Security & open source solutions

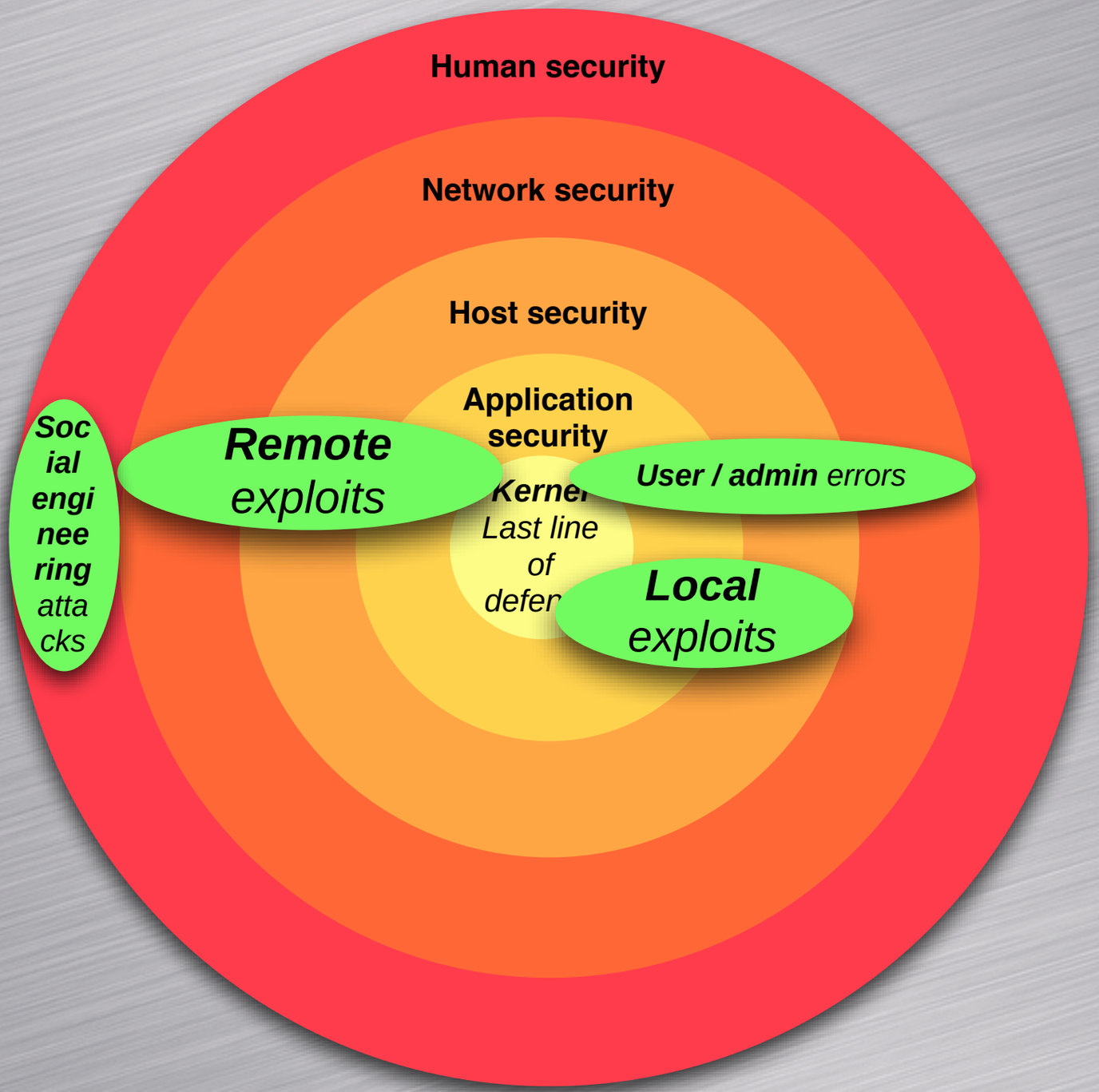
Robert Malmgren
rom@romab.com
+46-708-330378
www.romab.com

Robert Malmgren AB
Trust is good
***control* is better**

Outline of talk

- Description and comparison of standard security controls
  - Linux, FreeBSD, OpenBSD and (Open)Solaris
- Description of advanced/extended features
- Example hardened network service - DNS server
- Fun stuff you could do: log handling, honeypot

Attack surfaces



Important security concepts

- Hardening (*Less is more*)
- Simplicity beats complexity (Kiss)
- Defence in depth (Layered protection)
- There is always someone (***something***) there to get you...
- The threat is ever changing

Security considerations

- Open vs closed source wrt security
- When someone sell you services/products, how do they track the code base they relate to?
- Many closed source products ***silently*** use OSS/freeware component. The important question: *Do they provide updates when bugs are exploited?*

Backdoor to the Linux kernel

```
if((options==(__WCLONE|__WALL)) && (current->uid==0))
    retval = -EINVAL;
```

- Addition to a system call
- Really hard to find by just eyeballing. The one finding the offending code did *not* realize it was a backdoor, later someone uncovered this on a mailing list
- The author did know what he/she did
- *Nice* (?) way to create a backdoor…

Backdoors

- The classic example…
  - Ken Thompsons backdoor in the UNIX C compiler
- Borland Interbase
  - Was found when Borland released it as OSS
  - Tests revealed that the backdoor was available in the commercial version for 7 year!
- ”Netscape engineers are weenies”. Microsoft Front Page Extensions

Quis custodiet ipsos custodes?

Operating systems features

- Standard file protection
- Standard process execution environment protection
- Standard user protection
- Standard network protection
  - Additional network security features: built in filtering

Slick security features

- FreeBSD portaudit(1)
  - makes sure you're always up to date

```
rot13# portaudit -F
auditfile.tbz                                 100% of   39 kB   38 kBps
New database installed.
rot13# portaudit
0 problem(s) in your installed packages found.
```

- Check all your systems from a central point

```
rot13# ssh some_remote_host pkg_info | awk '{ print $1 }' | xargs portaudit
```

Slick security features

- Lock downs / Virtualizations
  - Unix generic - `chroot(8)`
  - FreeBSD - `jail(8)`
  - Open/NetBSD - `systrace(8)`
  - Linux - `uml, xen, OpenVZ,VMWare`
  - Solaris - `zones`

Slick security features

- Solaris capabilities / privileges
  - Fine grained authorization - Better than the binary `root` vs *user* separation
  - Enables removal of setuid
  - Analyze applications need of capability with `ppriv`

Advanced, really slick security controls

- SELinux* & FreeBSD**
  - MAC, MLS, Biba
  - Type Enforcement
  - Existing templates (policies), policy test tools
- Grsecurity / Apparmor
- Exec shield

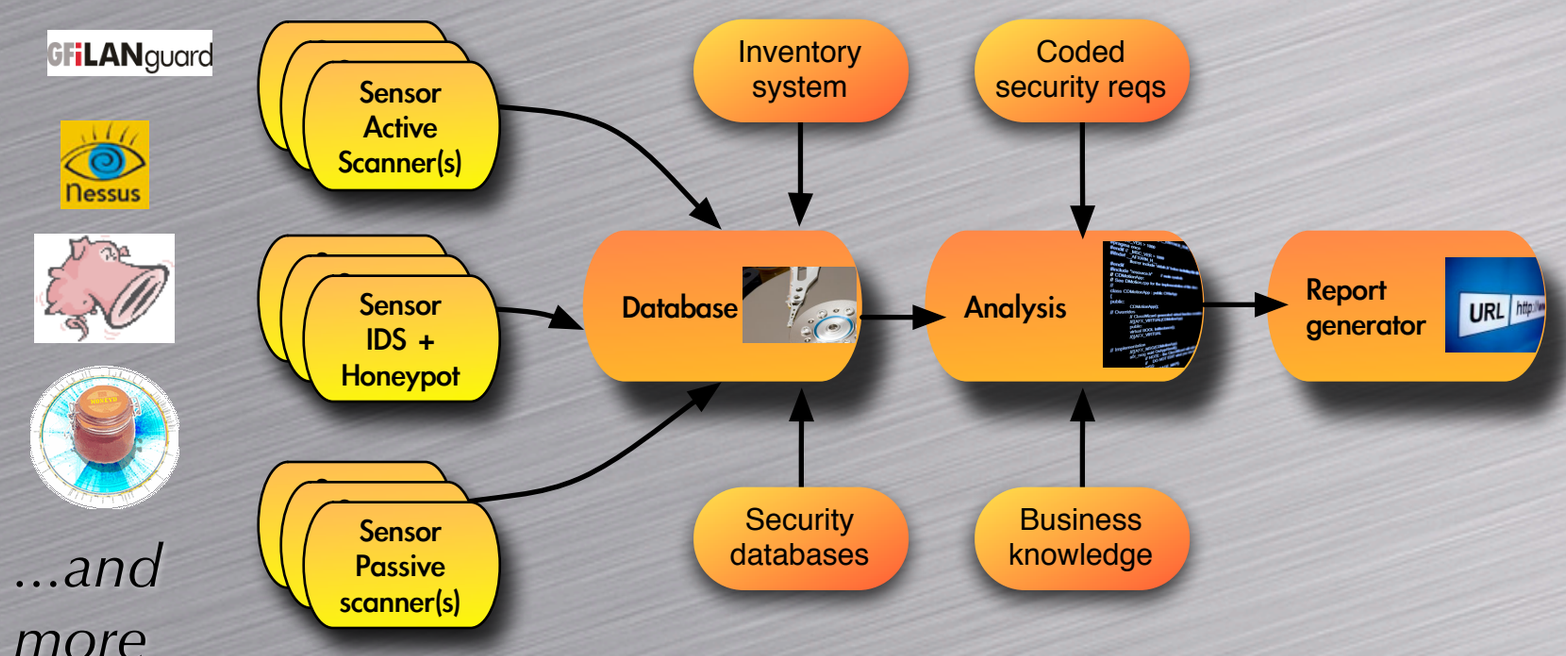
* http://www.nsa.gov/selinux/
** http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mac.html

Ideas for security solutions

- Automated, inhouse security checker
- Secured DNS server
- Honeypot
- Centralized log server

Robert Malmgren AB
Trust is good
***control* is better**

Autohack style security / compliance checker



Top management compliance reports

Mid/low management status reports

Technical experts detailed reports

Original data for (non) security tests and reports

Internal honeypots

- Attach honeypots to strategical places on the internal network
- `Honeyd` can emulate a single machine or subnets of machines
  - IP stacks
  - Network services

```
bind source ip = 192.168.0.0/16 10.0.0.5 cisco
bind source ip = 10.0.0.0/8 10.0.0.5 juniper
```

Internal honeypots

- Can be great *early warning component* (in a larger security solution)
- Good use of old (*little used*) hardware which is too limited to be useful for other functions (e.g. IDS, firewall, proxies) that requires computing power

Secured DNS server

- Based on OpenBSD + bind
  - Hardened OS dist
- Have several partitions in /var

```
A /dev/wd0a /                    ffs rw,softdep 1 1
  /dev/wd0e /home                ffs rw,nodev,nosuid,softdep,noexec 1 2
  /dev/wd0d /tmp                 ffs rw,nodev,nosuid,softdep,noexec 1 2
  /dev/wd0f /usr                 ffs rw,nodev,softdep 1 2
  /dev/wd0k /var                 ffs rw,nodev,nosuid,softdep,noexec 1 2
  /dev/wd0g /var/local           ffs ro,nodev,nosuid 1 2
B /dev/wd0h /var/local/named     ffs ro,nodev,nosuid,noexec 1 2
  /dev/wd0i /var/local/named/bin ffs ro,nodev,nosuid 1 2
C /dev/wd0j /var/local/named/tmp ffs rw,nodev,nosuid,noexec 1 2
  /dev/wd0l /var/log             ffs rw,nodev,nosuid,noexec,softdep 1 2
D /dev/wd0b /var/local/named/dev/ mfs union,rw,nosuid,noexec
  /dev/wd0b /var/local/named/tmp/ mfs union,rw,nosuid,noexec
```

Secured DNS server

- Run bind with chroot + low priv user

```
named -t /var/local/named/ -u named
```

- Use systrace to tighten down what bind can do

```
systrace -i -a -d /root/.systrace/ named -t
/var/local/named/ -u named
```

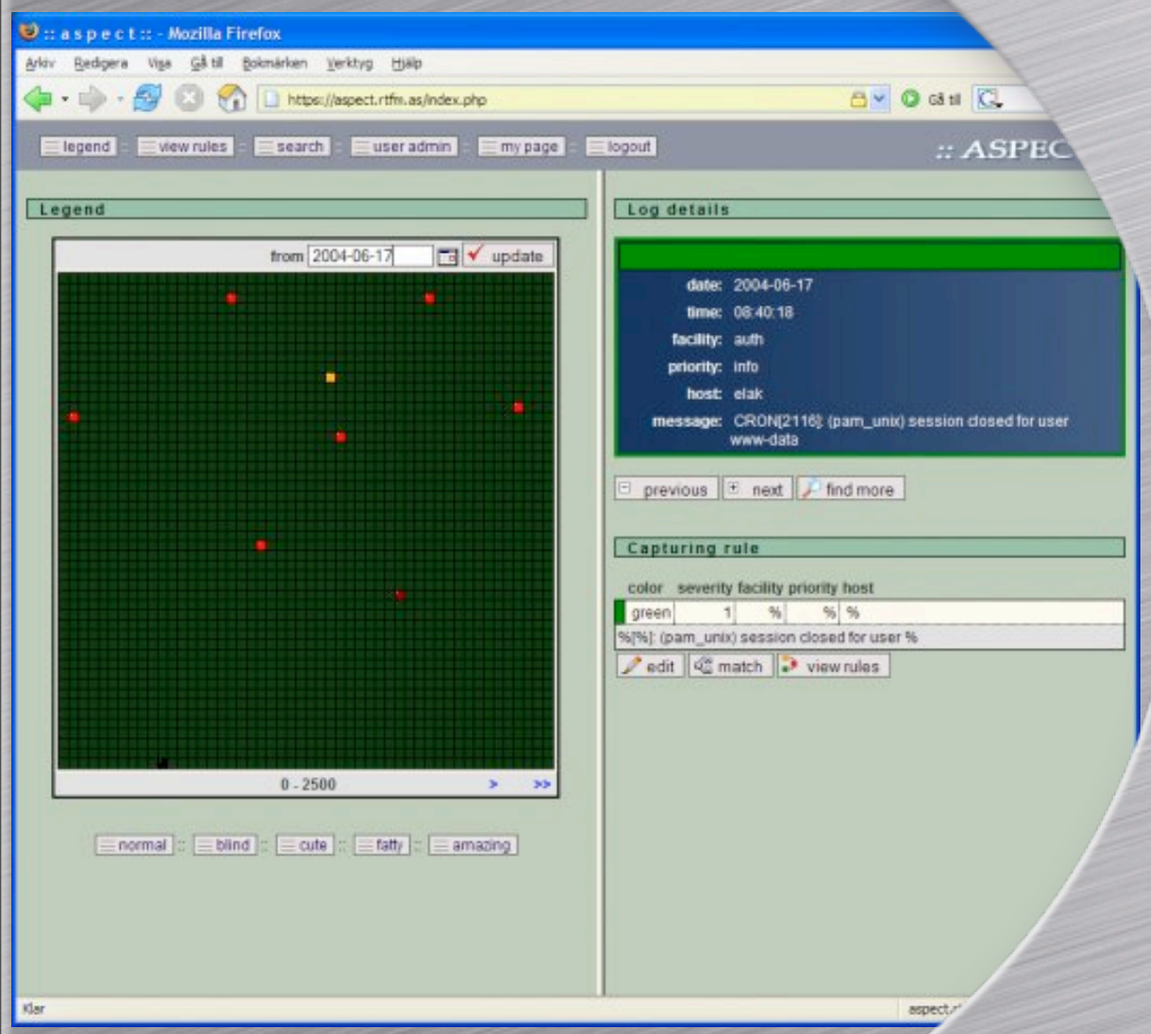
- Create systrace policy by using *systrace* ***-A*** *named* ***...***

- Edit systrace policy to be more restrictive than created by wizard

Secured DNS server

- Enable NTP for time synchronization
- Use SSH/Kerberos for remote admin
- Setup local firewall with `pf`
- Patch and update frequently

Log handling



- Aspect tool for better ***manageability*** of logs
- Tool to visually inspect syslog entries
- Built on LAMP concept

Log handling

- syslog-ng / msyslog
  - TCP based loggning
  - signatures
  - Filtering / script possibilities

```
bind source ip = 192.168.0.0/16 10.0.0.5 cisco
bind source ip = 10.0.0.0/8 10.0.0.5 juniper
```

Cool distros

- Backtrack
- Pentoo
- VMWares virtual appliances
- OPHCrack Live-CD

Summary

- Many tools exist for creation of good / cool security solutions
  - Transparance for business if they are proprietary or OSS solutions
- Important to have good, mandatory, procedures for downloading and installing OSS (*and* other software)
- Create complete solutions, enhance existing solutions or just pick a single function that is nice to have/use

FreeBSD säkerhet

www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/securing-freebsd.html

OpenBSD säkerhetsutökningar

www.openbsd.org/

Linux kernel säkerhetsutökningar

www.grsecurity.net
www.nsa.gov/selinux

Honungsfällor

www.honeyd.org/

Logghantering

aspect.sourceforge.net

www.balabit.com/products/syslog_ng/

Virtuella appliance

www.vmware.com/vmtn/appliances/directory/

OPHCrack Live-CD

ophcrack.sourceforge.net/