



# Whitepaper

H.-C. Hanebeck  
VP, Product Management & Marketing  
chris.hanebeck@reveresecurity.com

February 2011

## Securing Edge Devices

[www.reveresecurity.com](http://www.reveresecurity.com)

proprietary information

Revere Security 4500 Westgrove Drive, Suite 335 Addison, TX 75001 Phone: 972.930.7200 Fax: 972.930.7204

## 1. The Value of Security

It is often difficult to illustrate the need for and value of security. Security enables safety, which, in essence, is nothing more than the absence of disorder or chaos. Take modern society for example. Without security, established through governments and laws and enforced by courts, police and the military, we would still live in the same world our forebears faced thousands of years ago. All forms of human organization are means to provide stability in our interactions and to establish socio-political systems that enforce the reliability of economic and interpersonal transactions. In this sense, the ten commandments of the bible are as much an effort to secure our world as is the advent of modern warfare. We have long learned that we have to rely on a secure world in order to live peacefully and to accomplish our dreams.

The same applies to modern information systems in that they are only as good as the trust that we place in them. An information system where the validity of its data is constantly second-guessed is not useful. Without the knowledge that we can safely exchange money for goods on the Internet for example, e-commerce could not exist. Security is truly the foundation and basis for our modern lives. Oftentimes, we only notice the need for security when it is absent. This is true for fraud on the Internet as much as for attacks on computer and communication systems that automate business processes. In 1976, when Whitfield Diffie, Martin Hellman and Ralph Merkle developed public key cryptography and others began to define the concept of Public Key Infrastructure (PKI), their work ultimately enabled modern electronic commerce. Arguably the Internet would not be what it is today without their invaluable contributions to cryptography and the use of public keys. The core advantage of PKI became apparent very quickly: if Bob has a valid certificate (it includes Bob's name and a unique public key for Bob) and Alice has a valid certificate, then they are able to trust that they are who they claim to be. Thus, Bob and Alice establish secure communications and are assured that their data remains confidential. Public key cryptography has been successfully applied to websites, email and commercial transactions.

As Thomas Friedman has convincingly argued, our world has become flat long before we've entered the 21<sup>st</sup> century: most commerce is global, communication and information technologies connect even the remotest locations into worldwide networks and, Friedman termed them "steroids," ever-increasing means to access and manipulate data on the Internet e.g. smart phones, PDAs and tablets emerge with rapid speed. These new and often small, resource-constrained devices can be very difficult to secure and may not always permit traditional IT security to operate efficiently. In addition to Friedman's steroids, **there are billions of often overlooked edge devices that range from smart power meters to industrial control systems and RFID tags, which are even harder to secure.** We find that all of these devices at the edge of the network are vulnerable to attacks and can lead to catastrophic failures in large systems such as the electric grid or an industrial manufacturing complex.

Edge Devices are *things* enabled by small, resource-constrained microprocessors. Examples include RFID tags, smart meters or industrial controllers.



## 2. A New World of Vulnerabilities

Whether we realize it or not, edge devices have long become pervasive. An average American house uses between fifty and sixty sensors that regulate temperatures, lights and appliances among other things. A mid-sized sedan uses between sixty and a hundred microchips to ensure passenger safety, enable improved handling and provide a maximum of comfort. In North Texas alone, 4.5 million smart meters have been deployed recently. These meters communicate via wireless networks to report the use of energy in households on a near real-time basis. According to industry analyst IDC, there could be as many as 14 billion connected edge devices by 2015. The consequence is that we see increasing numbers of edge devices running on 8-bit or 16-bit microprocessors. **To hackers, whether economically or politically motivated, each of these new, low-power edge devices is a promising opportunity to gain access to critical systems or to cause disruption.** The comforts we have gained thus can be turned against us to threaten our way of life.

Take Stuxnet for example. Its malicious code is the most complex and in many ways most sophisticated cyber attack that has been launched to date. When its inner workings were revealed at a recent gathering of security experts from around the world in Washington DC, it quickly became apparent that we are dealing with a new type of threat. Stuxnet targeted a nuclear facility in Iran and was likely developed by one or more nation states. Its implementation relied on a very detailed understanding of the facility and its industrial control systems. The deployment required intelligence operatives on the ground to place the code into the right (and unsuspecting) hands. Stuxnet leverages four different zero day attacks on a Microsoft operating system, gains access to a Siemens PLC software (Siematic Manager) and writes its code onto the ladder logic of the PLC itself. Once fully deployed, it is impossible to stop. For the Iranian facility in question, it proved to be fatal. By many accounts, Stuxnet is the first known successful cyber weapon and one that avoided the use of conventional force such as missiles and airstrikes.



The good news was that Stuxnet achieved its objective to disrupt Iranian nuclear progress without the loss of lives and at a cost probably far below that of a military campaign. The bad news is that the cat is now out of the bag. While it was the world's first virus targeting industrial control systems, it will hardly be the last. The global hacker community has already begun to understand its operation in depth and, according to insiders, has developed new strands of attacks on small, resource-constrained devices already. These new viruses can lead to attacks on industrial facilities that range from automotive plants to consumer good

companies, all of which leverage sophisticated industrial control systems. One might argue that the cost to society is bearable when a brand of ketchup temporarily vanishes from shelves. However, underlying all of this, there is a very serious danger. **Hackers can leverage industrial control system (ICS) attack capabilities to extort ransom payments, simply shut down operations for gamesmanship or play the stock market as they disrupt industrial production.** This latter scheme has become an especially attractive tool. The criminally minded entrepreneur can sit back to earn millions by shorting or buying stocks all while his association to a cyber-attacker never becomes apparent.

### 3. Applications for Edge Security

Industrial control systems are not the only ones vulnerable to attacks. In fact, any system that offers an economic incentive is a target. The higher the perceived monetary or intangible gains are, the better the prospects for an attack. After all, hackers, just like the rest of us, are subject to cost-benefit considerations. Take into account the fact that no system is ever truly secure and we have a grave issue on our hands. The situation becomes even more challenging due to the sheer quantity of edge devices, which are either not or only superficially protected. Industrial-strength security is simply hard to implement and our sensitivity for existing vulnerabilities has not yet fully developed. Even when the t's are crossed and the i's dotted, there is still a chance that an attacker finds a backdoor, discovers a new vulnerability or simply exploits weaknesses that are outside of our immediate control, such as gaining access through social engineering. In the light of this bleak outlook, what should be done? **Establish the best security available!** Any measure that makes it harder for an attacker reduces the economic incentive. We often hear from senior executives that they do not aim to be completely secure. It just needs to be easier to attack their peers. The underlying lion-chase logic is certainly fitting.

Let's look at another example. There are many millions of smart meters deployed in the US alone. The vast majority are not secure, yet. An attacker can wirelessly and anonymously access hundreds of thousands of smart meters to shut down power and try to cause a cascading effect. In a recent briefing on the economic consequences of smart grid attacks, a senior US official illustrated that critical supply chains will dry up after about three days and that chaos will likely ensue after about three to four additional days. Given that without power there is no electronic communication, no heating or cooling, no refrigeration and eventually no transportation, it is certainly conceivable that the majority of us will find ourselves in a

[www.reversesecurity.com](http://www.reversesecurity.com)

proprietary information

position to fight for our survival after about a week. According to informed sources these kinds of attacks are already possible today. Potential attackers include disgruntled employees, organized crime and hostile nation states. Michael McConnell, the former US Director of National Intelligence, told CBS' 60 Minutes that intelligence has long known about the vulnerabilities of critical US infrastructure such as the power grid and is not prepared for these kinds of attacks. In a slightly different scenario, attackers can leverage edge devices to gain entry into much larger backend systems by tunneling into them. IBM's Scott Lunsford demonstrated this capability in 2007 when the security expert broke into a US nuclear facility through an ICS device and gained control of vital operations. In a similar, more recent attack in Europe, friendly attackers were able to gain access to all client data in a public utility system.

**An often overlooked, yet critical application area for edge security involves radio-frequency identification (RFID) devices.** RFID tags leverage close proximity wireless communication to send data to a reader, which passes it along to higher level information systems that process and utilize the information. As long as RFID tags only store a simple identifier, usually an abstract number, security concerns are low. However, when the same tags hold vital information, then the economic incentives and thus target attractiveness can increase dramatically. The parts on large commercial aircraft are a good example. The companies that assemble these aircraft place passive RFID tags on between 1,750 and 2,500 critical parts. These tags store information about the part, its maintenance history and also in which aircraft models it can or cannot be used. The use of information-rich RFID tags is absolutely necessary since there are many different airline customers who rely on this crucial information every day. At the same time, the airlines cannot access the data anywhere but on RFID tags. Imagine what could happen when an attacker reprograms the RFID tag on an inflight computer so that it is installed on the wrong plane. It merely takes a few thousand dollars to obtain the equipment necessary for such an attack. Fortunately, all aerospace manufacturers we are aware of these vulnerabilities and plan to protect their RFID tags through encryption and authentication. Similarly, the US Department of Energy tracks its containers for nuclear waste through RFID tags. The ability to quickly locate nuclear waste by reading information on RFID tags, for example during transport, can be leveraged for malicious purposes in many ways. The same logic for seeking robust edge security applies.

#### 4. Edge Security Architecture

A central question in all of this is how to protect key assets, prevent access to information and **ensure that attackers do not leverage the least protected nodes in a network, its edge devices**, to gain access to larger, more sophisticated systems. There are a number of important capabilities that need to be in place on every edge device, even the most resource-constrained ones.

Data sent to and received from edge devices has to be protected. This necessitates the use of encryption and decryption enabled by a cipher – an algorithm that scrambles and de-scrambles information so that unauthorized parties are unable to make sense of it. The list of ciphers in use today is long. However, very few fit on small, resource constrained devices so that they do not impede operations in substantial ways. **Revere Security has developed the 128-bit key strength Hummingbird cipher, which has been specifically designed for edge devices.** In fact, the initial funding for Hummingbird came through a Department of Homeland Security (DHS) project to secure ICS devices that could not be protected in any other way. It is also vital to authenticate the communication with edge devices. The Hummingbird cipher accomplishes this through a built-in encryption and message authentication scheme that eliminates the need for an additional Hash algorithm, saving valuable computation time and space on the microchip.

##### Edge Security requires more than just an ultra-efficient 128-bit cipher:

- built-in single pass data authentication
- protocol-based identity authentication
- anonymous communication
- highly scalable key management system
- fast key query performance
- ability to cloak

As initially mentioned, when two parties can verify one another's identities, they can trust each other. **Hummingbird leverages a mutual authentication protocol** for this purpose. It prevents unauthorized

[www.reveresecurity.com](http://www.reveresecurity.com)

proprietary information

parties from talking to edge devices through a sophisticated challenge-response. This mechanism ensures anonymity, ensuring security and privacy protection. Simply put, both parties know a shared secret and are able to communicate with trust. The beauty of this design lies in the fact that the shared secret is never actually exchanged and cannot be intercepted.

One of the biggest challenges in information security has always been the handling of these shared secrets. A cipher uses a key as its shared secret to encrypt and decrypt information. Once an attacker has access to the key, the system is no longer secure. Distributing and then finding symmetric keys are two of the requirements that edge security providers must address. Small, resource-constrained devices such as ICS controllers, smart meters or RFID tags are usually spread out. Also, there often isn't just one domain that controls access to these edge devices. In consequence, the management of keys from insertion of the first key to reliable revocation of keys can be an enormous undertaking. Sound edge security enables the exchange of keys in regular intervals and timely revocation of keys. It is yet another pivotal requirement to establish the security of the entire system.

**Revere Security has designed an innovative key management and distribution system that allows for multi-domain key management**, meaning that more than one organization can share access to keys without giving up access to their own systems. Here, Hummingbird's capability to communicate the shared secret without transmitting it leads to complete confidentiality within each domain and between them. No organization is forced to share their secrets with others. This very issue lies at the heart of enabling true edge security. The principle is best explained when we look at an example such as a toll tag, which leverages RFID technology. Today, toll tags only work with one tolling provider. Using the innovative, patent-pending Hummingbird key management and distribution system, toll tags can be used with as many tolling providers as desired. Each is able to validate the tags' key by simply accessing its own database and, when it does not return satisfactory results, sending a query through Revere's secure key distribution system to other tolling providers. The tag will send information about its "owner" along to simplify and speed up the process. In this manner, a specific toll tag can be used by any other system as long as it has the capability to look up and find the right secret key.

## 5. Conclusion and Outlook

We live in a world with billions of smart devices, most of which connect to networks and backend systems through wireless communication. These devices are a tremendous help in our daily lives. Yet, they also pose new security vulnerabilities, which, if not mitigated and attacked, could cause major disruptions to the way in which we live and work. For system operators, the task is to identify these threats and to mitigate them while there is still time. One of the biggest challenges under these circumstances is that the rapidly emerging field of edge security is not yet covered by traditional IT security standards. This is only natural since standards have much longer development cycles than the security technologies that are needed to protect critical infrastructure today. In the interim, many companies are forced to make a tough decision: implement available security today or wait for standards to evolve first. Hackers are unlikely to wait for standards. So, the decision may not be as difficult as it seems. In fact one answer lies in what we have heard from the industry executives: **to be safe you have to deploy just a little more security than the next guy**. In essence, if you implement edge security today, you will find that you are (a) better equipped to improve your overall security while edge standards evolve and (b) you are less likely to be attacked while many edge devices are still unprotected.



At Revere, we found that a knight's armor, one of the most effective protections for medieval "edge" devices, is an appropriate analogy. Would you be able to walk around in 100 lbs. of armor today and handle most of your daily tasks? Probably not and you may well find yourself in very peculiar situations. The same is true for edge security. We cannot protect small, resource constrained devices with yesterday's armor of IT security. **After all, you probably shouldn't bring old armor to a hacker fight ...**

[www.reveresecurity.com](http://www.reveresecurity.com)

proprietary information