Counter-cryptanalysis

analyzing Flame's new collision attack

Marc Stevens
marc.stevens @ cwi.nl

CWI Amsterdam

Overview

- Introduction
  - What if?
  - New paradigm: counter-cryptanalysis
  - Applications
- Counter-cryptanalysis
- Flame: background
- Flame: counter-cryptanalysis
- (Preliminary) conclusions

What if a cryptographic primitive gets broken?

Symmetric encryption schemes

- Only two parties using a communications channel
- Together: negotiate more secure encryption schemes
- New communication secure
- Old communications: no sense in re-encrypting older communications

- Impossible to detect (passive) cryptanalytic attacks at cryptographic level

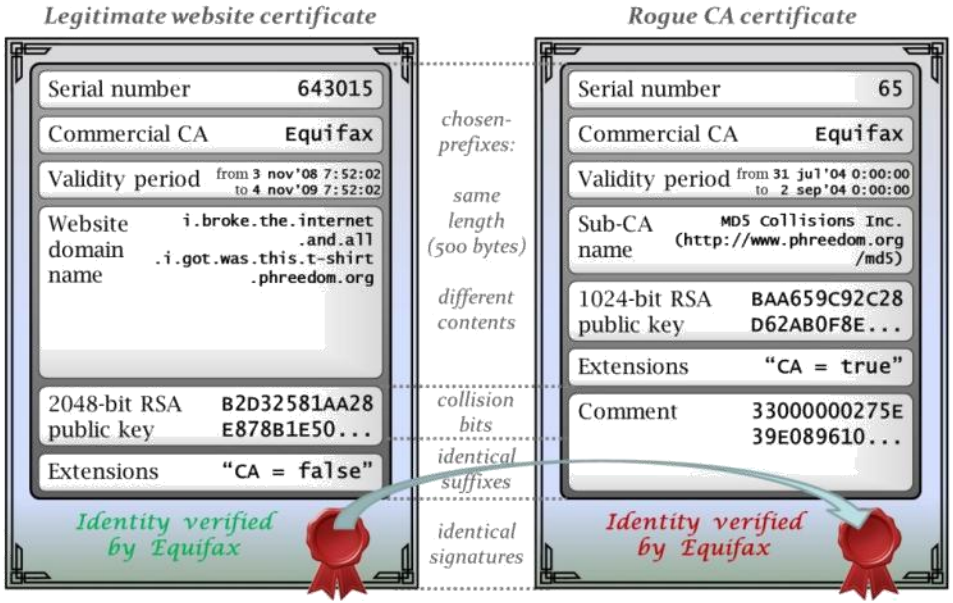
Digital signature schemes

- Up to three parties: requester, signer, verifier
- Signer can switch to more secure scheme
- New signatures secure
- Old signatures: signer may not be able to replace them
- Verifier vulnerable while older weak scheme is still supported
- Is it possible to detect dubious signatures at cryptographic level?

  Answer: YES

Example: MD5-based signatures

- MD5 practically broken since 2004 [WY05]
- Shown to be a realistic threat to TLS/SSL in 2008 [SSA+09]
- MD5-based signatures prohibited to public CA's from 31 Dec 2010

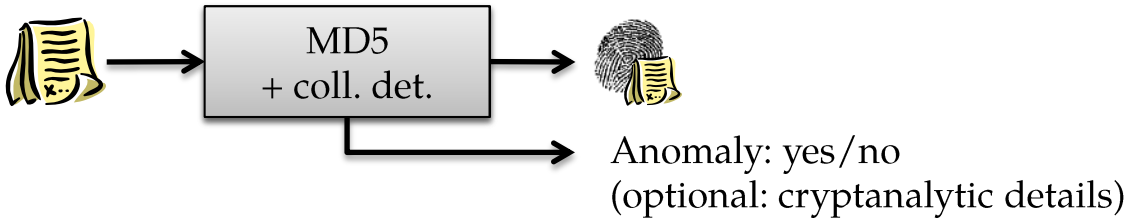


- Yet 'older' MD5-based signatures still supported everywhere
- Abuse still possible for applications not using public CA's

New paradigm: counter-cryptanalysis

- New paradigm: *counter-cryptanalysis*
  - Use cryptanalytic techniques of attacks against them
  - Detect and/or reconstruct cryptanalytic attacks at cryptographic level

- First practical example [Ste12]:
  - Detection whether message is constructed with cryptanalytic attack
    - Computational cost: MD5: x 224
      SHA-1: x 15
  - Works for single given message of collision pair, other sibling not necessary



Anomaly detection for digital signatures

- Online: active protection
  - Signer: protection against malicious signature requests
  - Verifier: protection against forged signatures
  - E.g., for TLS/SSL, OSs (drivers, executables, updates), etc.

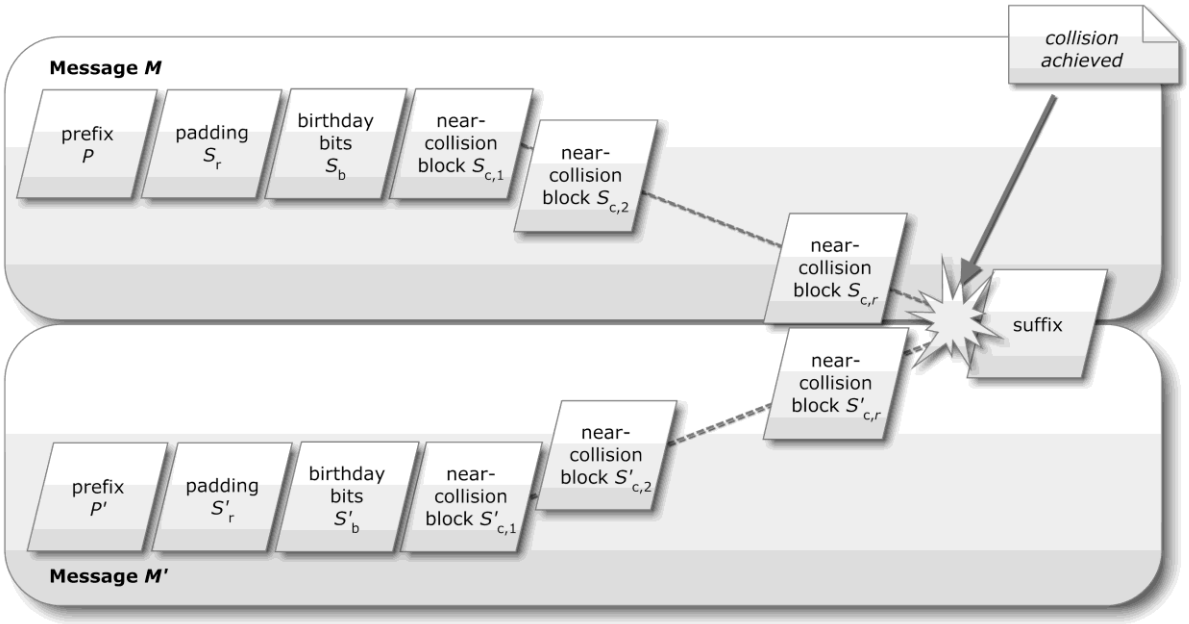
- Offline: forensic analysis
  - Main example: spyware Flame
  - Confirm use of chosen-prefix collision attack
  - Reconstruction of cryptanalytic attack details
  - Interesting discovery:
    - Variant of our chosen-prefix collision attack [SSA+09]
    - But: used algorithms and approaches not in scientific literature

Overview

- Introduction
- Counter-cryptanalysis
  - Cryptanalysis of MD5
  - Cryptanalytic tell-tales
  - Recovering near-collision blocks
- Flame: background
- Flame: counter-cryptanalysis
- (Preliminary) conclusions

Counter-cryptanalysis
Cryptanalysis of MD5

- Collision attacks on MD5 & SHA-1 based on near-collision attacks
- Near-collision attack:
  - Given input chaining value pair
  - Computes message block pair
  - Such that output chaining value pair has 'desired' differences
  - Based on differential path



Counter-cryptanalysis
Cryptanalysis of MD5

Differential path

- Precise description of how differences propagate through compression function
- Last 40 steps determine most of attack's complexity

  ⇒ trivial differential steps *required* for feasible attacks

  ⇒ very limited set of suitable message differences (MD5: 200+)

t	Bits Q_t: $b_{31} \dots b_0$				#
−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	.....	.....	.....	+.....	

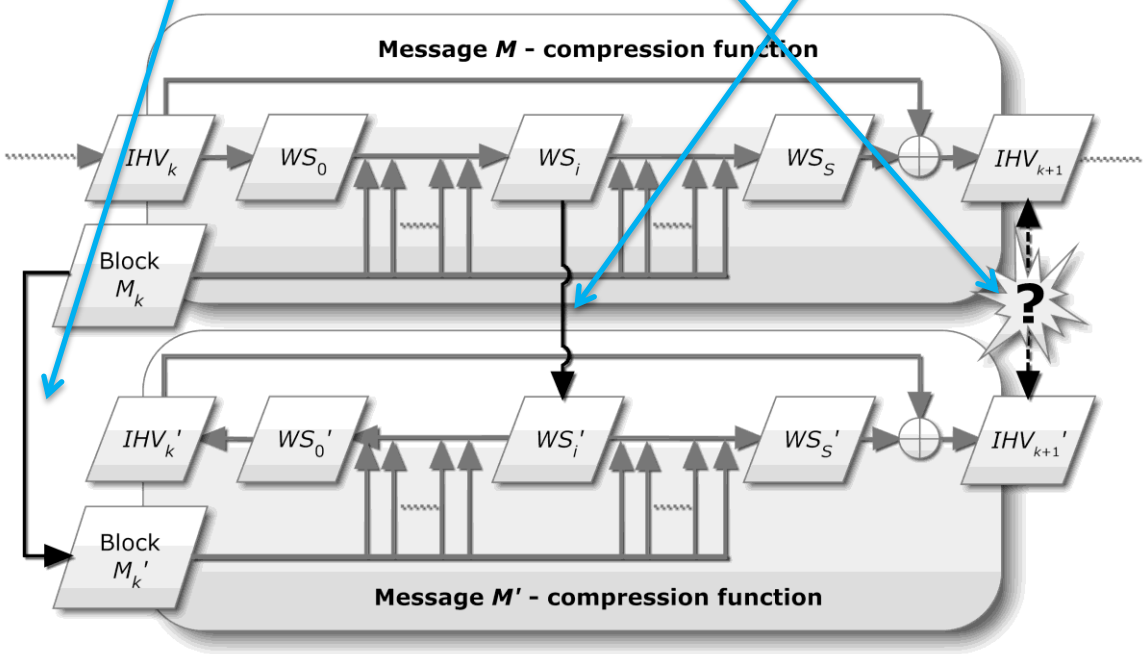
Counter-cryptanalysis

Based on:

- that for given message the entire hash computation is known
- that cryptanalytic collision attacks are highly specialized
  - Very limited set of suitable message differences
  - MD5: 200+ (very few actually used in implemented attacks)
  - SHA-1: 15+ (no actual collisions known yet)
- that cryptanalytic collision attacks 'require' trivial differential steps
  - MD5: known attacks use at least 16 trivial differential steps
    either zero difference state (0,0,0,0) or MSB difference state $(2^{31}, 2^{31}, 2^{31}, 2^{31})$
  - SHA-1: known approaches use at least 6 trivial differential steps
    zero difference state (0,0,0,0,0)

Counter-cryptanalysis
Recovering near-collision blocks

- Guess message block difference & working state difference at step *i*
- Reconstruct computation
- Check whether collision in chaining value is obtained
- For each guess cost is equivalent to compression function call
- Work backwards to recover more near-collision blocks

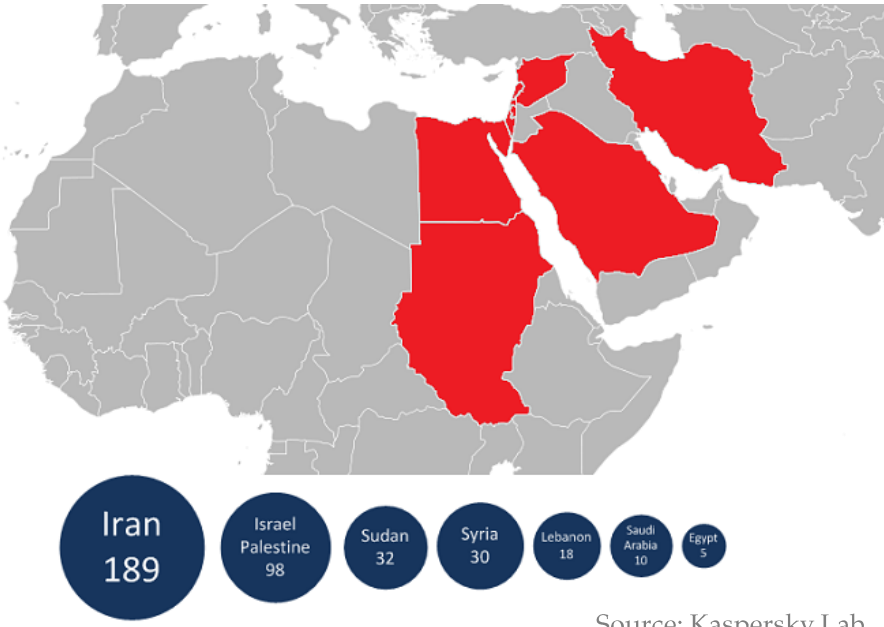


Overview

- Introduction
- Counter-cryptanalysis
- Flame: background
  - Overview of Flame
  - Propagation
  - Certificate hierarchy
  - ‘Free’ signatures
  - Chosen-prefix collision attack
  - Predicting variable certificate fields
- Flame: counter-cryptanalysis
- (Preliminary) conclusions

Flame: background
Overview of Flame

- Malware
- Discovered in May 2012
- Active since 2010 or earlier
- Complex
  - Almost 20MB
  - Up to 20 modular components
  - Advanced info-stealing
  - Advanced propagation
- Surgical-precision attacks
- Initial response: "Flame is lame"
  most aspects have been seen before
- Until discovery in June 2012:
  Flame is the first to use a cryptanalytic attack in the wild…



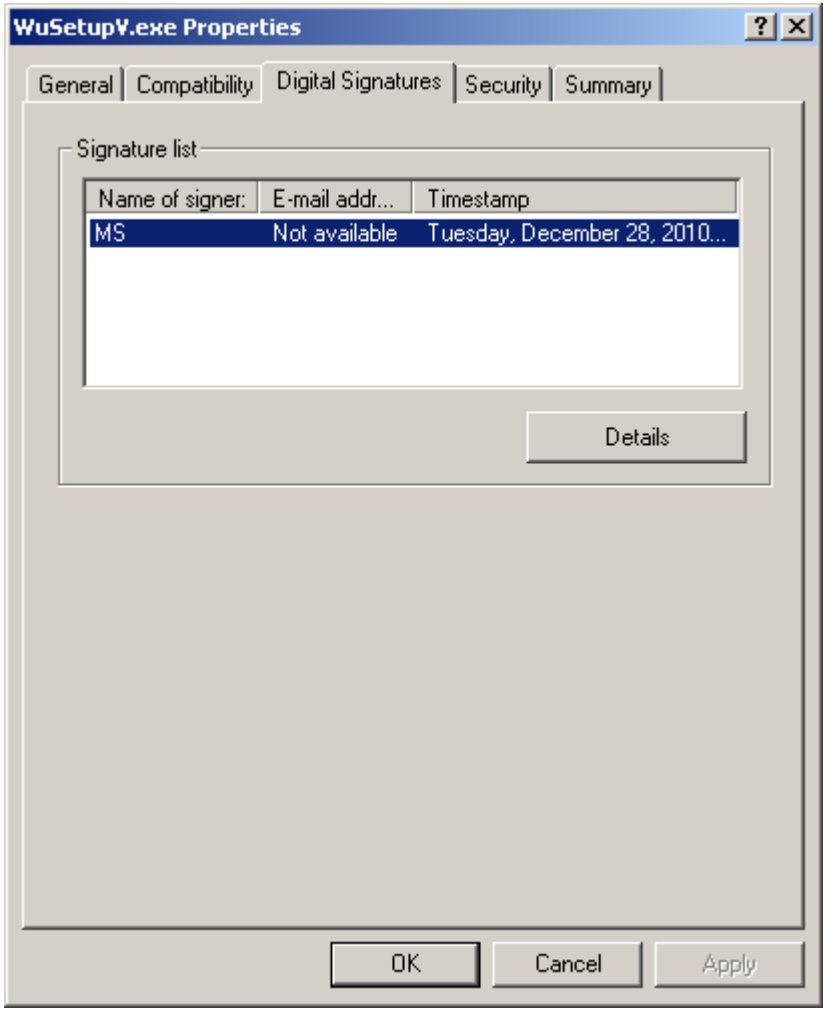
Source: Kaspersky Lab

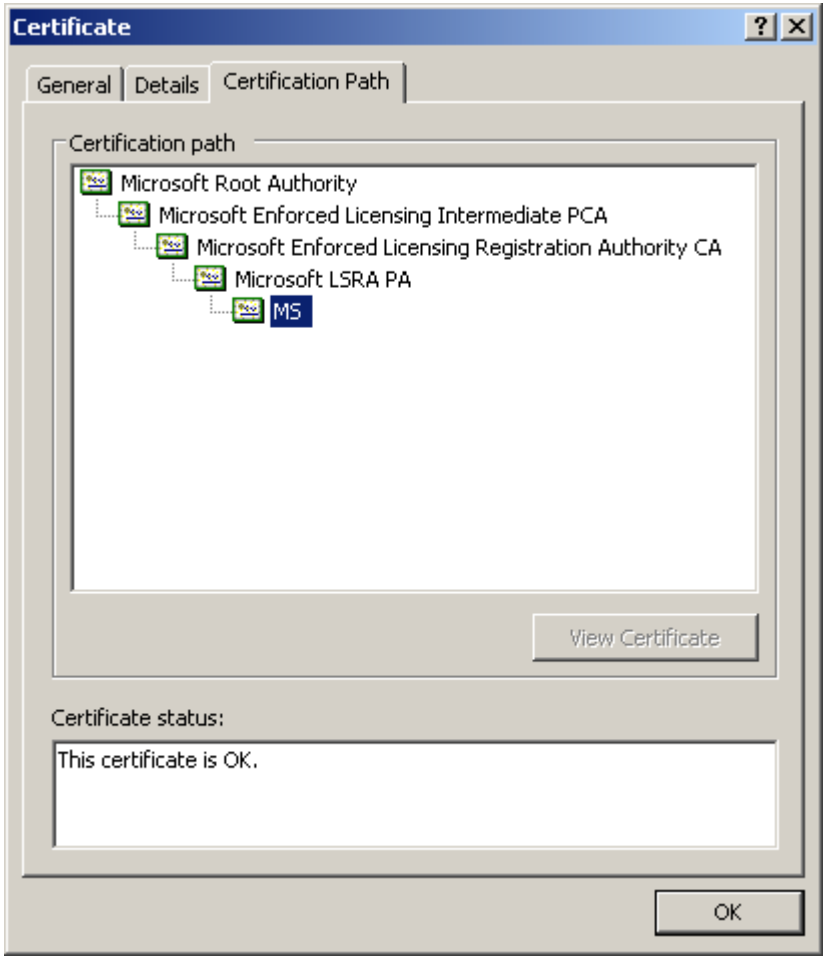
[Kas12,Sot12]

Flame: background
Propagation

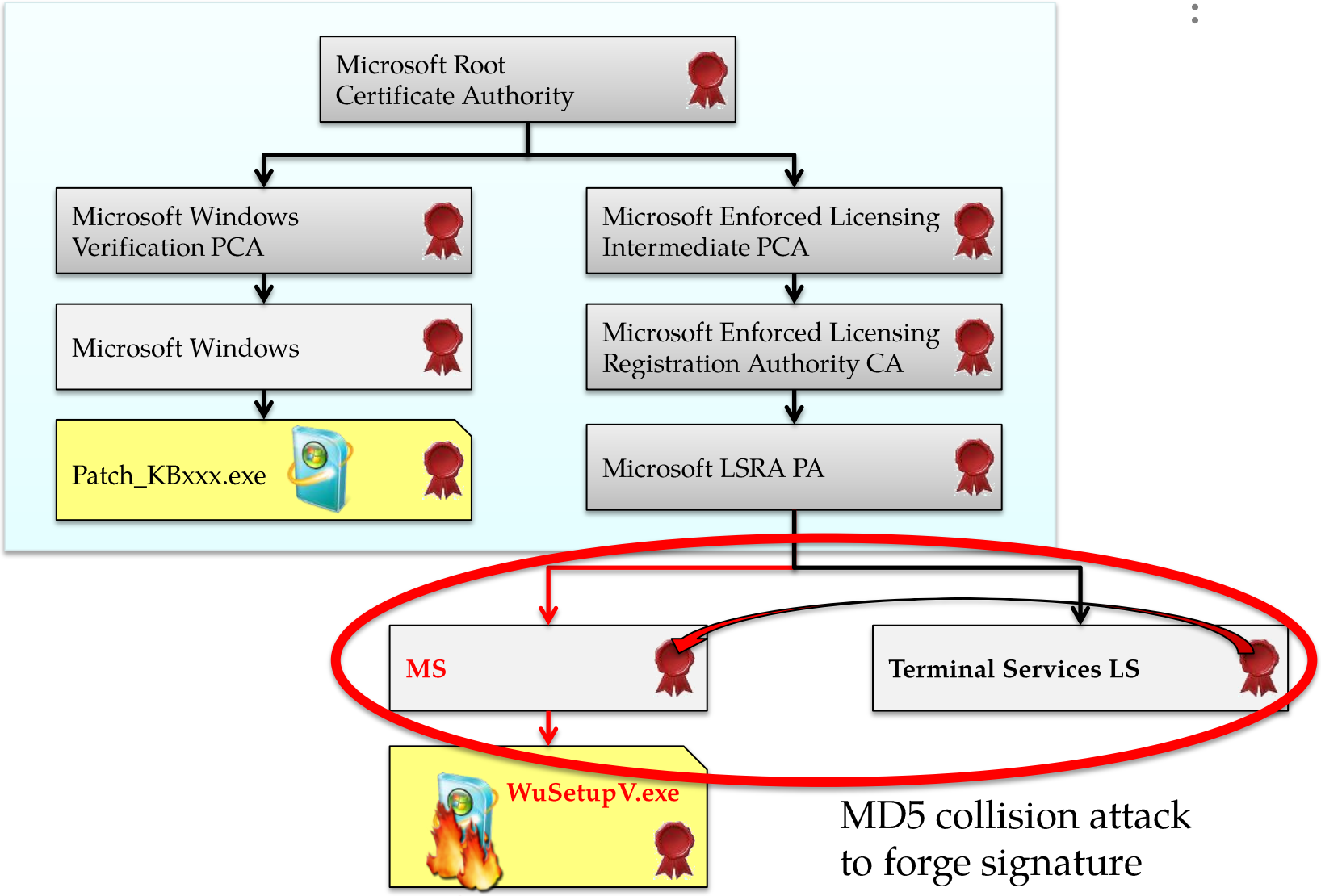
- Man-in-the-middle attack on Windows Update
- Local network attack
  - Registers itself as proxy server for **update.microsoft.com** using WPAD (Web Proxy Auto-Discovery)
  - Windows Update falls back to insecure HTTP
    - depends on digital signatures for security
    - no need to subvert TLS/SSL connection
- Propagation
  - Flame serves fake 'security update' through Windows Update
  - Requires properly-signed 'security update'
  - **Uses illegitimate sub-CA** (valid since Feb 2010)

Flame: background
Certificate hierarchy





Flame: background
Certificate hierarchy



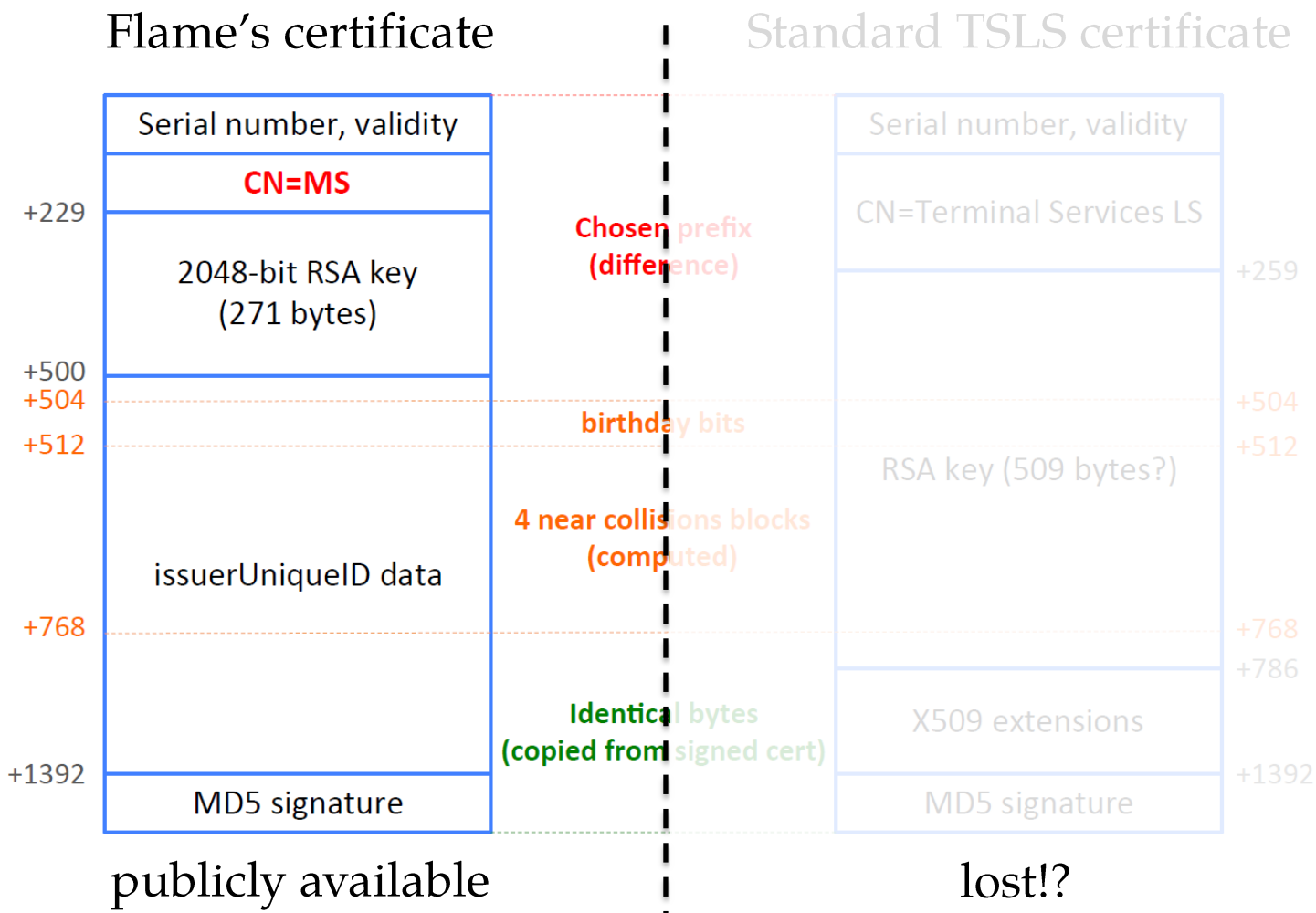
MD5 collision attack to forge signature

Flame: background
‘Free’ Signatures

- License management system for Terminal Services clients
  - Based on X.509 certificate hierarchy under “Microsoft Root CA”
  - “Microsoft LSRA PA” provides signed certificates to servers
  - Fully automated process
  - Fixed fields:
    - CommonName: “Terminal Services LS”
    - X.509 extensions
  - Fields chosen by signing server
    - validity period
    - serial number
    - sufficiently predictable
  - Free to choose fields
    - public key
    - used to hide collision bits

Flame: background
Chosen-prefix collision attack

Uses chosen-prefix collision attack [SLdW07]:



Source: Alex Sotirov

Flame: background
Predicting variable certificate fields

- Predicting variable certificate fields [Sot12]
  - Validity period
    - Fully automated ⇒ accurately predictable
    - 1 second window
    - 'Easy': previously done by hand [SSA+09]
  - Serial number
    - Based on sequential number and current time (ms since boot)
    - Certificate request acts as Query & Increment operation
    - 1 millisecond window
    - Significantly harder ⇒ probably needs many attempts

Overview

- Introduction
- Counter-cryptanalysis
- Flame: background
- Flame: counter-cryptanalysis
  - Analyzing Flame's attack
  - Recovered differential paths
  - First observations
- (Preliminary) conclusions

Flame: counter-cryptanalysis
Analyzing Flame's attack

- Only Flame's "MS" sub-CA certificate public
- The colliding "TSLS" certificate is not public (lost?)
- Use of chosen-prefix collision is exposed through identical suffix
  - TSLS X.509 extensions visible in "MS" IssuerUniqueID-field

- First example for counter-cryptanalysis
  - Assumed chosen-prefix collision attack
  - Only 1 of the 2 colliding certificates available to us
  - Ran proof-of-concept implementation (from 2009)
    - chosen-prefix collision detected
    - 4 near-collision blocks recovered
    - all differential paths reconstructed
    - <0.03 seconds
  - Big surprise looking at differential paths

Flame: counter-cryptanalysis
Recovered differential paths

```
dm4=[!31!] dm11=[!15!] dm14=[!31!]
Q-3:          |........ ........ ........ ..-.....|
Q-2:          |00...... .1.1.01. ...1..+. ..-.10..|
Q-1:          |110-+..1 .1.-.00. .+.+.... ..-110..|
Q0:           |+-100..0 .-0+^++1 .0.+0.11 .110-+..| ok p=1
Q1:           |0+-++..- .-0++-+0 011-0..1 110+++..| ok p=0.49707
Q2:           |+0-0-.00 .-++00+- 0-1-+.1+ 1+-0++^.| ok p=0.166016
Q3:           |+010-000 .-+++0+1 +--.+^1+ -+-+++-.| ok p=1
Q4:           |-00-10+. .11-+-0+ +++11--0 -101-+0.| ok p=1
Q5:           |0-+-++-^ ^0110+1- -110+0-0 -0001+1^| ok p=1
Q6:           |++----+- ---+---- -----+++ ++++++++| ok p=1
Q7:           |111.-111 1101011. 110-1001 +0100.00| ok p=1
Q8:           |00+0.111 10111101 -1101100 .1110011| ok p=0.170898
Q9:           |..0.1... .....-.. 0.10+... 0-....0.| ok p=0.563477
Q10:          |..0^...1 ^....0.. 0^0-1... .1....+.| ok p=0.121094
Q11:          |..0-...1 +....-.. .+-01... .0..^.1.| ok p=0.899414
Q12:          |.1-1..^+ 1....+.. .0+0.... ....+.1.| ok p=0.946289
Q13:          |.0+1..-+ 1....0.. 100....1 ....0...| ok p=0.655273
Q14:          |.-+...1. .....1.. 1.+....1 ....1...| ok p=0.578125
Q15:          |.0+...10 ........ -.0....- ....-...| ok p=0.989258
Q16:          |.1+..... .0...... ..^..... ........| ok p=0.887695
Q17:          |..1..... .1....0. ^......^ ....^...| ok p=1
Q18:          |..0..... .+....1. ........ ........| ok p=0.998047
Q19:          |........ ......-. ........ ........| ok p=0.864258
Q20:          |0....... .^...... ........ ........| ok p=1
Q21:          |0....... ......^. ........ ........| ok p=0.501953
Q22:          |-....... ........ ........ ........| ok p=0.517578
Q23:          |........ ........ ........ ........| ok p=1
Q24:          |^....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q25-32:       |........ ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q33:          |0....... ........ ........ ........| ok p=1
Q34:          |1....... ........ ........ ........| ok p=0.507812
-----------------------------------------------------------------
Q35-59:       |±....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q60:          |+.11110. ........ ........ ........| ok p=1
Q61:          |+.11000. ........ .001.00. ........| ok p=1
Q62:          |-.+----. ........ ...0.... ........| ok p=0.426758
Q63:          |+.?0??+. ........ .--+.+-. ........| ok p=0.855469
Q64:          |+......+ ++++++.. -..-.+-. .....+-.|
```

differential path
near-collision block 1

```
dm4=[!31!] dm11=[!-15!] dm14=[!31!]
Q-3:          |+....... ........ ........ ..-.....|
Q-2:          |-1....+. .1.1.0.. 0....1+. .-+...0.|
Q-1:          |+01.-.+1 .0-+.0^. 011+---1 -++.0.10|
Q0:           |1-0.1.+0 ^-0+1+-1 -1011+-0 001.1^-1| ok p=0.749023
Q1:           |10-.01.+ +++-0+10 --+111+- +--0-+1-| ok p=0.425781
Q2:           |.01.-011 00+-++0+ 0--+.--0 ++10+0+0| ok p=0.492188
Q3:           |..1.-+11 +001++^+ 01-+0110 0+1++0++| ok p=0.833008
Q4:           |..-.1-11 ++1-++-+ -1111--+ ++0+-+-1| ok p=1
Q5:           |^^1^+1-- 10-01011 0+10-1-+ 0-+++000| ok p=0.499023
Q6:           |+-++++++ ++++---- ------+- --+-----| ok p=1
Q7:           |0010-000 01111011 1011-111 10.10010| ok p=1
Q8:           |00000100 1111111+ -1001111 1-010111| ok p=0.672852
Q9:           |...-1... .-.....1 0..1+... .1....^.| ok p=0.495117
Q10:          |...0...0 ^0.....0 1..+0... .0....-.| ok p=0.895508
Q11:          |..0+..^0 -1...^.. ...01... ......1.| ok p=0.807617
Q12:          |.001..-+ 0....-.. ..01.... ......1.| ok p=1
Q13:          |.1-1..0- 1....0.. 1^1....1 ....1...| ok p=1
Q14:          |.-+...10 .....0.. 1-+....1 ....1...| ok p=0.586914
Q15:          |.0+....0 ........ +01....+ ....-...| ok p=0.994141
Q16:          |.^+..... .0...... .^^..... ........| ok p=0.879883
Q17:          |..1..... .1....0. ^......^ ....^...| ok p=1
Q18:          |..0..... .-....1. ........ ........| ok p=0.999023
Q19:          |........ ......-. ........ ........| ok p=0.895508
Q20:          |0....... .^...... ........ ........| ok p=1
Q21:          |0....... ......^. ........ ........| ok p=0.487305
Q22:          |-....... ........ ........ ........| ok p=0.508789
Q23:          |........ ........ ........ ........| ok p=1
Q24:          |^....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q25-32:       |........ ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q33:          |1....... ........ ........ ........| ok p=1
Q34:          |0....... ........ ........ ........| ok p=0.507812
-----------------------------------------------------------------
Q35-58:       |±....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q59:          |+....... ........ ........ ..0.....| ok p=1
Q60:          |+.....0. ........ ...1001. 110.....| ok p=0.506836
Q61:          |-....100 ...0.... ...1..1. 00+.....| ok p=0.749023
Q62:          |+....1-. ........ ...-+++. +--.....| ok p=0.948242
Q63:          |+....++- ...+.... ...???-. ?+-.....| ok p=0.261719
Q64:          |......-- ..+..... .-....-. .+-....+|
```

differential path
near-collision block 2

Flame: counter-cryptanalysis
Recovered differential paths

```
dm4=[!31!] dm11=[!15!] dm14=[!31!]
Q-3:          |........ ........ ........ ........|
Q-2:          |.1.10100 .....11. 10...... ..0.....|
Q-1:          |^0.0101- .1.0^10. 11.0.... ..1.100^|
Q0:           |++1-++++ 1001---. --.1.... .1+.110-| ok p=1
Q1:           |0-111110 1-1+1+-^ --1+.... .01^++-0| ok p=0.96875
Q2:           |10-01110 +++1---+ +10+.... 0-0++++1| ok p=0.374023
Q3:           |-0-01^1+ +0+1--10 0-++^^.0 01+0+00.| ok p=1
Q4:           |--0++-00 0-0+11++ ++-1-+10 -+00+-1.| ok p=1
Q5:           |-1++-0-1 +1-00+1- +0++110- -1--1+^^| ok p=1
Q6:           |++----+- ---+---- -----+++ ++++++++| ok p=1
Q7:           |1000-010 00.1010. 101-0101 +0001.00| ok p=1
Q8:           |11+1.101 01011100 -1000101 .1000011| ok p=0.0566406
Q9:           |..0.1... .....-.. 0.10+... 0-....0.| ok p=0.573242
Q10:          |..0^...1 ^....0.. 0^0-1... .1....+.| ok p=0.120117
Q11:          |..0-...1 +....-.. .+-01... .0..^.1.| ok p=0.889648
Q12:          |.1-1..^+ 1....+.. .0+0.... ....+.1.| ok p=0.948242
Q13:          |.0+1..-+ 1....0.. 100....1 ....0...| ok p=0.631836
Q14:          |.-+...1. .....1.. 1.+....1 ....1...| ok p=0.585938
Q15:          |.0+...10 ........ -.0....- ....-...| ok p=0.993164
Q16:          |.1+..... .0...... ..^..... ........| ok p=0.868164
Q17:          |..1..... .1....0. ^......^ ....^...| ok p=1
Q18:          |..0..... .+....1. ........ ........| ok p=0.999023
Q19:          |........ ......-. ........ ........| ok p=0.868164
Q20:          |0....... .^...... ........ ........| ok p=1
Q21:          |0....... ......^. ........ ........| ok p=0.495117
Q22:          |-....... ........ ........ ........| ok p=0.509766
Q23:          |........ ........ ........ ........| ok p=1
Q24:          |^....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q25-32:       |........ ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q33:          |1....... ........ ........ ........| ok p=1
Q34:          |1....... ........ ........ ........| ok p=0.493164
-----------------------------------------------------------------
Q35-59:       |±....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q60:          |-.....0. ........ ......1. ........| ok p=1
Q61:          |-.0110.0 ........ .1....0. ........| ok p=0.514648
Q62:          |+..01.+. ........ .0....+. ........| ok p=0.492188
Q63:          |+.+---?- ........ .-....+. ........| ok p=0.395508
Q64:          |.+...+.- ....++++ -.....+. ....-...|
```

differential path
near-collision block 3

```
dm4=[!31!] dm11=[!-15!] dm14=[!31!]
Q-3:          |+....... ........ ........ ........|
Q-2:          |+....0+. ........ 000+---. ..000..1|
Q-1:          |+....+-. 11...-++ ++1101+. 10011..1|
Q0:           |001.1+-. 01^.^111 -++----0 11+-+11-| ok p=1
Q1:           |011.0.+. -+-^++1+ ++0000-1 +--0-11+| ok p=0.742188
Q2:           |+--.-0-. -+1+0--0 1+1-1-++ -1-00+--| ok p=0.756836
Q3:           |+--1-^1. .+100--+ 10---1+0 ---0++-1| ok p=1
Q4:           |-010+-1. 10-1-01+ 0-000-1- 0+-10-1-| ok p=1
Q5:           |+00-+00^ 0++-11-0 +++0-111 01-+-100| ok p=1
Q6:           |+-++++++ ++++---- ------+- --+-----| ok p=0.506836
Q7:           |.111-110 01.010.0 0101-110 1101.011| ok p=0.735352
Q8:           |11110110 0101000+ -0101111 0-100111| ok p=0.0507812
Q9:           |...-1... .-.....1 0..1+... .1....^.| ok p=0.522461
Q10:          |...0...0 ^0.....0 1..+0... .0....-.| ok p=0.895508
Q11:          |..0+..^0 -1...^.. ...01... ......1.| ok p=0.822266
Q12:          |.001..-+ 0....-.. .111.... ......1.| ok p=1
Q13:          |.1-1..0- 1....0.. 100....1 ....1...| ok p=1
Q14:          |.-+...10 .....0.. 1-+....1 ....1...| ok p=0.556641
Q15:          |.0+....0 ........ +01....+ ....-...| ok p=0.998047
Q16:          |.^+..... .0...... .^^..... ........| ok p=0.892578
Q17:          |..1..... .1....0. ^......^ ....^...| ok p=1
Q18:          |..0..... .-....1. ........ ........| ok p=0.999023
Q19:          |........ ......-. ........ ........| ok p=0.860352
Q20:          |0....... .^...... ........ ........| ok p=1
Q21:          |0....... ......^. ........ ........| ok p=0.485352
Q22:          |+....... ........ ........ ........| ok p=0.501953
Q23:          |........ ........ ........ ........| ok p=1
Q24:          |^....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q25-32:       |........ ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q33:          |0....... ........ ........ ........| ok p=1
Q34:          |1....... ........ ........ ........| ok p=0.498047
-----------------------------------------------------------------
Q35-59:       |±....... ........ ........ ........| ok p=1
-----------------------------------------------------------------
Q60:          |+.....0. ........ .....00. ........| ok p=1
Q61:          |+.....1. ........ 11....1. ........| ok p=0.525391
Q62:          |-.....-. ........ 10...-+. ........| ok p=0.493164
Q63:          |+.....-. ........ +-...?-. ........| ok p=0.50293
Q64:          |....-++. ........ +-....-. ..-.+..+|
```

differential path
near-collision block 4

Flame: counter-cryptanalysis
First observations

- Differential path family
  - Based on differential path of first MD5 collision attack [WY05]
    - Same message differences for all 4 near-collision attacks

      $\delta m_4 = 2^{31}, \qquad \delta m_{11} = \pm 2^{15}, \qquad \delta m_{14} = 2^{31}$
    - Variations: uses other differences in last 4 steps

WY	([31],	[31,25],	[31,25],	[31,25])
1.	([31],	[31,25],	[31,25,-14,-12,9],	[31,25,-18,-15,-12,9,1])
2.	([31,5],	[31,-25,-9,5],	[31,26,24,20,-9,5],	[-26,24,21,-14,-9,5,0])
3.	([31],	[31,25,9],	[31,25,24,-14,9],	[30,26,-24,20,-17,15,9,-3])
4.	([31],	[31,-25,-9],	[31,-25,14,-9],	[-25,14,-9,-5,3,0])

    - No apparent systematic approach: difficult analysis
  - Different from known chosen-prefix collision attack [SSA+09]
    - Family of message differences: $\delta m_{11} = 2^b$
    - Allows systematic elimination of differences: $([], [b+10], [b+10], [b+10] + r)$
    - Uses birthday search that results in $(0, x, x, y)$ for arbitrary x and y

Flame: counter-cryptanalysis
First observations

- Differential path construction
  - Uses differences in *all* bit positions of Q6 in *all* 4 near-collision attacks:
    - 1st Q6: `|++-----+- ---+---- -------+++ ++++++++|`
    - 2nd Q6: `|+-++++++ +++++---- ------+- --+-----|`
    - 3rd Q6: `|++-----+- ---+---- -------+++ ++++++++|`
    - 4th Q6: `|+-++++++ +++++---- ------+- --+-----|`
  - Not a characteristic of known construction algorithms
    - Known construction algorithms aim at a low number of bit conditions
    - Differences in all bit positions for any Q*i* may occur, but unlikely
  - Seems 'by design'
  - Does not aid in collision search ⇒ must aid in path construction

Overview

- Introduction
- Counter-cryptanalysis
- Flame: background
- Flame: counter-cryptanalysis
- (Preliminary) conclusions

(Preliminary) conclusions

- Real-time signature forgery detection possible
  - works for collision attacks on MD5 & SHA-1 [Ste12]
  - recovers full differential paths
  - protects verifiers against malicious signatures when still supporting MD5 & SHA-1 based signatures

- Flame uses chosen-prefix collision attack 'in the wild'
  - But an entirely new variant!
  - Different differential path family than [SSA+09]
  - Yet unknown birthday search
  - Yet unknown block-wise elimination procedure
  - Yet unknown differential path construction algorithm

Open questions

Open questions

- Who did it?
  - Evidence points to world-class cryptanalysts, not hackers
  - Adds to speculation of nation-state behind Flame

- Why develop a new variant attack?
  - Requires large effort
  - But our attack implementation is public since 2009 (see [Ste12])
  - Also preliminary results indicates new attack not faster than [SSA+09]
  - (but may be more cost effective on massively parallel architectures)
  - Nevertheless: exposes their cryptanalytic knowledge

- How does it compare to our attack [SSA+09]

Thank you for your attention

Questions?

References

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

[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/)

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