



Univerzita Palackého
v Olomouci

Elektronické volby (nejen) na UP



Univerzita Palackého
v Olomouci

digitalizace

To není jednoduchý proces ta ~~přestavba~~.
Není. To je proces, bych řekl, v kterém se ne
každý dost vyzná a proces, do kterého mohou
vstoupit nepřátelé a vypadají přitom jako
přátelé, určitou dobu.

Miloš Jakeš
Generální tajemník ÚV KSČ
Červený Hrádek, 17. 7. 1989



Univerzita Palackého
v Olomouci

**Nacházíme se
v přelomové
době a určit
směr
není snadné**





Univerzita Palackého
v Olomouci

To není jednoduchý proces, ta digitalizace ...

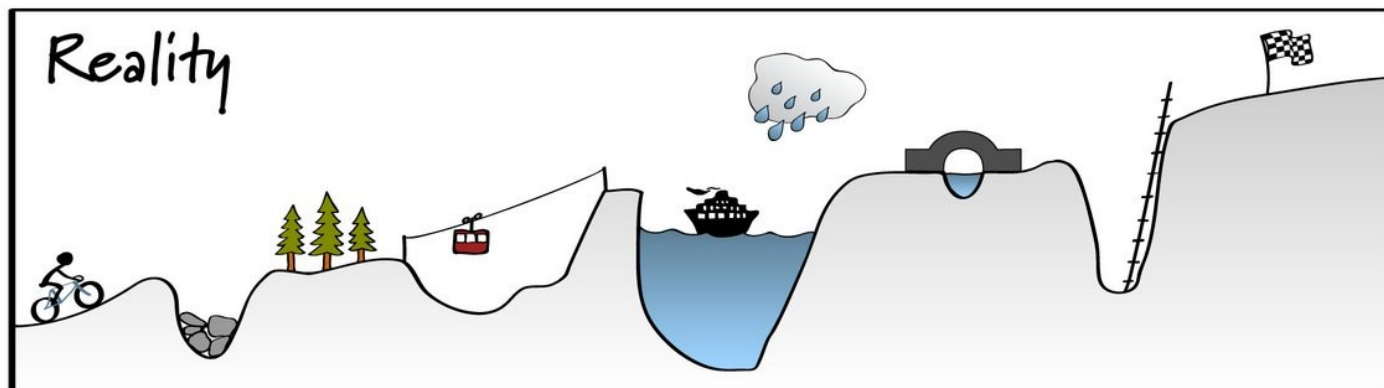
PROČ?

1. Proces není jasně definován ani v analogové formě
2. Komplexita digitalizovaných procesů je nad rámec chápání normálních lidí
3. Digitalizace nutí lidi chovat se jako stroje
4. Digitalizace není zadarmo
5. Vzniká digitální tma
6. Digitalizují se agendy, u kterých se to nevyplatí
7. Existují procesy, které by se z bezpečnostních důvodů vůbec digitalizovat neměly



Univerzita Palackého
v Olomouci

1. Proces není jasně definován ani v analogové formě





1. Proces není jasně definován ani v analogové formě

- Proces v analogové formě vůbec neexistuje nebo probíhá ad hoc nahodile
- Proces nemá jednoznačného vlastníka, který může rozhodnout o podobě procesu a prosadit jej
- Proces není v analogové formě otestován
- Proces bývá často vymyšlen až v rámci digitalizace
- Proces vymýšlejí ajťáci, nikoli management
- Selhává analytická fáze, selhává testovací fáze



Univerzita Palackého
v Olomouci

2. Komplexita digitalizovaných procesů je nad rámec chápání normálních lidí





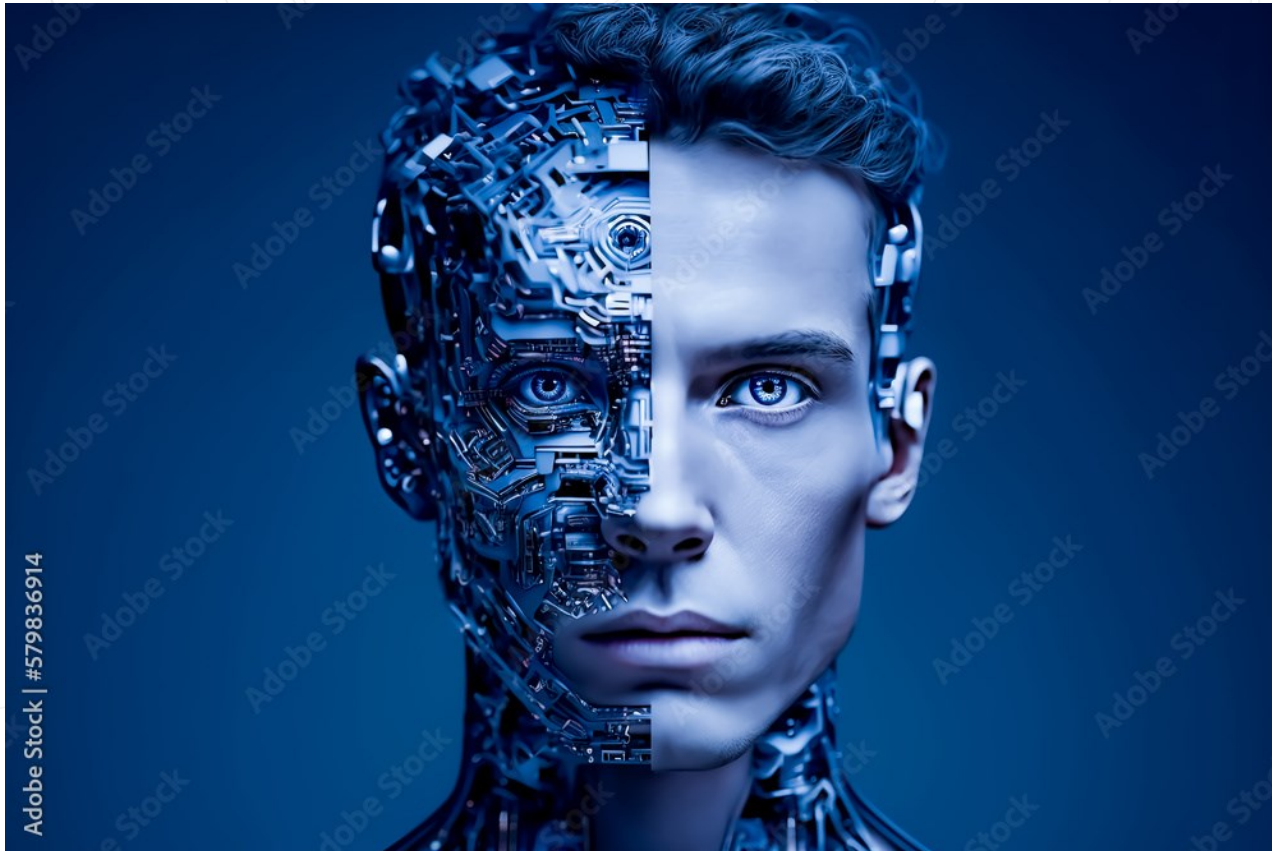
2. Komplexita digitalizovaných procesů je nad rámec chápání normálních lidí

- Snaha procesně podchytit komplexitu života vede k velmi komplexním informačním systémům
- Systémy jsou digitalizovány odděleně, neuralgickým bodem je systémová integrace
- BFU nemá šanci intuitivně pochopit
- Nemá šanci se to naučit
- Když se to naučí tak to zapomene, nepoužívá-li to denně
- Nemluvě o seniorech



Univerzita Palackého
v Olomouci

3. Digitalizace nutí lidi chovat se jako stroje





3. Digitalizace nutí lidi chovat se jako stroje

- Digitalizace má nekompromisní časovou auditní stopu
- Mizí flexibilita papíru
- Ukazuje se, že legislativa nikdy nebyla striktně dodržována a proces nikdy neprobíhal tak, jak je popsán
- Digitalizace některých procesů může paralyzovat organizaci



Univerzita Palackého
v Olomouci

4. Digitalizace není zadarmo





4. Digitalizace není zadarmo

- Náklady na prvotní vývoj. Náklady na úpravy. Servisní náklady. Vendor lock.
- Náklady na infrastrukturu, náklady na periodickou obnovu infrastruktury
- Náklady na provoz datových úložišť
- Digitalizace je na elektřinu. 24/7



Univerzita Palackého
v Olomouci

5. Vzniká digitální tma





5. Vzniká digitální tma

- Za několik století se děti budou učit, že po roce 2020 nastala digitální tma a o dění v pozdějších letech nemáme žádné historické záznamy
- Data se ztratí, budou ve formátech, které nikdo nepřečte, na nosičích, které nikdo nepřečte



Univerzita Palackého
v Olomouci

6. Digitalizují se agendy, u kterých se to nevyplatí





6. Digitalizují se agendy, u kterých se to nevyplatí

- Papír není sprosté slovo!!!
- Digitalizace mnohdy práci vůbec neušetří, naopak jí přidá
 - Digitalizovaný systém může být mnohem komplexnější než papírový a žádný pořádný byrokrat si tuto příležitost nenechá ujít
- Šetří se práce nízko kvalifikovaných/příjmových pracovníků
- Digitalizují se agendy, které člověk dělá jen zřídka, někdy jednou za život



Univerzita Palackého
v Olomouci

7. Existují procesy, které by se z bezpečnostních důvodů vůbec digitalizovat neměly





Univerzita Palackého
v Olomouci

7. Existují procesy, které by se z bezpečnostních důvodů vůbec digitalizovat neměly

Třeba volby.

- A když se do toho pustíte, mělo by se to udělat hodně pořádně.



Univerzita Palackého
v Olomouci

Oslí můstek k elektronickým volbám





Univerzita Palackého
v Olomouci

Volební aplikace UP

- Aplikace primárně pro volby do akademických senátů školy
 - Ale také např. kolejní rada, soutěže o ceny děkana, studentský ombudsman
- V provozu od cca 2017 z poptávky několika fakult
- Rozšíření v průběhu COVIDu
- Webová aplikace vlastní výroby, ASP .NET framework, C#
- Přihlášení uživatele prostřednictvím SSO Shibboleth
- Responzivní design
- Implementovány různé volební algoritmy



Univerzita Palackého
v Olomouci

Volební aplikace UP

– Velmi jednoduché uživatelské rozhraní

Oblíbená zvířata

Kandidáti

1. Barevný Chameleon	
2. Čistotné Prase	
3. Chudá Myš	
4. Drzá Veverka	>
5. Líná Veš	>
6. Lstivá Liška	>

Moje volba

1	☒ 1. Barevný Chameleon	↑ ↓
	☒ 2. Čistotné Prase	2 <input checked="" type="button" value="↑"/> <input checked="" type="button" value="↓"/>
	☒ 3. Chudá Myš	↑ ↓

Máte vybráno 3 z 11 možných kandidátů

3 [Pokračovat na rekapitulaci >](#)



Zabezpečení „by design“

- Volební hlas je jednoduchý řetězec (comma separated) tvořený kódem kurie a pořadovými čísly kandidátů
- Hlas je uložen do tabulky v databázi (urny), hlas není svázán s uživatelem, evidujeme pouze fakt, že uživatel hlasoval
- Primárním klíčem je guid, není zde stopa v jakém pořadí byly hlasy vloženy



Zabezpečení „by design“

- Hlas je kódovaný asymetrickým RSA šifrováním s délkou klíče 2048 bitů, kódování je NA KLIENTOVI
- RSA klíče si vytváří volební komise sama – máme na to aplikaci, případně lze využít OpenSSL
- Veřejný klíč je uložen v konfiguraci (mimo databázi), je k dispozici na klientovi
- Soukromý klíč je uložen na flešce v trezoru na děkanátě = v průběhu voleb není možné zjistit obsah urny
- Hlas má náhodný padding = stejné hlasy vypadají zašifrované jinak
- Bez vstupu volební komise není možné volby rozšifrovat/vyhodnotit



Zabezpečení „by design“

- Hlasy, padající do urny, jsou průběžně šifrovány symetrickým klíčem (klíč je natvrdo v kódu) = nelze např. podvrhnout jinou databázi
- Při přidání hlasu do databáze je generován a průběžně ukládán checksum = nelze např. nahradit jeden řádek v tabulce jiným
 - Důsledkem je, že vkládání hlasů do databáze je chráněno kritickou sekcí, probíhá sekvenčně, nelze paralelizovat, má efekt na výkon
- Uživateli se zobrazí segment jeho hlasu a obsah urny = může si ověřit, že jeho hlas je v urně
 - Ale pouze jednou za 24 hodin = nelze např. provádět snapshoty urny
- Obdobně komise může jednou denně zobrazit obsah zašifrované urny = jistota že např. včera odevzdané hlasy v urně stále jsou



Vyhodnocení voleb

- Hlasy jsou dešifrovány symetrickým klíčem
- Zkontroluje se sekvence checksumů
- **Komise vloží privátní klíč**
- Dešifrují se hlasy
- Aplikuje se volební algoritmus
- Zobrazí se výsledky
- Vyhodnocení lze provést i ručně pomocí skriptů a OpenSSL knihovny



Organizační zabezpečení

- Volební komise si sama generuje pár klíčů – máme na to aplikaci, případně využije OpenSSL. IT oddělení nezná privátní klíč.
- Opatření na straně IT: správce databáze nemá přístup ke kódu; programátor nemá přístup k databázi, správce serveru nemá přístup ke kódu ani k databázi



Poznatky ze života

- Pokud volební komise ztratí privátní klíč, volby nelze vyhodnotit. Fakt to nejde. Věřte nám.
- Je třeba upravit volební řád, např.
 - Volební řád připouštěl neplatné hlasy. Aplikace může platnost hlasu hlídat, ale lze to vypnout.
 - Volební řád předpokládal konání např. od 8 do 16 hodin, ale aplikaci jsme na noc nevypínali
- Před volbami je dobré uspořádat testovací běh
- Není dobré dávat začátek voleb na půlnoc
- Seznamy voličů i seznamy kandidátů dodává vždy volební komise (nejsou generovány ze systémů za běhu), nelze je měnit

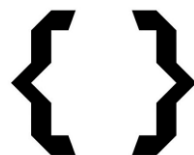


Univerzita Palackého
v Olomouci

System používají i jiné školy



UNIVERZITA
PARDUBICE



UHK



Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM





Univerzita Palackého
v Olomouci

Elektronické volby fungují skvěle zatím žádný průšvih

**Situace je, bych řekl, nadmíru výtečná.
Všechny orgány plní své úkoly, jak mají.**

...

Igor Němec, primátor hl. m. Prahy, 13. srpna 2002

O několik hodin později bylo zaplaveno 17 kilometrů metra



Univerzita Palackého
v Olomouci