The Future Of Perimeter Security

"Securing The Mobile Edge™"

By: Norm Laudermilch
Chief Security Officer
Trust Digital, Inc

Abstract:

The notion of perimeter security is not a new one. Securing the enterprise connection points where the trusted network meets the untrusted world has been well studied and scoped. We, as industry security experts, have a handle on perimeter security. Or, do we? Do we really know the extent to which the trusted network creeps into the unsecure unknown? Does this connectivity creep have to be hardwired to count? Or do wireless access methods, USB wristwatches, and Pocket PC's present the same threats that uncontrolled Internet access points did five years ago, and therefore fall into the same category? These types of connections are in fact, a real security problem, for real world environments -- one that poses huge threats to the integrity of our businesses. The purpose of this paper is to examine the security threats posed by emerging mobile and wireless technologies and present a lasting solution for securing the Mobile Edge™.

What's NOT the Problem?

The number of discussions and presentations that attempt to describe and categorize the nature and scope of the mobile security problem *IS* staggering. We get bombarded by falling sky headlines and three-paragraph trade articles all day, but I've yet to see a meaningful solution presented.

"Mobile Data Places IT Security At Risk"
"Tiny Storage Devices Carry A Big Risk"
"Mobile Phones – An Ear Full of Worms"

This is frustrating, because being educated on the threats and problems is only part of the reason we read about these things. When reading about a problem, I'd also like to read about a solution! To avoid forcing this annoyance on you, I'd like to start by examining that which is NOT the problem, and then present a rationale that leads us to a solution. To start, we know that the problem at hand is NOT about:

- user authentication,
- software integrity,
- encryption and privacy,
- writing security policy, or,
- today's mobile devices.

While these are well understood tenants of enterprise security that can be utilized along with best practices to provide a reasonable level of security, they are nonetheless point solutions which are not capable of addressing the new problems associated with highly mobile devices.

Understanding the True Extent of the Problem:

The *solution* to the problem may consist of some, many, or none of these elements, but *the actual* problem has nothing to do with any of these elements directly. Interestingly enough, the companies trying to solve the mobile security problem have enthusiastically focused on point solutions in each of these categories.

The reality is that technology changes too quickly to merit a solution specifically targeted to today's mobile devices. Today's mobile devices will be tomorrow's eBay fire sales and doggy chew toys. What happens to those point solutions then? User authentication, software integrity, encryption and privacy – all of these areas have fully baked products, algorithms, methods, and processes today and many of them are effective. However, focusing on any of them specifically is silly, because the lasting solution will not be tied to any of today's specific implementations. A lasting solution must be tolerant of implementation evolution.

Having established that the existing point solutions are insufficient, let's address the real problem. Sun Microsystems thought they were clever back in the 90s with their "The Network is the Computer" slogan. The real issue now is that everything is the network, the network carries data that needs to be secured, and therefore everything needs security. Overly dramatic, I know, but the point is that there are many devices on "the network" that can participate as gateways now, and therefore defining the "perimeter" becomes more complex. In fact, the perimeter as we think of it has now effectively grown to include *every* node on the network, essentially dissolving the historical definition.

With every node on the network now capable of extending the network perimeter, we are presented with a much broader security problem. No longer can we protect our wired Ethernet network and be safe; we now have to worry about devices with IRDA, Bluetooth, 802.11 and other over the air technologies, as well as removable mass storage via USB and traditional physical port connections as well as standard plug-n-play devices such as floppy drives, CD/R drives and other modes of mobile data storage. Each point of connection provides a new avenue for data leakage as well as a new vector for introduction of malicious software. Also, the plethora of portable devices that connect to our network and then walk away with our data, like iPods, Smartphones, PocketPC's, RIM's, and Palm Pilots, also creates new challenges. Figure 1 shows an example of one of these mobile devices and highlights a few areas where it can interface and exchange data – introducing even new vectors for corporate data exchange as well as new vulnerabilities.

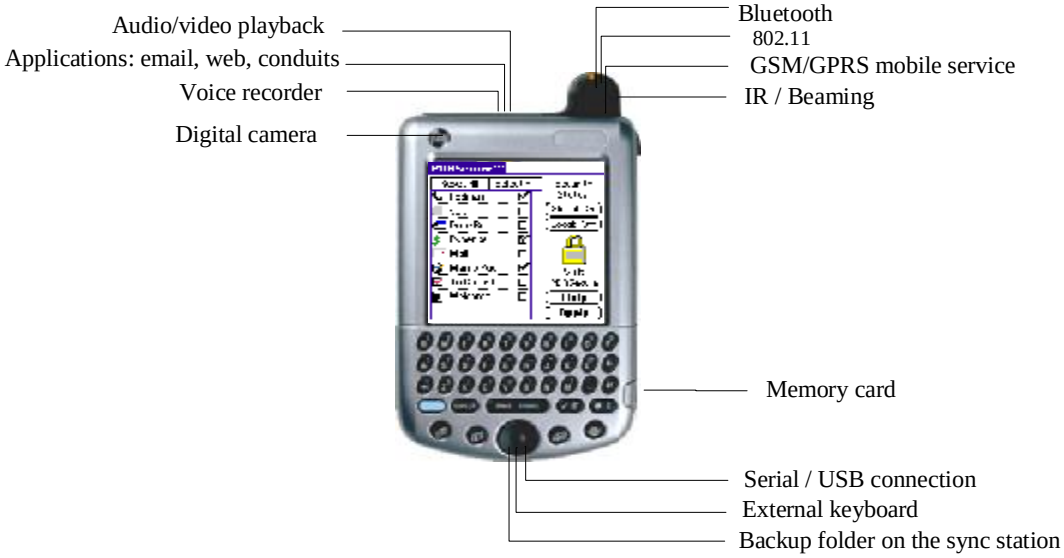

Figure 1

The fact that these portable gateway devices do not always operate as "real-time" gateways only compounds the security risk. I present the following example as an illustration:

- Joe brings his new handheld computing device to work. He connects the device to his desktop computer USB port, accepts the default answers to the questions he is asked from the sync software, and effectively copies all of the information in his corporate email/calendar/contact application to the handheld device. The device, firmly affixed to Joe's belt, walks out the front door of the office building at 5:01PM and ends up connected to his desktop machine at home an hour later. The sync software does its job, copies all of the information to his home desktop email/calendar/contact application, where it is immediately picked up by the worm/trojan of the month and sent over the Internet in clear text via Joe's cable modem. A week later, the company directory with home and cell phone numbers, as well as several presentations about the company's 10-year strategy show up on message boards and are picked up by the competition.

The definition of a Network Gateway from Wikipedia is: A network node equipped for interfacing with another network. As you can see, even without any traditional networking capabilities, the mobile device in the example above participated as a network gateway and allowed the release of proprietary company information from inside the Company's network to the Internet. With the complete lack of security mechanisms in this example, a security administrator would have a very difficult time piecing together what happened when confronted by upper management. There was no authentication required to take this data out of the corporate environment, no auditing or logging of what was taken or who took it, and certainly no security mechanisms to protect the data transfer itself.

Imagine how this scenario could have magnified if the handheld device had 802.11 or Bluetooth wireless capabilities? What if the device were lost or stolen? Could the same thing have happened? Absolutely. Now, let's take it one step further. In an extension of the above scenario, the handheld device could have easily carried malicious code into the corporate network, creating a bi-directional security threat and therefore, adding additional risk and liability not to mention the administrative headaches and other resources required to clean up these types of messes.

So, we now understand the network perimeter system to be a chaotic, morphing, and ever changing system that is never at rest. We are stuck with a dynamic and undefined perimeter! We are stuck with the task of constantly assessing the changing risk on that perimeter, defining the appropriate instantaneous security policies at a changing number of points, and enforcing those policies in real-time.

And the Stakes Are Getting Higher…

So, what does this mean for the future of enterprise security? To date, we have focused on only a very small portion of our network security. The changes in security brought about by ΔM (the dynamic nature of mobile devices based on their ever changing location, network connection, software use and other traits) are significant, and are not being adequately addressed by point solutions. Remember the rule of enterprise security - your network is only as secure as its weakest link. So, if we continue to think that the security provided by firewalls and intrusion detection devices at wired perimeters is sufficient to protect a company's intellectual property, we will all be victims of the highly vulnerable, and unsecured Mobile Edge™.

What good are standard security practices if the activity you are trying to manage and secure is basically invisible?

- No authentication
- No authorization
- No auditing
- No privacy
- No policy enforcement
- And more

Of course, you *do* have these security mechanisms in place on your wired network, but if you have tens or even hundreds of other access points that bypass these controls, what good are they?

The failure to address this security problem has opened up new categories of propagation vectors to the malicious community for the distribution of worms, viruses, Trojan horses, and other forms of malicious code. We now see worms that propagate through Bluetooth – how long will it be before malicious attackers determine that the least protected point of access to the corporate network is via our mobile "productivity enhancers"?

Additionally, we are at imminent risk of failing ever-expanding compliance mandates. Our failure to take sufficient action likely violates one or more regulatory requirements as set forth in HIPAA, GLBA, SB1386, SARBOX, and other regulatory vehicles. Not only are financial and criminal penalties possible, but the entire FATE OF A COMPANY falls into risk when sensitive, proprietary data falls into the wrong hands.

Why Having a Bunch of Ineffective Point Solutions Around Isn't All Bad…

As you can well imagine, the proliferation of point solutions speaks of a poorly understood problem being addressed by band aids. Even though these point solutions may provide temporary pain relief, the 'rush to solve' mentality is a

shortsighted, ineffective means to addressing the problem. But all is not lost, because we're actually tracking to progress in a roundabout way. History presents us with numerous affirmations of the following axiom:

- The frequency with which point solutions appear is directly related to the proximity of a real innovation in the field

Let's call this "Norman's Law". Basically, the scope and definition of a problem can morph as detailed knowledge of that problem grows. In the beginning, it may seem that the lack of encryption is the problem and a point solution is created to address it. But, hold on a minute, authentication is also part of the problem, so another point solution is released. And, ugh, hang on, trusted applications too – better generate another point solution. Ultimately, once the problem is fully understood, a revolutionary approach to the problem is generated, and truly effective innovation is born. Examples include assembly lines, the printing press, Ethernet, etc. The good news is that we have enough fundamental understanding of the extent of the problem under our belts, that we now know how to construct a meaningful solution.

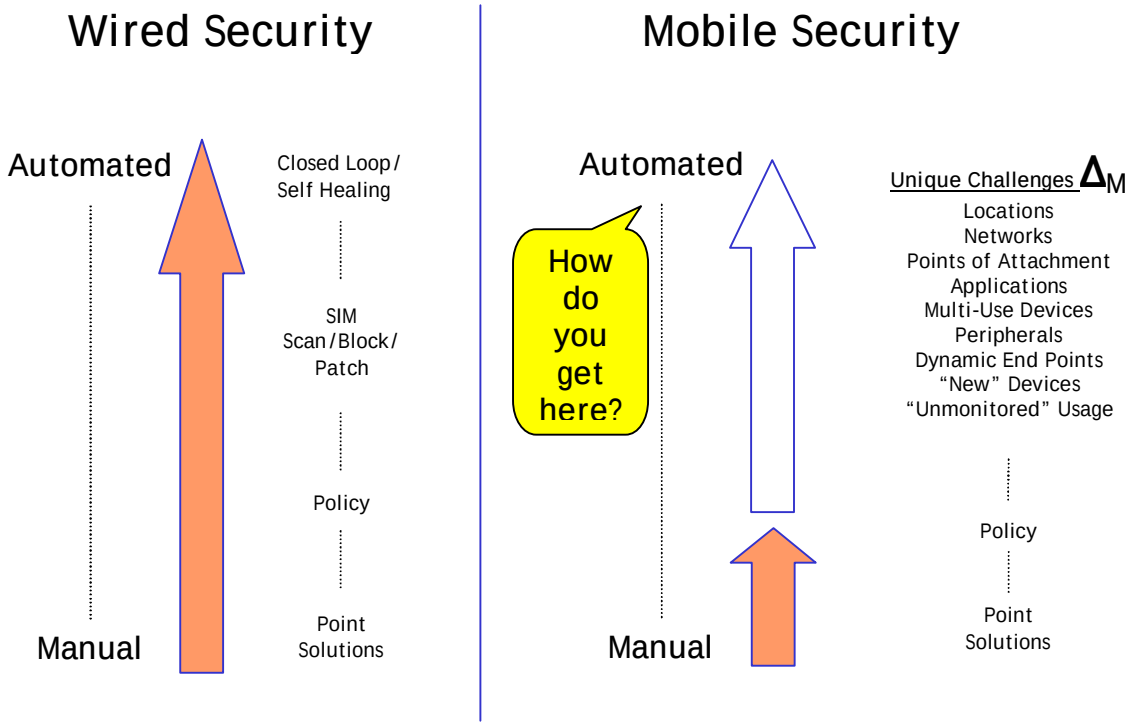

Figure 2

Figure 2 shows how the perimeter changes brought about by mobility, something I will call ΔM, compare with traditional wired security technologies. Constant technology change drives additional point solutions, but the rate of technology change has outpaced the ability of innovators to create point solutions.

With an Understanding of the Problem in Hand, We Can Establish a Mission, and Map to a Solution:

The problem of securing the Mobile Edge™, or the ever changing network perimeter, is that an extensible framework does not exist today. But to create one that provides constant assessment of dynamic risk, generates policy automatically to mitigate that risk, and enforces that security policy across the Mobile Edge™ is difficult. The current point solutions on the market don't cut it. Additionally, we need a solution that abstracts the key security parameters from the end devices and provides the modularity to change as mobile technology continues to evolve. We need a framework that automates security in a transparent way and still allows the flexibility and productivity increases that the mobile user demands.

I'm a strong believer that the best way to define and build a solution to a set of technical problems is to describe your desired output from the beginning. This is the fastest road to a revolution, as point solutions only address each small piece of the problem from one perspective. Based on the arguments and the analysis of the problem, a starting "mission" for our solution might look something like this:

- Apply sound, security practices to the metamorphic perimeter in real-time without impacting the usability of the devices involved or the productivity gains those devices provide.

It's a good starting point, but the problem with this mission is that it doesn't address how we're going to make the solution stand the test of time. If we start with the mission above, we may very well end up with yet another, albeit much broader, point solution that relies on current technologies and solves the problem of security at the Mobile Edge™ only until that point at which technology changes again. This mission also doesn't capture the ubiquitous mobility factor that has become a staple of modern computing. Furthermore, this mission fails to capture the fact that the only way for a solution like this to be effective is for it to be a centralized, enterprise solution that removes the requirement of end-user involvement. A more appropriate mission that states the problem as well as the requirements for timelessness, mobility, and centralization would look something like this:

- Provide a centrally managed extensible framework for the discovery of risk, the automated definition of security policies, and the enforcement of those policies to the metamorphic Mobile Edge™ in real-time, without impacting the usability of the devices involved or the productivity gains those devices provide.

This mission is much more complete. It captures one very important element: the tool really required to solve this problem is likely a framework, or wiring harness, that provides the *foundation* for solving the bigger problem. This core structure or backbone would allow point solutions and technology du jour to plug into functional sockets. Let me give you another illustrative example:

- Back in the early and mid 1970's Robert Metcalfe was doing some interesting work in computer networking at the Xerox Palo Alto Research Center (PARC) in Palo Alto, California. There had been many previous advances (point solutions) in the area of networking, but none were widely adopted. All of the solutions could pass data, but the solutions only worked for a small number of computers, some didn't pass data fast enough, some could not detect collisions on the network, etc. You see, none of these point solutions solved the broader problem because the focus, scope, and definition of the problem had not fully matured. Along came Metcalfe, who defined the problem more broadly, building a framework that defined how to transmit data and how to detect collisions, rather than how to use current technology to solve a point problem. Arguably, his mission (make it fast enough for the new Xerox laser printer and connect hundreds of computers) is still shortsighted by today's standards, but Metcalfe displayed genius by making his solution modular and extensible, addressing the problem once and for all.

Why is this example important? The most commonly used local area networking technology today is Ethernet. The Ethernet framework that was developed at PARC over 30 years ago has withstood the test of time and lived through all of the technology advances. Our networks today are over 1000 times faster than the original, but the underlying framework is still there. The solution was a revolution, and it remains timeless. Henry Ford's assembly line approach is another superb example of a timeless quantum leap in refining and improving quality of production.

Mapping to the Working Solution…

With such examples in mind, let me introduce a working perimeter security framework that provides a constant 'discover, decide and secure' model based on the dynamics of mobile device usage.

The Mobile Edge™ Security Framework solves the security problems presented by ΔM (Figure 2) by applying traditional security mechanisms, but it deploys them using a different approach. We needed to apply a different approach in order to reckon with the fact that traditional security mechanisms do not handle perimeter flux very well. And, by creating an abstracted security layer that augments many of the existing wired security systems in place today, we effectively leverage existing investments but apply them in unique ways based on a clear understanding of dynamics of mobile device usage.

To achieve our stated mission, we set forth the following goals for our framework:

- Provide the tools to discover mobile data threats across the enterprise to augment existing vulnerability and compliance tools
- Enhance existing intrusion control systems by creating a way to describe the trusted "state" of these mobile devices as a basis for identification and access control. (While not inherently different from evolving NAC/NAP approaches, this provides a layer of protection, independent of point of connection – PC, WiFi, Internet,, Cellular)
- Provide a centrally managed policy engine to apply common end point security practices and mechanisms in their mobile context including:
  - Authentication
  - Application Management
  - Data Protection (Encryption)
  - Device, Resource and Physical Port Management
  - Management of other technologies such as personal firewalls, enterprise VPN access and anti-virus applications (as required on smaller, mobile device form factors)
- Leverage existing security policy information such as password policies, firewall policies, and VPN policies, by crawling through existing enterprise management tools and pre-populating relevant Mobile Edge™ security policy fields for time and cost savings

To ensure the longevity of this approach, the framework architecture would obviously be modular in the way it defines and manages each of the end point security functions so that it could be quickly adaptable to the ever changing threat characteristics and their associated solutions. The management of these components at the center of the network, rather than at the mobile perimeter,

further ensures flexibility to detect and quarantine new features or devices even before solutions have been created.

If we proceed with these goals in mind, we can develop a revolutionary solution.

- **DISCOVER**: Discover the exact state of the Mobile Edge™ at a single point in time, and persistently update edge state information
- **DECIDE:** Apply information about edge vulnerabilities to the current state of the edge to determine its instantaneous vulnerability state and then based on known risk factors and enterprise policies, automatically generate a security policy to mitigate the instantaneous risk state at the edge
- **SECURE**: Push security policy to the edge and enforce security decisions set forth in that policy

The desire to perform this action hints at the area where most of the Mobile Edge™ Framework focuses. In particular, the Framework is a set of services that monitors the state of the Mobile Edge™, and processes admission criteria and associated rights of Mobile Edge™ Devices and enforces security policies based on the actions being attempted by the device.

Figure 4 shows how the components work together logically.

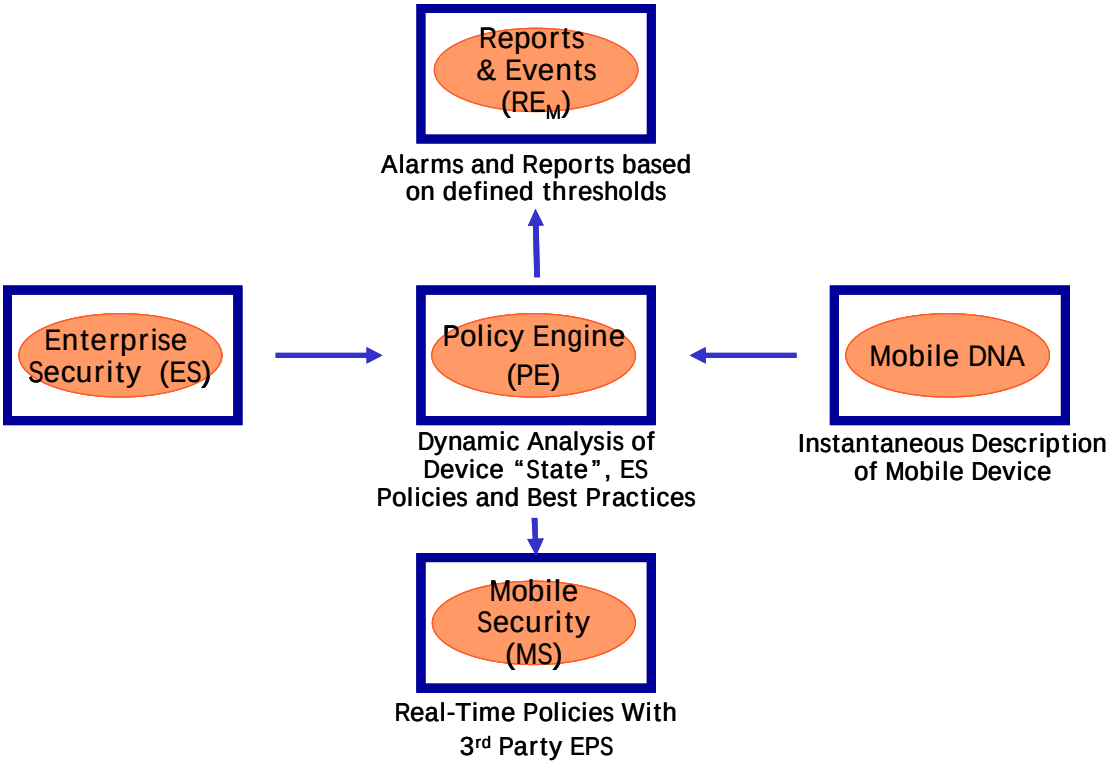

Figure 4

The combination of these Framework components provides a comprehensive solution for applying standard security practices at the Mobile Edge™. It allows the application of appropriate, fully baked, security processes and protocols (auth, crypto, etc) in a framework that solves a much bigger problem. It gives the ability to plug in or unplug technologies as they change, eliminating the need to change the framework or underlying infrastructure as technology progresses. It also provides a mechanism for dynamically assessing risk at the Mobile Edge™ and enforcing policies that transparently protect that edge in real time. In essence, the Mobile Edge™ Security Framework achieves the goals that we set out to achieve in the beginning, and provides an extensible solution that completes our stated mission.

The Benefits:

There are many benefits to a solution like the Mobile Edge™ Security Framework. For instance:

- The continuous 'discover, decide, and secure' cycle assures security administrators that security vulnerabilities are discovered and mitigated quickly, effectively, and automatically. New security vulnerabilities that cannot be associated with some form of policy logic can be quarantined and be quickly brought to the attention of the security officers

- The longevity of this approach is critical for justifying the investment. By leveraging existing investments in IT and security infrastructure and providing the modularity to support future requirements, this framework becomes the foundation for secure and productive access to mobile information.

  The cost of maintaining a centrally managed and controlled framework is significantly less than the manual, resource intensive oversight of disconnected point solutions on individual devices or platforms.

- This end to end approach to securing and managing the mobile perimeter ensures user productivity without creating unnecessary corporate and regulatory risks while also minimizing IT headaches. It provides end-to-end data protection to eliminate risks associated with lost or stolen devices. It protects corporate data and mobile resources from unauthorized mobile device intrusions.

- And finally, it ensures predictable and secure mobile device usage for everyone.

The Evolution of a Revolution

Although news and hype about point solutions muddy our ability to effectively understand the Mobile Edge™ security crisis, we have become far smarter in our ability to understand the dynamic nature of the problem. According to "Norman's Law", we are approaching that point in time when meaningful whole solutions manifest from the relative chaos of point solutions. As discussed, our ability to more deeply understand the technology challenges with the new mobile perimeter creates opportunity for revolutionary leaps in effectively addressing these challenges. Such is the case with the Mobile Edge™ security crisis. As evolutionary understanding takes place, effective innovation is right around the corner. The approach outlined above is not simply representative of the latest progressive thinking on mobile security solutions; this approach has been effectively productized by Trust Digital, with clients now benefiting from its enterprise infrastructure focus, scalability, and modularity.

