De supermalware Flame: Hoe kan cryptanalyse de volgende Flame-achtige aanval voorkomen?

Marc Stevens
marc.stevens @ cwi.nl

CWI Amsterdam

Digital Signature Schemes Die Hard

Onveilige digital signature schemes sterven moeilijk:

1. Onveilige signature schemes blijven jarenlang overal ondersteund
   - Veel signatures prolifereren buiten de macht van de originele signer
   - Stoppen van ondersteuning leidt tot allerlei problemen
   - Vervalsingen kunnen overal en op iedereen misbruikt worden

2. Onveilige signature schemes nog te lang actief gebruikt
   - Wereldwijd langzame migratie door signers
   - Myriade aan redenen: onwetendheid, laxheid, economische, managements, …
   - Genoeg mogelijkheden voor nieuwe vervalsingen

Cryptanalytische aanvallen op MD5

MD5-based signature schemes:

1991 MD5 ontworpen [R91]
1993 Eerste zwakheden gevonden [dBB93]

2004 Eerste praktische collision aanval op MD5 [WY05]
2005 Colliding X.509 certificaten met verschillende Public Key [LWdW05]

2006 Sterkere praktische collision aanval op MD5 [SLdW07]
2006 Colliding X.509 certificaten met verschillende Common Names [SLdW07]

2008 Verbeterde aanvallen op MD5 [SSA+09]
2008 Vervalst X.509 Certificaat Autoriteit [SSA+09]

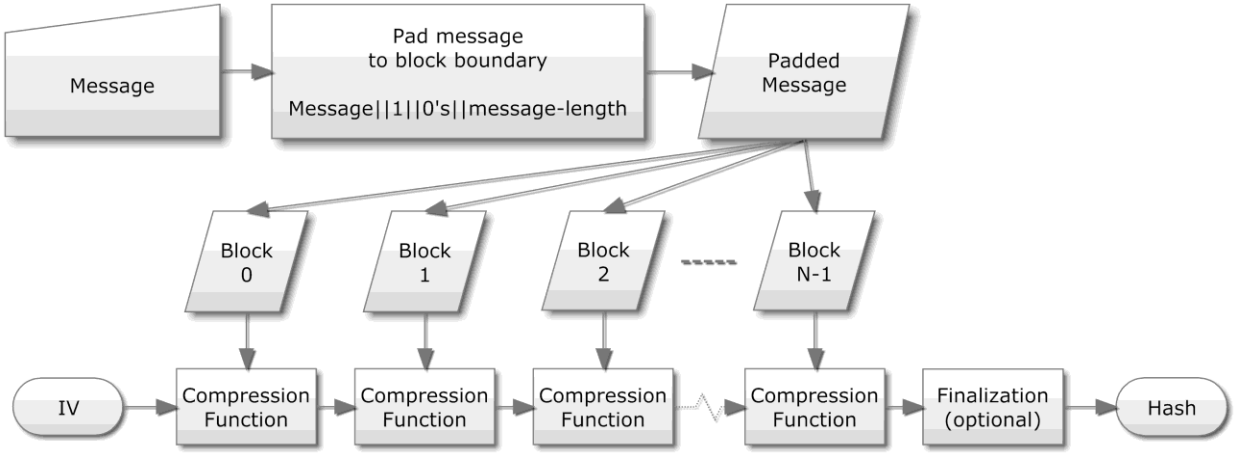
2012 Flame: vervalst `Windows Update' X.509 certificaat [Kas12]

2013-… nog meer vervalste certificaten?
2013 Oplossing: detecteer vervalsingen on-the-go! [Ste13]

Cryptanalytische aanvallen op MD5

MD5-RSA scheme:

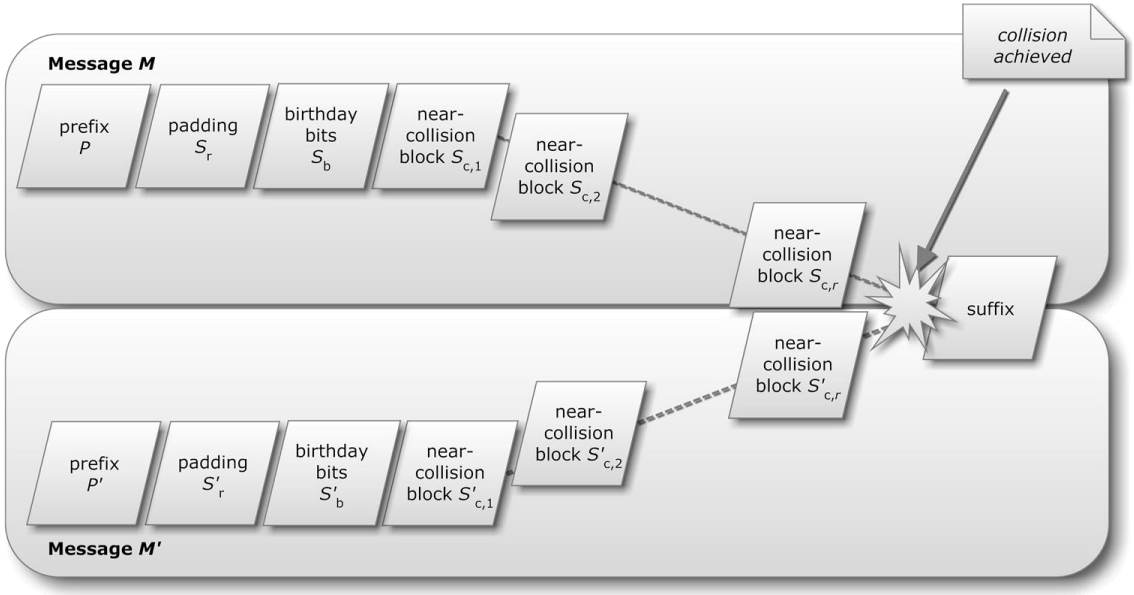
- Hash-then-sign:
  - Hash: bereken ‘digital fingerprint’ van het bericht (128-bit hash)
  - Sign: 1 RSA-operatie op de hash
- MD5 is een cryptografische hash function [R91]
  - Deelt het bericht op in 512-bit blokken
  - Verwerkt deze blokken iteratief m.b.v. de Compression Function



  - Collisions (twee berichten met dezelfde hash) impliceren vervalsingen

Cryptanalytische aanvallen op MD5

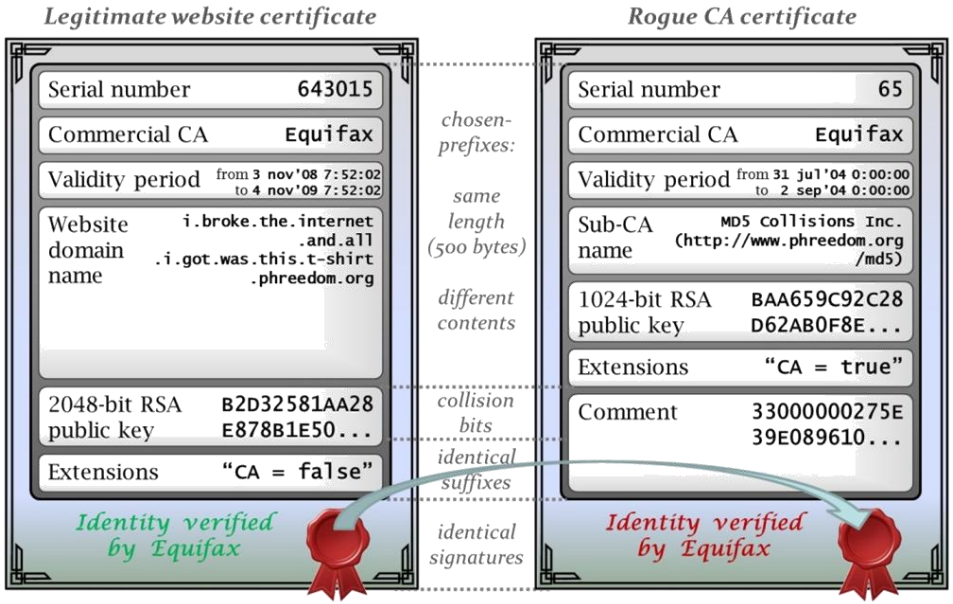
- Praktische **Chosen-Prefix Collision aanval** op MD5 in 2007 [SLdW07]



- Rekenkost: ca. 2^{39} MD5 berekeningen / 1 dag op quadcore-pc
- Krachtige voorbeelden:
  - Colliding X.509 certificates “Marc Stevens” & “Arjen K. Lenstra” [SLdW07]
  - Colliding PDF files: 12 voorspellingen voor de VS presidentsverkiezingen 2008 (onze voorspelling was correct)

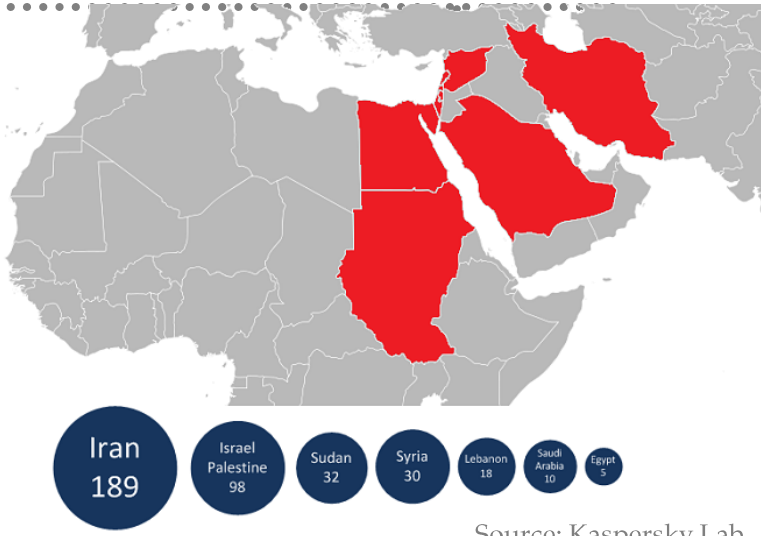
Cryptanalytische aanvallen op MD5

- MD5 aantoonbaar gevaarlijk voor TLS/SSL in 2008 [SSA+09]
- Rogue Certification Authority certificaat ondertekend door Equifax (VeriSign)



- MD5-based signatures niet meer toegestaan voor public CA's sinds 31-12-2010
- MD5-based signatures nog steeds gebruikt door allerlei partijen (bijv. voor signed-executables voor Windows 2000)
- MD5-based signatures nog massaal ondersteund in software

Supermalware Flame



Source: Kaspersky Lab

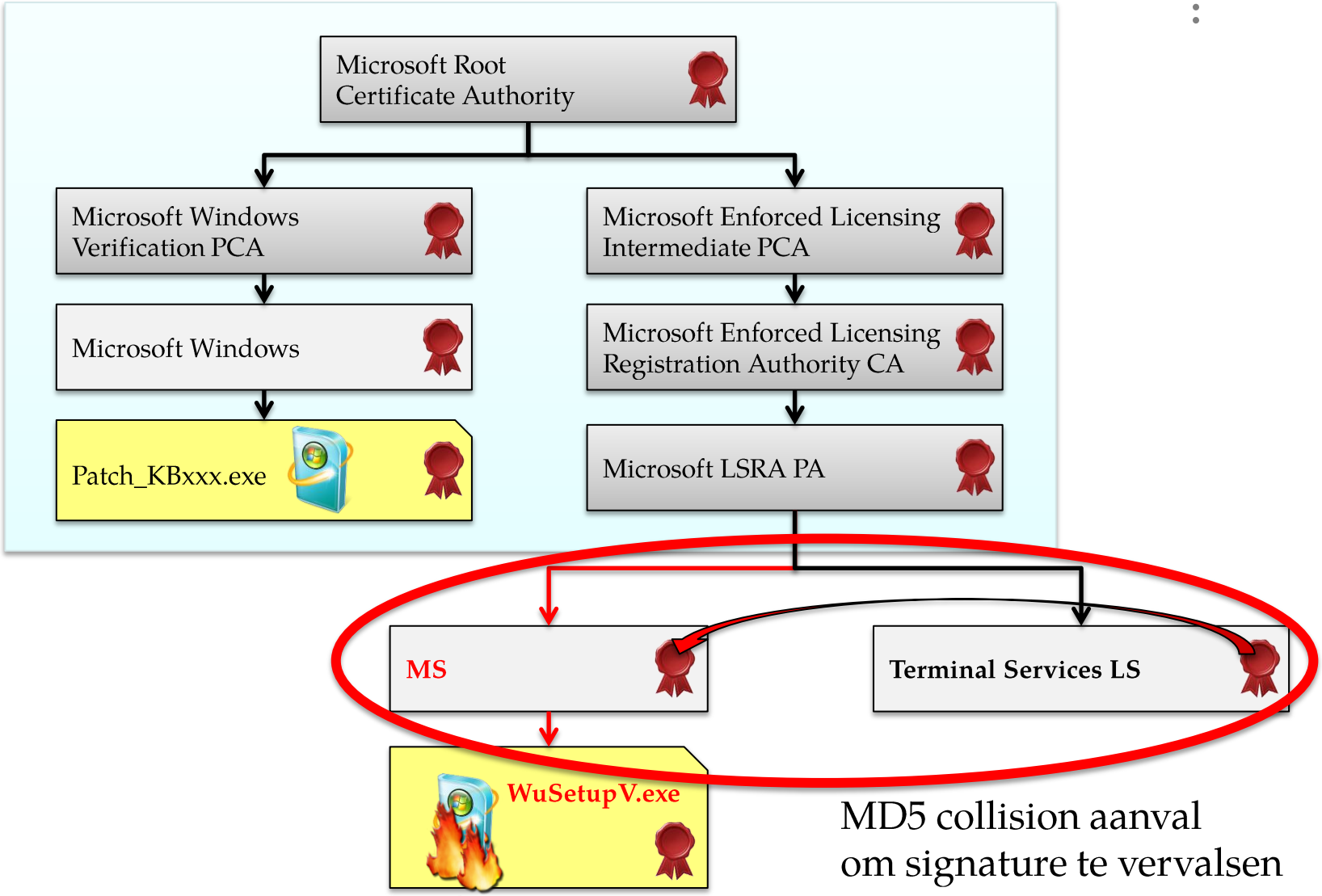
Cf. [Kas12,Sot12]

- Zeer geavanceerde malware
- Gericht op het Midden-Oosten
- Ontdekt in mei 2012
- Actief sinds 2007 of eerder
- Onkarakteristieke eigenschappen
  - Tot 20 modules: elke module zorgvuldig gekozen per infectie
  - Bijna 20MB: bevat Lua VM & libraries voor compression, database, …
  - Niet wijd verspreid & voorkwam ontdekking for ~5 jaar
  - Chirurgische precisie aanvallen: elk doelwit zorgvuldig geselecteerd
  - Verspreidde zichzelf lokaal via het Windows Update platform
  - Eerste cryptanalytische aanval op MD5 in het wild
  - Cryptanalytische aanval gebruikt niet-gepubliceerde methoden [Ste13]

Supermalware Flame

- Lokale man-in-the-middle aanval op Windows Update
  - Dient als lokale proxy server voor **update.microsoft.com** m.b.v. WPAD (Web Proxy Auto-Discovery)
  - Windows Update werkt ook via onveilig HTTP
    - Digital signatures voor veiligheid
    - Behoeft geen aanval op TLS/SSL
  - Verspreid valse 'security update' met correcte signature
  - **Gebruikt illegitieme sub-CA** geldig sinds **Feb 2010**
    ⇒ sub-CA ongeldig daarvoor
    ⇒ deze attack was niet veel eerder gedaan dan Feb 2010

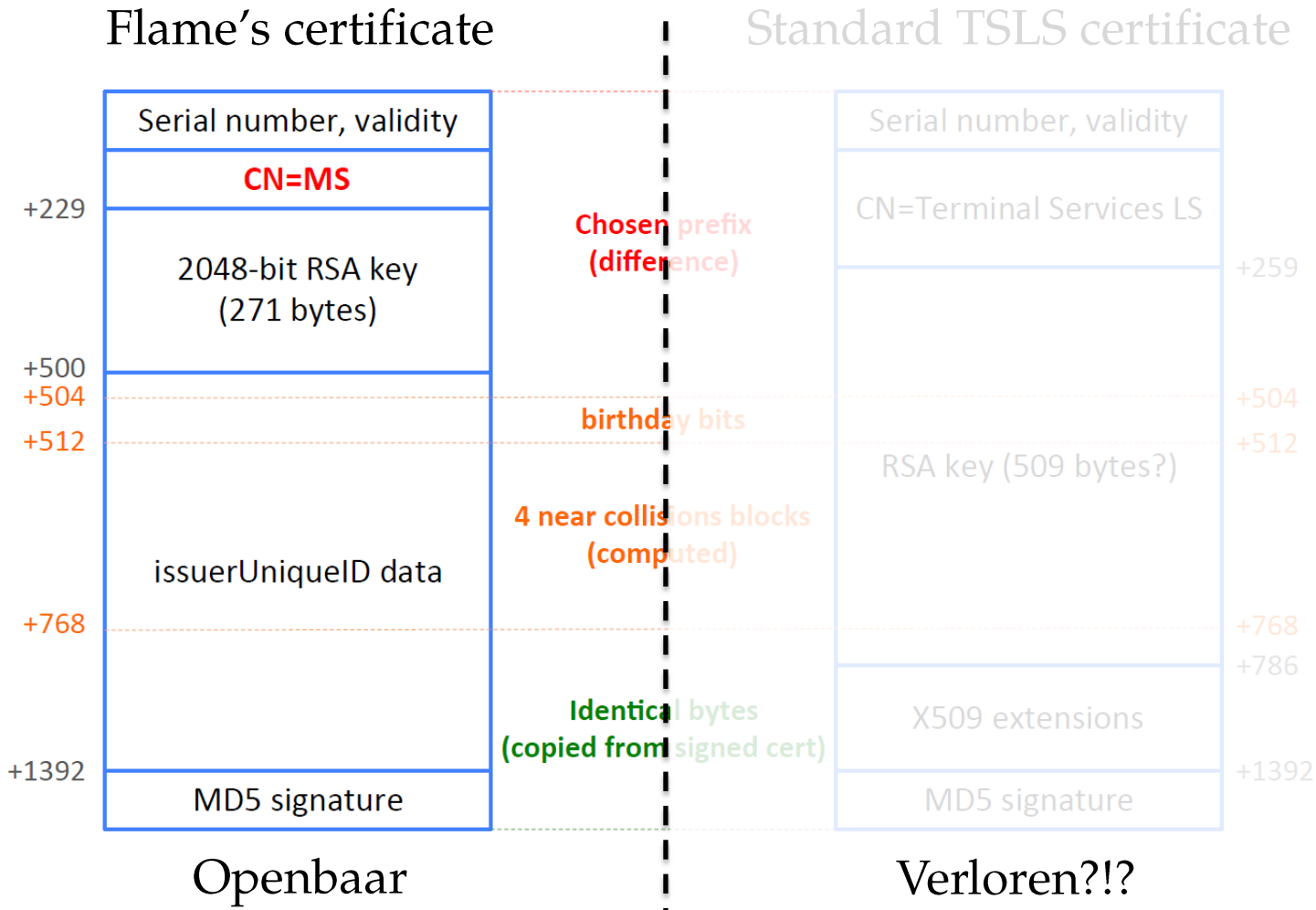
Supermalware Flame



MD5 collision aanval
om signature te vervalsen

Supermalware Flame

Gebruikt Chosen-Prefix Collision aanval

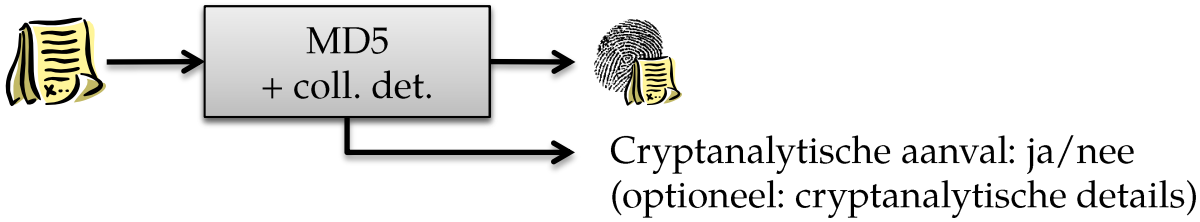


Source: Alex Sotirov

Counter-cryptanalyse

- Nieuwe techniek: *counter-cryptanalyse*
  - Gebruik cryptanalytische technieken *tegen* aanvallen
  - Detecteer en/of reconstrueer aanvallen in de cryptografische laag

- Eerste praktische instantie [Ste12]:
  - Detectie van een cryptanalytische aanval in een bericht
    - Rekentijd kosten: MD5: x 224 / SHA-1: x 15 (veel minder met nieuwe technieken)
  - Werkt voor slechts één bericht van een collision paar, het andere bericht is niet nodig



Counter-cryptanalyse

Detecteren van vervalste signatures

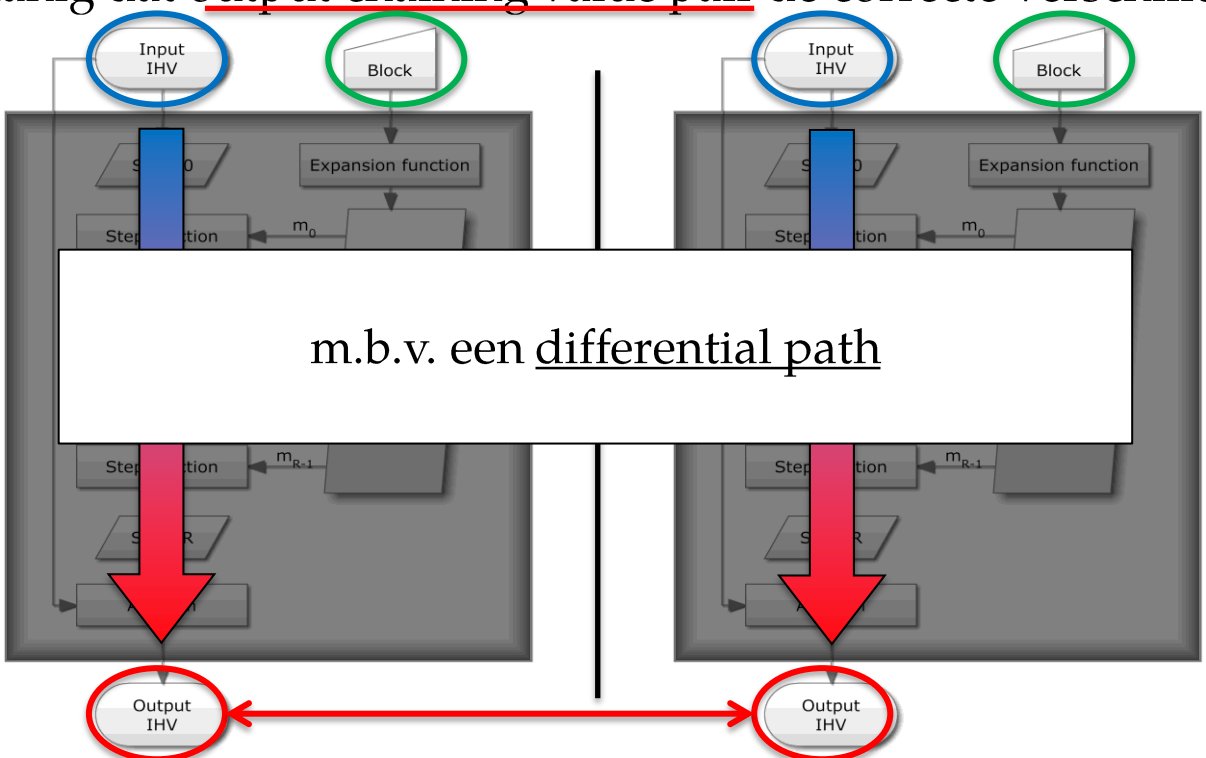
- Online: actieve bescherming
  - Signer: bescherming tegen verdachte requests
  - Verifier: bescherming tegen vervalste signatures
  - Bijv. voor TLS/SSL, OS'en (drivers, executables, updates), etc.

- Offline: forensische analyse
  - Grote voorbeeld: supermalware Flame
  - Bevestiging van Chosen-Prefix Collision aanval in Flame
  - Reconstructie van cryptanalytische details
  - Interessante ontdekking
    - Variant van onze Chosen-Prefix Collision aanval [SSA+09]
    - Gebruik van niet gepubliceerde algoritmen en methoden

Counter-cryptanalyse

Collision aanvallen opgebouwd uit near-collision aanvallen:

- Near-collision aanvallen op compression function:
  - Gegeven input chaining value pair
  - Bereken message block pair
  - Zodanig dat output chaining value pair de correcte verschillen heeft



m.b.v. een differential path

Counter-cryptanalyse

Differential path

- Exacte beschrijving hoe de verschillen door de compression function lopen
- Laatste 40 stappen bepalen voornamelijk de rekentijd

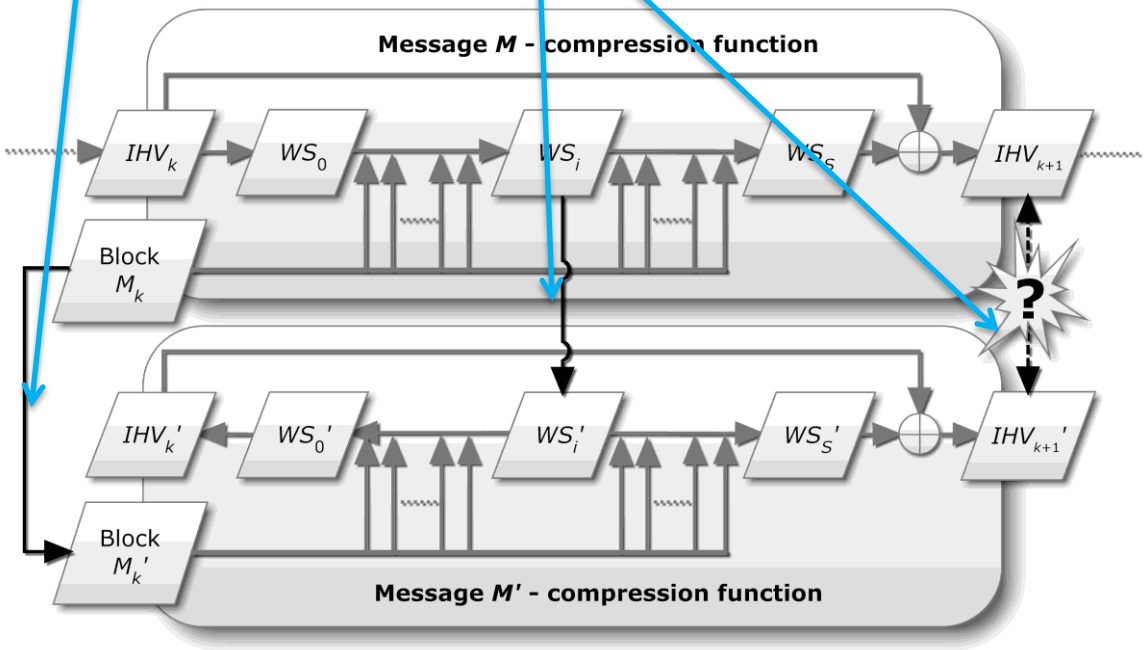
⇒ triviale differential steps *benodigd* voor haalbare aanvallen

⇒ zeer beperkte verzameling van block-differences (MD5: 200+)

t	Bits Q_t: $b_{31} \ldots b_0$				#
−3	10001010	11111100	01010110	11011110	32
−2	11000100	10011010	01100010	-0-10110	32
−1	01111101	01010011	01101110	-0-11110	32
0	11101011	00011111	000010-+	+0-11010	32
1	..0..0..	....11..	0-0-..01	-1-.....	13
2	.1.!0+..	....1+..	-0++..00	--+.....	15
3	.1!.01..	.0..+-..	1-0-....	--+.....	14
4	!-..-1..	.0..+-!.	+1++....	.+.....	13
5	!-00-.00	^-001-.0	101+0000	1+000000	30
6	!+11-011	++11--01	1.+-1111	1.111111	30
7	!1..-...	00.^--.!	-.01....	.1^.^...	15
8	!1..+...	10!-....	-.0-.0..	..+0+..0	15
9	..!.1...	...010..	-..+.0..	.!001^.0	14
10	00.!-010	00.1..10	.00+!+.0	.01+1-1-	25
11	110.-111	1100^011	01110+01	001-000+	31
12	.11^00+1	0010+1+^	00^1111.	1-0-0+-0	30
13	^1+----0	1-0+0+0-	+++++++1	+--+-++0	32
14	--1110-+	+++++0+1	00000010	+--0---.	31
15	1+1+1-1-	011-1+10	0000000-	011-.10.	30
16	01...00+	10111+1.	..+..1..	100-^01.	21
17	.0.^.+.1	.1.^.+..	..-..1.^	.0.0..0.	13
18	1	.+...+..	..1..+..	.1.1..1.	8
19	0....^.+	....0-..	..-.....	.-....-.	8
20	1...0...	.^..1-..	0....^..	.1.....0	9
21	+...1..^	...0-0..	1.^.....	.0....^0	11
22	....+...	...1.^..	+.....	.1.....+	6
23	^.....0	..0-^...	1.....	.+.0....	8
24	....^..1	..10....	0.....0.	...1...^	8
25	.....-	..-+....	.....	.^.-....	5
26	..0.....	...-....	.....0+.	.....	4
27	..1....^	..^1....	.....1+.	...^....	7
28	..+.....	...0....	.....+-.	.....	4
29	..0.....	.....	.....0.	.....	2
30	.-.....	.....	.....^1.	.....	3
31	..!.....	.....	.....	.....	1
32	..!.....	.....	.....	.....	0
33	..!.....	.....	.....	.....	1
34 − 60	.....	.....	.....	.....	0
61	.....	.....	.....	.....	
62	.....	.....	.....	+.....	
63	.....	.....	.....	+.....	
64	.....	.....	.....	+.....	

Counter-cryptanalyse

- Gok <u>block difference</u> & <u>state difference</u> in stap *i*
- Reconstrueer berekening `colliding' block
- Controleer op een collision
- Werk terug voor andere near-collision blocks



Flame's aanval

- Alleen Flame's "MS" sub-CA certificaat openbaar
- Colliding "TSLS" certificaat is niet openbaar (verloren?)
- Chosen-Prefix Collision is zichtbaar vanwege de identieke suffix
  - TSLS X.509 extensies zichtbaar in "MS" IssuerUniqueID-veld

- Eerste toepassing van counter-cryptanalyse
  - Chosen-Prefix Collision aanval niet 100% bevestigd
  - Slechts 1 van de 2 colliding certificaten beschikbaar
  - Mbv proof-of-concept implementatie (uit 2008)
    - Chosen-Prefix Collision gedetecteerd
    - 4 near-collision blocks gereconstreerd
    - Inclusief de 4 differential paths
    - <0.03 seconds
  - Resultaten leidde tot zeer interessante verrassing: aantoonbaar gebruik van ongepubliceerde methoden

Flame's aanval

- Differential path familie
  - Onze Chosen-Prefix Collision aanval [SSA+09]
    - Familie van block-differences $\delta m_{11} = 2^b$
    - Systematische eliminatie door b te variëren
  - Flame: gebaseerd op [WY05]
    - Zelfde block-differences voor alle 4 near-collision aanvallen
      $\delta m_4 = 2^{31}, \qquad \delta m_{11} = \pm 2^{15}, \qquad \delta m_{14} = 2^{31}$
    - Variaties in de laatste 4 stappen van de differential paths
    - Geen systematische eliminatie

Flame's aanval

- Differential path constructie
  - Verschillen in *alle* bit posities van Q6 in *alle* 4 near-collisions:
    - 1st Q6: |++-----+- ---+---- -------+++ ++++++++|
    - 2nd Q6: |+-++++++ +++++---- ------++- --+-----|
    - 3rd Q6: |++-----+- ---+---- -------+++ ++++++++|
    - 4th Q6: |+-++++++ +++++---- ------++- --+-----|
  - Lijkt vereiste voor gebruikte diff.path constructie algoritme
  - Echter komt niet overeen met bekende constructie algoritmes

  - Voorlopige analyse:
    - zeer inefficient in vergelijking met onze methodes:
      runtime <15 seconden en 50+ bitrestricties minder
    - Minstens factor 6000 langzamer vanwege bovenstaande vereiste

Flame's aanval

- Near-collision block vinden (m.b.v. diff.path)
  - Ondergrenzen voor de rekenkosten (in MD5 berekeningen):
    1. $C_1 \geq 2^{37}$
    2. $C_2 \geq 2^{45}$
    3. $C_3 \geq 2^{31.8}$
    4. $C_4 \geq 2^{31.5}$
- Birthday search:
  - Eenvoudige ondergrens op basis van karakteristieken: $C_b \geq 2^{42}$
- Totale rekenkost <u>minstens</u> $2^{45.2}$ MD5 berekeningen
- [SSA+09]: gemiddelde rekenkost van $2^{44.6}$ MD5 berekeningen

- Flame's aanval is dus langzamer
  (maar is wel mogelijk kost effectiever op GPUs etc.)

Voorlopige conclusies

- Real-time vervalste signatures detecteren
  - werkt tegen collision aanvallen op MD5 & SHA-1 [Ste13]
  - Reconstrueert differential paths
  - Beschermt verifiers tegen vervalsingen
    zolang signatures op basis van MD5 & SHA-1 ondersteund blijven

- Flame gebruikte Chosen-Prefix Collision aanval 'in het wild'
  - Maar een geheel nieuwe onbekende variant!
  - Andere differential path familie dan [SSA+09]
  - Nog onbekende birthday search
  - Nog onbekende eliminatie procedure
  - Nog onbekende differential path constructie algoritme
  - Nieuwe aanval is zeker langzamer dan [SSA+09]
  - (maar zou meer kost effectief kunnen zijn op GPUs etc.)

Open vragen

- Wie zat er achter Flame?
  - Duidelijke betrokkenheid van wereldklasse cryptanalysten
  - Ondersteund meest geaccepteerde speculatie van een Natiestaat
- Waarom een nieuwe aanval in februari 2010?
  - Onze implementaties zijn openbaar sinds juni 2009 [Ste12]
  - Vereist veel onderzoek, waarschijnlijk parallel uitgevoerd
  - Niettemin: verraadt cryptanalytische technieken
- Hoe veel langzamer is de nieuwe aanval t.o.v. [SSA+09]?
- Waar wordt MD5 nog steeds actief gebruikt?
- Zal de eerste SHA-1 aanval wel uit de academische wereld komen?
  - Afgelopen jaren zeer weinig onderzoek naar zwakheden in SHA-1
  - Flame 's aanval op MD5 was onafhankelijk en parallel uitgevonden
  - Dus misschien geldt dit ook voor aanvallen op SHA-1…
  - Bovendien hebben grote Natiestaten veel meer resources dan academia

Dank voor uw aandacht

References

[M04] *Practical attacks on Digital Signatures using MD5 Message Digest*, Ondrej Mikle, 2004.

[K04] *MD5 considered to be harmful someday*, Dan Kaminsky, 2004

[Kas12] *Flame*, Kaspersky Lab, http://www.kaspersky.com/flame

[R91] *MD5*, Ron Rivest, 1991, RFC 1321

[Sot12] *Analyzing the MD5 collision in Flame*, Alex Sotirov,
SummerCon conference, New York, June 2012.

[SLdW07] *Chosen-prefix collisions and colliding X.509 certificates for different identities*,
M. Stevens, A.K. Lenstra, B. de Weger,
EUROCRYPT 2007, LNCS Vol. 4515, pp. 1-22, Springer, 2007.

[SSA+09] *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate*,
M. Stevens, A. Sotirov, J. Appelbaum, A.K. Lenstra, D. Molnar, D.A. Osvik, B. de Weger,
CRYPTO 2009, LNCS Vol. 5677, pp. 55-69, Springer, 2009.

[Ste12] *Attacks on Hash Functions and Applications*, Marc Stevens, PhD thesis, Leiden University.
(See also the open-source project at: http://code.google.com/p/hashclash/)

[Ste13] *Counter-cryptanalysis: reconstructing Flame's new variant collision attack*,
M. Stevens, CRYPTO 2013, LNCS Vol. ?, pp. ?-?, Springer, 2013.

[WY04] *How to break MD5 and other hash functions*, X. Wang, H. Yu,
EUROCRYPT 2005, LNCS Vol. 3494, pp. 19-35, Springer, 2005.