Mobile VoIP Steganography

From Framework to Implementation

Marcus Nutzinger Rainer Poisel Jürgen Wurzer

Institute of IT Security Research
St. Pölten University of Applied Sciences

DeepSec 2010
November 25^{th} 2010

Introduction

Us, Ourselves, and We

- Studied "Telecommunications and Media"
- Employed at the Institute for IT Security Research at St. Pölten University of Applied Sciences
  - Project StegIT-2
  - Digital Forensics

Introduction

Cryptology, Cryptography and Steganography

Cryptography

- Study and practice of hiding information
- Protection of secret data
- Data transfer obvious

Steganography

- Science of covert communication
- Conceals the existence of secret information

Cryptology

Science that incorporates both cryptography and cryptanalysis.

Introduction

Cryptology, Cryptography and Steganography

Cryptography

- Study and practice of hiding information
- Protection of secret data
- Data transfer obvious

Steganography

- Science of covert communication
- Conceals the existence of secret information

Cryptology

Science that incorporates both cryptography and cryptanalysis.

Introduction

Cryptology, Cryptography and Steganography

Cryptography

- Study and practice of hiding information
- Protection of secret data
- Data transfer obvious

Steganography

- Science of covert communication
- Conceals the existence of secret information

Cryptology

Science that incorporates both cryptography and cryptanalysis.

Introduction

Filtering of internet services and applications

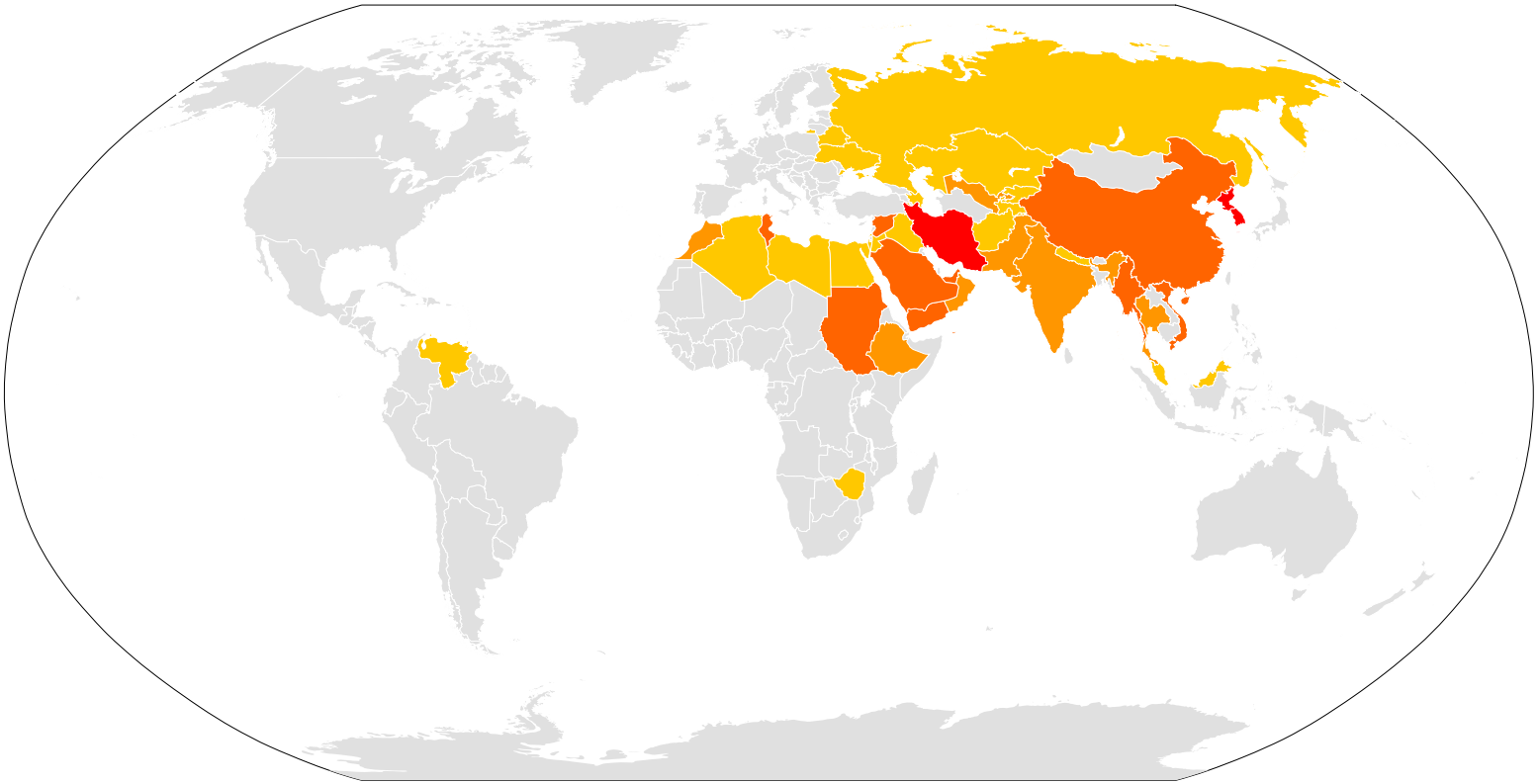

Figure: Worldmap of internet filtering (Source: OpenNet Initiative, 2010)

Introduction

Steganography in Brief

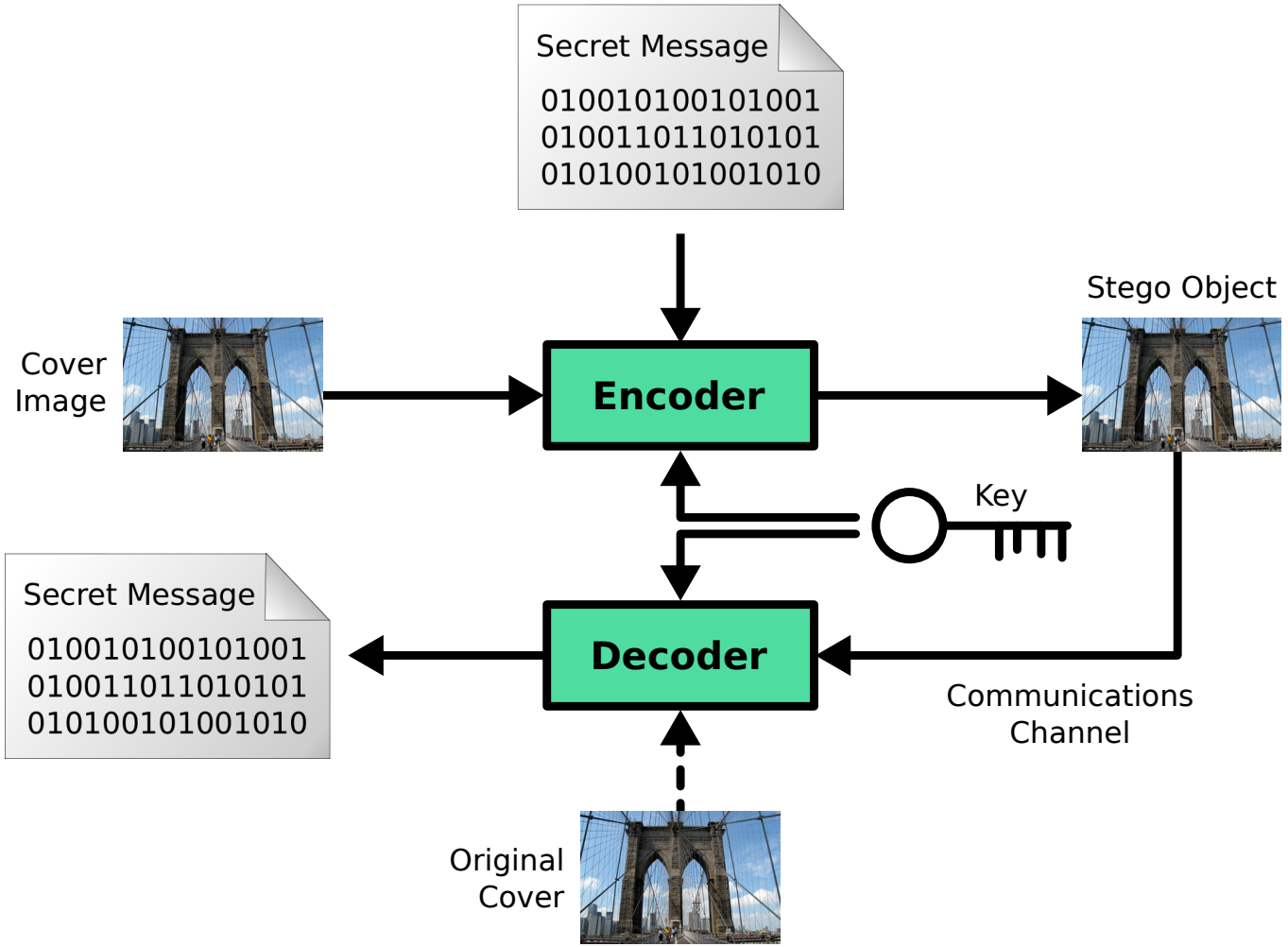

Figure: Generic procedure of steganography

Technical Details

Functional Overview – The Framework

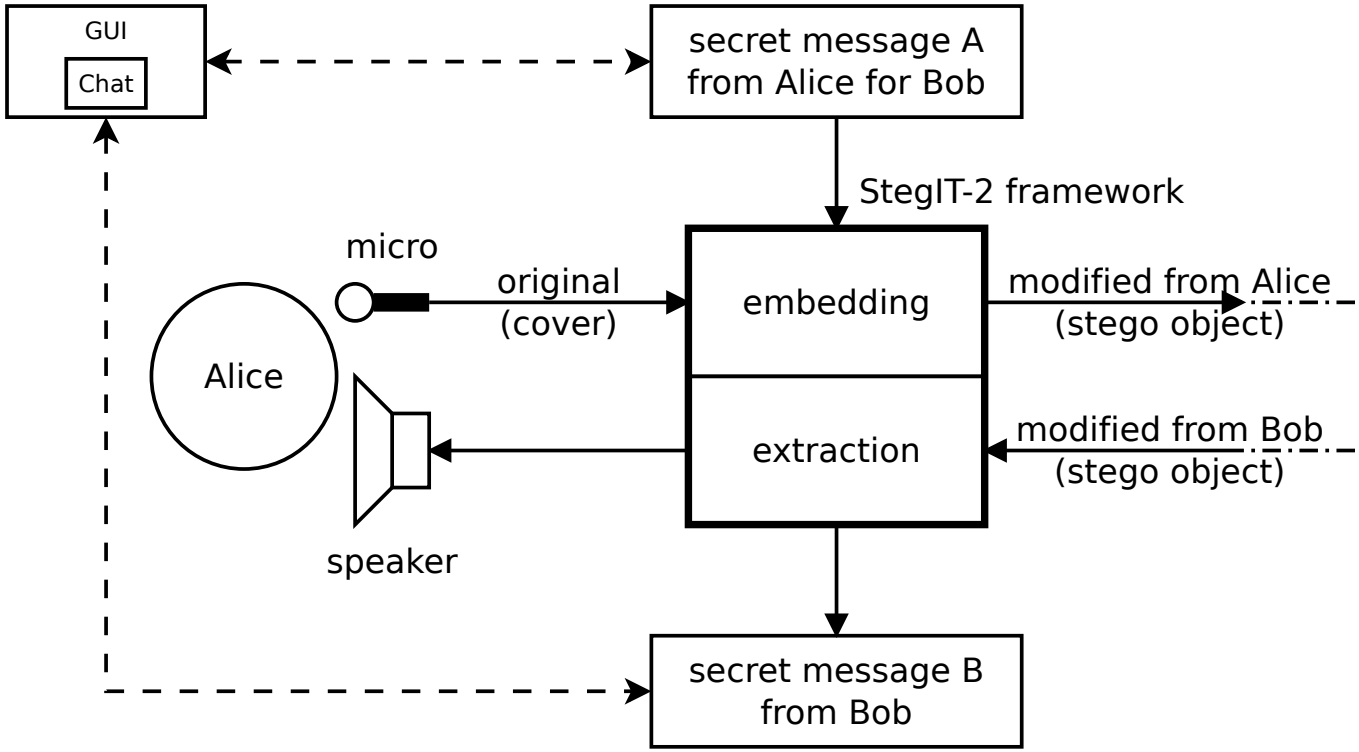

Figure: Principle of the StegIT-2 Framework

Technical Details

Functional Overview – VoIP

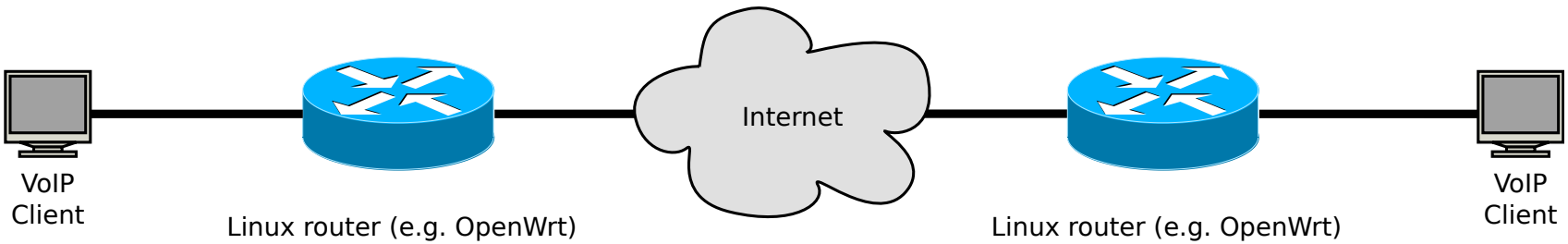

Figure: Using the framework for VoIP-Steganography

Technical Details

Functional Overview – VoIP

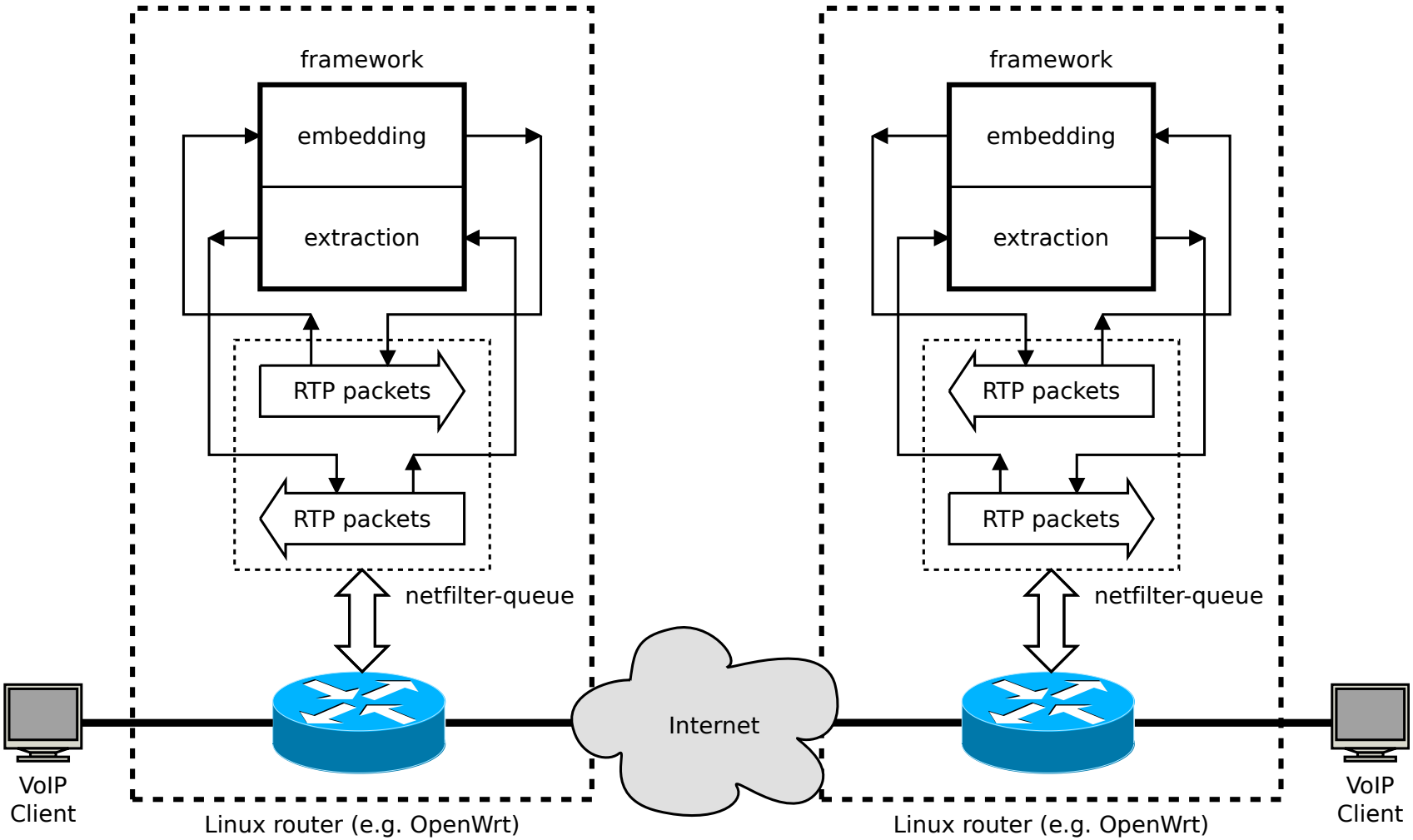

Figure: Using the framework for VoIP-Steganography

Technical Details

Functional Overview – GSM

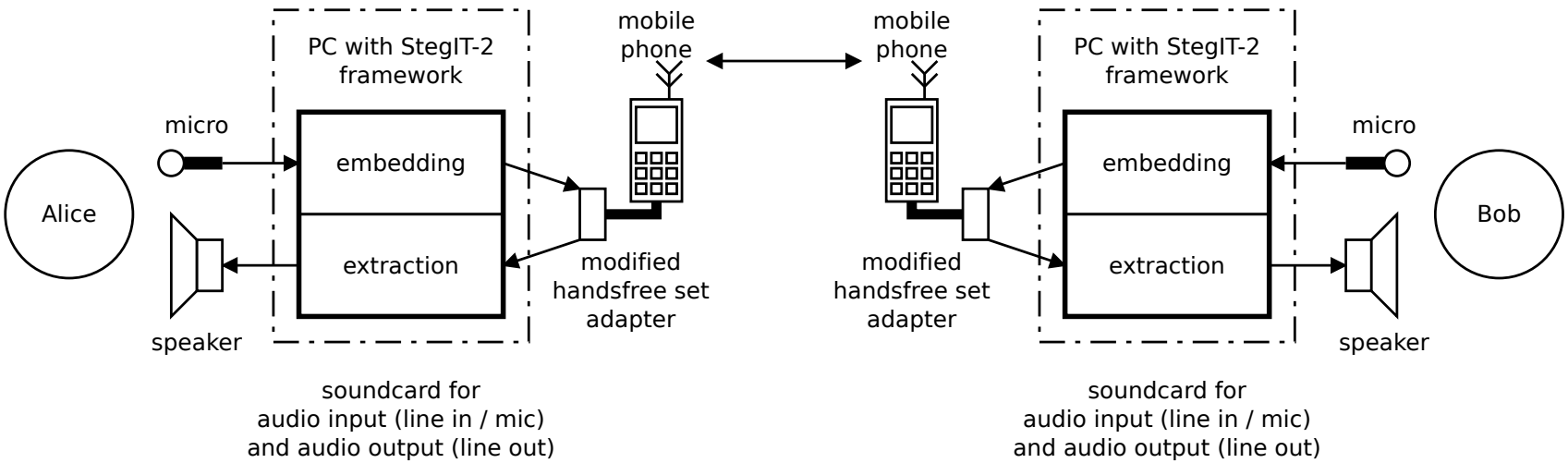

Figure: Using the framework for Steganography in GSM-calls

Technical Details

Outlining the Components

Components

- Protocol for data flow handling
- Integrity check of embedded data
- Segmentation of data for transmission
- Unification of secret data and cover medium
- Management of component instantiation
- Interfaces for third party software

Technical Details

Layered Approach

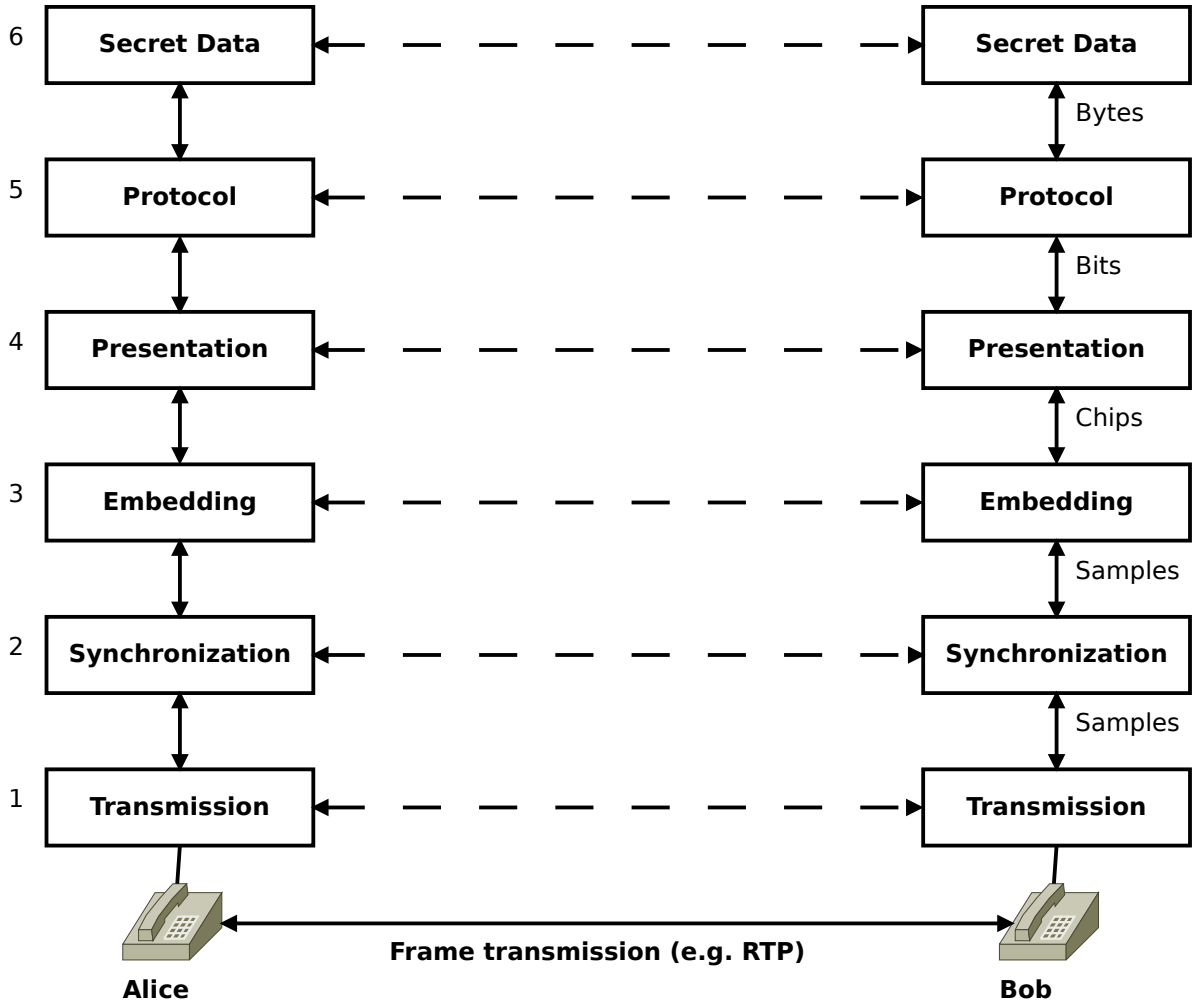

Figure: Steganographic data exchange as a layered model

Technical Details

Software-Architecture I

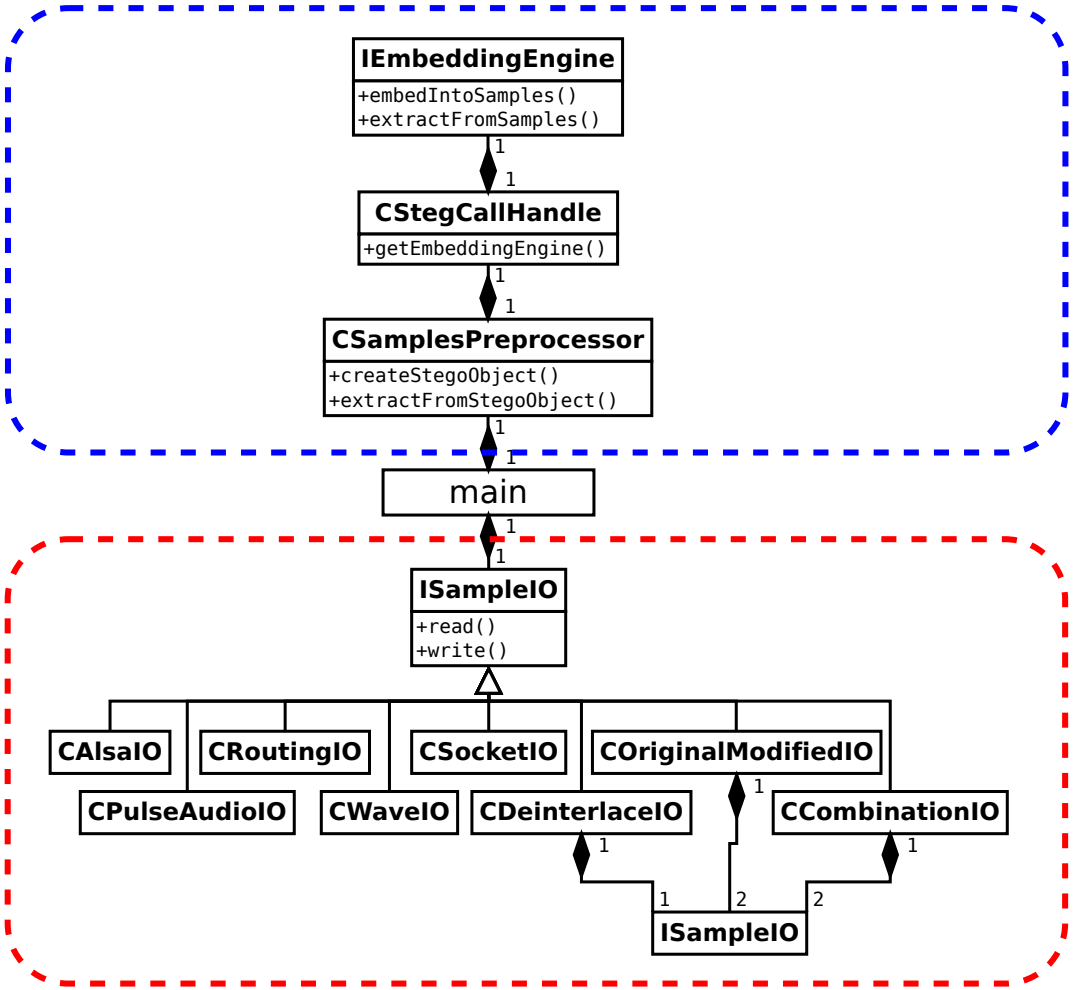

Figure: Architecture for IO-components

Technical Details

Software-Architecture II

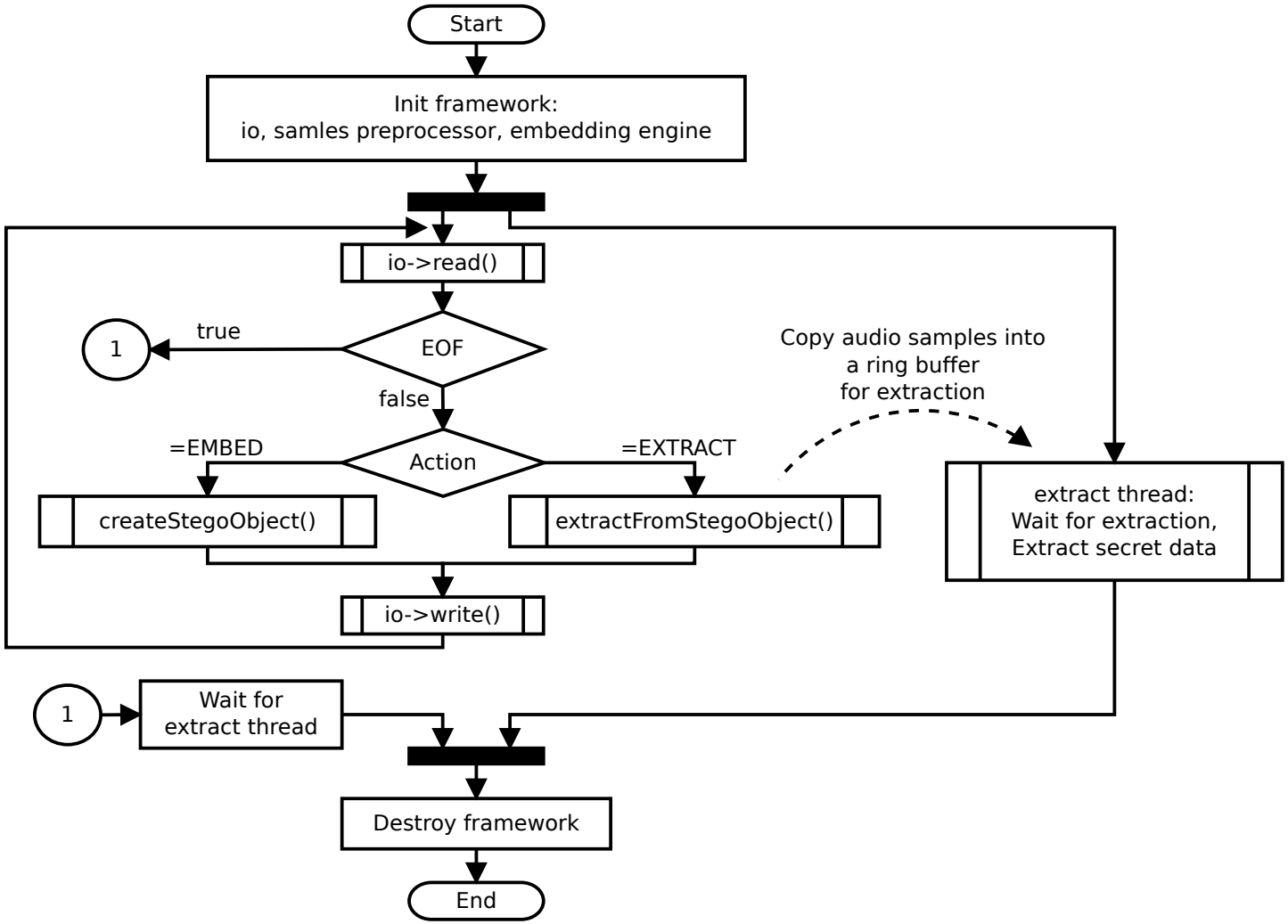

Figure: Flowchart of the main-routine

Technical Details

Software-Architecture III

Spatial Domain

- Digital representation
  - Codec-specific
  - e. g. LSB Hiding

Transform Domain

- Analogue representation
  - Echo Hiding
  - Spread Spectrum
  - Phase Coding

Technical Details

Software-Architecture III

Spatial Domain

- Digital representation
  - Codec-specific
  - e. g. LSB Hiding

Transform Domain

- Analogue representation
  - Echo Hiding
  - Spread Spectrum
  - Phase Coding

Technical Details

Software-Architecture III

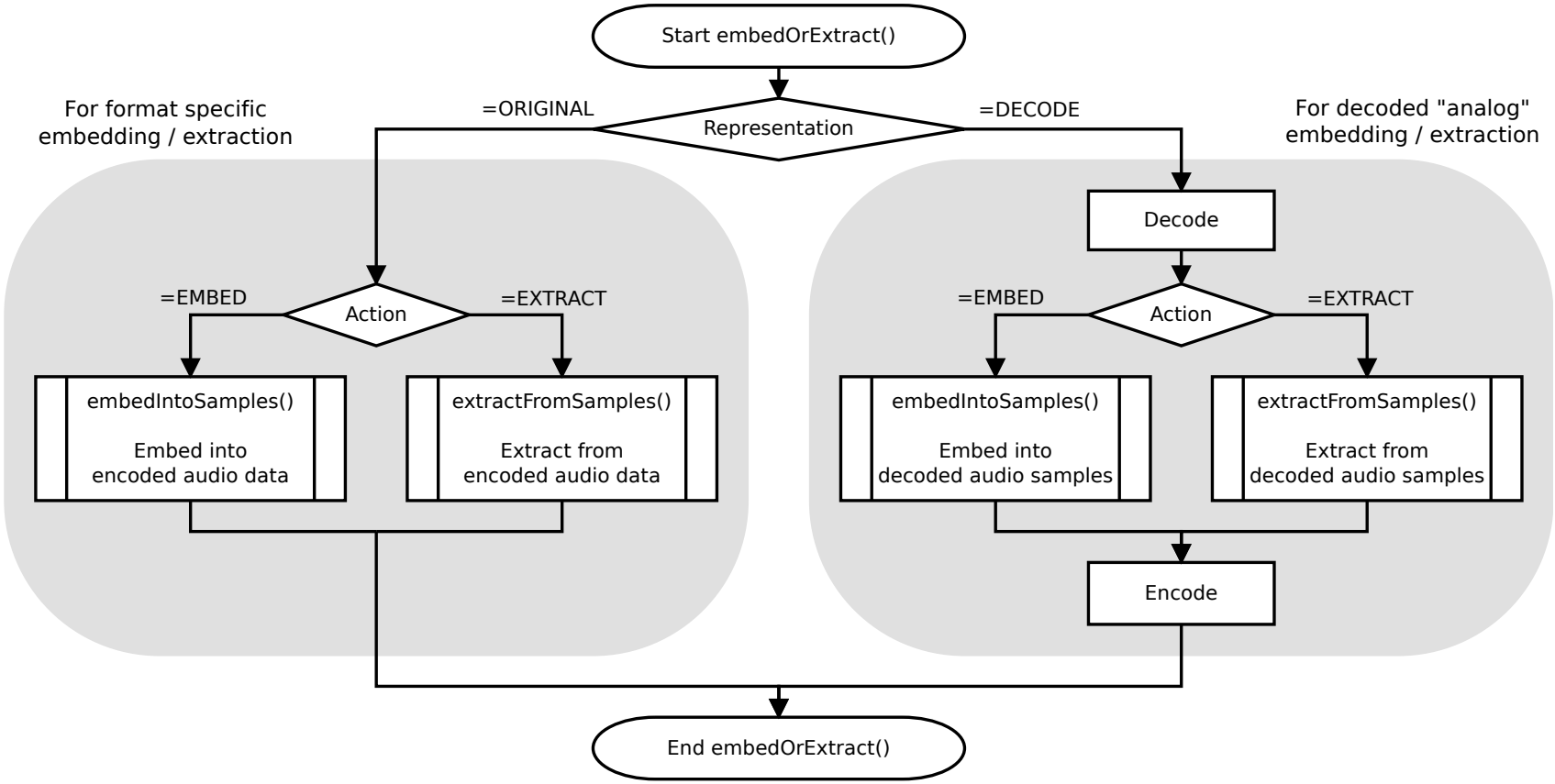

Figure: Different modes for Samples-Handling

Technical Details

Software-Architecture IV

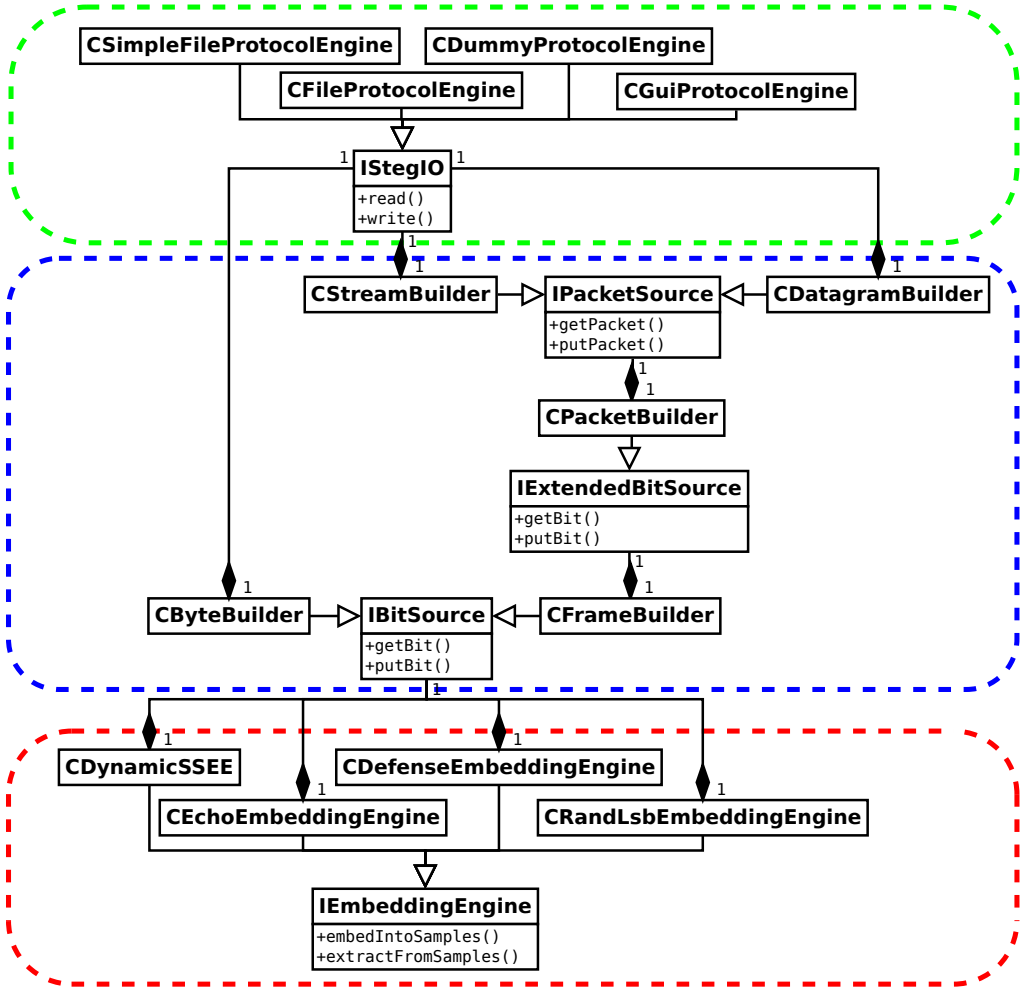

Figure: Architecture for embedding components

Technical Details

Platforms - Commodity Hardware

Mipsel

- Asus WL-500g Premium v1, based on Broadcom 4704
- (modified) OpenWrt SDK
- Port to other platforms:
  - Routing-Interface
  - Audio-Interface

OpenWrt SDK: Adaptions

- Support for NFQUEUE
- Additional packages added
- Customized firewall settings
- Customized start scripts

Technical Details

Platforms - Commodity Hardware

Mipsel

- Asus WL-500g Premium v1, based on Broadcom 4704
- (modified) OpenWrt SDK
- Port to other platforms:
  - Routing-Interface
  - Audio-Interface

OpenWrt SDK: Adaptions

- Support for NFQUEUE
- Additional packages added
- Customized firewall settings
- Customized start scripts

Technical Details

Platforms - Mobile- and Smartphones

Possibly usage on smartphones

- currently only Linux based phones considered
- e. g. Android powered smartphones
  - NDK allows for reuse of our C++ codebase

Scenarios

- VoIP
- Raw Voice-Data

Technical Details

Platforms - Mobile- and Smartphones

Possibly usage on smartphones

- currently only Linux based phones considered
- e. g. Android powered smartphones
  - NDK allows for reuse of our C++ codebase

Scenarios

- VoIP
- Raw Voice-Data

Defense

Analyzing robustness

Preventing steganography

- Project goal
- No steganalysis
- Different approaches
  - Noise
  - Jitter
  - Frequency shifting (semitone)
  - Signal cancelling

Demonstration

Setup

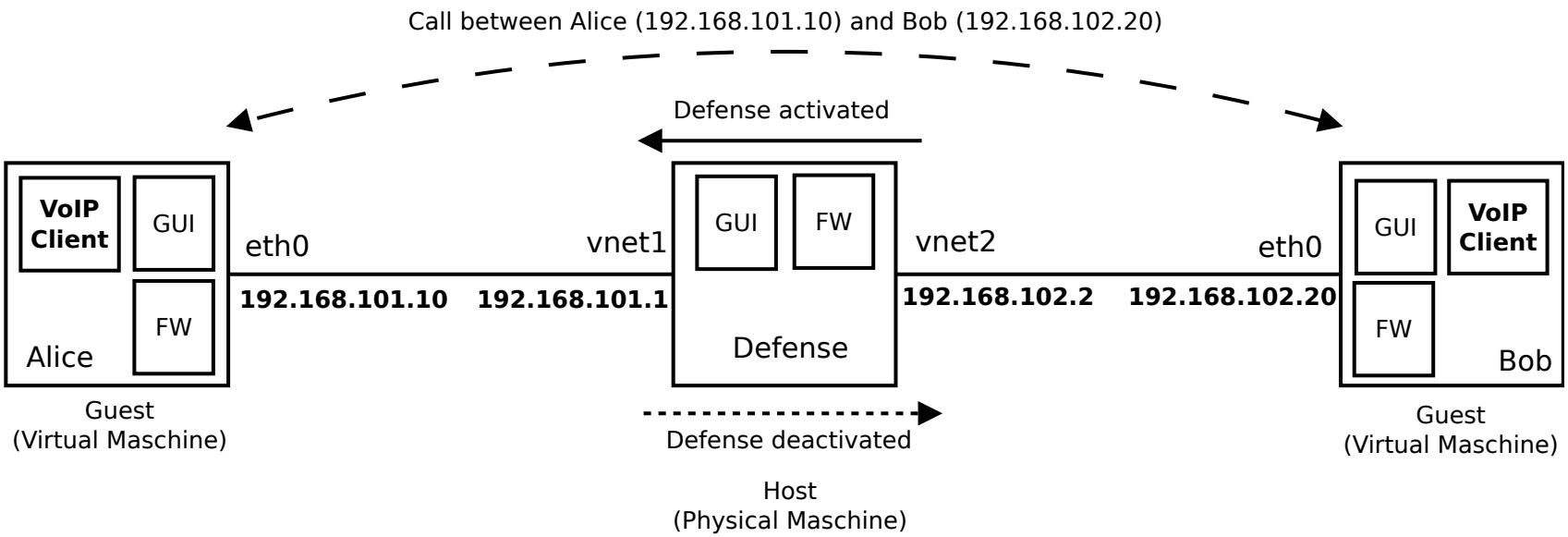

Figure: Architecture for embedding components

Outlook

Future scenarios

- Video streams as cover medium
- Windows-Port
- Better usability
- Improved data throughput
- Smaller, more powerful devices
- Use of steganographic loaders

Questions and Answers

Thank you for your attention!

Any questions?