


This presentation examines the issues surrounding security for remote communications using cellular networks.



Common myths and misconceptions are exposed and key security technologies are highlighted along with best practices for creating a secure remote links using public cellular wireless networks.



About Proxicast

A privately-held US-based manufacturer of the LAN-Cell 3G Mobile Gateway which integrates a cellular modem, Ethernet switch, advanced NAT router, VPN and firewall features into a single device.

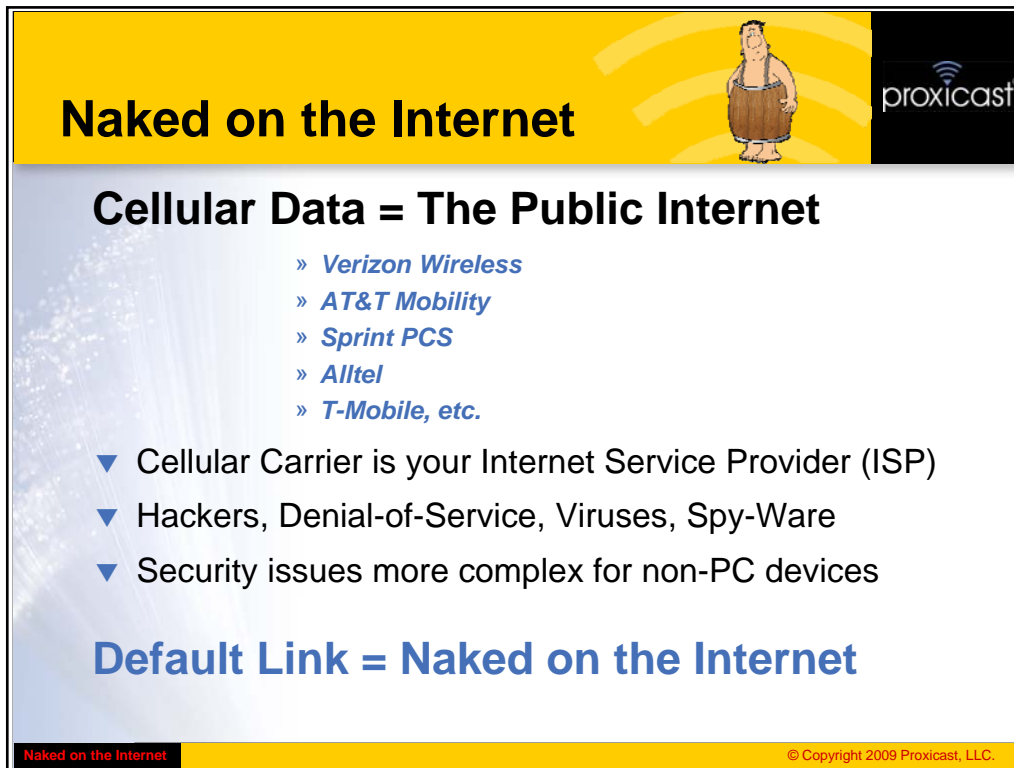
The LAN-Cell is the industry's most secure communications solution for industrial & commercial remote access using cellular data networks.



Naked on the Internet © Copyright 2009 Proxicast, LLC.

Proxicast manufactures rugged secure communications equipment for use on all cellular networks worldwide.

Our LAN-Cell family of gateways including the LAN-Cell 2 Wireless 3G cellular router and the Cell-PAK portable battery-powered 3G + Wi-Fi HotSpot are the most secure “all-in-one” solution for connecting remote sites to cellular data networks.



Naked on the Internet

Cellular Data = The Public Internet

- » *Verizon Wireless*
- » *AT&T Mobility*
- » *Sprint PCS*
- » *Alltel*
- » *T-Mobile, etc.*

- ▼ Cellular Carrier is your Internet Service Provider (ISP)
- ▼ Hackers, Denial-of-Service, Viruses, Spy-Ware
- ▼ Security issues more complex for non-PC devices

Default Link = Naked on the Internet

Naked on the Internet © Copyright 2009 Proxicast, LLC.

Many people are not aware that the cellular data services offered by all of the major wireless network operators provide a direct link to the public Internet. The cellular company is effect your ISP.

This means that cellular data networks are subject to all of the same threats that are present on the traditional “wired” Internet like hackers, denial-of-service attacks, spy-ware, etc.

Furthermore, cellular data networks are often used to provide connectivity to non-PC equipment like data loggers, cameras, PLCs, and sensors. Protecting this type of equipment is inherently more difficult due to its “closed” and often proprietary nature.

The bottom line is that if you deploy a cellular data connection without implementing any additional security solutions, you have an unprotected connection and your equipment is Naked on the Internet.

Where's the Risk?

90% of data breaches involve systems:

- ▼ *Unknown to the I/T security group*
- ▼ *Storing or transmitting data unknown to the organization*
- ▼ *Having undocumented network connectivity*
- ▼ *Having unauthorized system privileges*

Attack Pathway	Percentage
Remote Access & Control	33%
Web-Based Systems	26%
Internet Connected Systems	18%
Physical Access	16%
Wi-Fi Network	7%

Source: Verizon Business Risk Team – 2008 Data Breach Investigations Report (500 incidents)

Naked on the Internet © Copyright 2009 Proxicast, LLC.

A recent study by Verizon reveals that attackers are successfully penetrating systems that are not well protected by I/T security policies and technologies. In many cases, these “rogue” systems are installed by individual business units to meet operational requirements, but they are not properly secured to prevent unauthorized access.

Over two-thirds of the attacks studied involve remote access, web and other Internet-connected systems, highlighting the “invisible” threat from being Naked on the Internet.

Key Terms

- ▼ Public IP vs. Private IP addresses
- ▼ Cellular Modem
- ▼ Router
- ▼ NAT – network address translation
- ▼ VPN – virtual private network
- ▼ Firewall
- ▼ Gateway

The diagram illustrates the network architecture for securing remote cellular data communications. It shows a Private Network connected to Remote Equipment (laptop and server). This network is linked to a Gateway, which contains a Firewall, VPN, NAT Router, and Cellular Modem. The Gateway is connected to a Cell Tower, which in turn connects to the Public Internet.

Naked on the Internet © Copyright 2009 Proxicast, LLC.

In order to understand cellular security issues, it is necessary to be familiar with some common networking concepts:

Public IP address can be sent over the Internet; Private IP addresses can't.

A modem converts between the cellular radio signals and a usable data stream.

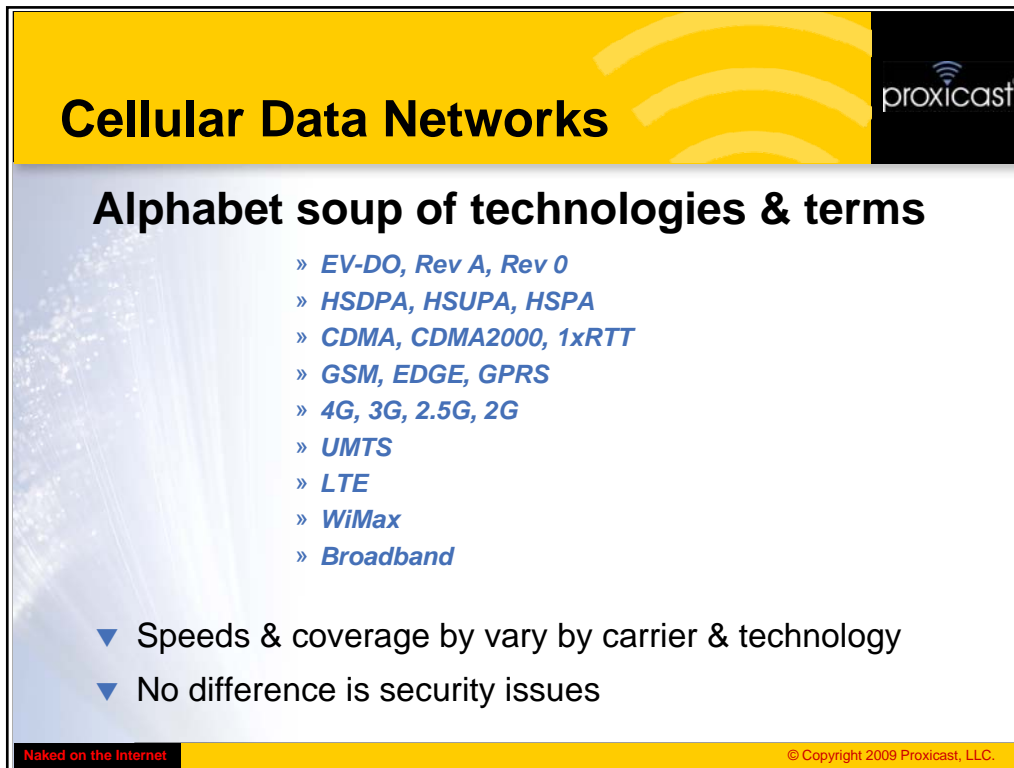
A router is used to allow 2 different networks to communicate.

Network Address Translation is a technique for mapping Private IP addresses to Public IP addresses.

A Virtual Private Network is a technique for creating a secure link between 2 private networks over a public network. It provides a very high level of communications security.

A firewall is software which controls what data may pass through it based on a series of user-defined rules. It is used to prevent unwanted traffic from reaching private networks.

A Gateway is a device which incorporates the functions of a Firewall, VPN, NAT/Router and Modem into a single device.



Cellular Data Networks

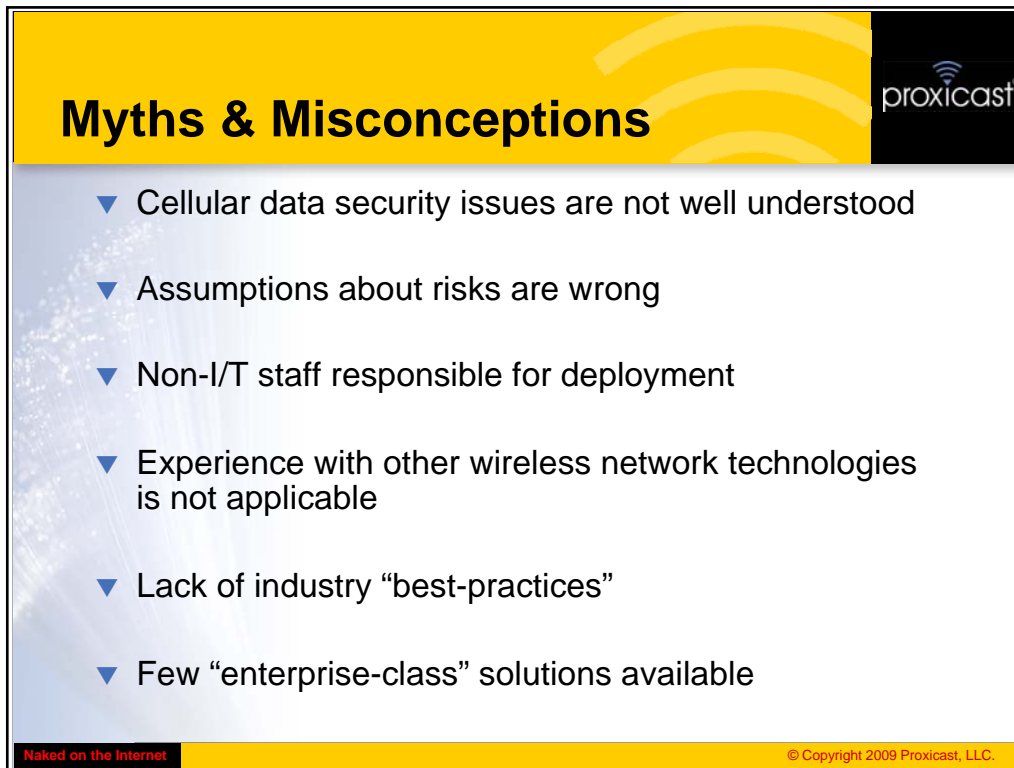
Alphabet soup of technologies & terms

- » *EV-DO, Rev A, Rev 0*
- » *HSDPA, HSUPA, HSPA*
- » *CDMA, CDMA2000, 1xRTT*
- » *GSM, EDGE, GPRS*
- » *4G, 3G, 2.5G, 2G*
- » *UMTS*
- » *LTE*
- » *WiMax*
- » *Broadband*

- ▼ Speeds & coverage vary by carrier & technology
- ▼ No difference in security issues

Naked on the Internet © Copyright 2009 Proxicast, LLC.

Cellular data networks encompass many different technologies. The specific services and speeds available vary by carrier and location. But when it comes to securing access to remote equipment, all cellular data networks present the same challenges.



Myths & Misconceptions

- ▼ Cellular data security issues are not well understood
- ▼ Assumptions about risks are wrong
- ▼ Non-I/T staff responsible for deployment
- ▼ Experience with other wireless network technologies is not applicable
- ▼ Lack of industry “best-practices”
- ▼ Few “enterprise-class” solutions available

Naked on the Internet © Copyright 2009 Proxicast, LLC.

We have found that often the reason why adequate security measures are not put in place for cellular data connections is that user’s are operating under inaccurate myths or misconceptions about the issues. We will explore some of the more common ones in a moment.

Often, remote equipment is under the purview of non-I/T staff who may not be familiar with state-of-the-art security technologies or the risks of accessing the public Internet.

Users may have had experience installing other wireless technologies such as WiFi, UHF, or 900 MHz point-to-point links and be unaware of the differences in security requirements for cellular links.


Because use of the cellular networks for “mission-critical” data transmission is relatively new, there is not a widely accepted set of security “best practices”.

Also, only a few vendors are providing true enterprise-class security solutions for cellular networks.

Myth:

No one else cares about my data

- ▼ Probably true
- ▼ Hackers aren't always looking for your data – They want to control your devices
 - » Zombie servers – spam
 - » Back-door to corporate network
 - » Data loss / corruption
 - » Increased telecom costs
- ▼ Connection might carry interesting data in the future
- ▼ Competitors might care about your data (e.g. Oil/Gas well output)



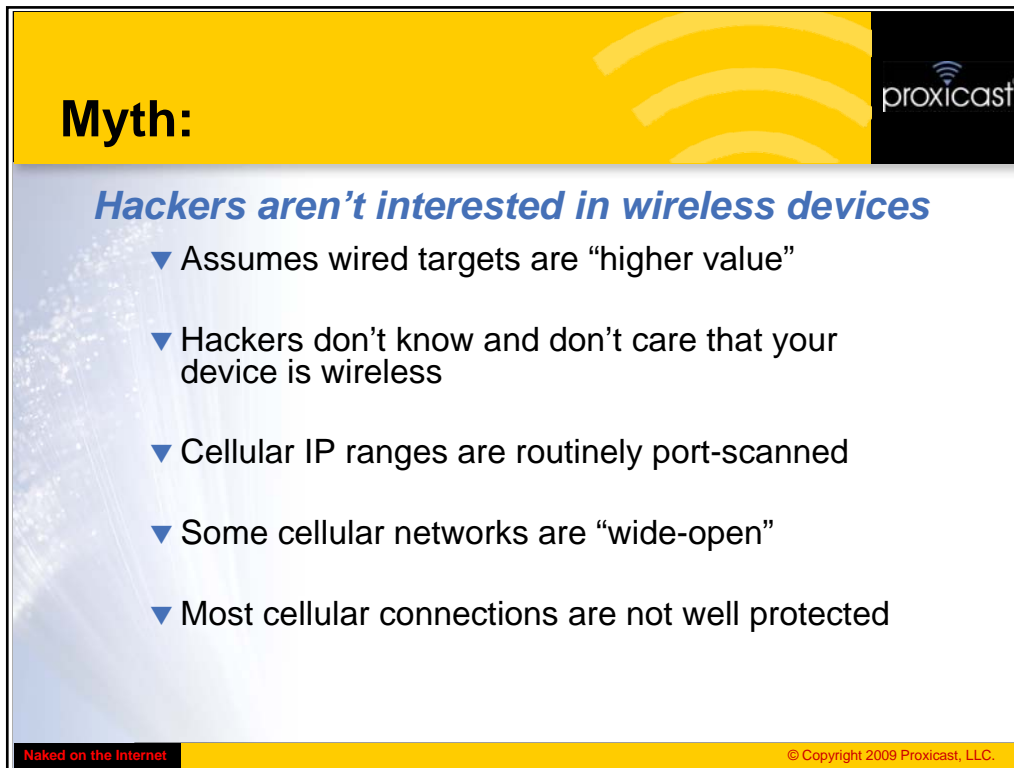
Naked on the Internet © Copyright 2009 Proxicast, LLC.

One of the most common statements we hear from customers is “no one cares about my data” or “I don’t care if anyone sees this data”.

It’s probably true that your data stream itself may not be interesting to hackers. But hackers are much more interested in controlling your devices for their own purposes. Creating Spam-bots and back doors into your corporate network are often their true objectives. And even if hackers don’t want your data, their actions may result in loss or corruption of your data and will likely increase your telecom costs.

Just because your current data isn’t interesting doesn’t mean that the cellular link won’t be used for something else in the future.

Maybe your data is more interesting than you think, especially if hackers can compile it from multiple remote sites.



Myth:

Hackers aren't interested in wireless devices

- ▼ Assumes wired targets are “higher value”
- ▼ Hackers don't know and don't care that your device is wireless
- ▼ Cellular IP ranges are routinely port-scanned
- ▼ Some cellular networks are “wide-open”
- ▼ Most cellular connections are not well protected

Naked on the Internet © Copyright 2009 Proxicast, LLC.

There is a perception that hackers are focused on “high value wired targets” like bank financial systems, credit cards, and military sites. This is a tiny minority of hacking activity.

Most hacking involves indiscriminate “port-scanning” to find vulnerable sites. Hackers don't know and don't care what's on the other end, as long as they can compromise it. Since cellular data networks link your equipment to the public Internet, hackers will port-scan your devices as well.

Some carriers attempt to minimize hacking activity via firewalls on their networks – others are “wide-open” and put all of the security burden on you.

As we've mentioned, most cellular data connections are not well protected. Hackers know this and may even be targeting cellular links as since they are potentially more vulnerable.

Hack Attempts on Cellular Net

#	Time	Message	Source	Destination	Note
1	2008-09-28 01:51:41	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8081	ACCESS DROPPED
2	2008-09-28 01:51:39	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8118	ACCESS DROPPED
3	2008-09-28 01:51:36	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:6588	ACCESS DROPPED
4	2008-09-28 01:51:34	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:7788	ACCESS DROPPED
5	2008-09-28 01:51:34	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8800	ACCESS DROPPED
6	2008-09-28 01:51:25	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8000	ACCESS DROPPED
7	2008-09-28 01:51:20	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8080	ACCESS DROPPED
8	2008-09-28 01:51:18	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8088	ACCESS DROPPED
9	2008-09-28 00:45:16	Firewall default policy: TCP (CE to CE/LC)	80.93.212.194:1119	166.139.37.167:27001	ACCESS DROPPED
10	2008-09-26 23:52:13	Firewall session time out, sent TCP RST	192.168.1.33:4259	64.233.161.147:80	TCP RST
11	2008-09-26 23:52:13	Firewall session time out, sent TCP RST	64.233.161.147:80	192.168.1.33:4259	TCP RST
12	2008-09-26 21:35:44	Firewall default policy: TCP (CE to CE/LC)	116.252.185.77:6000	166.139.37.167:1433	ACCESS DROPPED
13	2008-09-26 19:22:46	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8081	ACCESS DROPPED
14	2008-09-26 19:22:46	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8118	ACCESS DROPPED
15	2008-09-26 19:22:32	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:1080	ACCESS DROPPED
16	2008-09-26 19:22:30	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8000	ACCESS DROPPED
17	2008-09-26 19:22:20	Firewall default policy: TCP (CE to CE/LC)	60.172.222.17:12200	166.139.37.167:8088	ACCESS DROPPED
18	2008-09-26 18:15:52	Firewall default policy: TCP (CE to CE/LC)	118.165.87.26:2141	166.139.37.167:25	ACCESS DROPPED
19	2008-09-26 14:20:23	Cellular connection is up.			Cellular

Port Scans (rows 1-9)

Login Attempt (rows 10-11)

Port Scans (rows 12-17)

E-Mail Relay Attempt (row 18)


Naked on the Internet
© Copyright 2009 Proxicast, LLC.

Here's section of a security log from a LAN-Cell showing several different types of hack attempts over the course of a day.

Myth:

Non-PC equipment is immune to threats

- ▼ Embedded Windows, Linux, Windows CE & other OS are vulnerable
 - » *Do you know what OS your equipment is running?*
- ▼ Unknown vulnerabilities in other OSes
- ▼ Industrial devices not routinely patched
- ▼ Denial of Service attacks



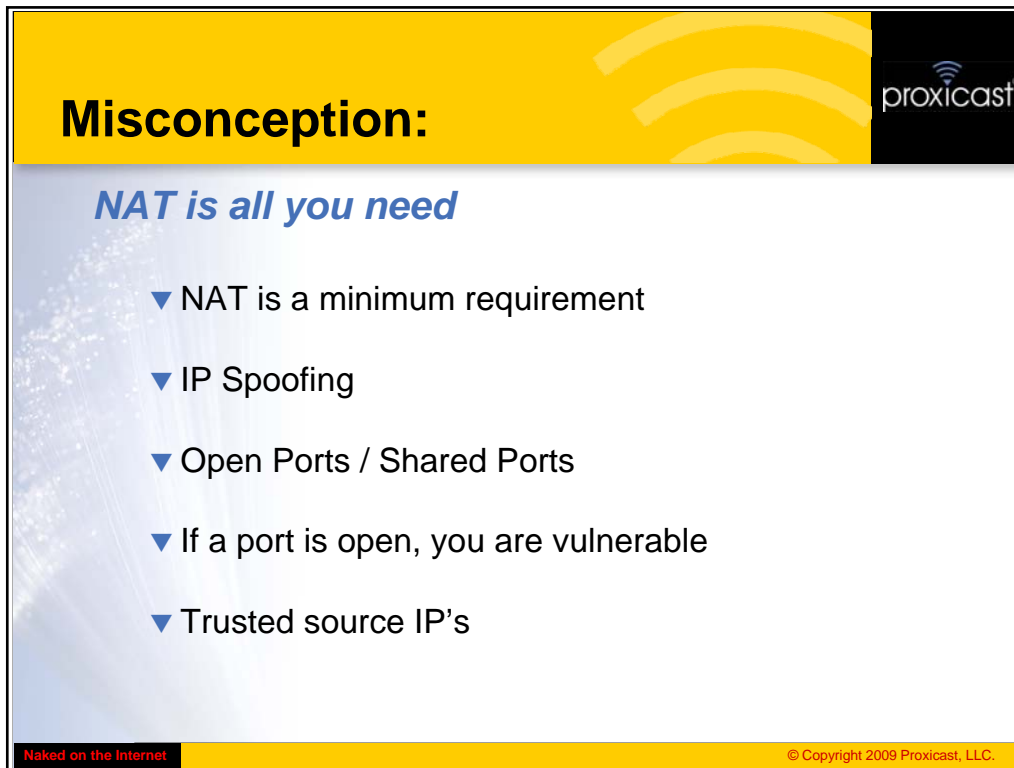
Naked on the Internet © Copyright 2009 Proxicast, LLC.

Some users mistakenly believe that because the equipment be connected at their remote site isn't a Windows-based PC, it is immune to threats.

Do you really know what OS your equipment is running? Linux, Windows CE and Windows-Embedded are very popular, esp. for newer, higher function devices. These OS's have the same vulnerabilities as their desktop counterparts.

Even if you're equipment is running a "proprietary" OS, it may be vulnerable. Industrial devices are not typically tested as thoroughly for security holes as are desktop systems. Nor are these devices routinely patched or updated as are most desktop & server systems.

All devices connected to the Internet are vulnerable to denial-of-service attacks where hackers aren't necessarily attempting to break into your equipment, just to disrupt your communications.



Misconception:

NAT is all you need

- ▼ NAT is a minimum requirement
- ▼ IP Spoofing
- ▼ Open Ports / Shared Ports
- ▼ If a port is open, you are vulnerable
- ▼ Trusted source IP's

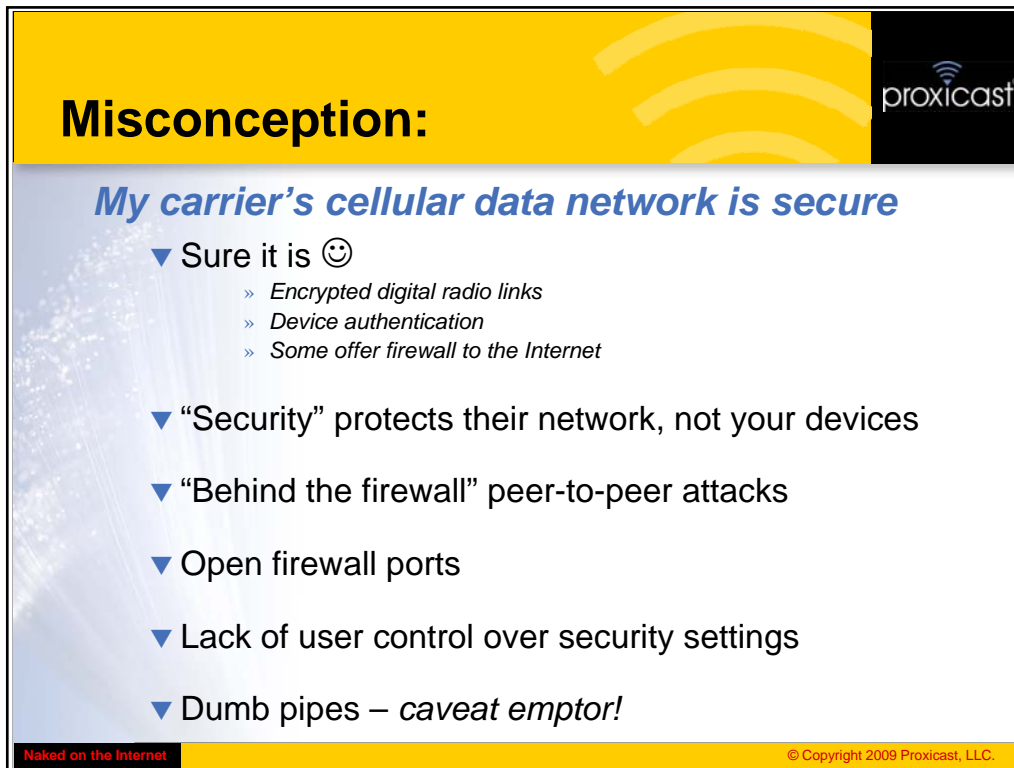
Naked on the Internet © Copyright 2009 Proxicast, LLC.

Network Address Translation provides a basic form of firewalling by allowing one or more private IP addresses to “masquerade” as a public IP address. Some users feel that this is sufficient protection.

NAT alone does not adequately protect against IP Spoofing – that is, hackers fooling the NAT device into thinking that their IP address is part of the private network.

Also, in order for you to communicate to your equipment from an Internet site, you must open one or more “ports” for communications. Once you do this, you have opened a door that can potentially be exploited by a hacker.

One way to reduce this vulnerability is to enforce access control lists so that only trusted IP addresses can open ports and communicate with your remote sites.



Misconception:

My carrier's cellular data network is secure

- ▼ Sure it is 😊
 - » Encrypted digital radio links
 - » Device authentication
 - » Some offer firewall to the Internet
- ▼ “Security” protects their network, not your devices
- ▼ “Behind the firewall” peer-to-peer attacks
- ▼ Open firewall ports
- ▼ Lack of user control over security settings
- ▼ Dumb pipes – *caveat emptor!*

Naked on the Internet © Copyright 2009 Proxicast, LLC.

Cellular carriers often tout the security of their networks. Some users are willing to turn over all security concerns to the carrier.

Cellular networks are indeed secure. But carriers are protecting their network, not your data or your devices. Secure radio links and device authentication prevent unauthorized users from accessing the network. Carrier firewalls prevent outside hackers from attacking the network.

You are still vulnerable to “behind the firewall” attacks. For example, an infected laptop somewhere else on the cellular network could attempt to access your devices.

The carrier will have to open firewall ports (if they operate a firewall) to let you in, therefore the hackers have a way in. By letting the carrier run the firewall, you are giving up all control over the security settings and are subject to their policies and procedures.

Regardless of what the carrier's promise, you should consider all cellular data networks just to be “dumb pipes” and take responsibility for providing and managing your own security solution.

Misconception:

Cellular private IP's are safe

- ▼ Requires both ends of the connection to be on the cellular network
- ▼ Bandwidth limitations for connection to multiple remote sites
- ▼ Limits network design flexibility
- ▼ Peer-to-Peer attacks – e.g. infected laptop

Naked on the Internet © Copyright 2009 Proxicast, LLC.


Some cellular carriers offer “private IP” solutions so that your traffic does not have to go across the Internet.

Often, this solution requires that both ends of your connection be connected to the cellular network, since you have no access to the Internet. This increases your communications costs. If you need to communicate with more than 1 remote site, bandwidth may become an issue since cellular links typically offer less capacity than wired links.

In general, private IP solutions from the carrier limit your network design options and make it difficult to access your remote sites from anywhere other than a specific location.





As we mentioned earlier, you are still vulnerable to attacks from peer devices on the private network that are outside of your control.

Misconception:



Can't use a VPN with industrial devices

- ▼ PLC's, sensors, data loggers, cameras, etc.
- ▼ Hardware VPN option
- ▼ Other end can be fixed or mobile device
- ▼ No software or configuration of devices
- ▼ Cost & performance factors



Naked on the Internet© Copyright 2009 Proxicast, LLC.

Many users know that a VPN offers the most secure means of communicating over the Internet. But because their remote equipment consist of things like PLCs, sensors and other non-PC equipment, they think that a VPN cannot be employed.

The solution is a hardware VPN option – installing a device between the equipment and the router & cellular modem to serve as the end-point of a VPN tunnel.


The other end of the VPN tunnel can be either another piece of VPN hardware or can be software running on one or more PC's.

This approach does not require any software or configuration changes on the remote equipment and allows any type of remote equipment to communicate securely through the VPN tunnel.

The downside is that there is a cost for the VPN hardware and communication performance will be slightly degraded due to the overhead associated with encrypting packets.

Key Security Technologies

- ▼ NAT & Firewalls
- ▼ VPN & Encryption
- ▼ Remote Monitoring & Alerts
- ▼ Modems vs. Gateways




Naked on the Internet

© Copyright 2009 Proxicast, LLC.

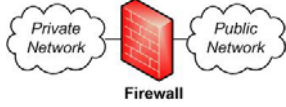
proxicast®

Let's take a closer look at some of the key security technologies that go into creating a secure cellular data communications link.

Firewalls: Good, Bad, Ugly



- ▼ NAT is a basic type of firewall – no granular control
- ▼ Stateful Packet Inspection Firewalls
 - ▼ *Pass/Reject Rules & Filters:*
 - ▼ By Port
 - ▼ By Protocol & Packet Type
 - ▼ By Source / Destination IP
 - ▼ By Time of Day
 - ▼ Rules sets for every packet direction
 - ▼ Anti-probing & denial-of-service protection
 - ▼ Alerting & Logging



Naked on the Internet © Copyright 2009 Proxicast, LLC.

Firewall is a broad term that encompasses many different approaches to controlling access to remote equipment.


As we've mentioned, NAT is a very basic type of firewall, but it gives you little control over how and when access is permitted.

The most common and best type of firewall are stateful packet inspection firewalls which look at each packet of data and track the source and destination of data stream connections. SPI firewalls typically allow you to define the rules by which packets are accepted or rejected based on things like port being used, protocol/packet type, source and/or destination IP address, even type of day that the rules should apply.


Firewalls should allow you to define rules for every possible packet direction in your system to minimize unexpected access requests. They should provide techniques for minimizing probes and DoS attacks to make it harder for hackers to find and exploit your systems.

A good firewalls should also have a means of proactively logging and alerting you to attacks as they happen.

Virtual Private Networks



- ▼ Most secure communication option
- ▼ IPSec, PPTP, L2TP, GRE
- ▼ Site-to-Site
- ▼ Client-to-Site
- ▼ Hardware vs. Software VPN
- ▼ Pre-shared Keys vs. Digital Certificates
- ▼ Encryption – DES, 3DES, AES
- ▼ Performance issues



Naked on the Internet

© Copyright 2009 Proxicast, LLC.

A virtual private network provides the most secure communications between sites across the Internet.

Several different types of VPN connections are possible, the most common being IPSec.


VPNs can be established between private networks at 2 different sites. They can also be created between a single PC and a remote site.

VPNs can be implemented via specialized hardware or in software on general purpose PC's and servers.


The security of a VPN comes via the algorithms used to encrypt data before it is transmitted over the Internet. Simple VPNs use a "key" that is shared between the 2 sites. Public key encryption using digital certificates provides much more robust way of authenticating the sender.

Encryption algorithms for VPNs range in complexity – however the "stronger" the encryption, the larger the performance degradation.

Remote Monitoring & Alerting



- ▼ Proactive notification of security events
 - ▼ Unauthorized access attempts
 - ▼ Configuration changes
 - ▼ Port scans
 - ▼ Service attacks
- ▼ Syslog Server
- ▼ Central Management Console
- ▼ E-Mail / Pager
- ▼ SNMP traps



Naked on the Internet © Copyright 2009 Proxicast, LLC.

An often overlooked aspect to remote security is the proactive monitoring of events.


Particularly in situations where your remote sites are “unmanned”, it is important to have your remote security equipment record suspicious activity and even alert you in real-time to certain events such as login attempts, changes to system settings, excessive port scans or other types of attacks.

Security events can be consolidated across sites via a Syslog server, or sent via E-Mail or pager message. Some products even support SNMP traps for security related events.

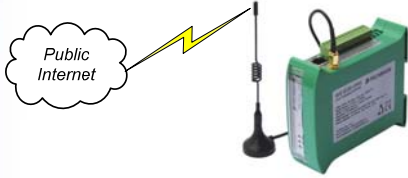
Modems vs. Gateways

Modem = Unprotected Internet connection

- ▼ Is a modem alone good enough at home or work?



- ▼ Embedded modem = Internet directly into your device



- ▼ Multiple external devices required for full protection

Naked on the Internet © Copyright 2009 Proxicast, LLC.

We started out discussing how just connecting to a cellular data network can leave you exposed to all sorts of threats.

The most common way that users connect to the cellular Internet is by installing a cellular modem. This might be an external device or a card installed in a laptop.

Strangely, at home and at work, most users realize that they need more than a DSL or cable modem when connecting to the Internet – they install routers, firewall software, etc. You need the same sorts of protection on the cellular Internet.

If your remote equipment has an embedded cellular modem – the Internet is now “inside” your equipment making it nearly impossible for you to implement strong security. For the best protection you need to combine the cellular modem with a NAT router, firewall VPN and remote monitoring solution.

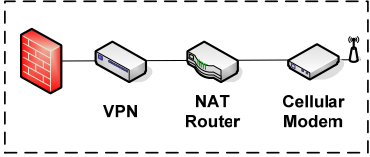
This combination of devices is commonly called a “Gateway”.

Modems vs. Gateways


proxicast®

Gateway = Secure Internet access via 1 device

- ▼ Modem +
 - ▼ Firewall
 - ▼ VPN & Encryption
 - ▼ NAT Routing & Port Forwarding
 - ▼ Event monitoring & alerting



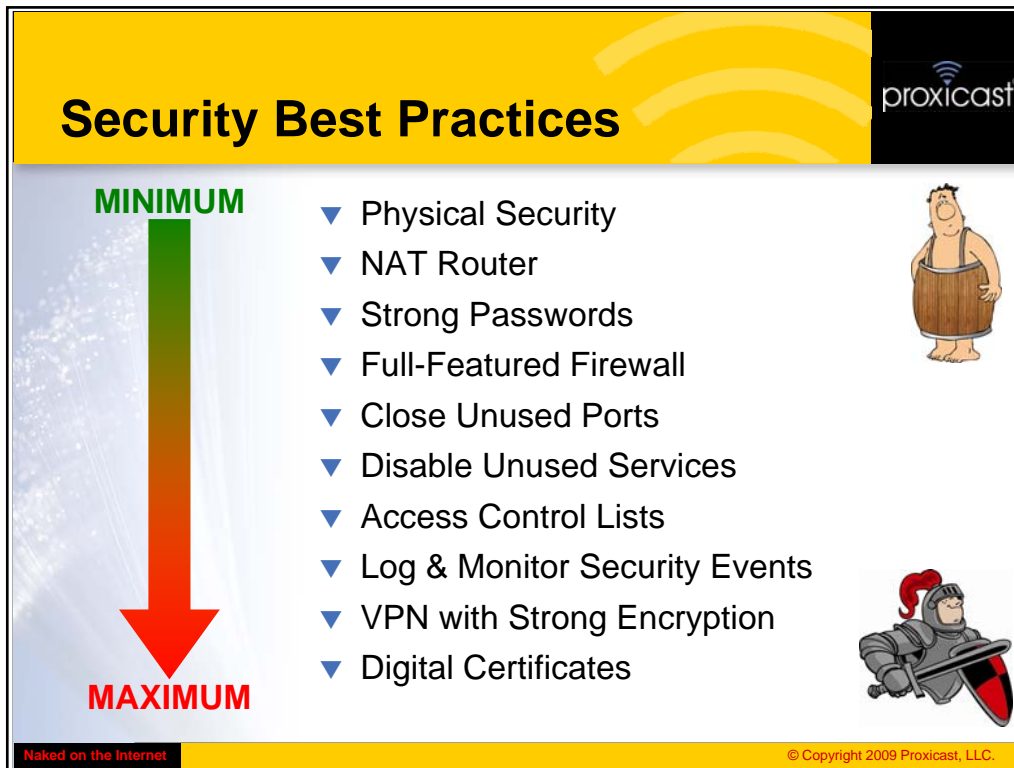
Secure Communications Gateway



Naked on the Internet © Copyright 2009 Proxicast, LLC.

As we mentioned in the beginning of this presentation, a Gateway typically consists of a modem plus a firewall, VPN, NAT Router and management functionality.

This combination provides much greater security and flexibility than a modem alone.



The slide features a yellow header with the title "Security Best Practices" and the Proxicast logo. A vertical arrow on the left transitions from green at the top (labeled "MINIMUM") to red at the bottom (labeled "MAXIMUM"). To the right of the arrow is a list of ten security practices, each preceded by a blue downward-pointing triangle. On the far right, there are two cartoon illustrations: a man in a wooden barrel and a Roman soldier in full armor.

Security Best Practices

- ▼ Physical Security
- ▼ NAT Router
- ▼ Strong Passwords
- ▼ Full-Featured Firewall
- ▼ Close Unused Ports
- ▼ Disable Unused Services
- ▼ Access Control Lists
- ▼ Log & Monitor Security Events
- ▼ VPN with Strong Encryption
- ▼ Digital Certificates

Naked on the Internet © Copyright 2009 Proxicast, LLC.

In summary, the best practices for securing remote cellular data communications involve a “layered” approach.

We’ve skipped over physical security, but if unauthorized users can access your remote equipment – all bets are off.

A NAT Router gives you a good first-line of defense. Remember to change the default password and implement strong passwords everywhere.

Couple the router with a full featured SPI firewall. Create rules that close all unnecessary ports and disable all unused services on your remote equipment. Implement access control lists to limit who can access what when.

Implement remote logging of security events.

If feasible, implement a VPN with strong encryption and digital certificates.

By implementing these Security Best Practices, you can go from Naked on the Internet to fully protected against any threat.

Q & A



▼ More Questions?

- ▼ *Web Site:* <http://www.proxicast.com>
- ▼ *E-Mail:* info@proxicast.com
- ▼ *Slides:* <http://www.proxicast.com/slides>
- ▼ *Phone:* 1-877-77PROXI (877-777-7694)
1-412-213-2477

Naked on the Internet © Copyright 2009 Proxicast, LLC.



Please visit www.proxicast.com for additional information on the LAN-Cell 2 Mobile Gateway series including detailed product specifications, manuals, tech notes and other resources.