IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5220

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour. 

# Applying the Target and Shield Model to Wireless Technologies

Laura Lally

BCIS/QM Dept, Hofstra University, Hempstead, NY 11549-134, acslhl@hofstra.edu

James J. Nolan

Systems Eng., InterDigital Communications Corp, 2 Huntington Quad., 4th Floor, S. Wing, Melville, NY 11747, james.nolan@interdigital.com

## ABSTRACT

This paper presents Lally's Target and Shield model and its implications for Wireless Technologies. The Target and Shield model, which is grounded in Normal Accident Theory and the Theory of High Reliability Organizations provides a framework for examining how IT can be used both as a target of malicious attacks as well as how IT can be used as a shield against such attacks or to mitigate their impact should they occur. Wireless technologies, their vulnerabilities to attack, and their use in preventing further attacks are examined. Suggestions for designing more secure and resilient systems in the future conclude the paper.

## IT SECURITY CHALLENGES

Information Technology **(IT)** Security has become an issue of growing importance.

Increased reliance on computer based systems adds to the vulnerability and to the potential for widespread effects. DETER and EMIST (2002) argue:

*As the Internet has become pervasive and our critical infrastructures have become inextricably tied to information systems, the risk for economic, social and physical disruption due to the insecurities of information systems has increased immeasurably.*

Furthermore, IT based systems may also be used as a weapon in attacks against other key infrastructure systems such as electric power and water (National Research Council, 2002). Designing secure, resilient systems in the face of these new threats will be a major challenge.

However, this paper will argue that, IT based systems can also be used to mitigate the impacts of the damage of both terror attacks and non-malicious accidents with proper design, implementation and training. This analysis will argue, therefore, that IT based systems are not only a **target**, a source of vulnerability, but that they can also be a **shield**, a means of combating the threats and mitigating the damage malicious individuals are able to accomplish.

This research will present Lally's (2005) **"Target and Shield"** conceptual model of the sources, propagation and potential impacts of IT related threats, as well as the means by which IT can be used to identify, eliminate and mitigate the damages caused by other sources of threats. This paper will focus on the challenges of implementing this model in the context of terrorist attacks in large urban areas. The conceptual model draws on two theoretical perspectives, an extended version of Perrow's Normal Accident Theory, and the Theory of High Reliability Organizations.

## THEORETCAL FOUNDATIONS

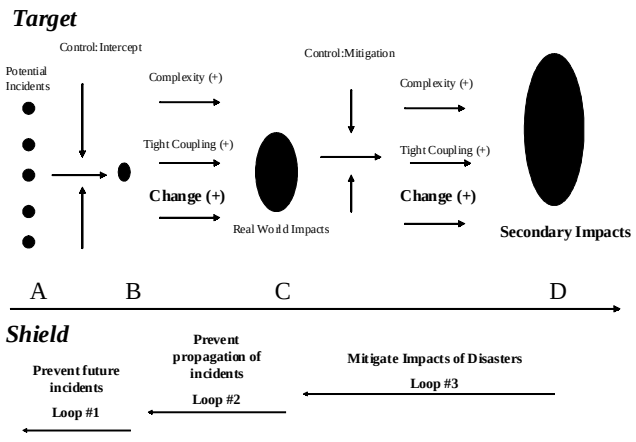
Normal Accident Theory (Perrow, 1984) argues that characteristics of a system's design make it more or less prone to accidents. The first key characteristic of accident prone systems is their complexity. Normal Accident Theory argues that as systems become more complex, they become more accident prone. Normal Accident Theory distinguishes a second characteristic of systems that exacerbate potential problems brought about as a result of complexity — tight coupling. Tight coupling means there is no slack time or buffering of resources between tasks, interactions happen immediately. Both complexity and tight coupling are often more efficient from a productivity standpoint. However, incidents tend to propagate faster and their impact becomes more severe because there is no lag time during which human intervention can occur.

Researchers in High Reliability Organizations have examined organizations in which complex, tightly coupled, technologically based systems appeared to be coping successfully with the potential for disaster. They emphasize the importance of good communication, shared mental models of systems, shared value of the importance of safety, continual organizational learning, and redundancy of key systems (Grabowski and Roberts, 1997), (Klein, Bigley, and Roberts, 1995), (LaPorte and Consolini, 1991), (Sagan, 1993), (Turner, 1976), and (Weick, 1993).

Lally (1996) argued that Normal Accident Theory was a sound theoretical perspective for understanding the risks of Information Technology, because IT is complex, and tightly coupled and often poorly controlled. She also argued (Lally, 1996), (Lally, 1997) that IT based systems do not operate in isolation but in organizational settings where failures in IT can lead to more widespread secondary failures in organizations. Additionally, she argued (Lally, 2002) that the frequent rapid change in both IT based systems and the work processes they support can further exacerbate the potential for disaster. Lally (2005) further extended her model and argued that IT based systems are not only a **target** used as a weapon of destruction to cause serious accidents, but that IT based systems can be a **shield** used to prevent damage from future incidents, whether they be IT based or physical. This **"Target and Shield"** conceptual model drew on insights from the Theory of High Reliability Organizations and suggests that IT designers and managers, as well as government and law enforcement agencies learn from past experiences and embody this knowledge in the design and implementation of future IT based systems. The resulting systems should not only be more secure and resilient, they should aid in preventing future IT based or physical attacks, or mitigating their impact should they occur. Figure 1 illustrates the **Target and Shield** conceptual model for analyzing the source, propagation and impacts of IT based threats, as well as ways in which IT can be used to identify, and mitigate the impact of, future threats.

The Target and Shield model incorporates Lally's extensions to Normal Accident Theory. The model also contains *three significant feedback loops*, which allow IT to play a positive role in preventing future incidents from materializing, having real world impacts, and mitigating their impacts when they do occur. In the Feedback Loop #1, **Prevent future incidents**, controls can be built into the system to prevent future incidents from materializing.

*Figure 1. Target and Shield Model*




In Feedback Loop #2, **Prevent Propagation of Incidents**, controls can be built into the system to prevent future incidents that have materialized from turning into accidents.

In the Feedback Loop #3, **Mitigate Impact of Disasters**, IT based systems can be developed to prevent accidents resulting from IT based or physical attacks from propagating even further.

## APPLYING THE MODEL TO WIRELESS TECHNOLOGIES

Wireless technologies and the information they transmit and receive can be targets of malicious attackers (hackers, cyber-terrorists) in a similar manner as wired voice and data traffic. Wireless voice and data network traffic are evolving from circuit switched traffic to packet switched (IP based) traffic. Once wireless voice and data is transported over the Internet it is just as vulnerable as packet switched data from any other wired Internet data traffic source (via Dial-up, T1, DSL, and Cable Modem). The one significant difference is that wireless transmissions can be sniffed (acquired, decoded and recorded and reused to spoof or attack transmitters) over the air, making the data vulnerable to anyone with equipment that can receive and decode those signals.

The authors have extended the Target and Shield Model to wireless technologies (Cellular and unlicensed Wireless) in Figure 2. Text bolded and highlighted signifies future enhancements that could be added to future versions of wireless standards or be added as proprietary extensions to current implementations of wireless standards by original equipment manufacturers (OEMs). Plain text signifies current systems features created to limit theft of service or to mitigate the impacts of external factors that cause unstable system operation. The list of targets or shields (recovery loops) is by no means exhaustive; it is a representative list that differentiates the varying levels of protection in the different technologies. A trend that can be seen in the table is that security (encryption, authentication and authorization) increases as the range (physical area covered) that the technology supports or to the degree that the network is public network.

The authors also present Figure 3 as well for notional view of level of security by technology and generation of a technology.

At the Air Interface level (transmission over the air) wireless networks could be disabled by denial of service (DNS) attacks by coordinated malicious attacks. This technique would spawn multiple access (requests for service by multiple users) attempts by attackers to exhaust all available resources (access channels or entire channel bandwidth). Other denials of service methods include jamming (broadcast of a broadband noise signal) which limits the ability of a wireless receiver to discern a wanted signal from background noise. Although these denial of service attack methods and/or other attacks on system fail-safes features that have been built into wireless networks to prevent catastrophic failures are different in nature, their potential impacts are similar. These types of attacks would in a worst case scenario result in disabling one basestation or one cell but would not disrupt (take-down) an entire network.

*Figure 2. Lally's Target and Shield Applied to Wireless Technologies*

| **Target** | | | **Shield** | | |
|---|---|---|---|---|---|
| **Technology** | **Impact** | **Method** | **Feedback Loop #1** | **Feedback Loop #2** | **Feedback Loop #3** |
| **WWAN** | Block Access to Network | Co-ordinated Simulateous Access Attempts | *Networks Disable Malicious Terminals from Making Access Attempts* | Admission Control of Users (to xx% of capacity, block additional call attempts | Network limits signaling and response to rogue users. |
| | | Jam Basestation with High Power Jammer | | Some radio networks limit new users after noise level goes too high | Network disable Basestation, report alarm to central office an 911 |
| | Block terminal Reception | Jam Terminals (Broadband noise Jammer) | | Terminals report noise to network when connected | Network isolate area based location information and notify 911 |
| | Eavesdropping -conversations -transactions | Sniffer sniff for transmissions | VPN using IPSec of SSL for secure data transmission. | Encryption | |
| | Spoofing | Retransmit tapped signals | | Authentication, Authorization | |
| | Suspected terrorist use of cell phone | | | Tracking of known numbers disable/decode (or provide keys) encryption | Legislation (USA patriot Act allows wireless eavesdropping ov gov't security agencies) |
| **WLAN** | Block Access to Network | Co-ordinated Simulateous Access Attempts | Add protection (Admission Control, Block new attempts), currently access attempts not limited. Efficiency/throughput drops with excessive attempts. | | System degrades gracefully, looses node, traffic to/from Internet not impacted |
| | | Jam Basestation with High Power Jammer | | BS measure Noise background and back-of data rate. | |
| | Block STA (terminal reception) | Jam terminals (Broadband Noise Jammer) | | Terminals Measure Noise background and back-off data rate. | |
| | Eavesdropping -conversations -transactions | Sniffer sniff for transmissions | VPN using IPSec or SSL for secure data transaction Upgrade security 802.11 | Encytion (WEP) | |
| **WPAN (BT, UWB, Zigbee** | | Steal user data | For Bluetooth, turn discovery off, enable bonding and pairing require PIN for both devices. | | |

Other attacks could target user's data directly by snooping, decoding and using over the air signaling or data for theft of service or redirection of IP traffic for malicious purposes. Encryption protects against unwarranted decoding of data, while authentication and authorization are network processes that prevent unauthorized access to the telecommunications network and to the PDN (Public Data Network — the Internet). Cellular systems traditionally have much stronger security systems, with more robust encryption and authentication (AAA) to verify users then other wireless systems designed for operation in unlicensed spectrum (WPAN, WLAN).

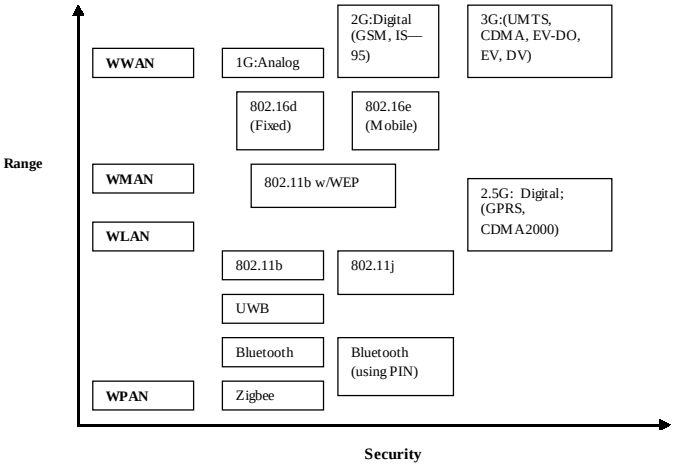
## WIRELESS AS A TARGET

Vulnerability of wireless technologies is directly tied to several factors, including;

- Range/distance or area covered by technology. Typically the larger the cell size the greater the safeguards and recovery mechanisms (required by Standards or by regulation).
- Whether networks are public or private. Public networks with purchased spectrum and customers who pay for access and calls expect a greater level of security, quality of service (QoS), and integrity.
- Complexity of Radio Access Network. Cellular wireless networks are historically hierarchal and include significant control of resources and access (guaranteeing higher spectrum utilization, to 80-90%) while unlicensed technologies have simpler resource allocation schemes and accept much lower utilization (30-50% typical), e.g. Reservation based vs. CSMA (Collision Sense Multiple Access) schemes of Medium Access.

The relative security of each wireless technology and their evolution through generations of standards is presented by the authors graphically in Figure 3.

*Figure 3. Relative Security of Wireless Technologies - Notional (Encrption and Authentication)*




Cellular technologies have increased their standards have evolved. Security (encryption and authentication) has increased in scope and complexity as we have moved from analog systems to digital systems. WiFi has also experienced significant security issues in its first generation as well. It is estimated that 70-80% of all WiFi Access Points (APs) have no encryption enabled and those that are enabled typically use WEP (Wired Equivalency Protocol), which has been demonstrated by security experts and hackers as being insecure and easily broken. A proposed software upgrade to WiFi standards, 802.11i, will provide enhanced security while other upgrades (802.11e, 802.11k) will enable quality of service, resource management and user measurement improvements. These steps enhance WLAN capabilities and their ability particularly in Enterprise and Hotspot deployments to deny rogue users and malicious attackers'unauthorized access.

WiMax (802.16d, e) standards are intended to operate as Wireless Metropolitan Area Networks (WMAN) for fixed or mobile data services in unlicensed spectrum. As a wide coverage area technology it has incorporated more robust security than WLAN. While WPANs, Wireless Personal Area Networks (802.15 family of standards; Bluetooth, Ultra Wideband, Zigbee) are meant for short range use in the home or office and have more limited security features. Note Bluetooth's (NT) ability to actively discover ("Discovery") other BT enabled terminals in its proximity makes it ripe for capture and hacking. Its standards do define a more secure mode of operation where devices are paired and then bond using a PIN for authentication at both devices to allow operation between the two[1]. This may be acceptable for small office home office (SOHO) or home use but will limit distinct features and capabilities of Bluetooth in more public settings.

## WIRELESS AS A SHIELD

The technologies that can provide the greatest protection against malicious attack (cyberterrorism) include:

- Distributed Networks or Mesh Networks; provide redundant paths between basestation and IP backbone connections limiting catastrophic loss to entire service areas. For example, a 9/11 type attack where a Central Office or major cell sites being disabled impacted service beyond the immediate area.
- Peer to Peer Virtual Private Networks – VPN using IPSec or SSL provide end to end secure transmission
- Emergence of Multimode Multiband Terminals that can switch to other technologies if a basestation is disabled. For example, Nextel iDen & CDMA2000, GSM/GPRS and FDD.
- Enhanced encryption and authentication algorithms and implementations.

## DESIGNING MORE ROBUST SYSTEMS IN THE FUTURE

The gradual evolution in cellular networks away from hierarchal network architecture typical of switched wireless telecommunications networks to router based IP architectures will enable more distributed ad-hoc architectures such as mesh networks. This will provide greater redundancy of paths to/from the Internet. Other levels of systems redundancy include support of multiple air interface standards within terminals (e.g. GSM/UMTS/WLAN, CDMA2000/UMTS/WLAN). Robustness against loss of cells can be solved by move to smaller (Micro/Pico) Basestations with smaller range. This trend has been underway over the last few years, cellular operators are providing greater voice/data coverage to very dense urban environments with smaller cells targeted to concentrations of users. The unintended positive impact from a robustness perspective is that this has provided greater redundancy via hierarchal cell structures, where macro, micro, and pico cells are overlaid in the same geographic area in adjacent frequency channels. These multiple overlapping cell layouts at adjacent channels frequencies within allocated bands also provide a level of redundancy in the frequency domain. The evolution of wireless (WLAN) is toward the addition of cellular like features for security, robustness, quality of service, while maintaining a smaller less complex infrastructure.

Other improvements to cellular systems for homeland security, law enforcement or first responders could leverage location aware devices (GPS or GPS assisted devices) that periodically report location of any terminal once turned on. This would enable tracking of first responders in dangerous rescue attempts. Location aware devices and location awareness (of users) of networks could be used for tracking suspected cyber-attackers (assuming warrants are used based on legal guidelines) include reporting of location.

Other advancements that offer more robust systems are software defined radio (SDR) platforms that are digital signal processing (DSP) based soft implementations of wireless standards. Changes, security upgrades, patches to a handset/terminal will be by software down load.

## CONCLUSION

The above analysis indicates that Wireless Technologies map readily onto the Target and Shield model. Emerging wireless initiatives must address current vulnerabilities to attacks and develop more robust solutions to counter attacks in the future. Case studies of these applications will strengthen the research model.

## ACKNOWLEDGEMENTS

The authors would like to thank the wonderful students in the InterDigital EMBA course: Pascal M. Adjakple, Peter E. Becker, Richard J. Brezski, Ana Iacono, Michael E. Jeronis, Scott H. Kalish, Michael T. McEntee, Narayan Menon, Stephen Noskewicz, Robert L. Olesen, Linda G. Ontiveros, Renuka Racha, Daniel Steinback, and Rui Yang for all their insights into Wireless Technologies.

This research has been funded in part by a Summer Research Grant from the Frank G. Zarb School of Business at Hofstra University.

## REFERENCES

DETER and EMIST Projects. (2004). Cyber Defense Technology Networking and Evaluation. Communications of the ACM, March, 58-61.

Grabowski, M. and Roberts, K. (1997). Risk mitigation in large scale systems: Lessons from high reliability organizations. *California Management Review,* Summer, 152-162.

Klein, R.L., Bigley, G.A., Roberts, K.H. (1995). Organizational culture in High Reliability Organizations. *Human Relations*, 48:7. 771-792.

Lally, L. (1996). Enumerating the risks of reengineered processes. *Proceedings of 1996 ACM Computer Science Conference,* 18-23.

Lally, L. (1997). Are reengineered organizations disaster prone?" *Proceedings of the National Decision Sciences Conference*, 178-182.

Lally, L. (2002). Complexity, coupling, control and change: An IT based extension to Normal Accident Theory. *Proceedings of the International Information Resources Management Conference*, 1089-1095.

Lally, L. (2005) Information Technology as a Target and Shield in the Post 9/11 Environment. *Information Resources Management Journal,* Jan-Mar, Volume 18, No. 1.

LaPorte, T. R. & Consolini. P. (1991). Working in practice but not in theory: Theoretical challenges of High Reliability Organizations. *Journal of Public Administration,* 1, 19-47.

National Research Council. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Washington, D.C.: National Academies Press.

Perrow, Charles. (1984) *Normal Accidents: Living with High Risk Technologies.* New York: Basic Books.

Sagan, Scott. (1993). *The Limits of Safety*. Princeton New Jersey: Princeton University Press.

Turner, B.M. (1976). The organizational and interorganizational development of disasters. *Administrative Science Quarterly*, 21, 378-397.

Weick, K.E.and Roberts, K. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, 38, 357-381.