Using Wireless Technologies to Fight Camera Theft

Crime stories are fascinating and raise attention—so let us start with one. At the end of this past March, a burglar stole my camera equipment. The theft represented a financial loss for me—but, more than that, a sudden disruption to how I spend my leisure time. As I am a member of several Web communities

focused on photography, I published a list of the stolen equipment and discovered that Web 2.0 actually works. A community member referred me to a Web site operating in his home country in Eastern Europe, on which my stuff was listed for sale! He actually contacted the local police, but they had no interest in following up on the matter. So I called the German police, who showed great interest, yet lacked two important capabilities: agility and the ability to execute (in Eastern Europe) on the crime. I assume they filed a high-quality report and closed the case.

I began to question the value of identifying objects (such as my camera equipment) and visibility on the Internet of Things, if the ability to react accordingly in a timely manner is absent. (Could this be the reason why the Internet of Things is still far from becoming a reality?) I contacted the director of the Cambridge Auto-ID Lab, Mark Harrison, with whom I share an interest in the Internet of Things, as well as a common hobby—photography. Consequently, a discussion began about how the Internet of Things could be used to provide a (future) solution to the problem. Cameras, as well as lenses, have a unique identifier, which is provided as human-readable text and sometimes as 2-D bar codes printed on the outside of an item's housing. Such identifiers could additionally be stored on a chip within a camera or lens.

The IDs could be communicated as soon as a camera was connected to the Internet—which would likely happen, since the easy sharing of pictures and online printing is one of the

major advantages of digital photography. If the camera were reported as stolen, a remote locking command could deactivate that camera, as well as the connected lens. It is even possible to consider direct online connections between the camera and the Internet of Things, through embedded SIM modules similar to the SIM cards used in mobile phones. RFID is an optional technology that could be employed instead of SIM-based connections. However, since RFID read points are still far from being ubiquitous, a SIM-based approach would be more promising at this time.

From this general idea, Mark and I developed some requirements. There should be the capability for the legitimate owner of a stolen item to remotely and reversibly lock that device, so that it would be rendered inoperable except for the display of a message on the screen to indicate that the property was stolen and should be handed over to the police. There would also need to be support for legitimate second-hand sales, as well as for the legitimate transfer of ownership from the original purchaser to a new owner—and from that individual to the subsequent owner down then line. This means that the locking key associated with a device's particular unique ID number should be updated upon each legitimate change of ownership. Finally, one or more central repositories or product identifier authentication lookup services must be put into place that, ideally, would co-operate in a federated manner, and provide the following services and access to the following roles:

• Enabling a legitimate owner to register the unique ID number of a device given the lock key provided to that individual by the selling party, to thereby generate a locking key that should be known only to the current legitimate owner; all previous locking keys associated with that unique ID should then be unlinked and rendered inactive for that device's unique ID.

• Allowing a legitimate owner to record and report a device as

stolen, by providing its unique ID number and locking key as parameters to an appropriate method or function.

• Enabling a seller to verify whether an item had already been reported as stolen, based on querying with a unique ID.

• Allowing the police to verify the legitimate owner's identity (based on querying with a unique ID and that person's authentication credentials) and to authorize a chargeback/reversal of the transaction so that anyone who buys stolen property could be reimbursed upon returning the stolen goods to a police station. This, however, would require the co-operation of one or multiple trusted billing services. All of these requirements could be implemented as follows:

The hardware. The device (a camera, for example) would contain an embedded SIM module with mobile reception, which would check its status with the manufacturer's product identifier authentication database every time it was switched on. It would start up immediately, but if it received a response indicating it had been reported as stolen, the device would then switch to a disabled state and display a message advising that it be taken to the nearest police station. The messages for performing the check about whether the item was stolen, and for reporting it as such, could probably be formatted as regular SMS text messages, within 160 characters. If the device was equipped with GPS functionality (some current digital cameras already offer this capability), the stolen equipment's location could be transmitted as well. The IDs of attached accessories (lenses, for example) would be transmitted through the main device, which could deactivate them. As an alternative to connecting through the main device's embedded SIM module, a connection to the Internet could be established through a wired USB connection to a PC.

The registration authorities. The device's legitimate original owner would register that item's unique ID number with a standardized service hosted at the manufacturer, or with a

service such as Immobilise, and would receive a key code enabling the reversible remote deactivation of the device. The different manufacturers and third-party services would be interlinked through standardized interfaces and discovery services. Any legitimate purchasers of second-hand devices would receive the key code from the previous owner, which they could then use, together with the equipment's unique ID, to register the item as their property. This would generate a new locking key for that device (which would be provided to the new owner) and would permanently deactivate the locking key held by the previous owner, so that the prior user would not be able to remotely lock that device transferring ownership. The locking key for each object owned could be securely stored within a service such as Immobilise, together with a description and IDs or serial numbers, as well as photographs, scanned receipts (as proof of purchase) and so forth.

The event. In the event of a theft, the legitimate owner could potentially use Immobilise or a similar service to remotely lock the stolen devices for which they were the legitimate owner. The service would then update its own product identifier authentication service, and/or that operated by the relevant manufacturer, so that the next time the device called home upon startup to check if it had been stolen, it would know that it should disable itself and display the message advising the bearer to deliver it to the nearest police station. **Executive authorities.** The police would be granted access to the database behind services such as immobilise.com to trace and contact the current legitimate owner, by querying with the device's unique ID number and their own police authentication credentials. The stolen goods would be returned to the legitimate owner, who could then use the blocking key to unlock and reactivate the equipment. A purchaser of stolen goods could present those items, along with proof of purchase, to the police, who would instruct the auction site, online retailer or payment operator to perform a chargeback/reverse transaction that would fully reimburse the purchaser and debit

the seller's account, so that nobody would be able to profit from selling stolen goods. Sellers could also be levied an additional penalty for trading in such items, provided that all sellers were granted limited access to the product identifier authentication database so they could check whether goods had been marked as stolen. They would receive an electronic time-stamped receipt as confirmation of their check (such checking should be performed before selling goods). If the items were already sold before being reported as stolen, then the selling party would still be liable for the chargeback, but possibly not for the additional penalty.

The business case. Some manufacturers might not see an advantage in supporting a corresponding system. Most likely, any stolen device would result in new sales. Identical replacements would be unlikely, though, and buying a new device would offer the possibility of switching to another brand. In the described camera burglary, the camera manufacturer did not offer any discount for replacing the camera—and as a result, that company may lose a customer who had invested a considerable amount of money in cameras, lenses and accessories over the years. However, there is also a business case in the security service itself. Potential buyers could base their buying decisions on the availability of this service. Additionally, optional charges (an annual fee, for instance) could be offered to compensate for the necessary infrastructure. Moreover, insurance policies could offer correspondingly reduced rate.

Remote locking mechanisms for digital goods through an Internet of Things may help to cut down on crime. The necessary technologies are available, and as the use of radio frequency identification read points becomes more widespread, RFID tags could be employed in addition to—or instead of—SIM modules.

Dieter Uckelmann is a manager at the University of Bremen's LogDynamics Lab, which serves as a research center for the use

of RFID, sensors and other mobile technologies within logistics. Mark Harrison, the director of the Cambridge Auto-ID Lab, provides expertise in information architectures and technologies. Harrison is deeply involved in standardization activities at EPCglobal, and has cochaired the Tag Data Translation Work Group and the Data Discovery Joint Requirements Group. He currently co-chairs the Discovery Services Work Group, and also participates in EPCglobal's Architecture Review Committee and GS1's Architecture Group.