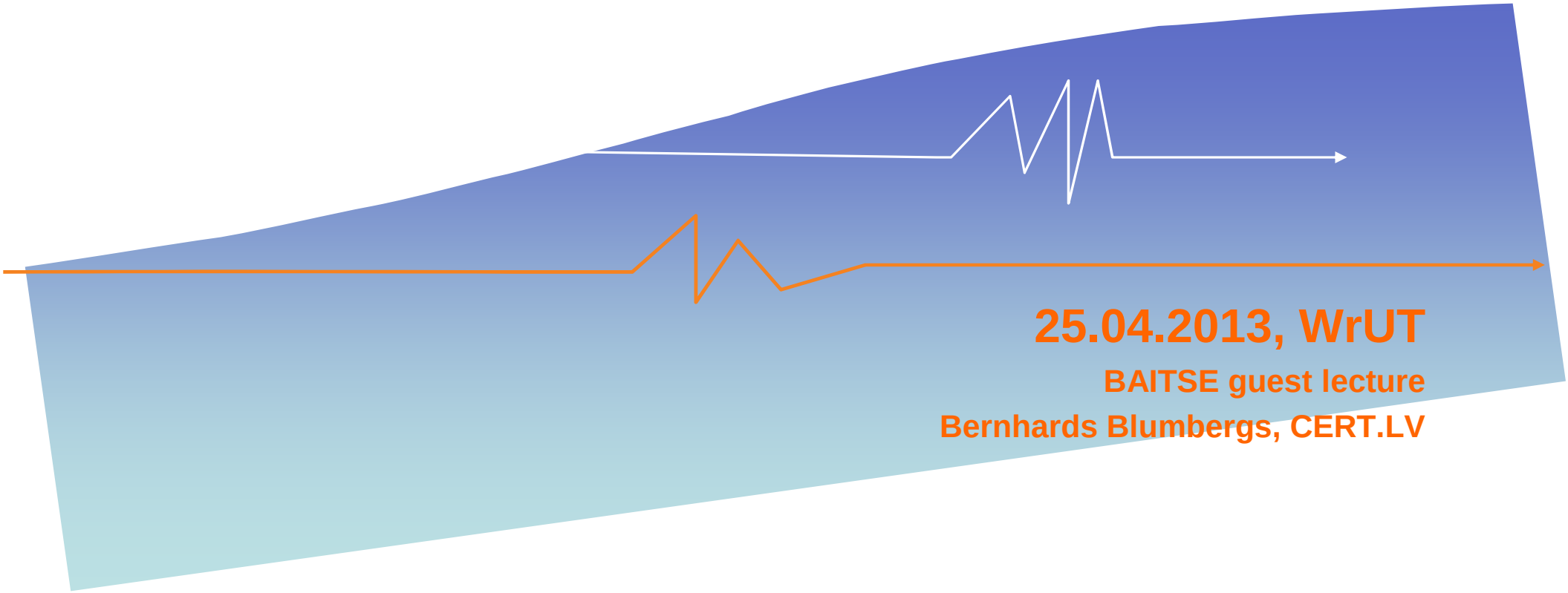
CERT.LV

Introduction to network penetration testing



25.04.2013, WrUT

BAITSE guest lecture

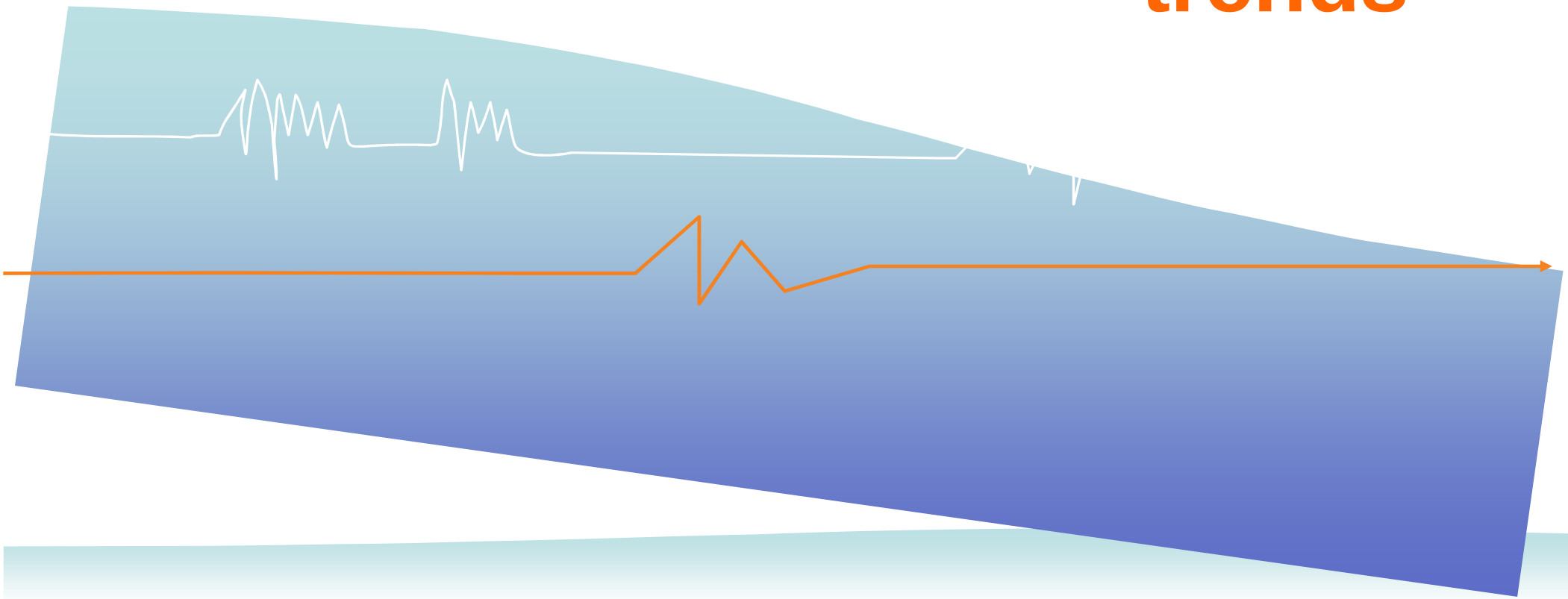
Bernhards Blumbergs, CERT.LV

Outline

- Current IT security trends
- IT Security principles
- The need for IT security testing
- Terminology explained
- Applicable standards and models
- Reporting results

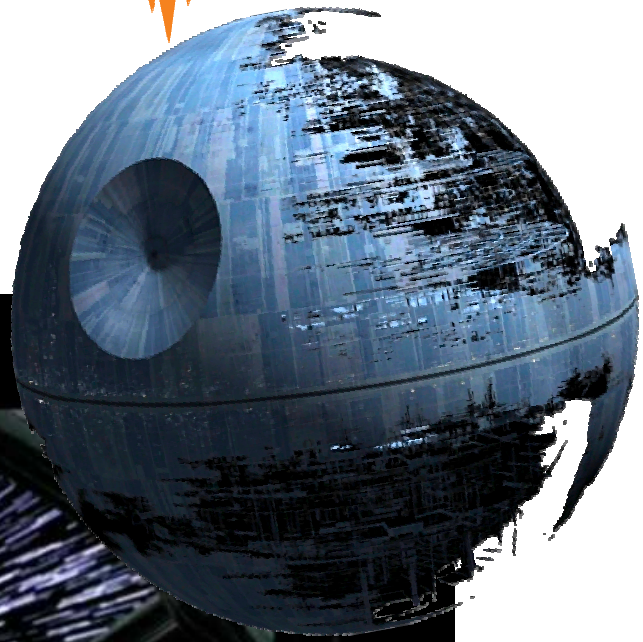
CERT.LV

Current IT security trends



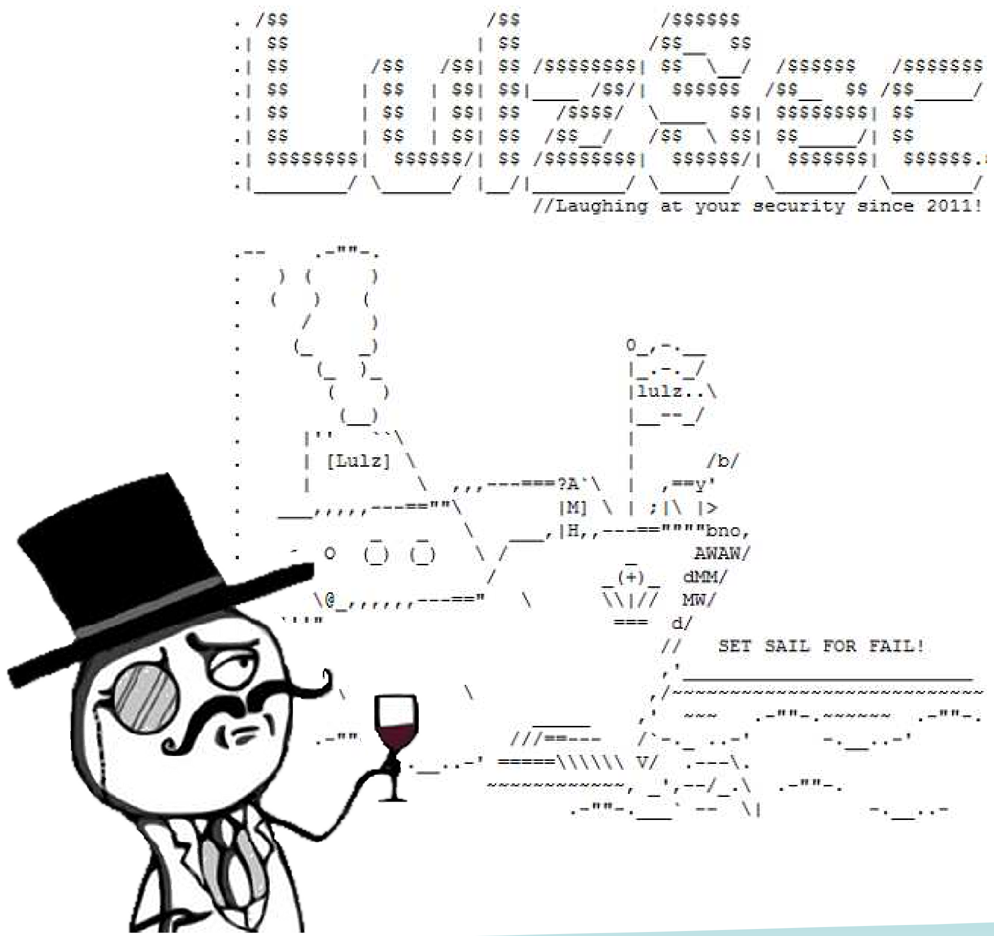
Not long time ago...

- In a galaxy nearby....



The story so far...

- Hacktivism



ANONYMOUS

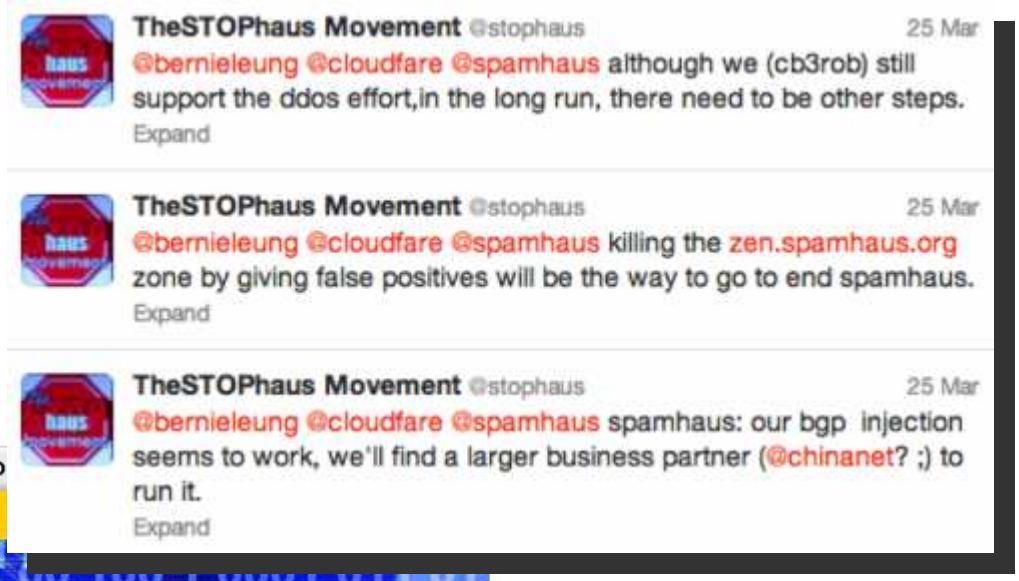
The story so far...

- Cyber warfare

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.ST
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MHN
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTA
      flame_props.FLAME_VERSION_CONFIG_KEY = "
      flame_props.SUCCESSFUL_INTERNET_TIMES_CO
      flame_props.INTERNET_CHECK_KEY = "CONNEC
      flame_props.BPS_CONFIG = "GATOR.LEAK.BAND
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PRO
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CO
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CON
          return l_1_0(l_1_1)
        end
```

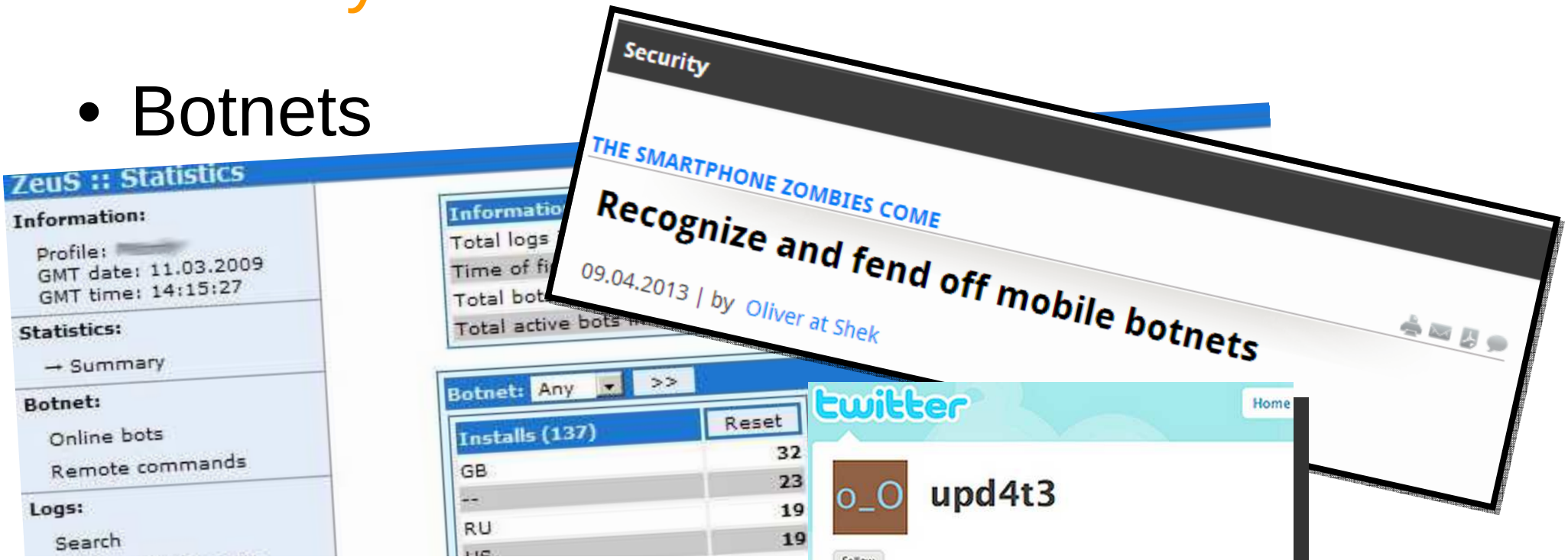
The story so far...

- Revenge attacks



The story so far...

- Botnets



Beware! DNS Changer's IP Blocks are re-allocated and advertised!

On August 11, 2012 By bgreene

From Senki.org .... By bgreene On August 10, 2012 · As of Friday morning (August 10, 2012), the IP address blocks us by the Rove Digital criminal operations have been re-allocat by RIPE-NCC and advertised to the Internet: http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRC001&query=1&arg=85.255.112.0%2F20 Read Full Article →

The story so far...

- Espionage

The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor

GReAT
Kaspersky Lab Expert
Posted February 27, 14:00 GMT
Tags: Adobe PDF, Obfuscation, Data Encryption, Targeted Attacks, Adobe, Vulnerabilities and exploits

(or, how many cool words can you fit into one title)

15 January 2013, 16:16

Operation Red October - large-scale cyber-espionage uncovered

Security experts at Kaspersky Lab have apparently uncovered a massive case of cyber-espionage. An analysis published on Monday states that computer networks in diplomatic missions, government and trade organisations, energy companies, and research, aerospace and military institutions have been infiltrated for an estimated five years. A sophisticated infrastructure appears to have enabled the unknown hackers to make off with terabytes of highly confidential geopolitical information and other data.

Kaspersky reports that it first found indications of the existence of the espionage infrastructure,

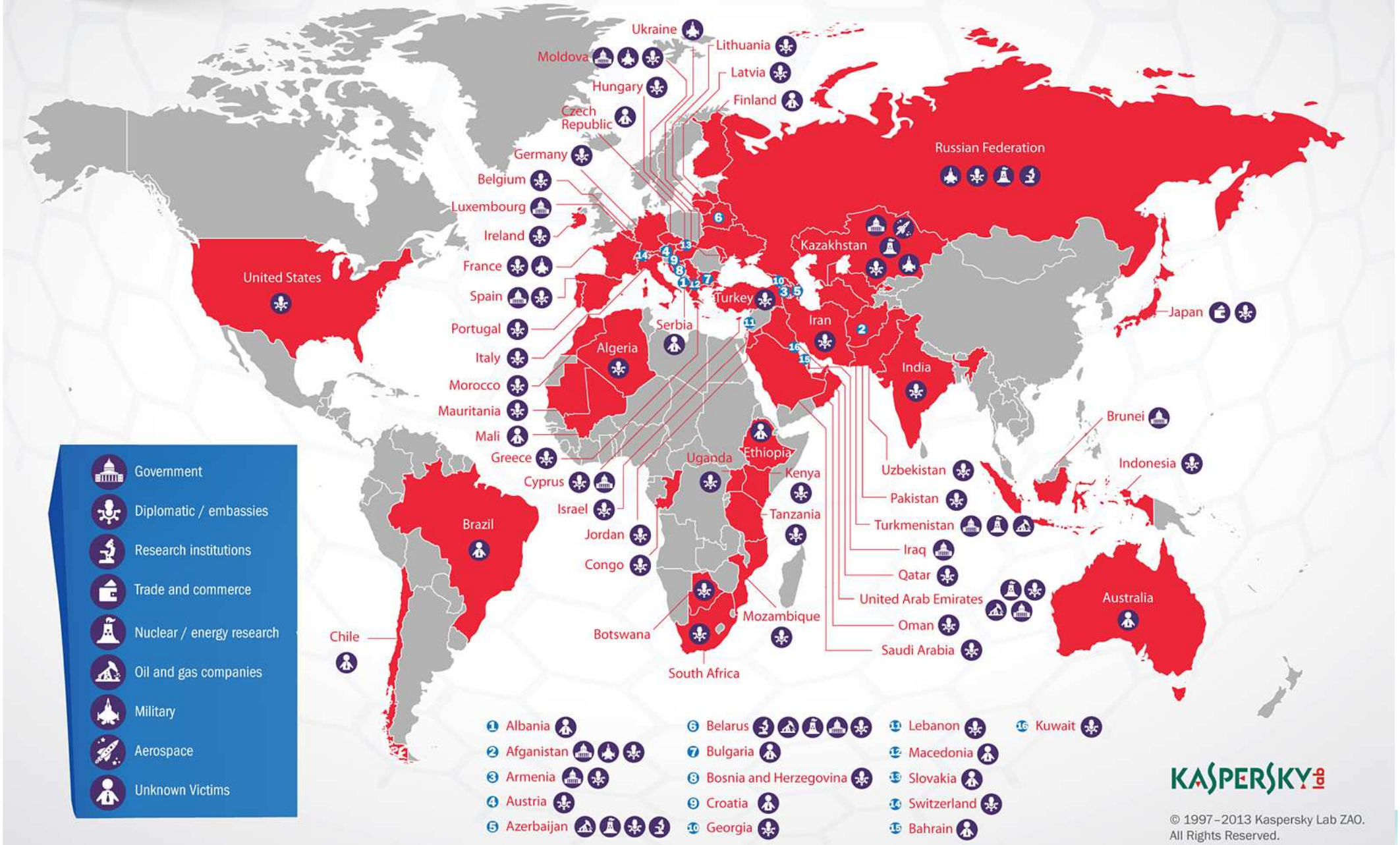
The structure of the command and control servers serves to conceal the actual point of origin
Source: Kaspersky Lab

Microsoft releases law enforcement Skype, user content disclosure figures

Summary: Weeks after US privacy groups called on Microsoft to disclose law enforcement requests to Skype, amid controversy over China surveillance and snooping, the software giant did. While China appears low in the table, the devil is in the details.

Operation "Red October"

Victims of advanced cyber-espionage network



KASPERSKY lab

The story so far...

- Ransomware

The story so far...

- WEBapp vulnerabilities

5,000+ sites hacked in 2 days by Indonesian Top Hacker Hmei7

Reported by Sabari Selvan on Wednesday, January 02, 2013 |

Like 145 +1 3 Tweet 223 StumbleUpon 0 Digg 0 Share 414

N°	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1.	iskorpitx	76015	392768	470783	267387	203396
2.	1923Turk	37353	169080	206433	78151	128282
3.	Hmei7	37204	91131	128335	63295	65040
4.	GHoST61	22411	265212	287623	168544	119079
5.	Fatal Error	21518	42603	64121	57820	6301
6.	kaMtiEz	14871	16435	31306	10010	21296
7.	SA3D HaCk3D	13032	32342	45374	12985	32389
8.	ZoRRoKiN	11298	9679	20977	7860	13117
9.	misafir	10047	28823	38870	6689	32181
10.	Ashiyane Digital Security Team	9573	33591	43164	14783	28381

Indonesian Top Hacker named "Hmei7" , known for Mass Defacements, has claimed to have defaced more than 5000 websites in two days(31 Dec 2012 and 1 Jan 2013).

So far , he hacked lot of high profile website including IBM, Microsoft, SIEMENS, AVG, Foxconn. He also defaced thousands of Government websites belong to different countries.

Mirror saved on: 2013-02-12 02:55:40

Notified by: Hmei7 **Domain:** http://bienestar.unimagdalena.edu.co/x.txt **IP address:** 190.254.21.212

System: Win 2008 **Web server:** IIS/7.5 Notifier stats

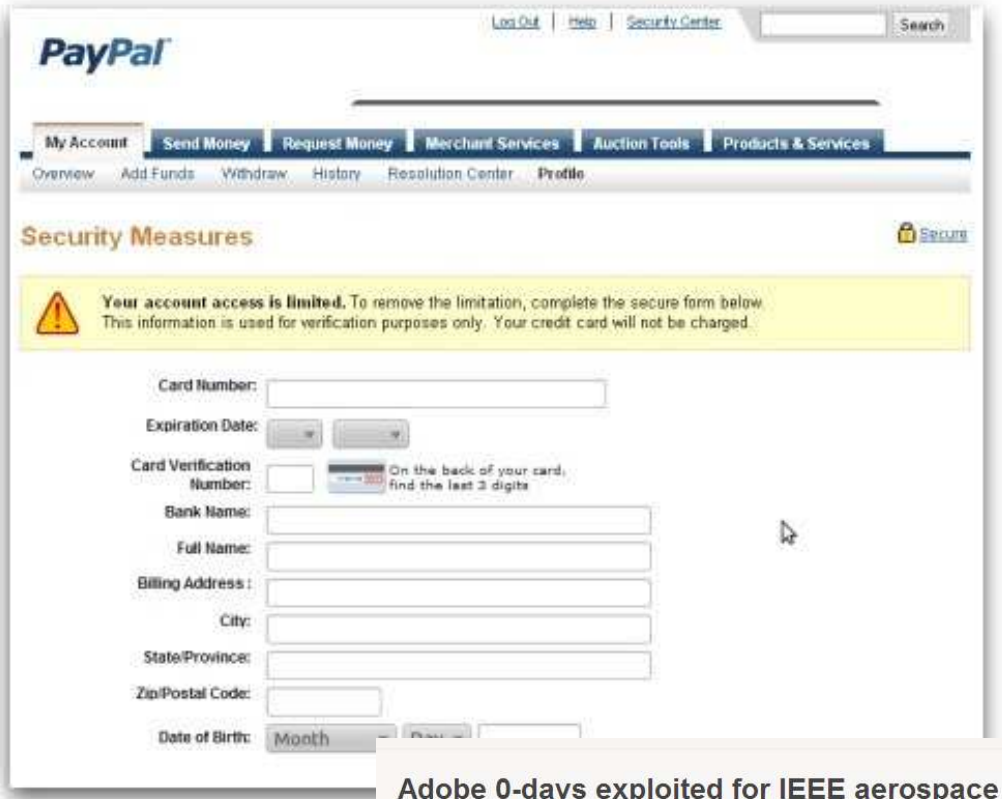
This is a CACHE (mirror) page of the site when it was saved by our robot on 2013-02-12 02:55:40

```
hacked by Hmei7
```

e just upload a file named "x.txt" or

The story so far...

- Phishing



The story so far...

- Application vulnerabilities

12 Fat Patch Tuesday

FEB 13

Adobe and **Microsoft** each have issued security updates to fix multiple critic vulnerabilities in their products. Adobe released updates for **Flash Player**, **AIR** a **Shockwave**; Microsoft pushed out a dozen patches addressing at least 57 security ho in **Windows**, **Office**, **Internet Explorer**, **Exchange** and **.NET Framework**.

Five of the 12 patches Microsoft released today earned its most dire "critical" label, meaning these updates fix vulnerabilities that attackers or malware could exploit to seize complete control over a PC with no help from users.

Examining How Facebook Got Hacked

Zero-Day Exploit Bypassed Java Protections to Install Malware

By Eric Chabrow, February 16, 2013. Follow Eric @GovInfoSecurity

Credit Eligible Email Tweet Like Share

Even the most savvy information technologists aren't immune from cyber-attacks. Just ask Facebook. The social-media titan victim to a sophisticated attack discov exploit allowed mal

's it fell
an

Adobe to patch Reader zero-day this week with rush update

Hackers exploiting sandbox-bypass bug

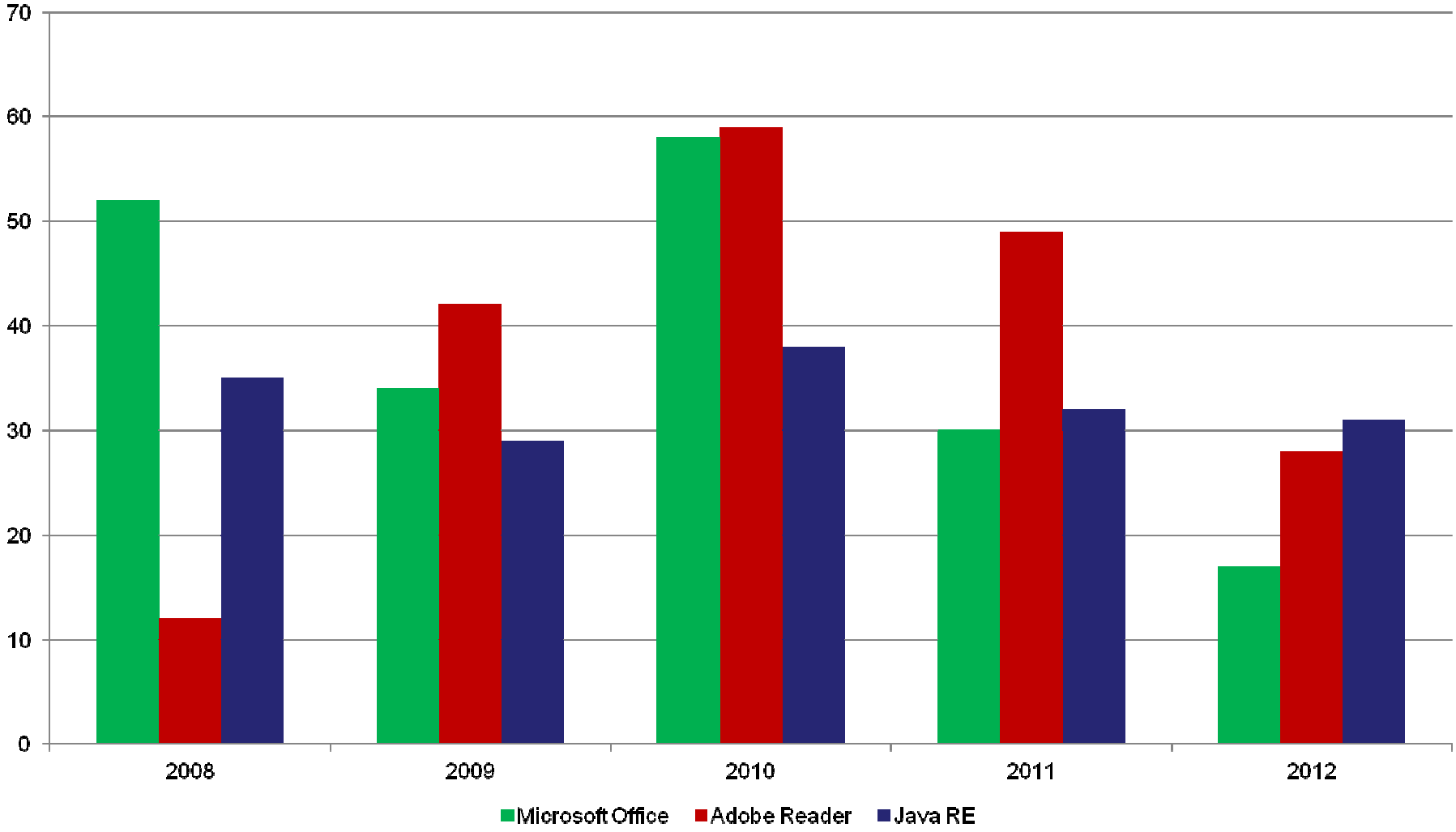
Gregg Keizer (Computerworld (US)) | 17 February, 2013 22:59 | Comments | Like 72 +1 2

Exclusive: Apple, Macs hit by hackers who targeted Facebook

Recommend 3,009 people recommend this. Sign Up to see what your friends recommend.

Tweet 1,581
Share 165
Share this
+1 341
Email

Critical vulnerabilities



Source: NIST National Vulnerability Database

The story so far...

- Exploit kits and drive-by exploits

July 16, 2012, 9:54AM

Black Hole Exploit Kit Targeting Java CVE-2012-1723 Flaw

by Dennis Fisher

Follow @DennisF

Share Like 0 +1 5

Comment

Exploit Kits

A new fork of the Black Hole exploit kit is making quick work of a recently patched Java vulnerability and security researchers say that the attackers are registering new sites quickly to exploit users with vulnerable browsers.

13 November 2012

CVE-2012-4969 and the Unnamed Admin Panel

While CVE-2012-4969 isn't new, we are still curious about the various ways this vulnerability can be exploited. Today we've stumbled upon a new instance of it. Let's have a look.

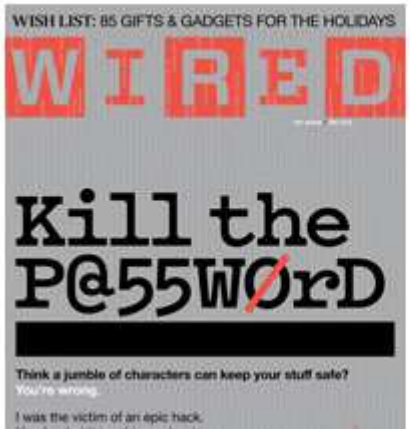
```
<html>
<body>
    <SCRIPT>
        var imgx = window.document.createElement("img");
        imgx.src = "a";
    </SCRIPT>
    <iframe src='ie.html' width='1' height='1'></iframe>
</body>
</html>
```

The story so far...

- Mobile devices and BYOD

The story so far...

- Targeted attacks



Your email. Your bank account. Your address and credit card number. Photos of your kids or, worse, of yourself, naked. The precise location where you're sitting right now as you read these words. Since the dawn of the information age, we've bought into the idea that a password, so long as it's elaborate enough, is an adequate means of protecting all this precious data. But in 2012 that's a fallacy, a fantasy, an outdated sales pitch. And anyone who still mouths it is a sucker—or someone who takes *you* for one.

No matter how complex, no matter how unique, your passwords can no longer protect you.

SECURITY ALERT Practical security advice

ANTIVIRUS SOFTWARE malware

Lockheed-Martin Attack Signals New Era of Cyber Espionage

By Tony Bradley, PCWorld May 28, 2011 9:40 PM

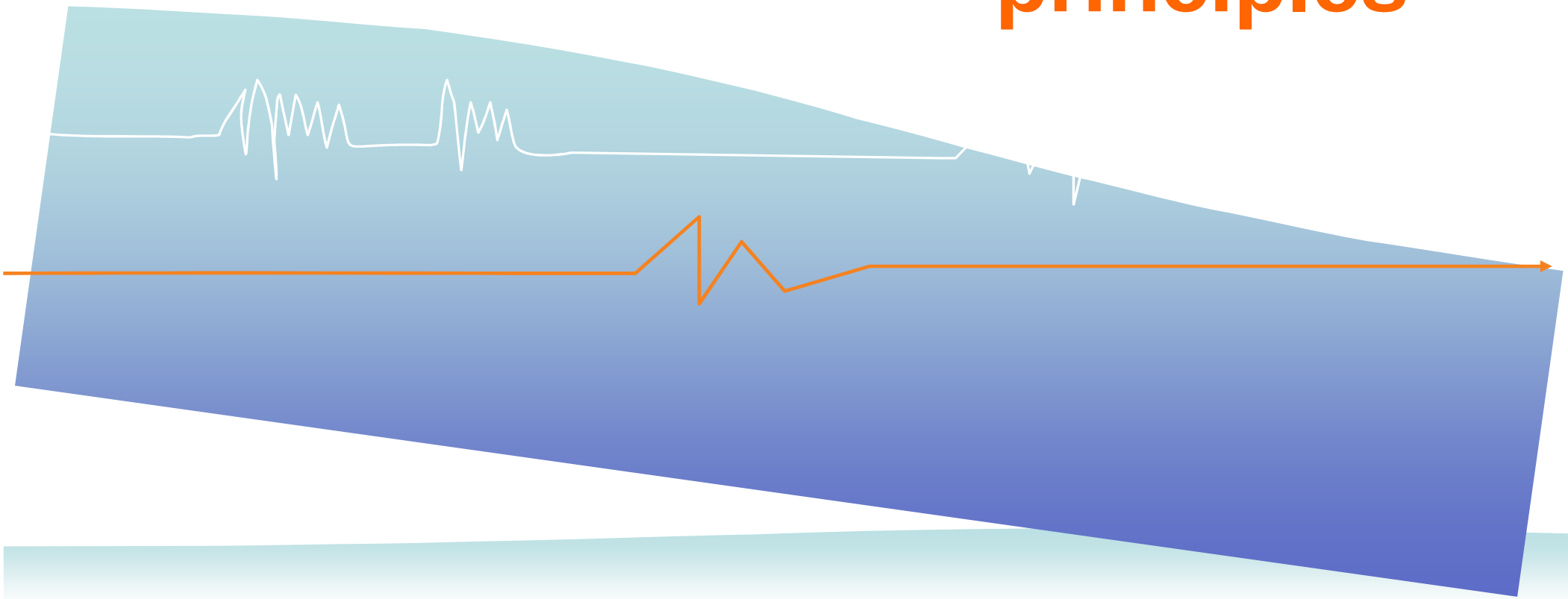
The network of defense contractor Lockheed-Martin was attacked using counterfeit electronic keys. Since the RSA Security network was hacked and the keys to its SecurID tokens were compromised a few months ago, the world has been waiting for the proverbial other shoe to drop. Well, it dropped.

The story continues...

- On light side you stay

CERT.LV

IT security principles

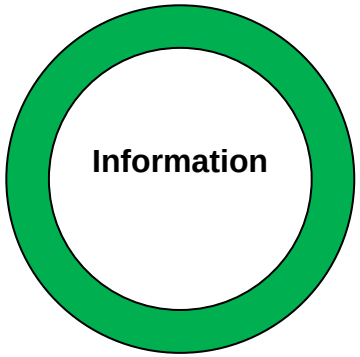


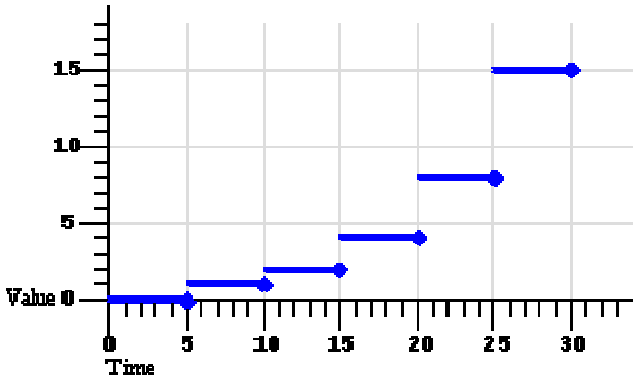
IT security principles

- What is security?

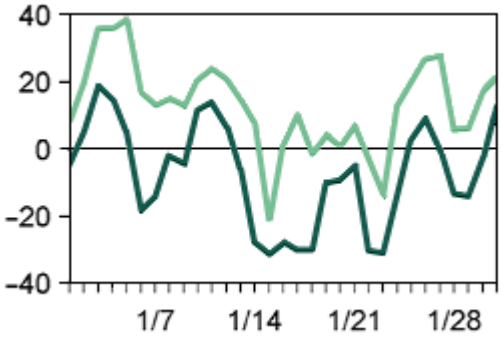
IT security principles

- What is Information Systems and Information Technology security?





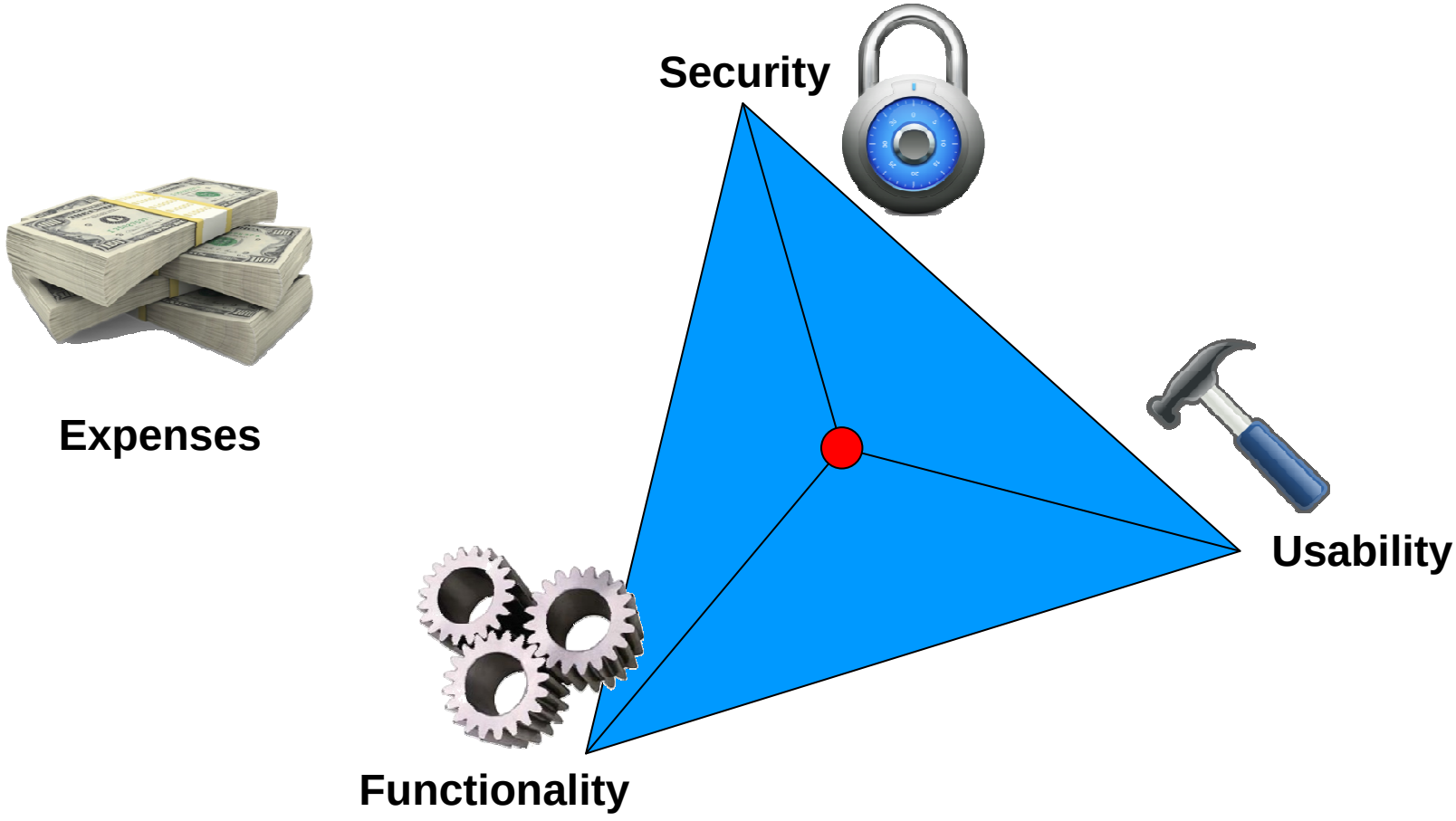
Static / State



Dynamic / Process

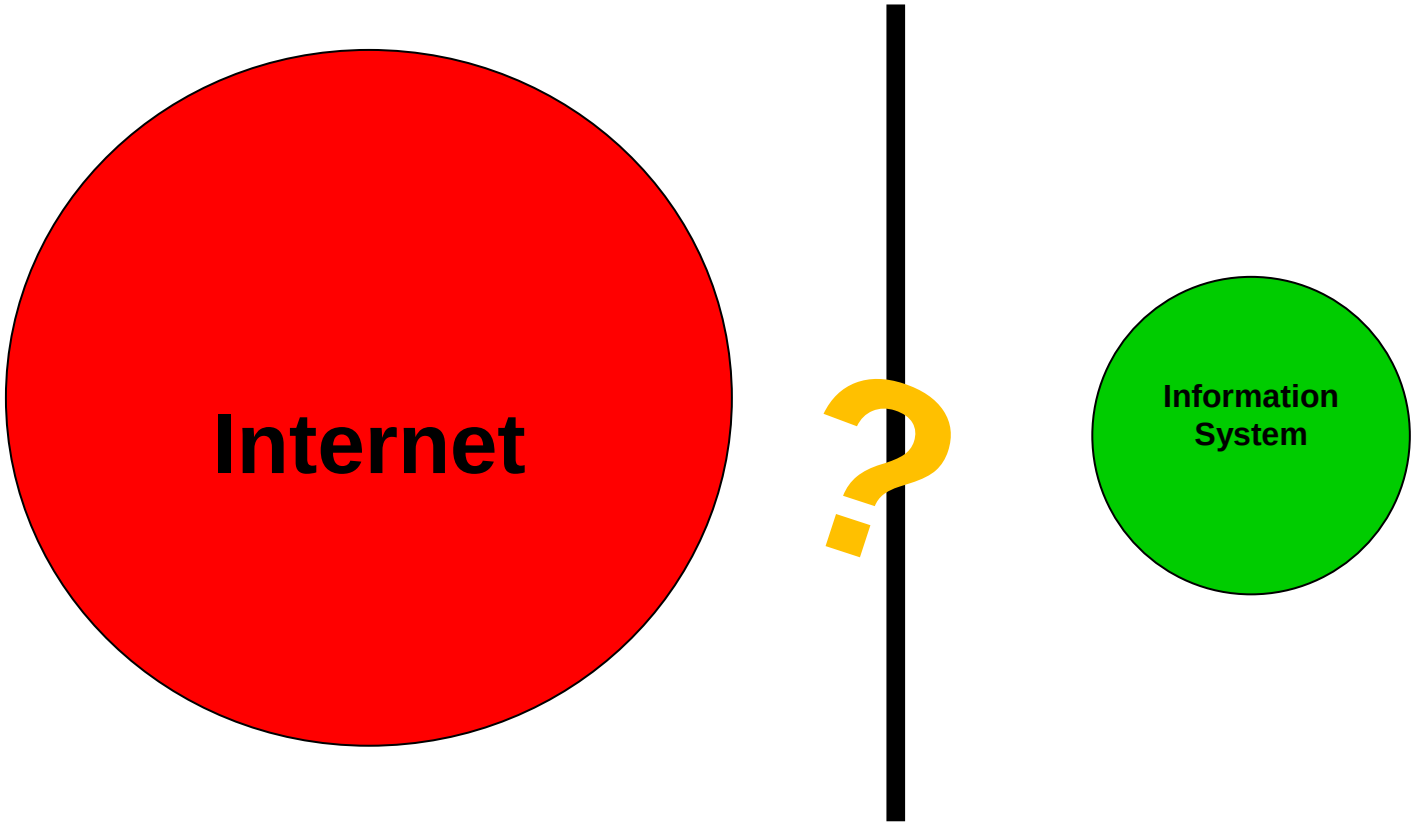
IT security principles

- Security trade-off



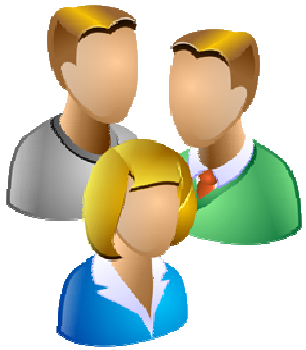
IT security principles

- Information System perimeter



IT security principles

- Information System elements



Users

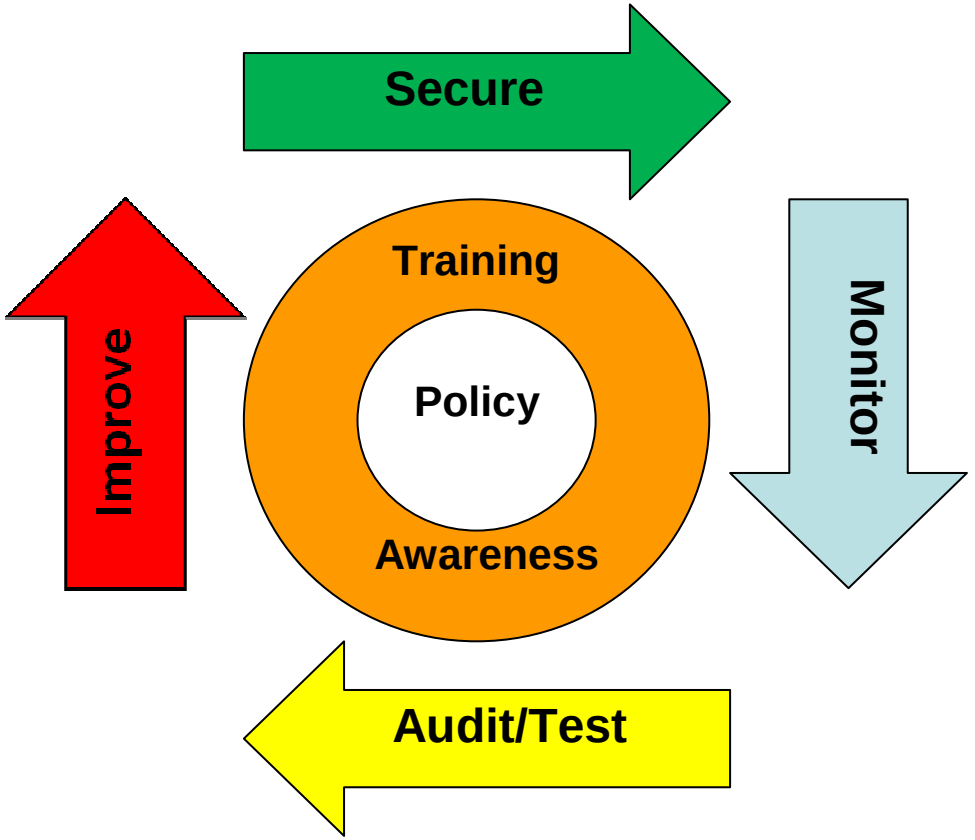
Information

Applications

Infrastructure

IT security principles

- Security lifecycle



IT security principles

- The need for IT security testing

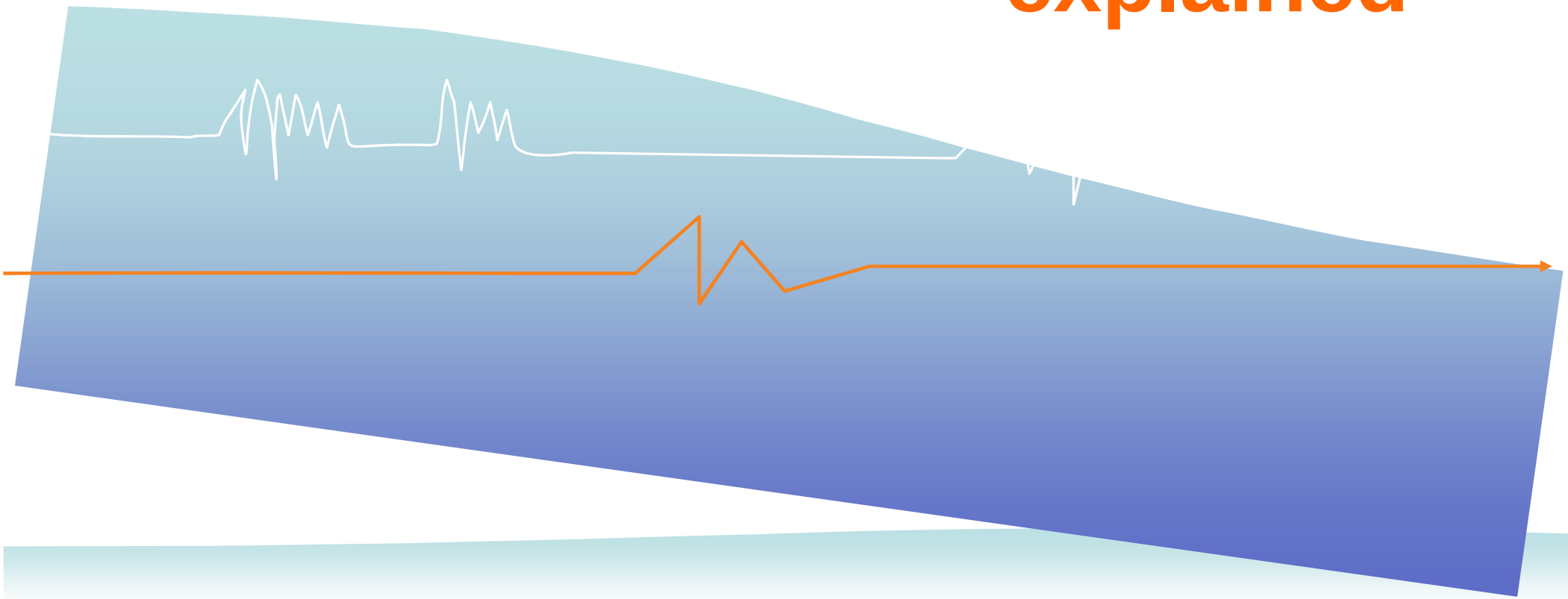
Video on «Cyber Security Evolved»

IT security principles

- So what is security?

CERT.LV

Terminology explained



Terminology explained

w00t

1337

5(R1p7 |<1D|)13

H4XX0r

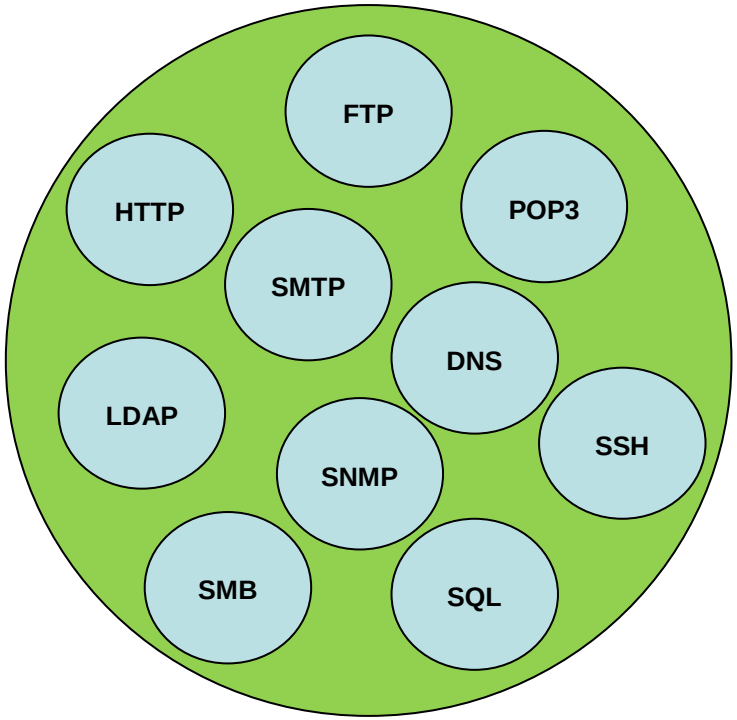
pwned!!!111

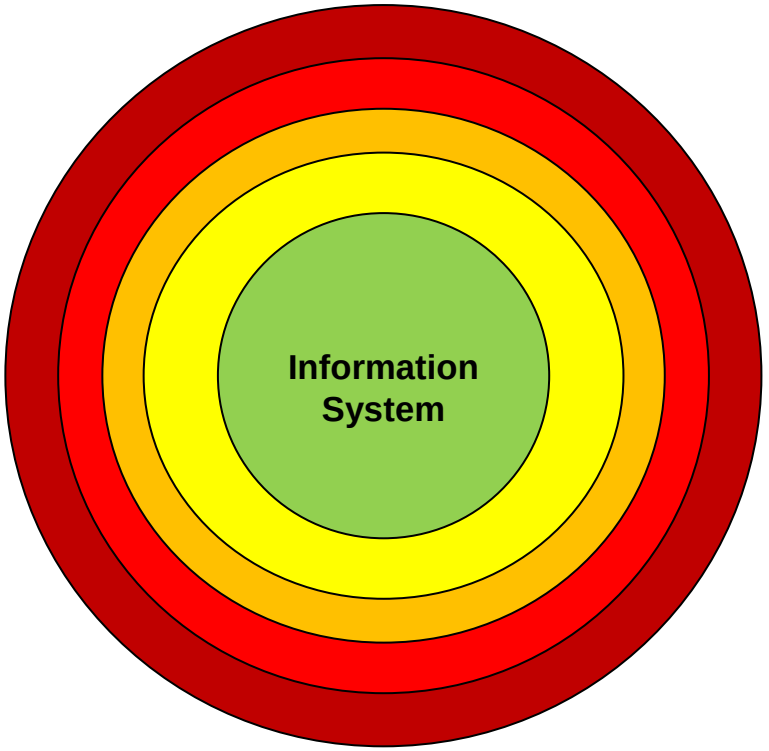
L@m3r

all your base are belong to us

Terminology explained

- Attack surface and defense-in-depth



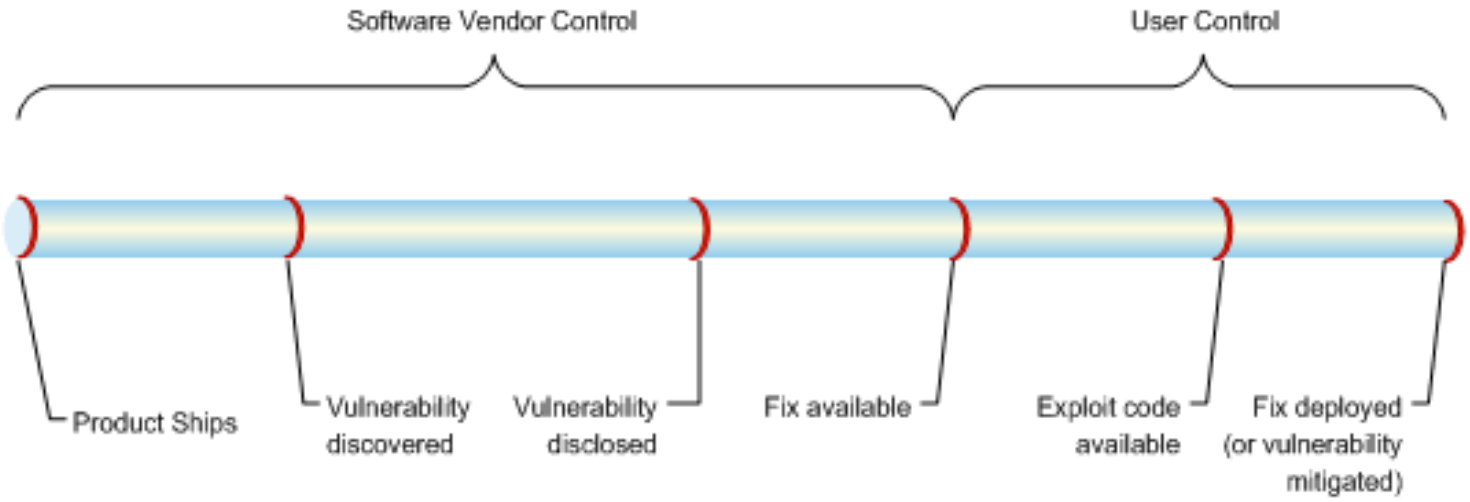


Terminology explained

- Weakness
  - A flaw, that leaves asset vulnerable to attack
- Exposure
  - A point of access to the weakness
- Vulnerability
  - An instance of the exposure of a weakness
- Exploit
  - The act of taking advantage of a vulnerability

Terminology explained

- Vulnerability lifecycle



- 0-Day

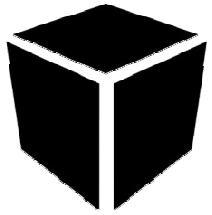
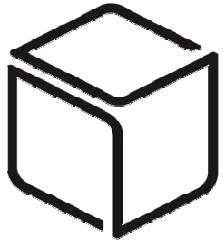
Terminology explained

- Threat
  - Potential event endangering a system
- Risk
  - A probability of threat becoming true
- Risk management
  - Process of risk assessment and analysis
  - Affect on Confidentiality, Integrity, Availability, Accounting
  - Accept, mitigate, eliminate, transfer

Terminology explained

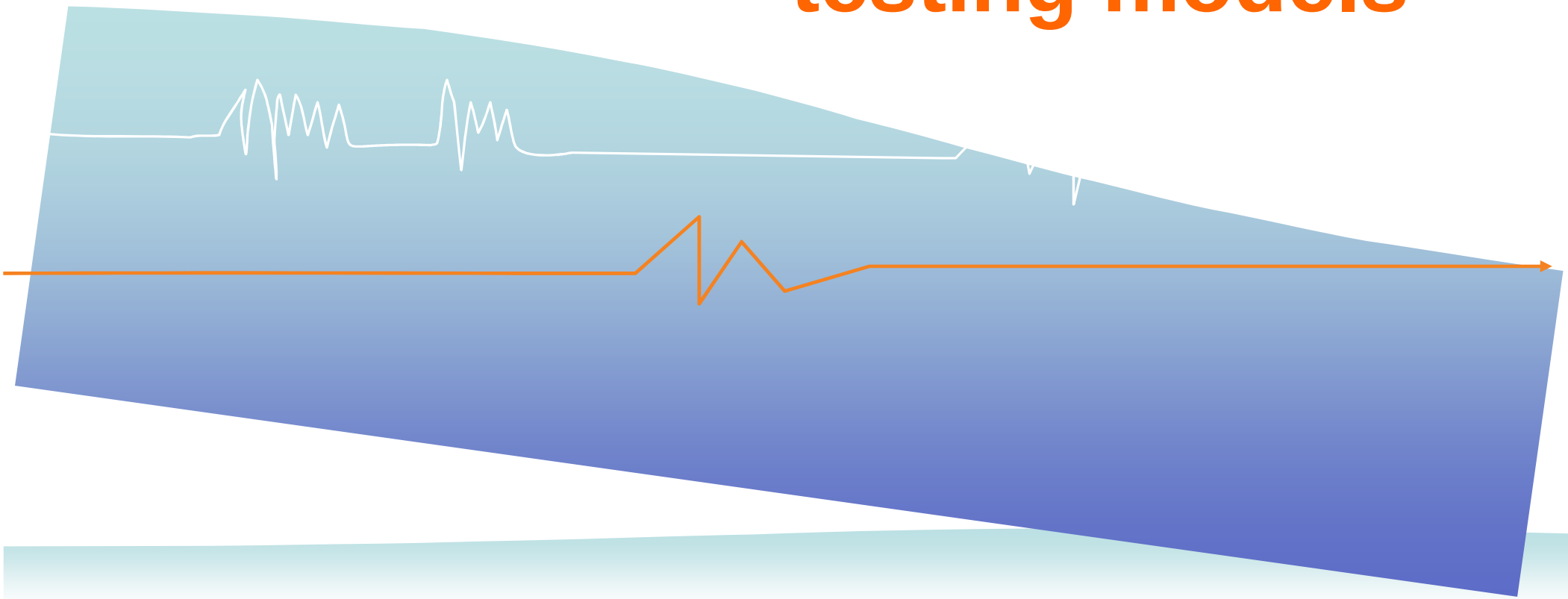
- Types of hackers
  - Hacktivists
  - Black-hat hackers
  - White-hat hackers
  - Grey-hat hackers
  - Suicide hackers

Terminology explained

- Types of system vulnerability tests
  - Black-box 
  - White-box 
  - Grey-box 
  - Announced and unannounced

CERT.LV

Network penetration testing models



Testing methodology

- Applicable standards
  - NIST 800-115
  - EC-Council, CE|H
  - PTES
  - Open Source Security Testing Methodology Manual (OSSTMM)
  - ISO/IEC 17799:2005 and 27000-series
  - Payment Card Industry Data Security Standard (PCI DSS)

Testing methodology

- Accepted penetration testing approach

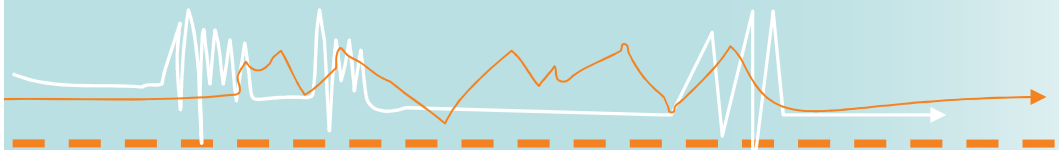
NIST	PTES	CEH
Planning	Pre-engagement Interactions	Reconnaissance
	Intelligence Gathering	
Discovery	Threat Modeling	
	Vulnerability Analysis	Scanning
Attack	Exploitation	Gaining access
	Post Exploitation	Maintaining access
		Clearing tracks
Reporting	Reporting	Reporting

Reporting results

- Outcome and reporting
  - Meets the predefined scope and goals
  - Answers to the stakeholder's questions or provides basis for decision making
  - Methodological, can be recreated or have proof-of-concept
  - Is well formed and understandable to the stakeholders

Reporting results

- Sample structure of a PT report:
  - Executive summary
  - Scope and objectives
  - Summary of findings and recommendations
  - Methodology used and test execution
  - Detailed findings
  - Appendixes: vulnerability reports, scan results and other technical data



CERT.LV

Thank you!

http://www.cert.lv/

cert@cert.lv