**EMCS2010: Applied Cryptography and Data Privacy**

Assignment: Dealing with Outdated Crypto

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*Answer the following questions in essay format: What can be done to discontinue the use of outdated crypto? Specifically, consider TLS that checks whether a website that a user is trying to connect to has a valid certificate. How can we discontinue TLS certificates that use SHA-1? What would be the consequences of doing that -- what would be the burden on users and websites?*

#### The Problem

Outdated crypto is a tricky problem. Owners of websites tend to want to cater to the lowest common denominator. And, who can blame them. Who wants to update software? Nobody does! Consumers just want things to work! If merchants are the only ones that enforce the rules, and they are given the choice of enforcing vs selling … they will probably sell. Lucky for us the merchants are not the only ones in the equation.

#### Requiring Updates at the Payment Processor Level

Merchants seldom build their own credit card checkout systems. Even if they did build most of it, merchants still can’t actually process a credit card. Visa, Mastercard, AMEX and Discover provide tools to the merchants and those that make tools for merchants to process transactions. These tools could enforce the use of current cryptography. Who is in the best position to force companies like Visa to do anything? The Government with a ground swell of public support.

That being said, states could easily seek to enforce that payment processors use a certain level of crypto as a “stick approach” for those payment processors who do not comply. As a “carrot approach” there could be benefits for those who use state approved crypto. The problem with solving the issue at this level is that many merchants operate outside their state and interstate commerce is under Federal jurisdiction. Frankly the States and the Federal Government don’t have a good track record of enforcement at this level.

#### Pressuring Payment Processors with Advocacy

Companies tend to respond to pressure when there is a groundswell of public support. Creating this ground swell is usually the work of an advocacy group with capital. In the viral / digital age creating this type of attention for an issue is not just a matter of having the money to the marketing, but it is also have a brief, easy to understand and yet compelling message. In other words it takes talent to formulate a message that non-technical people understand. I could see this type of movement incentivizing more payment processor to pay attention to the versions of software they are using in the wild.

#### Requiring Updates at the Browser / OS Level

Last, but not least in any sense is enforcement at the browser level. Change here could be swift if Google Chrome enforced the latest version of TLS. The could not only enforce it, but they could redirect people to the proper place to read our the risk out dated crypto causes. Companies like Apple and Google tend to stay out of the enforcement role, but it’s actually not a very smart long term strategy. Good security and more educated consumer is better for the ecosystem. The more trust we have in the system the more likely we are to use it. Once the browser ( especially Chrome ) gives an alert or warning that a site is not using the proper version of TLS. I am sure merchants and payment processors would straighten up very fast.