Keywords: security, encryption, privacy, authentication

APPLICATION NOTE 5932

FUNDAMENTALS OF ELECTRONIC SECURITY: WHAT DOES SECURITY REALLY MEAN?

By: Ben Smith, Software Manager

Abstract: In this article we will explore the very basic concept of security—when physical locks are less mportant than the logical and virtual fences that we place around our online lives. In subsequent articles we will look at what security means in a massively interconnected world, the factors that threaten security, and the factors that pose apparent threats but are actually benign. We will also explore how security should work and what may be coming in the future.

A similar version of this article appeared October 5, 2014 on *Embedded*.

Introduction

Electronic security. This topic seems to be on every tongue today, and for good reason. In our increasingly interconnected world, security is essential if we are to preserve privacy, promote business, and reduce criminal activity. In a simpler time, enhancing security might have meant putting better locks on the front door. But we live in a world where every home has a high-speed connection to millions of other computers, where business transactions take place at the speed of light through glass fiber, and where stored value can mean a sequence of digits embedded in a bar code. So what does "security" really mean today?

In this article we will explore the very basic concept of security—when physical locks are less important than the logical and virtual fences that we place around our online lives. In subsequent articles we will look at what security means in a massively interconnected world, the factors that threaten security, and the factors that pose apparent threats but are actually benign. We will also explore how security should work and what may be coming in the future.[1]

Essential Functions of a Secure System

All of us have a casual understanding of what we mean by security. We expect that no one will break into our home while we are away. We expect that our money in the bank will still be there when we want to withdraw funds. We expect that the channels of transactions will always be open and safe. We expect that our messages will be delivered and not intercepted by others. If we are running a business, we expect reliable operations with consistent uptime and without electronic disruptions or threats. In simple terms, we want what we expect in any given context.

This all seems straightforward…so far. But it is more difficult to define exactly what we expect from a system that claims to be "secure." We still want what we want, but translating notions of safety and reliability into a set of policy and operational rules (not to mention algorithms and code) can be daunting.

Perhaps the best way, or the most efficient way, to define security is to examine what it should do. As a starting point, here are a few concepts that exemplify a secure system. A secure system must:

Protect an *identity*. It ensures that no one can effectively impersonate anyone else.

Protect my *privacy*. I must be able to choose the information I wish to reveal, and to whom I will reveal it.[2] Reciprocally, I will not receive information not intended for my eyes.

Be *accurate*. Any information that I send to, or receive from another must be transmitted verbatim. It cannot be altered, whether accidentally (because of transmission errors or other factors that inadvertently corrupt the message) or intentionally (because an attacker intercepts the message and changes something). If information becomes altered along the way, the receiving party must be able to determine that the message was corrupted en route.

Guarantee *authenticity*. Someone receiving a message must be able to verify who sent it.

Protect *place*. There are places, private and public, personal and business, with controlled entry. As private owners or business managers, we must be able to authorize or deny access with complete confidence in the integrity of our systems.

Resist the use of *force*. We should expect a secure system to put up a valiant effort to resist any threat. We should also expect a secure system to mitigate threatened force by any of several techniques that might include rendering the valuable content worthless to the attacker, or at least notifying the rightful owner that someone is trying to invade.

Protect against any potential *opponents*. Even if attackers are well funded, clever, and determined, a truly secure system must continue operating as designed even in the face of a sophisticated assault.

This list is long enough. There are undoubtedly more fundamental criteria for a secure system, but just from this brief list you can see that security is *hard to do*. Well-funded, determined opponents can, and have, broken barriers thought to be very secure.[3] Identities are stolen, documents are forged, and reputations are destroyed. Very smart people have spent very long hours attempting to craft security systems, and equally smart people are, regrettably, working long hours to break every security measure.

Reduce the Threat by Raising the Risk

We should now ask two fundamental questions. First, what measures *can* we take to make our personal and professional assets a less attractive target? Second, how much security is enough? Simply put, can we make an attack on security so costly, so risky that it exceeds the value derived from the attack? Yes, we can. And in doing so, we will stop some attacks before they start.

Every aspect of our assets that presents an opponent an opportunity for attack can be classified as an *attack surface*. And the actions that we can take to mitigate the consequences of an attack are classified as *countermeasures*. Our objective in designing a secure system is twofold: to limit the availability of attack surfaces; and, wherever we must expose an attack surface, to incorporate effective countermeasures to reduce the attractiveness of the attack surface.

Consider a simple example. If you heard that burglars were breaking into neighborhood homes by picking the front door lock, you might select from a fairly standard set of countermeasures: a stronger lock, a guard dog, or perhaps a security system with signs prominently posted. You cannot eliminate every attack surface —bricking in the front entryway is not an option. But you can certainly raise the cost of an attack by raising the effort required to gain access (the improved lock), escape the threat of physical harm (the dog), or avoid detection and prosecution (the alarm).

So when securing commercial products and services, that is exactly what we have to do: raise the risk of mounting an attack. We must, moreover, reduce the likelihood that an attack, once mounted, will be successful and increase the probability that any attack, successful or not, will be detected.

Closer Look at Attack Surfaces

Not surprisingly, many commercial products and services share a common set of attack surfaces.

Communications interfaces. In our hyperconnected, always-on world, everything communicates. Not surprisingly, the phrase “Internet of Things” (IoT) has become a dominant meme. But an always-on communication interface is a tempting attack surface. In the past, one could mitigate such a threat by unplugging a modem or turning off a radio, but no more.

Software. With the price of embedded intelligence approaching zero, it is tempting to put some kind of intelligence in just about everything. And that means that just about everything contains a software component. But because software, by its very nature, is ephemeral, it is a tempting attack surface.

Peripheral interfaces. For a credit-card terminal, it is the card reader. For an automotive microcontroller, it is a sensor. For a smart electricity meter, it is the metrology components. All of these peripheral interfaces are subject to attacks attempting to fool the device into behaving in ways that the designer did not intend. By manipulating these interface points, an attacker could cause the device to provide bogus billing information to a retailer, to change the performance profile of the car, or obtain free or low-cost electricity.

Environment. In a sense, it is amazing that the devices we carry around in our pockets are capable of performing billions of operations per second on billions of bits of information, and do this task without error. But if errors can be induced by some physical disturbance, an attacker may be able to exploit those errors in an attack scenario.

Sensitive material. Increasingly, smart devices deal with extremely sensitive information, whether of a financial, legal, or medical nature. Any highly sensitive or classified material is not, by itself, an attack surface, but this content makes any device housing it an attractive target.

Summary

In many ways the pace of technology has evolved more rapidly than our ability to use it securely. Even the very concepts with which we deal daily—identity theft, viruses, Trojans, and spoofing, among many others—would have sounded like a foreign language just a generation ago. But with every new attack front we also find a new opportunity to make our lives more secure and our enterprises more fruitful.

Once you understand the role and critical need for security, then it is time to assess any attack threats. That is what we will do in our next article on attack methods. In future articles, we will examine the measures that we can employ to make those attacks unsuccessful.

References

1. The marketing consultant group, Experian, reports in their **2014 Data Breach Industry Forecast** that: "The number of data breaches both experienced and reported is expected to continue to rise, with new security threats and regulations pushing for more transparency on the horizon. All signs are pointing to 2014 being a critical year for companies to better prepare to respond to security incidents and data breaches." See www.experian.com/data-breach/data-breach-industry-forecast.html.
2. CSID is "a leading provider of global enterprise level identity protection and fraud detection solutions and technologies." www.csid.com/. They note that credit and debit cards are the most commonly beached credentials, together representing 62% of the information breached," www.csid.com/resources/stats/data-breaches-by-industry/.
3. IT Business Edge records **The 10 Worst Data Breaches of 2013**, www.itbusinessedge.com/slideshows/the-10-worst-data-breaches-of-2013.html. Some security breaches in prior months are discussed by David Andeen in the Maxim Integrated application note 5537, "Smart Grid Security: Recent History Demonstrated the Dire Need," also at **Power Systems Design**, "Smart-grid security; history demonstrates need," December 2012, pp. 33 – 36, www.powersystemsdesign.com/library/resources/images/IssuePDF/psde_december12.pdf.

IBM reports **1.5 million monitored cyber attacks in the United States in 2013**. We should note that this report focused on the U.S. only, so we can easily understand the magnitude of the problem worldwide. They continue: "Data breaches are among the most common and costly security failures in organizations of any size. In fact, studies show that companies are attacked an average of 16,856 times a year, and that many of those attacks result in a quantifiable data breach. And with today's data moving freely between corporate networks, mobile devices, and the cloud, data breach statistics show this disturbing trend is rapidly accelerating." See www-935.ibm.com/services/us/en/it-services/security-services/data-breach/.

CSID tracks data breaches by industry, focusing on business, education, financial, government, and healthcare. They comment that "Data Breaches are a threat across all industries." www.csid.com/resources/stats/data-breaches-by-industry/.

Related Parts		
MAX32590	DeepCover Secure Microcontroller with ARM926EJ-S Processor Core	Free Samples
MAX71637	Energy Measurement SoCs	Free Samples
MAXQ1010	DeepCover Secure Microcontroller for Security Tokens with RTC and USB	
MAXQ1050	DeepCover Secure Microcontroller with USB and Hardware Cryptography	

More Information
For Technical Support: http://www.maximintegrated.com/en/support
For Samples: http://www.maximintegrated.com/en/samples
Other Questions and Comments: http://www.maximintegrated.com/en/contact

Application Note 5932: http://www.maximintegrated.com/en/an5932
APPLICATION NOTE 5932, AN5932, AN 5932, APP5932, Appnote5932, Appnote 5932