Revised Attacks on Norwegian Banks

Oleksandr Kazymyrov, Kjell Jørgen Hole

Selmer Center, Department of Informatics,
University of Bergen, Norway
Oleksandr.Kazymyrov@uib.no

Winter School, Finse'13

Outline

1. Introduction
2. PIN Attack

Previous Work

This is an independent IT-security analysis based on the article

Kjell Jørgen Hole, Vebjørn Moen, Thomas Tjøstheim, Case Study: Online Banking Security. IEEE Security & Privacy 4(2): 14-20 (2006).

Terminology

ID number or SSN (Fødselsnummer)

An eleven digit number is assigned at birth or registration in the National Population Register.

PIN code

A personal identification number (PIN) is a secret numeric password shared between a user and a system.

Personal Password (PP) or password

A password is a secret string of characters that is used for authentication.

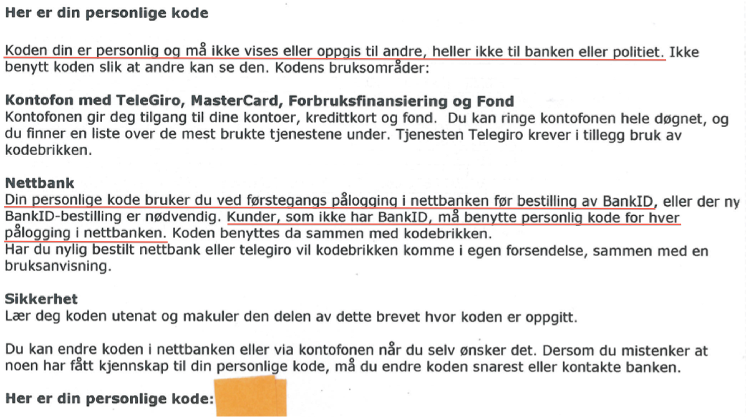
One-time password (OTP)

A password that is valid for only one login session and/or transaction.

Getting a Netbank Account at DNB

- Become a customer of the bank
- Request a netbank account
- The bank sends a 4 digits PIN code and an OTP generator in two separate mails
- PIN and SSN (and OTP) are used for registration
- After registration a customer has OTP generator, PIN and personal password(PP)

Example of the Letter



Her er din personlige kode

Koden din er personlig og må ikke vises eller oppgis til andre, heller ikke til banken eller politiet. Ikke benytt koden slik at andre kan se den. Kodens bruksområder:

Kontofon med TeleGiro, MasterCard, Forbruksfinansiering og Fond
Kontofonen gir deg tilgang til dine kontoer, kredittkort og fond. Du kan ringe kontofonen hele døgnet, og du finner en liste over de mest brukte tjenestene under. Tjenesten Telegiro krever i tillegg bruk av kodebrikken.

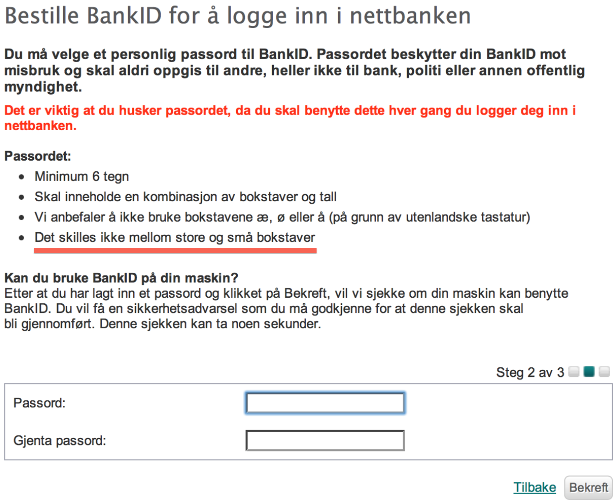
Nettbank
Din personlige kode bruker du ved førstegangs pålogging i nettbanken før bestilling av BankID, eller der ny BankID-bestilling er nødvendig. Kunder, som ikke har BankID, må benytte personlig kode for hver pålogging i nettbanken. Koden benyttes da sammen med kodebrikken.
Har du nylig bestilt nettbank eller telegiro vil kodebrikken komme i egen forsendelse, sammen med en bruksanvisning.

Sikkerhet
Lær deg koden utenat og makuler den delen av dette brevet hvor koden er oppgitt.

Du kan endre koden i nettbanken eller via kontofonen når du selv ønsker det. Dersom du mistenker at noen har fått kjennskap til din personlige kode, må du endre koden snarest eller kontakte banken.

Her er din personlige kode: [redacted]

Password Requirements



Bestille BankID for å logge inn i nettbanken

Du må velge et personlig passord til BankID. Passordet beskytter din BankID mot misbruk og skal aldri oppgis til andre, heller ikke til bank, politi eller annen offentlig myndighet.

Det er viktig at du husker passordet, da du skal benytte dette hver gang du logger deg inn i nettbanken.

Passordet:

- Minimum 6 tegn
- Skal inneholde en kombinasjon av bokstaver og tall
- Vi anbefaler å ikke bruke bokstavene æ, ø eller å (på grunn av utenlandske tastatur)
- Det skilles ikke mellom store og små bokstaver

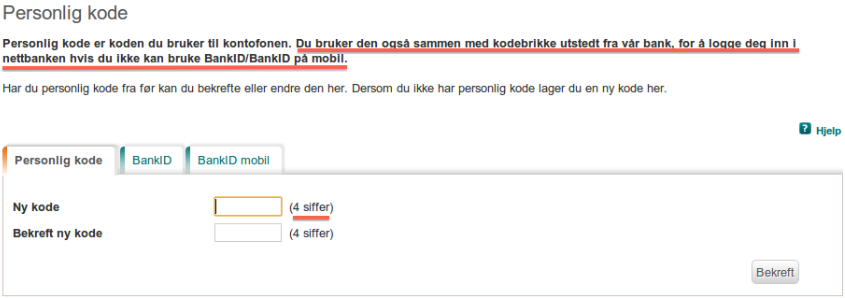
Kan du bruke BankID på din maskin?
Etter at du har lagt inn et passord og klikket på Bekreft, vil vi sjekke om din maskin kan benytte BankID. Du vil få en sikkerhetsadvarsel som du må godkjenne for at denne sjekken skal bli gjennomført. Denne sjekken kan ta noen sekunder.

Steg 2 av 3 □ ■ □

Passord:

Gjenta passord:

Changing Password



Personlig kode

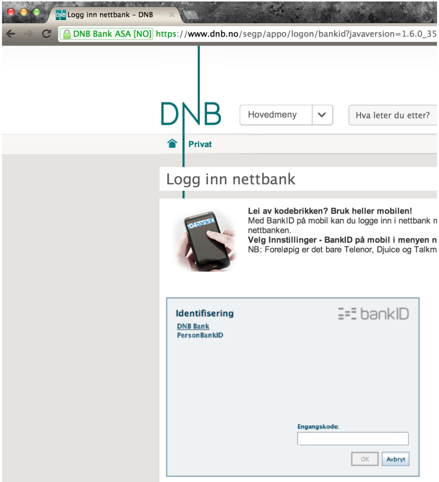
Personlig kode er koden du bruker til kontofonen. Du bruker den også sammen med kodebrikke utstedt fra vår bank, for å logge deg inn i nettbanken hvis du ikke kan bruke BankID/BankID på mobil.

Har du personlig kode fra før kan du bekrefte eller endre den her. Dersom du ikke har personlig kode lager du en ny kode her.

Ny kode		(4 siffer)
Bekreft ny kode		(4 siffer)

Logging Netbank

Normal log in using SSN, OTP and PP.


Logg inn nettbank – DNB
DNB Bank ASA [NO] https://www.dnb.no/segp/appo/logon/bankid?javaversion=1.6.0_35
DNB
Hovedmeny
Hva leter du etter?
Privat
bankID
bankID
OK
Avbryt

Logg inn nettbank

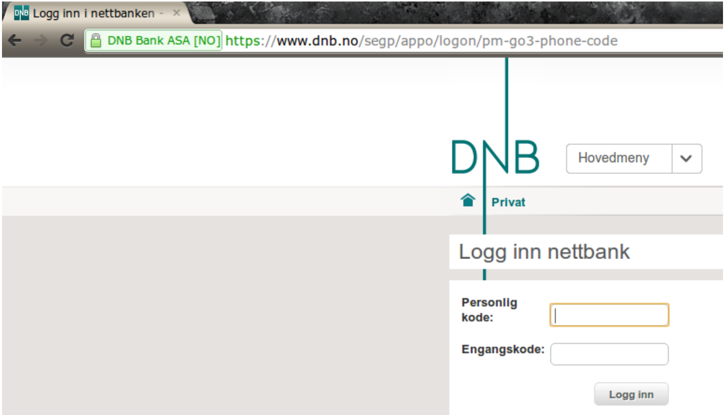
Lei av kodebrikken? Bruk heller mobilen!
Med BankID på mobil kan du logge inn i nettbank n
nettbanken.
Velg Innstillinger - BankID på mobil i menyen n
NB: Foreløpig er det bare Telenor, Djuice og Talkm

Identifisering
DNB Bank
PersonBankID

Engangskode:

Logging Netbank

Mobile log in (browser) using SSN, PIN and OTP.



Logg inn i nettbanken

DNB Bank ASA [NO] https://www.dnb.no/segp/appo/logon/pm-go3-phone-code

DNB

Hovedmeny

Privat

Logg inn nettbank

Personlig kode:

Engangskode:

Logg inn

General Representation of Attacks

1. disable (delete) Java
2. use the authorization page for mobile devices
3. for all SSN numbers brute force PIN and OTP
4. for specific person
    - find SSN number of a victim
    - brute force PIN and OTP

General Theoretical Approach

Suppose SSN, PP and OTP are unknown. Then

$$\begin{aligned} P_{\text{one account}} &= P_{SSN} \cdot P_{PP} \cdot P_{OTP} = \\ &= \frac{1}{10^{11}} \cdot \frac{1}{11^{6}} \cdot \frac{1}{10^{6}} \approx 5.64 \cdot 10^{-24} \approx 2^{-77} \end{aligned}$$

Suppose SSN, PIN and OTP are unknown. Then

$$\begin{aligned} P_{\text{one account}} &= P_{SSN} \cdot P_{PIN} \cdot P_{OTP} = \\ &= \frac{1}{10^{11}} \cdot \frac{1}{10^{4}} \cdot \frac{1}{10^{6}} = 10^{-21} \approx 2^{-70} \end{aligned}$$

Scenario 1

Scenario 1

An adversary tries to obtain the SSN of a particular victim.

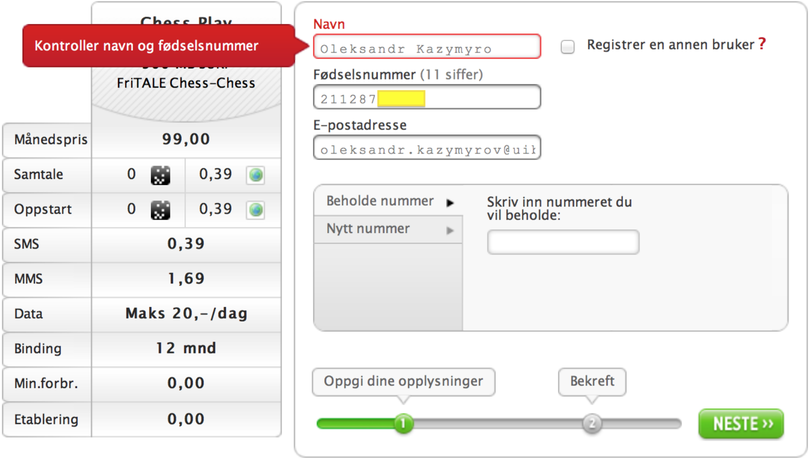
SSN has the structure

$$d_1d_2m_1m_2y_1y_2i_1i_2i_3c_1c_2$$

Date of birth can be found from different sources

- social networks (Facebook, Twitter, LinkId ...)
- using public services including skattelister.no, skatteetaten.no, 1881.no ...
- identification card

SSN Determination for Known DoB



Chess Play

Kontroller navn og fødselsnummer

FriTALE Chess-Chess

Månedspris	99,00			
Samtale	0	▦	0,39	●
Oppstart	0	▦	0,39	●
SMS	0,39			
MMS	1,69			
Data	Maks 20,-/dag			
Binding	12 mnd			
Min.forbr.	0,00			
Etablering	0,00			

Navn: Oleksandr Kazymyro

☐ Registrer en annen bruker ?

Fødselsnummer (11 siffer): 211287[redacted]

E-postadresse: oleksandr.kazymyrov@uik

Beholde nummer ▸

Nytt nummer ▸

Skriv inn nummeret du vil beholde:

Scenario 1

Suppose all variables are unknown except the date of birth. Then

$$P_{\text{one account}} = \frac{1}{10^5} \cdot \frac{1}{10^4} \cdot \frac{1}{10^6} = 10^{-15} \approx 2^{-50}$$

The theoretical calculation for known SSN

$$P_{\text{one account}} = \frac{1}{10^4} \cdot \frac{1}{10^6} = 10^{-10} \approx 2^{-34}$$

Attacks progress

$$2^{\infty} \overset{PP_{res}}{\rightarrow} 2^{-77} \overset{PIN}{\rightarrow} 2^{-70} \overset{DoB}{\rightarrow} 2^{-50} \overset{SSN}{\rightarrow} 2^{-34}$$

Scenario 2

Scenario 2

An adversary knows the SSN and tries to obtain PIN of the victim.

There are two different types of brute force attacks

- passive (acquire PIN code)
- active (access to netbank)

Brute Force Attack. Active

- The main steps of active brute force attack
  1. check all SSNs
  2. attack as fast as possible
  3. distribute interactions with the netbank (use many IPs)
- The probability of the successful attack for Q users

$$P_{\text{at least one account}} = 1 - (1 - P_{\text{one account}})^{Q}$$

$$P_{\text{at least one account}} = 1 - (1 - 5 \cdot \frac{1}{10^4} \cdot \frac{1}{10^6})^{3 \cdot 10^5} \approx$$

$$\approx 10^{-4} \approx 2^{-14}$$

Brute Force Attack. Active

$$P_{\text{one account}} = 5 \cdot \frac{1}{10^4} \cdot \frac{1}{10^6}$$

	PIN	Frequency, %
#1	1234	10.713
#2	1111	6.016
#3	0000	1.881
#4	1212	1.197
#5	7777	0.745

Brute Force Attack. Active

$$P_{\text{one account}} = 0.20552 \cdot \frac{1}{10^6} = \frac{2055.2}{10^4} \cdot \frac{1}{10^6}$$

	PIN	Frequency, %
#1	1234	10.713
#2	1111	6.016
#3	0000	1.881
#4	1212	1.197
#5	7777	0.745

$$P_{\text{at least one account}} = 1 - (1 - \frac{2055.2}{10^4} \cdot \frac{1}{10^6})^{3 \cdot 10^5} \approx$$
$$\approx 0.06 \approx 2^{-4}$$

Brute Force Attack. Passive

- The main steps of passive brute force attack
  1. log in less than 5 times for each SSN
  2. spread attack over a long time period
  3. use different IP addresses
  4. geographically distribute interactions with the netbank
- The probability of the successful attack for Q users and T times

$$P_{\text{at least one account}} = 1 - (1 - P_{\text{one account}})^{Q \cdot T}$$

$$P_{\text{at least one account}} = (1 - (1 - 4 \cdot \frac{1}{10^4} \cdot \frac{1}{10^6})^{3 \cdot 10^5 \cdot 5}) \approx$$

$$\approx 6 \cdot 10^{-4} \approx 2^{-11} \overset{PIN_{destr}}{\approx} 0.077$$

Conclusions and Propositions

Conclusions

- after decade the bank(s) are still vulnerable to brute force attack with high probability
- DDoS attack may result into gray swan
- it is possible at least partially to obtain private data from communication between server and client using open tools

Conclusions and Propositions

Conclusions

- after decade the bank(s) are still vulnerable to brute force attack with high probability
- DDoS attack may result into gray swan
- it is possible at least partially to obtain private data from communication between server and client using open tools

Propositions

- protect servers from BEAST attack
- it is necessary to establish a procedure for independent auditing

Open Questions

1. Is it possible to use the same OTP for log in and transfer money?
2. What is the difference between common code generator, "digipass" and "BankID på mobil"?
3. Analyze `http://m.dnb.no` in more detailed way.
4. Are the problems listed above specific for the DNB bank or this is a general problem?
5. Can we use "BankID på mobil" service for spam or DoS attack?