Security Architecture

2:45 to 3:45 PM	**Hot Topics - Security Architecture**	**Steve Kellogg**
	I will present on Penn State's current and future strategies for Identity and Access Management along with our efforts to affect better security of the endpoints. I am looking for other presentations on topics related to enterprise security architecture. Suggested topics might be other's take on identity and access management, network security measures, multi-tiered service provisioning, social engineering, computer forensics, or any number of other topics that make up what we think of as components of a security architecture.	

Session Details, Presentations and Notes

Indiana University

Presentations and Links

Indiana-Update-ITANA-08.ppt

> *From Jim Phelps' blog...*
>
> *Completed a 10 year Strategic Plan which worked because they connected money to it. You couldn't get funding unless you showed how your project connected to one of the 71 strategic initiatives. Completed a 10 year tactical Telecom Plan. Instead of replacing 1/4 of the switches every year for four years, they want to replace all switches in one year so they can take advantage of new features.*
>
> *802.11X access solution based on MAC addresses or logins. Getting to automated, policy-based network access. What is the value of this and what have people done in this area? What are the policy zones? This can flip it over so that we are both protecting our network from devices as well as protecting devices from our network.*
>
> *This group could develop some design templates that schools could use in discussions with vendors.*

UW-Madison - Stefan Wahe

Presentations and Links

ITANA-Security Architecture Wisconsin v2.ppt
OCIS site
UW-Madison IT Security Principles
UW-Madison IT Risk Assessment Process

> *Should there even be a Security Architecture? Shouldn't security be embedded in all of the groups and users? When Stefan started in 2001, he always was asked, "Why" about security items. Why do I need to use a firewall? Why should I have logging turned on? Set a set of principles:*
> *• Security is Everyone's Responsibility*
> *• Security is Part of the Development Life Cycle*
> *• Security is Asset Management (classifying the information)*
> *• Security is a Common Understanding*
> *We have a five step process for doing a risk assessment. First we agree to the assessment scope, then conduct the assessment, develop a draft report, communicate the findings then re-assess as needed.*
>
> *Risk = (Impact X Likelihood) / (Mitigation Controls)*
>
> *Impact is related to costs. How do you monetize reputation? You can ask how would you spend to prevent this from happening. This is a Risk Prioritization process.*
>
> *How do you balance the security principles against the development principles (scalability et al).*

Penn State - Steve Kellogg

Presentations and Links

http://www.personal.psu.edu/kellogg/Presentations/ITANAf2f.18june08.pdf