COMS E6998-9:

Software Security and Exploitation

Lecture 1: Introduction

Hugh Thompson, Ph.D.
hthompson@cs.columbia.edu

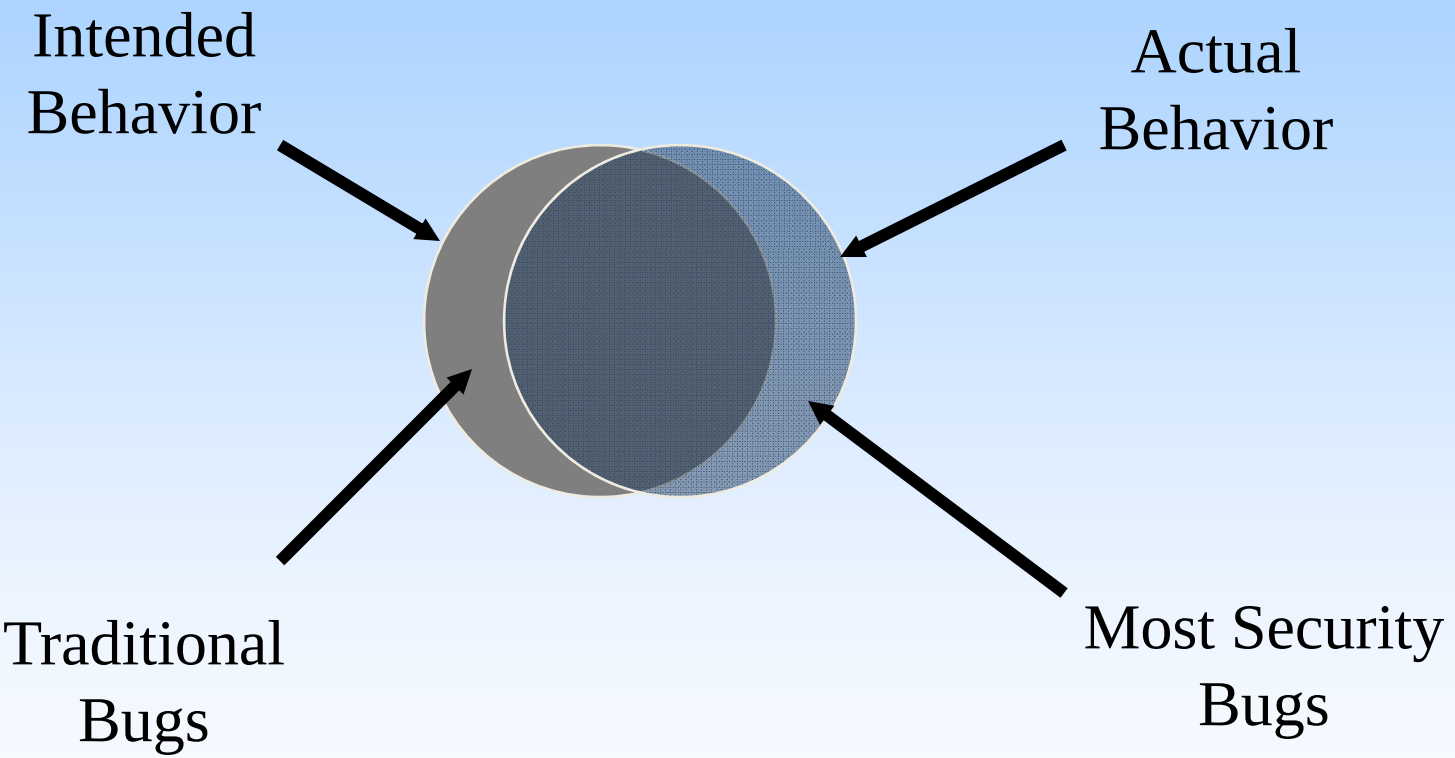
Columbia University

Understanding the difference between "bugs" and "vulnerabilities"

Functional flaws are usually specification violations

…security bugs are different

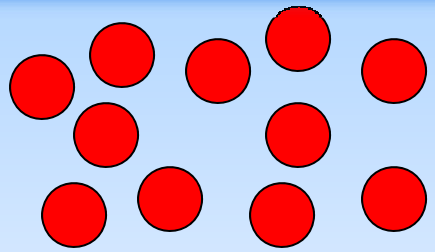
Understanding security vulnerabilities*



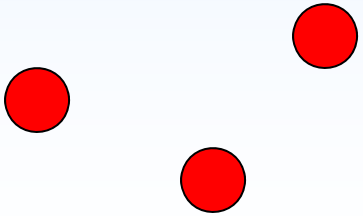
* Source: *How to Break Software Security* by J. Whittaker and H. Thompson. Addison Wesley, 2003.

Overall, this class is designed to help you…

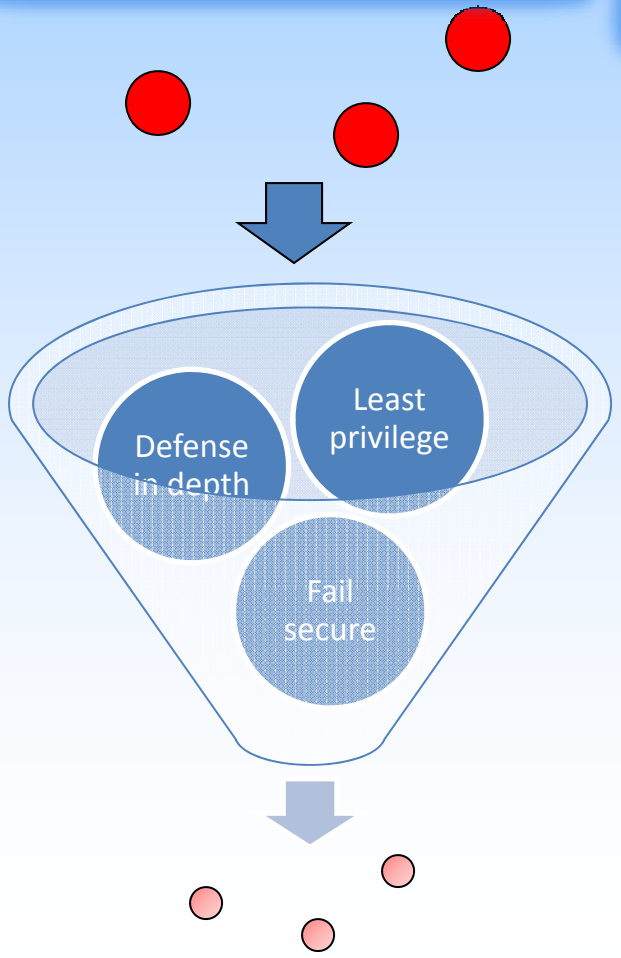
Learn secure coding techniques to reduce the number of vulnerabilities



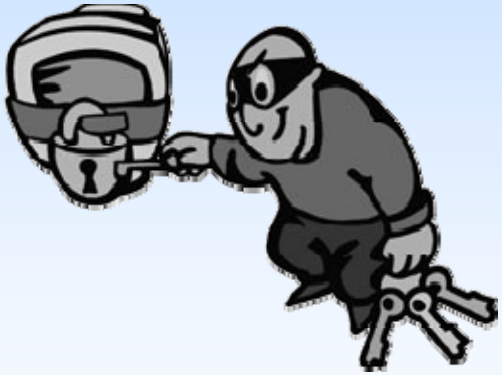
- Input validation
- Authentication
- Proper use of cryptography



Reduce the severity of vulnerabilities that survive

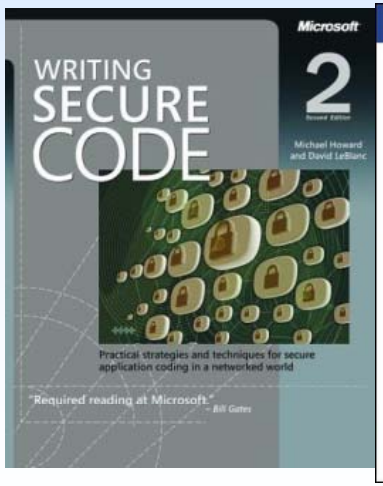


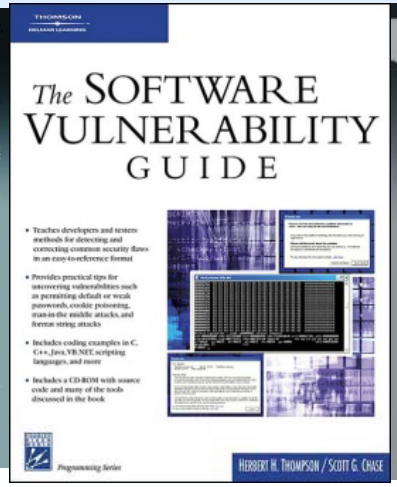
Understand exploitation techniques and emerging low-level defensive techniques

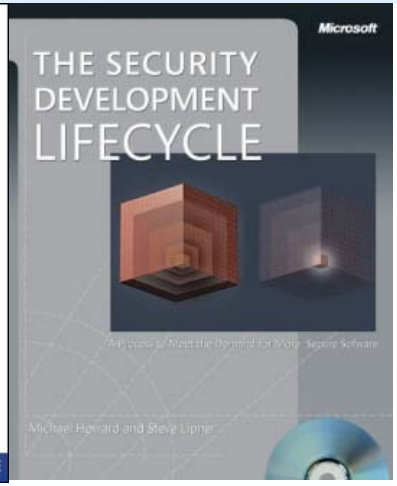


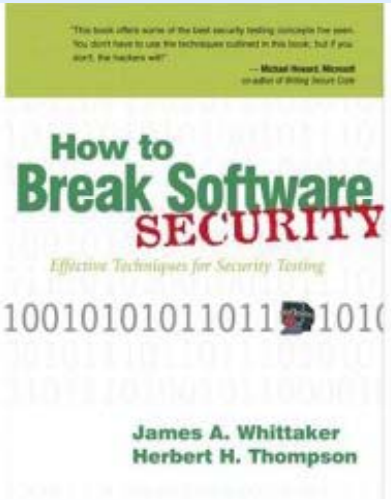
Textbook

- No textbooks are required for this class.
- Midterm exam will be based on class materials and reading assignments (papers, etc.)
- Some books recommended are:

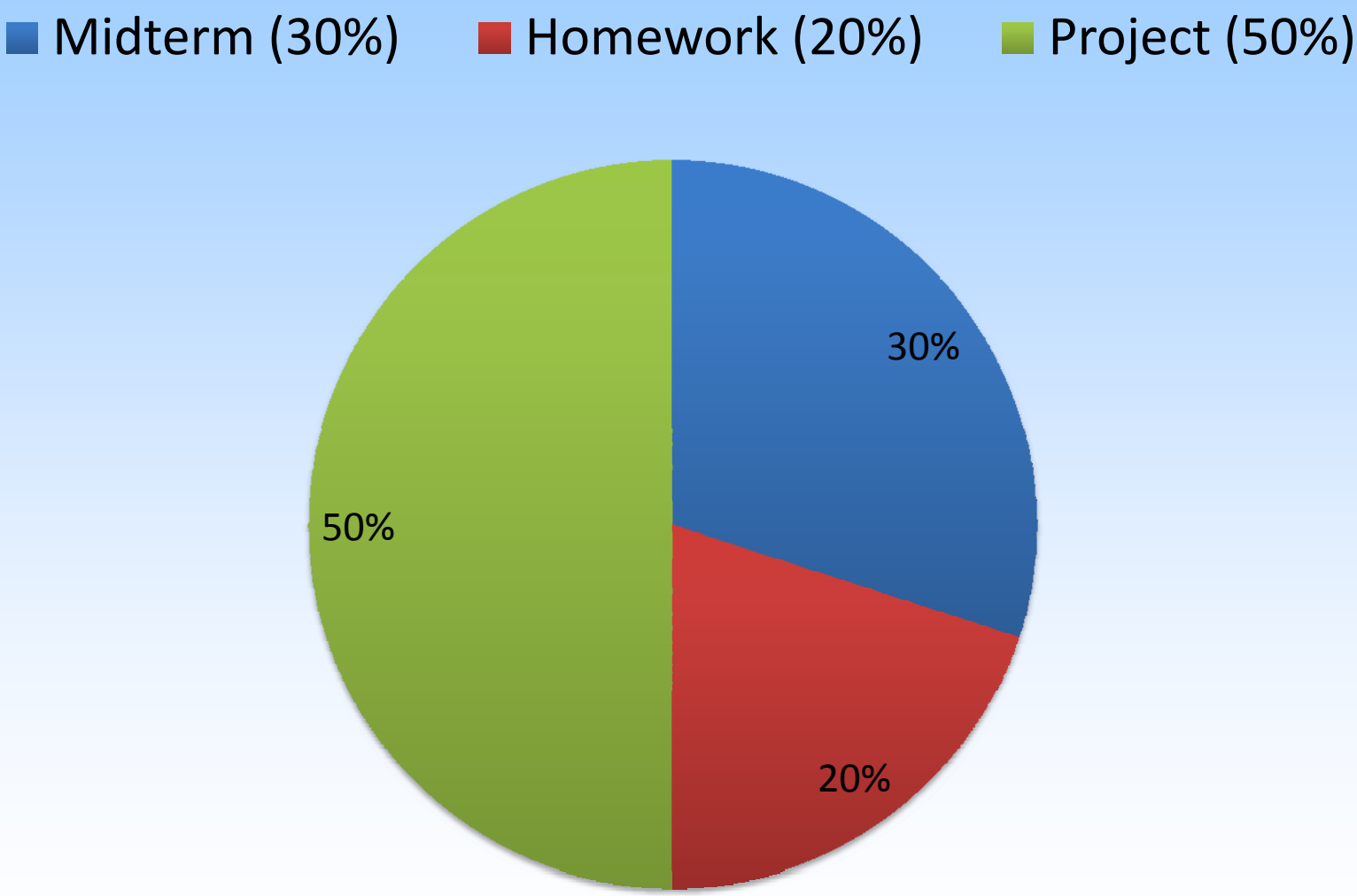








Assessment



Contact Info and Office Hours

- Regular office hours will be announced next class.
- You can also schedule a call/meeting through the week by email and feel free to email anytime.
- Course webpage:
  - http://www.cs.columbia.edu/~hthompson
- Email address:
  - hthompson@cs.columbia.edu

Project

- Your project is worth half of your grade.
- It will focus on one of the topics we cover in class or something related.
- Think about the topics over the next two weeks.
- **A project proposal** that describes your project, lists your team members etc. will be **due by email on February 23rd**.

Potential Project Topics

- Reverse engineering
- Fuzzing
- Privacy
- Exploitation methodologies
- Secure software development models
- Social networks and their relationship to software security
- Web security vulnerabilities and exploitation techniques
- Many more!

The Shifting IT Environment

(…or why security is becoming one of the most important issues in software development)

Shift: Technology

- Software communications is fundamentally changing – many transaction occur over the web:
  - Service Oriented Architecture (SOA), AJAX, …
- Network defenses are covering a shrinking portion of the attack surface
- Legacy code is being exposed widely with web front ends
- The security model has changed from good people vs. bad people to enabling partial trust
  - There are more "levels" of access: Extranets, partner access, customer access, identity management, …

Shift: Attackers

- Attackers are becoming organized and profit-driven
- An entire underground economy has been created:
  - Meeting place for buyers and sellers (chat rooms, auction sites, etc.)
  - What they are trading: vulnerabilities, botnet time, credit card numbers, PII, …
  - New ways to exchange of "value" anonymously and in non-sovereign currency

Massive Group Inc. - Windows Internet Explorer

http://massive-groupsvc.com/e/

File Edit View Favorites Tools Help

Google Search Bookmarks Check Translate Sign In

Search web...

M.. Mas... Mas... Red... Red... Red... Inva... Inv...

Page Tools

Massive Group Inc.

Login

Password

OK

Forgot password? Registration

ABOUT US SERVICES NEWS VACANCIES OUR PARTNERS CONTACTS

Bulgarian

Danish

Deutsche

08/06/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

08/04/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

08/02/2009 - Lead Generation via

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Andy Simerman. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

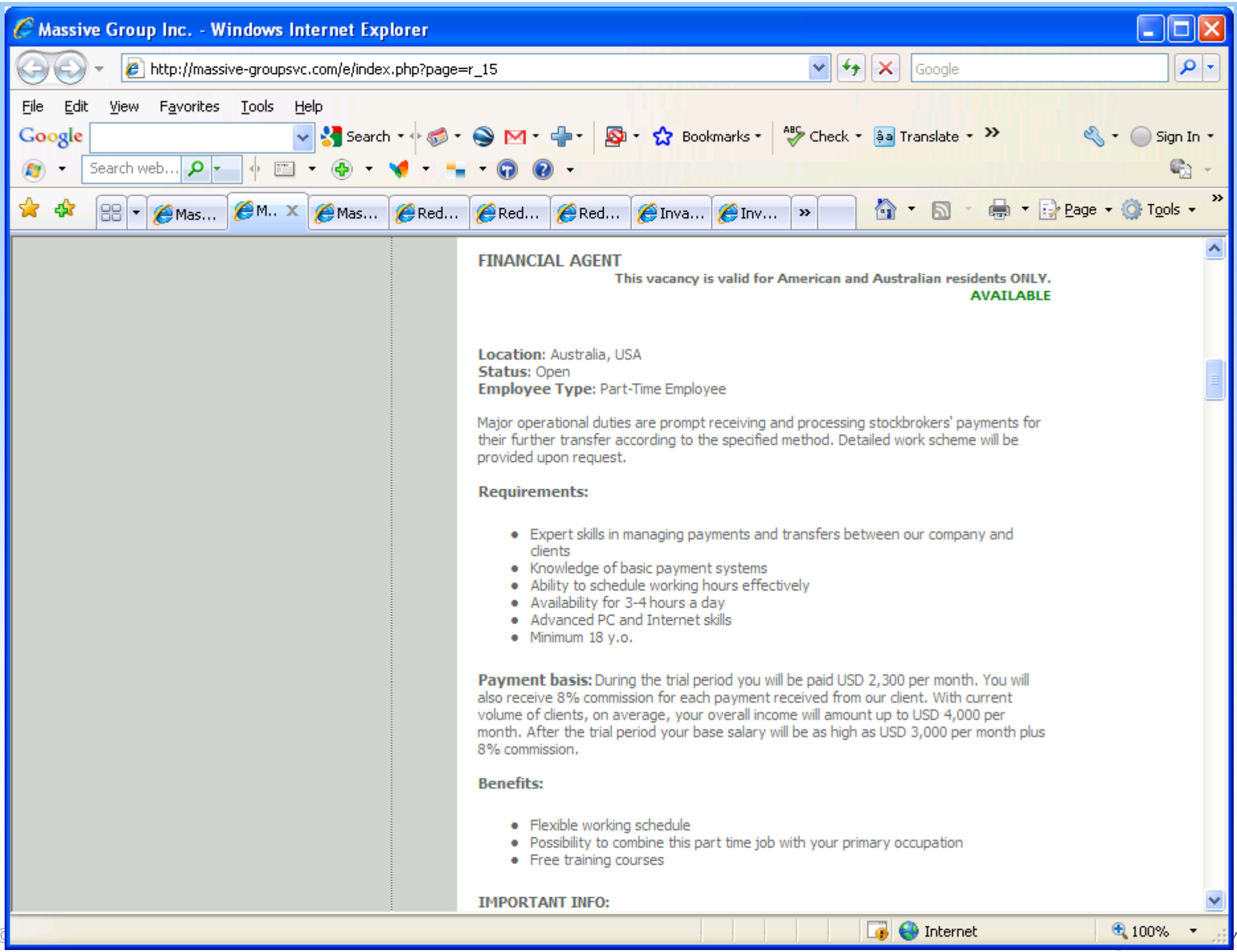
What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Internet 100%



FINANCIAL AGENT

This vacancy is valid for American and Australian residents ONLY.

AVAILABLE

Location: Australia, USA
Status: Open
Employee Type: Part-Time Employee

Major operational duties are prompt receiving and processing stockbrokers' payments for their further transfer according to the specified method. Detailed work scheme will be provided upon request.

Requirements:

- Expert skills in managing payments and transfers between our company and clients
- Knowledge of basic payment systems
- Ability to schedule working hours effectively
- Availability for 3-4 hours a day
- Advanced PC and Internet skills
- Minimum 18 y.o.

Payment basis: During the trial period you will be paid USD 2,300 per month. You will also receive 8% commission for each payment received from our client. With current volume of clients, on average, your overall income will amount up to USD 4,000 per month. After the trial period your base salary will be as high as USD 3,000 per month plus 8% commission.

Benefits:

- Flexible working schedule
- Possibility to combine this part time job with your primary occupation
- Free training courses

IMPORTANT INFO:

Massive Group Inc. - Windows Internet Explorer

http://massive-groupsvc.com/e/index.php?page=r_4

File Edit View Favorites Tools Help

Google Search Bookmarks Check Translate Sign In

Search web...

Mas... Mas... M.. Red... Red... Red... Inva... Inv... Page Tools

Massive Group Inc.

Login

Password

OK

Forgot password? Registration

ABOUT US SERVICES NEWS VACANCIES OUR PARTNERS CONTACTS

Bulgarian

Danish

Deutsche

08/06/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

08/04/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

08/02/2009 - Lead Generation via

Management Team

President of the company: Andy Simerman

Andy Simerman is the founder of the company. He has higher economic and legal education. For 15 years Mr. Andy Simerman has been occupied in the sphere of finance and banking. He has risen from a clerk to the chief executive of a large bank. Andy Simerman is the creator of unique financial flows management schemes repeatedly awarded for achievements in finance and investment. He is among top-100 world's leading financiers. Andy Simerman also gives lectures on business fundamentals and investment policy in the world's largest universities.

Chief executive: Brian Taylor

Brian Taylor is a co-founder of the company and a member of the Board of Directors. He boasts 2 diplomas of higher financial education being a graduate of the US university and a post-graduate of higher educational institution of England. Before the company was set up he had been working at the European leading trading site (oil and gas sphere). In the company Brian Taylor supervises the major trends of activity. Investment projects

Internet 100%

Redeye Group Inc. - Windows Internet Explorer

http://redeye-groupco.com/e/

File Edit View Favorites Tools Help

Deutsche Danish Bulgarian

Redeye Group Inc.

Our services:

- Brokerage Services
- Depositary
- Corporate Finance

About Us Services News Vacancies Our Partners Contacts

Login

Password

OK

Forgot password? Registration

08/21/2009 - eBay Watch: Half.com Bolsters PowerSellers

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Johnathan Smith. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

Internet 100%

Redeye Group Inc. - Windows Internet Explorer

http://redeye-groupco.com/e/index.php?page=r_4

File Edit View Favorites Tools Help

Our services:

- Brokerage Services
- Depositary
- Corporate Finance

About Us | Services | News | Vacancies | Our Partners | Contacts

Login

Password

OK

Forgot password? Registration

08/21/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

08/19/2009 - Wanted: Online Classifieds

Management Team

President of the company: Johnathan Smith

Johnathan Smith is the founder of the company. He has higher economic and legal education. For 15 years Mr. Johnathan Smith has been occupied in the sphere of finance and banking. He has risen from a clerk to the chief executive of a large bank. Johnathan Smith is the creator of unique financial flows management schemes repeatedly awarded for achievements in finance and investment. He is among top-100 world's leading financiers. Johnathan Smith also gives lectures on business fundamentals and investment policy in the world's largest universities.

Chief executive: Brian Taylor

Brian Taylor is a co-founder of the company and a member of the Board of Directors. He boasts 2 diplomas of higher financial education being a graduate of the US university and a post-graduate of higher educational institution of England. Before the company was set up he had been working at the European

Internet 100%


Invalda Group Inc - Windows Internet Explorer
http://invalda-groupmain.cn/e/
Google
File Edit View Favorites Tools Help
Search
Bookmarks
Check
Translate
Sign In
Search web...
Page
Tools
Invalda Group Inc
24.09.2009 17:58:52 (GMT)
ABOUT THE COMPANY
SERVICES
NEWS
VACANCIES
CONTACTS
OUR PARTNERS
Legal Services
Quick site access
Login:
Password:
Registration
Forgot password?
ok »
Welcome to our web-site
The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Richard Castner. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.
more »»
News & Events
What do we offer?
07/23/2009 - eBay Watch:
Done
Internet
100%

Invalda Group Inc - Windows Internet Explorer

http://invalda-groupmain.cn/e/index.php?page=r_4

File Edit View Favorites Tools Help

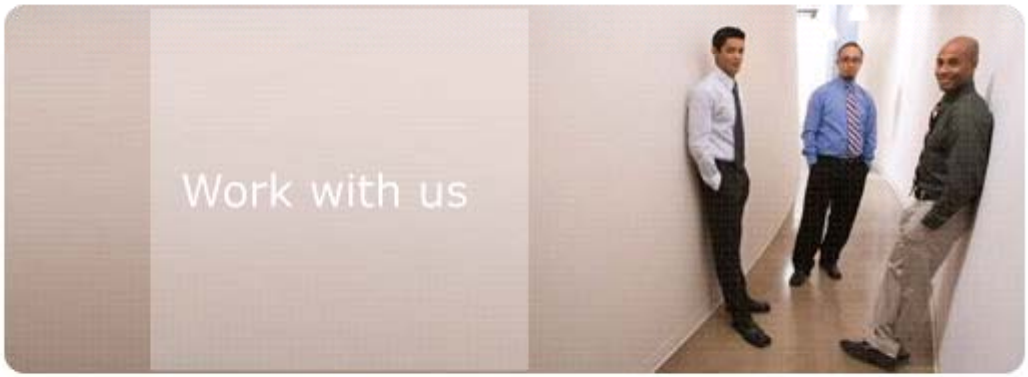
Google Search Bookmarks Check Translate Sign In

Search web...

Massi... Rede... Rede... Rede... Inval... Inval... In...

Page Tools

- ABOUT THE COMPANY
- SERVICES
- NEWS
- VACANCIES
- CONTACTS
- OUR PARTNERS



Quick site access

Login:

Password:

Registration
Forgot password?

ok »

News & Events

07/23/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Management Team

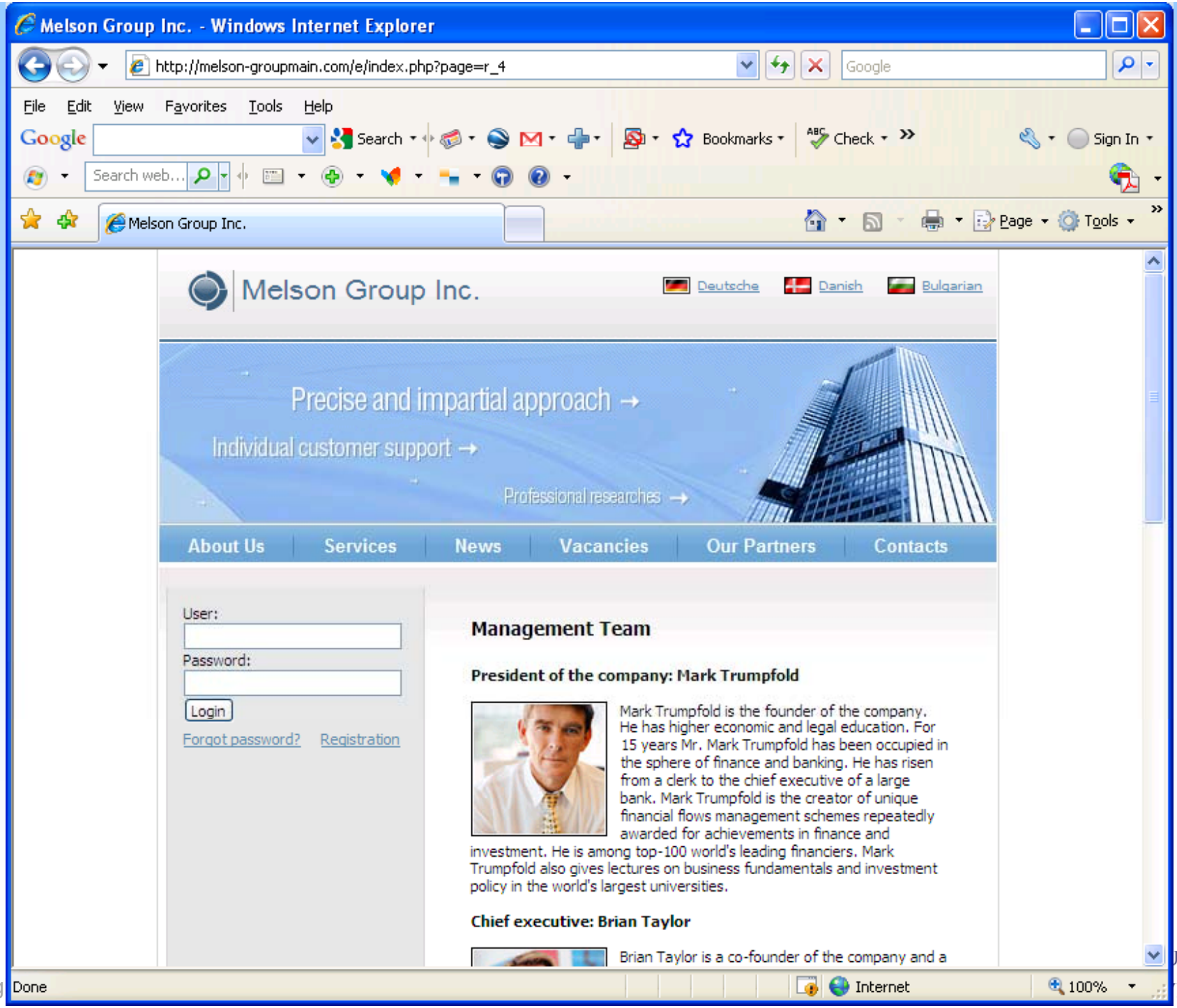
President of the company: Richard Castner

Richard Castner is the founder of the company. He has higher economic and legal education. For 15 years Mr. Richard Castner has been occupied in the sphere of finance and banking. He has risen from a clerk to the chief executive of a large bank. Richard Castner is the creator of unique financial flows management schemes repeatedly awarded for achievements in finance and investment. He is among top-100 world's leading financiers. Richard Castner also gives lectures on business fundamentals and investment policy in the world's largest universities.

Chief executive: Brian Taylor

Brian Taylor is a co-founder of the company and a member of the Board of Directors. He boasts 2 diplomas of higher financial education being a graduate of the US university and a post-graduate of higher educational institution of England. Before the company was set up he had been working at the European

Done Internet 100%



Affina Group Inc - Windows Internet Explorer

http://affina-groupnet.com/e/index.php?page=r_4

File Edit View Favorites Tools Help

Affina Group Inc

Deutsche Danish Bulgarian

- About Us
- Services
- News
- Vacancies
- Our Partners
- Contacts

Login

Password

OK

Forgot password? Registration

Management Team

President of the company: George Hankleton

George Hankleton is the founder of the company. He has higher economic and legal education. For 15 years Mr. George Hankleton has been occupied in the sphere of finance and banking. He has risen from a clerk to the chief executive of a large bank. George Hankleton is the creator of unique financial flows management schemes repeatedly awarded for achievements in finance and investment. He is among top-100 world's leading financiers. George Hankleton also gives lectures on business fundamentals and investment policy in the world's largest universities.

Done Internet 100%

Shift: Compliance and Consequences

- The business has to adhere to regulations, guidelines, standards,…
  - SAS 112 – has upped the ante on financial audits (and supporting IT systems) for not-for-profit organizations (such as Columbia) in the same way that SOX has for publicly traded companies
  - PCI DSS – requirements on companies that process payment cards
  - HIPAA, GLBA, BASEL II, …, many more
- Audits are changing the economics of risk and create an "impending event"

  Hackers *may* attack you but auditors *will* show up
- Disclosure laws mean that the consequences of failure have increased
  - Waves of disclosure legislation

Shift: Consumer expectations

- Software consumers, especially businesses, are starting to use security as a discriminator
- In many ways security has become a non-negotiable expectation of business software
- Banks, photocopiers, pens, etc. are being sold based on security…
- Security starting to be woven into service level agreements (SLAs)

The Result: Software Security is Becoming a Very Serious Issue

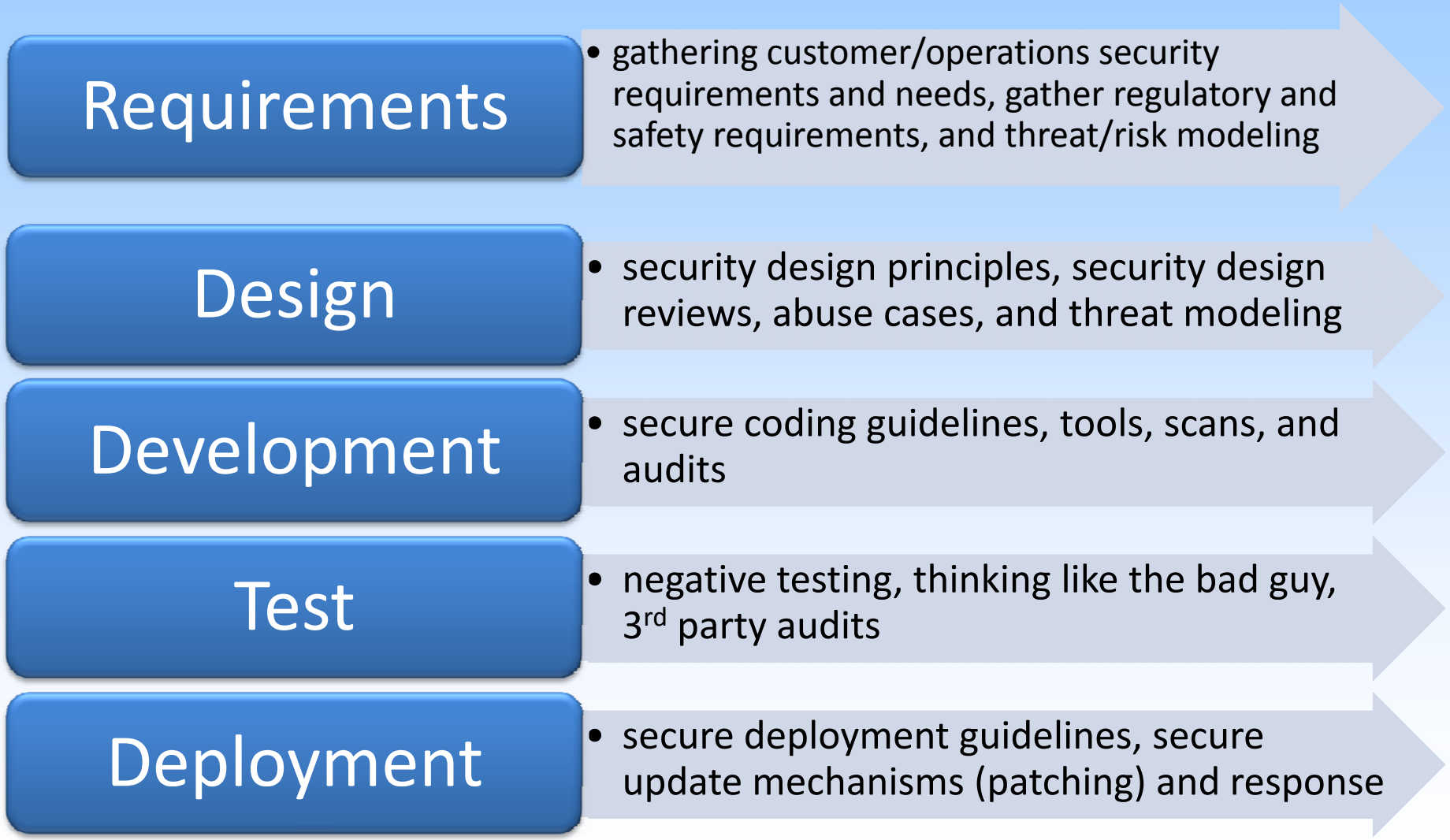
- Most "network" vulnerabilities come from software vulnerabilities:
  - Vulnerable software running on a system connected to the network is usually to blame
  - Software can be created in a way that makes it "easy" to use or configure insecurely
  - Over 70% of attacks are now at the *Application Layer*, not at the system or network layer (source: Gartner)

Security in the Software Development Life Cycle (SDLC)

What we know so far…

- Security must be integrated throughout the SDLC to be effective
- Everybody in the SDLC has security responsibility
- Security isn't a natural outcome of good traditional software quality practices; it take focused effort
- Vulnerabilities are much more expensive to fix the later they are discovered in the SDLC

Overview



Requirements

- Activities
  - Threat Modeling*
    - The process of transforming “bad things” that could happen into tangible security requirements
  - Gather Customer/Operations Requirements
    - Legal requirements: SOX, SAS 112, GLBA, HIPAA, SB 1386, Regulation E, and many more
    - Safety requirements, contractual requirements, customer needs
    - Establish negative requirements: “The system *should not*…”

References: *http://msdn.microsoft.com/security/securecode/threatmodeling

Design

- Activities
  - It's about designing security features correctly and designing functional features securely
  - Defining a security design baseline (secure design patterns)
    - Principle of least privilege, defense in depth, compartmentalization, ... (more about these later in the course)
  - Develop *abuse cases* that specifically address what the attacker can or would do
  - Review design based on threat models, principles and requirements

Development

- Activities
  - Training: probably the most effective defense against coding vulnerabilities is to understand how software can be abuse (this course will be a huge step forward there)
  - Secure code reviews, secure coding baseline, software security policies
  - Tools: source code scanning, …

Testing

- Security testing is about thinking like the attacker; understanding *abuse* as well as *use.*
- Activities
  - Security testing techniques – 19 “attacks” (to be discussed later)
  - Fuzz-testing
  - Training
  - Using tools to catch low-hanging fruit

Deployment

- Activities
  - Document “security assumptions” about the product to pass to operations
  - Develop a secure deployment guide
  - Produce/deploy updates in a way that meets customer requirements. Things to consider:
    - Cost of deployment
    - Timeliness
    - Level of compatibility testing
    - Determining authenticity of patches

Thinking Like an Attacker

(…and defending against them)

Rethinking Software Security

- Software security is about minimizing business risks that come from software:
  - Ensuring the presence of security functionality (make sure security-related code is correct)
  - Ensuring that functional code behaves securely (absence of software security defects)
  - Thinking like the bad guy and considering business risks (compliance, attacker economics)

Abuse vs. Use

Use

We usually think of development in terms of use and ***use cases***.

Thinking: What is the most likely path a user will take to perform a task.

Abuse

For security, we need to think more broadly and develop ***abuse cases*** for features.

Thinking: What could a motivated person do to leverage this feature to do something we never intended them to do.

Threat modeling: STRIDE*

Spoofing	• ***Lying about identity***
Tampering with data	• ***Manipulating, corrupting or destroying data***
Repudiation	• ***Lying about whether or not an action was performed***
Information disclosure	• ***Exposing sensitive information***
Denial of service	• ***Preventing users from doing something they are entitled to do***
Elevation of privilege	• ***Obtaining rights that were never granted***

* Source: *Writing Secure Code, 2nd Ed.,* by Michael Howard and David LeBlanc, Microsoft Press

Other things to consider

- Obtaining unauthorized service
- Repurposing of a product/application
- Integrity of logs
- 19 attacks* (more on this later in the course)
- Attacker economics

* Source: *How to Break Software Security* by J. Whittaker and H. Thompson. Addison Wesley, 2003.

BUG OF ZEN