Attacking the Verification Code Mechanism in the Norwegian Internet Voting System

Reto E. Koenig, Philipp Locher, Rolf Haenni

Bern University of Applied Sciences

17.07.2013

Supported by the Swiss National Science Foundation
(project No. 200021L_140650)

Outline

Outline

Outline

Why This Talk?

The Norwegian E-Voting System...

Why This Talk?

The Norwegian E-Voting System...

- ...allows vote updating
- ...uses SMS as out-of-band post channel
- ...uses smart-phone as trusted device
- ...faces a secure platform problem
- ...cannot provide the required vote integrity by verification-code
- ...can be fixed!

Why This Talk?

The Norwegian E-Voting System...

- ...allows vote updating
- ...uses SMS as out-of-band post channel
- ...uses smart-phone as trusted device
- ...faces a secure platform problem
- ...cannot provide the required vote integrity by verification-code
- ...can be fixed!

Why This Talk?

The Norwegian E-Voting System...

- ...allows vote updating
- ...uses SMS as out-of-band post channel
- ...uses smart-phone as trusted device
- ...faces a secure platform problem
- ...cannot provide the required vote integrity by verification-code
- ...can be fixed!

Why This Talk?

The Norwegian E-Voting System...

- ...allows vote updating
- ...uses SMS as out-of-band post channel
- ...uses smart-phone as trusted device
- ...faces a secure platform problem
- ...cannot provide the required vote integrity by verification-code
- ...can be fixed!

Why This Talk?

The Norwegian E-Voting System...

- ...allows vote updating
- ...uses SMS as out-of-band post channel
- ...uses smart-phone as trusted device
- ...faces a secure platform problem
- ...cannot provide the required vote integrity by verification-code
- ...can be fixed!

Why This Talk?

The Norwegian E-Voting System...

- ...allows vote updating
- ...uses SMS as out-of-band post channel
- ...uses smart-phone as trusted device
- ...faces a secure platform problem
- ...cannot provide the required vote integrity by verification-code
- ...can be fixed!

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

...assumes server side to be honest

...accepts a malicious browser (MitB)

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...assumes server side to be honest
- ...accepts a malicious browser (MITB)
- $\rightarrow$ *cannot guarantee privacy (at the voter side)*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...assumes server side to be honest
- ...accepts a malicious browser (MITB)
- → *cannot guarantee privacy (at the voter side)*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...assumes server side to be honest
- ...accepts a malicious browser (MITB)
- $\rightarrow$ *cannot guarantee privacy (at the voter side)*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- creates voter-individual and candidate-based verification codes (on the server side)
- sends verification codes to the voter via out-of-band channels

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...creates voter-individual and candidate based verification code (at the server side)
- ...sends verification codes to the voter via out-of-band channels
  - ex.: mail, postal mail (secure printing)
- $\rightarrow$ provides vote integrity: *cast and recorded as intended*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...creates voter-individual and candidate based verification code (at the server side)
- ...sends verification codes to the voter via out-of-band channels
  - pre-channel postal mail (secure printing)
  - post-channel SMS (cryptographic receipt-generator)
  - → provides vote integrity: *cast and recorded as intended*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...creates voter-individual and candidate based verification code (at the server side)
- ...sends verification codes to the voter via out-of-band channels
  - pre-channel: postal mail (secure printing)
  - post-channel: SMS (cryptographic receipt-generator)
- → provides vote integrity: *cast and recorded as intended*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...

- ...creates voter-individual and candidate based verification code (at the server side)
- ...sends verification codes to the voter via out-of-band channels

  pre-channel postal mail (secure printing)
  post-channel SMS (cryptographic receipt-generator)
- → provides vote integrity: *cast and recorded as intended*

Adversary Model and Trust Assumptions

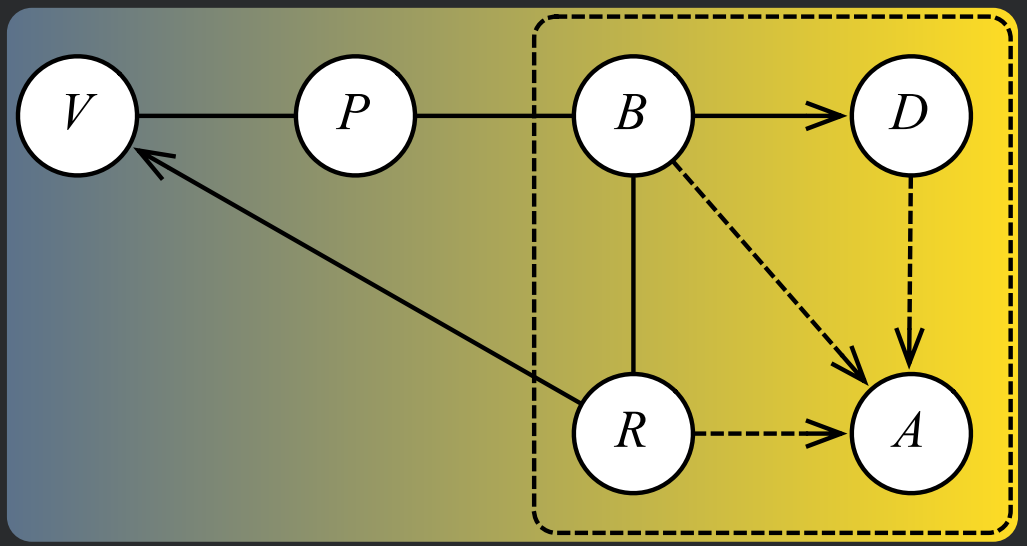
The Norwegian E-Voting System...

- ...creates voter-individual and candidate based verification code (at the server side)
- ...sends verification codes to the voter via out-of-band channels

  pre-channel postal mail (secure printing)
  post-channel SMS (cryptographic receipt-generator)
- $\rightarrow$ provides vote integrity: *cast and recorded as intended*

Adversary Model and Trust Assumptions

The Norwegian E-Voting System...



Verification Code: Recoginizing an Attack

If...

- ... correct receipt appears after the vote: Good!
- ... wrong receipt appears after the vote: Bad!

Verification Code: Recoginizing an Attack

If...

- ...correct receipt appears after the vote: Good
- ... wrong receipt appears after the vote: Bad
- ... no receipt appears after the vote: Bad
- ... receipt appears without prior vote: Bad

Verification Code: Recoginizing an Attack

If...

- ...correct receipt appears after the vote: Good
- ... wrong receipt appears after the vote: Bad
- ... no receipt appears after the vote: Bad
- ... receipt appears without prior vote: Bad

Verification Code: Recoginizing an Attack

If...

- ...correct receipt appears after the vote: Good
- ... wrong receipt appears after the vote: Bad
- ... no receipt appears after the vote: Bad
- ... receipt appears without prior vote: Bad

Verification Code: Recoginizing an Attack

If...

- ...correct receipt appears after the vote: Good
- ... wrong receipt appears after the vote: Bad
- ... no receipt appears after the vote: Bad
- ... receipt appears without prior vote: Bad

Speciality

The Norwegian E-Voting System...

...allows vote updating!

Out-of-Band Post-Channel

The Norwegian E-Voting System...

...uses SMS-channel

Enhanced Adversary model

Man in the...

...*Browser & SMS-Channel*

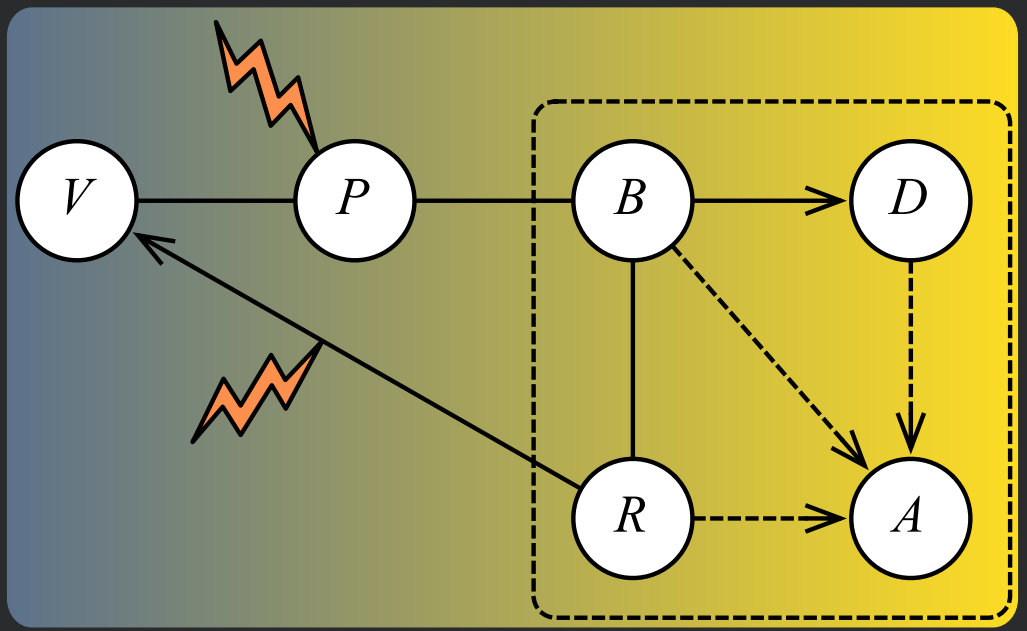
Enhanced Adversary model

Man in the...

...*B*rowser & *S*MS-Channel

SMS-Channel: No more Out-of-Band

MIT(B + S) + Vote-Updating $\mapsto$ Compromized System



Fake GSM Base Transceiver *Dedicated Hardware*

IMSI-catcher: Demonstrated live @ Defcon 2010

Fake GSM Base Transceiver *Dedicated Hardware*

IMSI-catcher: Demonstrated live @ Defcon 2010

- Hardware: 1500$ (off-the-shelf HW)
- Software: 0$ (Open Source)
- Task: Proxy GSM-network $\leftrightarrow$ GSM-phone
- Range $\approx$ 35km

Fake GSM Base Transceiver *Dedicated Hardware*

IMSI-catcher: Demonstrated live @ Defcon 2010

- Hardware: 1500$ (off-the-shelf HW)
- Software: 0$ (Open Source)

- Task: Proxy GSM-network $\leftrightarrow$ GSM-phone
- Range $\approx$ 35km

Fake GSM Base Transceiver *Dedicated Hardware*

IMSI-catcher: Demonstrated live @ Defcon 2010

- Hardware: 1500$ (off-the-shelf HW)
- Software: 0$ (Open Source)

- Task: Proxy GSM-network $\leftrightarrow$ GSM-phone
- Range $\approx$ 35km

Fake GSM Base Transceiver *Dedicated Hardware*

IMSI-catcher: Demonstrated live @ Defcon 2010

- Hardware: 1500$ (off-the-shelf HW)
- Software: 0$ (Open Source)

- Task: Proxy GSM-network $\leftrightarrow$ GSM-phone
- Range $\approx$ 35km

Malicious Browser & Fake GSM Base Transceiver
Dedicated Hardware

Logic

- MITB informs IMSI-catcher to withold every second SMS: receipt generator $\mapsto$ voter's phone

$\rightarrow$ *Silent Vote Update*

Malicious Browser & Fake GSM Base Transceiver
Dedicated Hardware

Logic

- MITB informs IMSI-catcher to withold every second SMS: receipt generator $\mapsto$ voter's phone

$\rightarrow$ *Silent Vote Update*

Malicious Browser & Fake GSM Base Transceiver
Dedicated Hardware

Logic

- MITB informs IMSI-catcher to withold every second SMS: receipt generator $\mapsto$ voter's phone

1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter's phone
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (MITB votes)
4. SMS: receipt generator $\not\mapsto$ voter's phone (IMSI-catcher blocks)

$\rightarrow$ *Silent Vote Update*

Malicious Browser & Fake GSM Base Transceiver
Dedicated Hardware

Logic

- MITB informs IMSI-catcher to withold every second SMS: receipt generator $\mapsto$ voter's phone

1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter's phone
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (MITB votes)
4. SMS: receipt generator $\not\mapsto$ voter's phone (IMSI-catcher blocks)

$\rightarrow$ *Silent Vote Update*

Malicious Browser & Fake GSM Base Transceiver
Dedicated Hardware

Logic

- MITB informs IMSI-catcher to withold every second SMS: receipt generator $\mapsto$ voter's phone

1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter's phone
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (MITB votes)
4. SMS: receipt generator $\not\mapsto$ voter's phone (IMSI-catcher blocks)

$\rightarrow$ *Silent Vote Update*

Malicious Browser & Fake GSM Base Transceiver
Dedicated Hardware

Logic

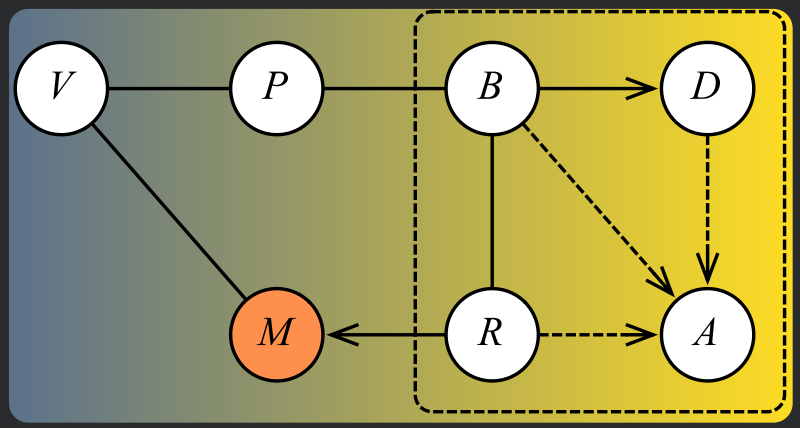
- MITB informs IMSI-catcher to withold every second SMS: receipt generator $\mapsto$ voter's phone

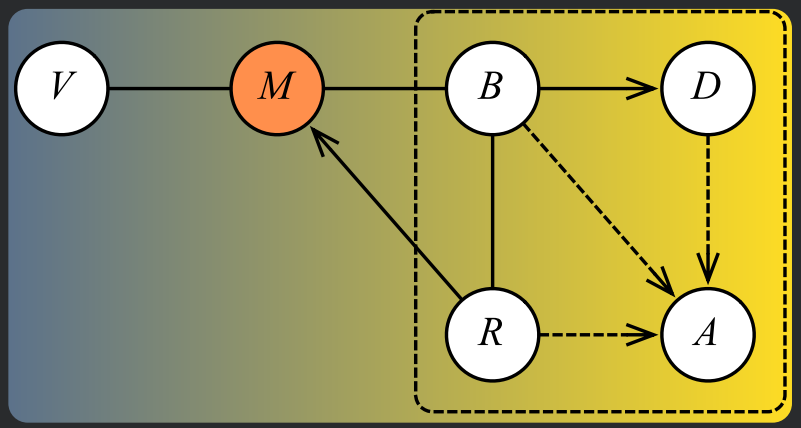
1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter's phone
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (MITB votes)
4. SMS: receipt generator $\not\mapsto$ voter's phone (IMSI-catcher blocks)

$\rightarrow$ *Silent Vote Update*

SMS-Channel: No more Out-of-Band

Introduction of Smart-Phone Technology to the Norwegian System





Enhanced Adversary model

Man in the...

...*Browser & Smart-Phone*

Enhanced Adversary model

Man in the...

...*B*rowser & *S*mart-Phone

Malicious Browser & SMS-App Software

1

Web-Buddy & SMS-Buddy: Demonstrated live @ SIC [1] 2013

- Hardware: OS (Yocto's device)
- Software: UI (Open Source)

[1] Swiss Informatics Competition

Malicious Browser & SMS-App Software

1

Web-Buddy & SMS-Buddy: Demonstrated live @ SIC [1] 2013

- Hardware: 0$ (Voter's device)
- Software: 0$ (Open Source)
- Task: Proxy smart-phone $\leftrightarrow$ voter
- Range $\approx \infty$

[1] Swiss Informatics Competition

Malicious Browser & SMS-App Software

1

Web-Buddy & SMS-Buddy: Demonstrated live @ SIC [1] 2013

- Hardware: 0$ (Voter's device)
- Software: 0$ (Open Source)

- Task: Proxy smart-phone $\leftrightarrow$ voter
- Range $\approx \infty$

[1] Swiss Informatics Competition

Malicious Browser & SMS-App Software

1

Web-Buddy & SMS-Buddy: Demonstrated live @ SIC [1] 2013

- Hardware: 0$ (Voter's device)
- Software: 0$ (Open Source)

- Task: Proxy smart-phone $\leftrightarrow$ voter
- Range $\approx \infty$

[1] Swiss Informatics Competition

Malicious Browser & SMS-App Software

1

Web-Buddy & SMS-Buddy: Demonstrated live @ SIC [1] 2013

- Hardware: 0$ (Voter's device)
- Software: 0$ (Open Source)

- Task: Proxy smart-phone $\leftrightarrow$ voter
- Range $\approx \infty$

[1] Swiss Informatics Competition

Malicious Browser & SMS-App

Logic

- Web-Buddy informs SMS-Buddy to withold every second SMS from receipt generator

→ *Silent Vote Update*

Malicious Browser & SMS-App

Logic

- Web-Buddy informs SMS-Buddy to withold every second SMS from receipt generator

→ *Silent Vote Update*

Malicious Browser & SMS-App

Logic

- Web-Buddy informs SMS-Buddy to withold every second SMS from receipt generator

1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (Web-Buddy votes)
4. SMS: receipt generator $\not\mapsto$ voter (SMS-Buddy blocks)

$\rightarrow$ *Silent Vote Update*

Malicious Browser & SMS-App

Logic

- Web-Buddy informs SMS-Buddy to withold every second SMS from receipt generator

1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (Web-Buddy votes)
4. SMS: receipt generator $\nrightarrow$ voter (SMS-Buddy blocks)

$\rightarrow$ *Silent Vote Update*

Malicious Browser & SMS-App

Logic

- Web-Buddy informs SMS-Buddy to withold every second SMS from receipt generator

1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (Web-Buddy votes)
4. SMS: receipt generator $\not\mapsto$ voter (SMS-Buddy blocks)

$\rightarrow$ *Silent Vote Update*

Malicious Browser & SMS-App

Logic

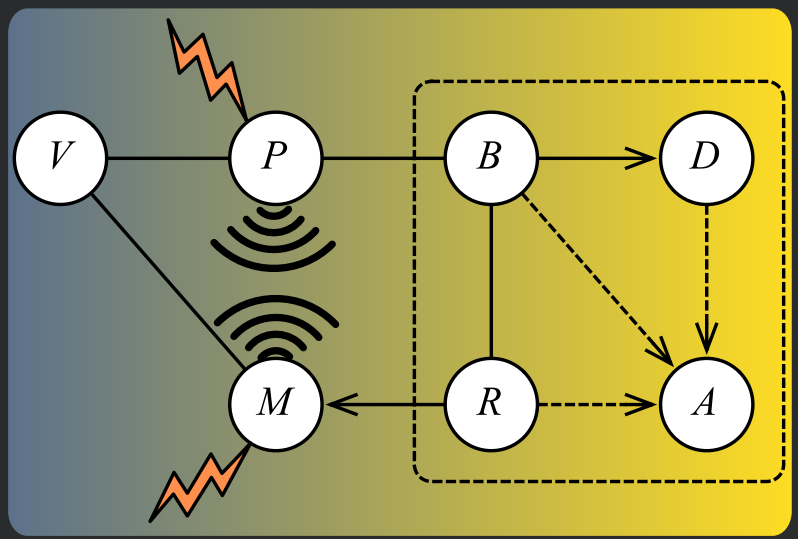
- Web-Buddy informs SMS-Buddy to withold every second SMS from receipt generator

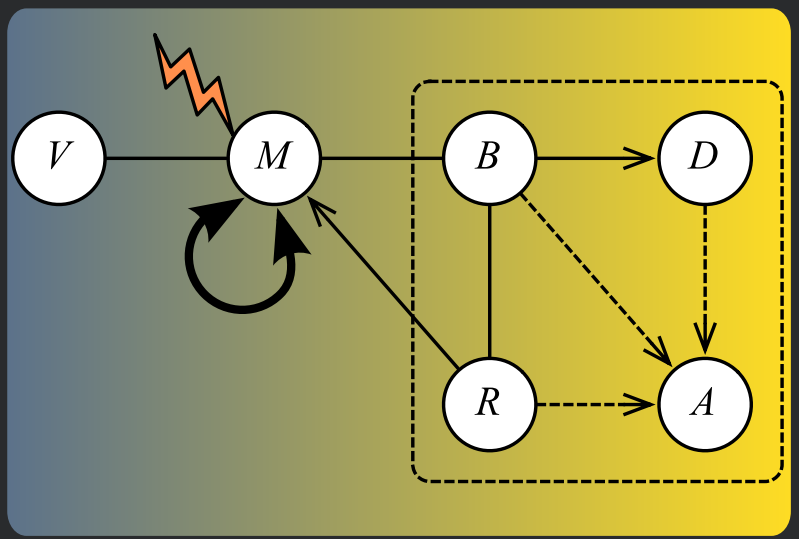
1. Voter votes in an e-voting session (via MITB)
2. SMS: receipt generator $\mapsto$ voter
3. Malicious vote update: MITB silently performs a vote-cast in the voter's e-voting session (Web-Buddy votes)
4. SMS: receipt generator $\nrightarrow$ voter (SMS-Buddy blocks)

$\rightarrow$ *Silent Vote Update*

'Silent-Channel' communication

How They Communicate





Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate

None SMS-Buddy is programmed to block every second SMS from receipt generator

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate

None SMS-Buddy is programmed to block every second SMS from receipt generator

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate

None SMS-Buddy is programmed to block every second SMS from receipt generator

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate: Two Devices (Smart-phone, Tablet)

Web-Buddy only allowed to use the Internet

SMS-Buddy only allowed to read/write SMS

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate: Two Devices (Smart-phone, Tablet)

Internet-SMS-Gateway	Web-Buddy only allowed to use the internet
SMS-Internet-Gateway	SMS-Buddy only allowed to read/write SMS

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate: Two Devices (Smart-phone, Tablet)

Internet-SMS-Gateway	Web-Buddy only allowed to use the internet
SMS-Internet-Gateway	SMS-Buddy only allowed to read/write SMS

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate: Two Devices (Smart-phone, Tablet)

Internet-SMS-Gateway	Web-Buddy only allowed to use the internet
SMS-Internet-Gateway	SMS-Buddy only allowed to read/write SMS

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How They Communicate: Two Devices (Smart-phone, Tablet)

Internet-SMS-Gateway	Web-Buddy only allowed to use the internet
SMS-Internet-Gateway	SMS-Buddy only allowed to read/write SMS

Implementation available

Channel: SMS-Buddy → Web-Buddy

How They Communicate: Two Devices (Smart-Phone, Notebook)

Ultra-Sonic SMS-Buddy broadcasts via loudspeaker
Web-Buddy listens via microphone

Proof of Concept available

Channel: SMS-Buddy → Web-Buddy

How They Communicate: Two Devices (Smart-Phone, Notebook)

Ultra-Sonic SMS-Buddy broadcasts via loudspeaker
Web-Buddy listens via microphone

Proof of Concept available

Channel: SMS-Buddy → Web-Buddy

How They Communicate: Two Devices (Smart-Phone, Notebook)

Ultra-Sonic SMS-Buddy broadcasts via loudspeaker
Web-Buddy listens via microphone

Proof of Concept available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How they communicate: Single device (tablet)

Inter-Process-Communication SMS-Buddy & Web-Buddy on same device (Tablet)

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How they communicate: Single device (tablet)

Inter-Process-Communication — SMS-Buddy & Web-Buddy on same device (Tablet)

Implementation available

Channel: SMS-Buddy $\leftrightarrow$ Web-Buddy

How they communicate: Single device (tablet)

Inter-Process-Communication — SMS-Buddy & Web-Buddy on same device (Tablet)

Implementation available

How to Infect the Smart-Phone

Assumption: The browser is already infected

How to Infect the Smart-Phone

Assumption: The browser is already infected

Social-Engineering SMS-Buddy is designed to guard privacy! No additional permissions needed!
Web-Buddy keeps 'nagging'

Cloud-Based After user has logged into cloud (Google-Play-Store / Apple-App-Store / ...)
Web-Buddy directly downloads SMS-Buddy

Implementations and success-stories available (Eurograbber et al)

How to Infect the Smart-Phone

Assumption: The browser is already infected

Social-Engineering SMS-Buddy is designed to guard privacy! No additional permissions needed!
Web-Buddy keeps 'nagging'

Cloud-Based After user has logged into cloud (Google-Play-Store / Apple-App-Store / ...)
Web-Buddy directly downloads SMS-Buddy

Implementations and success-stories available (Eurograbber et al)

How to Infect the Smart-Phone

Assumption: The browser is already infected

Social-Engineering SMS-Buddy is designed to guard privacy! No additional permissions needed!
Web-Buddy keeps 'nagging'

Cloud-Based After user has logged into cloud (Google-Play-Store / Apple-App-Store / ...)
Web-Buddy directly downloads SMS-Buddy

Implementations and success-stories available (Eurograbber et al)

How to Infect the Smart-Phone

Assumption: The browser is already infected

Social-Engineering SMS-Buddy is designed to guard privacy! No additional permissions needed!
Web-Buddy keeps 'nagging'

Cloud-Based After user has logged into cloud (Google-Play-Store / Apple-App-Store / ...)
Web-Buddy directly downloads SMS-Buddy

Implementations and success-stories available (Eurograbber et al)

How to Void this Attack on the Norwegian E-Voting System

One Vote only...

How to Void this Attack on the Norwegian E-Voting System

One Vote only...

Per Voting-Session MinID used to authenticate and authorize voter. Equal to e-banking mTAN.
This is no real solution, as Web-Buddy and SMS-Buddy are designed to break e-banking mTAN $\mapsto$ attacking MinID

! No vote updating ... no successful attack.

How to Void this Attack on the Norwegian E-Voting System

One Vote only...

Per Voting-Session MinID used to authenticate and authorize voter. Equal to e-banking mTAN.
This is no real solution, as Web-Buddy and SMS-Buddy are designed to break e-banking mTAN $\mapsto$ attacking MinID

! No vote updating ... no successful attack.

How to Void this Attack on the Norwegian E-Voting System

Dedicated Hardware Device

- Implementation available: ZTIC(IBM UBS)
  Cronto-Device (Steven Murdoch)
- Success-Story available: E-Banking (UBS)

How to Void this Attack on the Norwegian E-Voting System

Dedicated Hardware Device

SMS-Receiver A must, if MinID alike infrastructure shall remain.
However, Fake GSM-Attack still possible.

Trusted Hardware Token Secure Display, Secure Keyboard
Messages E2E encrypted (over the Internet).

Implementation available: ZTIC(IBM UBS)
Cronto-Device (Steven Murdoch)

Success-Story available: E-Banking (UBS)

How to Void this Attack on the Norwegian E-Voting System

Dedicated Hardware Device

SMS-Receiver A must, if MinID alike infrastructure shall remain.
However, Fake GSM-Attack still possible.

Trusted Hardware Token Secure Display, Secure Keyboard
Messages E2E encrypted (over the Internet).

Implementation available: ZTIC(IBM UBS)
Cronto-Device (Steven Murdoch)

Success-Story available: E-Banking (UBS)

How to Void this Attack on the Norwegian E-Voting System

Dedicated Hardware Device

SMS-Receiver A must, if MinID alike infrastructure shall remain.
However, Fake GSM-Attack still possible.

Trusted Hardware Token Secure Display, Secure Keyboard
Messages E2E encrypted (over the Internet).

Implementation available: ZTIC(IBM UBS)
Cronto-Device (Steven Murdoch)

Success-Story available: E-Banking (UBS)

How to Void this Attack on the Norwegian E-Voting System

Dedicated Hardware Device

SMS-Receiver A must, if MinID alike infrastructure shall remain.
However, Fake GSM-Attack still possible.

Trusted Hardware Token Secure Display, Secure Keyboard
Messages E2E encrypted (over the Internet).

Implementation available: ZTIC(IBM UBS)
Cronto-Device (Steven Murdoch)

Success-Story available: E-Banking (UBS)

Smart-Phones Do Not Provide any Out-of-Band Channel

Stop using smart-phones as trusted device

Your system will be grounded by a *script kiddie*

Smart-Phones Do Not Provide any Out-of-Band Channel

Stop using smart-phones as trusted device

Your system will be grounded by a *script kiddie*