IT@Intel White Paper

Intel IT
IT Best Practices
IT Consumerization and Information Security
September 2011

Enabling Smart Phones in Intel's Factory Environment

Eran Birk
IT Client Security Architect
Intel IT

Jay Alexander
Project/Program Manager
IT Factory Automation

Executive Overview

Intel IT is investigating the feasibility of allowing manufacturing employees to use corporate-owned smart phones in the factory environment. Smart phones are not permitted in factories due to concerns about intellectual property leakage and radio frequency interference with manufacturing process equipment.

We conducted a proof of concept (PoC) that explored how we might allow factory employees to benefit from smart phones while at the same time protecting Intel's intellectual property and manufacturing processes.

Currently, manufacturing employees can use only basic corporate-owned cell phones with voice and text messaging features. These phones have no camera, video, or Wi-Fi* features, nor do they support e-mail, enterprise applications, or advanced mobile capabilities. This means that factory employees cannot take advantage of the productivity features of smart phones when in other environments—such as in the office, at home, or while traveling. We must also consider that basic phones without cameras and Wi-Fi have become difficult to find in today's marketplace.

Because enabling Intel's factory employees to use smart phones would provide them with the mobility and productivity benefits that other Intel employees enjoy, we conducted a proof of concept (PoC) that explored how we might allow factory employees to use smart phones while at the same time protecting Intel's intellectual property and manufacturing processes. We tested a system that performed four primary functions:

- Detected that a device was about to enter the factory environment.
- Determined if the device was IT-managed.
- If the device was IT-managed, used over-the-air technology to remotely disable features such as Wi-Fi connectivity and the camera.
- If the device was not IT-managed, alerted the floor supervisor to the presence and the location of the device. The supervisor could then apply standard business processes to enforce policies and deal with violations.

The system detected approximately 70 percent of unauthorized cellular devices (if they were turned on) at the entrance to the restricted area; beyond the entrance, the detection rate of unauthorized cell phones inside the factory—those that were not detected at the entrance—was 100 percent. Using sensors and triangulation, we could pinpoint the exact location of unauthorized devices on the factory floor.

Based on these results, we plan to fine-tune the system to increase the detection rate of unauthorized cellular devices at the factory entrance. We also anticipate incorporating a production version of the detection system at some of Intel's newer factories.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Intel employees use smart phones to increase productivity, flexibility, and mobility throughout the enterprise. In particular, corporate and personally owned smart phones enable anytime anywhere access to corporate data—such as e-mail, contacts, and calendar—and other select enterprise applications.

However, we do not permit employees to use smart phones or any sort of personally owned cell phones in Intel's wafer factories, for two critical reasons:

- Smart phone cameras pose significant risk to Intel's intellectual property, such as sensitive manufacturing process data.
- Certain fabrication processes and process equipment are sensitive to radio frequency (RF) interference. Intel employees inside the factory environment can use only Intel-approved phones that operate at low power levels.

We do allow employees in the factory environment to use simple, corporate-owned cell phones—without a camera, video capabilities, or Wi-Fi* access. Unfortunately, these devices do not offer our factory workers the same gains in productivity and job satisfaction that other Intel employees have achieved through smart phone use. We also find that it is becoming increasingly difficult to find this type of basic device, as suppliers consider the technology obsolete.

We want to allow corporate-owned smart phones in our factory environment to enable new advanced mobility capabilities and productivity gains. Therefore, we are investigating the best way to provide these benefits without negatively affecting the security of Intel's intellectual property or making changes to factory process.

Before we can enable smart phones in our factories, we need to be able to:

- Remotely disable device features, such as cameras or Wi-Fi* connectivity, using over-the-air (OTA) mobile device management (MDM) technology.
- Detect and alert management to the presence of unauthorized devices in the factory.

PROOF OF CONCEPT

We conducted a proof of concept (PoC) at one factory site, testing a context-aware security policy that detected and controlled corporate-owned smart phones in the factory environment.

The system under test performed four key functions:

- Detected that a device was about to enter the factory environment.
- Determined if the device was IT-managed.
- If the device was IT-managed, used OTA MDM to remotely disable features such as Wi-Fi connectivity and the camera.
- If the device was not IT-managed, alerted the floor supervisor to the presence of the device.

One of the advantages of this system was that it enabled us to disable certain smart phone features inside the factory, while still allowing employees to benefit from these same features when outside the factory environment, such as in the office, at home, or while traveling. We do not anticipate enabling personally owned smart phones within Intel factories at this time.

PoC Test Environment

During the PoC, we simulated an entrance to a restricted area. The physical layout of Intel's factories is particularly good for implementing a gateway concept because there is usually only one entrance into the cleanroom area. This is where we deployed our simulated system gateway.

As shown in Figure 1, the components of the detection system included:

- Badge reader system
- RF-shielded room at the entrance, also called an "attenuator corridor," that shielded cell phones from receiving RF signals
- Cellular signal detection sensors at the entrance and inside the factory
- MDM systems
- Information system to manage and integrate system components

Employees swiped their badges as usual to gain entrance to the manufacturing area. Using the badge information, we could determine if an employee had been issued an authorized corporate cell phone.

- If the employee had an Intel-authorized phone, and it was turned on, the MDM system disabled certain features, such as camera, Wi-Fi connectivity, and data storage.
- The combination of the attenuator corridor and the RF detection system enabled us to detect an unauthorized phone before it entered the restricted area when the phone was turned on.
- Because the RF detector at the entrance could not detect a phone that was turned off, we also located RF sensors inside the factory and tested them by turning smart phones on in the restricted area.
  - If an employee were to bring an unauthorized phone inside the factory and then turn it on, the sensors inside the factory would set off an alarm.
  - Using triangulation, the sensors could also locate the unauthorized device.

We posted clear signage at the simulated gateway that informed employees about the test, satisfying Human Resource guidelines.

Results

The system detected approximately 70 percent of those unauthorized cellular devices that were turned on at the entrance to the restricted area. We are working on an improved solution that we anticipate will significantly increase the detection rate, to about 95 percent.

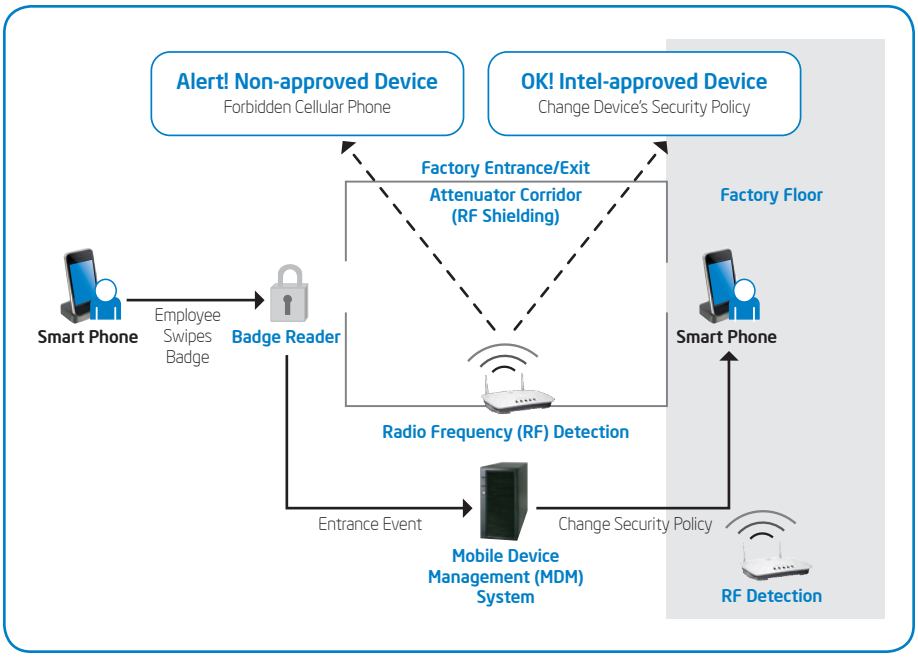

Figure 1. At the factory entrance, we need to be able to detect unauthorized cellular devices and control authorized devices. Inside the factory, we need to detect devices that are turned on.

Beyond the entrance, the detection rate of unauthorized cell phones inside the factory—those that were not detected at the entrance—was 100 percent.

NEXT STEPS

We plan to implement a production version of our smart phone detection and control system in Intel factories. We will prioritize factories that house new manufacturing processes that are most sensitive to intellectual property leakage.

As we fine-tune the system, we will continue to investigate the following areas:

- In the PoC we used a Faraday cage[1] to provide 100-percent RF shielding; this forced smart phones to lose their connections to the cellular network. Upon exiting the Faraday cage, the phones automatically tried to reconnect to the network and therefore transmitted RF signals, which we could then detect. With this method, the sensors only "listen" for cellular signals. We found that this method was not reliable enough—detection success at the Faraday cage exit was not 100 percent. In the next phase of the project, we will use an active cellular detection system at the entrance, which causes every device entering the area to transmit an RF signal. Using this method, we anticipate a higher detection rate.

  Using the active detection method, we will not need 100-percent RF shielding. We will still need to provide some RF shielding, but only to nullify the impact to phones outside of the entrance area and to optimize the effectiveness of the detection system.
- We will continue to investigate the number of sensors required for accurately detecting and locating unauthorized devices inside the factory. To increase accuracy, more sensors are required; however, this increases the cost of the system.
- Currently, we cannot tell the difference between an authorized and unauthorized phone if they both use the same frequency and/or channel. The new active detection system will address this by providing us with the International Mobile Equipment Identity (IMEI) or International Mobile Subscriber Identity (IMSI) number of the phone and comparing it to an authorized list.

CONCLUSION

Concerns about intellectual property leakage and RF interference with the manufacturing process have prevented us from allowing factory employees to use smart phones. This limitation has prevented these employees from taking advantage of smart phone productivity features, such as e-mail, contacts, and calendar information, when they are in the office, at home, or traveling.

We conducted a PoC that explored the feasibility of allowing factory employees to use corporate-owned smart phones while protecting Intel's intellectual property and processes. The PoC tested a system that detected cellular devices at the factory entrance, before they entered the factory floor, as well as cellular devices that were turned on within the factory environment. The system used OTA technology to temporarily disable features such as camera, video, and Wi-Fi connectivity on authorized smart phones.

We plan to continue fine-tuning our cellular device detection system and conducting more PoCs, with the intention of eventually incorporating the system into new Intel fabrication facilities. The advantage of such a system is that it would protect Intel's factory environment from intellectual property theft and manufacturing process disruption, while at the same time enabling factory employees to enjoy the benefits of increased productivity, flexibility, and job satisfaction offered by smart phones.

ACRONYMS

IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MDM	mobile device management
OTA	over the air
PoC	proof of concept
RF	radio frequency

For more information on Intel IT best practices, visit www.intel.com/it.

[1] A metallic enclosure that prevents the entry or escape of an electromagnetic field.

Printed in USA
0911/JLG/KC/PDF

Please Recycle
325587-001US