Designing a terminal

Pavel Tuček

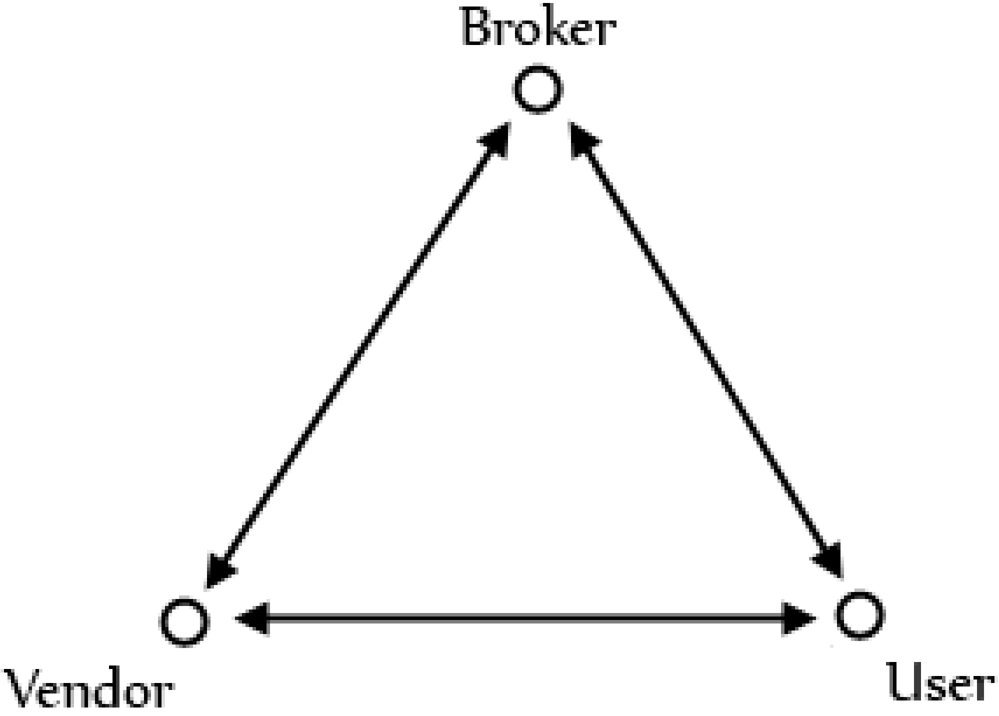
2010, FI MU

Introduction

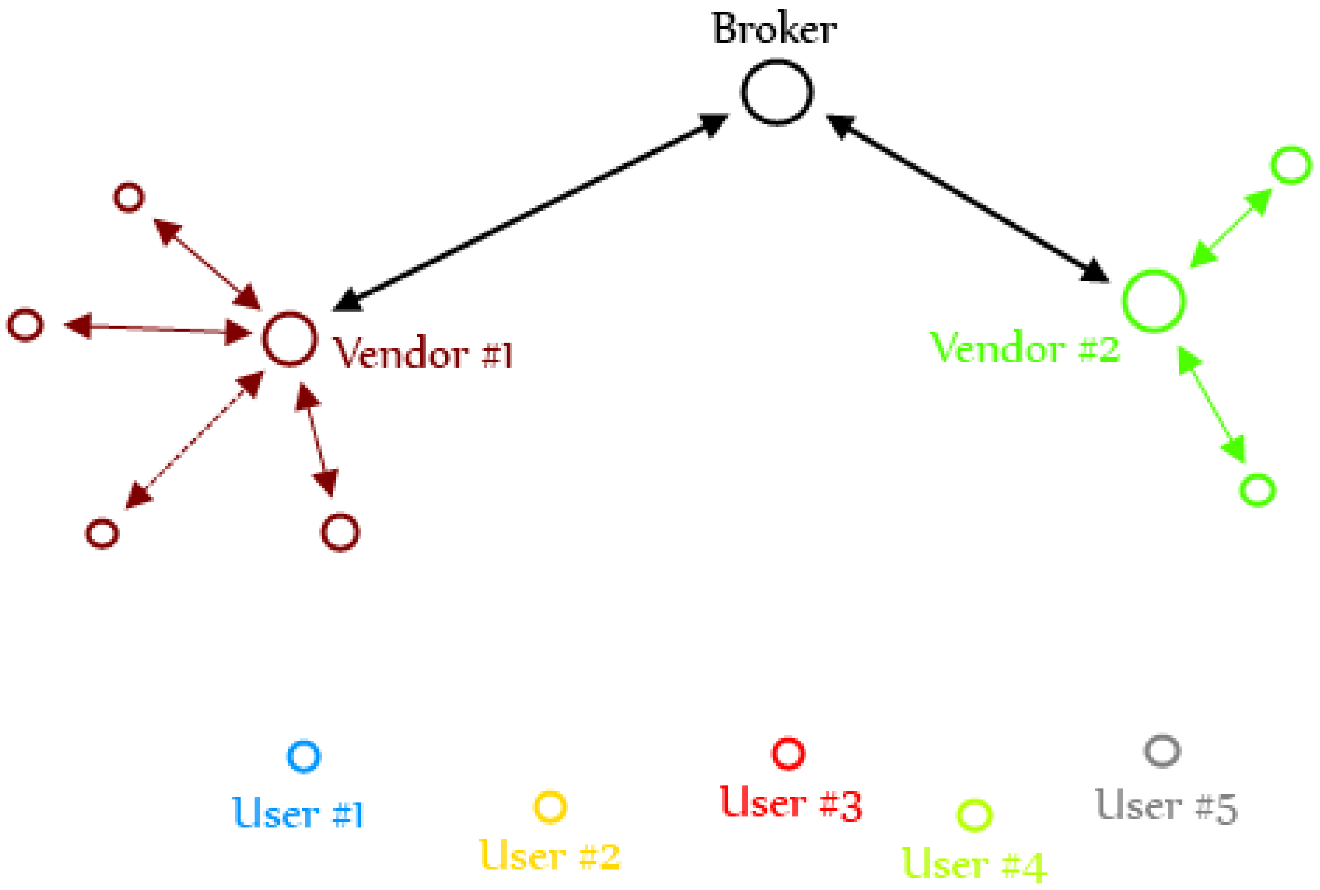
1. Micropayment scheme
2. Environment
3. Types of terminals
4. Other parts of system
5. Future work

Micropayment scheme

Main participants:



Environment for terminals



Types of terminals

Types of terminals should be as few as possible! But one type is not enough.

Let's split our micropayment scheme into two parts:

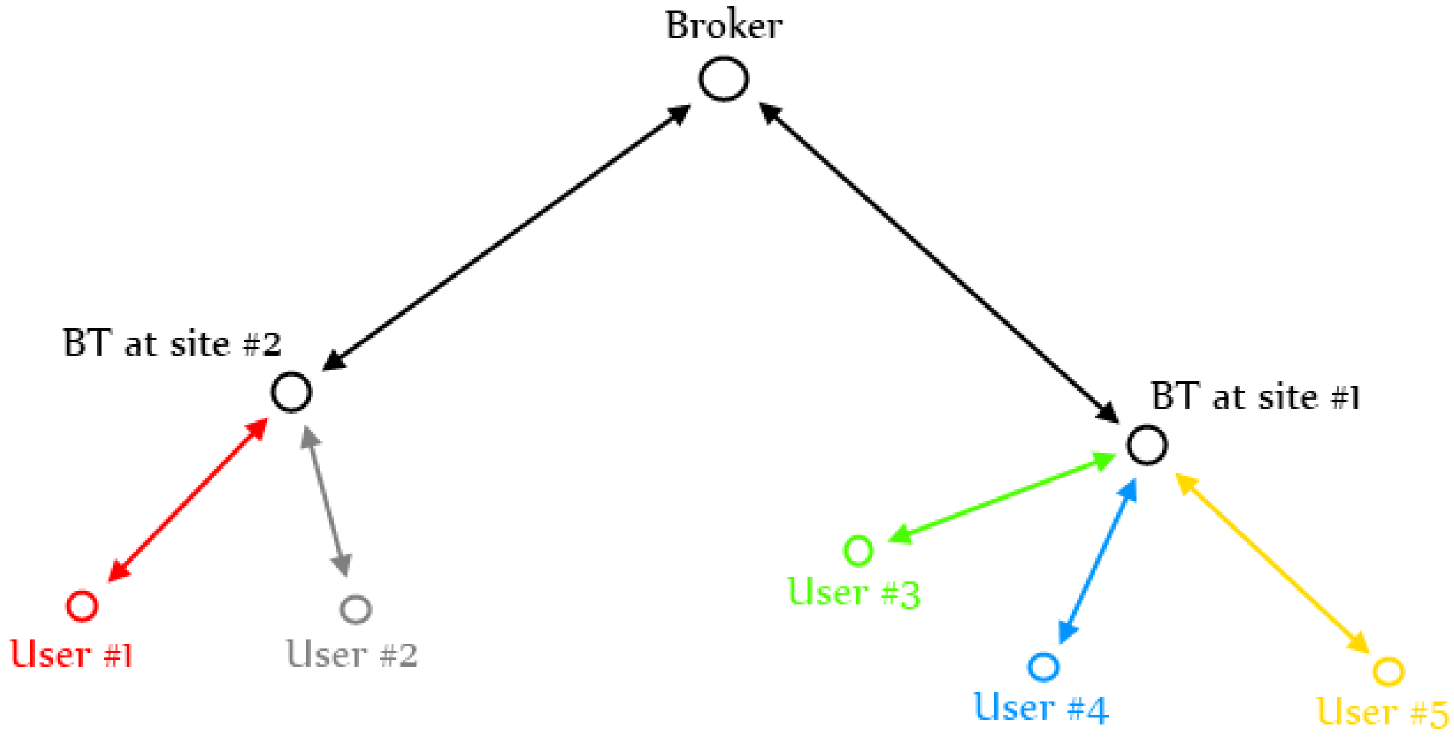
1. Broker's relationship to users.
2. Broker's relationship to vendors.

Motivation for this step is increasing trustworthiness of the whole system. In case there will be only one terminal, users might doubt whether their communication with broker wasn't monitored or even intercepted by the vendor.

Types of terminals

Terminal type #1 – Broker's terminal (BT)

BT is intended to be the center for customer care at the vendor's site, but managed by broker. This terminal must be online.



Types of terminals

Terminal type #1 – Broker's terminal (BT)

BT is intended to be the center for customer care at the vendor's site, but managed by broker. This terminal must be online.

Functions depending on the payment scheme:

- user registration with broker,
- user certificate revocation by user upon key compromise.

Other functions:

- money recharging,
- account management,
- creating transaction logs.

Types of terminals

Terminal type #2 – Vendor's terminal (VT)

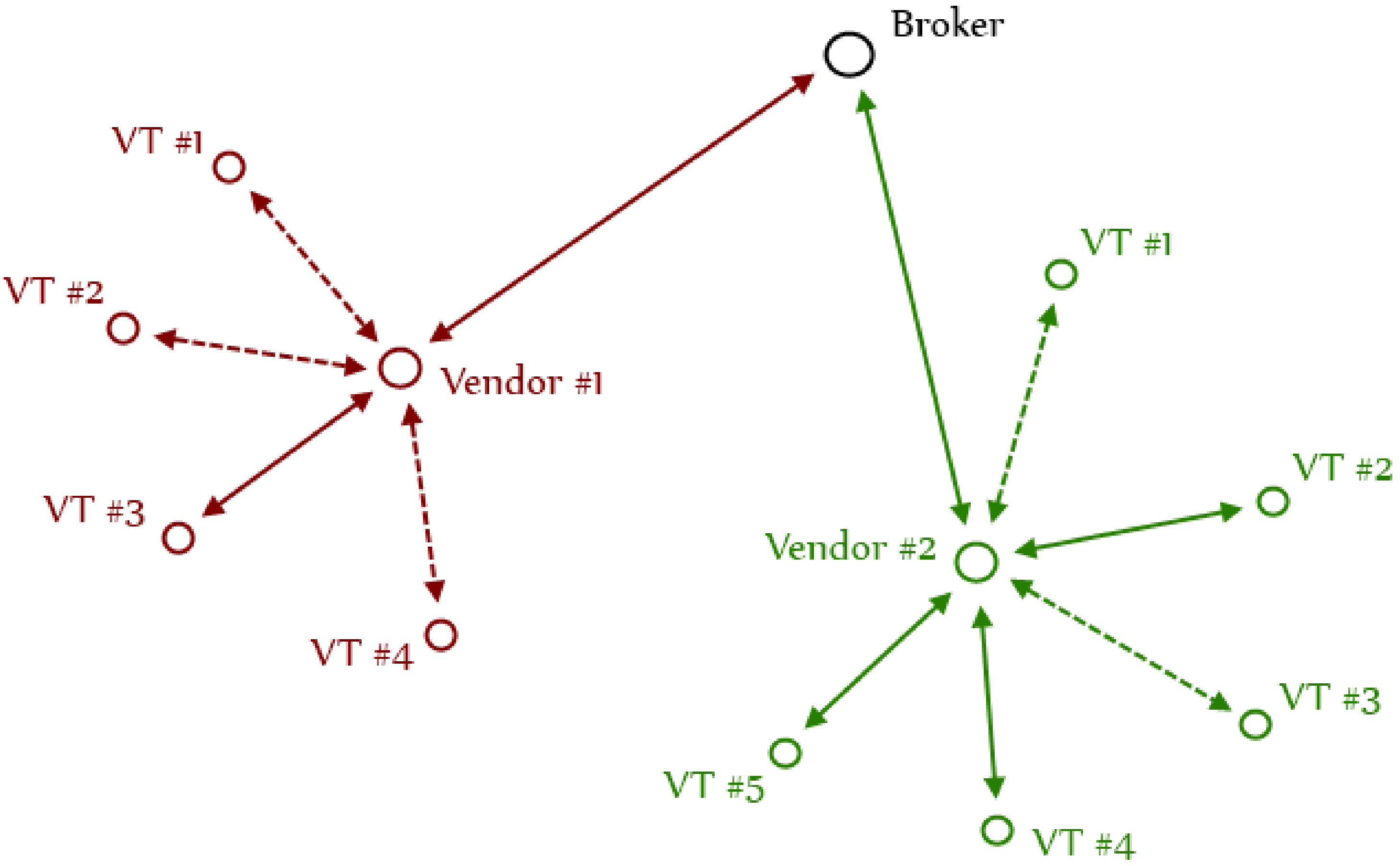
VT is intended to be connected to a device which needs to be served by it. That might be a printer, vending machines for hot and cold drinks, and snacks, etc. VT might be online or offline according to the vendor's infrastructure, but it will be definitely offline considering the broker's infrastructure.

Functions depending on the payment scheme:

- item purchase by user at vendor.

Types of terminals

Terminal type #2 – Vendor's terminal (VT)



Types of terminals

Terminal type #2 – Vendor's terminal (VT)

VT is intended to be connected to a device which needs to be served by it. That might be a printer, vending machines for hot and cold drinks, and snacks, etc. VT might be online or offline according to the vendor's infrastructure, but it will be definitely offline considering broker's infrastructure.

Other functions:

- picking coin per transaction,
- sending coins to vendor's management server (VMS),
- creating transaction logs, error logs,...
- sending data to VMS (transaction logs, errors,...).

Terminals’ specifications

Hardware requirements:

- card reader,
- display,
- input device (pin pad/keyboard/display),
- CPU,
- memory (RAM/ROM/flash),
- network component (industry standards[1]/Wi-Fi/BT/GSM/none),
- management connection (if talking about offline terminal: industry standards/USB/Wi-Fi/BT),
- smart card or TPM,
- connection to the served device.

[1] ANT, 6LoWPAN, DASH7, ONE-NET, ZigBee, MiWi, Wibree and others.

Terminals’ specifications

There are several candidates for the main CPU, but we can divide them into to groups.

The x86 compatible CPUs (Intel Atom, AMD Athlon Neo, VIA Nano)

ARM-based CPUs or more precisely SoCs (TI's OMAP 3 series and Freescale's i.MX51 based on the Cortex-A8 processor, or the Qualcomm Snapdragon and Marvell Armada 500/600 based on custom ARMv7 implementations)

The main difference is in design, while x86 compatible CPUs are CISC, the ARM-based CPUs are RISC. This implies different size of chip (number of transistors) and it’s different power consumption.

Terminals’ specifications

Cryptographic requirements:

- certificate store,
- random number generator,
- SHA-2 family hash function,
- RSA algorithm,
- AES encryption.

Other parts of system

Broker’s management server （BMS）

BMS will be the management center for taking care of users and vendors. Most likely it will be an information system or a server application.

Functions depending on the payment scheme:

- user certificate issuance by broker,
- vendor registration with broker,
- vendor certificate issuance by broker,
- user certificate revocation by broker,
- vendor certificate revocation by broker,
- vendor elimination from the system.

Other functions:

- send data to all VMSs （broker’s blacklist,....）
- create transaction logs.

Other parts of system

Vendor’s management server (VMS)

VMS is intended to be the main center for the customer care at the vendor’s place. One of its purposes is the management function for all VMSs and the other is communication with BMS. VMS will be a computer/server with a special-purpose operating system.

Functions depending on the payment scheme:

- item claim by user at vendor,
- vendor certificate revocation by vendor upon key compromise.

Other functions:

- collecting coins from all VTs,
- sending coins to BMS for redemption,
- sending data to all VTs (broker’s blacklist, vendor’s blacklist,....),
- managing vendor’s blacklist,
- VT certificate issuance,
- creating transaction logs.

Other parts of system

Mobile broker’s terminal （MBT）

An application with similar or same functionality as the Broker’s terminal has. Application will be intended to use in mobile phones and personal computers equipped with smart card or smart card reader.

Future work

1. Layout of the terminal mainboard.
2. Connections of single components in the terminal.
3. Temper resistance of the terminal.
4. Certification of the terminal.
5. Broker's and vendor's management servers.
6. Running 3rd party's application in an untrustworthy environment.

Questions

Questions are appreciated!

Thanks

Thank you for attention!

EVROPSKÁ UNIE

MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ