



SecurusGlobal

SDL-What?

Steve Darrall

Agenda

- About me/Securus Global
- Why care about security?
- Secure software challenges
- Secure SDLC overview

About Me/Securus Global

- Technical background (System Administrator)
- Information Security (12 years)
- Risk Analysis & Management
- Web Application Security
- I am not a developer (my code is ugly, but suffices ...)
- We perform penetration testing on many organizations



SecurusGlobal

Why Care About Security?

When good code goes bad

smh.com.au
The Sydney Morning Herald
itpro

IT Pro Cloud Security Business IT G

You are here: Home > IT Pro > Security > Article >

Millions of passwords posted online

June 7, 2012

Join the conversation

You're the only person reading this now. Tell your friends

17 comments

Recommend 192

Tweet 41

Related Coverage

VIDEO LinkedIn passwords leaked online

Top IT Pro articles

1. Kogan browser stunt a slippery slope?
2. Ombudsman to face pirate software inquiry
3. The data miner that's watching every move you make
4. IT departments told to 'evolve'



Mobiles Computers Apps Consumer Security Games

Security > Article >

Last.fm and eHarmony passwords stolen

012

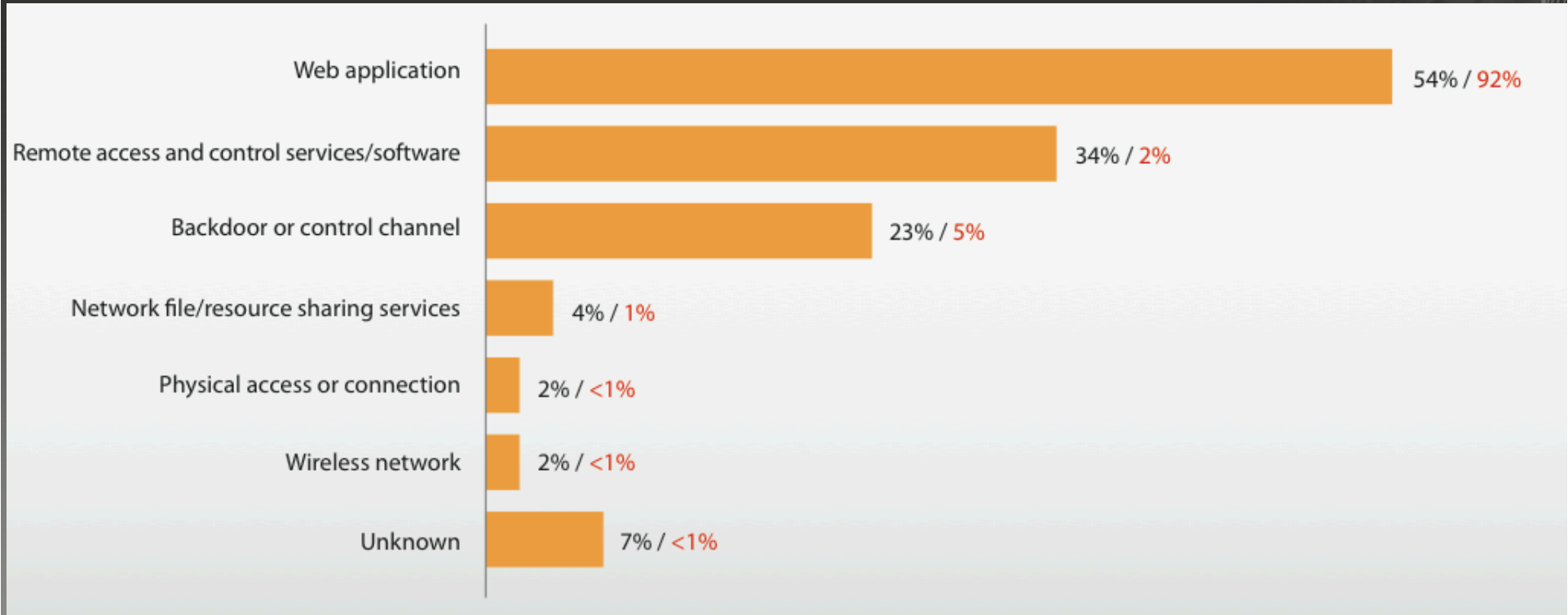
[★ Read later](#)

Last.fm music site and the eHarmony dating service said user passwords were stolen, a day after another online site, LinkedIn, confirmed a security breach.

Last.fm is currently investigating the leak of some Last.fm user passwords," the London-based company, which recommends listeners, said today on its website. "As a precautionary measure, we're asking all our users to change their passwords immediately."

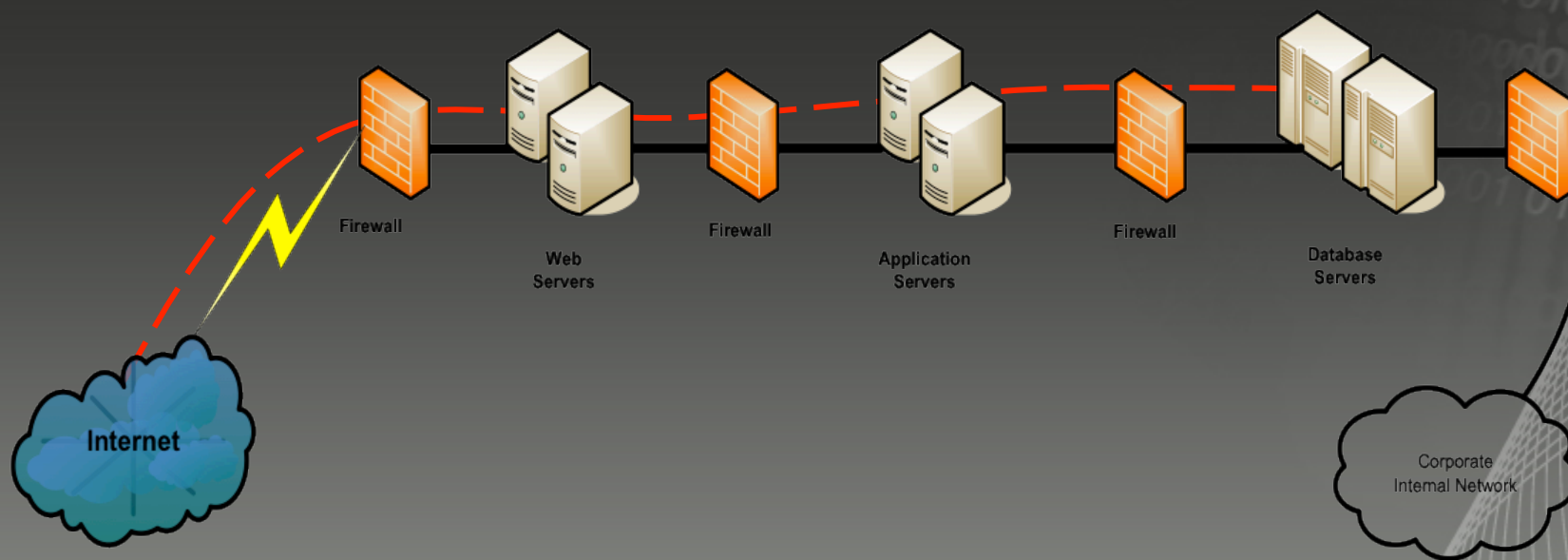
We're secure. We have a firewall!

Attack pathways by percent of breaches within incidents and percent of records



Source: Verizon 2010 Data Breach Investigations Report

Path of least resistance



Key Points

- People will hack what they can reach
- Web application code is exposed – therefore it will be attacked
- If you know about the vulnerabilities, you can write code to protect against them
- Good security is not a product, it's a process
- Consider security throughout the SDLC

Secure Software Is...

- Is that which protects the **confidentiality**, **integrity** and **availability** of information.
- Is also that which protects the **integrity** and **availability** of processing resources under the control of the manager or administrator of the software system.

Principle of “Least Privilege”

- At each layer of the computing environment, every **process** or **user** must be able to access **only** the information and resources that are necessary for its legitimate purpose.



SecurusGlobal

Secure Software Challenges

Myths

- “My deadline is more important”
- “We are secure - we have firewall”
- “We are secure - we use cryptography”
- “No-one would do this!”
- “Why would someone do this?”
- “It doesn’t work that way”
- “No one asked for it to be ‘secure’!”
- “We have never been attacked!”



Before a fire



During a fire



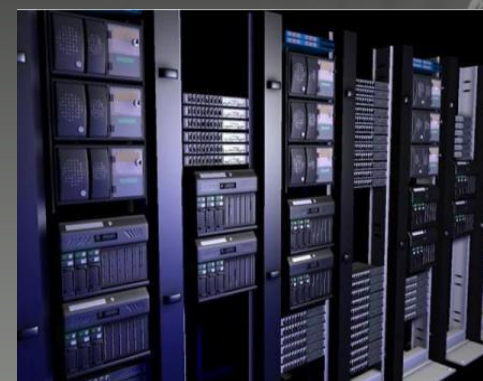
After a fire



Before an attack



During an attack



After an attack

Secure Software Challenges

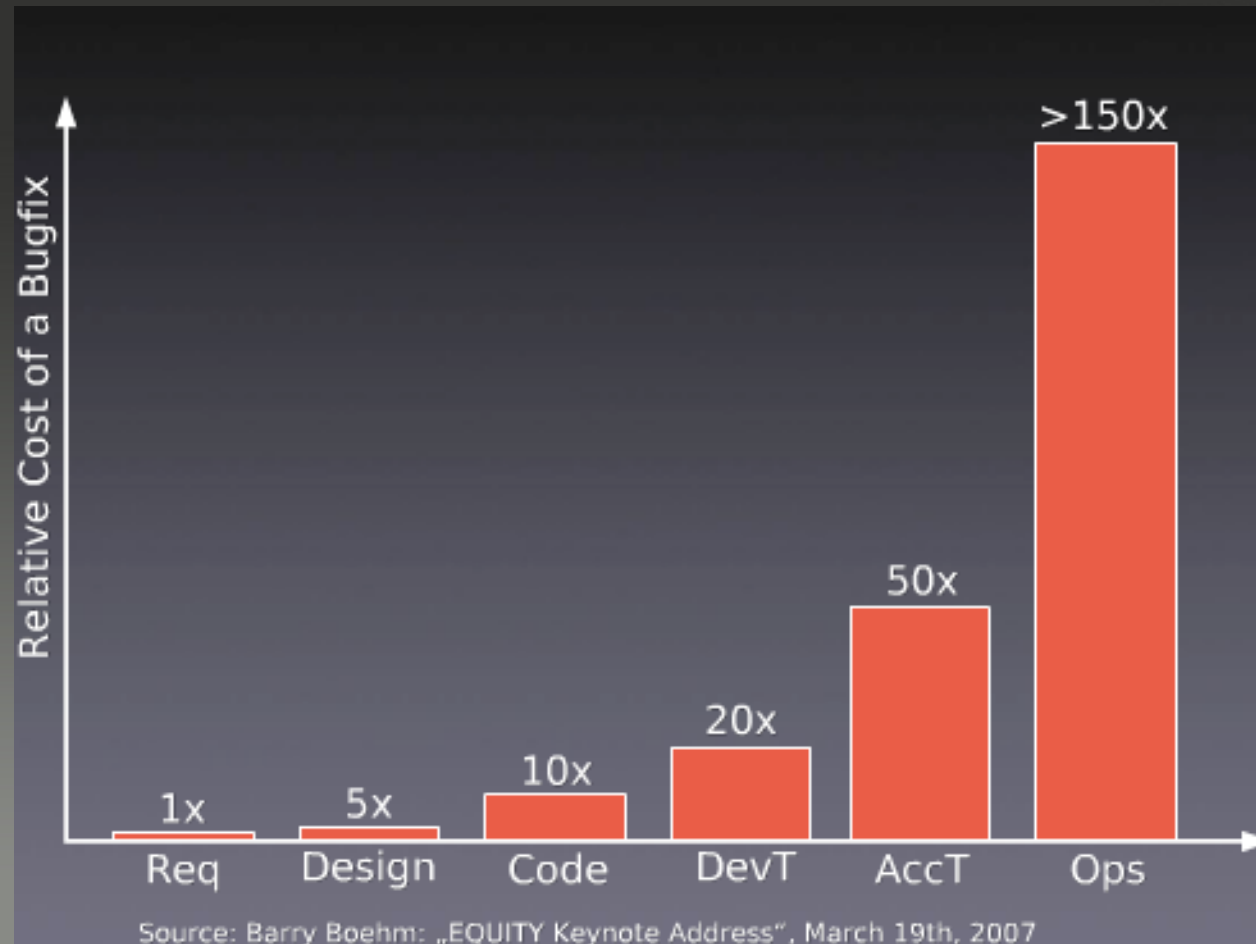
- An attacker only needs to discover one vulnerability
- The defender needs to know all the vulnerable points
- The attacker's time is unlimited
- The defender's time is "tight"



SecurusGlobal

Secure SDLC

Secure SDLC – Why?



Secure SDLC – What?

- Incorporating security into all of the phases of your SDLC
- Team members
 - Developers
 - Architects
 - Program managers
 - System owners
 - **Security**
 - Legal advisor
 - Privacy officer
 - ...



Secure SDLC Requirements

- Initial Risk Assessment
 - **Identify Business Risks** – does application pose any risk to your corporate reputation, relationships with partners, vendors and regulators, proprietary planning or corporate data? Why?
- Explicit security requirements
 - Regulatory & continuity compliance
- Threat Modelling during use cases
 - Structured approach to identify, evaluate and mitigate risks associated with the application
 - Have you prepared for each threat?
 - If not, iterate.

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

Secure SDLC Analysis & Design

- Architecture Review
 - Define intended user of feature or function
 - Describe how to deploy the feature in a secure fashion
- Elaboration of Tests
 - Application Security
 - Contingency Planning



Secure SDLC Implementation

- Application development standards
- Iterative code reviews
- Automated code testing
 - Many tools available



Secure SDLC Testing

- Execution of performance & contingency tests
- Execution of security tests
 - Application penetration testing
 - Automated scanning



Secure SDLC Deployment

- Go live testing
- Security baselines
 - To assist in detecting unauthorized changes
 - Examples:
 - System executables
 - Application executables
 - Configuration and parameter files
- Specific updates
 - New vulnerabilities & patches



Secure SDLC Tips

- It is a continual process, must be treated as one
- Security risk is not static
- SSDLC requires education
 - Ongoing training within development group
- Continuous improvement
 - Evaluation of processes
 - Changes for new technology & threats





SecurusGlobal

Questions?

info@securusglobal.com