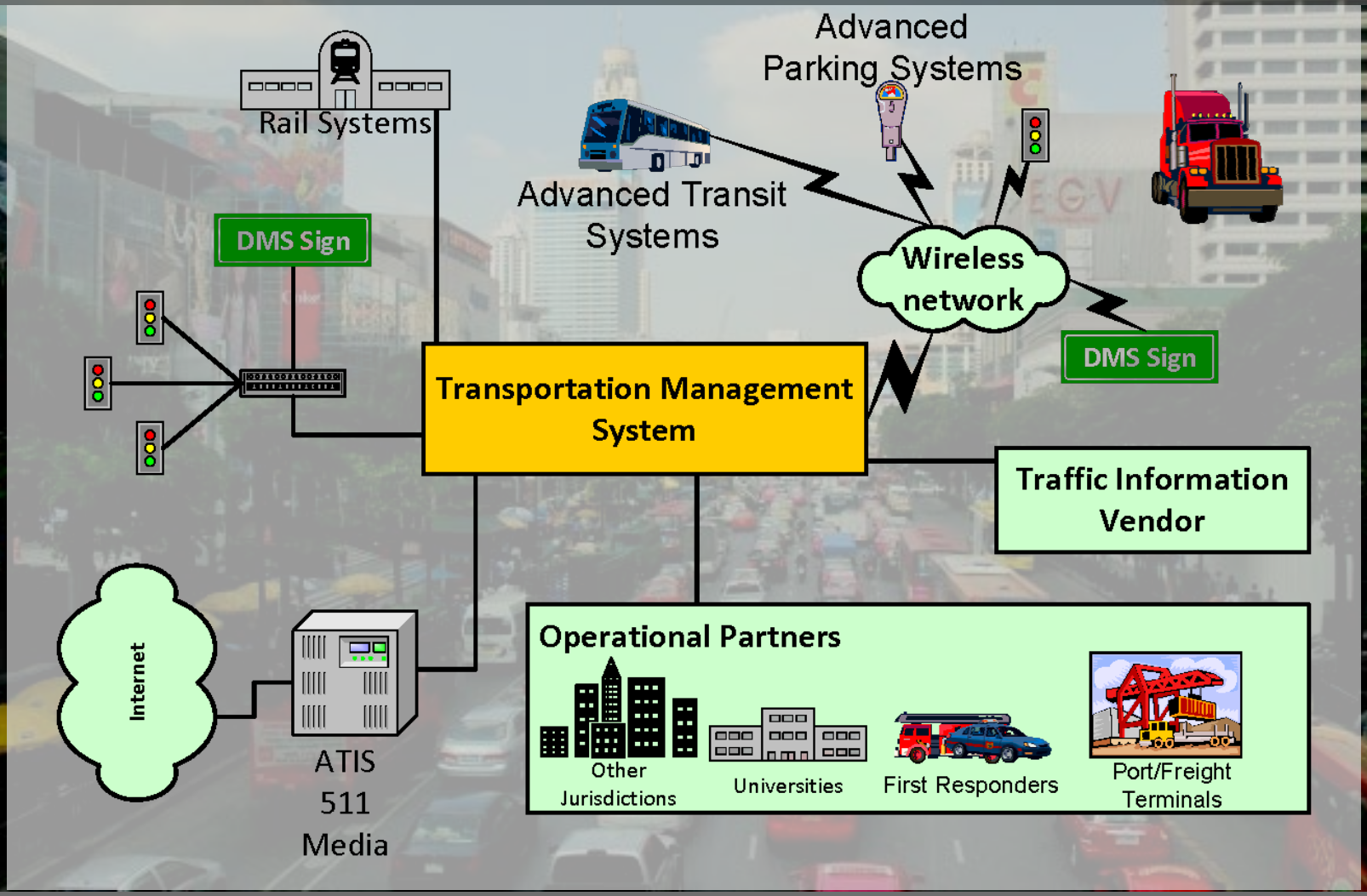
Cyber Concerns for Transportation Organizations – an Overview

FHWA Resource Center in San Francisco

Office of Technical Service - Operations Technical Service Team

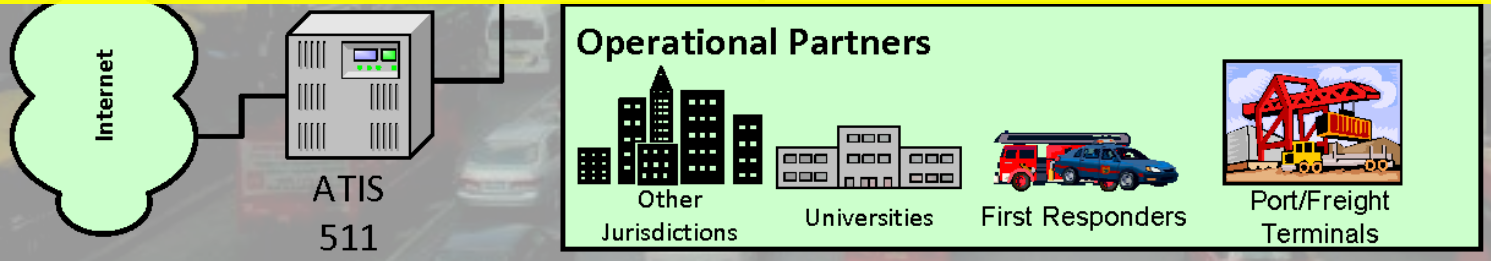
Edward Fok

Transportation Management System



Transportation Management System

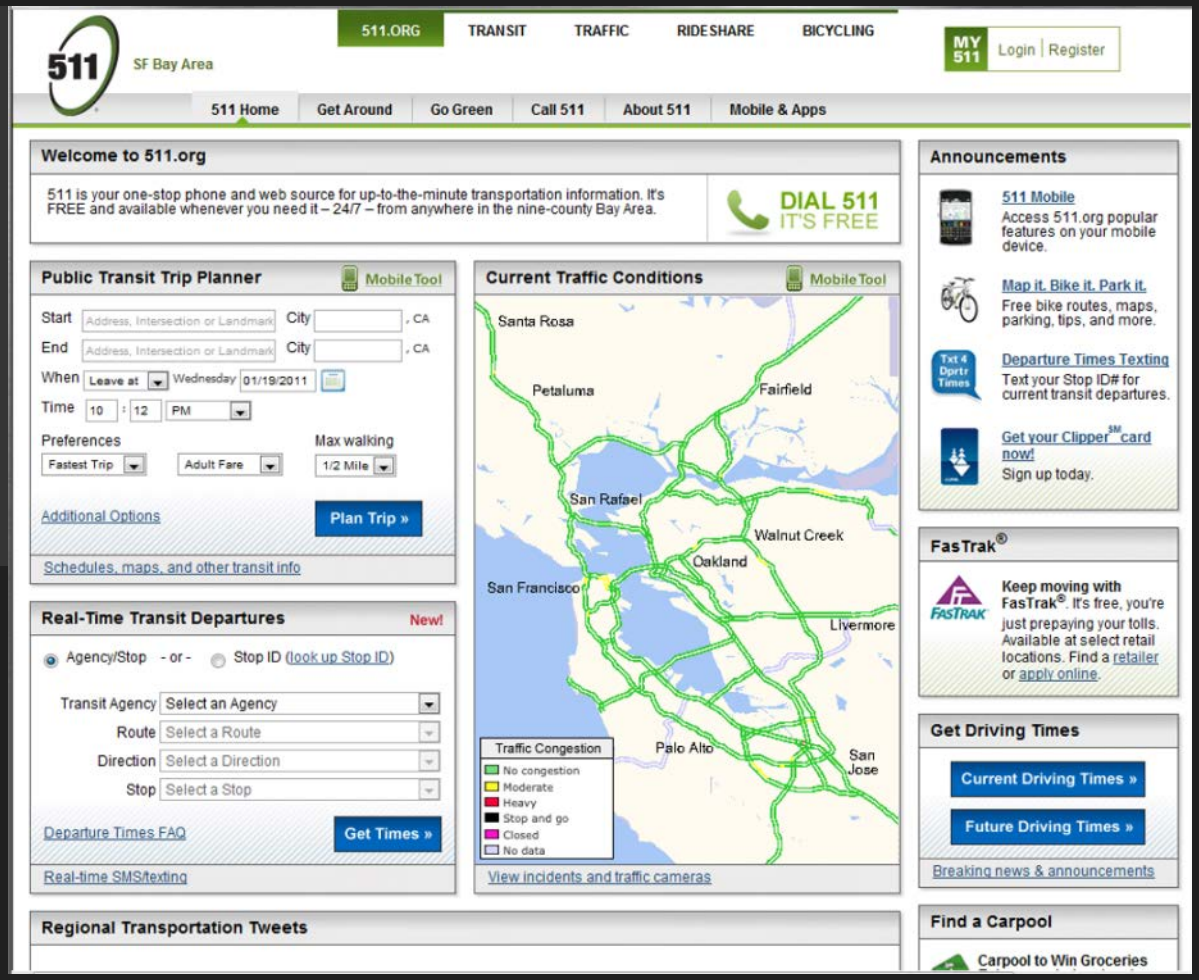
Safe assignment of right of ways
Maintain movement along major transportation facilities
Provide reliable and relevant information



Advanced Traveler Information Systems (ATIS)

Share risk similar to commercial web

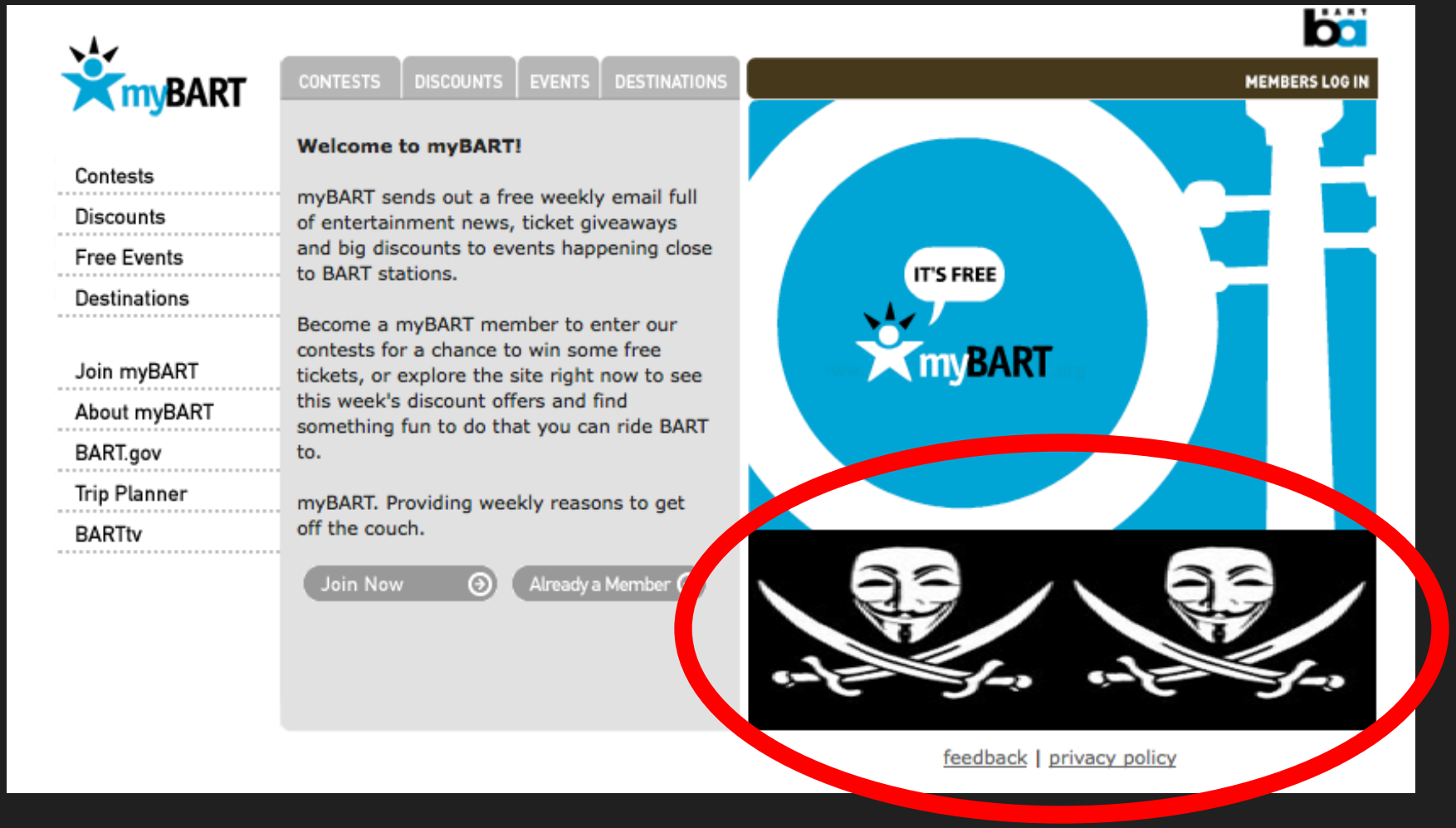
Best practices exist for hardening – just need to follow it



myBART.org, August 14, 2011

Sources: networkwold.com, sfgate.com, sfappeal.com, twitter.com, BART.gov

myBART.org, August 14, 2011



Sources: networkwold.com, sfgate.com, sfappeal.com, twitter.com, BART.gov

myBART.org, August 14, 2011

"Sooner or later the people in this country gotta realize the government
does not give a fuck about them. The government doesn't care about you, or your children,
or your rights, or your welfare, or your safety, it simply doesn't give a fuck about you.
It's interested in its own power, that's the only thing, keeping it and expanding it wherever possible."

#OpBart #Bart-Action #FREETOPIARY #FREEMERCEDES #FREEBRADLEYMANNING #Justice for Oscar Grant
No Justice, No Bart ### UA In The Bay ### Bay Of Rage ### Anti-sec #Justice for Charles Hill

Your Website has been hacked and database has been leaked by:
#tOnicwater #Bl4ckAbby #NaDa #Tanko #Anonymous #hackers

Dear Bay Area Rapid Transit, The People and All Government Agencies,

We are Anonymous, we are your citizens, we are the people, WE DO NOT TOLERATE OPPRESSION FROM ANY GOVERNMENT AGENCY.
BART has proved multiple times that they have no problem exploiting and abusing the people.
First they displayed this by the two recent killings by BART police. Under no circumstance, unless police are shot at,
make police killings acceptable. Non-lethal weapons were available to use during both incidents,
providing even that was necessary, but instead they shot to kill. Next they violated the people's right to assembly and prevented
other bystanders from using emergency services by blocking cell phone signals in order to stop a protest against the BART police murders.
Lastly, they set up this website called mybart.gov and they stored their members information with virtually no security.
The data was stored and easily obtainable via basic sqli. Any 8 year old with a internet connection
could have done what we did to find it. On top of that none of the info, including the passwords,
was encrypted. It is obvious BART does no give a fuck about its customers, funders and tax payers,THE PEOPLE.

The governments and government agencies of the world are becoming tyrannical and oppressive,
and the people are responding and will not take your shit for much longer. The people will fight
this oppression with protests, demonstrations, riots, hacking, ddos, online attacks and by any other means.
We will not allow ourselves to be killed, exploited, or get shitted on. From the streets of Chile,

Sources: networkwold.com, sfgate.com, sfappeal.com, twitter.com, BART.gov

Field Devices

Ramp/Gate/Signal Controllers

Fixed Dynamic Message Signs

Portable Dynamic Message Signs

Enforcement Systems

Payment Systems

Field Devices – Equipment Manuals

Ramp/Gate/Signal Controllers

Fixed Dynamic Message Signs

Portable Dynamic Message Signs

Enforcement Systems

Payment Systems

2.3. Passwords

Be sure to record your passwords in a safe location.

2.3.1. Restricted User Password

This allows access to basic sign operation, message activation, radar control and turning the sign off. The message sign is shipped with a default restricted password of "Guest".

2.3.2. Normal User Password

This allows access to basic sign operation, plus permission to create, modify and delete messages. The message sign is shipped with the default NTCIP user password of "Public", plus "ABCD".

Field Devices – Equipment Manuals

Ramp/Gate/Signal Controllers

Fixed Dynamic Message Signs

Portable Dynamic Message Signs

Enforcement Systems

Payment Systems

2.3. Passwords

Be sure to record your passwords in a safe location.

2.3.1. Restricted User Password

This allows access to basic sign operation, message activation, radar control and turning the sign off. The message sign is shipped with a default restricted password of "Guest".

2.3.2. Normal User Password

This allows access to basic sign operation, plus permission to create, modify and delete messages. The message sign is shipped with the default NTCIP user password of "Public", plus "ABCD".

Lodz, Poland, January 2008

4 light rail trams derailed, 12 people hurt

Tool used: Converted television IR remote

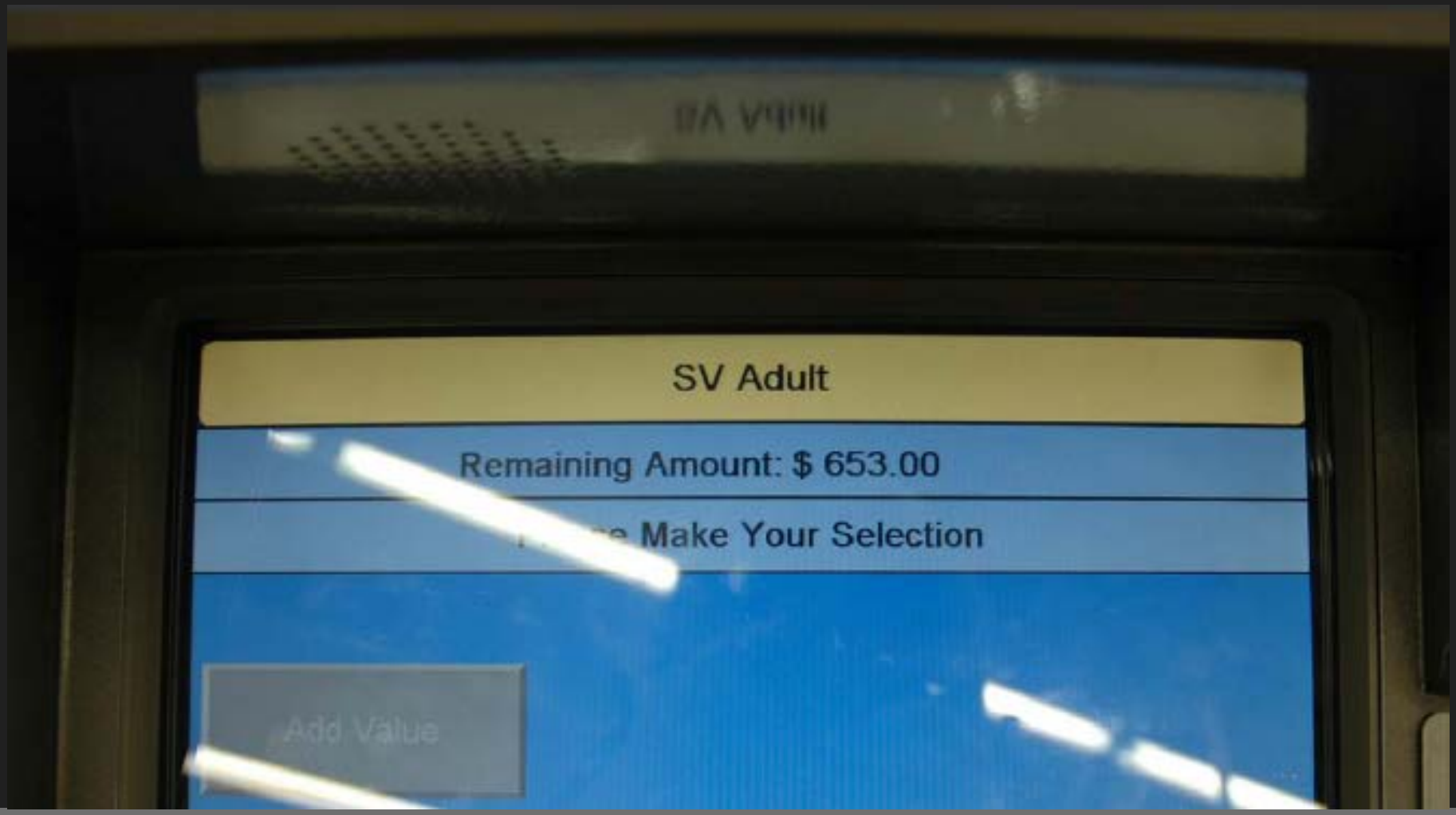
Lodz, Poland, January 2008

4 light rail trams derailed, 12 people hurt

Tool used: Converted television IR remote

Exploit: Locks to disable track changes when vehicle are present was not installed.

Bored with DMS? – RFID Transit Card

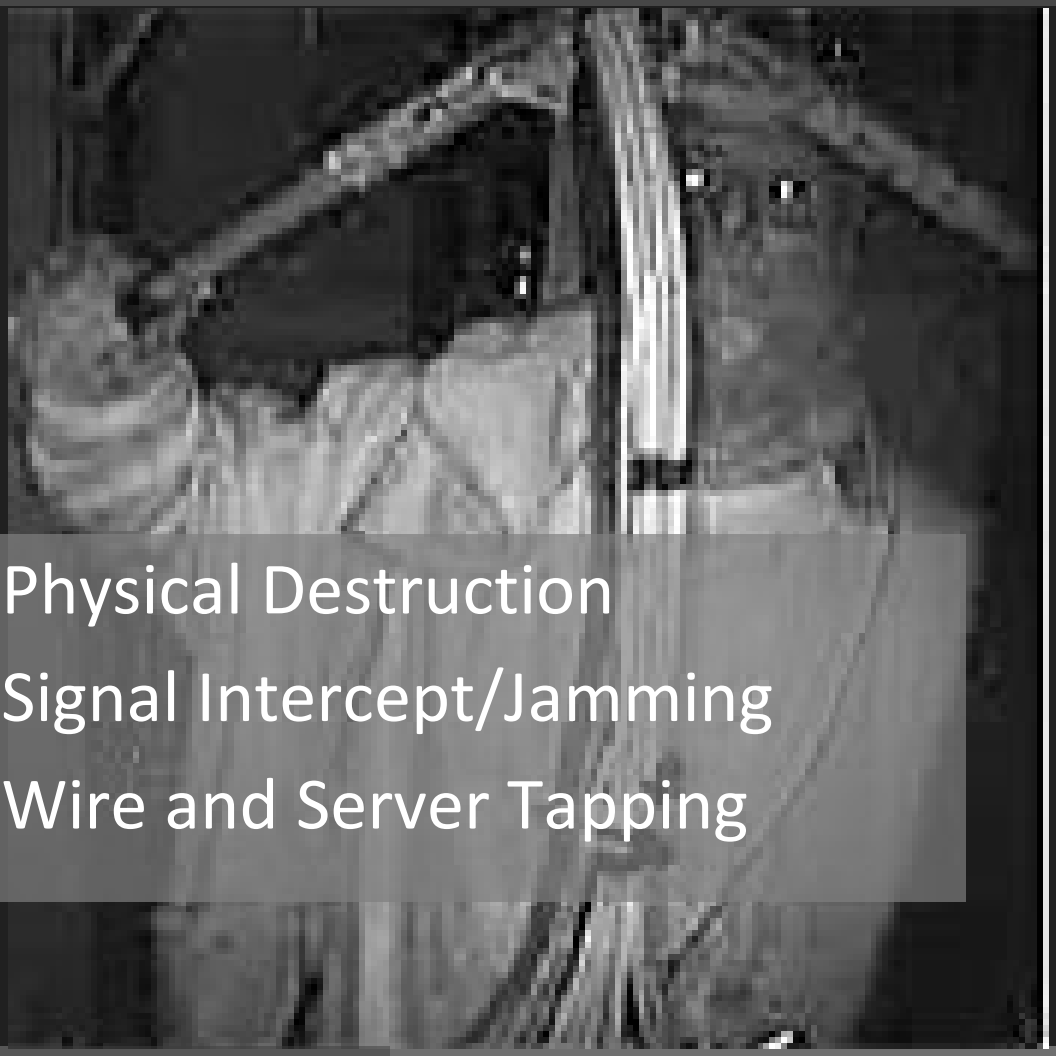


Bored with DMS? – Electronic Parking Meter

Center to Field (C2F) Network

- Monitor field equipment health and status
- Command and Control of field equipment
- Transmission of sensor/video information and images

C2F Network - Threats

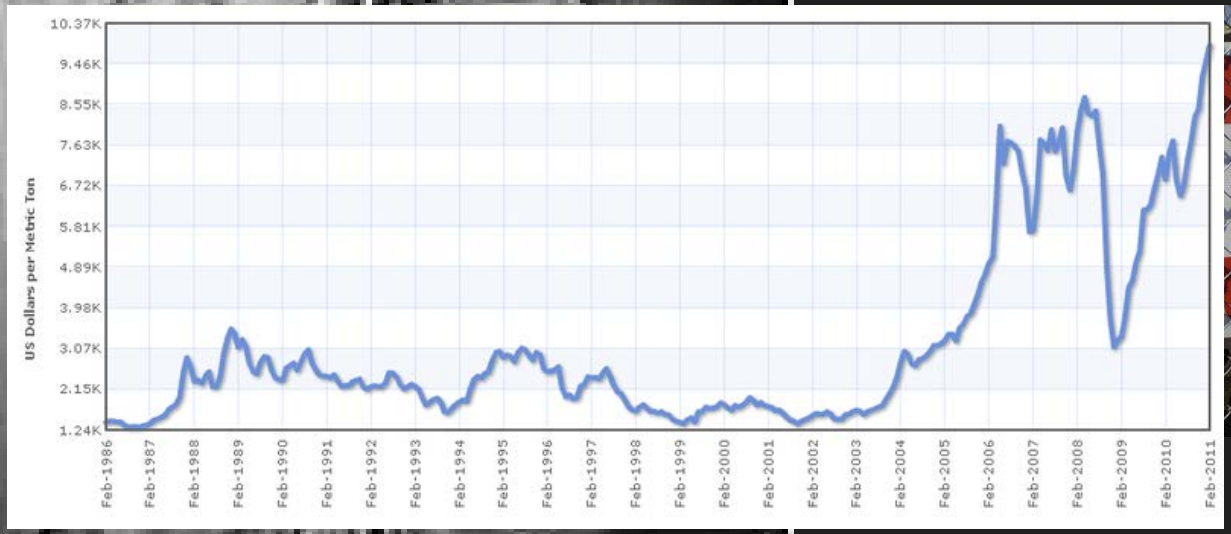


- Physical Destruction
- Signal Intercept/Jamming
- Wire and Server Tapping

Copper Statistic Source - Wikipedia

C2F Network - Threats

- Physical Destruction
- Signal Intercept/Jamming
- Wire and Server Tapping



Copper Statistic Source - Wikipedia

C2F - Wireless System Vulnerabilities

	Threat	Defendable?	Offensive Measures	Damage Potential
Eavesdropping	Low	No	No	Low
Communication Jamming	Moderate	No	Yes	High
Denial of Service Attacks	**High**	Yes	Some	High
Injection and Modification of Data	**High**	Yes	Yes	Low
Man-In-The-Middle Attacks	**High**	Yes	Yes	Moderate
Rogue Client	**High**	Yes	Yes	Low
Rogue Access Points	**High**	Yes	Yes	Moderate
Client to Client Attacks	Moderate	Yes	Yes	High
Network Equipment Attacks	Moderate	Yes	Yes	High

Threat = Probability of threat occurring to a transportation network

Defendable = Does solution exist to defend against this type of vulnerability?

Offensive Measures = Can offensive measure be taken against the attacker?

Damage Potential = Potential impact to vulnerable segment of the Transportation Network

C2F – Cellular Base Station Cloning

DEFCON 2010 - Fake GSM Base Station assembled using open source software and $1500 of hardware.

C2F – Cellular Base Station Cloning

DEFCON 2010 - Fake GSM Base Station assembled using open source software and $1500 of hardware.

DEFCON 2011 – GSM, CDMA, 1xRTT, WiMAX all cloned….

Source: http://seclists.org/fulldisclosure/2011/Aug/76

C2F Network - Summary

Open Ethernet ports

Wiretapping

So you think Fiber is better?

- *Passive Splitter*
- *Evanescent coupler*
- *Phase conjugation*

C2F Network - Summary

Open Ethernet ports

Wiretapping

So you think Fiber is better?

- *Passive Splitter*
- *Evanescent coupler*
- *Phase conjugation*

Deny Access to physical plant

Monitor network behavior

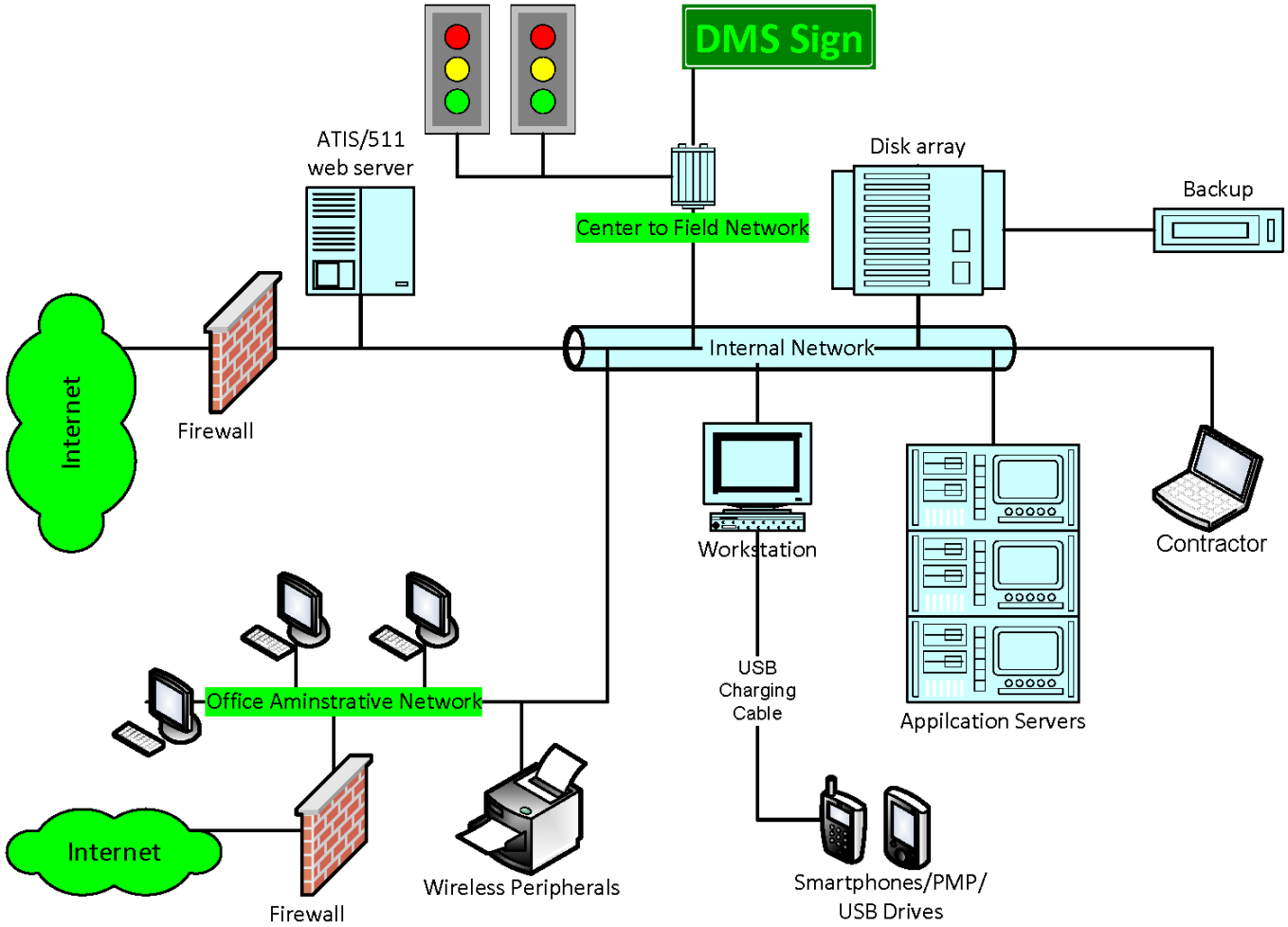
- *Traffic Analysis*
- *Data routing*
- *Communication interruption*
- *Time-domain Reflectometer*

How Paranoid are you?

- *Encrypted traffic*
- *Deep packet inspection*

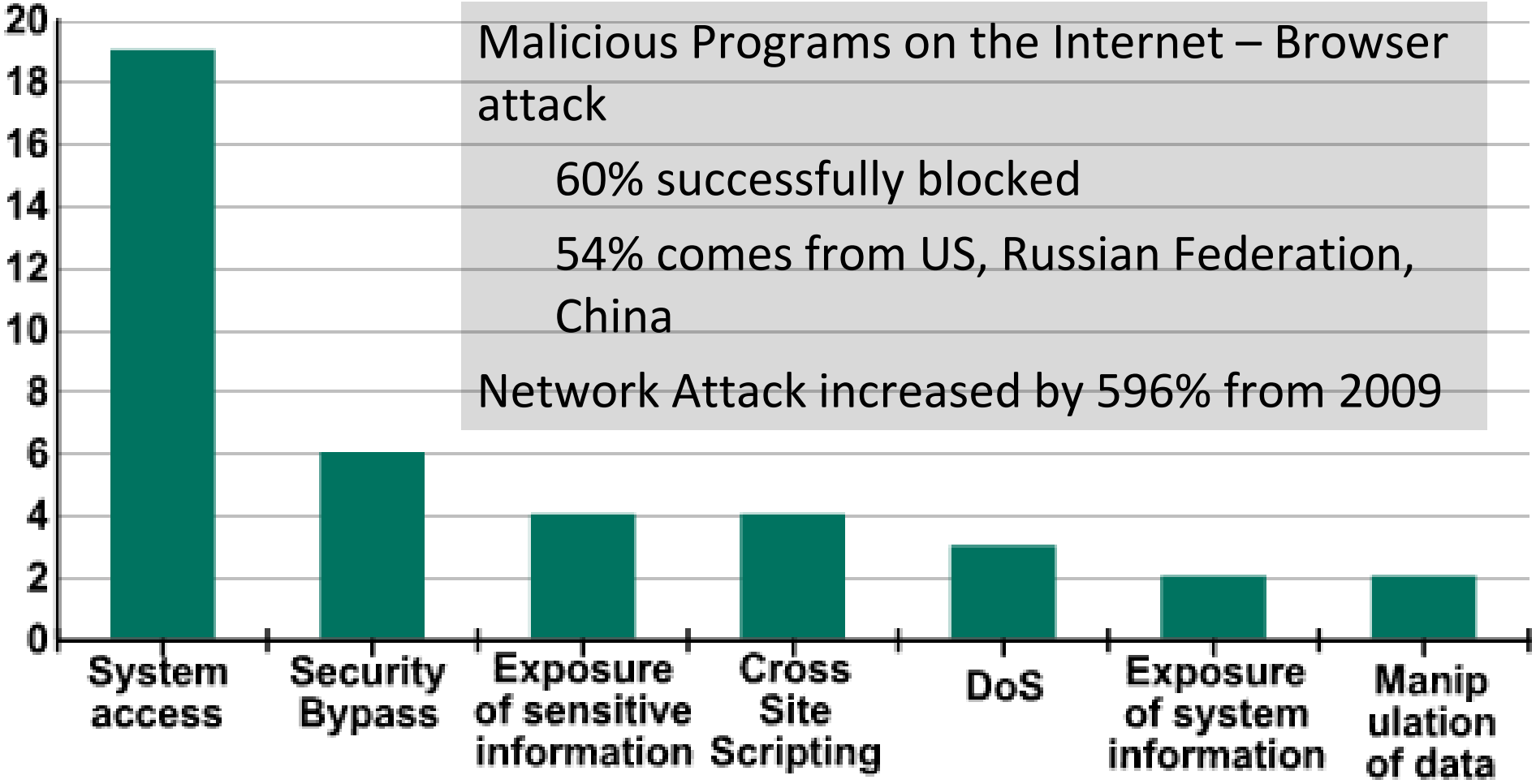
Back Office – The Management Center

Back Office – The Management Center



Back Office – Attack Vector

Kaspersky Lab



Malicious Programs on the Internet – Browser attack

- 60% successfully blocked
- 54% comes from US, Russian Federation, China

Network Attack increased by 596% from 2009

Statistic Source - Kaspersky Security Bulletin 2010 Statistics 2010

Davis-Besse Nuclear Plant, Ohio: January 25, 2003

16:00 – network slow down noticed

16:50 – Safety Parameter Display System (SPDS) crashes

17:13 – Plant Process Computer crashes, this has analog backup.

Source – securityfocus

Davis-Besse Nuclear Plant, Ohio: January 25, 2003

16:00 – network slow down noticed

16:50 – Safety Parameter Display System (SPDS) crashes

17:13 – Plant Process Computer crashes, this has analog backup.

Cause:

Dedicated line connecting the reactor to a contractor's network. A machine on that network was infected.

Source – securityfocus

Back Office

Image from 2003 Paramount Picture Film: "The Italian Job"

Back Office – Summary

- Lose remote control of field devices
- Lose ability to communicate/exchange data
- Remote control by unauthorized parties
- Vulnerable to Blackmail

The Washington Post

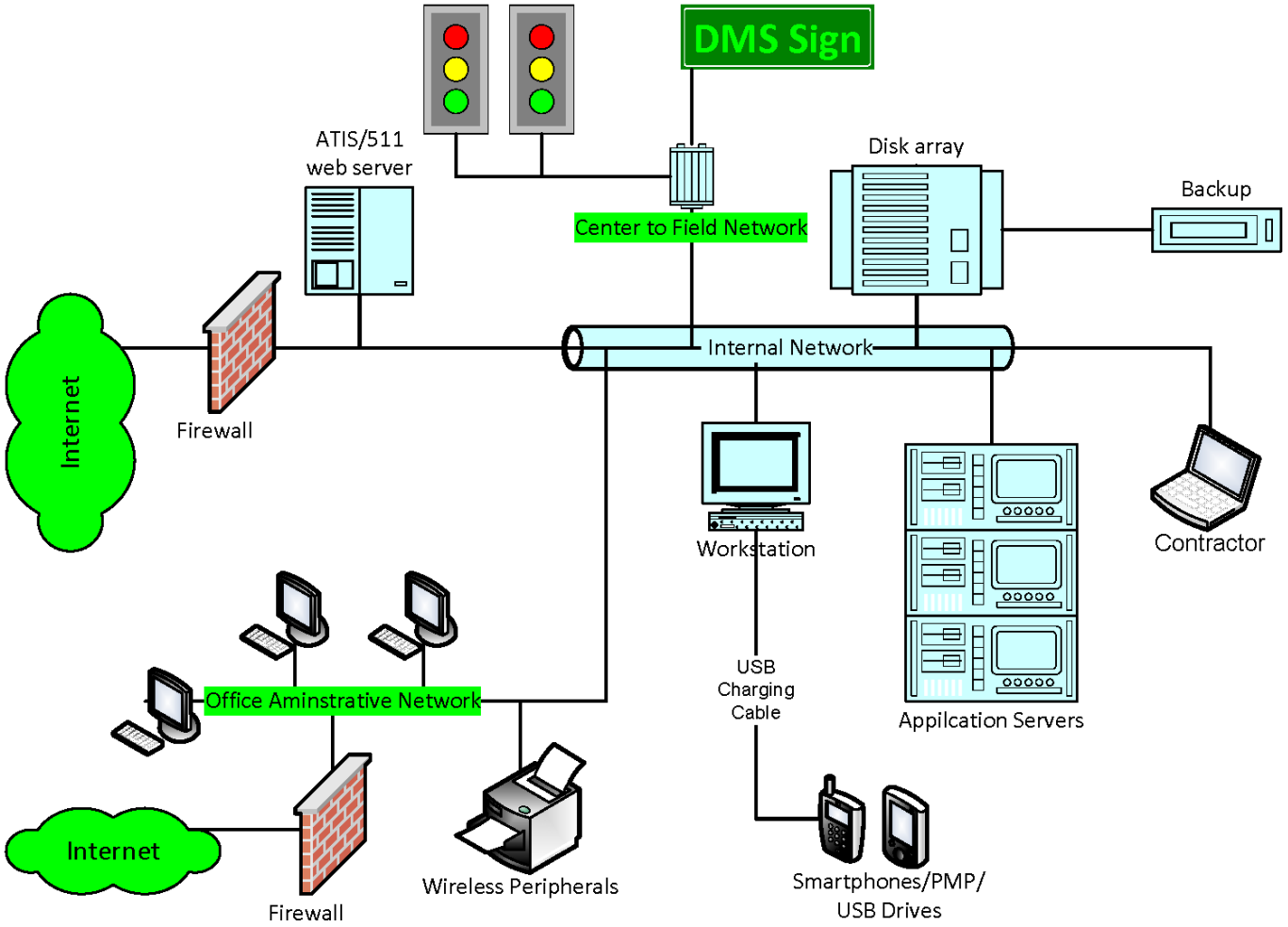
Humming along with technology, until it's not

Computer meltdown creates traffic-light chaos

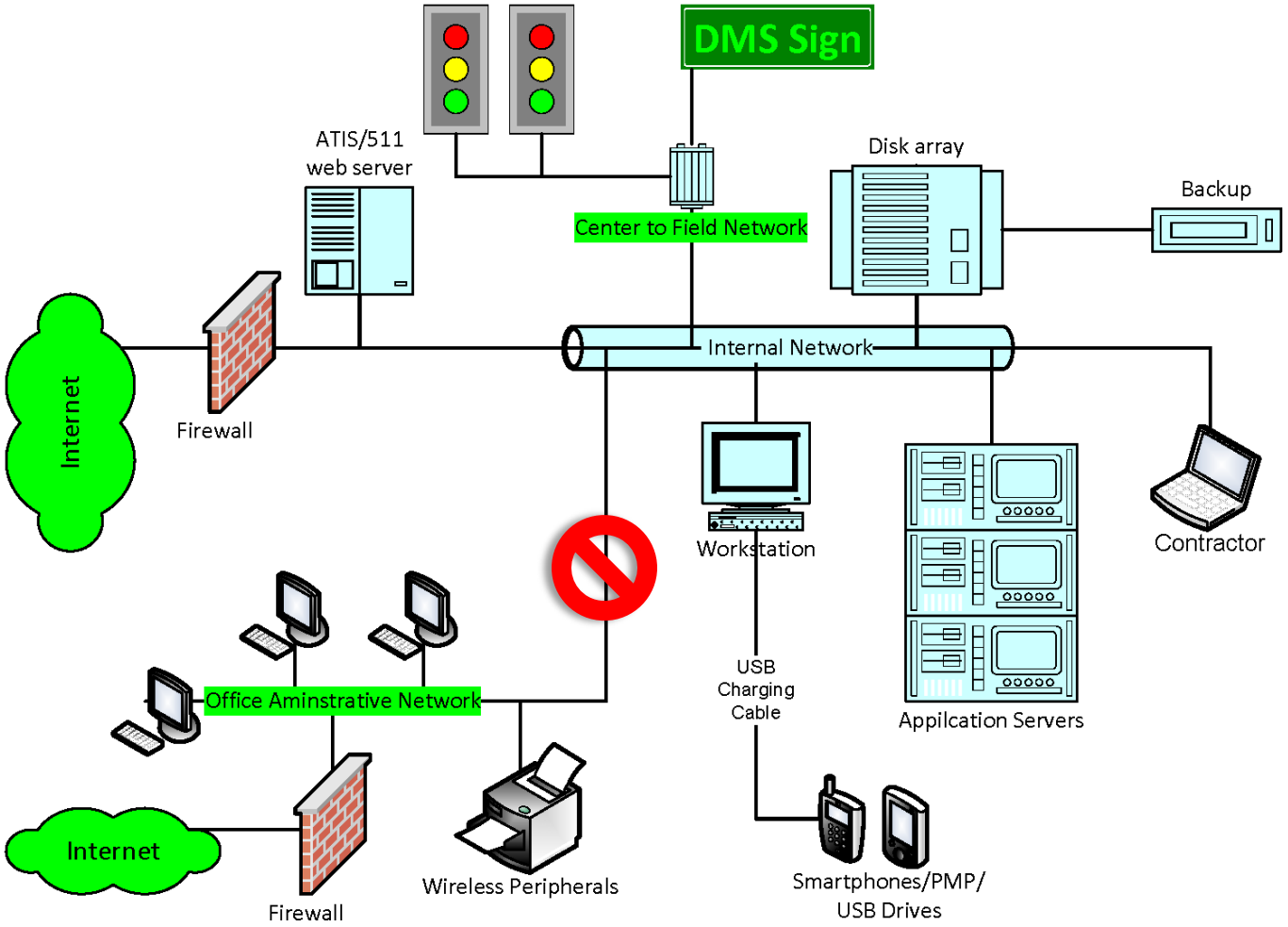
By Ashley Halsey III
Washington Post Staff Writer
Thursday, November 5, 2009

Image from 2003 Paramount Picture Film: "The Italian Job"

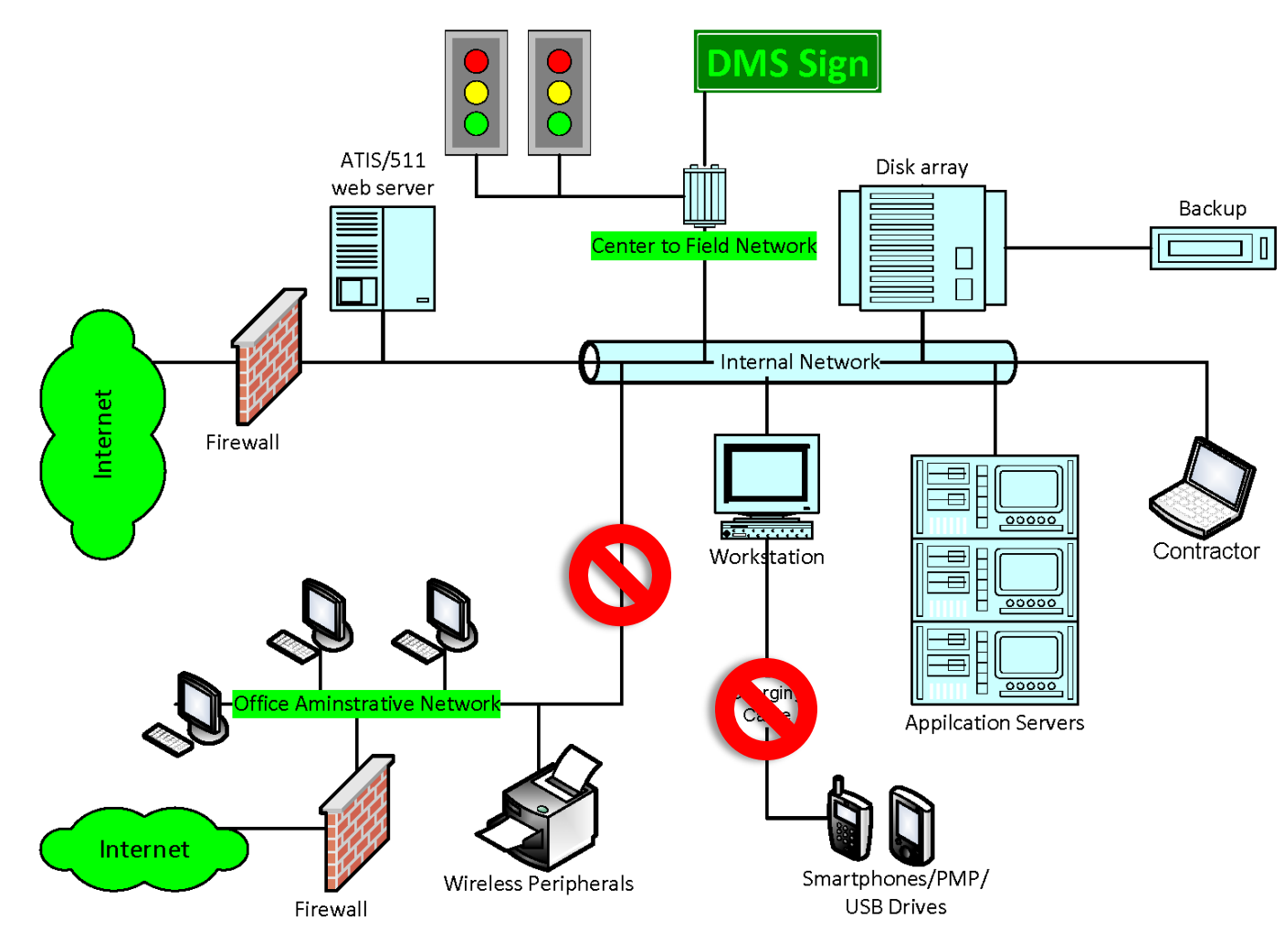
BackOffice – Hardening by Design



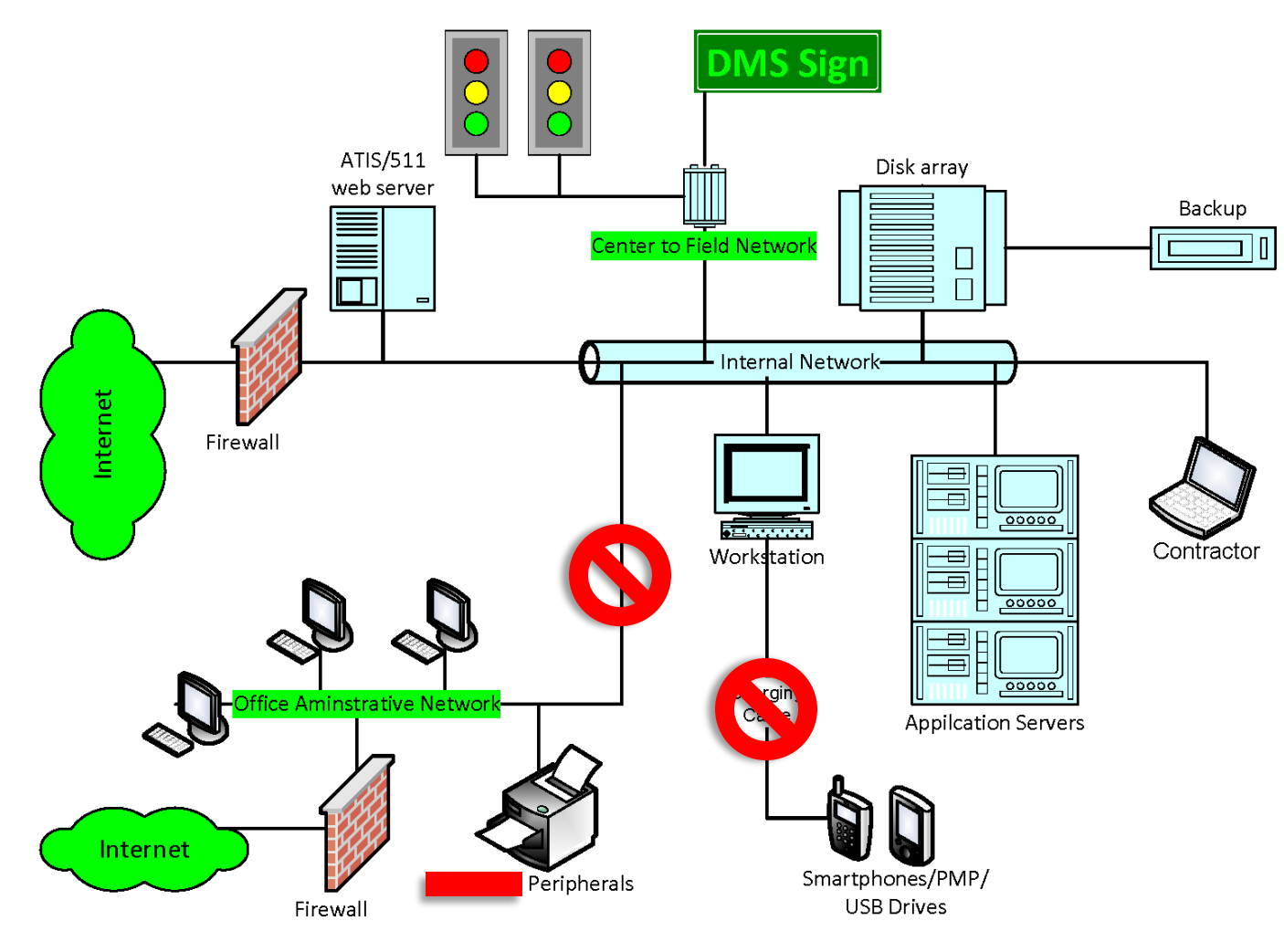
BackOffice – Hardening by Design



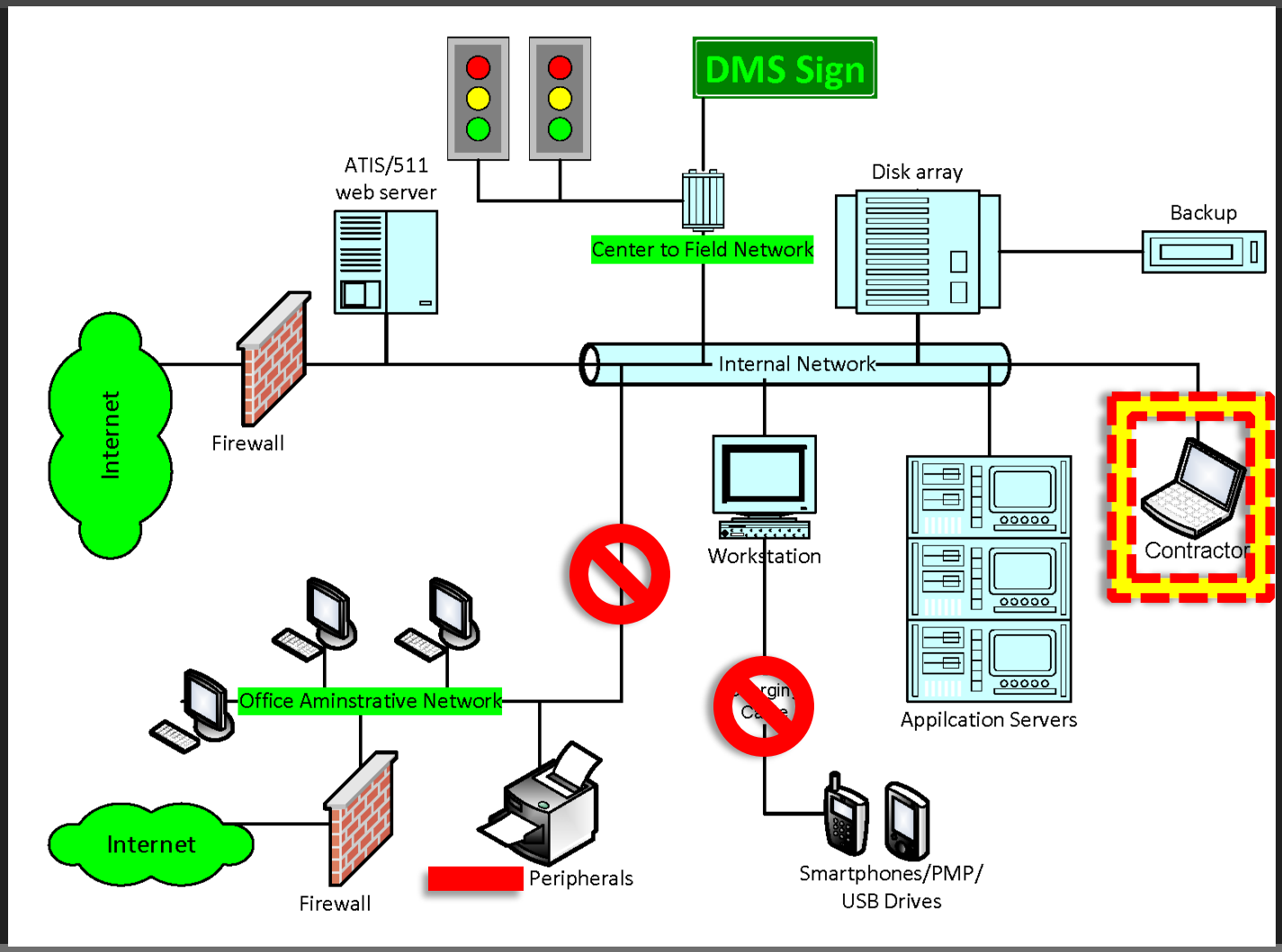
BackOffice – Hardening by Design



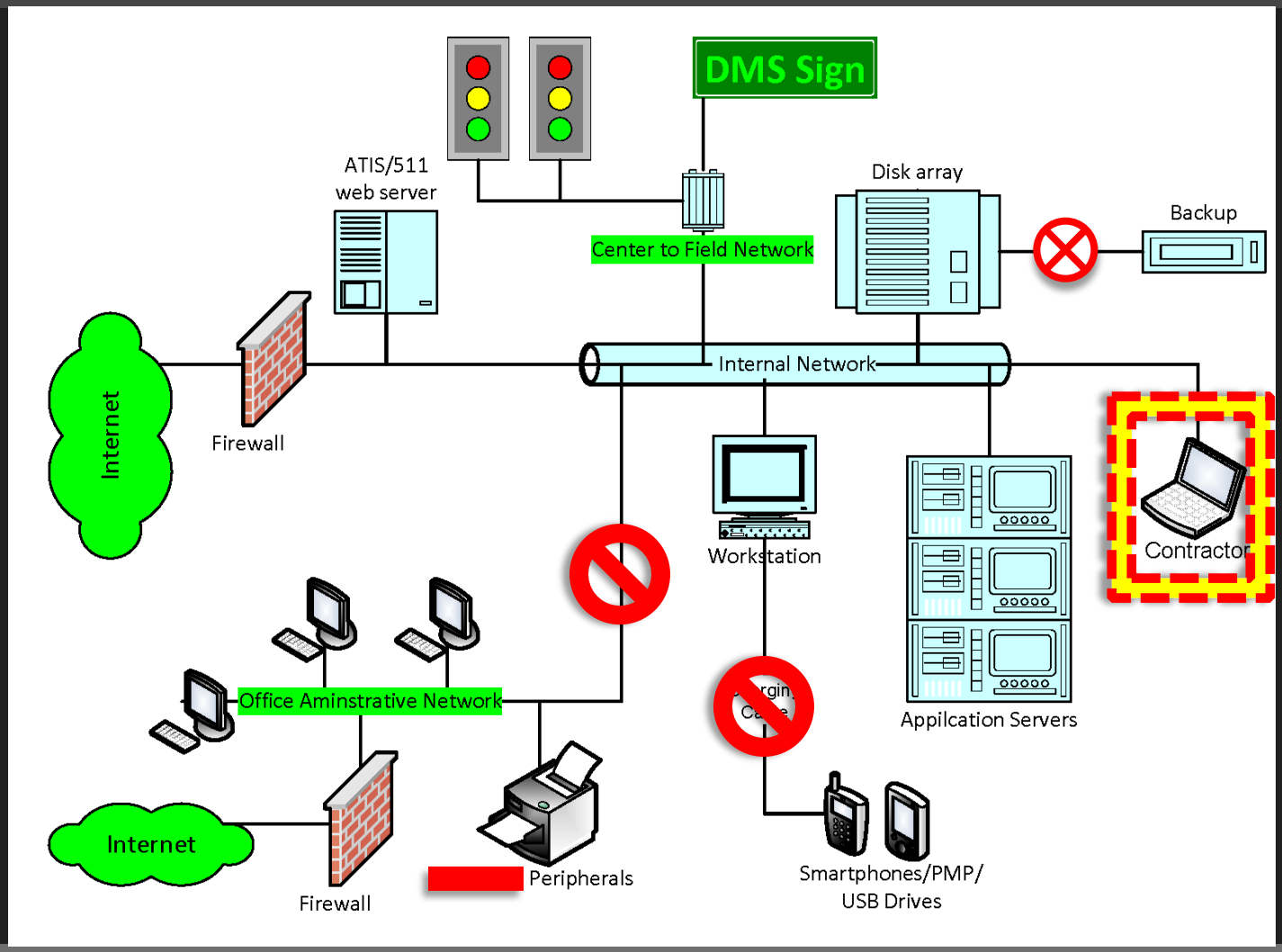
BackOffice – Hardening by Design



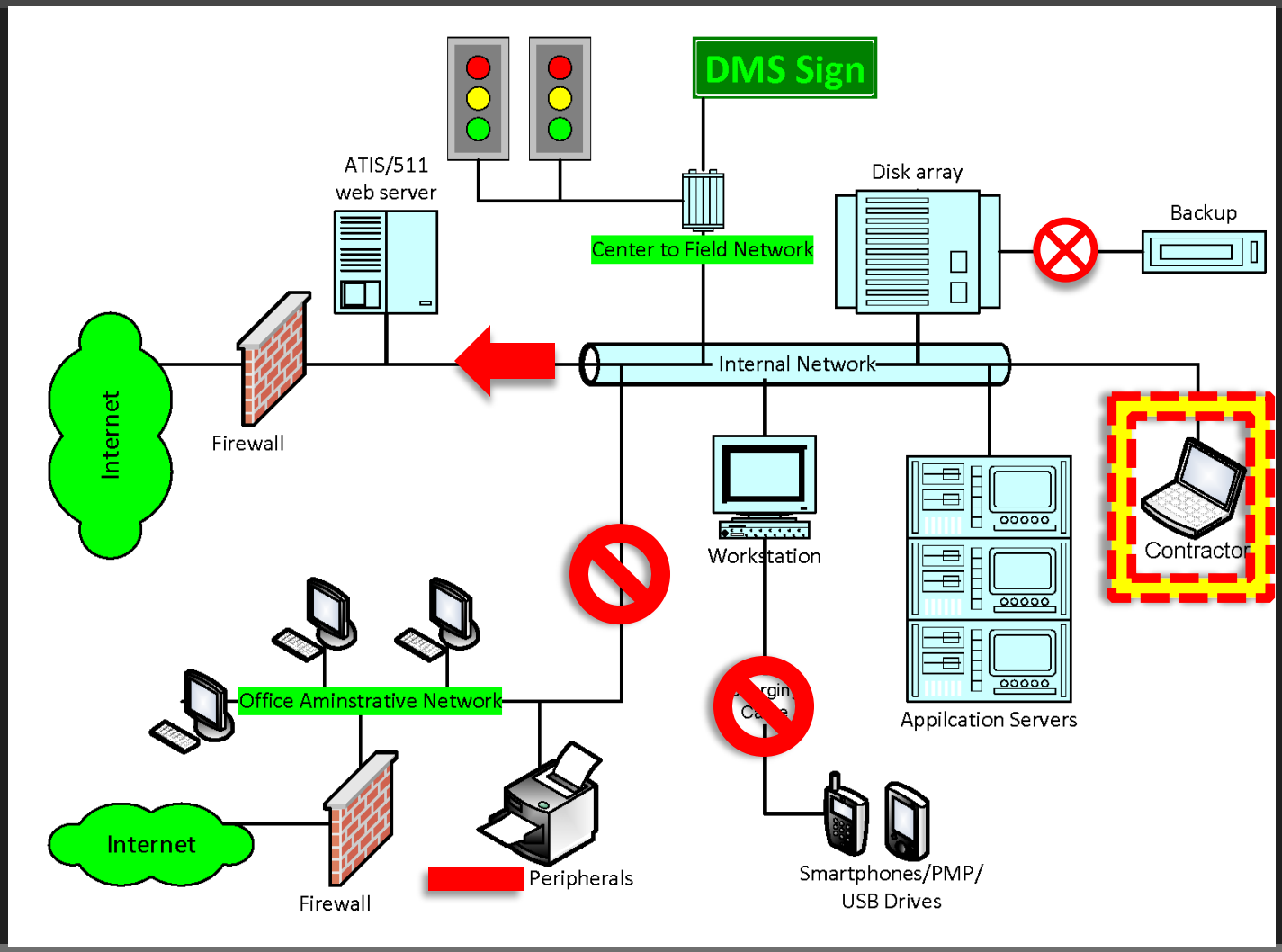
BackOffice – Hardening by Design



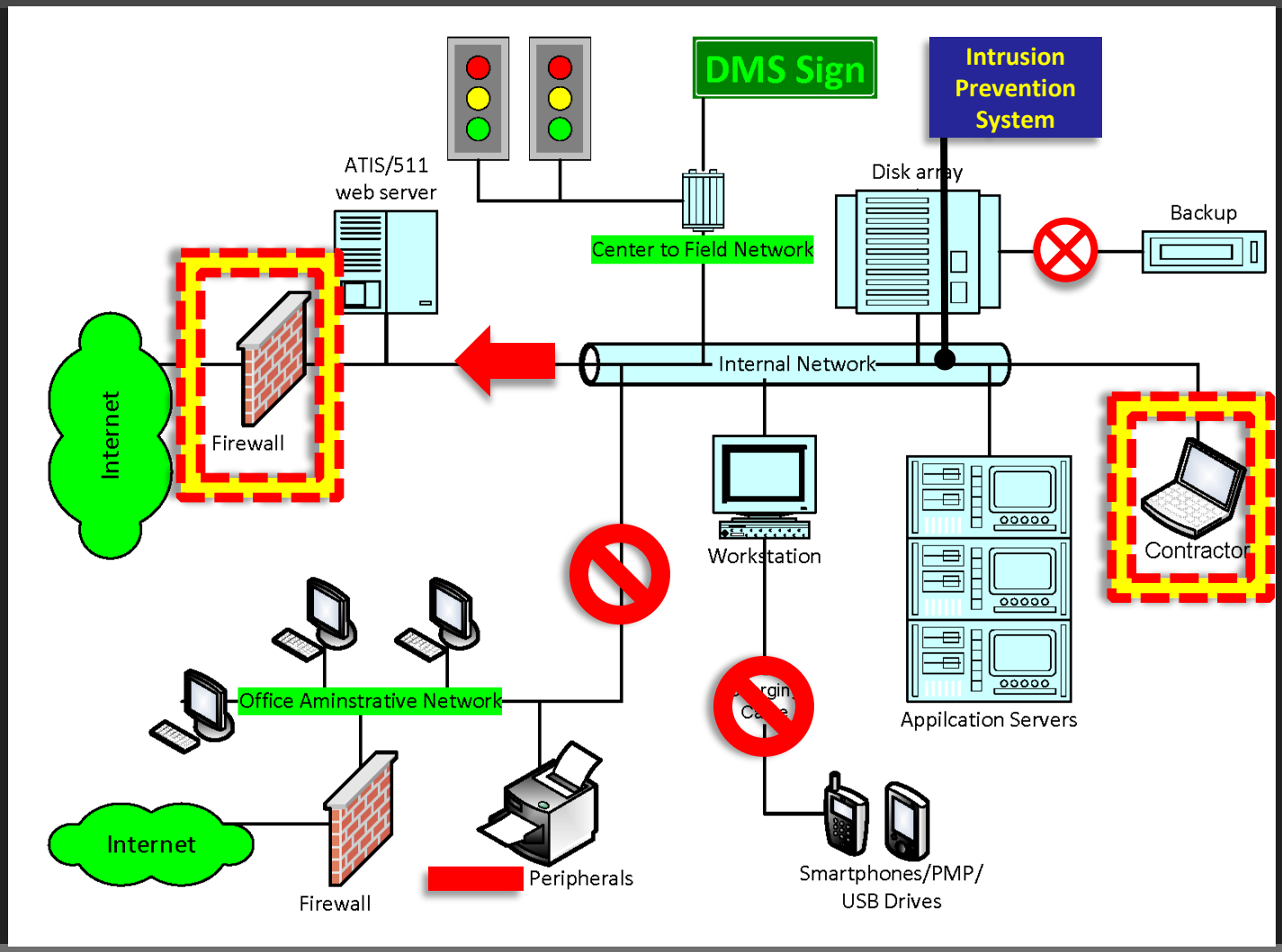
BackOffice – Hardening by Design



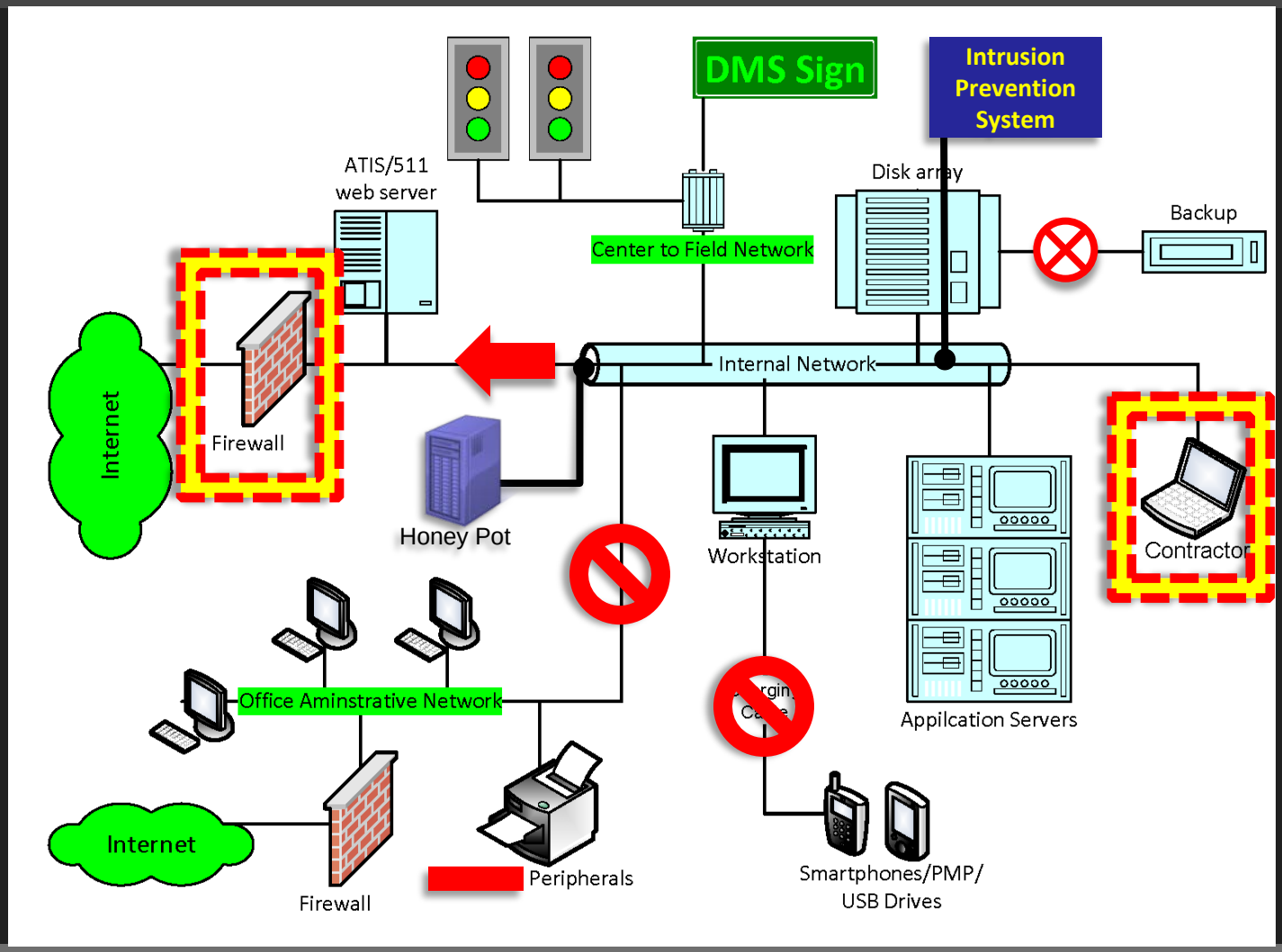
BackOffice – Hardening by Design



BackOffice – Hardening by Design



BackOffice – Hardening by Design



Emerging Challenges – Stuxnet & Duqu

Stuxnet is Cyber warfare munitions

Targeted against embedded/industrial devices

Duqu – spawn of Stuxnet

```
unicode 0, <)) select @t=rtrim(text) from dbo.syscomments c, dbo.syso>
unicode 0, <bjects o where o.id = c.id and c.id = object_id(N>
dw 27h
unicode 0, <[dbo].[MCPVREADVARPERCON]>
dw 27h
unicode 0, <) set @e=charindex(>
dw 27h
unicode 0, <,openrowset>
dw 27h
unicode 0, <,@t) if @e=0 set @t=right(@t,len(@t)-7) else begin set @f>
.
.
unicode 0, <Server=.\WinCC;uid=WinCCConnect;pwd=2WSXcder>
```

Source: Wired, The Register, eWeek, Symantec, Kaspersky Lab

Emerging Challenges – Stuxnet & Duqu

Stuxnet is Cyber warfare munitions

Targeted against embedded/industrial devices

Duqu – spawn of Stuxnet

Vulnerability to Transportation

~307,000 traffic signal controllers today

~98,000 uses some kind of operating system

Unknown numbers are networked together and to the web

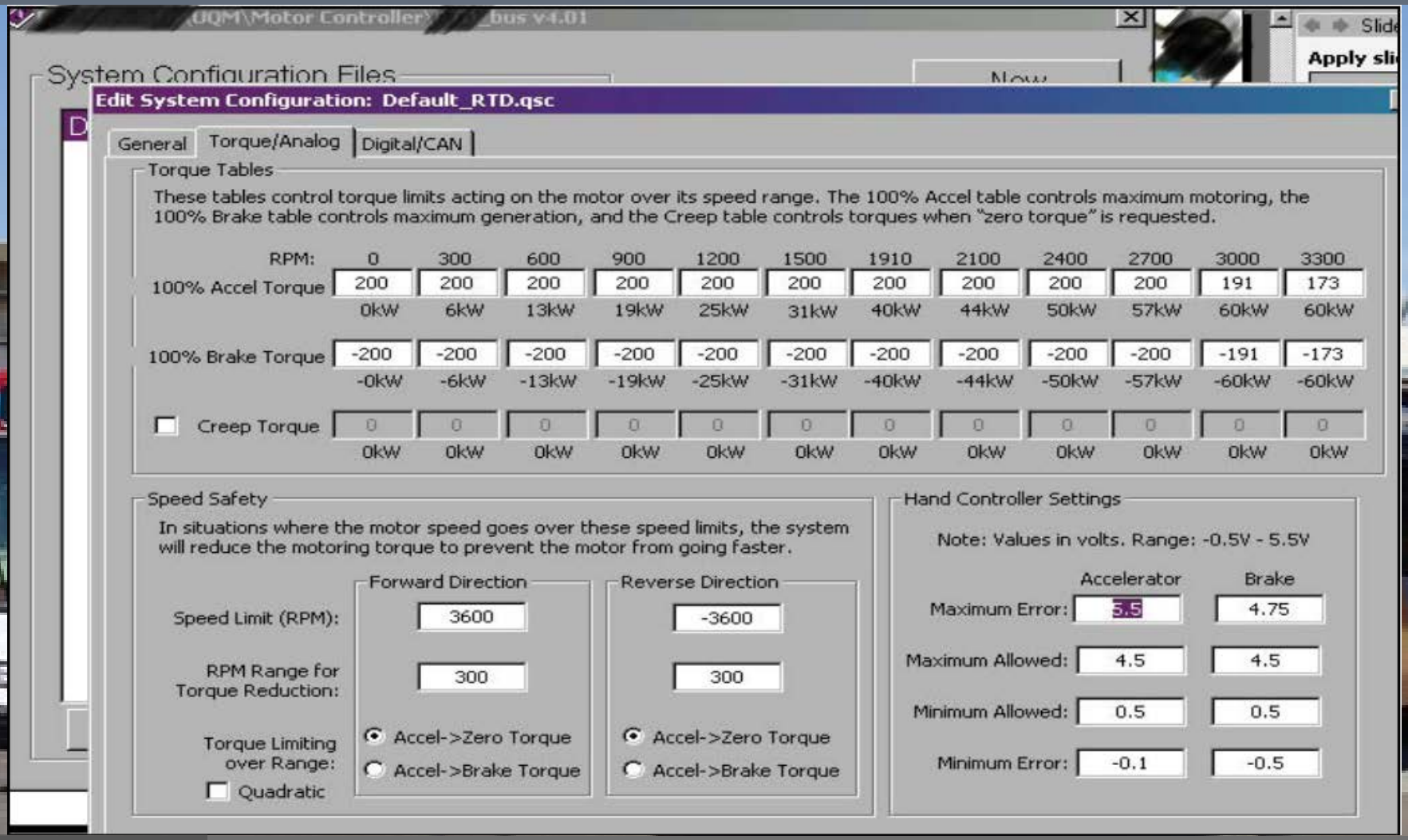
Source: Wired, The Register, eWeek, Symantec, Kaspersky Lab

Emerging Challenges – Transit

Emerging Challenges – Transit

These vulnerabilities were discussed at DEFCON. No actual incidents have been confirmed to date.

Emerging Challenges – Transit



Source: DEFCON 18

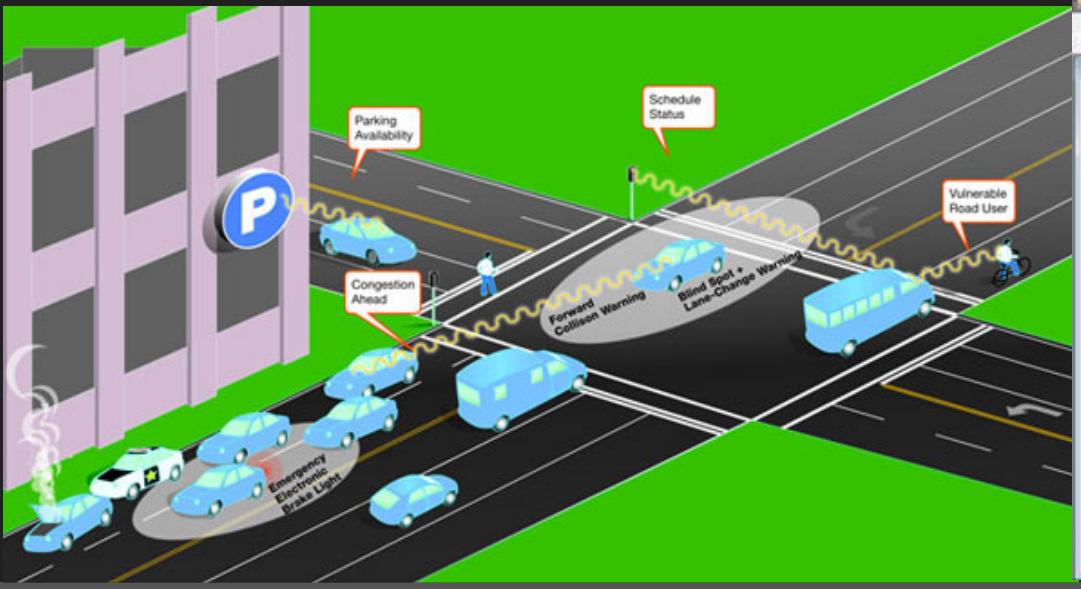
Future Challenges – Connected Vehicle

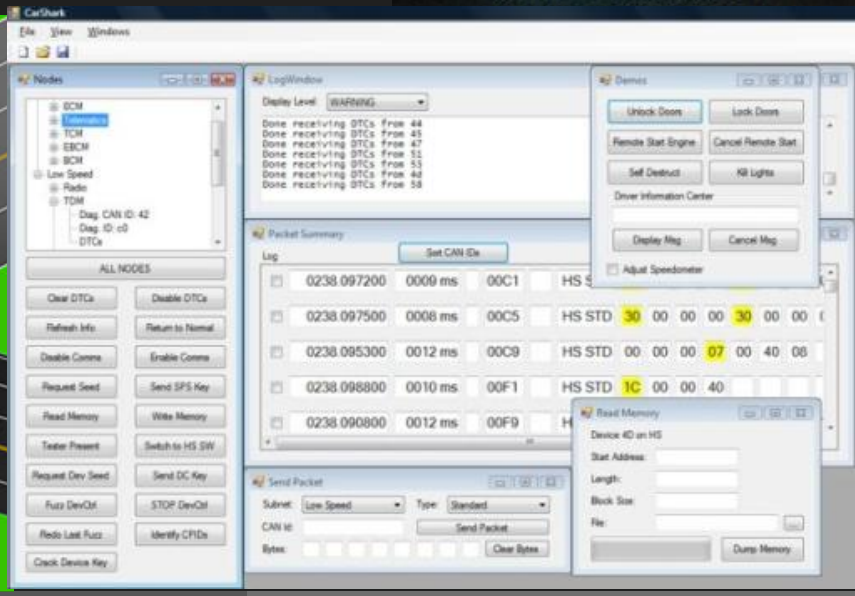
DSRC - 5.9GHz Dedicated Short Range Communication

RSE – Road Side Equipment

OBE – On Board Equipment, may connect to CANBUS/OBD

ASD – Aftermarket Safety Devices





Source - *Experimental Security Analysis of a Modern Automobile*. *2010 IEEE Symposium on Security and Privacy*

Recap

- Technical challenge and obscurity can no longer be considered a deterrent
- Anything with an operating system should be Hardened
- Keep all back up current
- The network is as vulnerable as the weakest link…and that includes the all of us the system users/vendors/operator/owners.

Information Resources

- Federal Desktop Core Configuration
  - http://fdcc.nist.gov
- Computer Emergency Response Team (CERT)
  - Very good source on Insider Threat and Prevention
- Microsoft Technet
  - Windows Vista Security Guide
  - Windows XP Security Guide
  - http://technet.microsoft.com
- ISO/IEC 27000
- Book: "Standard of Good Practice" – Information Security Forum

Computer Security references:

- National Institute of Standards and Technology
  - http://csrc.nist.gov/index.html
- SANS Institute
  - http://www.sans.org
- National Vulnerability Database
  - http://nvd.nist.gov

Antivirus Reviews

- http://av-comparatives.org/

Warning Centers

- Computer Emergency Response Team (CERT)
  - http://www.cert.org/
- Internet Storm Center
  - http://isc.sans.org/