

# Credit Cards: Guessing CVV, Spoofing Payment and Experiences with Fraud Detection Systems

Micha Borrmann

SySS GmbH

May 31, 2012

# About my Point of View

- In most cases I run black box tests against systems and applications
- I'm employed at a company which is offering professional penetration tests exclusively
- My point of view is from the attacking perspective; I do neither know the application source code nor detailed network maps
- All descriptions were found in the course of real professional penetration tests (with strong NDAs): no company names will be published

# First Project

- Long time ago (2007), a popular website ordered a professional penetration test
- However, they represented a minority of analyzed sites, as I found no SQL injection and only few of the typical issues
- But there was a possibility at the website for account verification, which could be used with a valid credit card
- It means, a valid credit card number had to be typed into the website to verify an account

# Using a Credit Card on the Web

- Card Holder Name
- Credit card number
- Expiration date
- Card Security Code (CVV)

## Card security code

The card security code (CSC), sometimes called Card Verification Data (CVD), Card Verification Value (CVV or CVV2), Card Verification Value Code (CVVC), Card Verification Code (CVC or CVC2), Verification Code (V-Code or V Code), or Card Code Verification (CCV) are different terms for security features for credit or debit card transactions, providing increased protection against credit card fraud.


[http://en.wikipedia.org/wiki/Card\\_security\\_code](http://en.wikipedia.org/wiki/Card_security_code)

## Generation of card security codes

CVC1, CVV1, CVC2 and CVV2 values are generated when the card is issued. The values are calculated by encrypting the bank card number (also known as the primary account number or PAN), expiration date and service code with encryption keys (often called Card Verification Key or CVK) known only to the issuing bank, and decimalising the result.

[http://en.wikipedia.org/wiki/Card\\_security\\_code#Generation\\_of\\_card\\_security\\_codes](http://en.wikipedia.org/wiki/Card_security_code#Generation_of_card_security_codes)

# PCI (Payment Card Industry)



		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data <sup>1</sup>	Full Magnetic Stripe Data <sup>2</sup>	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS **applies only** if PANs are stored, processed and/or transmitted.

<sup>1</sup> Sensitive authentication data must not be stored after authorization (even if encrypted).  
<sup>2</sup> Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

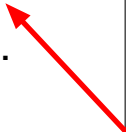
*Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0*  
Copyright 2010 PCI Security Standards Council LLC

October 2010  
Page 7

[https://www.pcisecuritystandards.org/documents/navigating\\_dss\\_v20.pdf](https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf)

# PCI (Payment Card Industry)

**Sensitive authentication data must not be stored after authorization (even if encrypted).**



PCI Security Standards Council

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data <sup>1</sup>	Full Magnetic Stripe Data <sup>2</sup>	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS **applies only** if PANs are stored, processed and/or transmitted.

<sup>1</sup> Sensitive authentication data must not be stored after authorization (even if encrypted).  
Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0  
Copyright 2010 PCI Security Standards Council LLC

October 2010  
Page 7

[https://www.pcisecuritystandards.org/documents/navigating\\_dss\\_v20.pdf](https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf)

# Guessing CVV?

## Client

- Not our business
- There are a lot of fraud detection systems bank-side and your check will fail
- You can check it if you want (yeah!)



# Guessing CVV?

## Client

- Not our business
- There are a lot of fraud detection systems bank-side and your check will fail
- You can check it if you want (yeah!)

## Result (using the **MASTERCARD** of my boss)

- A script which can easily be written runs all possible CVV (000 to 999) for a given credit card number (needs around some hours)

# Guessing CVV?

## Client

- Not our business
- There are a lot of fraud detection systems bank-side and your check will fail
- You can check it if you want (yeah!)

## Result (using the **MASTERCARD** of my boss)

- A script which can easily be written runs all possible CVV (000 to 999) for a given credit card number (needs around some hours)
- 999 error messages were received and 1 success message
- The CVV to a given credit card number was successfully guessed
- Where was the fraud prevention system?

# Brave CVV Guessing

- Only expiration date, credit card number and CVV had to be put in (no card holder name)
- CVV is not possible to know
- What happens if the expiration date is not known either?

# Brave CVV Guessing

- Only expiration date, credit card number and CVV had to be put in (no card holder name)
- CVV is not possible to know
- What happens if the expiration date is not known either?

## Check

36 parallel scripts were run (for the next 36 months as expiration date)

# Brave CVV Guessing

- Only expiration date, credit card number and CVV had to be put in (no card holder name)
- CVV is not possible to know
- What happens if the expiration date is not known either?

## Check

36 parallel scripts were run (for the next 36 months as expiration date)

## Result

The issuing bank called my boss as they detected strange activities on his **MASTERCARD** and the card was revoked immediately.  
Fraud detection systems do exist!

# Expiration Date

- It is not absolutely necessary to guess it because it is not tagged as *secure*
- Written on a lot of receipts, sometimes also with the entire credit card number

# Expiration Date

- It is not absolutely necessary to guess it because it is not tagged as *secure*
- Written on a lot of receipts, sometimes also with the entire credit card number



# Expiration Date

- It is not absolutely necessary to guess it because it is not tagged as *secure*
- Written on a lot of receipts, sometimes also with the entire credit card number





# The Never Ending Story Starts

- In November 2007 a hack into a big German website was in the media
- The website used to sell tickets for self-print out
- The stolen data also included CVV data
- A German TV team asked: What do you know about credit card security?
- The answer was: We can guess the CVV of your credit cards
- The TV guys asked for a demonstration
- Used another website (not my customer's website), as the attack was not against a website but against a credit card number
- I had checked my script one day before the appointment with the TV guys successfully (with the new credit card of my boss)

# First CVV Guessing in the Media

- The website changed their setup and behaviour on that day, when the TV guys were in my office
- More live demonstration than I expected before
- They xeroxed a front side of a VISA and a MASTERCARD and this sheet of paper was given to me

# First CVV Guessing in the Media

- The website changed their setup and behaviour on that day, when the TV guys were in my office
- More live demonstration than I expected before
- They xeroxed a front side of a VISA and a MASTERCARD and this sheet of paper was given to me
- Well, after waiting less than two hours, I got the current CVV values!
- No fraud detection system could be detected

# First CVV Guessing in the Media

- The website changed their setup and behaviour on that day, when the TV guys were in my office
- More live demonstration than I expected before
- They xeroxed a front side of a VISA and a MASTERCARD and this sheet of paper was given to me
- Well, after waiting less than two hours, I got the current CVV values!
- No fraud detection system could be detected

## Statement from Credit Card Industry

VISA: Additional measurements enforce, that stolen credit card data are only minimally useable by criminals

# The Story Goes On

- In May 2011 a journalist of the German magazine DIE ZEIT was investigating about insecurity and he detected the formerly published attack of CVV guessing.
- He asked me, is it still possible?
- Well, let's try!
- I also got two credit card data (credit card number and expiration date): 1 MASTERCARD and 1 VISA (both represent more than 90% of the market in Germany)
- It was not possible for me to simple increase the numbers for the CVV as there was an automatic fraud detection system. Wow!

# Analyzing the Detected Anti Fraud System

- After 3 invalid CVV within 15 minutes a message came back indicating that such a solution seems to be active:  
Payment declined by AFDS (AFDS-HFC)
- AFDS sounds like Automatic Fraud Detection System, isn't?!
- You can wait for 15 minutes after 3 invalid attempts, but it takes too much time
- Need for speed?
- Change the source IP number!
- It can be scripted with open proxies, TOR PROJECT ...

## Result

4 years after the first public demonstration, an automatic fraud detection system simply to be bypassed was detected

# Strange Results

## Result

4 years after the first public demonstration, an automatic fraud detection system simply to be bypassed was detected

## VISA

Two valid useable CVV for the given VISA card were detected. One was printed on the backside the other one is an additional value. Maybe, there is a collision attack within the generating algorithm.



- The article in the magazine DIE ZEIT was read by a radio journalist
- He did not believe that this was a true story (in summer 2011)
- He interviewed me for a radio station and he sent me two credit card numbers and the expiration dates via text message (but of course, no CVV and no cardholders name)
- I used the name “Joe Smith” as cardholder’s name but you can expect the result

- The article in the magazine DIE ZEIT was read by a radio journalist
- He did not believe that this was a true story (in summer 2011)
- He interviewed me for a radio station and he sent me two credit card numbers and the expiration dates via text message (but of course, no CVV and no cardholders name)
- I used the name “Joe Smith” as cardholder’s name but you can expect the result
- I successfully detected the CVV
- This radio interview was also heard by Ukrainian people
- There was another interview and the first non-German notice about it: <http://www.dw.de/dw/article/0,,15295808,00.html>

# Bypassing Credit Card Payment, First Minds

- Do you remember the first little film with the increasing numbers on my laptop screen?
- The numbers on the screen were mostly for the TV guys
- However, during the time the cameraman was behind me, I detected a strange behaviour:
  - an invalid CVV was responded with a redirect to `https://webshop.com/error.php`
  - but the valid CVV was responded with a redirect to `https://webshop.com/success.php`

## Big question

What happens if I go to `https://webshop.com/success.php` directly?

# Using a Payment Provider

- These providers are popular because the web shops do not store credit card data and do not need a PCI certificate
- How does the communication between the web shop and the payment provider work?
  - directly
  - via the browser of the user (this is useful for manipulations, yeah)

# Using a Payment Provider (via the User's Browser)



webshop.com



paymentprovider.com



user

# Using a Payment Provider (via the User's Browser)



webshop.com



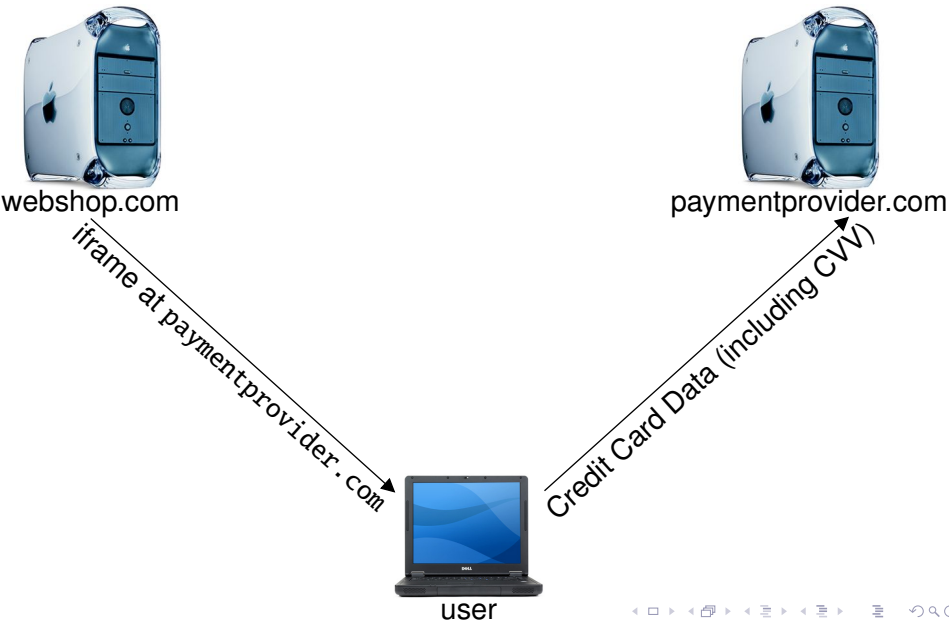
paymentprovider.com

*iframe at paymentprovider.com*

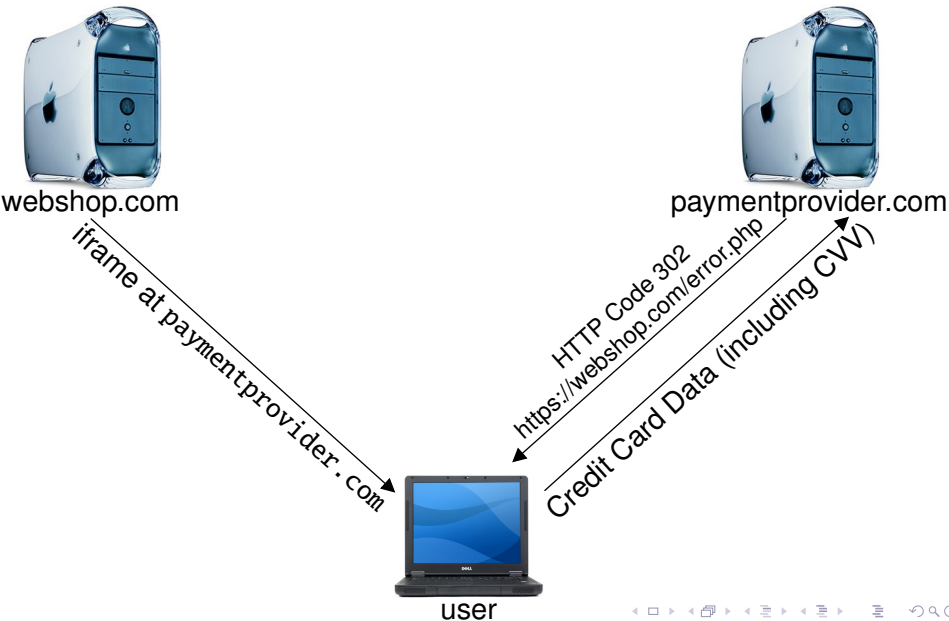


user

# Using a Payment Provider (via the User's Browser)

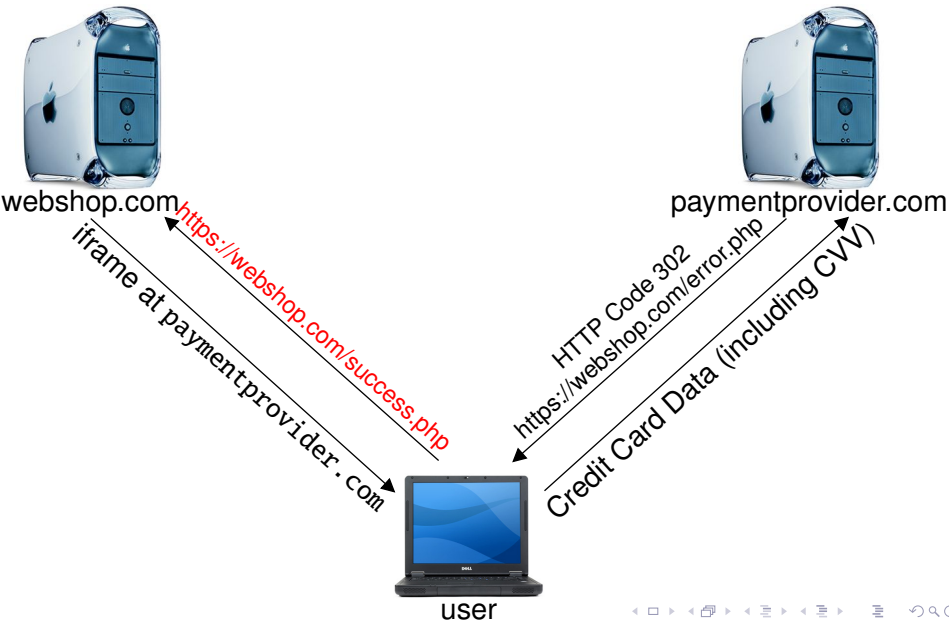


# Using a Payment Provider (via the User's Browser)

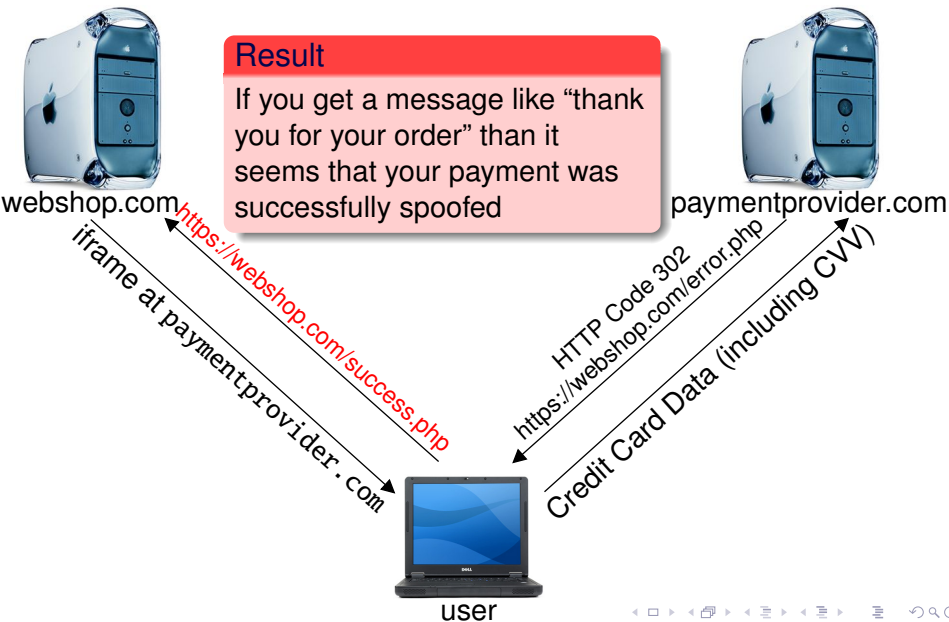




# Using a Payment Provider (via the User's Browser)



# Using a Payment Provider (via the User's Browser)



# Successfully Bypassing Credit Card Payment

- Successfully tested against a friendly shop in January 2008
- On some payment providers, the web shop can enable an optional (!!!) security feature: a hash is calculated over a string which includes a password and the total to be paid and this hash is additionally transferred

# Successfully Bypassing Credit Card Payment

- Successfully tested against a friendly shop in January 2008
- On some payment providers, the web shop can enable an optional (!!!) security feature: a hash is calculated over a string which includes a password and the total to be paid and this hash is additionally transferred
- Has anybody ever heard of a replay attack?
- An article for a German computer magazine (c't) was held back until the trade fair CEBIT 2008
- This kind of attack was described and presented at the CEBIT (March 2008)

# Successfully Bypassing Credit Card Payment

- Successfully tested against a friendly shop in January 2008
- On some payment providers, the web shop can enable an optional (!!!) security feature: a hash is calculated over a string which includes a password and the total to be paid and this hash is additionally transferred
- Has anybody ever heard of a replay attack?
- An article for a German computer magazine (c't) was held back until the trade fair CEBIT 2008
- This kind of attack was described and presented at the CEBIT (March 2008)
- In summer 2008 I was penetration testing a foreign web shop
- It was possible for me to successfully spoof a valid credit card payment for the first time; the box with the product was shipped to Germany

## Other topics with payment providers

- Parameter `fraud_detection=yes`
- Not only related to payment with credit cards
- Thibault Koechlin from NBS SYSTEM talked about NAXSI (<http://code.google.com/p/naxsi/>) this morning
- NBS SYSTEM has written an advisory for a similar attack: <http://www.nbs-system.co.uk/blog-2/security/magento-paypal-vulnerability.html>

## Other topics with payment providers

- Parameter `fraud_detection=yes`
- Not only related to payment with credit cards
- Thibault Koechlin from NBS SYSTEM talked about NAXSI (<http://code.google.com/p/naxsi/>) this morning
- NBS SYSTEM has written an advisory for a similar attack:  
<http://www.nbs-system.co.uk/blog-2/security/magento-paypal-vulnerability.html>

### Attention

This kind of bypassing payment is not only related to credit card payment (see advisory related to PAYPAL) and can not be secured with a web application firewall

# Summary and Hints

- Be careful with credit card receipts
- Check your credit card balance
- Do not expect fraud detection systems for CVV guessing
- Do not trust automatic fraud detection systems for CVV guessing



# Summary and Hints

- Be careful with credit card receipts
- Check your credit card balance
- Do not expect fraud detection systems for CVV guessing
- Do not trust automatic fraud detection systems for CVV guessing
- Do not call CVV a security feature
- Do not expect IT security awareness from your payment provider if you are in charge for a web shop
- Do not trust data from the web shops if you are a payment provider
- Think about the unthought issues if you are a web programmer ☺

- `micha.borrmann@sys.de`
- PGP fingerprint:  
6897 7B33 B359 B8BA 0884 969F FC67 EBA9 1B51 128A