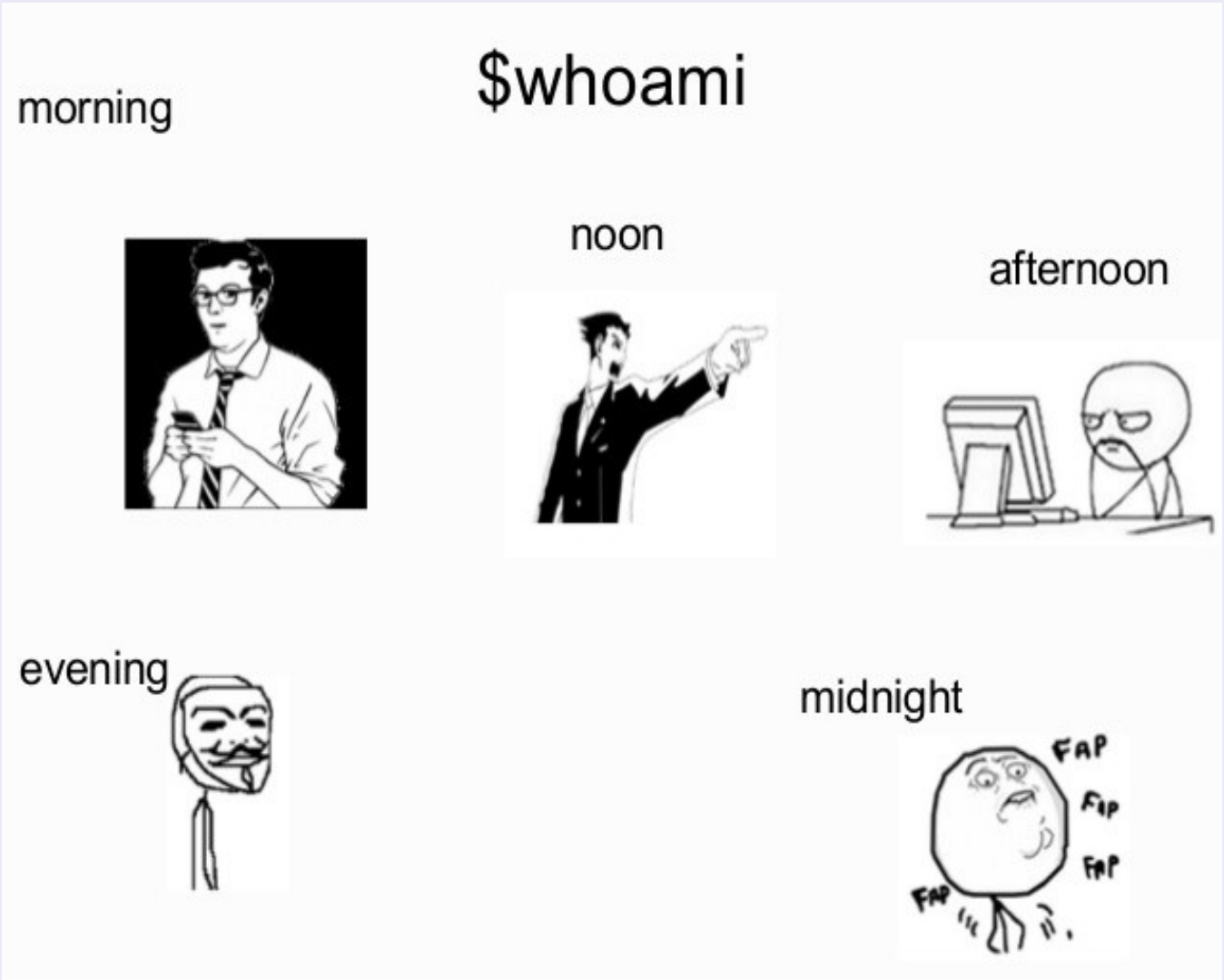
Salami slicing Attacks

gamma95@gmail.com

OWASP
The Open Web Application Security Project

$whoami

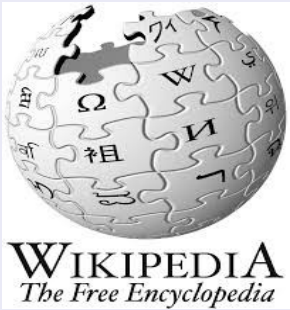

$whoami
morning
noon
afternoon
evening
midnight
FAP
FAP
FAP
FAP

What's salami slicing attacks?

OWASP
The Open Web Application Security Project

Salami slicing refers to a **series of many small actions**, often performed by **clandestine means**, that as an accumulated whole produces a much larger action or result that would be difficult or unlawful to perform all at once. The term is typically used **pejoratively**. Although salami slicing is often used to carry out illegal activities, it is only a **strategy for gaining an advantage** over time by accumulating it in small increments, so it can be used in **perfectly legal ways** as well.

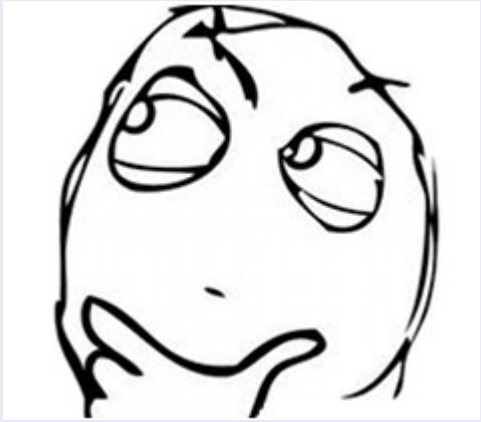
In information security, a salami attack is a **series of minor attacks** that together results in a **larger attack**. Computers are ideally suited to **automating** this type of attack.



WIKIPEDIA
The Free Encyclopedia

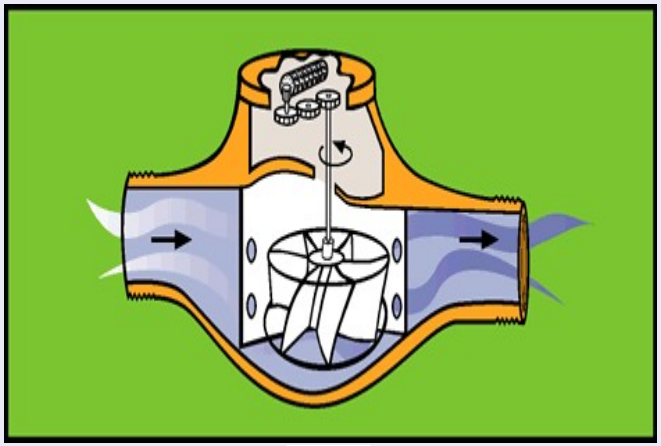
OWASP
The Open Web Application Security Project

Salami slicing
How to cheat water meter



Salami slicing
How to cheat water meter

OWASP
The Open Web Application Security Project



Rounding attacks

OWASP
The Open Web Application Security Project

OWASP
The Open Web Application Security Project

Real life example

- How much do you *really* pay?
- What about:

  2.85$ + 3.20$ = 6.05$?
- How much does the seller win from rounding?

- We are a bit vulnerable…

Rounding attacks

OWASP
The Open Web Application Security Project

y	round down (towards −∞)	round up (towards +∞)	round towards zero	round away from zero	round to nearest
+23.67	+23	+24	+23	+24	+24
+23.50	+23	+24	+23	+24	+24
+23.35	+23	+24	+23	+24	+23
+23.00	+23	+23	+23	+23	+23
0	0	0	0	0	0
−23.00	−23	−23	−23	−23	−23
−23.35	−24	−23	−23	−24	−23
−23.50	−24	−23	−23	−24	−24
−23.67	−24	−23	−23	−24	−24

OWASP
The Open Web Application Security Project

In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60 [redacted] 0210000001360445	EUR	0.67
Current Account	RO66 [redacted] 0210000001360434	RON	49.00

- What happens when you transfer 8.3436 EUR to your account?

  Amount += 8.34 EUR => Bank wins 0.0036 EUR

Rounding attacks
Ex1: Internet banking

OWASP
The Open Web Application Security Project

Rounding vulnerabilities

ZeroNights 2013

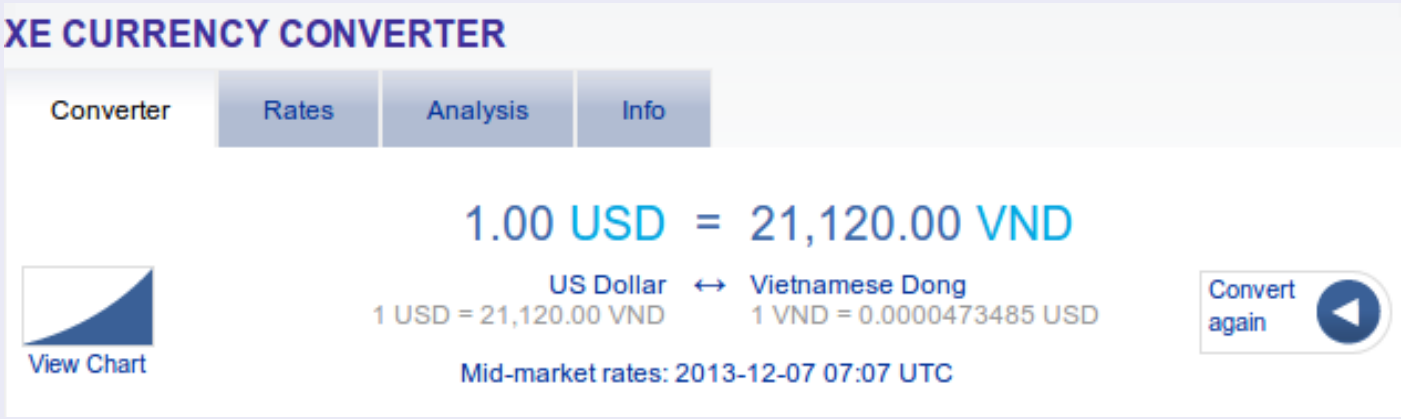
In Internet Banking apps

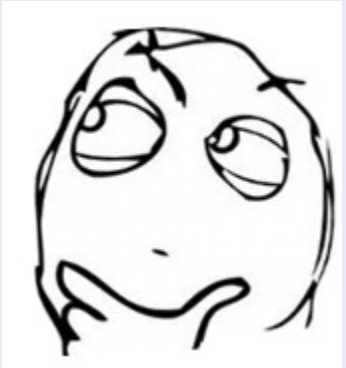
- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60 [redacted] 0210000001360445	EUR	0.67
Current Account	RO66 [redacted] 0210000001360434	RON	49.00

- What happens when you transfer 8.3436 EUR to your account?
  - Amount += 8.34 EUR => Bank wins 0.0036 EUR
- What happens when you transfer 8.3478 EUR to your account?
  - Amount += 8.35 EUR => Bank loses 0.0022 EUR
- Max to win/lose: 0.005 EUR / transaction
  - Rounding is done to the closest value (two decimals)

Rounding attacks
Ex1: Internet banking





Rounding attacks

XE CURRENCY CONVERTER

Converter | Rates | Analysis | Info

105.60 VND = 0.00500000 USD

Vietnamese Dong ↔ US Dollar
1 VND = 0.0000473485 USD 1 USD = 21,120.00 VND

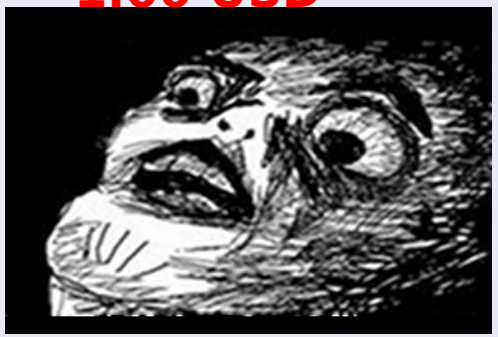
View Chart

Convert again

Mid-market rates: 2013-12-07 06:53 UTC

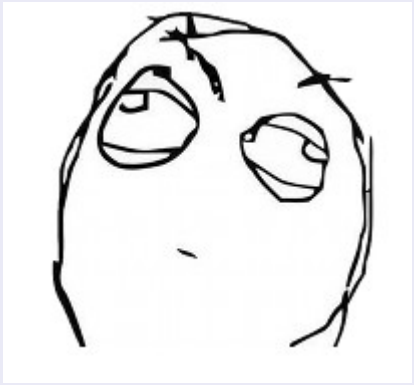
Round(0.005, 2)=0.01 USD = 1 cent

100 * (105.60 VND -> 0.01 USD) => 10,560.00 VND = 1.00 USD



Rounding attacks
Ex2: Petrol station

OWASP
The Open Web Application Security Project



Rounding attacks
Ex2: Petrol station

22,200.00 VNĐ --> 1 litre

200 VNĐ --> 0.009009009...

Round(0.00909, 2)=0.01 litre

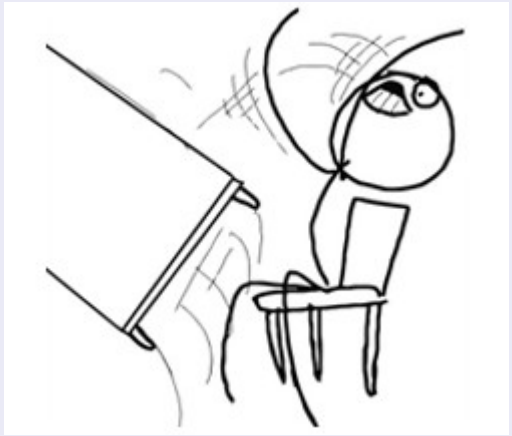
100 * (200 VND -> 0.01 lire) => 20,000.00 VND = 1 litre

Rounding attacks
Ex2: Petrol station

22,200.00 VNĐ --> 1 litre

50,000.00 VNĐ --> 2.2522522522...

Round(2.252252, 2)=2.25 litre

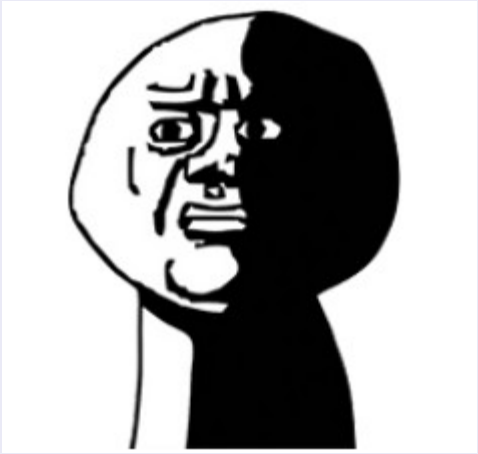


Rounding attacks
Ex2: Petrol station

OWASP
The Open Web Application Security Project

In Viet Nam, Petrol station uses round down/ truncate function. That means you guys always lose :)

y	round down (towards −∞)
+23.67	+23
+23.50	+23
+23.35	+23
+23.00	+23
0	0
−23.00	−23
−23.35	−24
−23.50	−24
−23.67	−24



Deposit account Ex 3

OWASP
The Open Web Application Security Project

Lãi suất dành cho khách hàng cá nhân

Branch: Nam Sài Gòn

Kỳ hạn	VND	EUR	USD
Tiết kiệm			
Không kỳ hạn	1.20 %		0.10 %
7 ngày	1.20 %		
14 ngày	1.20 %		
1 tháng	5.00 %	0.01 %	1.20 %
2 tháng	6.50 %	0.01 %	1.20 %
3 tháng	6.80 %	0.01 %	1.20 %
6 tháng	7.00 %	0.01 %	1.20 %
9 tháng	7.00 %	0.02 %	1.20 %
12 tháng	7.50 %	0.10 %	1.20 %
24 tháng	7.75 %	0.50 %	1.20 %
36 tháng	7.75 %	0.50 %	1.20 %
48 tháng	7.75 %		
60 tháng	7.75 %	0.50 %	1.20 %

You have 100$, you deposit 100$ --> 1.2$/month
You deposit **42** cents --> **0.00504$**/month
Round(0.00504,2) = 0.01$ = 1 cent/month
You should share 100$ to 238 accounts (42 cents per account). After one month, You will get **238 x 0.01**$ = **2.38**$:)

References

1.Salami attack at Asia Commercial Bank

http://www.vnsecurity.net/2008/05/salami-attack-at-asia-commercial-bank/

2. Adrian Furtuna - Practical exploitation of rounding vulnerabilities in internet banking applications

http://2013.zeronights.org/materials

3. Is Your Online Bank Vulnerable To Currency Rounding Attacks

http://blog.acrossecurity.com/2012/01/is-your-online-bank-vulnerable-to.html

4. http://en.wikipedia.org/wiki/Rounding

Questions?