

Yubikey

Hypetystä tervejärkisesti

Ilkka Pirttimaa

Autentikointi

- Kuka yrittää käyttää järjestelmää?
 - Mikä on sopiva riskitaso hakkeroinnin vs. käytettävyyden välillä?
- Kuinka monen tekijän tunnistautuminen halutaan?

Esim. Koti → 2:n tekijän turvaratkaisu (fyysinen avain + tieto mihin taloon se käy)

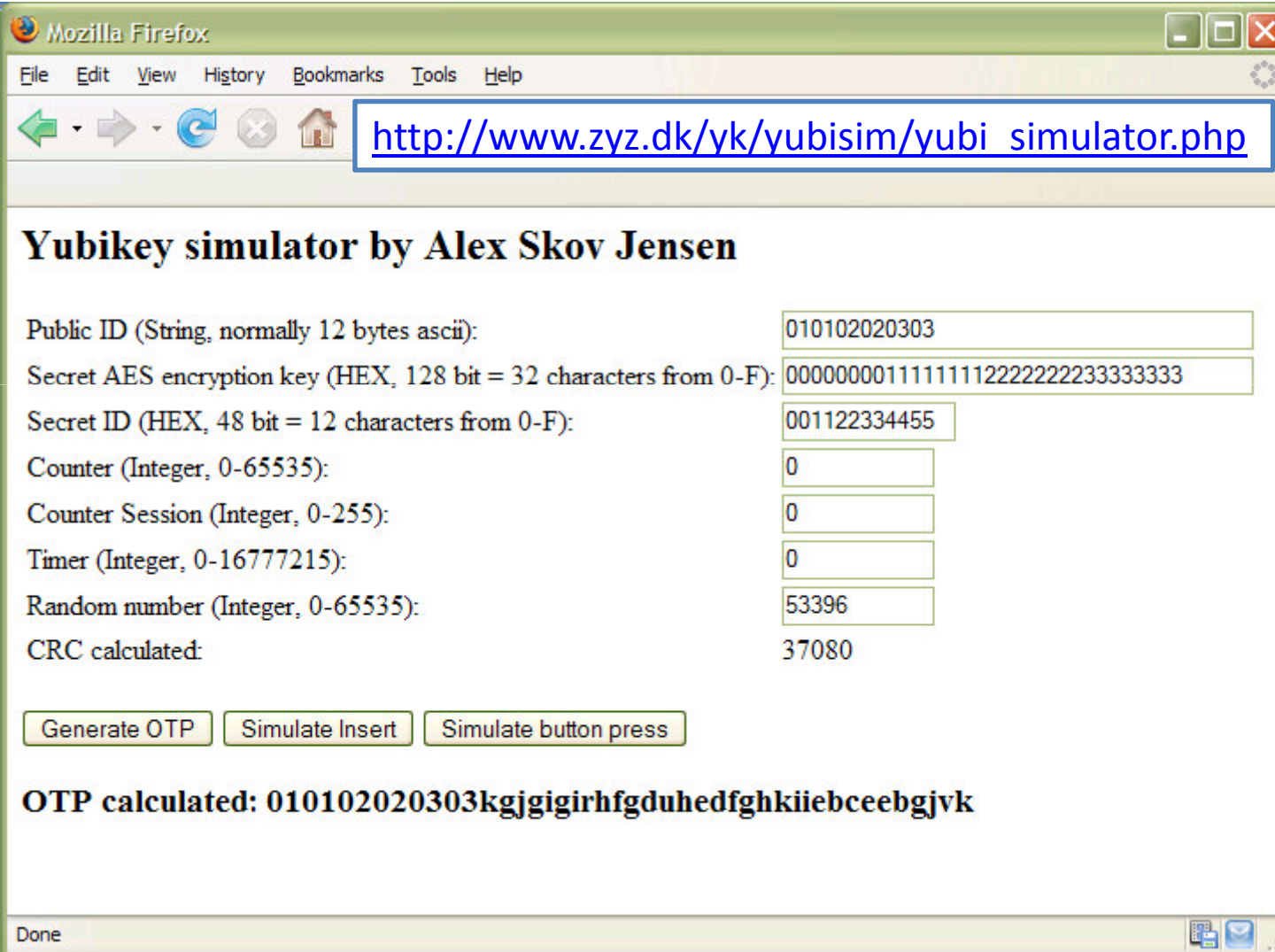
Kirjautuminen monitekijätunnistuksella

Tekijä	Pankkiauto- maatti	Windos- kirjautuminen	Verkko- pankki	SecurID	YUBIKEY
Jotain mitä tiedät	Tunnusluku	Käyttäjätunnus + Salasana	Asiakas- numero + Salasana, seuraavan koodin numero	Käyttäjä- tunnus + PIN-koodi	* (käytä mitä haluat)
Jotain mitä sinulla on	Kortti		Tunnus- koodilista	SecurID- avain + maksullinen backend	UBIKEY + OpenSource backend
Jotain mitä olet		Sormenjälki			* (käytä mitä haluat)

Innovaatio: USB-näppis!

- USB-näppis ei tarvitse ajuria missään ympäristössä (Windows, MacOS, Linux)
- Yksi nappi, joka tuottaa joka kerta yksilöllisen ”blaablaan”, josta oikealla salausavaimella tarkistettavissa:
 - Mikä Yubikey? (jokaisessa yksilöllinen tunnus)
 - Tuottiko Yubikey ko. avaimen liitetyn salaisen avaimen mukaisen sisällön?
 - Replay-attack estetty kirjaamalla varmennuspalveluun joka kerta kasvava numerokoodi
- Merkittävin ero muihin: Businessmalli on myydä laitetta, ei ohjelmistoja → Avoimet ohjelmointirajapinnat ja paljon valmiita toteutuksia

UbiKey simulaattori



The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL http://www.zyz.dk/yk/yubisim/yubi_simulator.php. The page title is "Yubikey simulator by Alex Skov Jensen". The interface includes several input fields for simulation parameters and a set of control buttons.

Public ID (String, normally 12 bytes ascii):	010102020303
Secret AES encryption key (HEX, 128 bit = 32 characters from 0-F):	00000000111111112222222233333333
Secret ID (HEX, 48 bit = 12 characters from 0-F):	001122334455
Counter (Integer, 0-65535):	0
Counter Session (Integer, 0-255):	0
Timer (Integer, 0-16777215):	0
Random number (Integer, 0-65535):	53396
CRC calculated:	37080

Buttons:

OTP calculated: 010102020303kgjgigirhfgduhedfghkiiebceebgjvk

Done

UbiKey simulaattori / 2

Yubikey simulator by Alex Skov Jensen

Public ID (String, normally 12 bytes ascii):	<input type="text" value="010102020303"/>
Secret AES encryption key (HEX, 128 bit = 32 characters from 0-F):	<input type="text" value="00000000111111112222222233333333"/>
Secret ID (HEX, 48 bit = 12 characters from 0-F):	<input type="text" value="001122334455"/>
Counter (Integer, 0-65535):	<input type="text" value="1"/>
Counter Session (Integer, 0-255):	<input type="text" value="1"/>
Timer (Integer, 0-16777215):	<input type="text" value="144"/>
Random number (Integer, 0-65535):	<input type="text" value="62764"/>
CRC calculated:	36520

OTP calculated: 010102020303jbbhhlufjhjdiuebltjhdbcttklftcff

Done

Mihin voi käyttää?

- Suoraan ”laatikosta”:
 - Mikä tahansa OpenID-kirjautumista tukeva järjestelmä (Paljon Web 2.0 –saitteja)
 - Yubico.comin webservice-rajapinnat
- Paljon valmiita OpenSource-ratkaisuja, mm. Ssh-kirjautuminen, windows-kirjautuminen
- Oma sovellus, esim.
 - Sovellus luottaa Windows-kirjautumiseen
 - ADMIN-näytölle lisätään yksi kenttä, johon pitää syöttää YUBIKEY-koodi
 - Palvelin tarkistaa ennen tietojen hyväksymistä, käytettiinkö ko. käyttäjään liitettyä avainta ja oliko avaimen antama koodi aito ja ei aiemmin nähty

OpenID

