clarified security

- we break security to bring clarity -

From one click to 0wning your network

(a live hacking demo)

Mehis Hakkaja

CEO/Founder/Owner

mehis@clarifiedsecurity.com

http://linkedin.com/in/mehishakkaja

- **Estonia** - IT solutions that make sense and work
- **Security out of necessity** - "*e-way of life*", too late to turn back
- **Web layer** - the *"glue" & delivery* method
- **"Devil in the details"** – end-point implementations, unique & custom-made solutions **<=** typical places to fail with typical vulnerabilities

Clarified Security OÜ

Estonian pentesting company & practical security trainer,

immersed in the Estonian "IT fairy tale", **validating** its **practical security implementations** since 2011.

"There can never be too much of clarity"
Jani Kenttälä - Clarified Networks OY

Keeping it honest – practical security only

Penetration testing

"We break security to bring clarity"

Do you want the **red** or **blue** pill?

WebApps, Networks, devices/hardware ...

Hands-on security trainings

"We teach what we do and know the best"

over **2000** hrs of: ***WebApp Security***, ***Hands-on Hacking***, ***Secure Logging***

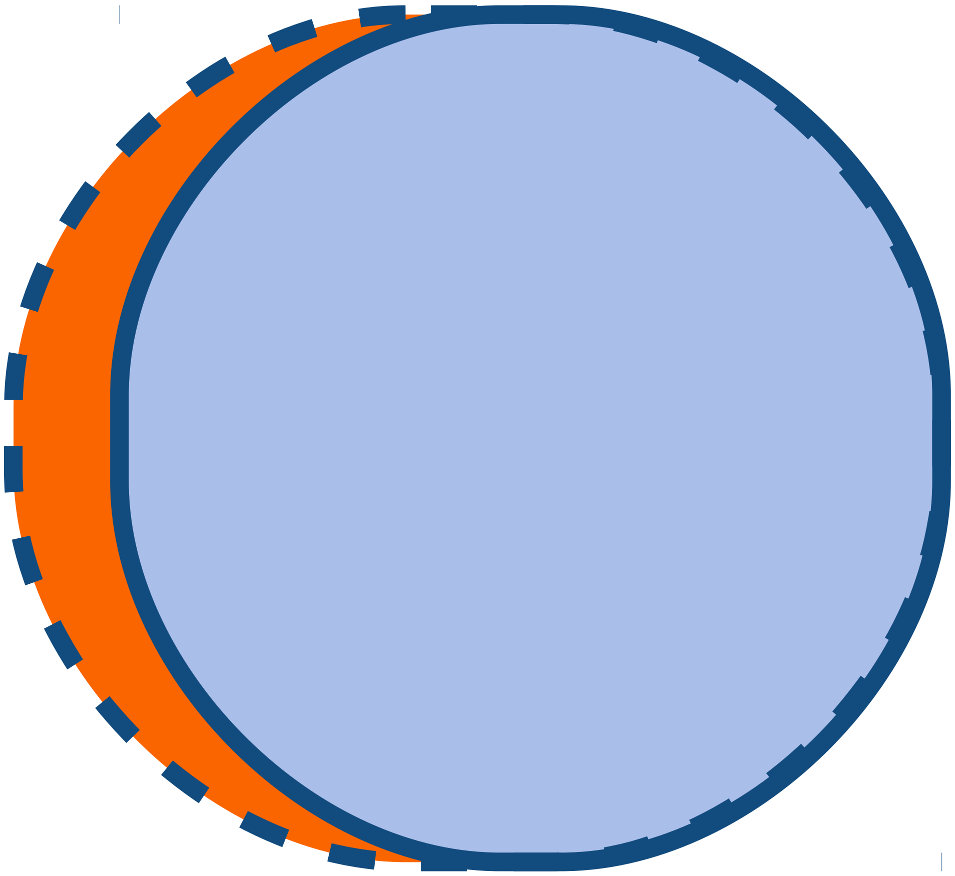
Red Teaming & cyber exercises

NATO CCDCoE large-scale Cyber Defence Exercises (CDX):

2010 May - "**Baltic Cyber Shield**", 6 Blue Teams (***BT***), Red Team (***RT***) size ~20
2012 Mar - "**Locked Shields**", 9 BT, RT ~40
2013 Apr - "**Locked Shields**", 10 BT, RT ~40
2014 May - "**Locked Shields**", 12 BT, RT 50+
2015 Apr - "**Locked Shields**", 15 BT, RT 50+
2016 - "**Locked Shields**", 16...20 BT ?

LOCKED
SHIELDS

Bug

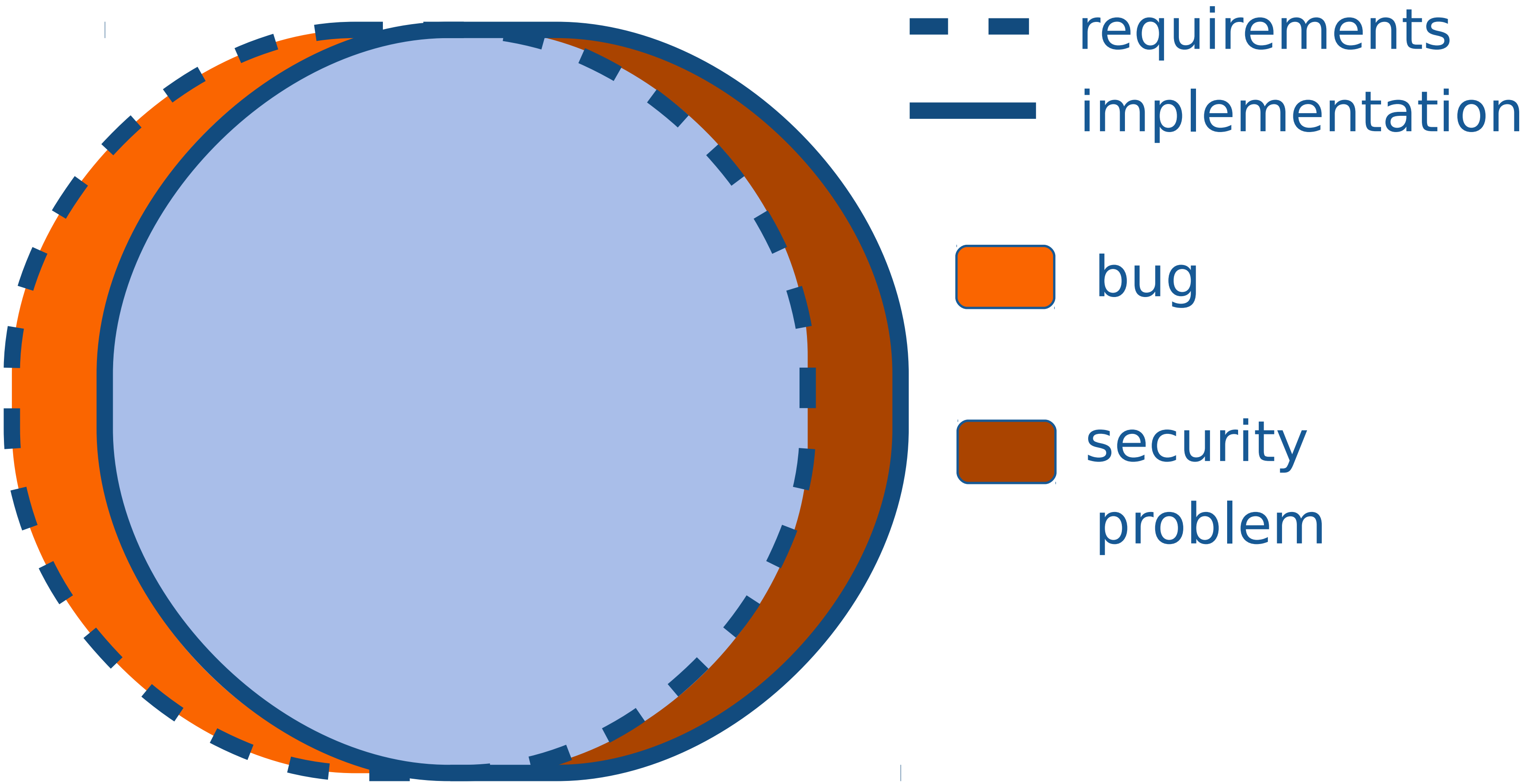


- - requirements

— implementation

🟧 bug

Bug, Security Problem



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

Reliable software does
what it is supposed to do.

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

Ivan Arce

Developers do what they are asked to do …
… examples of someone doing the unexpected

- Business logic implementation errors, gotta love those :)

a) **CHEAP** shopping

banklinks - standard things implemented wrong @ end point (e-shop, e-service, …)

* goodies for the price of 1 item ← is the payment **AMOUNT** actually verified?

dumbuser: 2 bank payment windows open, same shopping cart id, different amounts …

1337 haxor: changes the amount with FF Data Tamper Add-on / Web Proxy tool

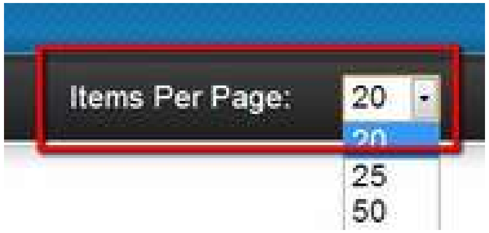
b) **FREE** shopping

* finding a hidden URL & broken access control **=** free LCD TV

c) **MAKING MONEY** while shopping

* try **negative** amounts in a shopping cart with credit card payments

- Missing server-side controls
  - killing the front- & back-end server with only one query :)



Caught up in the mix?

* Your digital life lost in the cloud

(social engineering, social media, cloud, authentication, devices, back-ups...)

www.wired.com/gadgetlab/2012/08/apple-amazon-**mat-honan**-hacking

* By a compromised computer in the IP range you want

krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms

Are YOU keeping up?

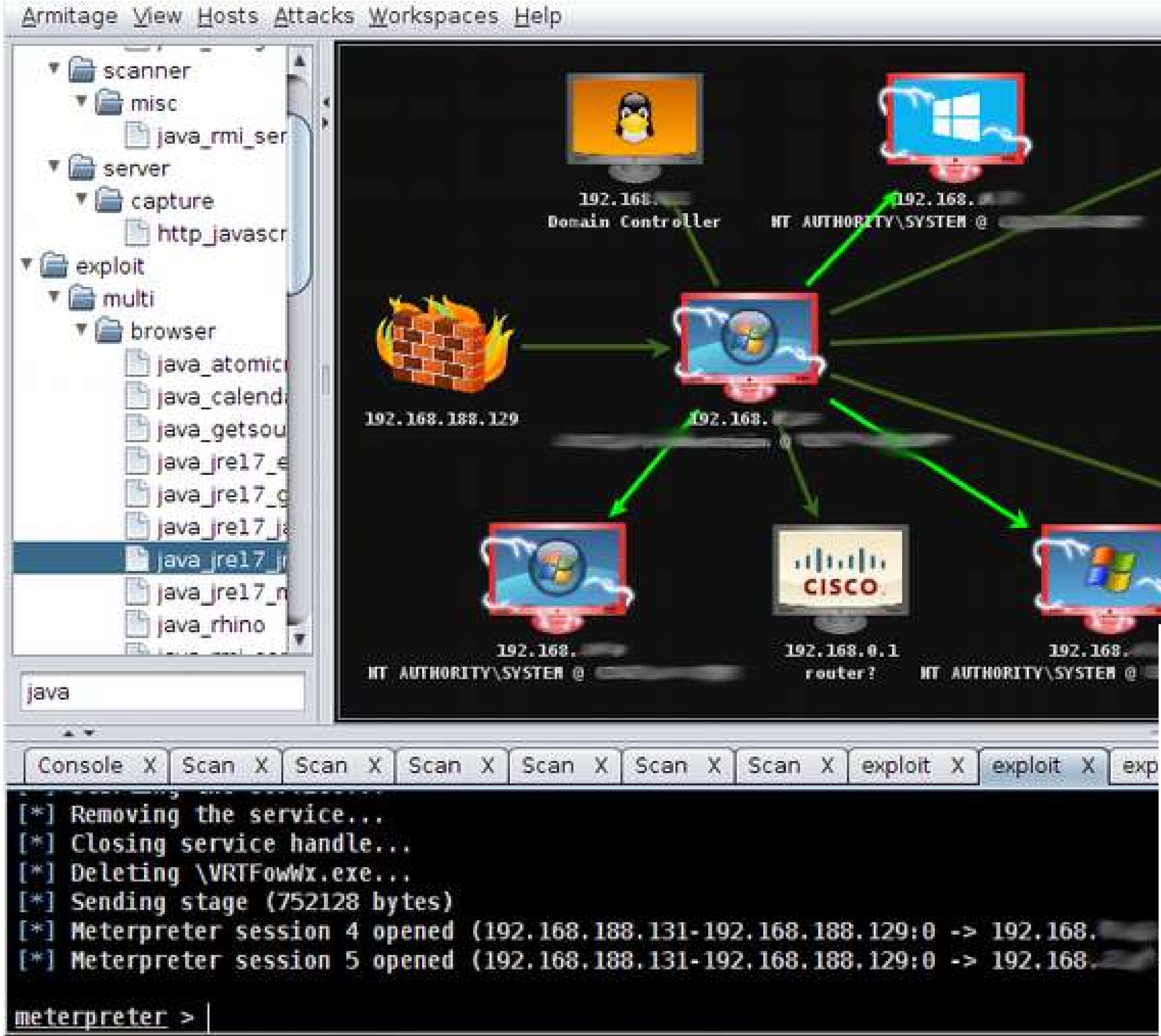
- Perimeter defense alone is long dead, **networks are soft inside** and attackers know it!
- Patching cycles: **MS "black tuesday"**, 3rd party soft, plugins (PDF reader, browser, Java, Flash, ...)
- Even if you stay on top of patching, there are **0-day** vulnerabilites (... and human factor)
- **Client-side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

You either already are or will be owned!

Hacking Demo:

clarified security
- we break security to bring clarity -

Web vulnerability as a vector for taking over your entire network



```
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \VRTFowWx.exe...
[*] Sending stage (752128 bytes)
[*] Meterpreter session 4 opened (192.168.188.131-192.168.188.129:0 -> 192.168.[redacted]
[*] Meterpreter session 5 opened (192.168.188.131-192.168.188.129:0 -> 192.168.[redacted]

meterpreter > |
```

Do not be the weakest lamb in the herd!

- Do the essentials: configure, update, back-up, AV, keep good hygiene *(least privilege*, *passwords*, *personal info*, *social media)*
- Do a bit extra: use encryption, VPN, multi-factor authentication *(e.g. that free Google auth.)*. Keep in mind trusted vs. untrusted devices/networks & activities.
- Be alert: a healthy dose of paranoia is good for you on Internet and especially on social media.
- Have plan B: recovery features, password container, back up data that matters & not *(only)* in the cloud!
- Your employer is trying to do the same thing for you and your workplace – play along, not against the rules :)

clarified security

- we break security to bring clarity -

„What can we break for you?“

facebook.com/clarifiedsec

clarifiedsecurity.com/trainings

Hands on Hacking Essentials (**HOHE**), *2 days*
Hands on Hacking Advanced (**HOHA**), *3 days*
Web Application Security (**WAS**), *4 days*
Logging Security (**LOGSEC**), *1 day*