

You're listening to the Sun Microsystems Podcast Network.

Welcome to this edition of Innovating@Sun, with your host Hal Stern. Today's topic: Systemic Security. And now, here's Hal Stern.

Hal: Hello, and welcome to Innovating@Sun. I'm your host, Hal Stern, vice president of systems engineering. And my guest today is distinguished engineer, Glenn Brunette who is a fellow Jersey native and also one of our Sun experts in security. And we're going to talk today about systemic security. So, Glenn, welcome to the show, and tell me why we're talking about systemic security and not secure systems.

Glenn: Thank you, Hal. Thank you for having me. It's very important that customers realize that security is not about products. It's about how all of the products and the processes that they have fit together into a comprehensive ecosystem that protects their information and information assets.

Hal: And one of the things I know that you've developed in this architecture for systemic security is the notion of a set of modular components -- a set of modular micro patterns, if you will, to go off and address a variety of security problems.

Glenn: Absolutely. One of the things that we realized early on was that there are quite a few architectural patterns that present themselves from customer deployments, and if we can ensure that these patterns contain certain security properties, then we can instantiate these patterns with a variety of products and services based on our individual customer requirements while maintaining the integrity of the security architecture.

Hal: So, drill into that a little bit more. What kinds of security properties are we trying to capture?

Glenn: There's quite a few. The most salient ones that come up are things like self-preservation, that every element within the environment should be able to protect itself from attack, things like defense and depth, and the need for mutual reinforcing layered security controls, and certainly other ones, more traditional ones like compartmentalization and least privileges to contain and limit exposure. And each of these properties is really integrated within each of the security patterns that are part of the systemic security architecture.

Hal: And part of the reason for going modular here is to accommodate change? I guess one of my concerns is that you make something secure, and then you forget about it, and now you want to worry about, "Well, I've gone and changed one thing. I've gone and added some new components. How do I ensure that the new results are equally as secure as what I started from?"

Glenn: Absolutely. In fact, there's really two points here. The first one is that often when you present customers with a comprehensive architecture, they look and "Well, that's really nice, but you know, I have an existing legacy environment to deal with." So, one of our concerns was being able to slowly adapt a customer's architecture to leverage these principles and these patterns over time so that they can gradually become more secure, more easily reach their target. But to your point about agility, it's also quite important that as products change, as technology changes, as business requirements change, that we be able to keep up and adapt. And that requires a high degree of agility within the architecture, and that is certainly

why we use the architectural patterns.

Hal: So, what are the specific pieces we're using here of Sun technology from elements of Solaris through some of the patterns that you've developed? What are the pieces that make up the secret sauce?

Glenn: Well, there's quite a few patterns themselves that start out with the notion of a secure component and a secure execution container. Moving up into the network, you have secure network enclaves and shared secure services in both an infrastructure and application sense. And you build on that all the way out to presentation level services and secure desktop services. And the goal is that you can isolate and identify interfaces between each of these that can be more tightly controlled than in an environment where everything is basically flat out all sprawled out in the same environment or in the same network.

Hal: So, you mentioned defense and depth before. I'm reminded of the old example of the castle with the drawbridge and the moat and talk about managing interfaces. The same idea there of knowing what goes over the boundary?

Glenn: Absolutely. I think there have been quite a few examples over time and Alec Muffett has a great video of this that's on his blog that shows this in kind of a PBS kind of look and feel. But fundamentally what this is about is about ensuring that no single control -- if a single control fails, that we don't violate the entire architecture. And the need for the standard interfaces, the APIs and things of that nature allow us to plug and play different products as technology evolves. And this allows also customer's choice, so that they can choose the products and capabilities that are most preferable to their environment.

Hal: So, what elements of Solaris come into play here and add value to the systemic security architectures?

Glenn: That's a great question. Solaris plays a very key role here in both a secure component sense and a secure execution container sense. So, fundamentally, Solaris and its secure-by-default properties with Solaris 10 provides a rock solid foundation on which you can deploy services. Add to that the notion of Solaris zones and containers, the resource management capabilities, the fine grain privileges in RBAC and add to that even the detection capabilities with Solaris auditing. You really put together an environment that is capable not only of protecting itself and protecting the services it provides, but also providing a good deal of auditing and measurement about what's going on on the system.

Hal: So, we have clearly the Solaris distributions we're getting out into the market. How do we get the rest of the systemic security architectures into our customers' hands? Is that something you buy or is that something you get?

Glenn: Well, it's a little bit of both. I mean, the systemic security architecture is an approach. It is an idea to show how these various components fit together in a holistic way, and can build actually a mutual reinforcing kind of view of security across the entire architecture. But you know, we have products -- Sun's not known as a security products vendor in the traditional sense of a firewall or intrusion detection. But what we do have is actually we build security into our entire portfolio. So, whether you're talking about Solaris, whether you're talking about our Niagara processors and their crypto acceleration properties or even things like our secure application switch, our crypto accelerator, or even going up the stack into our

identity and our SOA offerings, we can build security to each of these layers all the way out to the user in the form of the portal, the Sun Ray, and even the secure global desktop. So, really we have a very comprehensive view on this entire problem.

Hal: So, if I'm a customer and I want to get access to the systemic security patterns, what do I do?

Glenn: The best place to go today is sun.com/security. And there is a number of things on that Web site including white papers and presentations that we can offer customers to get up to speed on this.

Hal: So, we've really kind of taken the Open Source route with the architectures themselves, telling everybody how it works.

Glenn: Absolutely. We've taken the openness absolutely to heart. We continue to evolve this material, and produce updates so that it becomes a living document, not just something that's thrown out there over the wall once.

Hal: And you made a great point just a minute ago when you were talking about using the features in Solaris to go build systems that have auditing and integrity and self-preservation built into them. Do you see that security becomes a developer issue and a function of a general purpose system as opposed to something that gets buried into a firewall or an appliance and is something that is on the perimeter of the network?

Glenn: Absolutely. And really that's one of the core elements of systemic security is that every element has a security role to play, however small or large it may be. And from the developer's standpoint, there is actually quite a few things developers can do to build software more securely or take advantage of the features of the underlying platforms on which they're running. Sun systemic series doesn't mandate you do it, because we are positioning a very open and extensible architecture, but there are certainly a lot of benefits that you can achieve if you can take advantage of Solaris zones and privileges in RBAC, for example.

Hal: Great. So, a chance to brag. Something unique to Sun? Something more general in the market?

Glenn: Well, I think it is something unique to Sun. I think in part this is because Sun has visibility across the entire stack from the processors and storage subsystems all the way out to the clients. And because of this, it gives us really a systems view of the world, an architectural view of the world that allows us to build security into this entire portfolio. But one of the interesting things about Sun is that combined with our innovation is really our openness. And so, our insistence upon open standards and APIs and interfaces mean that customers aren't locked in to Sun only solution, although we believe that there are certain benefits that they can realize by using one.

Hal Stern: So, Glenn, any final thoughts on security in general?

Glenn: Well, one of the things I would want to mention is that security again is not a point in time activity, getting into your point earlier about building it secure and keeping it secure. So, one of the things we'd encourage customers to do is take a maturity oriented view of their environment. And so they can understand how they can apply these architectural patterns

and processes and reference architectures and all of the various things that are out there. They first need to understand where they are operationally. We can't go in and throw a large complex solution to a customer who's not able to maintain it. But conversely there are customers who have developed a strong model of operational maturity, and that allows them to build really complex, but very sophisticated and effective security systems.

Hal: Well, Glenn, thanks for joining us. And you have been listening to this Podcast of Innovating@Sun.

Glenn: Thank you very much.

You've been listening to Innovating@Sun. Join us next time for the latest in innovation from Sun Microsystems. Only on the Sun Microsystems Podcast Network.