could possibly happen?

- May bring negative effects if not implemented/deployed properly
- Crypto attacks might become serious:
  - Plaintext (full/partial) recovery
  - Key compromise
  - Phising
- Often platform independent

What should we do?

- Kerckhoffs's principle: do not design/implement your own cryptographic protocols in secret. Eventually they will be discovered.
- Design your own cryptosystem? Do not deploy it, instead, submit for peer review
- Use of approved cryptographic libraries, e.g., cryptlib, crypto++, openssl
- Implementing on your own? Pay attention strictly to all the details of the protocol specification and recommendations
- Deploying an implementation? Check the assumptions attached to the cryptographic and protocol designs

What should we do?

- What to do if even things like RFCs and IEEE are flawed?
  - Low risk, but high damage: risk x damage might still be considerable
  - No one man's job to prevent the problems
  - Last significant word: cryptography is about practice and studies of an (expanding) set of mathematical techniques toward achieving certain security objectives:
    - Multi-factor authentication
    - Multi-layer security
    - Backup
    - Incidence response plans
    - Business continuity plans
    - etc.