Brad Semrad
SE-4930
January 9, 2012
Article Review 2

The article selected is SCION: Scalability, Control and Isolation on Next-Generation Networks from the 2011 IEEE Symposium on Security and Privacy.

The article discussed a new way, SCION, to handle Internet Routing to improve security without giving up too much of the current internet ways. They center on the security features of creating isolation, control, and scalability to help create a secure network. The next following paragraphs describe the key features of the new network at a high level without going into as much details as the original article does.

The first security feature is to create isolation or trust domains. Currently, the internet will listen to different routing broadcast by any point on the internet. This causes routing issues that can flow traffic, increase the route, and cause naming conflicts on domains. The solution proposed is to create trusted domains that can only affect the flow of within the trusted domains. The idea here is that trusted domains that share a common contractual, legal or other limited trust and control the communication within the domain. This prevents outside or untrusted domains from changing the control flow or flood a domain with routing message. The cross domain communications follow a human set path in SCION. Currently, the domains are not separated but are essentially keep in a tree structure that will propagate message about control possibly through the whole internet.

The other feature is to allow both the source and destination to choose the routing paths. Currently, only the source gets to choose the routing path. This additional control can allow the destination to avoid untrusted paths of communication. This creates control over the routing paths to avoid nodes that could have been taken over or prevent the flooding of control messages to a node. Currently, the source is allowed to choose the path but the destination is not given a choice. This is the reason why it can be insecure. You could send your banking credentials through a secure route but receive the account information back through an unsecure route. Another security feature was to use Accountable IP address when looking up routing information. This uses a public key and certificate mechanism to validate the route is valid. When the packet is in transit, it will keep track of the paths to allow other nodes to forward the messages.

For scalability, the top domain cores are the only allowed to propagate routing message internally. Currently, any node in the domain can update and broadcast path information. This can cause numerous messages to be forwarded and required more processing power to handle all the nodes. This means that one node could flood the domain with message on the current system. In comparison, the new system will only let a few trusted source control the flow and send those types of messages. The other reason is that cross domains follow a set path that would not be frequently be updated and therefore do not require as much listening on the device. In addition, each top domain holds its topology and not all domains hold other domain's topology. This provided numerous nodes of failure without the whole internet going down.

Brad Semrad
SE-4930
December 11, 2011
Article Review 1

In the article, I learned a little bit more about network routing and how the current model is insecure. These insecurities were due to how certain design choice were made. First, the paths are only allowed to be chosen from the source and not the destination. This means I can send all my data to a safe path but not receive the response back in a safe path. Another interesting point that I learned was how the current system can flood path updates. This can cause other routing issues internal to the domains due to other domains causing routing issues.

From the article, I picked up a few secure coding techniques. The first is to creation trust domains or separations between different components. This prevents corrupt nodes from changing a configuration on another node. This can easily be applied to any program and by treating each node as a component. The other idea for secure coding in the status of the network is let the senders choose the path. This can allow paths to be updated with the status and prevent information from being intercepted. In these cases, this would only apply to a network path. The other security features of validating who it is from and keeps track of where it is being sent to and from and create a certificate type system to help prevent from unauthorized modification. This is key to any application that does any network or inter-process communication.

The question that I have related scalability that each top domain has its core, but if that top domain fails, is there a failover or will that whole domain failure? What design features could be handled to handle this?