



build | integrate | secure

The Permanent Campaign: Driving a Secure Software Initiative in the Enterprise

John B. Dickson, CISSP

john@denimgroup.com

Twitter @johnbdickson

March 24, 2009

Texas Regional Infrastructure Security Conference

Denim Group Background

- *Professional services firm that builds & secures enterprise applications*
- *Risk and Vulnerability Assessment Services*
 - Application Penetration Testing
 - Secure Code Reviews
 - Secure Application Development Services
 - Commercial Product Assessment
 - Data Security Assessment
- *Security Training Services*
 - Application Security Principles Training

Personal Background

- *15-year information security consultant background*
- *Principal at Denim Group*
- *Ex-Air Force security analyst at AFCERT*
- *Trident Data Systems, KPMG, SecureLogix, and Denim Group information security consultant*
- *Works with CIO's and CSO's to build successful software security initiatives*
- *CISSP since 1998*

A Starting Point

- *Vast majority of literature on software security focused on technical and procedural fixes*
- *Dearth of information on “how” to successfully implement software security initiatives*
- *This presentation attempts to bridge that gap*

The Nature of the Problem

- *Building software is HARD*
- *Building secure software can be exponentially HARDER*
- *Convincing others that they should build secure software is the HARDEST challenge of all!*

The Core of the Problem

- *Different missions*
- *Wildly different cultures*
- *Status quo bias*
- *Complexity of software itself*

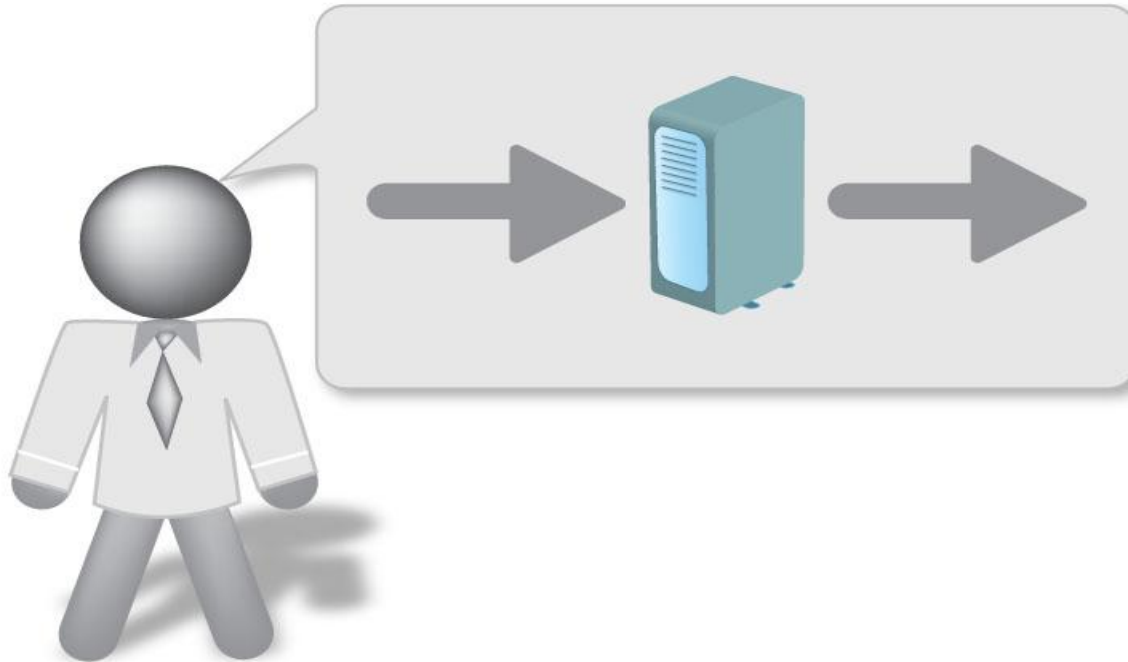
How Developers Think



```
    } else if ((arg2) && (arg2.length > 0)){
        if ( cmd == "LMSGetValue") {
            testquestionsObj.SetVariable(arg2,
SC0GetValue(arg1));
        } else if ( cmd == "LMSGetLastError") {
            testquestionsObj.SetVariable(arg2,
SC0GetLastError(arg1));
        } else if ( cmd == "LMSGetErrorString")
        {
            testquestionsObj.SetVariable(arg2,
SC0GetLastError(arg1));
        } else if ( cmd == "LMSGetDiagnostic")
        {
            testquestionsObj.SetVariable(arg2,
SC0GetDiagnostic(arg1));
        } else {
            // for unknown LMSGetxxxx extension
            v = eval('g_objAPI.' + cmd + '\\\' +
```

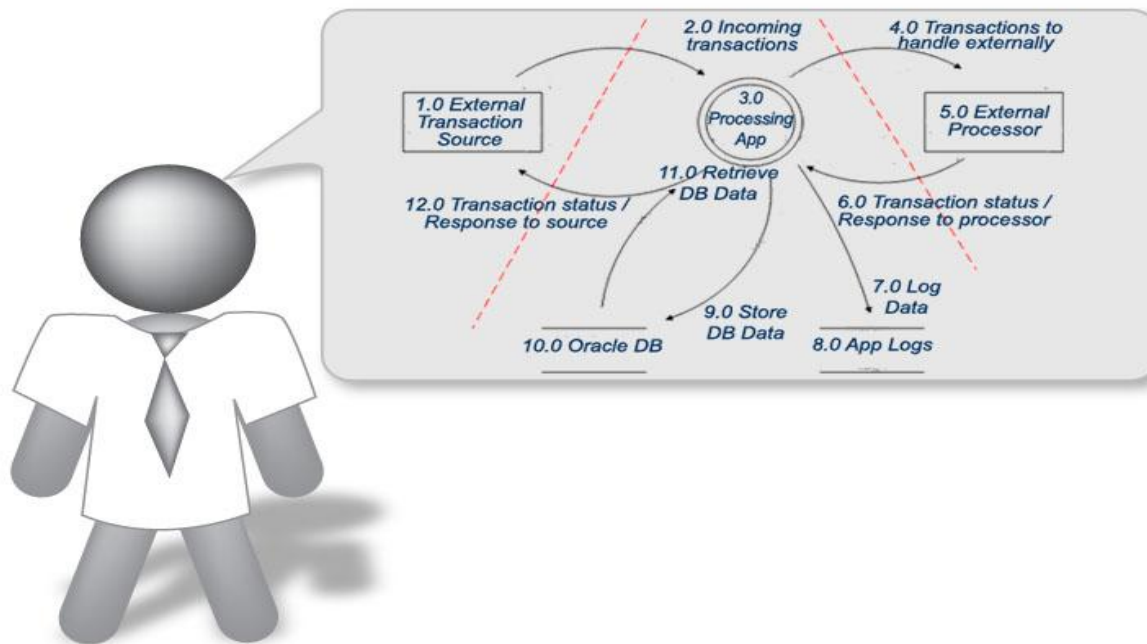
developer**THINK**

How Security Guys Think



securityTHINK

How Security Guys Should Think



idealTHINK

FUD Carpet Bombing?



Components to Driving a Secure Software Initiative

- Characterize the Landscape
- Secure Champions
- Define Standards & Strategy
- Execute
- Sustain & Repeat

Characterize the Landscape

- Compliance framework
- Cultural Norms
- SDLC's in place
- Existing artifacts of software security
- Gap between policy & practice

Secure Champions

- Executive sponsor(s)
- Internal audit
- Champions in the field

Define Standards & Strategy

- Inventory applications
- Conduct a “lightweight” risk assessment of applications
- Rank applications -pick one and conduct
- Set reasonable goals and communicate modest successes

Examples of Modest Goals

- Conduct a ½-day classroom overview of application security concepts for your development leads, architects, and project managers.
- Publish a “Top 10” list of coding standards that reflect fundamental security values for your organization. For example, define how your organization handles data at rest with encryption.
- With the help of internal or external resources, remediate one of the applications you assessed earlier in the process.
- Implement threat modeling at the early stages of a handful of big projects so you can begin to develop an internal competency to review applications at the earliest stages of development.
- Improve one facet of the SDLC to inject a software security “control.” This might include security peer review, black box testing, or a similar activity that improves the security of code being published.

Execute!

- Put Champions to Work!
- Pilot program or phased approach
- Tailor your approach to the audience
- Measure improvement via:
 - *Defect count*
 - *Vulnerability count*
 - *Response hours expended*
- Instill culture of threat modeling

Bottom line: Show quick wins, highlight behaviors, and do it over and over again, ratcheting up standards with each iteration.

Sustain & Repeat

- Regular, disciplined update of the regulatory framework must occur
- Follow commercial tools trends
- Monitor emerging risks

Why Should You Care?



THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON
August 2006

Dear Servicemember or Veteran:

I am writing to share with you the most current information regarding the theft of a laptop and a hard drive containing personal identifying data on servicemembers and veterans. You should have received a prior letter from me explaining that an employee took home electronic data from the VA, which he was not authorized to do. The data were downloaded to the hard drive. The employee's home was burglarized and the laptop and hard drive were stolen.

I am pleased to report that both the laptop and the hard drive have been recovered thanks to hardworking law enforcement officials in the local and federal communities. Based on the results of forensic tests, the Federal Bureau of Investigation (FBI) has told us that they are highly confident the sensitive data were not accessed.

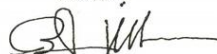
Given the FBI's high degree of confidence that the information was not compromised, individual credit monitoring will not be necessary. However, VA has obtained data breach analysis services as a means of further ensuring no misuse of this data occurs in the future. Data breach analysis is used to detect patterns of misuse related to a specific data loss incident. While it is highly unlikely that the data were accessed, data breach analysis will provide back-up assurances.

In addition, we encourage all servicemembers and veterans to be extra vigilant and carefully monitor their financial records. For information on how to protect yourself against identity theft, please visit the Federal Trade Commission's Web site (www.consumer.gov/idtheft) or call 1-877-438-4338.

We apologize for any concern that this situation may have caused you. Although this has been a painful lesson, it has identified gaps in VA's information security practices that we are correcting. I am committed to having our employees adequately trained, with strengthened policies and procedures in place so that this does not happen again. We are thoroughly examining every aspect of our information security program to ensure that veterans' sensitive data are not stolen or compromised. Veterans have a right to expect that VA will take all necessary precautions to safeguard their personal information. I am confident that VA will achieve the highest standards in the realm of cyber and information security, just as it has in the realm of electronic medical records and the delivery of health care to veterans. I appreciate your understanding through this difficult situation.

Even as we have been addressing this issue, VA has been attending to its core mission of caring for veterans – providing excellent health care, benefits, and burials – with no diminution of quality or commitment. For further information, please contact a Veterans Service Representative at 1-800-827-1000.

Sincerely yours,



R. James Nicholson



McCOMBS SCHOOL OF BUSINESS
THE UNIVERSITY OF TEXAS AT AUSTIN

Doan's Office GSB 2.104 • 1 University Station B6000 • Austin, Texas 78712-0201

May 8, 2006

Mr. John Boyd Dickson (uid:94950)
7111 Poniente Lane
San Antonio, TX 78209-3322-11

Dear Mr. John Boyd Dickson,

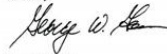
On April 23, 2006, the University announced a security breach discovered in the administrative information system at the McCombs School of Business. I am sorry to inform you that specific information about you was accessed (downloaded) by an unauthorized and unknown person. The following information was disclosed:

Your Name, Your Social Security Number, Your Email, Your UT-EID, Your Birthdate, Your Graduation Date

Since your Social Security number and/or date of birth were accessed, I strongly encourage you to take precautions to protect your credit. At minimum, as recommended by the Federal Trade Commission, it seems prudent to register for the no-charge, 90-day, renewable Fraud Alert services offered by the three national credit bureaus. Information on Fraud Alert sign-up and additional options you may wish to explore can be found on our special Web site, <http://www.mcombs.utexas.edu/data theft>. If you do not have access to the Internet, or if you wish to receive this information by telephone, please call 475-9020 (local Austin number) or 866-657-9400 (toll-free). Our help desk is open 8 a.m. to 6 p.m., Monday through Friday.

With so many positive activities and programs at the University and the McCombs School of Business, it is distressing to have to share news about a theft. We deeply regret the inconvenience and concern this crime may have caused you. The University is committed to doing everything it can to ensure the security of any personal information received from you, and we are working vigorously with law enforcement authorities to identify and prosecute those responsible for this intrusion.

Sincerely,



George W. Gau
Dean

P.S. Beyond the free basic Fraud Alert, there are commercial services that offer additional credit protection available for purchase that you may wish to consider. While we cannot recommend specific services, some firms are offering discounts to those whose records were exposed in the data theft at McCombs. Information can be found at our website, <http://www.mcombs.utexas.edu/data theft/discout.asp>. Your discount code is UTA-349408754

Questions and Answers

John B. Dickson, CISSP

john@denimgroup.com

210.572.4400

Follow me on Twitter at [johnbdickson](https://twitter.com/johnbdickson)