User ID:

Password: *********

Login

Úrovne autentifikácie

Ľubor Illek, Gordias sro., 2013

Autentifikácia

- Stále najčastejšie meno/heslo
- Funkčne triviálna
- Pre bezpečnosť kľúčová

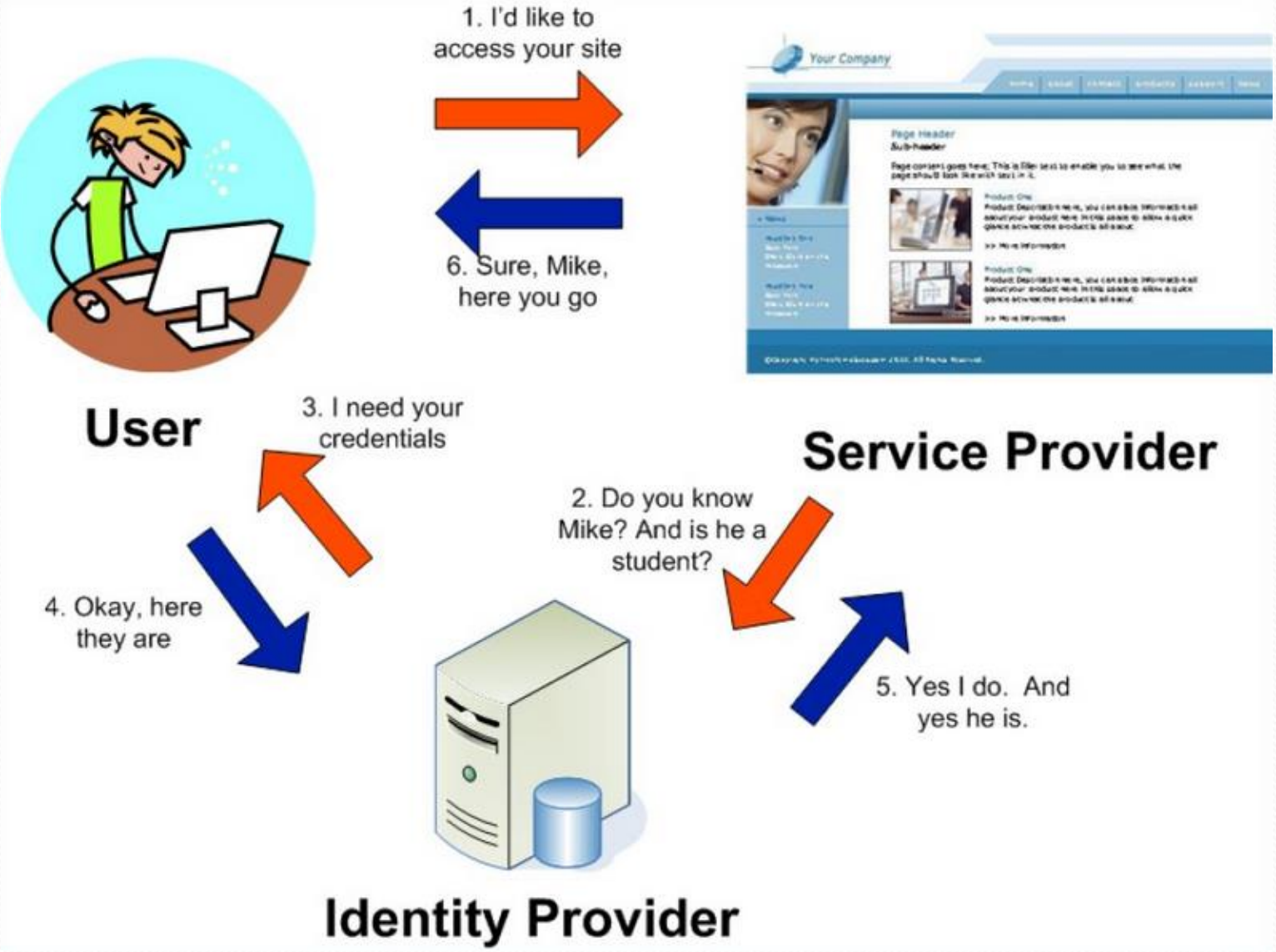
- Veľa chýb – návrh, algoritmy, implementácia
- Veľké úniky údajov

⇨ Najčastejšia cesta kompromitácie

Heslá - stav

- priemerný používateľ: 26 účtov, 5 rôznych hesiel
- 40% zdieľa heslo s inými
- >98% účtov má heslo spomedzi 10.000 najčastejších
- 0,5% hesiel má špeciálny znak, 41% iba písmená
- úniky hesiel
  - Twitter - 250.000, LinkedIn – 6.500.000 (zverejnené)
  - Yahoo - 450.000 , NVidia, Last.fm...
  - eHarmony - 1,5M; 80% prelomených do 3 dní

Úrovne autentifikácie



Zdroj: identity.it.ufl.edu

Kvalita autentifikácie

- 1. Procesy registračnej fázy
  - Kvalita registračnej procedúry / Spoľahlivosť vydania identity / Spoľahlivosť identity providera
- 2. Správa autentifikačných údajov
- 3. Autentifikačná fáza
  - Robustnosť mechanizmu / Bezpečnosť implementácie

1. Kvalita registračnej procedúry

⇨ Kto je žiadateľ?

- Miera prítomnosti
  - vzdialená/fyzická prítomnosť
- Kvalita identifikačných údajov
  - množstvo údajov / jednoznačná identifikácia
- Overenie vierohodnosti
  - kto potvrdzuje pravosť údajov?

1. Spoľahlivosť vydania identity

⇨ Ako sa k žiadateľovi údaje dostanú?

- Zaslanie autentfikačných údajov
  - mail / web / pošta / viacero kanálov
- Validácia adresáta
  - treťou stranou / do vlastných rúk
- Verifikácia adresáta
  - podpisom / prítomnosťou

1. Spoľahlivosť identity providera

⇨ Nakoľko sa dá IP dôverovať?

- Pohľad STORK: Oficiálnosť inštitúcie
  - Zmluva / certifikácia / štátna org. / smernica 1999/93/ES

- Záruky spoľahlivosti
  - formalizácia procesov / riadenia, vyspelosť org.
  - úroveň riešenia súladu
  - uchovávanie záznamov

2. Správa údajov

⇨ Nakoľko sú autentifikačné údaje chránené?

- Identity provider
  - ochrana systému, reakčné procesy
- Používateľ identity
  - ochrana pred stratou / zneužitím, ochrana PC

3. Robustnosť mechanizmu

⇨ Pomocou čoho sa prihlasujem?

- Meno / heslo / PIN
- Jednorazové heslo / GRID karta
- Certifikát / HW ochrana kľúča / kvalifikovaný certifikát

3. Bezpečnosť implementácie

⇨ Ochrana pred útokmi

- Hádanie / útok hrubou silou
- Odpočúvanie
- Hijacking (únos spojenia)
- Replay (opakovanie poslaných údajov)
- Man in the middle (útočník v strede spojenia)

STORK QAA

		Assurance Levels for Electronic Authentication pha			
		EA1	EA2	EA3	EA4
Assurance Levels for Registration phase	RP1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

- Výnos MF SR o štandardoch pre ISVS
  - povinné označovanie úrovne,
  - dodržiavanie pravidiel STORK

- Ďakujem za pozornosť