The transition from e-commerce to m-commerce will introduce additional security threats compared to the status quo; issues that have already been solved for e-commerce re-emerge as security is traded for performance on low-power mobile devices. Nonetheless, as business fundamentally relies on security – the fairness that both parties receive what they were promised – technology protecting intellectual property will most certainly become available. Despite hackers cracking almost every copy protection, online connections will allow implementing secure cryptographic envelopes to protect digital content.

It has now been more than one year that the recession or slump caused by a dramatic reduction of market capitalization in the new economy prevails. The public might perceive this as the Armageddon of E-commerce but fails to acknowledge the value already added to our daily lives. As the Economist (2001) writes, “the spectacular bursting of the Internet bubble has led some to question the very importance of the net.”

Nonetheless, a plethora of business transactions, i.e. exchanging goods and services, are already being conducted using electronic means of communication. The enabling technology in the future will most certainly be security. As the number of transactions increases ex-post controls are being rendered infeasible because checking logs would consume excessive resources. Moreover, the widely anticipated transition from E-commerce to M-commerce additionally leverages the significance of security requiring an unprecedented impetus to satisfy consumer needs.

The fundamental concept of commerce is to exchange goods and services in return for payment or in the case of a barter economy in return for other goods or services. This concept obviously only works in the interest of both parties if basic security requirements such as the atomicity of a transaction can be guaranteed. In the non-mobile IT world most of the involved challenges have already been addressed and at least conceptually solved if not yet widely implemented. The different characteristics of non-mobile E-commerce and M-commerce and their unique usage patterns entail various additional security threats.
mainly caused by the fact of mobility itself (Ghosh and Swaminatha 2001).

In addition to the economic slowdown, the transition from E-commerce to M-commerce weakens security – the aforementioned feature that is widely considered to be the decisive factor in broad acceptance. Currently, mobile devices lack even basic security concepts and when protocols, programming languages and operating systems were designed security was traded for performance. On mobile devices the need to conserve energy obviously limits processing power; as a result state-of-the-art security concepts have not been implemented. For instance, WML script – the mobile version of JavaScript – does not implement the sandbox model, allowing mobile code unlimited access to all local resources (Ghosh and Swaminatha 2001). Moreover, most PDAs (personal digital devices) lack memory protection mechanisms and support only basic access control – if any at all.

As the hype about E-commerce has passed its culmination, real consumer benefits will increasingly move into the center of interest. Given the experience that researchers – especially in the natural sciences, mathematics and computer sciences – have with computers, it is not surprising that they were among the first to integrate E-commerce transactions, such as using digital libraries, into their day-to-day lives. Beside supporting business transactions of brick-and-mortar companies, digital content – be it music, stock quotes or any other form of information – is the rationale for using electronic commerce at all.

Similar to the advances caused by fundamental inventions like electricity, the real benefits will be gradually introduced; they will first be adopted by large companies and technologically savvy people – often referred to as early-adopters. The lack of a ‘first-mover’ advantage may discourage companies to introduce M-commerce at early stages especially as there are many more security risks involved. Not only are mobile attackers inherently difficult to track down but most mobile devices such as cell phones or PDAs also do not support fundamental security concepts that are already well-established and mostly implemented in current desktop PCs and operating systems.

Recently, important steps have been made that are crucial to the protection of intellectual property and therefore – at least partly – for the success of M-commerce. Napster decided to distribute its digital content in form of cryptographic envelopes. This is by no means a very new concept. Some years ago IBM promoted cryptolope, a system that allows packing virtually any kind of digital content into so-called ‘cryptolopes’. Comparable systems were developed by other companies such as Infraworks (http://www.infraworks.com), OmniVa (http://www.omniva.com) or Authentica (http://www.authentica.com). The basic concept of all these products is similar: Even after passing on digital content to others (who might distribute it further), it can only be used after having been unlocked by a central server. The cryptographic envelope contacts a server to retrieve a key to unlock the content. After unlocking it displays or prints the content and destroys the key.

The fundamental flaw that most of these systems suffer from is that by making cryptographic envelopes available offline they can be broken without anyone noticing. An option is to require an online connection to use the envelopes’ content but this is presently still unacceptable for some applications, especially for home users. However, with the rise of mobile computing, simple devices like MP3 players will most likely be integrated into PDAs which will always be online, allowing online authentication and authorization to unlock the cryptographically protected digital content. The rationale for requiring a central server to unlock the content is that this server can keep track of how often it unlocks the digital envelope for a specific user. If the same user sends too many requests possibly from distant geographical locations, the account is probably being misused.

The second challenge is that digital content can often be copied when being displayed. Screen captures can be made to steal images, audio signals can be re-recorded at the line-out jack and screenshots of texts can
be transformed back to text using OCR. However, very robust digital watermarks have been developed that even survive the aforementioned attacks. If operating systems had built-in features detecting such watermarks and not allowing users to handle such files, copyright infringements would be made much harder. By integrating such detection algorithms for watermarks in hardware, e.g. in audio and video cards, they simply would refuse to display watermarked data if no authorization code is sent. Obviously, there would still be ways to circumvent these protections but most users would not be able to use these programs.

Despite the current drawbacks that all the solutions suffer from, companies selling intellectual property, e.g. Time Inc. and McGraw Hill, evaluate and partly use such products. However, there will most probably be no standard for cryptographic wrappers in the near future. However, due to its flexibility and yet standardized format XML might offer a near-term solution. Bertino et al. (2001), for instance, built AuthorX, a system that implements access control for XML documents at various levels of granularity. Basically, their approach is to encrypt sections of the XML document with different public keys so that only authorized people can decrypt them. Another example is Baltimore's X/Secure. It integrates the power of XML with the security of a public key infrastructure, for use within Java and C++ applications. Utilizing the industry-standard DOM API and established cryptographic standards and algorithms, X/Secure allows XML documents to be digitally signed and encrypted, providing guarantees of privacy, authentication, integrity and non-repudiation.

In summary, the increase in the standard of living is largely attributed to a capitalistic economy that is founded on the scarcity of resources. It is not within the scope of this article to discuss whether other, fundamentally different economic models would yield the same or even higher wealth. If, as I anticipate, economy will not change considerably, technology has to and most certainly will provide the means to effectively protect intellectual property – and increasingly competitive markets will guarantee that this happens efficiently, too.

REFERENCES

THE AUTHOR
Edgar Weippl is project manager at Software Competence Center Hagenberg (SCCH), a newly founded research center. Before joining the SCCH he taught Database Systems and Computer Security at Beloit College, WI. Besides developing agent-based database solutions for clients he continues teaching Computer Security at the Johannes Kepler University of Linz.