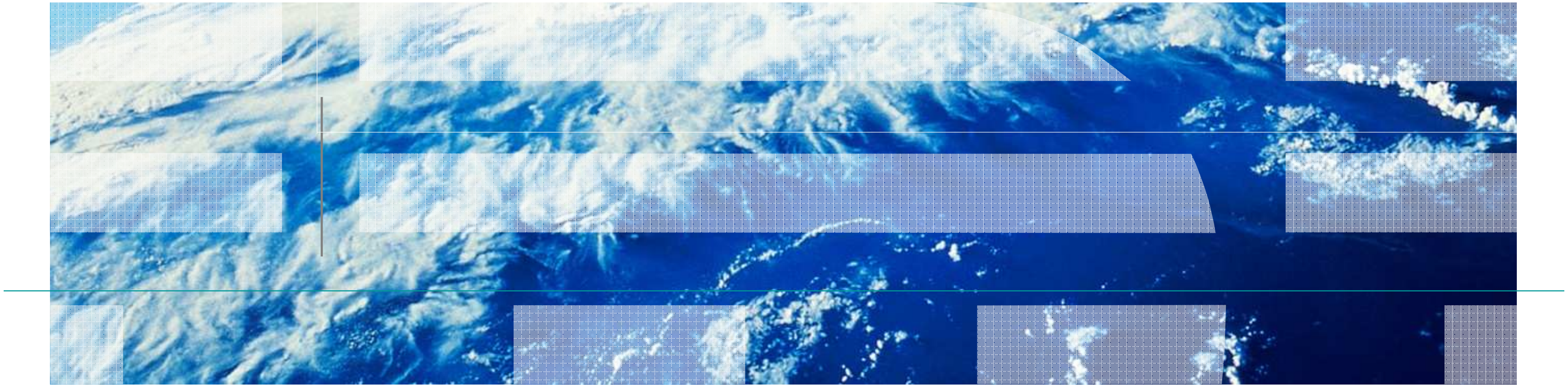
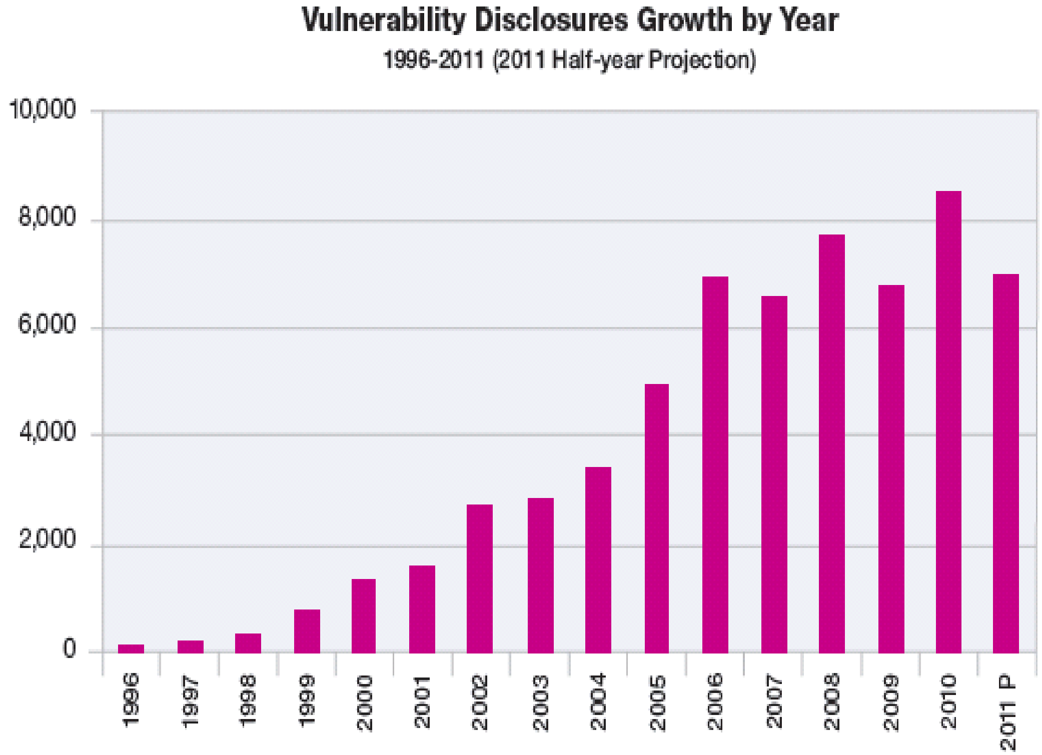
Application security tests

Simone Riccetti
EMEA PSS Security Services



Sistemi in continua evoluzione

- Complessità
- Integrazione
- Estensibilità
- Connettività



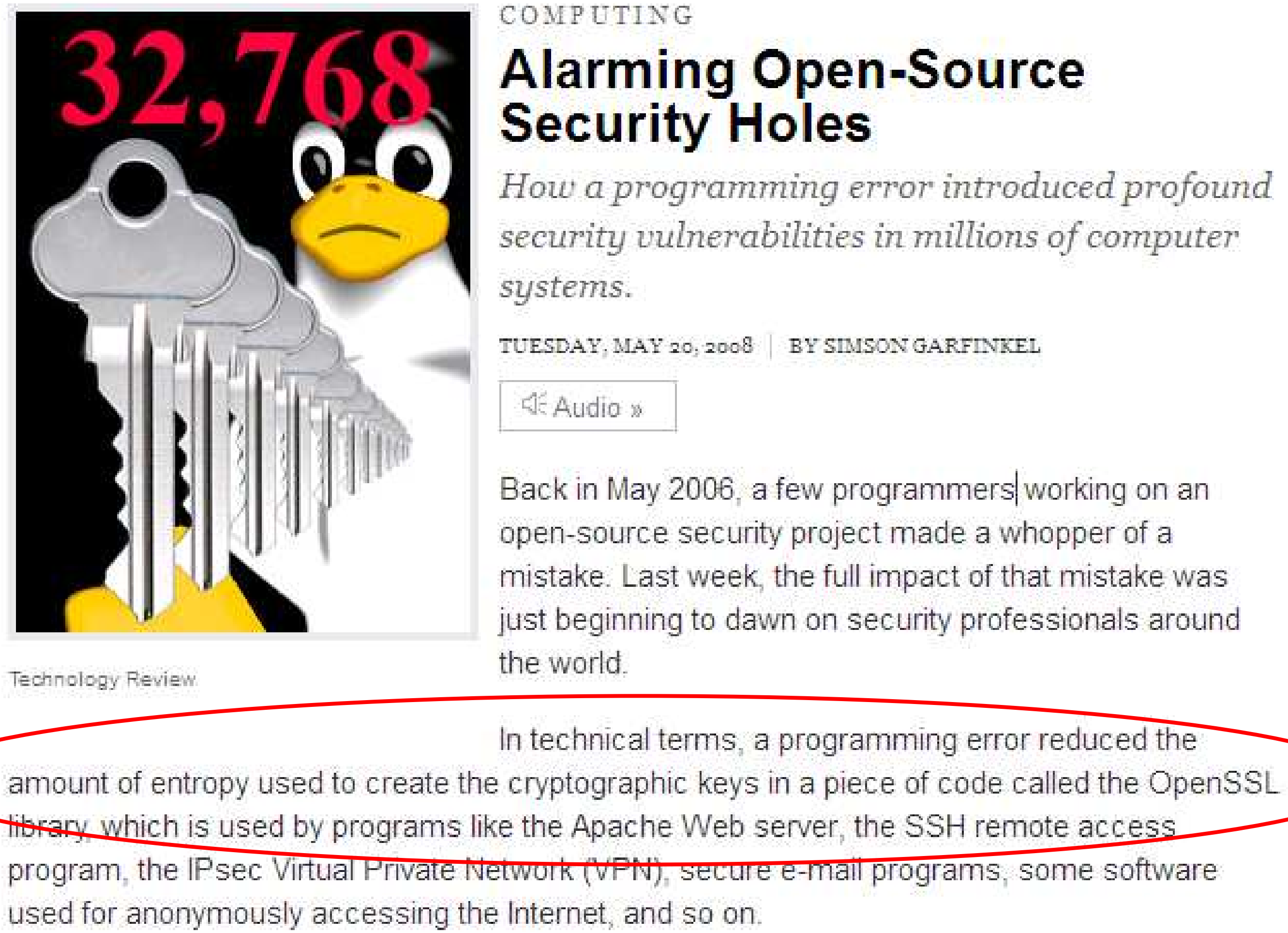
Perché la sicurezza del codice è così importante?

La maggior parte dei buchi di sicurezza del software non sono sfruttati in modo diretto da utenti malintenzionati, ma sono piuttosto sfruttati per errore da altri programmi o componenti, causando effetti imprevedibili che degradano la sicurezza e la qualità delle applicazioni.

Un esempio semplice….Buffer overflow foo

```
 void func(void)
{
                int i;
                char buffer[256];
        for(i=0;i<512;i++)
                        buffer[i]='A';
                return;
}
```

Non tutte le vulnerabilità sono facilmente individuabili….



Technology Review

COMPUTING

Alarming Open-Source Security Holes

How a programming error introduced profound security vulnerabilities in millions of computer systems.

TUESDAY, MAY 20, 2008 | BY SIMSON GARFINKEL

Audio »

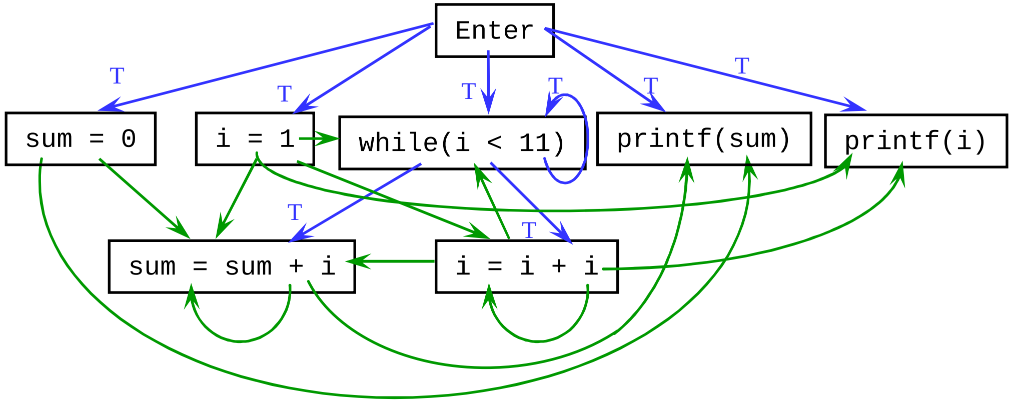
Back in May 2006, a few programmers working on an open-source security project made a whopper of a mistake. Last week, the full impact of that mistake was just beginning to dawn on security professionals around the world.

In technical terms, a programming error reduced the amount of entropy used to create the cryptographic keys in a piece of code called the OpenSSL library, which is used by programs like the Apache Web server, the SSH remote access program, the IPsec Virtual Private Network (VPN), secure e-mail programs, some software used for anonymously accessing the Internet, and so on.

http://www.technologyreview.com

Modeling e complessità

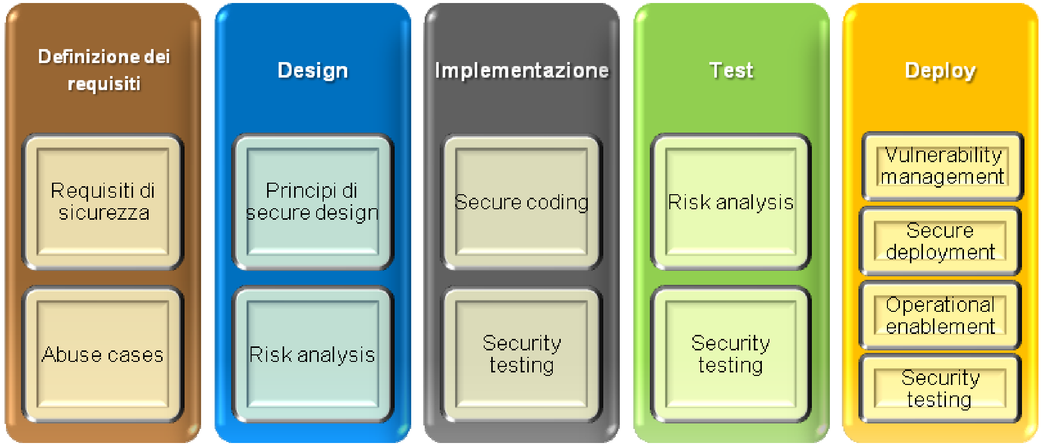
```
int main()
{
   int sum = 0;
   int i = 1;
   while (i < 11) {
       sum = sum + i;
       i = i + 1;
   }
   printf(“%d\n”,sum);
   printf(“%d\n”,i);
}
```



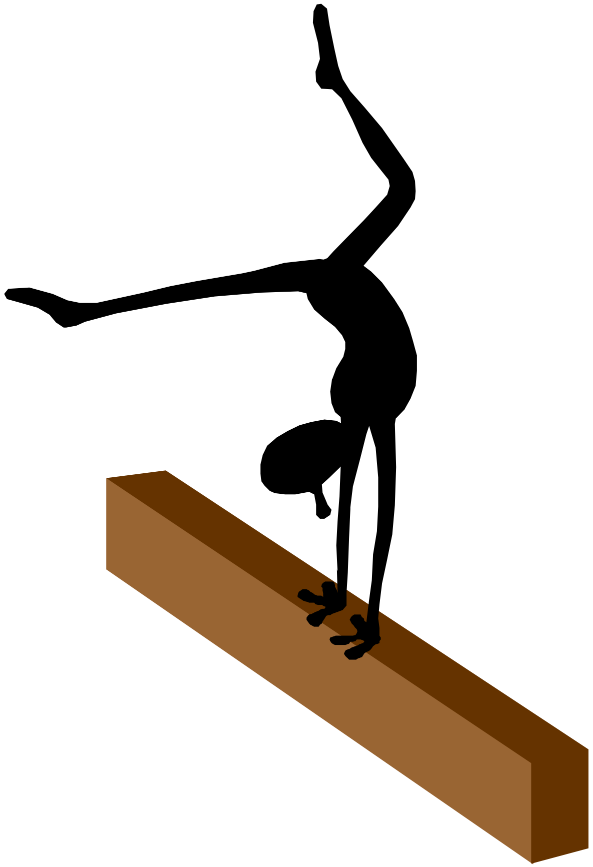
Metodologie e tecniche di test disponibili

- Dynamic analysis
  - Penetration test
  - Users priviledge escalation test
  - Denial of service
- Non repudiation testing
- Failure testing
- Cryptographic validation testing
- Privacy and Confidential testing
- Software security unit test
- Software security regression test
- Static analysis
- altri?

Che strategia di test adottare?



Che approccio adottare?

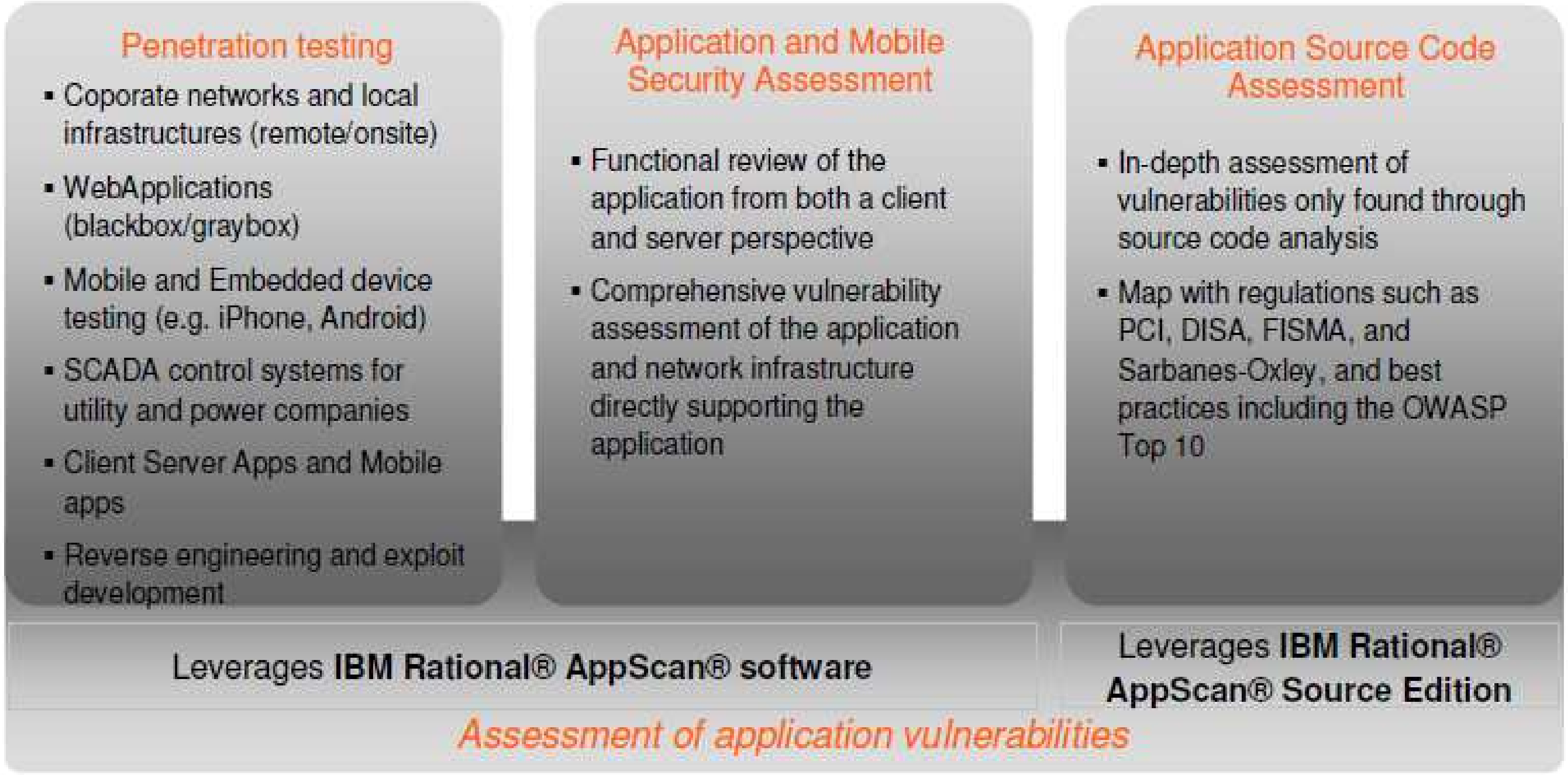


The Balancing Act

Dipende…

- Tipo di applicazione?
- Numero di KLOC?
- Tecnologie e framework?
- Prospettiva?
- Security skills
- Tipo di vulnerabilità che voglio individuare
- Organizzazione
- …..

Professional Security Services – Application security



Penetration testing

- Coporate networks and local infrastructures (remote/onsite)
- WebApplications (blackbox/graybox)
- Mobile and Embedded device testing (e.g. iPhone, Android)
- SCADA control systems for utility and power companies
- Client Server Apps and Mobile apps
- Reverse engineering and exploit development

Application and Mobile Security Assessment

- Functional review of the application from both a client and server perspective
- Comprehensive vulnerability assessment of the application and network infrastructure directly supporting the application

Application Source Code Assessment

- In-depth assessment of vulnerabilities only found through source code analysis
- Map with regulations such as PCI, DISA, FISMA, and Sarbanes-Oxley, and best practices including the OWASP Top 10

Leverages **IBM Rational® AppScan® software**

Leverages **IBM Rational® AppScan® Source Edition**

Assessment of application vulnerabilities

Grazie!

Simone.riccetti@it.ibm.com