clarified security

- we break security to bring clarity -

Penetration Testing The Red Pill

Mehis Hakkaja, Mait Peekma

www.clarifiedsecurity.com

Agenda

- What is security testing, penetration testing (pen-testing)?
- Why pentest? Threat landscape
- Web application attacks
- Social media, social engineering

What we do

- **Pentration testing** (WebApp and Network)

  We break security to bring clarity!

- **Hands-on security trainings**

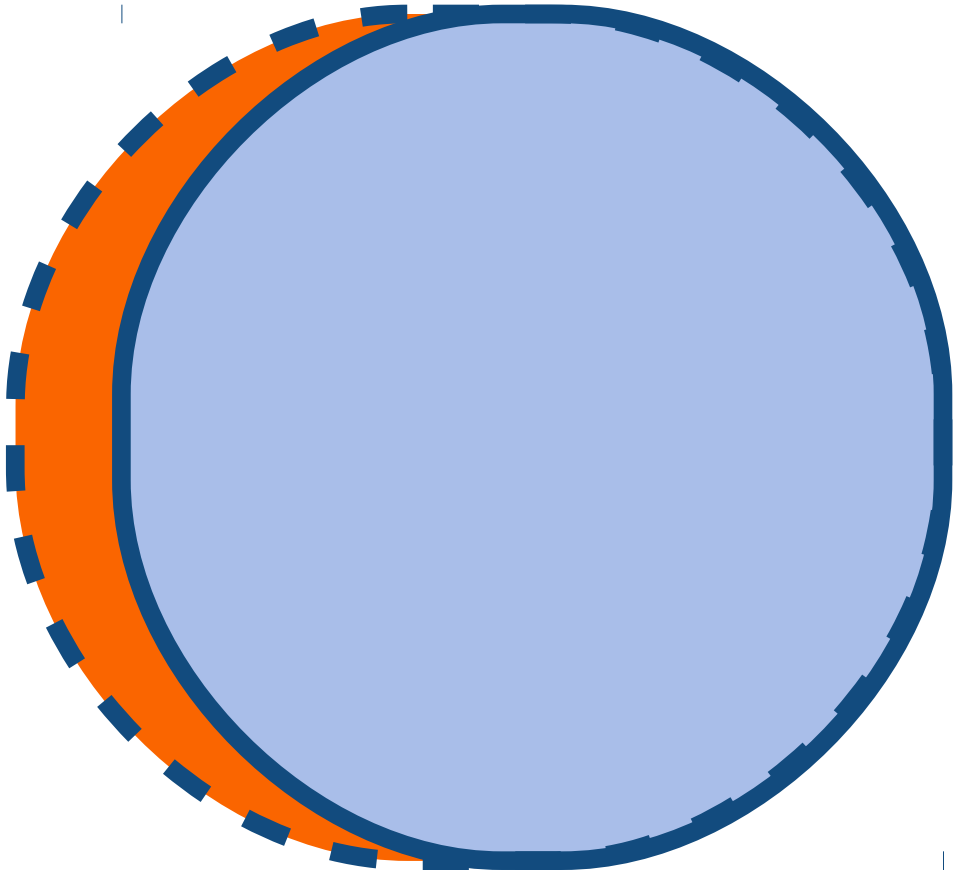
  We teach what we do and know the best!

- **Red Teaming** for large-scale NATO Cyber Defence Exercises (CDX)

  2010 May, "**Baltic Cyber Shield**"

  2012 Mar, "**Locked Shields**"

Bug

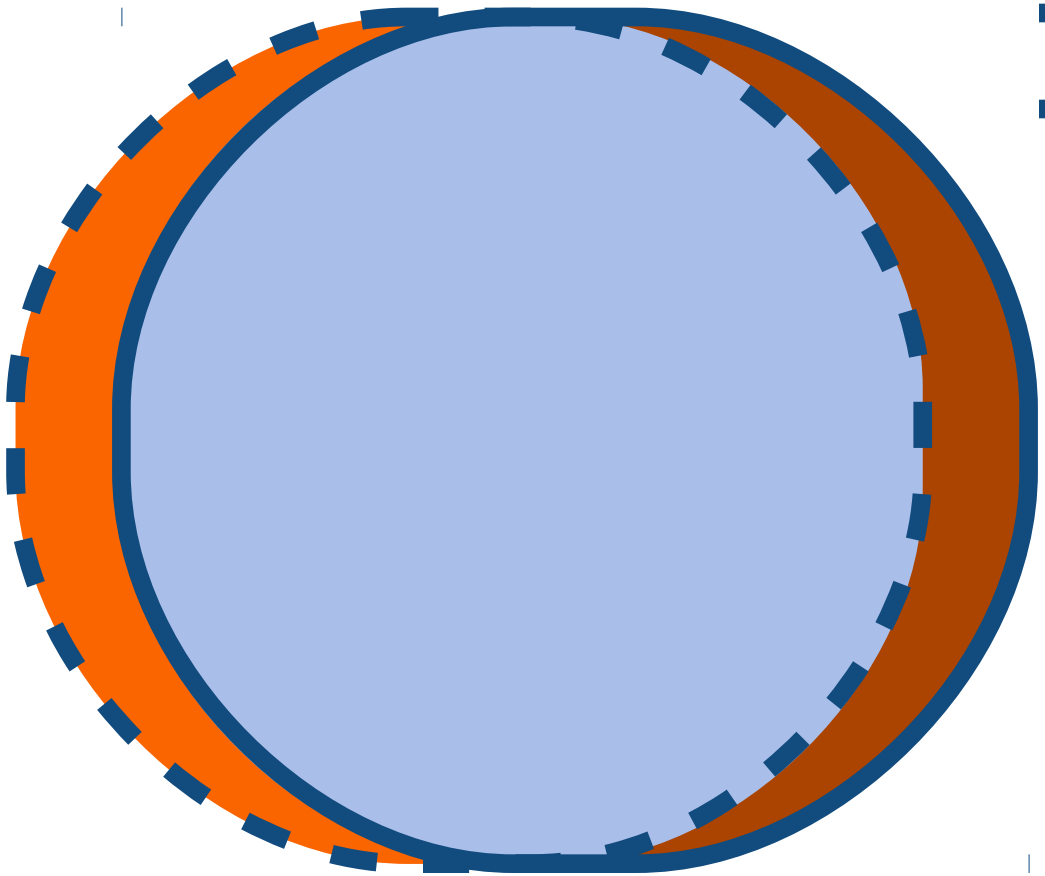


requirements

implementation

bug

Bug, Security Problem



requirements

implementation

bug

security problem

Whittaker, James A. - Thompson, Herbert - „How to Break Software Security“, 2003

Payment

100€ >= -10€

IF remitter_account_balance >= amount

THEN

100€ - (-10€) = 110€

remitter_account_balance =

remitter_account_balance – amount

200€ + (-10€) = 190€

beneficiary_account_balance =

beneficiary_account_balance + amount

Reliable, secure software

Reliable software does
what it is supposed to do.

Secure software does
what it is supposed to do,
and nothing else.

Ivan Arce

Security, penetration test

Security testing is to
find the security risks.

Penetration testing is to
prove the risks can occur.

Penetration test scope may include
information systems, premises, employees.

Why pentest?

- 2nd opinion or outsider look
- regular risk mitigation measure
- expert assessment (e.g. before go Live)
- the only way to know for sure
- to make people understand and believe
- a way of quality assurance

Red vs Blue pill

Reality vs Illusions

Money, espionage, hacktivism

- Cybercrime industrialized ~2003
- Main drive for cybercrime is (financial) gain
- Stolen information translates to money well, esp. in some countries
- Cyber has become a great unproportional weapon
- **Don't get caught unprepared**

Are YOU keeping up?

- Perimeter defense alone is long dead, **networks are soft inside** and attackers know it!
- Patching cycles: **MS "black tuesday"**, 3rd party soft, plugins (PDF reader, Java, Flash...)
- Even if you stay on top of patching, there are **0day** vulnerabilites
- **Client-side attacks** are the most likely ones to get your network compromised
- You may even loose "home field" advantage

Advanced Persistent Threat (APT) =

You either already are or will be owned!

Owned via known vuln...

Metasploit Framework, exploit-db.com, oldapps.com, Google...

http://en.wikipedia.org/wiki/Java_version_history#Java_6_updates

Java v6 Update <=30 (Feb '12) **any browser & OS**

Adobe Flash 11.1.102.55 (Feb '12) **any OS**

Adobe Reader <= 9.3.3 (Jun '10) **many exploits**

Mozilla Firefox <= 3.6.16 (Apr '11) **many exploits**

IE 7 or 8 and MS11-050 (patched 14 Jun '11)

Flashback trojan => 650 000 Apple Mac's infected via **Java** exploit (mostly clickjacking), used to spread via fake flash

SabPub trojan (Backdoor.OSX.SabPub.a) => drive-by **Java** exploit (more targeted & evil), used to spread via MS Word

Advanced Persistent Threat

- Mar 2009 “**GhostNet**” -> Dalai Lama, Tibetan Government-in-Exile,... Ghost RAT (**Poison Ivy**). 1295 infected computers in 103 countries, 397 high value.
- Dec 2009 "**Operation Aurora**" -> 0day in MS IE used as an entry point to exploit Google and at least 20-30 other companies
- Jun 2010 "**Stuxnet**" -> Iran, Siemens SCADA, 4 0days, Windows user-mode and kernel digitally signed rootkits, PLC rootkit, targeting only certain frequency ranges...
- Feb 2011 "**Night Dragon**" -> Starting Nov 2009, attacks against global oil, energy, and petrochemical companies. zwShell RAT, no 0days!

RSA hacked via APT

MAR 2011 "**RSA hacked**" -> Lockheed Martin and others hacked as the result.

- **Spear phishing**, 2 days to a small group of employees
- Attachment "**2011 Recruitment plan.xls**"
- **Adobe Flash 0-day** (CVE-2011-0609) v10.2.154.13
- 1 employee clicks -> **Poison Ivy** RAT installed, game over
- RSA says they **discovered the attack in progress** via detection and monitoring

Back down to earth:
Am I a target?

If not already, you will be owned if:

- you are unlucky and/or **unprepared?**
- someone is **motivated** enough (targeted attacks and random)
- the "**butterfly effect**"

Back to basics

It seems very simple:

Ensure you are not vulnerable:

from outside

from inside

have:

good **monitoring** and **incident response**

Pentesting types

Black box = no prior info

White box = full context and knowledge

Grey box = a mix

Remote (WebApps, public IPs)

On-site (WiFi, LAN, etc.)

Network pentesting

- Typically remote black box pentest of public IP ranges or DMZ servers
- Internal assessments - Internal networks still tend to be soft inside
- Target driven pentests - Could a motivated adversary really do it?

- Security awareness tests - Simple Phishing Toolkit (SPT) shows how phishable your employees are

Web application pentesting based on OWASP ASVS

Typically customers with external Website that contain:
monetary value or goods (e-bank, e-shop)
sensitive information (customer personal data)
key business processes (e-service, meter readings)

Don't forget internal WebApps!

> Buying goods for free - how about a few 40" LCD TVs?
> Accessing or modifying other user's data
> killing front- and backend servers with one single query

WebApp pentesting RoE

Rules of Engagement:

- typical case takes 2 weeks
- main testing conducted on test/pre-live env.
- comparison tests on Live environment
- no intentionally destructive attacks (but weird stuff happens)
- resource intensive queries identified (no DDoS)
- restrictions agreed (source IPs, time restrictions, intensity, etc.)

OWASP

Open Web Application Security Project (OWASP)

Application Security Verification Standard (ASVS)

OWASP Testing Guide

DEMO: Business logic flaw, Cross-site scripting (XSS), Direct Object Reference, SQL injection

ASVS Verification Levels

Level 1: Automated Verification

1A - Dynamic Scan (Partial Automated Verification)

1B - Source Code Scan (Partial Automated Verification)

Level 2: Manual Verification

2A - Security Test (Partial Manual Verification)

2B - Code Review (Partial Manual Verification)

Level 3: Design Verification

Level 4: Internal Verification

Social media

- Social media is "*the* ***Internet and mobile*** *technology based* ***channels of communication*** *in which* ***people share content*** *with each other*" (Financial Times Lexicon, 2011)

- Social media has became a part of our every day life.

- Can offer business advantages, but also substantsial risks

Main risks for businesses

- **Malware**
- **(unintentional) date leakage**
- wasted time, decreased productivity
- "**side-channel**" and targeted attacks (spearhead phishing)
  - privacy and habits (FB, tweet, Tripit...)
- social media and "**social engineering**"

Social engineering toolsets

- SET - Social Engineering Toolkit
- Metasploit, Armitage ...
- SPT - Simple Phishing Toolkit

- The victim only needs to click once and the Game is Over!

- **DEMO**: SET, Armitage

"Social engineering" on steroids

- **abusing trust and features**
  - chat, Like, follow, tweet, short URL, QR code...
  - eg. “village fool” case and facebook bankfraud
- "wildfire" effect (Samy worm, Twitter and hacktivism)
- dissapearing boundaries - "**always-on**" technology, clouds, pads, smartphones, ... corporate vs. personal

Test Responsibly!

Only test the systems that you own or have explicit permission for testing!

(incl ISP, cloud owner)

clarified security

- we break security to bring clarity -

- ✓ Pentesting and technical audits
- ✓ Hands-on security trainings
- ✓ Red Teaming for CDXs
- ✓ Security consulting

www.clarifiedsecurity.com

"There can never be too much of clarity"

Jani Kenttälä - Clarified Networks OY