Wireless Tablet Security

Comprehensive security architecture for the
GTL Inspire® wireless tablet.

Multiple Levels of Security

Understanding the complexities and concerns of the corrections market is at the foundation of all products and services that GTL delivers to the market. Nowhere is that more prevalent than with GTL's wireless inmate tablet program, which was built from the ground up with multiple levels of integrated security to ensure the safety and security of corrections staff, inmates, and the general public.

Introduction

The corrections market has begun to take advantage of the popular handheld computer devices (commonly known as tablets) that have become so prevalent in business and education. While the consumer market has seen explosive growth in the adoption of these devices, their application and usefulness in the corrections market has been difficult to address. This is due mainly to security concerns. With this in mind, GTL not only created a tablet specifically for inmates, but also built an integrated framework of security elements that work together to exceed the expectations of correctional facilities.

GTL's "Multi-Layer Security Architecture" for Inspire includes five distinct elements:

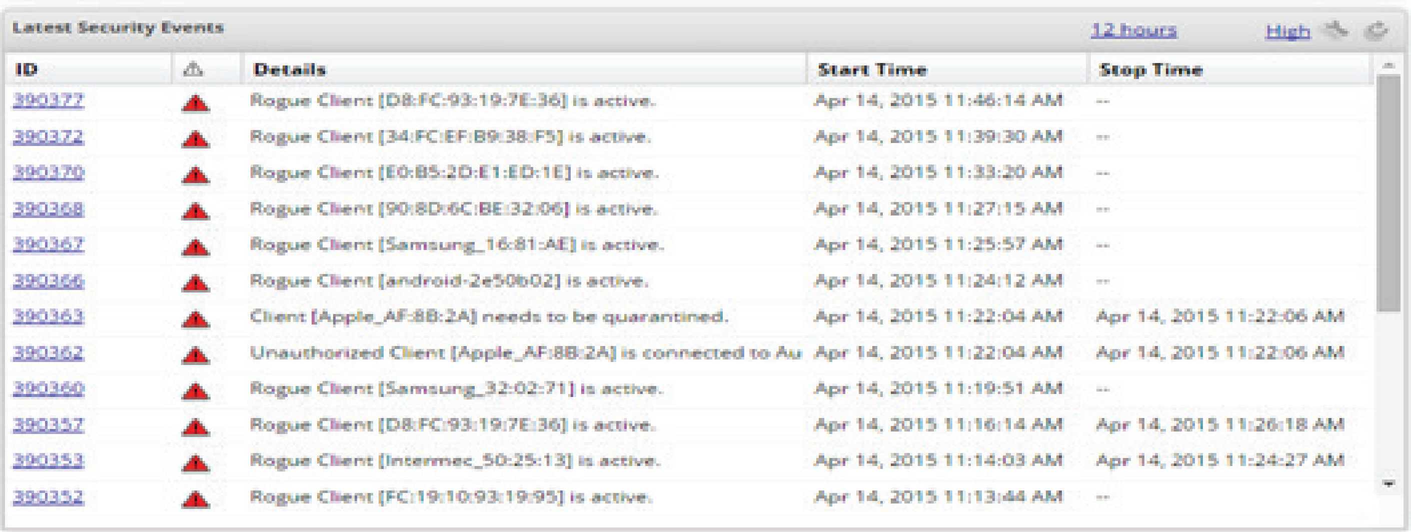
- **Network Security**
- **Wireless Security**
- **Operating System Security**
- **Hardware Security**
- **Application Security**

Pillar One: Network Security

Similar to military-grade networks, access to and from GTL's tablet network is highly controlled. Beginning with firewalls, all traffic in and out of the network is strictly controlled. A "deny all" approach is utilized, with the only exceptions being white-listed locations that are approved by GTL and corrections facility staff. In addition to access control lists (ACLs), GTL utilizes stateless inspection with attack-checking as a second measure of network security. Finally, all traffic originating from the Internet is automatically discarded.

Pillar Two: Wireless Security

While many correctional facilities are concerned about the introduction of a wireless network, wireless access point management software actually provides a second level of security. With our industry-leading wireless intrusion prevention system, the unique identifiers (MAC addresses) for all Inspire tablets are uploaded to the GTL wireless access management system. GTL is then able to perform real-time monitoring of the system and block unusual activity. Should unusual activity be detected, system administrators are notified immediately, and the suspected tablet's wireless access is immediately disabled. In addition, this system provides GTL and the facility with insights into all other wireless access points in the airspace.



Latest Security Events

ID	⚠	Details	Start Time	Stop Time
390377	▲	Rogue Client [D8:FC:93:19:7E:36] is active.	Apr 14, 2015 11:46:14 AM	--
390372	▲	Rogue Client [34:FC:EF:B9:38:F5] is active.	Apr 14, 2015 11:39:30 AM	--
390370	▲	Rogue Client [E0:B5:2D:E1:ED:1E] is active.	Apr 14, 2015 11:33:20 AM	--
390368	▲	Rogue Client [90:8D:6C:BE:32:06] is active.	Apr 14, 2015 11:27:15 AM	--
390367	▲	Rogue Client [Samsung_16:81:AE] is active.	Apr 14, 2015 11:25:57 AM	--
390366	▲	Rogue Client [android-2e50b02] is active.	Apr 14, 2015 11:24:12 AM	--
390363	▲	Client [Apple_AF:8B:2A] needs to be quarantined.	Apr 14, 2015 11:22:04 AM	Apr 14, 2015 11:22:06 AM
390362	▲	Unauthorized Client [Apple_AF:8B:2A] is connected to Au	Apr 14, 2015 11:22:04 AM	Apr 14, 2015 11:22:06 AM
390360	▲	Rogue Client [Samsung_32:02:71] is active.	Apr 14, 2015 11:19:51 AM	--
390357	▲	Rogue Client [D8:FC:93:19:7E:36] is active.	Apr 14, 2015 11:16:14 AM	Apr 14, 2015 11:26:18 AM
390353	▲	Rogue Client [Intermec_50:25:13] is active.	Apr 14, 2015 11:14:03 AM	Apr 14, 2015 11:24:27 AM
390352	▲	Rogue Client [FC:19:10:93:19:95] is active.	Apr 14, 2015 11:13:44 AM	--

Figure 1 – Example of Wireless Intrusion Detection

Pillar Three: Hardware Security

GTL's Inspire tablet is not an off-the-shelf device; rather, it is custom built to meet the rigorous demands of the corrections market. The tablet's internal components are housed in a hardened case with a transparent (not merely translucent) housing that is secured with eleven proprietary security screws.

Getting power to the device without compromising security was also a consideration when creating Inspire. Most commercially available tablets are charged via micro USB using a type of charger that if placed in a corrections setting could also be used to charge unauthorized devices such as cell phones and Bluetooth gear. What's more, a micro USB port on a tablet becomes a hacking risk. To avoid all of these problems, the Inspire tablets are charged using a basic barrel-style charger to reduce the likelihood of illicit activity.

Additionally, the Inspire tablet does not include an external speaker. Inmates must use headphones when listening to audio content or making phone calls from Inspire for purposes of privacy and to keep the inmate environment as quiet as possible.

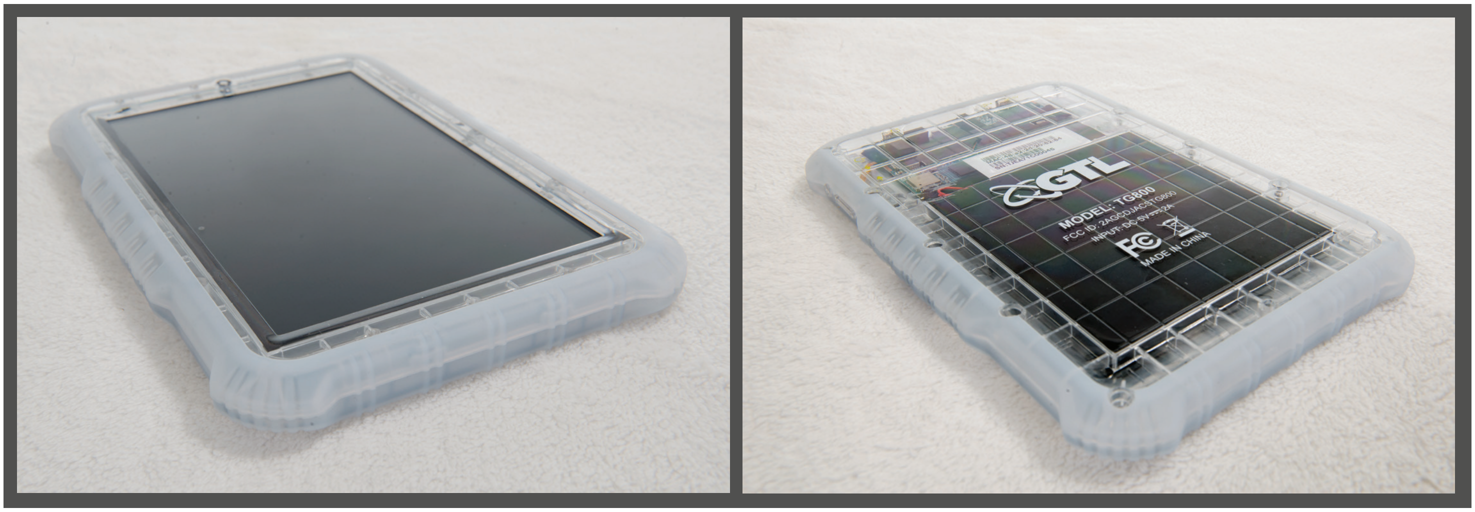


Figure 2 – GTL Inspire Wireless Tablet

Pillar Four: GTL's Customized Android Operating System

Many consumer-grade tablet operating systems present a myriad of issues and security risks that would not meet the high standards of the corrections market. To overcome those issues, GTL created a customized version of the Android operating system, and in doing so removed (not just disabled) all features deemed inappropriate for a corrections environment.

The following operating system features have been eliminated for security purposes:

- **Factory reset**
- **Safe boot**
- **All bloatware**
- **Bluetooth**
- **Copy and paste functionality**
- **Stock Android keyboard**
- **Wireless tethering**
- **Settings for elements removed from the user interface**

In addition, GTL's custom Android operating system is fully integrated with an industry leading secure mobility management platform, allowing device operating systems and applications to be updated over the air securely, efficiently, and silently. This mobility management software is built into the operating system to prevent any inmates from altering or removing this software.

Pillar Five: Application Security

The final piece of GTL's Security Architecture concerns what inmates interact with on a daily basis: the applications. Similar to the custom operating system, GTL has created purpose-built secure applications for the inmates. All applications are developed from the ground up to ensure the following:

- **External linkages have been eliminated.**
- **Unapproved content cannot be loaded.**
- **"Back door" access to tablet settings has been removed.**

Applications are tested both individually and holistically to ensure that they adhere to the strict parameters of the GTL wireless tablet program. Moreover, GTL has developed a secure Android launcher that acts as an additional protective measure to ensure that inmates do not have access to the tablet settings that would otherwise lead to unauthorized applications.

Conclusion

The introduction of new technologies to the corrections market such as tablets must be done through a thoughtful, iterative, and holistic product design. What's more, security must be the foundation of every component of the program. GTL's level of industry knowledge, expertise, and pragmatic approach to the development of the Inspire wireless tablet program means that correctional facilities can rest assured that inmates utilizing the tablets are doing so within the strict parameters of GTL's secure network architecture and correctional facility requirements.