Code & Money – the source of all evil!

17 May, 2008

John Fitzgerald
&
Tomasz Miklas

What are you going to learn today?

- What the CIOs and CISOs of organizations are hearing and seeing today
- How they are responding
- Where the opportunity is for you

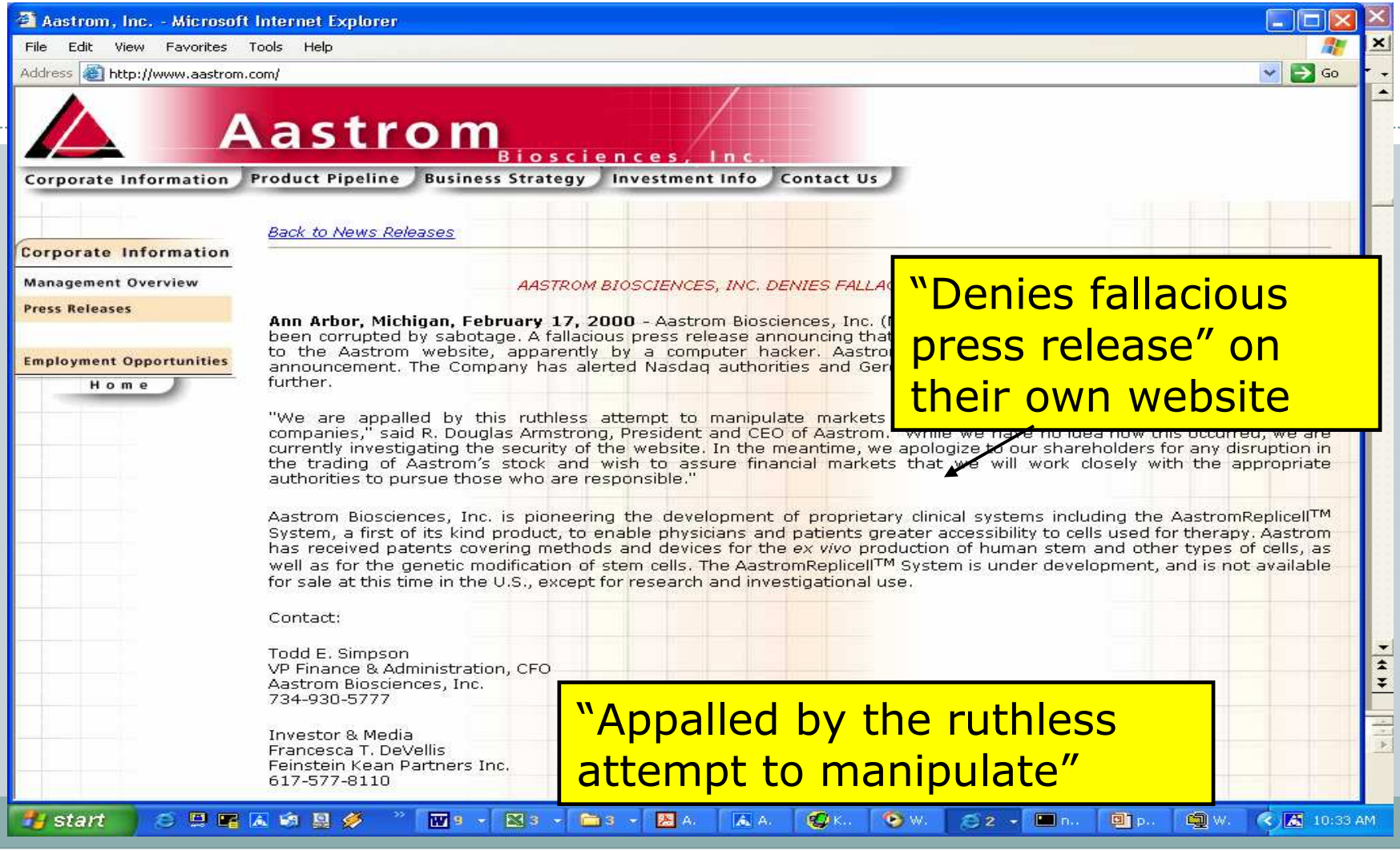
A Massive Financial Cyber Crime Wave

- The FBI is getting “more than one new cyber extortion case every day.”
- Online Broker e-Trade lost $18 million
- Bankers tell of 400% increases in cyber fraud from 2005 to 2006
- Organized crime groups in Eastern Europe recruit hackers for their cyber crime “business”
- Asian criminals coming on line.

How do they make money?

- Identity theft for stealing bank balances
- Credit card fraud
- Extortion
- Spam from zombies
- Unauthorized trades to pump&dump stocks
- Spyware
- Web defacement

Web Defacements and Changing "Official Information"



What do the people doing this look like?

Alexey Ivanov

Vasiliy Gorshkov

- Stole data from ecommerce sites using Microsoft IIS
- Threatened to disclose customers' credit card data
- Did disclose when the first victim refused
- $160,000 dollars each instance
- "They threatened to killed my parents"
- Pat Morrissey (US Secret Service): "Any organized crime group that is not using this technique should be sued for malpractice."

Why should we even worry?

- Terrorists raise money for bombs using the same techniques that organized crime uses to raise money
- FBI found bank's stolen money (through cyber fraud) "ended up in an account used by the terrorists to buy bombs."

Terrorists Rely On Cybercrime….

Imam Samudra, the "Bali Bomber" on death row in Indonesia

In his autobiography Samudra writes, "If hacking is successful, get ready to gain windfall income for just 3 to 6 hours of work, greater than the income a policeman earns in 6 months of work. But, please do not do that for money alone! I want to motivate the youth and Moslem men who are granted perfect mind by Allah; I want America and its cronies to be crushed in all aspects."

There Is A New Target?

- System software has become more secure
- Perimeter protection is tuned for system attacks
- Attackers discovered applications are vulnerable:
  - Back-up products
  - Anti-virus products

Why Applications Are A New Targets

- Data is the goal; applications provide direct access to sensitive data
- Most organizations do not effectively patch applications
- The number of vulnerabilities is enormous!

What do we understand by “code quality”?

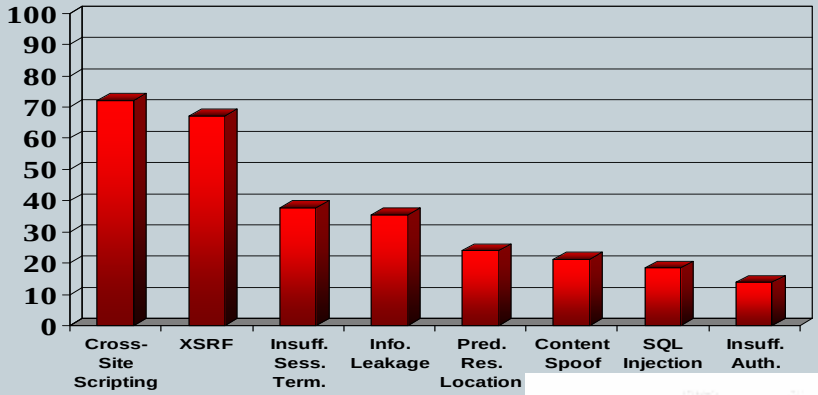
Code quality is usually understood literally:

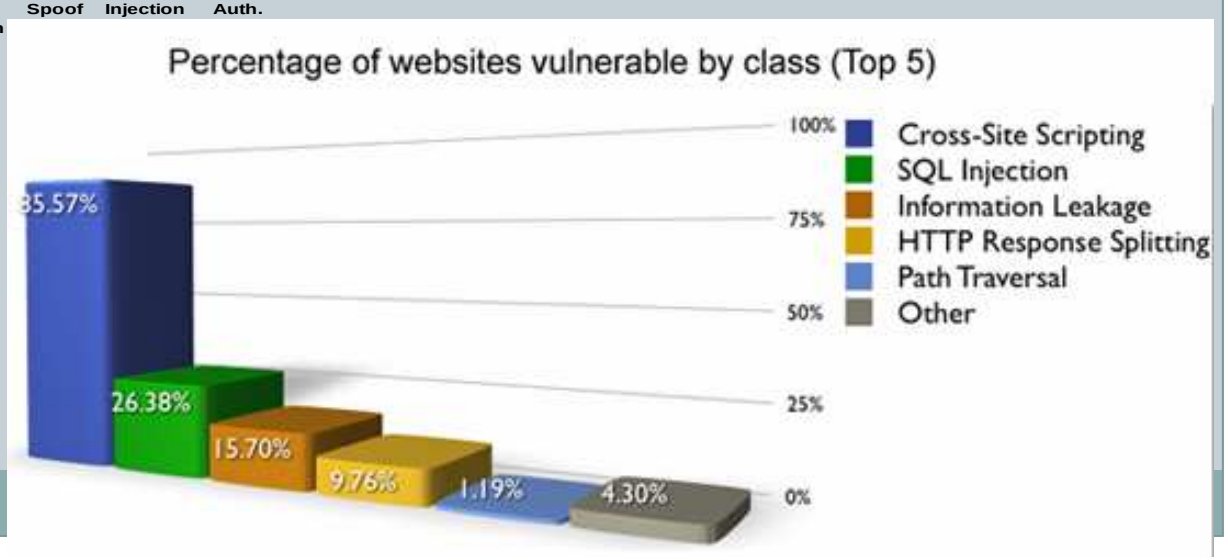
- Properly written code (code that compiles and works)
- Does the job… whatever that means
- Doesn’t have any unnecessary ‘blobs’ – leftovers from coding / debuging phase, no stupid comments, no variables that are declared but not used, etc.
- Code that is easy to read and maintain (design follows best practices).

When do we start discussing “SECURITY”?

How Vulnerable Are Applications?

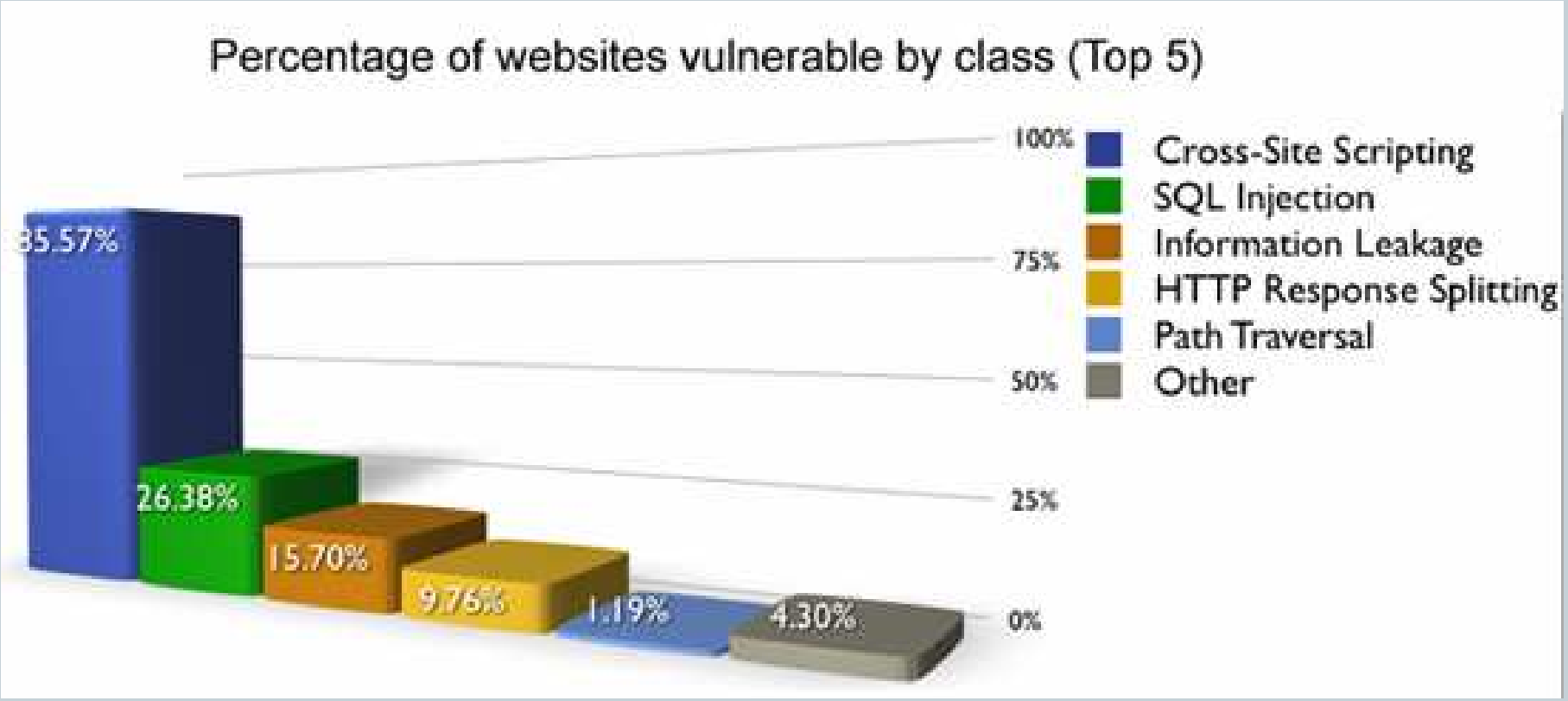
- Access data that can be used for extortion/ID theft.
- Lots of vulnerabilities: two large scale studies.





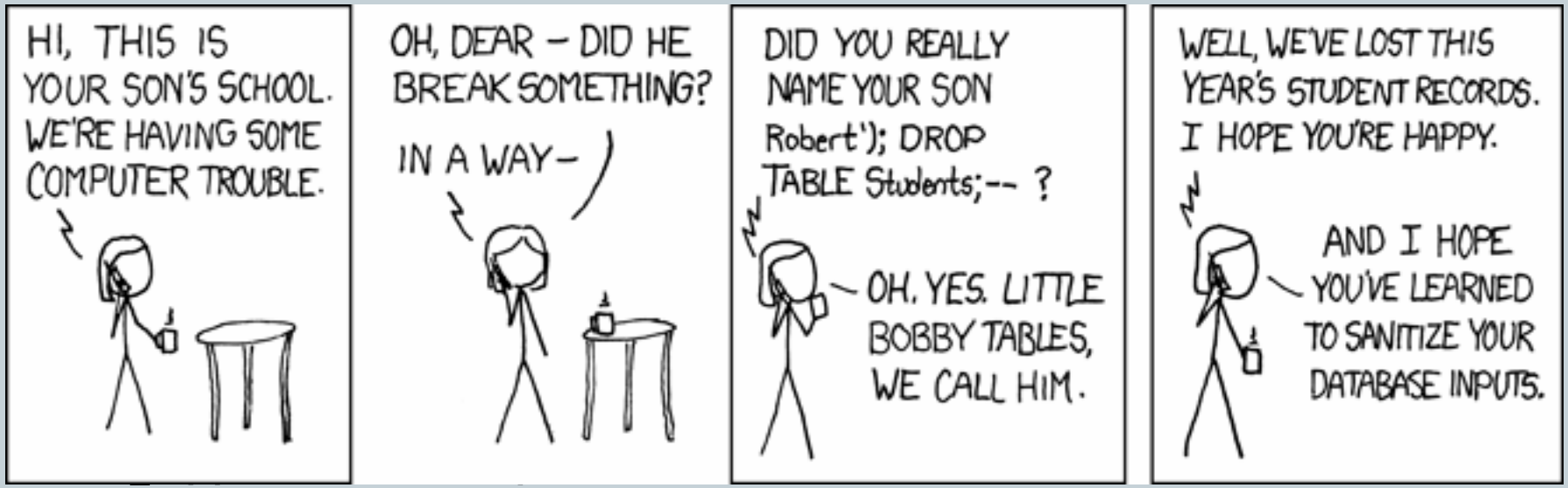
How Vulnerable Are Applications?

Vulnerability Statistics Survey (31,373 sites)



** http://www.webappsec.org/projects/statistics/

Soft SQL Injection



http://xkcd.com/327

Could this be avoided?

Yes – if only there was a proper design and testing in place instead of ‘dirty hack that works’ turned into a production system.

We all see the problems, we know about them, most people understand them very well… but we still make mistakes, even though we could avoid them.

… but do we learn from these mistakes?

Why So Many Vulnerabilities?

- Application programmers
  - were never taught to write secure code.
  - didn't think users could be malevolent
  - didn't test their code for security errors
- While most security teams focused on the systems and networks
  - perimeter protection, configuration, and patching

How do you fix the problem?

- A major initiative on application security with full time staff and top management support
- Risk-based application testing regimen
  - Source code testing
  - Application testing
  - Penetration testing
- Skills development for programmers and testers
- Skills testing for developers, testers, and auditors

The new questions for CISOs

- Where are the gaps in our programmers' secure coding knowledge and skills?
- Which of our programmers have the strongest secure coding skills?
- Do any of the current job candidates have solid secure programming skills?
- Do we have at last one security-savvy programmer on every critical development project?
- Are the security skills of our outsourcers in India, China, etc. good enough?
- Do the programmers at commercial companies that develop the software we buy have top secure coding skills?
- How do we ensure any programmer working for us has the skills and knowledge to write secure code?

What is a solution?

"Programmers don't wake up one morning and think of SQL injection or cross-site request forgery on their own. Yet you can't secure applications without understanding these attacks and others like them. SANS is doing a great service to the world by creating a way to assess programmers' knowledge in this critical area of security."

Jeff Williams OWASP Chairman

Here's one enlightened point of view

"ABN AMRO has learned that the most effective and efficient manner to deal with security issues is at the source. Practical secure coding standards focus the developer on avoiding problems that will prevent applications from going live. In finance, where risk management and time to market are key, initiatives such as the GSSP have real business value."

-Robert Mann, ABN AMRO, UK

Blueprints for Secure Programming; Tests that Measure Actual skills

Testing is useful only when it reliably measures the right skills and knowledge.

GSSP exam blueprints are living documents that present the best-available answers to two questions:

1. **What tasks must programmers do to write secure applications?**
2. **What knowledge and skills do programmers need to perform those tasks effectively**

Each task in the blueprints was rated on how frequently the task needed to be done and how critical a problem would result if the task were not completed effectively.

A test of secure programming skills and knowledge, not book learning

Consider the following program:

```
1.  #include <stdio.h>
2.  #include <string.h>
3.  void usage(char *ptCommand) {
4.  char usageInfo[1023];
5.      snprintf(usageInfo, 1023, "Usage: %s \n", ptCommand);
6.      printf(usageInfo);
7.  }
8.  int main(int argc, char * argv[]) {
9.      if (argc < 2)
10.         usage(argv[0]);
11. }
```

Q1. If in the above code argv[0] may be provided by a malicious user, what security problem can the code have?
A. Format string vulnerability
B. Out-of-bound array write
C. String null-termination error
D. String truncation

- The candidate is asked to find the best answer

GSSP Certification for Programmers

- GIAC Secure Software Programmer
  - In C (first exam administered August 14, 2007)
  - In Java (first exam administered August 14, 2007)
  - In .Net
  - In C++
  - In Perl
  - In PHP

How are the tests being used?

More than 400 organizations were surveyed and said:

- 83.7% said — To identify our programmers' secure programming gaps and fill them
- 62.1% said — To ensure consultants and vendors have security-skilled programmers
- 60.1% said — To evaluate programming candidates.
- 57.4% said — To select people with secure programming skills for critical projects.
- 44.1% said — To persuade universities to ensure CS graduates know secure coding.
- 38.9% said — To help give our customer confidence that we are delivering products that include code written by certified secure programmers.

Momentum has begun

- One of the five largest software companies: sent letters to ten top colleges where they hire programmers – “teach the CS graduates to write secure code; use GSSP to ensure they have learned it.”
- One of the five largest financial companies: told all programmers (1,200 in house, 5,000 outsourced in China and India) “you must pass secure coding tests by next summer or you will not be allowed to touch any code.”

  By July 30, 2008, “no software developer may write or change any (name of company) code if he or she has failed to pass (or not attempted) the secure coding exams.”

Enterprise Partner Program

- A through E: ABB, ABN AMRO, Amazon, American Express, AT&T, Boeing, Caremark, Carlson, CIBC, Cingular, Cisco, Depository Trust, EADS, eBay, etc.
- Unlimited access to online version of the exams so all current programmers, outsourcers, and job candidates can be tested in real time
- Customized exams to cover libraries and other programming rules unique to the Partner
- Shared access to the Consensus Secure Coding Guidelines and to management briefings

So…why are the enterprises so engaged?

- "As a participant in the development stages of the GIAC Secure Software Programmer (GSSP) certification, we are confident this certification will not only strengthen Siemens' customer offerings but also strengthen the software development industry as a whole," -- *John Fichtner, head of Siemens Computer Emergency Response Team.*

- "Participating in this initiative will ensure that our stakeholders always experience high quality deliverables in a secure environment as we continue to pioneer the quality standards for the future." -- *Mr N. Chandrasekaran, EVP, Tata Consultancy Services, India's largest technology firm.*

- "The controls designed into the architecture can be breached with one SQL injection error." *Brook Shonfield, Senior Security Architect, Cisco*

Who is building the tests?

- Randy Marchany, Ruiliang Chen, and Professor Jung Min Park of Virginia Tech.
- Professor Matt Bishop of UC Davis, author of "Computer Security: Art and Science"
- Ed Tracy of Booz Allen Hamilton
- Steve Christey of MITRE, and editor of the CVE project
- Ryan Berg and Jack Danahy of Ounce Labs
- Professor James Walden of Northern Kentucky University
- Brian Chess and Eric Cabetas of Fortify Software
- Bryan Sullivan and a large team at SPI Dynamics
- Danny Allen and Karl Snider of Watchfire
- Andrew Van der Stock and Jeff Williams of Aspect Security and OWASP
- Mandeep Khera of Cenzic
- Johannes Ullrich of SANS Internet Storm Center and SANS Technology Institute
- Robert Seacord of CERT/CC and author of "Secure Coding in C and C++"
- Craig Richardson
- Christopher Telfer of Concurrent
- David Hoelzer of the SANS Institute
- Justin Schuh of Neohapsis and co-author of "The Art of Software Security Assessment"
- Peter Francois of Rockwell
- Amish Shah of Net-Square
- Monty MacDougal of Raytheon
- Dario Forte of DF Labs
- Marc Schoenfeld from Germany
- Johan Peeters, Independent, based in Belgium
- Amit Klein from Israel
- And forty-two others

So what is the opportunity we spoke about?

- Application Pen Testing
- Secure Code Development
  - Low cost development environment
  - High quality development skills
  - Europe vs. India location
  - Learn English

About SANS
75,000+ Alumni (20,000+ certified)

- "SANS reminds me of 'The Matrix'. You can take the blue pill and go on happily thinking your network is safe, or you can take the red pill and find out what the computer world is really like. SANS training is the red pill, and if it doesn't drive you insane in the process, you will leave better prepared to handle the real world of security." (Shawn Wenzel, Par Pharmaceutical)
- "The light at the end of the tunnel is no longer looking like an oncoming train!" (Tom Gilbert, The Zenith National Insurance)
- "After two SANS courses, I feel that SANS provides the most in depth security training available." (Michael Mulqueeny, Charter Communications)

Questions

spa@sans.org