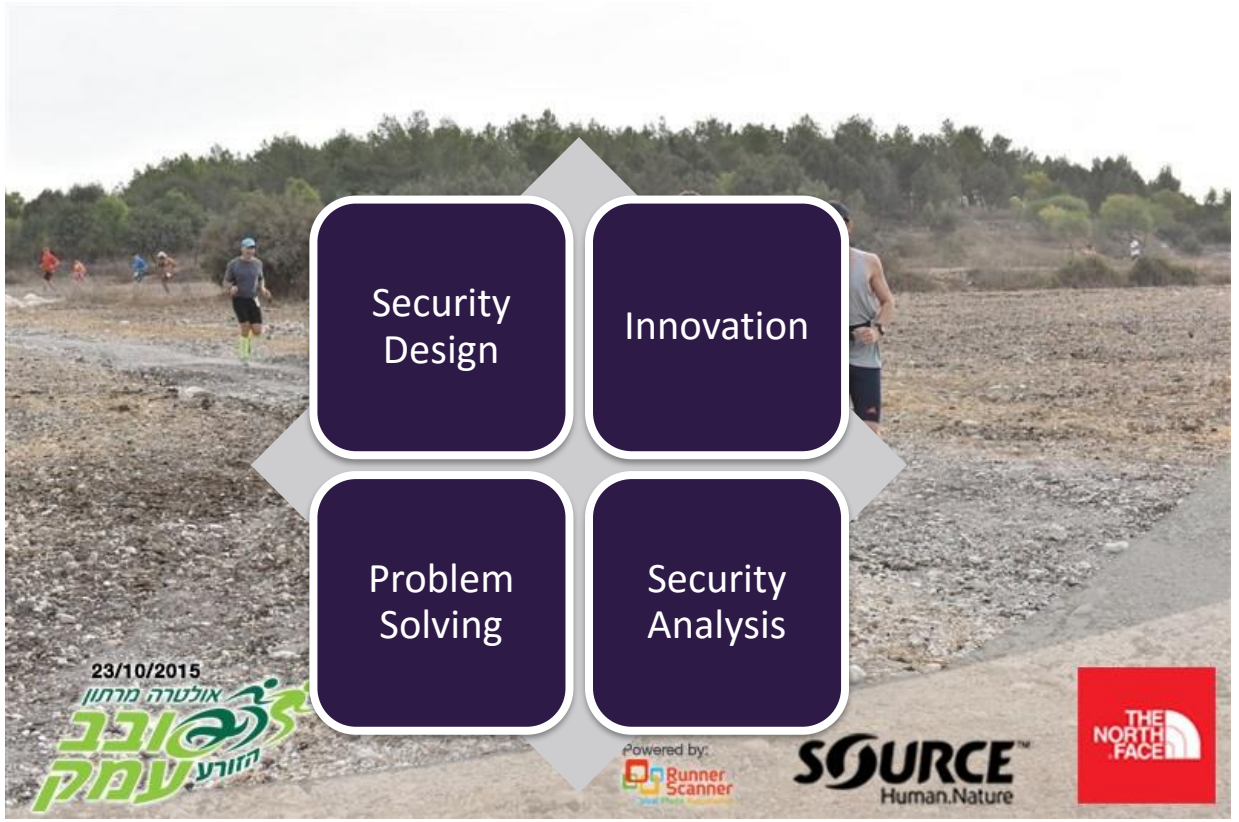
Bar-Mitzva Attack

Breaking SSL with 13-Year Old RC4 Weakness

Itsik Mantin

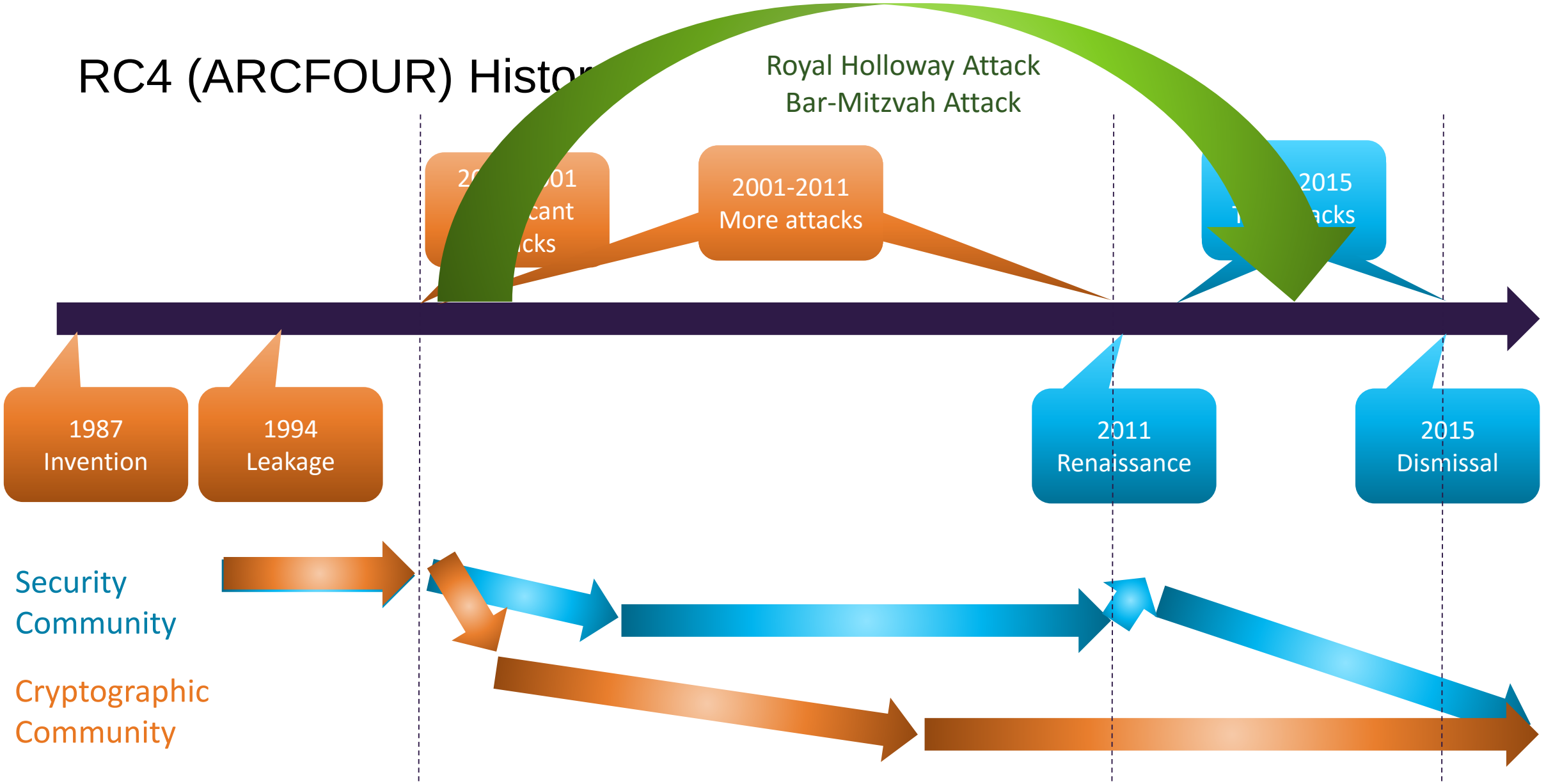
About Myself

- Ultra-Marathoner
- Director of Security Research at Imperva
- Application Defense Center (ADC)
- 16 years in various security domains
  - DRM systems, Web applications, Automotive systems, Insider threats, Cryptography and Cryptanalysis
- M. Sc. in Applied Math and Computer Science from the Weizmann institute
  - Cryptanalysis research with professor Adi Shamir
- https://www.linkedin.com/in/imantin



IMPERVA®

RC4 (ARCFOUR) Histor



IMPERVA®

RC4 Usage in TLS

- 150K sites, SSL-Pulse
- March 9, 2015

Not supported

37,840 25.5%

+ 2.3 %

Some RC4 suites enabled

75,986 51.2%

- 1.3 %

Used with modern browsers

34,660 23.3%

- 1.0 %

IMPERVA®

RC4 Usage in TLS

- 150K sites, SSL-Pulse
- July 15, 2015

Not supported
58,067 39.9%
+ 2.2 %

Some RC4 suites enabled
63,990 43.9%
- 1.1 %

Used with modern browsers
23,574 16.2%
- 1.1 %

IMPERVA®

RC4 Usage in TLS

- 150K sites, SSL-Pulse
- Dec 23, 2015

Not supported

72,669 51.2%

+ 1.8 %

Some RC4 suites enabled

54,262 38.2%

- 1.2 %

Used with modern browsers

14,959 10.5%

- 0.7 %

IMPERVA®

The Future of RC4

App Dev ▪ Cloud ▪ Data Center ▪ Mobile ▪ Open Source ▪ Security ▪ Deep Dives ▪ Reviews ▪ Resources/White Papers

InfoWorld Most Popular:

Home > Security

INFOWORLD TECH WATCH

By Fahmida Y. Rashid | Follow

About

Informed news analysis every weekday

Google, Mozilla, Microsoft browsers will dump RC4 encryption

MORE LIKE THIS

on IDG Answers

If I buy a Chromebook and can't get to grips with OS can I convert to windows?

IMPERVA®

Why Bar Mitzvah?

- The Invariance Weakness
  - ***"Weaknesses in the key scheduling algorithm of RC4"***. Fluhrer, Mantin, and Shamir (Selected Areas of Cryptography, 2001)
  - ***"Analysis of the stream cipher RC4"***. Mantin (My M. Sc. Thesis, 2001)

IMPERVA®

1

On TLS

IMPERVA®

TLS Objectives

Mutual Authentication

- Usually only Server authentication is used

Data Protection

- Data Integrity
- Data Confidentiality

IMPERVA®

Passive Attacker (Sniffing)

alice.wonder@gmail.com
Alice123!

IMPERVA®

Man-in-the-Middle Attacker (MitM)

alice.wonder@gmail.com
Alice123!

alice.wonder@gmail.com
Alice123!

IMPERVA®

TLS Security

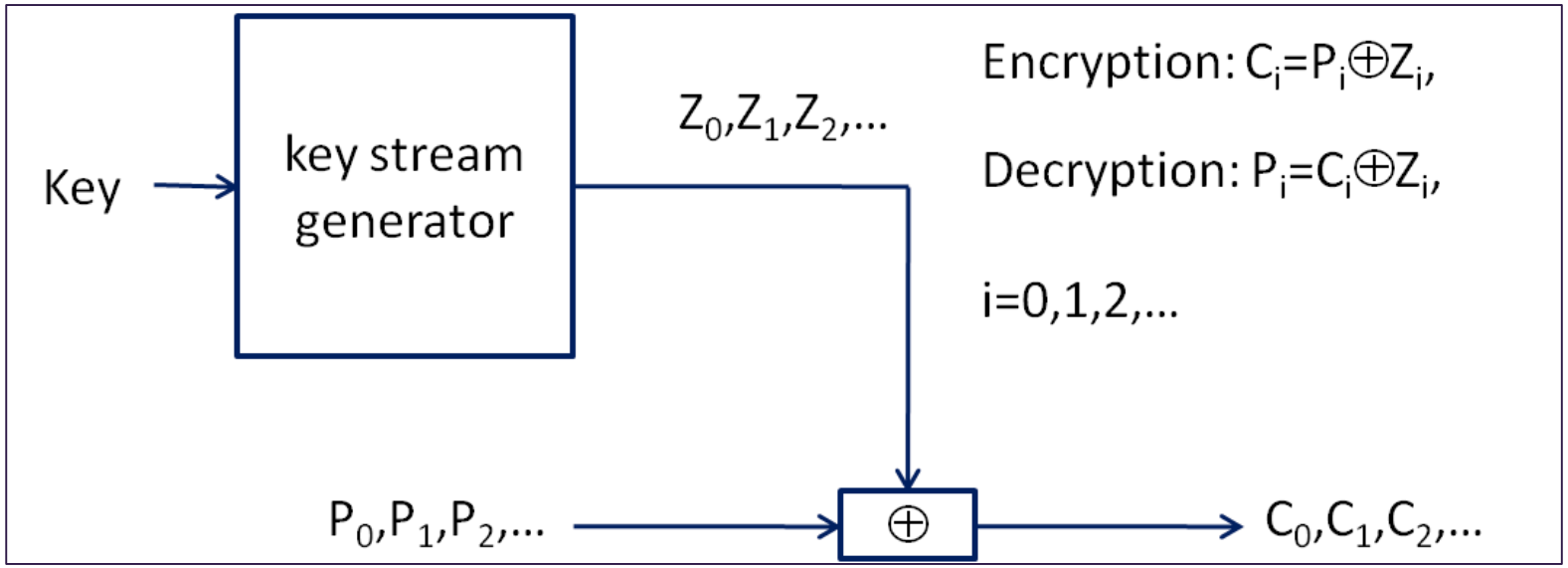
Cipher attacks	• BEAST (2011) • Royal Holloway (2013)
Compression attacks	• CRIME (2012) • TIME (2013) • BREACH (2013)
Downgrade attacks	• False Start (2012) • POODLE (2014) • FREAK (2014)
Padding Oracle attacks	• Lucky13 (2013)
Implementation attacks	• Heartbleed (2014)

IMPERVA®

2

On RC4

Stream Ciphers



Keystream randomness = plaintext security

IMPERVA®

RC4

- Rivest Code 4
- The most popular Stream Cipher for more than 25 years
- Details kept secret until the WEP attack in 2001

RC4 Algorithm

Key Scheduling Algorithm (KSA)

Pseudo-Random Generation Algorithm (PRGA)

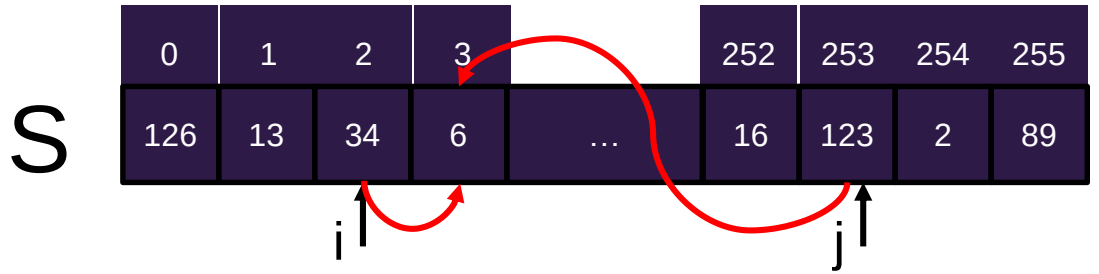
All operations are mod 256

```
KSA(K):
    j = 0
    S = [0, 1, 2, …, 255]
    for i = 0..255
        j = j + S[i] + K[i mode |K|]
        S[i] ↔ S[j]
```

```
PRGA(S0):
    i = 0
    j = 0
    S = S0
    While bytes are needed:
        i = i + 1
        j = j + S[i]
        S[i] ↔ S[j]
        Emit S[S[i]+S[j]]
```


IMPERVA®

RC4 Algorithm



KSA(K):

```
j = 0
S = [0, 1, 2, …, 255]
for i = 0..255
    j = j + S[i] + K[i mode |K|]
    S[i] ↔ S[j]
```

PRGA(S_0):

```
i = 0
j = 0
S = S0
While bytes are needed:
    i = i + 1
    j = j + S[i]
    S[i] ↔ S[j]
    Emit S[S[i]+S[j]]
```

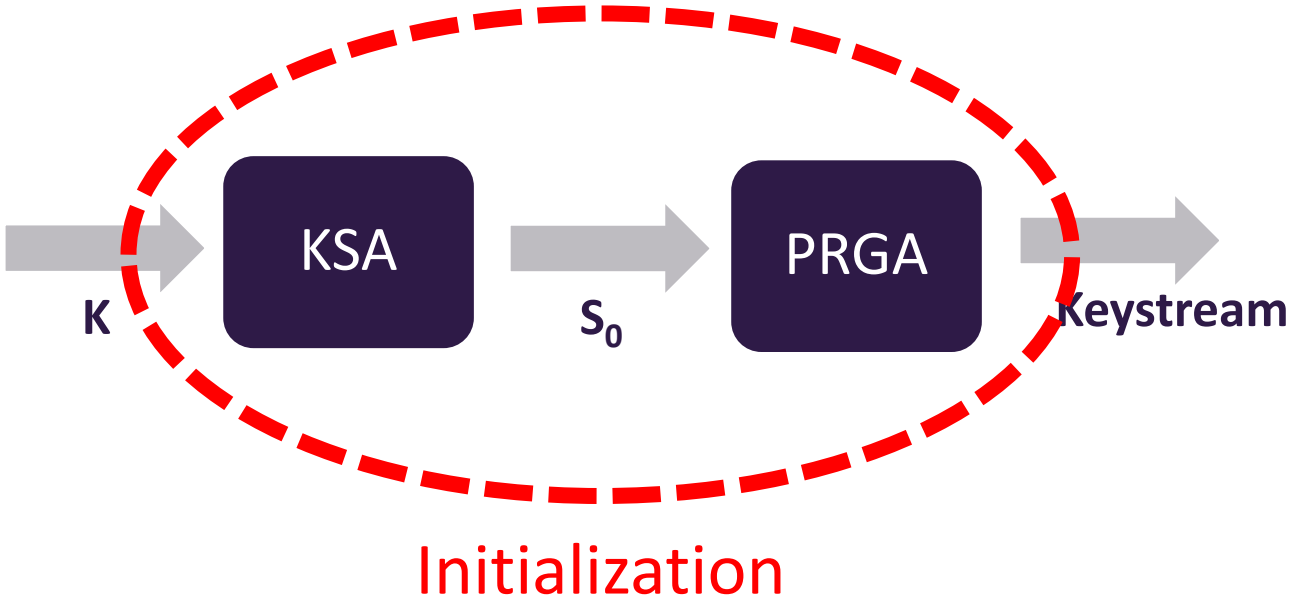

IMPERVA®

RC4 (In)Randomness

- RC4 in **NOT** pseudo-random
  - 2^{30} distinguishing algorithm
    Fluhrer-McGrew, 2000
    Patterns used in 2013 to attack TLS (the Royal-Holloway attack)
  - 2^{26} byte distinguishing algorithm
    Mantin, 2005
    Patterns used in July 2015 to attack WPA-TKIP and TLS
  - 2^{45} Prediction algorithm
    Mantin, 2005

RC4 Initialization

The weakest link of RC4 since 2001



IMPERVA®

RC4 Initialization

Keystream biases

- The second-byte bias (Mantin-Shamir, 2001)
- Many others

Initial permutation biases

- My thesis 2001, Mironov 2002

Key-keystream correlations

- The IV Weakness and the WEP Attack (Fluhrer-Mantin-Shamir, 2001)
- Enhanced WEP Attack I (Mantin, 2005)
- Enhanced WEP Attack II (Tews-Weinmann-Pyshkin, 2007)
- More Key-keystream correlations (Klein, 2005)
- The Invariance Weakness (Fluhrer-Mantin-Shamir, 2001)

3

The Invariance Weakness

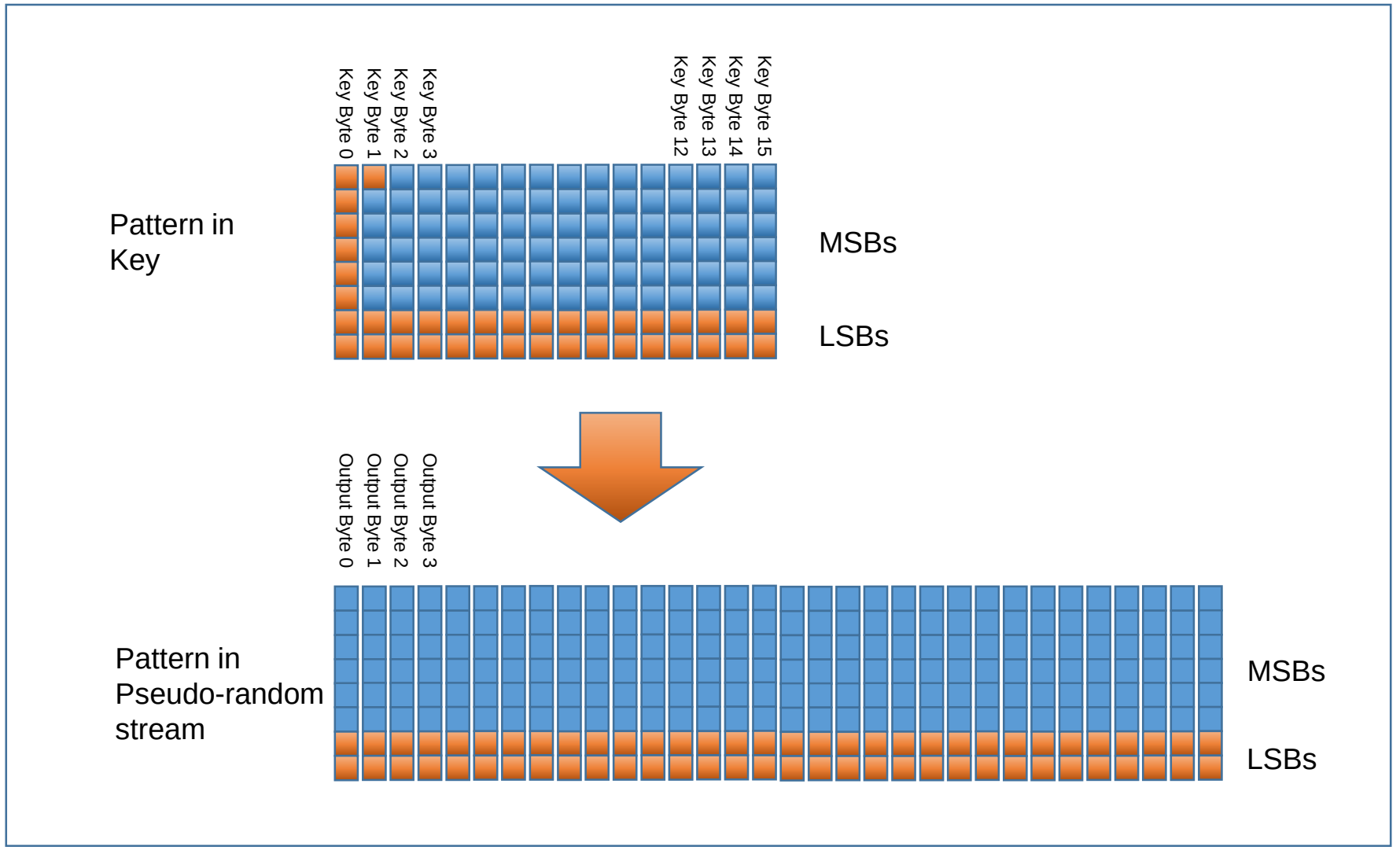
IMPERVA®

The Invariance Weakness

- The neglected counterpart of the IV Weakness
- Left in the shadows for 13 years

- RC4 weak keys
  - **Huge** class of keys (2^{-24} fraction for 128bit keys)
  - Bad mixing of the key with the permutation. Permutation parts remain **intact**

Key Patterns



IMPERVA®

Plaintext Leakage

IMPERVA®

Weak Key Classes

# LSBs	Applicability	Class Fraction (8-byte key)	Class Fraction (16-byte key)
1	Keys with even number of bytes	2^{-16}	2^{-24}
2	Keys with number of bytes that divides 4	2^{-23}	2^{-39}
3	Keys with number of bytes that divides 8	2^{-30}	2^{-54}
4	Keys with number of bytes that divides 16	2^{-37}	2^{-69}

IMPERVA®

Plaintext Leakage

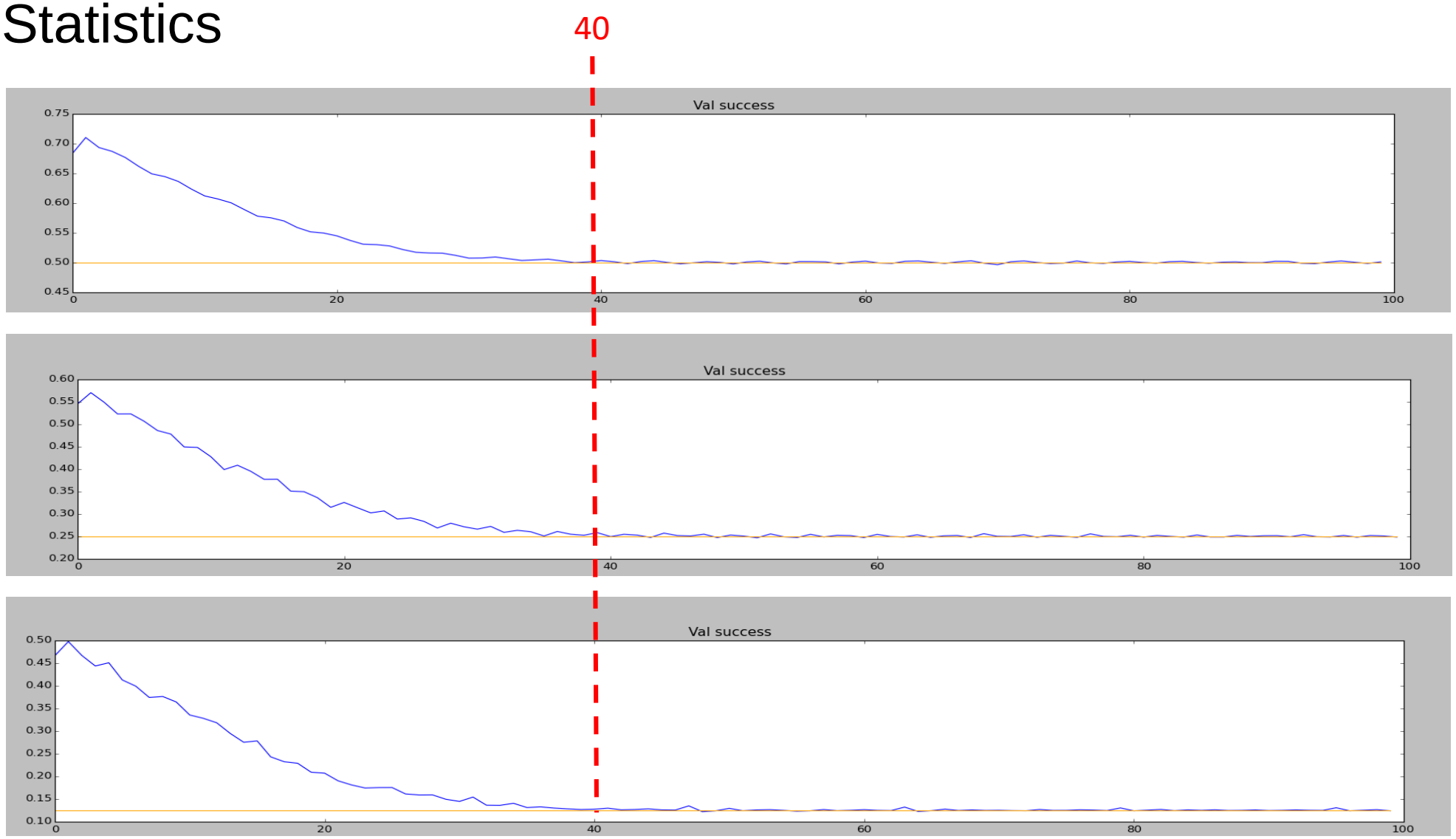
- When a weak key is used, “many” plaintext bit leak
- Q1: Can we tell when that happens?
  - Yes, when plaintext patterns exist
- Q2: How many bits?

Leakage Statistics

q=1

q=2

q=3

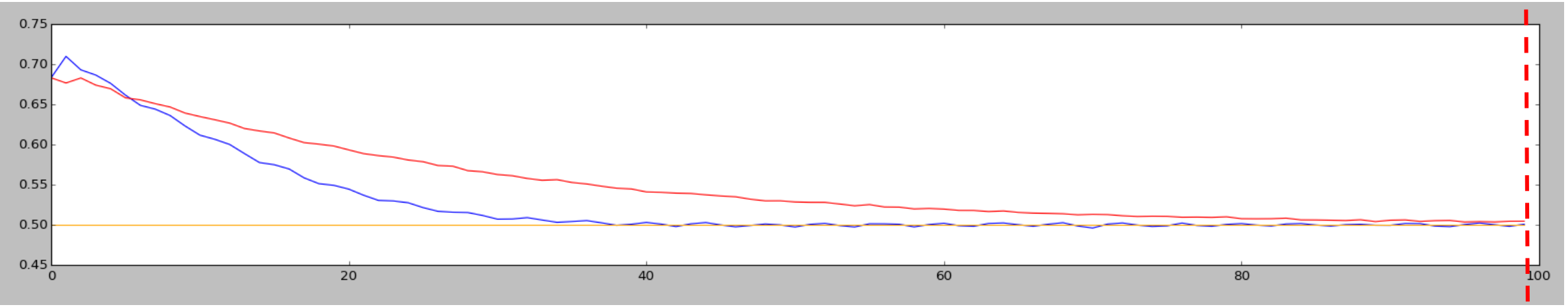


IMPERVA®

Diff-Based Leakage

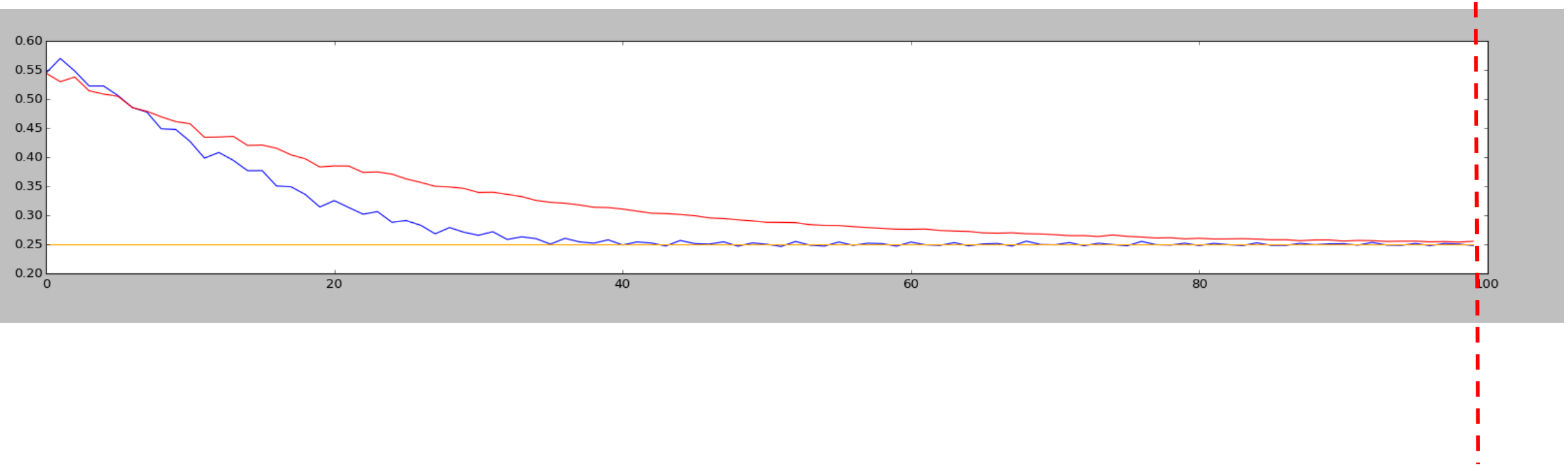
- The permutation is ruined with the keystream generation
- Bit prediction gets out of sync when j hits a “ruined” part
- Switch to diff

Diff-Based Leakage (q=1)



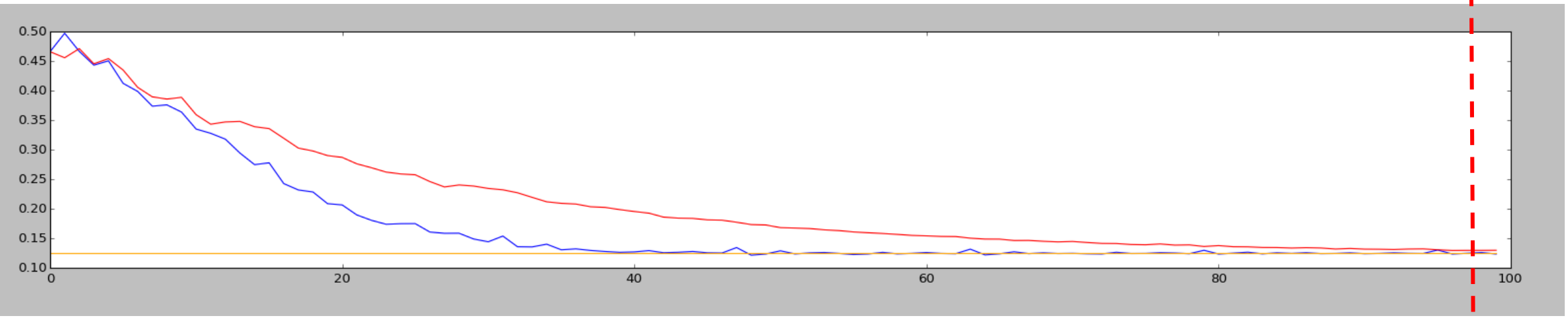
IMPERVA®

Diff-Based Leakage (q=2)



IMPERVA®

Diff-Based Leakage (q=3)



IMPERVA®

The Leakage

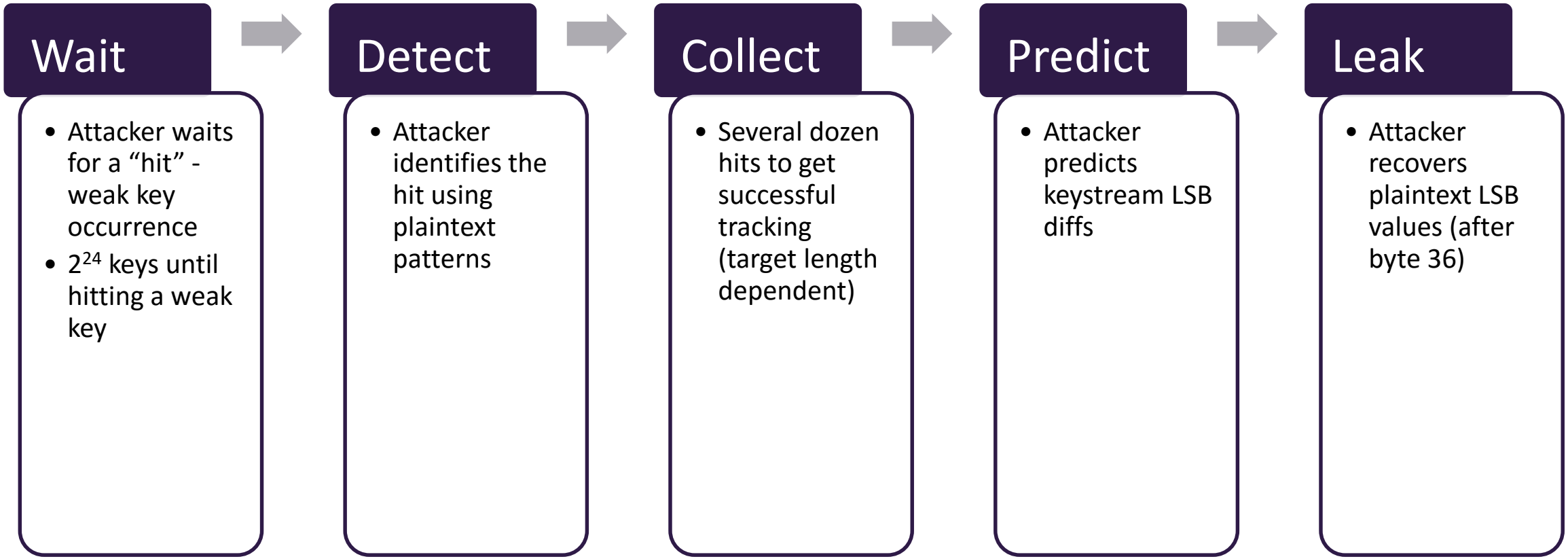
- Using the 1-Class
  - 1^{st} diff LSB is guessed correctly with probability 0.68
  - 37^{th} diff LSB is guessed correctly with probability of 0.546
  - 100^{th} diff LSB is guessed correctly with probability of 0.503
- Pattern tracking is possible for
  - 37 bytes with 1/22 advantage
  - 68 bytes with 1/64 advantage
  - 100 bytes with 1/330 advantage
- First 100 LSBs are exposed to leakage

4

The Attacks

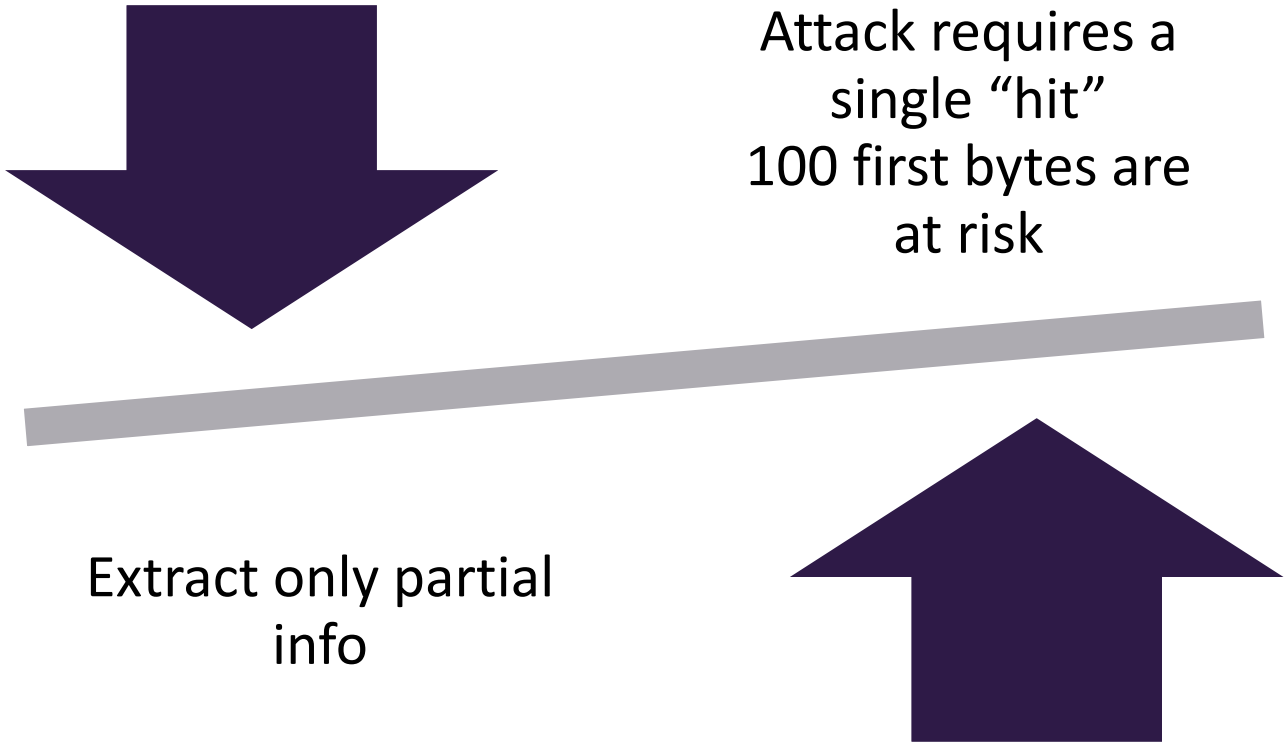
IMPERVA®

The Attack Basic Scenario



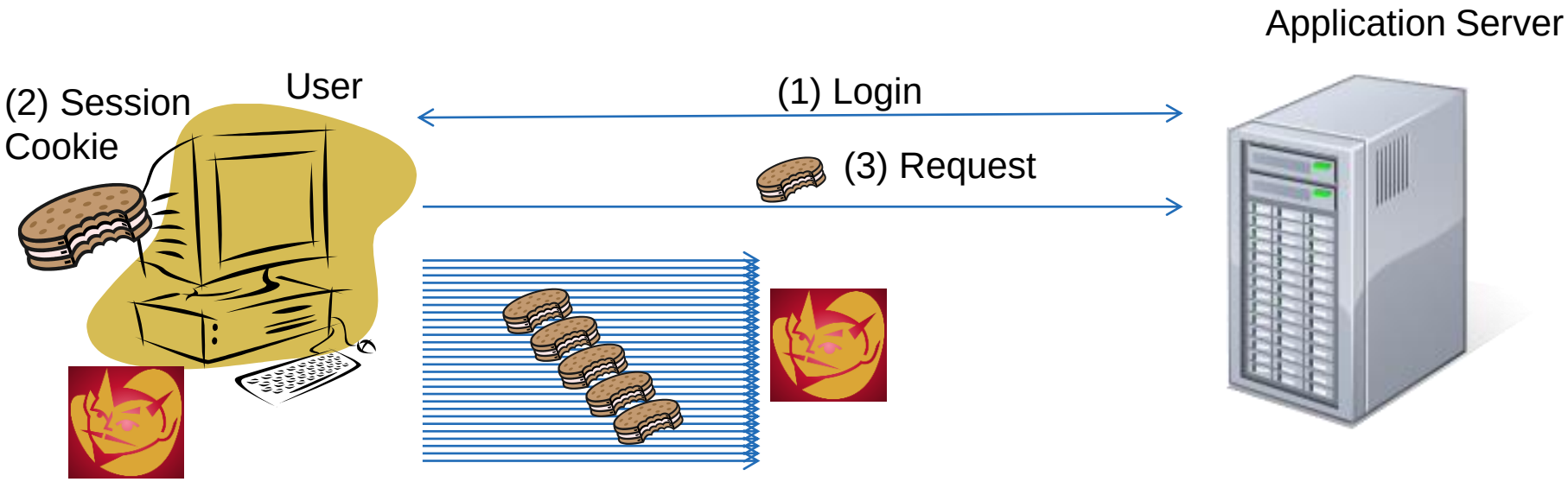
IMPERVA®

Attack Unique Characteristics



IMPERVA®

BEAST-like Attack



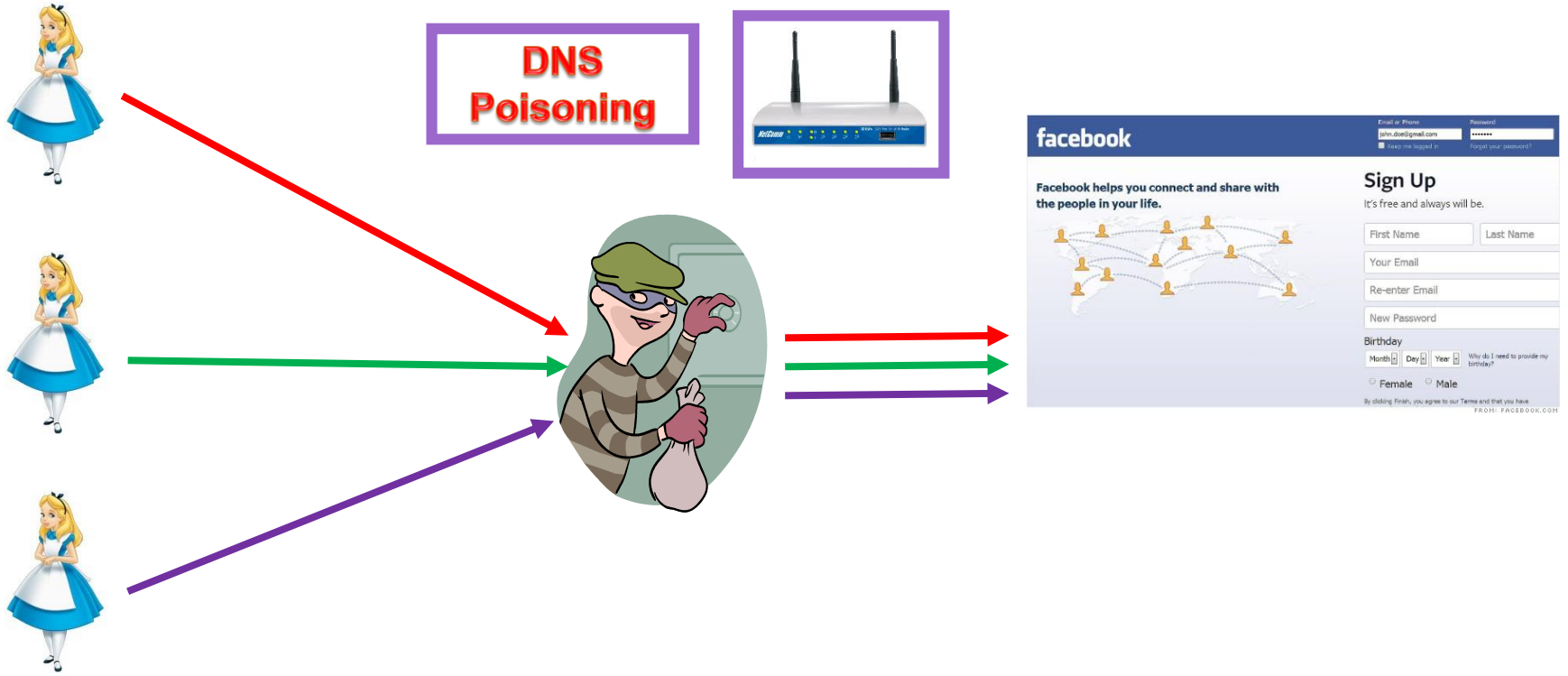
- 1 billion connections required
- Insensitive to Resets

IMPERVA®

Group Attack

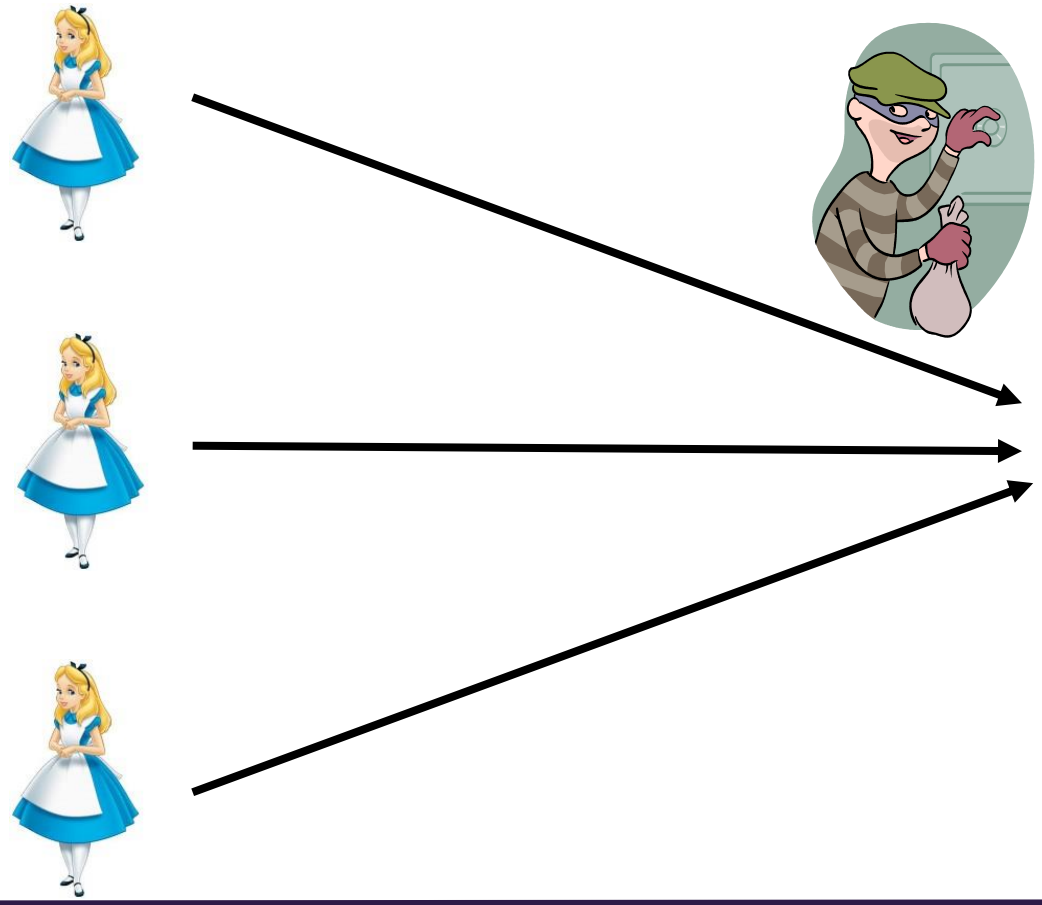
Attack requires a single hit

Pool of Potential Victims



IMPERVA®

Non-Targeted ***Passive*** Attack



Attack requires a single “hit”

Pool of Potential Victims

IMPERVA®

1 Billion Connections?

- Facebook has 890 million DAU (Daily Active Users)
- Most login more than once a day

IMPERVA®

A Concerning Fact

- Every time you send a secret over TLS/RC4 connection
  - You have a 1:16 million chance to get a bad key
  - You have a 1 in a billion chance to get unlucky and leak a significant portion of your secret
- Small numbers, but definitely not negligible
- RC4 stats (March 2015): 30% of Internet TLS connections

5

Conclusion

IMPERVA®

Summary

- The Invariance Weakness of RC4 can be used to mount new attacks on TLS
- The ***Reset Insensitivity*** nature of the attack opens the door to new attack scenarios
- First passive attack on TLS

Conclusions

- RC4 is a not a secure cipher (old news)
- The initialization mechanism of RC4 is very weak (old news)
- The impact of these facts on the (In)Security of systems using RC4 is underestimated
  (today this is also old news)

More info

- Report at Imperva ADC site:
  - http://www.imperva.com/DefenseCenter/HackerIntelligenceReports
- Blackhat materials (white paper and presentation)
  - https://www.blackhat.com/docs/asia-15/materials/asia-15-Mantin-Bar-Mitzvah-Attack-Breaking-SSL-With-13-Year-Old-RC4-Weakness-wp.pdf
  - https://www.blackhat.com/docs/asia-15/materials/asia-15-Mantin-Bar-Mitzvah-Attack-Breaking-SSL-With-13-Year-Old-RC4-Weakness.pdf
- Wiki of the attack
  - https://en.wikipedia.org/wiki/Bar_mitzvah_attack

heise Security News Hintergrund Tools Foren

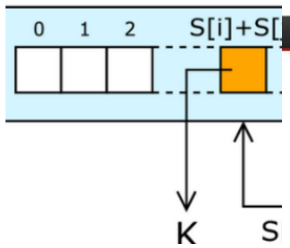
Security > News > 7-Tage-News > 2015 > KW 13 > Verschlüsselung: Deutlich verbesserte Angriffe auf RC4

« Vorige | Nächste »

Verschlüsselung: Deutlich verbesserte Angriffe auf RC4

27.03.2015 15:29 Uhr – Jürgen Schmidt

vorlesen



SSL 與 TLS 多年來被業界沿用為數據傳輸中的加密標準，但日前就有資安人員揭露指，原來上述兩種加密方式依然存在著根本上的漏洞，被發現的漏洞更出現長達 13 年之久，用戶敏感資料完全沒保障。

ars technica

Pattern Mining Webinar

Learn how to extract patterns from log data. Sign up for our webinar!

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

Noose around Internet's TLS system tightens with 2 new decryption attacks

Exploits pluck passwords and other sensitive data out of encrypted data streams.

by Dan Goodin - Mar 27, 2015 2:22am EET

Enlarge

André Mendes

The noose around the neck of the Internet's most widely used encryption scheme got a little tighter

Pattern Mining Webinar

Learn how to work with messy log data. Sign up for our webinar!

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Lying to your friends: Our 4 favorite bluffing games

Deception has never been so entertaining.

WATCH ARS VIDEO

ZDNet

DE-Edition Cloud Data & Storage IoT Mobile Sicherheit Unternehmen Workspace KMU Downloads Windows 10 Whitepaper

Bitdefender

MEHR FÜR SIE DRIN!

Schützt Server und Desktops (virtuell und physisch)

Windows Linux Mac

+3 MONATE GRATIS

ZUM VORTEILSANGEBOT

ZDNet / Sicherheit / Sicherheitsmanagement

Forscher demonstrieren Schwachstelle bei RC4-Verschlüsselung für SSL-Verbindungen

von Kai Schmerer am 27. März 2015, 18:21 Uhr

Der Sicherheitsspezialist Imperva hat eine neuen Hacker Intelligence Initiative (HII) Report veröffentlicht. Demnach hat sein Forschungsteam des Application Defense Center (ADC) neue Angriffsschwachstellen in dem verbreiteten Transport Layer Security (TLS/SSL)-Zertifikat entdeckt.

IMPERVA

Modernisierung der IT zur Steigerung der Produktivität und wie KMU das Wachstum fördern können

Herunterladen

Whitepaper silicon.de

InformationWeek Register Login to your account Welcome Guest Digital Subscription Contact Us About Us Advertise With Us

ixia LEARN MORE

DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

News & Commentary Authors Slideshows Video Radio Reports White Papers Events Black Hat SECURITY JOBS

ATTACKS/BREACHES

splunk>

SSL/TLS Suffers 'Bar Mitzvah Attack'

Researcher at Black Hat Asia shows how attackers could abuse a known-weak crypto algorithm to steal credentials and other data from encrypted communications.

SSL/TLS encryption once again is being haunted by an outdated and weak feature long past its prime: a newly discovered attack exploits a weakness in the older, less secure RC4 encryption algorithm option in SSL/TLS that's still supported in many browsers and servers.

Itsik Mantin, director of security research with Imperva, at Black Hat Asia in Singapore today will detail how an attacker could sniff credentials and other information during an SSL session in an attack he named the "Bar Mitzvah Attack" after 13-year-old weaknesses in the algorithm it abuses. The attack is

Kelly Jackson Higgins News

EDUCATIONAL RESOURCES

- Beyond Malware: Detecting the Undetectable
- Indicators of Attack vs. Indicators of Compromise
- Next Generation Endpoint Protection Case Study: Cardinal Innovations Healthcare
- Cyber Intrusion Services Report
- Crowdstrike Services Brochure

VIDEO WEBINAR TWITTER

IMPERVA®

IMPERVA®

http://www.imperva.com/DefenseCenter/HackerIntelligenceReports