Iran’s Real Life Cyberwar

Phillip Hallam-Baker
Comodo Group Inc.

[Some images from Wikimedia commons]

Be Very Afraid…


SUB-LAUNCH DETECTION
MISSILE WARNING
Is it a game, or is it real?
WARGAMES

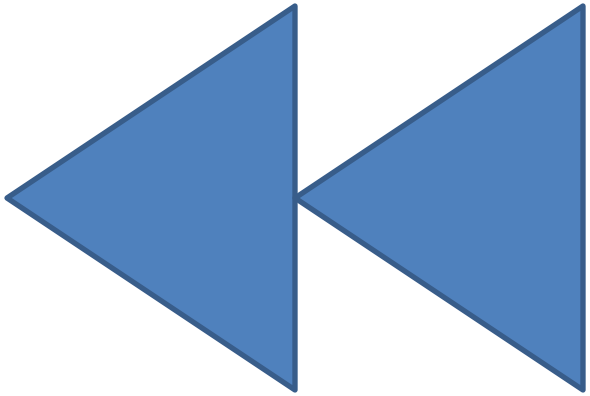
The Real Problem

YouTube

Browse

Gwapo's HF Money Making

Gwapo DDOS | Subscribe | 7 videos



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

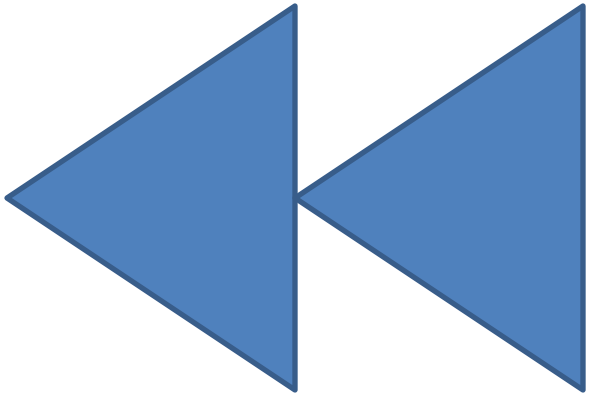
If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

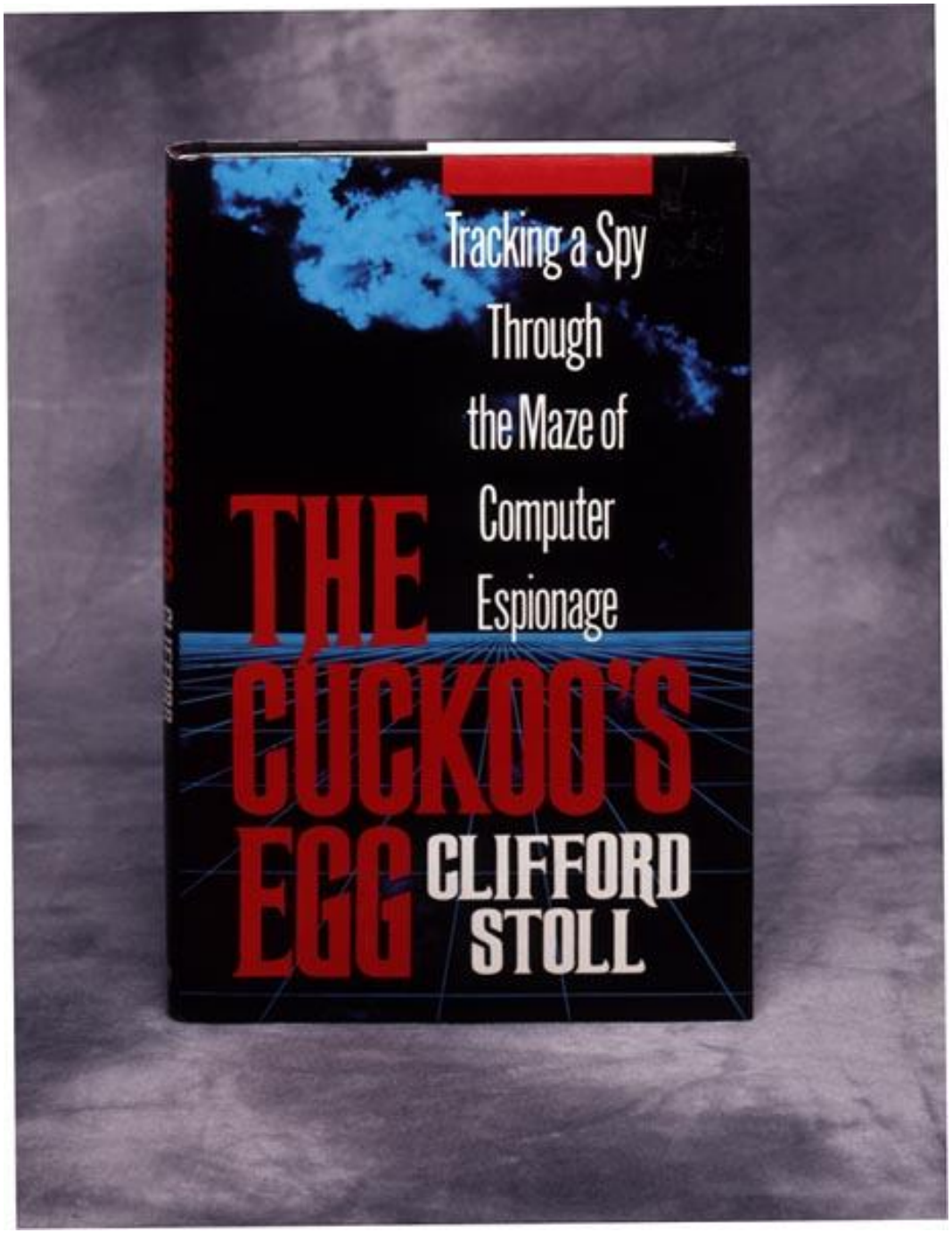
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102 (24 hour telephone contact) NLETS access code is VAUSM0000.

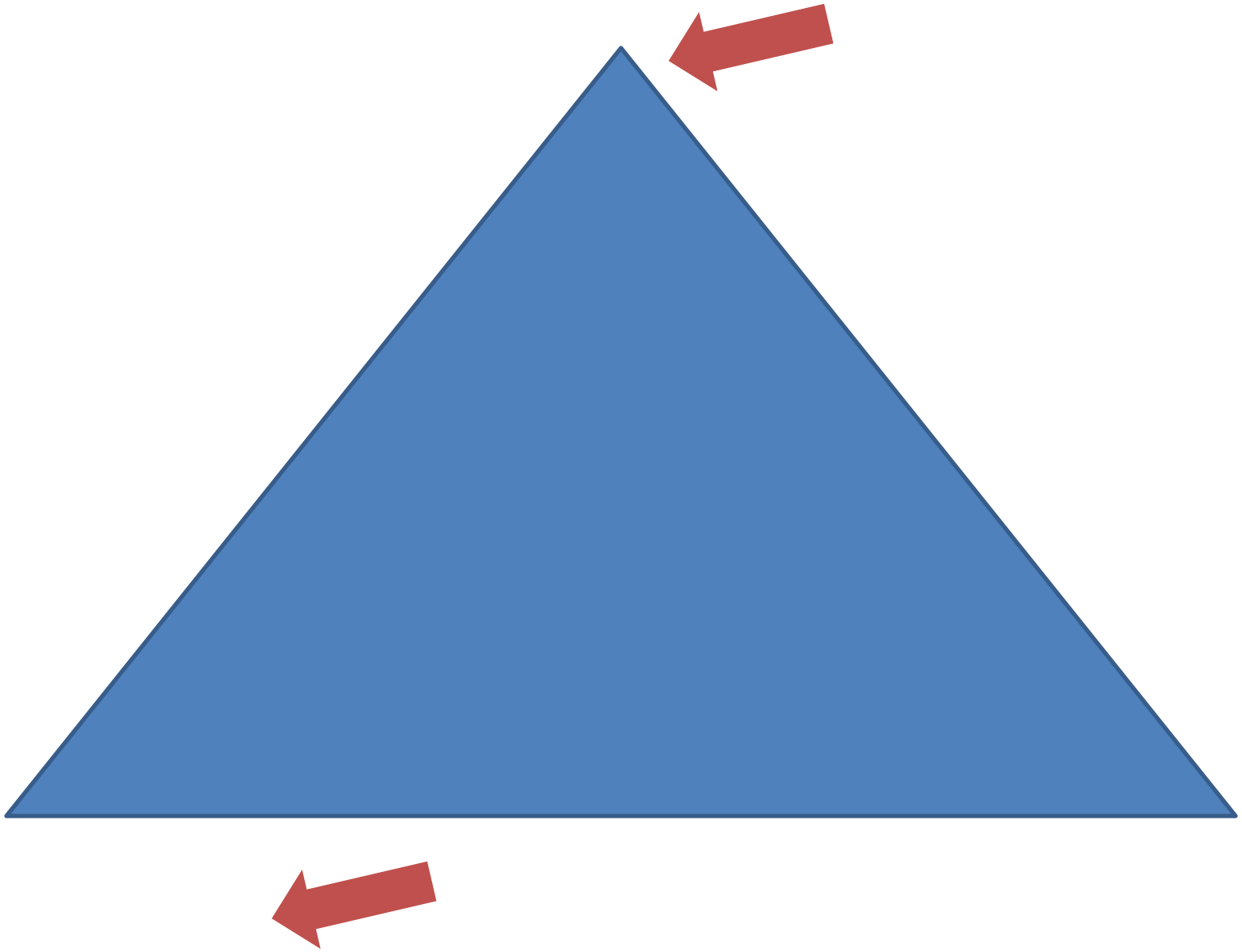
Form USM -132
(Rev. 3/2/82)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992



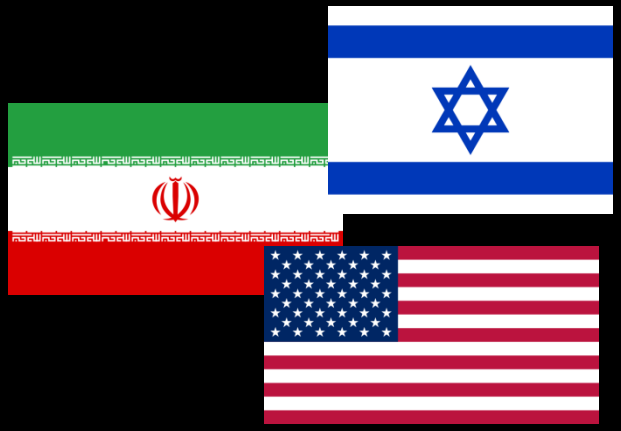

Tracking a Spy
Through
the Maze of
Computer
Espionage
THE
CUCKOO'S
EGG
CLIFFORD
STOLL



What Has Changed?

Motive


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
100
B 96195909 D
ONE HUNDRED DOLLARS



Capabilities

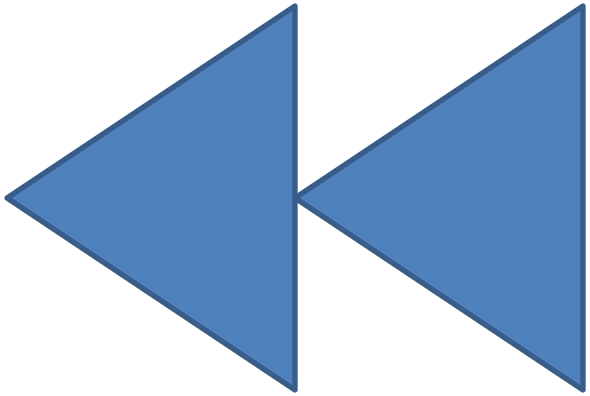
Targets


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
100
B 96195909 D
ONE HUNDRED DOLLARS


BETONDEMONTAGETE
LOVE & PEACE
WEST & EAST
Test
West

Iran


Key Petroleum Sector Facilities
YEREVAN
Armenia
Azerbaijan
BAKU
Caspian Sea
Turkey
Uzbekistan
Turkmenistan
ASHGABAT
Tabriz
Qazvin
Neka
Mashhad
Sarakhs
IGAT-2 under construction
TEHRAN
Shahr-e Ray
Qom
Kermanshah
Arak
Naft Shahr
BAGHDAD
Iraq
Afghanistan
Dehluran
Esfahan
Dezful
IGAT-2
Ahvaz
Darkhovin
Parsi
IGAT-1
Bandar-e Emam Khomeyni
Gach Saran
IGAT-3
Abadan
Rafsanjan
Kerman
KUWAIT
Kuwait
Nowruz
Aboozar
Dorood
Shiraz
Pakistan
Saudi Arabia
Esfandiar
Bushehr
Dalan
Aghar
Jazireh-ye Khark
Fereidoon
North Pars
Kangan
Persian Gulf
Kangan
South Pars
Jazireh-ye Lavan
Jazireh-ye Qeshm
Bandar 'Abbas
Strait of Hormuz
MANAMA
Bahrain
Balal
North Field
Jazireh-ye Siri
Siri
Oman
DOHA
Qatar
Salman
Gulf of Oman
ABU DHABI
Arabian Sea
Saudi Arabia
United Arab Emirates
Oman
MUSCAT
Oilfield
Oil pipeline
Gasfield
Gas pipeline
Refinery
Gas-processing plant
Tanker terminal
Agreed-upon maritime boundary
765849AI (C00260) 8-04



19th August 1953

4th November 1979

SEP 79 13 05Z

R P T 31125Z S P 7 STAFF

T HONG KONG 62139

IMMEDIATE DIRECTOR INF PRIORITY TEHRAN, TOKYO, BANGKOK.

IN 1. WYBAT AJAJ/ INTEL

S A. DIRECTOR 5855 13
B. TOKYO 86 82

1. SECRET CONFUSION ON LOCATION "MISSI," WHICH WAS PLACE NAME
TO CHINESE MAP AS SUBJECT REPS INDICATED AREA TO BE AVOIDED BY
IN GROUND TROOPS. SUBJECT CLASSIFIED SECRET THAT GROUND ASSAULT
PS COULD AVOID ENTIRE BORDER REGION FROM MANDALA SOUTH TO THE
(A GROUND FORCE INFILTRATION WOULD TAKE PLACE NORTH OF
2. THROUGH MOST MOUNTAINOUS TERRAIN.

E
T 41-120-7 R W VIEPPS DRV 09C

Media

2009 Protests

Media cycle

8th April 2011

Medium

facebook

Stuxnet

- Discovered July 2010
- At least 5 Variants
- Possibly reduced production of U-235 by 30%
- Used signed code
  - Legitimate code signing certificates
  - Stolen keys
  - Needed to sign driver code
- Estimated to cost > $1 million to write

Comodo Certificate Mis-Issue

- Reseller Breached March 15 2011
  - Vector unkown
  - Located API used to request certs
  - Requested issue of certs for 7 domains
- Breach detected March 15 2011
  - Reseller received email saying certificates ready
  - Reseller knew that request had not been made
  - Notified Comodo

Immediate Response

- Certificates Revoked
  - But browsers don’t check this properly
- Browser Providers notified
  - Development of patches begun
- Certificate Subjects notified
- All reseller issue authority suspended
- FBI notified

Information Gathered

- IP Address from which request launched
  - In Iran
- Requests for cert status
  - Same Iranian address
- Email correspondence from attacker
  - IP address is in Iran
  - Company purports to be Israeli
  - Content cut and pasted from actual Israeli firms

Disclosure

- Testing browser patches takes time
  - One requires 8 days
- Jacob Appelbaum discovers new CRL entries
  - Agrees not to disclose until patches complete
- Public Announcement 28th March
  - Reveals Iranian connection
  - Response: “You are just saying that to cover up”

Pastebin Spin:

- 1) So counted **green movement** people in Iran isn't most of Iran, so when Obama says I'm with Iranian young community, I should say as Iranian young simply I hate you and I'm not with you, at least 90% of youngs in Iran will tell you same thing, it's not my sentence. But you have bad advisors, they report you wrong details, maybe you would think better if you have better advisors.
- 2) To Ashton and others who do their best **to stop Iranian nuclear program**, to **Israel** who send terrorist to my country to **terror my country's nuclear scientist** (http://www.**presstv**.com/detail/153576.html), these type of works would not help you, **you even can't stop me**, there is a lot of more computer scientist in Iran, when you don't hear about our works inside Iran, that's simple, we don't share our findings as there is no use for us about sharing, so don't think Iran is so simple country, behind today's technology, you are far stronger then them, etc.

Response

Consequences

Action

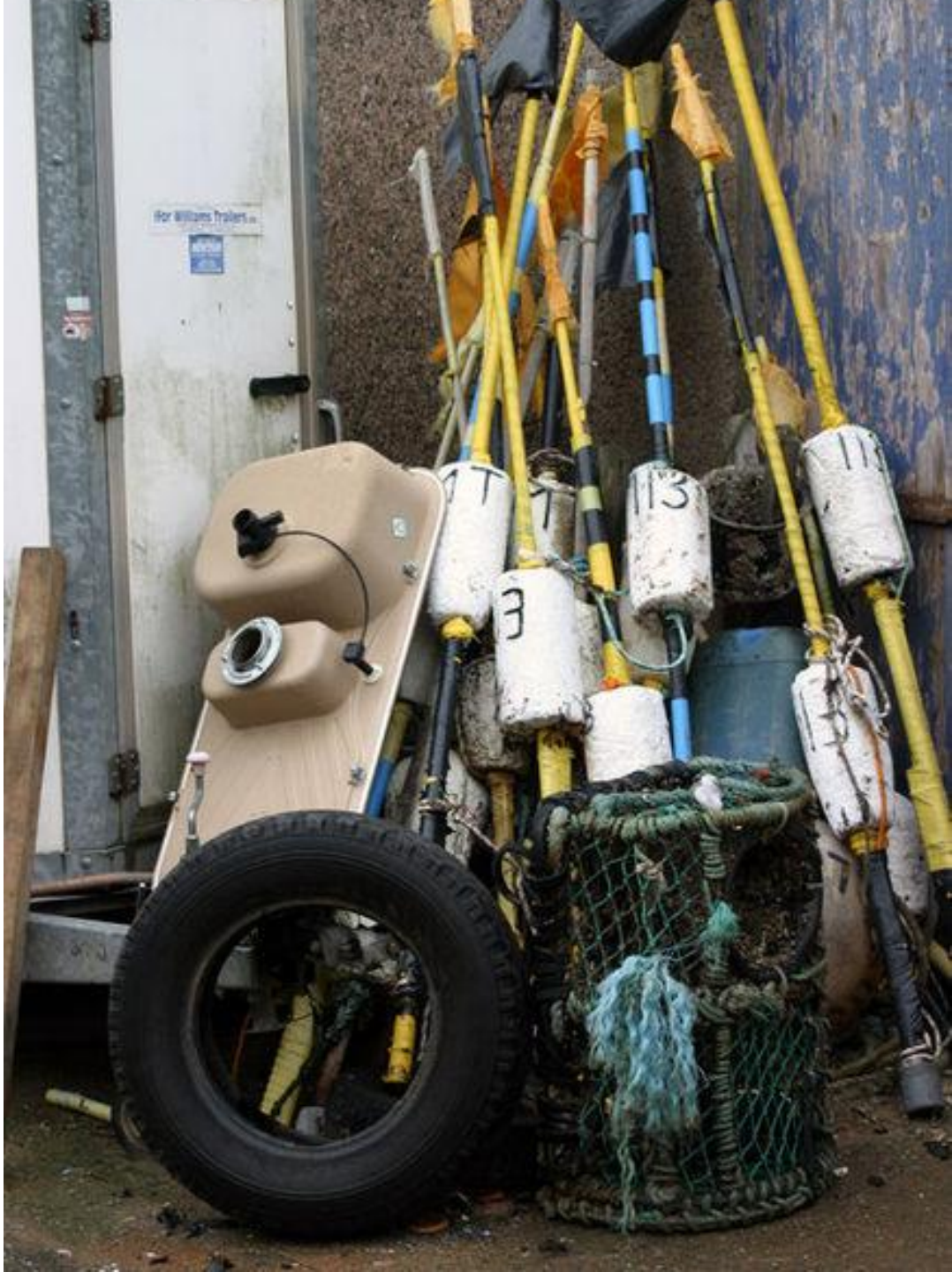
- Browsers agree to enable faster response
- Sharing of data on attacks amongst CAs
- Resellers

DigiNotar Breach

- Total Compromise
  - Lost control of signing unit (but not the key)
  - Machines with the audit logs
  - Unknown number of certificates issued
- Detected
  - Not reported
- CA liquidated
  - Public trust anchors (roots) revoked

But they had an audit!

Flame



Collateral Damage

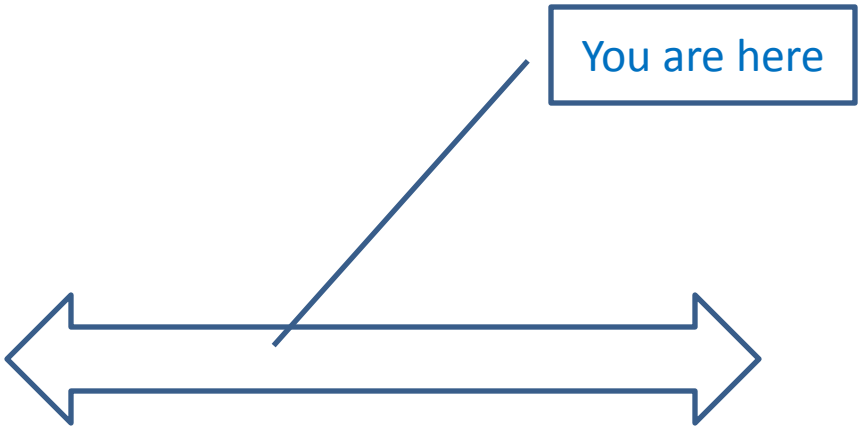
Microsoft

Cryptanalysis of MD5

- Sophisticated
- Novel

“Olympic Games”

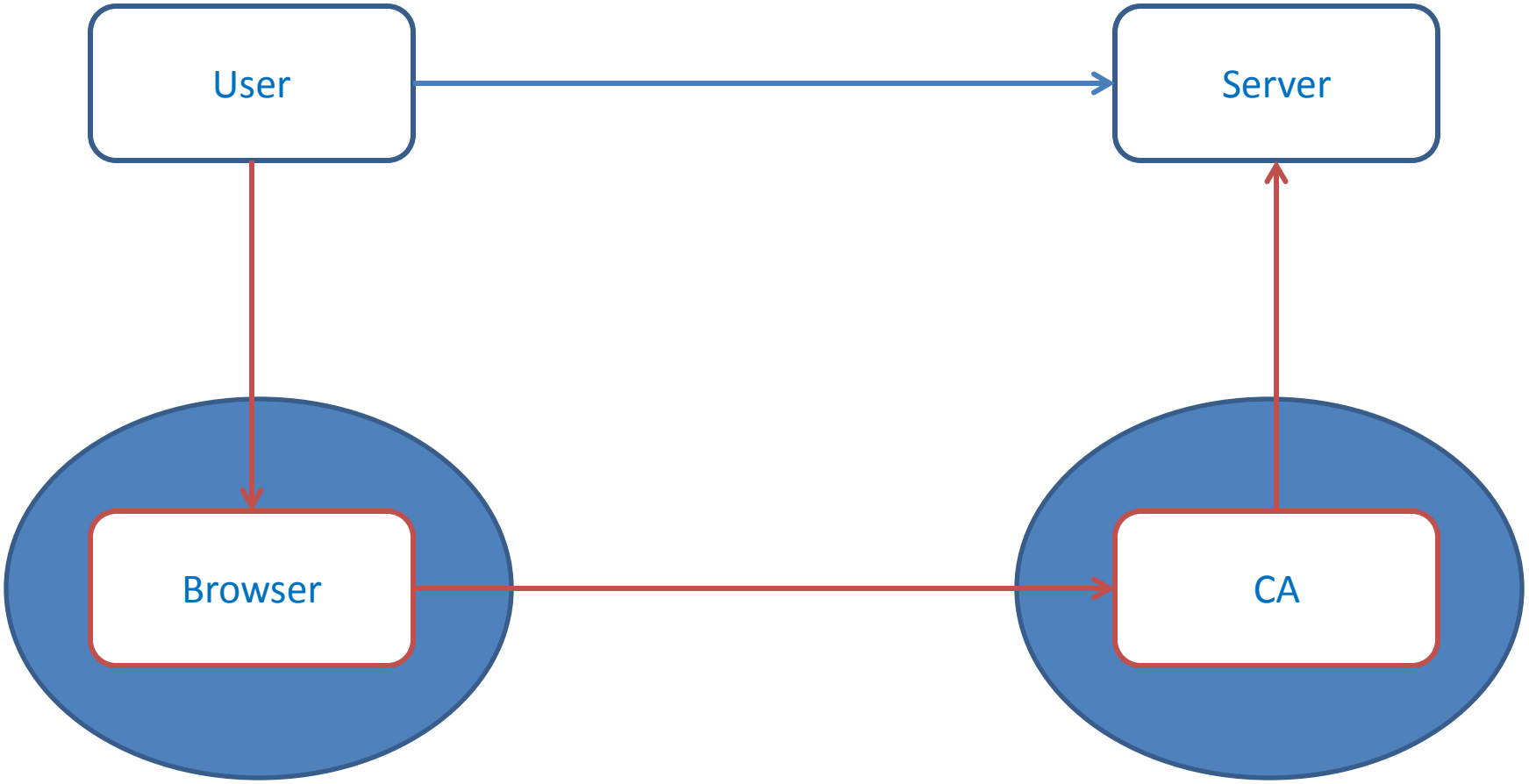
Situation Today



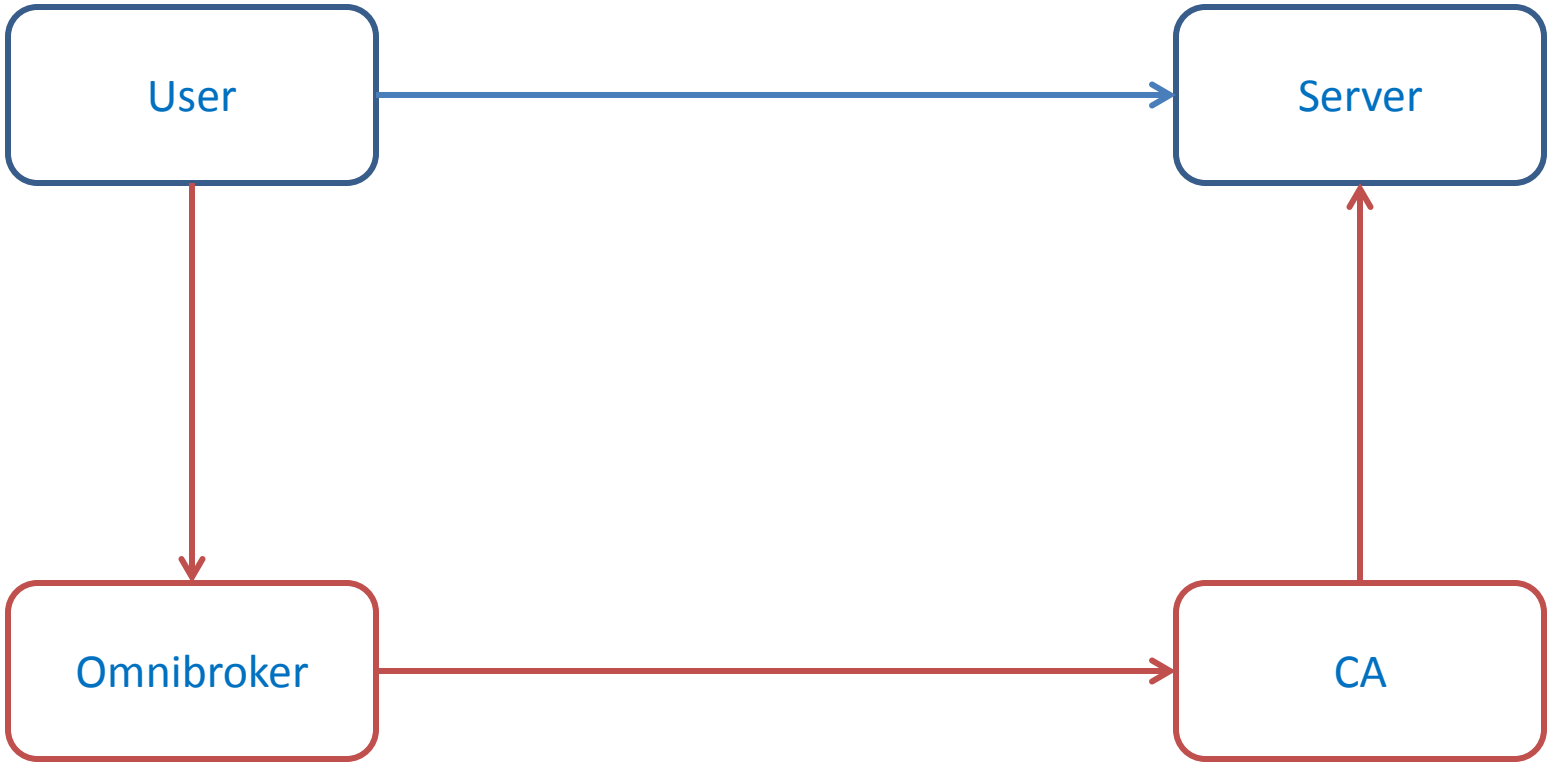
Changing the Infrastructure

- Perspectives, Convergence
- Sovereign Keys
- Certificate Transparency

The Problem



Omnibroker



Conclusions

- It isn't about the money
  - Can't defend by making attacks uneconomic
- State actors are now a threat
  - May be hit by either side
  - Motives likely political, ***not*** national security
- Work on reinforcing the trust infrastructure
  - Will take time
- Have a response plan