Security and Reliability of Automated Waste Registration in The Netherlands

Dick Visser Thijs Kinkhorst

February 2008

Diftar: differentiated tariffs

- Goal: reduce amount of waste

Diftar: differentiated tariffs

- Goal: reduce amount of waste
- Solution: households pay per amount of waste

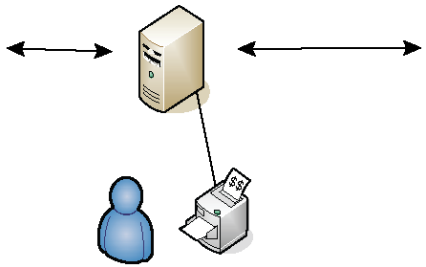
Diftar: differentiated tariffs

- Goal: reduce amount of waste
- Solution: households pay per amount of waste
  - Per kilogram waste
  - Per collected container

Diftar: differentiated tariffs

- Goal: reduce amount of waste
- Solution: households pay per amount of waste
  - Per kilogram waste
  - Per collected container
- Waste Registration!

Waste Registration Overview



- Personal containers
- Shared containers
- Data processing centre

Problem

- Many municipalities have an automated registration system

Problem

- Many municipalities have an automated registration system
- Systems use RFID, GPRS, WIFI...

Problem

- Many municipalities have an automated registration system
- Systems use RFID, GPRS, WIFI...
- Not much known about security and reliability of these systems

Our research questions:

Problem

- Many municipalities have an automated registration system
- Systems use RFID, GPRS, WIFI...
- Not much known about security and reliability of these systems

Our research questions:

- What are the requirements for a good automated waste registration system for domestic waste collection?

Problem

- Many municipalities have an automated registration system
- Systems use RFID, GPRS, WIFI...
- Not much known about security and reliability of these systems

Our research questions:

- What are the requirements for a good automated waste registration system for domestic waste collection?
- Which systems are available and do they meet these requirements?

Method

- No known prior research

Method

- No known prior research
- Theory of a secure system

Method

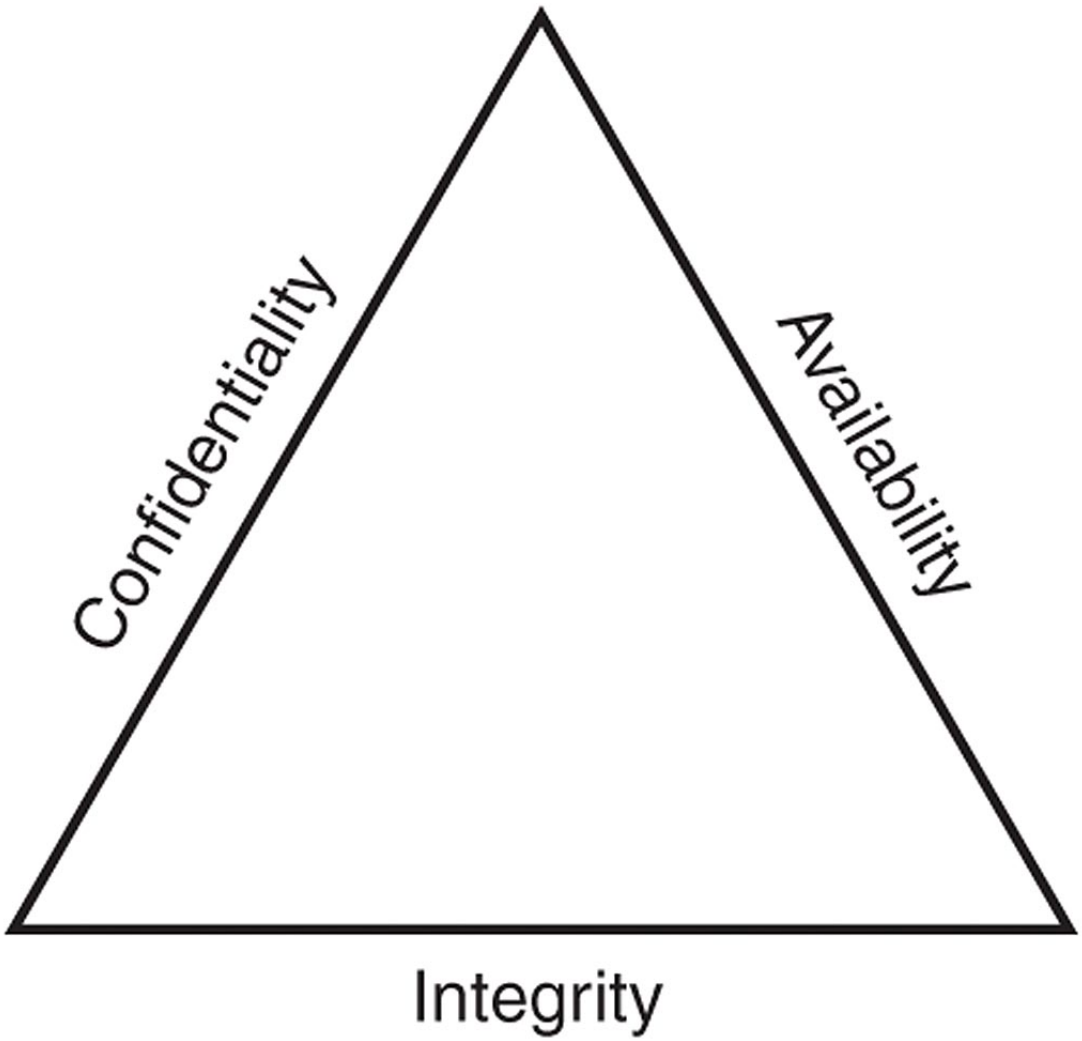
- No known prior research
- Theory of a secure system
- Defining tests

Method

- No known prior research
- Theory of a secure system
- Defining tests
- Field work around the country

Field work

CIA Triad



Implementing CIA

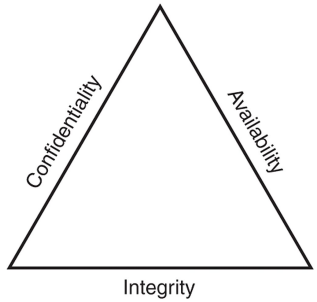
Techniques:

- Authentication

Implementing CIA

Techniques:

- Authentication
- Authorisation



Implementing CIA

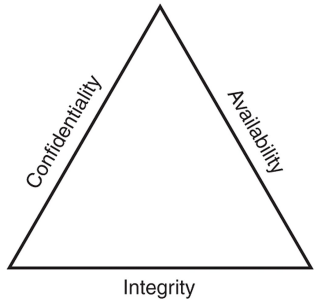
Techniques:

- Authentication
- Authorisation
- Cryptography

Implementing CIA

Techniques:

- Authentication
- Authorisation
- Cryptography
- Logging and monitoring



Implementing CIA

Techniques:

- Authentication
- Authorisation
- Cryptography
- Logging and monitoring
- Physical security

Implementing CIA

Techniques:

- Authentication
- Authorisation
- Cryptography
- Logging and monitoring
- Physical security
- Rate limiting

Implementing CIA

Techniques:

- Authentication
- Authorisation
- Cryptography
- Logging and monitoring
- Physical security
- Rate limiting

This was developed into specific tests, for example: is an RFID container ID clonable?

Personal Containers

	Oz	Kmpn	Mpl	Hgz	Ap
diftar	yes	yes	no	yes	yes
reading requires auth?	?	no	?	?	?
tagless bin emptied?	yes	no	no	no	no
unknown tag emptied?	yes	yes	no	yes	no
can blacklist tags?	yes	yes	yes	yes	yes
is tag crypted?	?	?	?	?	?
logging of events?	yes	yes	yes	yes	yes
rate limiting?	no	no	no	no	yes

Shared Containers

	Hfd	Kmpn	Mpl	Hgz	Ap
diftar?	no	yes	no	yes	yes
auth to read tag?	no	no	no	no	?
unknown tag works?	yes	no	no	no	no
can blacklist tag?	no	yes	yes	yes	yes
crypted tag?	no	yes	yes	yes	yes
rate limiting?	no	no	no	no	no
disrupt power?	yes	no	yes	no/yes	no
disrupt comms?	-	no	no	yes	no
DoS?	no	yes	no	yes	no

Data Processing Centre

	Oz	Kmpn	Mpl	Hgz	Ap
diftar?	yes	yes	no	yes	yes
requires read auth?	yes	yes	yes	yes	yes
shared requires read auth?	yes	yes	yes	yes	yes
can see user data?	no	no	no	no	no
comm user crypted?	-	-	no	no	-
comm shared crypted?	-	?	no	?	?
media crypted?	no	no	no	no	no
requires write auth?	yes	yes	yes	yes	yes
data signed?	no	no	no	no	?
uses logging?	yes	yes	yes	yes	?
can be DoSsed?	no	no	yes	no	no

Highlights

Some highlights:

- We have trivially cloned most shared container passes.

Highlights

Some highlights:

- We have trivially cloned most shared container passes.
- In Hoofddorp the shared containers can be opened by any EM4x02 card.

Highlights

Some highlights:

- We have trivially cloned most shared container passes.
- In Hoofddorp the shared containers can be opened by any EM4x02 card.
- In Kampen the tag type can prevent readout with a password, but this feature is unused.

Highlights

Some highlights:

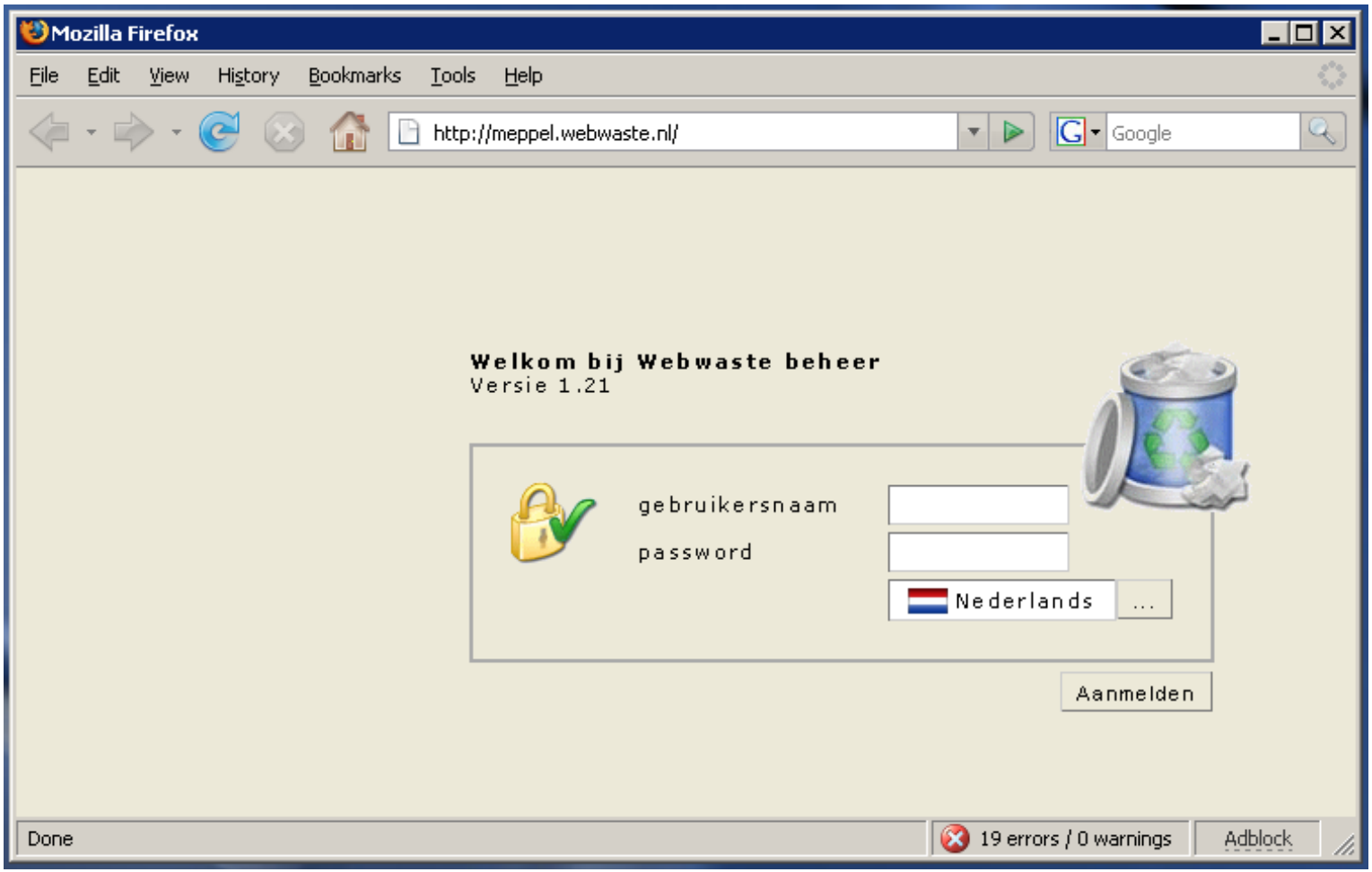
- We have trivially cloned most shared container passes.
- In Hoofddorp the shared containers can be opened by any EM4x02 card.
- In Kampen the tag type can prevent readout with a password, but this feature is unused.
- We couldn't read the tags in Oostzaan because they predate RFID standards – security through obsoleteness?

Highlights

Some highlights:

- We have trivially cloned most shared container passes.
- In Hoofddorp the shared containers can be opened by any EM4x02 card.
- In Kampen the tag type can prevent readout with a password, but this feature is unused.
- We couldn't read the tags in Oostzaan because they predate RFID standards – security through obsoleteness?
- Virtually no encryption is used in any of the communications, e.g. plain HTTP for worldwide backend access.

https?


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://meppel.webwaste.nl/
Google
Welkom bij Webwaste beheer
Versie 1.21
gebruikersnaam
password
Nederlands
...
Aanmelden
Done
19 errors / 0 warnings
Adblock

Conclusion

Our most important observations:

1. RFID tags must be better secured

Conclusion

Our most important observations:

1. RFID tags must be better secured
2. Encryption can enhance security of current systems

Conclusion

Our most important observations:

1. RFID tags must be better secured
2. Encryption can enhance security of current systems
3. Human monitoring and control is important

Conclusion

Our most important observations:

1. RFID tags must be better secured
2. Encryption can enhance security of current systems
3. Human monitoring and control is important
4. Not much security awareness among municipalities

Conclusion

Our most important observations:

1. RFID tags must be better secured
2. Encryption can enhance security of current systems
3. Human monitoring and control is important
4. Not much security awareness among municipalities
5. Many ideas for future research

Questions?

dvisser@os3.nl Dick Visser
tkinkhorst@os3.nl Thijs Kinkhorst