certicom | BlackBerry Subsidiary

WHY USE CRYPTOGRAPHY?

CONNECTED THINGS NEED STRONG AUTHENTICATION... AND MORE

It seems that every day new and increasingly dangerous viruses are infecting digital systems. Viruses with names such as Heartbleed, Shellshock, Poodle, and Bad USB have put innocent people at risk. Russian Cyber gangs (a.k.a. “CyberVor”) have exposed over a billion passwords.

The scary thing is that the attacks are targeted at the very security mechanisms that are meant to provide protection. Because the digital protection mechanisms themselves have become targets, they must be hardened.

This is especially important now that the digital universe is going through a type of Big Bang with the explosion of the Internet of Things (IoT) and other embedded networking, sending billions of little sensing and communicating processors all over the earth, like smart dust.

Growth in processing, communicating, and sensing semiconductors (which the IoT is made from) grew at a rate of over 36% in 2015 according to Gartner, dwarfing the overall semiconductor market growth of 5.7%

> *CONFIDENTIALITY.INTEGRITY. AUTHENTICITY.*
>
> *Smart, autonomous systems will multiply the number of sites for infection that hackers can attack by many orders of magnitude, making these 3 pillars of security absolutely necessary .*
>
> *Learn what forward thinking designers have already discovered about the future.*

IoT is better with Security

IoT nodes can be vulnerable in today's hyper-connected world.

It is not hard to see that trust in the data communicated by the IoT and smart systems will be necessary for wider adoption, especially as attackers become more sophisticated and more nodes become available to attack. Security matters. In fact, one of the recognized inventors of the Internet, Vint Cerf, completely agrees, saying that strong authentication is important for the IoT, and we need to make sure they are talking to the devices they are supposed to talk to.

There is much more to the story behind why the IoT and other smart systems need strong security. Because the world has become hyper-connected, financial and other sensitive transactions have become almost exclusively electronic. Money now is simply electronic data. Banks are really just databanks with marble lobbies. Databanks are where the money is kept. American bank robber, Willie Sutton, said he robbed banks because that is where the money was. Cyber criminals are attacking financial data because that is where the money is now. Corporate financial liability from data breaches is real and growing. So, CEOs should not be the least bit surprised when they start to be challenged by significant shareholder and class action lawsuits stemming from security breaches.

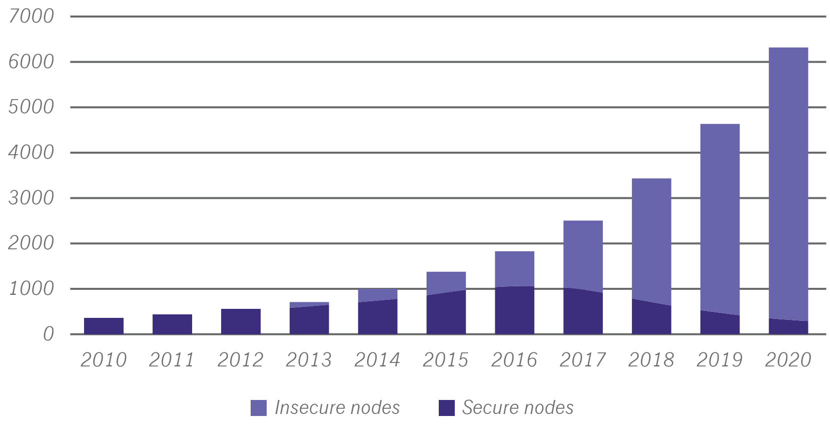
Despite being inadvertent, a disturbing number of companies and institutions are increasingly exposing the identities and sensitive information of millions of people, and they may not always be taking all the appropriate measures they could to ensure the security and safety of their products, data, and systems. This also applies to automotive companies not protecting against electronic hacking.

Exposure of personal data and safety risk from product hacking will translate to financial damages. You can be sure of that. Damages will translate to legal action.   The logic of tort and securities lawyers is that if proven methods to secure against hacking already exist, then it is the fiduciary duty of the leaders of corporations (i.e. the C-Suite occupants) to vigorously embrace such protection mechanisms, do so right now, and be able to prove that best practices were followed. Not doing so will likely be argued as being negligent.

Whether you agree with that premise or not, that line of argumentation is logical and inevitable. So, let this be a warning to CEOs, CTOs, and board members: you had better take note, because the lawyers already are. Data breaches, hacked cars, and other forms of insecurity can easily become the new class action playground, making “failure to secure” the new asbestos. It is not hard to imagine the TV commercials.

IoT Node Shipments by Year
Million Units

Source: Cisco, Ericsson, Gartner, IDC, ABI, IHS, Strategy Analytics, BI Intelligence

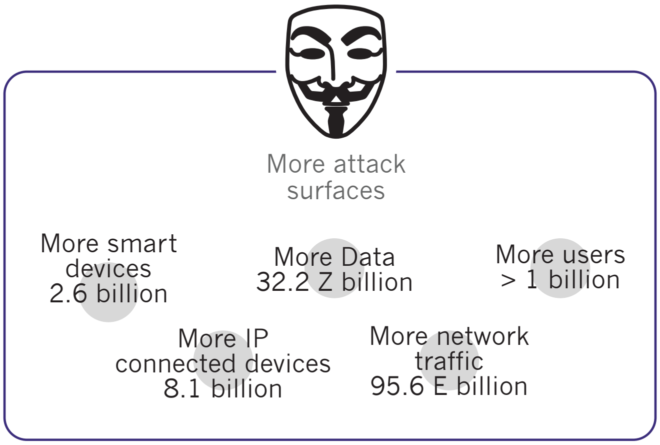


WHY CARE ABOUT SECURITY?

Because we all live in a bad digital neighborhood.

Hackers steal passwords, digital IDs, IP, and financial data, so security must be designed right into the product from the start. Emerging and evolving applications such as IoT, cloud computing, wearables, vehicle–to-vehicle communications, mobile, smart home, and others will give rise to billions of smart communicating devices andnodes that can be attacked from anywhere. Everyone is exposed to data breaches, and that can cause damages and unprecedented corporate liability. The US judicial system is now allowing lawsuits stemming from data breaches. And, the FTC has declared that security is the responsibility of companies.

Also, with the widespread use of contract manufacturing, control of the process is surrendered to the contract manufacturer, making companies vulnerable to cloning, counterfeiting, and overbuilding. So, it is a good idea to ensure that only authorized products get to market in order to protect a company's revenue stream, brand image, and reputation.


More attack surfaces
More smart devices 2.6 billion
More Data 32.2 Z billion
More users > 1 billion
More IP connected devices 8.1 billion
More network traffic 95.6 E billion

Today, everyone is everyone else's electronic neighbor, because we are connected to each other via the internet. This applies to medical, automotive, industrial, consumer, mobile and other devices, networks, and ecosystems. Unfortunately, that means that electronically we all live a bad neighborhood because bad operators can go everywhere electronically. Hackers, phishers, scammers, cyber criminals, state sponsored electronic armies, and

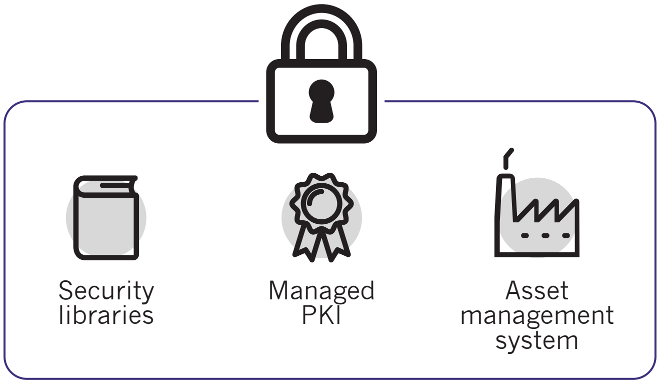
Beckstrom's Law of Cyber Security

1. Anything attached to a network can be hacked
2. Everything is being attached to networks
3. Everything is vulnerable

Rod Beckstrom, former president and CEO of ICANN, founding Director of US National Cybersecurity Center other bad actors can target anyone and anything. There are even search engines that help them find things that they can target.

Therefore, it is easy to see that security is a requirement in the connected world to build secure gated electronic communities. To put it another way, an ecosystem is not really useful unless it is secure, right from the start.

Tested and battle hardened security software libraries and certificate management solutions make it possible to create and manage a root of trust and certificate chain to implement secure ecosystems. Asset management systems can build security into electronic devices right from the start of their manufacture. These are all key elements of a comprehensive security profile. Certicom provides these critical elements, and in fact literally invented many of the fundamental algorithms that make robust security possible.



IF IT CONNECTS...CERTICOM PROTECTS

ECC: ELLIPTIC CURVE CRYPTOGRAPHY

ECC is both strong and fast enough for modern security apps.

ECC is a modern cryptographic technique which provides much stronger security for a given key size than other popularly deployed methods such as RSA. That makes ECC more efficient in terms of processing power to obtain a given level of security.   In other words, you get a bigger bang for the buck with ECC. More security for lower processing requirements reduces cost, size, and complexity of the crypto system. Smaller and less expensive processors can be used. Also, less memory is required, and less communication time is needed. In emerging automotive applications such as Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and even In-Cabin systems, ECC is becoming a requirement since older algorithms just cannot make the computations in time, which of course is critical.

Remember that the mathematics of security is based upon a key, and the strength of the key is directly related to the key size. A longer key size (i.e. a larger number) for a given algorithm always means stronger security. However, a given key size will have differing security levels when used in different security algorithms. In order to obtain commercial grade security, a key size of 256 bits is needed with ECC whereas 3,072 is needed with RSA, making ECC six times more efficient. For classified government grade security ECC is thirty times more efficient. And that is obviously a lot. So, you can see why automotive manufacturers are now considering ECC for their in-out-and-all-about security requirements going forward. This also applies to medical, industrial, commercial, military, financial, mobile, IoT, and other segments.

ECC's efficiency and strength make it ideal for Public Key Infrastructure (PKI) operations such as ECDSA (Elliptic curve Digital Signature Algorithm) which uses public and private key pairs to establish authenticity of products, people, code, IoT nodes like sensors and actuators, and other things. ECC is also used in confidentiality applications (i.e. encryption and decryption) to securely exchange keys without having to reveal private keys. A very elegantly simple yet highly secure technique called ECDH (Elliptic Curve Diffie Hellman) makes that possible. Once both sides have the same key then they can exchange encrypted messages and decrypt them without worrying about a man-in-the-middle obtaining the key and listening in or corrupting the data. Related techniques can be used to check that the encrypted message received has not been altered in any way thus providing data integrity. So, all three of the pillars of security, namely, Confidentiality, Integrity, and Authentication, can be easily and efficiently achieved using ECC-based crypto methodologies.

When it comes to robust security, Certicom offers Elliptic Curve Cryptography (ECC) algorithms validated to government-grade FIPS 140-2 Level 1, which is required to sell into Veteran's Administration (VA) hospitals and other governmental establishments. Validated crypto software libraries make it easy to add cryptographic algorithms to systems without having to become a crypto expert, and are among the most advanced in the industry to provide confidentiality, data integrity, and authenticity at the highest levels. The quality of the solutions makes perfect sense since Certicom invented and holds patents for many of the most fundamental ECC technologies. In fact, the National Security Agency (NSA) licensed Certicom's patents in order to make ECC a powerful crypto standard.

Using Certicom's government validated crypto libraries, PKI certificate solutions, and asset management system makes products, ecosystems, and supply chains not just secure, but BlackBerry Secure.

Not just secure... but BlackBerry secure

There is a reason that BlackBerry is synonymous with mobile security. It is because security is as elemental to an electronic system as DNA is to an organism—and security is BlackBerry's DNA.

Robust security cannot just be bolted on. It must be infused right from the start, which is why BlackBerry Security has been trusted by world leaders for over two decades and is the mobility partner of all G7 governments, 16 of the G20 governments, 10 out of 10 of the largest global banks and law firms, and the top five largest managed healthcare, investment services, and oil and gas companies. BlackBerry Security has earned more than 70 government certifications and approvals - greater than any other mobile vendor.

The iconic example of the depth of trust in BlackBerry Security is probably the NSA's licensing (and standardizing) of Certicom's Elliptic Curve Cryptography (ECC) algorithms, which are quickly becoming the accepted crypto standard for enterprise, government, automotive, mobile, medical, industrial, and IoT security.

Vulnerabilities are growing rapidly and present a serious risk for public and private sector organizations, so BlackBerry continues to expand its coverage with advanced technologies, tools, design consulting, and testing services for true end-to-end, layered security. The goal is simple: to ensure there are no back doors, open windows, or lost keys to exploit—anywhere in the system.

In mobile, coverage begins at the crucial hardware root of trust. OS and software authenticity is securely verified every single time any BlackBerry device in the world boots up. Data is encrypted right on the devices, in the trusted network, and behind the corporate firewall. In operating systems, the BlackBerry-QNX Neutrino microkernel ensures safe and reliable operation robust enough for over 40 car models, the space shuttle, and nuclear plants. It is designed to fail safe, and protect against malware, tampering and data leakage. Thanks to Certicom's Security Builder Software Libraries, certificate management solutions, and secure manufacturing systems, it is easy to obtain government approved

(FIPS 140-2 Level 1) validation, manage security certificates, and secure manufacturing lines without becoming a crypto expert. That's what is meant by "Not just secure, but BlackBerry Secure."

BlackBerry and its subsidiaries, Certicom and QNX, provide products and services that make things not just secure, but BlackBerry Secure.

Certicom Corp., subsidiary of BlackBerry manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM,General Dynamics, and SAP. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada.

www.certicom.com

QNX Software Systems Limited, subsidiary of BlackBerry is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada.

www.qnx.com