Digitally Signed Transcripts
Department of Computer Science, University of Wisconsin – Eau Claire

Student Researcher: Kevin M. Spinar (spinarkm@uwec.edu)
Faculty Mentor: Professor Paul J. Wagner (wagnerpj@uwec.edu)
Funded by: Department of Computer Science and University of Wisconsin – Eau Claire Differential Tuition

Problem
Every year, millions of college transcripts are printed, enveloped, stamped, and sent through the postal system. These transcripts could be sent just as easily by email almost instantaneously with virtually no cost. However, email is generally viewed as an insecure medium of exchange, allowing others to intercept and modify emails during their transit over the internet.

Objective
The objective of this research is to develop a method to send transcripts securely over the internet using digital signatures. Digital signatures have successfully been used to validate the authenticity of electronic documents, software, and emails. A digital signature is created by applying a private key, known only to the creator of the document, to the document, generating a unique signature. As long as the private key remains private, only the holder of the key can modify the document, ensuring the integrity of the contents. If the transcript has been digitally signed, even if it is sent over an insecure medium such as email, the receiver can be confident that the transcript has not been altered. The focus of this project is to create a system that will read in the student transcript information, generate a document, apply a signature, and transmit the secured document to the intended receiver.

Process
A student logs onto a computer (1) and submits the transcript request using an online form (2). The request is processed by a university server (3), which retrieves the student transcript information from the university’s database (4). The student information is combined with a document layout template (5a) to create an electronic transcript (5b). The document is then digitally signed using the university’s private key (5c). The resulting signed transcript is sent to the email server (6), which sends the document across the internet (7). Even though the email could be intercepted, the signed document cannot be modified without invalidating the signature. The email arrives at the destination email server (8) and is downloaded by the intended recipient (9). The digital signature is validated automatically by the recipient’s document viewing software against a certificate server (10), ensuring the authenticity of the document.

Implementation
This project attempts to provide all the functionality necessary for a university to set up a service to create and send digitally-signed transcripts with the least amount of effort possible. Unfortunately, as database configurations vary from university to university, individual universities will need to implement the extraction of the student information from their database (4) and convert the information into the format that the transcript generator requires. However, the remainder of the steps—creation of the transcript, signing of the transcript, and emailing of the document—is handled by the transcript transmission service.

Conclusion
The technology required to create and send digitally-signed transcripts has been available for many years. The issue resides in the reluctance of educational institutions to embrace technology and to trust the security inherent in digital signatures. With proper education and readily-available services to generate signed transcripts, educational institutions should continue to reduce the amount of documents physically transmitted and rely more on electronic transfers. This project is hopefully one step in that direction.