

# **Physical Security of Advanced Network and Systems Infrastructure**

Joe St Sauver, Ph.D.

(joe@uoregon.edu or joe@internet2.edu)

Internet2 Nationwide Security Programs Manager

Spring 2011 Internet2 Members Meeting

4:30-5:30 PM, Tuesday, April 19<sup>th</sup>, 2011

<http://pages.uoregon.edu/joe/phys-sec-i2mm/>

Disclaimer: all opinions expressed are those of the author

# **I. Introduction**

# Do IT Security People Care About Physical Security?

- If you're involved with IT system and network security, it's comparatively common to see security people continually worried about "online" security threats, paying relatively little attention to the physical security of systems and networks. Why?
- One factor may be that we all know the "whole world" can attack our systems and networks online via the Internet, while (in general) attackers need to be locally present to exploit physical security vulnerabilities. As a result, we continually see attacks from online sources, but if we're lucky, we may never have personally experienced a physical attack on IT systems and network resources.
- We may also (incorrectly) view physical security as something that's "someone else's problem" – for example, isn't the physical security of our systems and networks something that the campus police department will take care of? (Maybe, maybe not)

# Understanding The Physical Security Risk Model

## *What Might Happen?*

- Damage from a natural disaster, such as an earthquake or flood
- Accidental damage (e.g., backhoe fade on poorly marked fiber)
- Intentional vandalism (or complete destruction) of facilities
- Theft of hardware (servers, routers, core switches, etc.)
- Loss of system or network integrity (potentially with unauthorized disclosure of PII or other sensitive data)

# Understanding The Physical Security Risk Model

## *Who Might Do It?*

- Act of God
- Random individual (in the accidental case)
- Disgruntled insider (or former employee)
- Financially-motivated criminals
- (Maybe) ideologically-motivated actors (“terrorists”)
- (Or even) state-sponsored professionals (“spies”)

# A Couple of Headlines

- **“California Telecom Knocked-Out By Low-Tech Saboteur”**

**April 11<sup>th</sup>, 2009, <http://tinyurl.com/datfv3>**

Shortly before 1:30 a.m. on Thursday morning, four fiber-optic cables were severed in an underground vault along Monterey Highway in San Jose, Cal. About two hours later, another four were cut in San Carlos, followed by two more in San Jose shortly thereafter.

- **“Masked thieves storm into Chicago colocation (again!)”**

**November 2<sup>nd</sup>, 2007, <http://tinyurl.com/2pn32z>**

The recent armed robbery of a Chicago-based co-location facility has customers hopping mad after learning it was at least the fourth forced intrusion in two years. [...] In the most recent incident, "at least two masked intruders entered the suite after cutting into the reinforced walls with a power saw," according to a letter C I Host officials sent customers. "During the robbery, C I Host's night manager was repeatedly tazered and struck with a blunt instrument. After violently attacking the manager, the intruders stole equipment belonging to C I Host and its customers." At least 20 data servers were stolen [...]

**Fiber Runs Cross Bridges;  
Bridges Sometimes Fall Down:  
The I-35 Bridge, St Paul MN, August 1<sup>st</sup>, 2007**



Video: [http://www.youtube.com/watch?v=EKLjB\\_nq76c](http://www.youtube.com/watch?v=EKLjB_nq76c)

# **Fiber Runs Often Pass Through Tunnels; Tunnels Sometime Burn: The Howard St Tunnel Fire, Baltimore, July 18<sup>th</sup>, 2001**



Image: [www.baltimoresun.com/features/bal-trainfiregallery,0,1855948.photogallery](http://www.baltimoresun.com/features/bal-trainfiregallery,0,1855948.photogallery)

See also section 3.4.1 of [http://ntl.bts.gov/lib/jpodocs/repts\\_te/13754.html](http://ntl.bts.gov/lib/jpodocs/repts_te/13754.html)



# Tunnels Like The Howard Street One Can Be Key Physical Security Choke Points

A Silicon Valley company that tracks Internet traffic said Wednesday's train accident caused the worst congestion in cyberspace in the three years that it has monitored such data.

The link through Baltimore "is basically the I-95 of Internet traffic into and out of Washington," said Bill Jones, director of public services for Keynote Systems Inc. of San Mateo, Calif. This week's accident caused more disruption than an incident last winter when an act of sabotage against Microsoft Corp. tied up networks, he said.

The company, which monitors Internet flow by the hour on its Web site, said that the accident had almost no impact in some areas, including parts of Baltimore, while certain connections were 10 times slower than normal, such as the ones between Washington, D.C., and San Diego.

"There was a ripple effect around the country with corporate networks due to this Baltimore disaster," said Frank Stanton, an executive with Lexent Inc., a New York-based company that repaired fiber-optic cable after the World Trade Center bombing in 1993. "Everybody thinks they have redundancy, but these type incidents show people there are huge issues. When you cross rivers and bridges, these choke points are the Achilles' heel."

Source: [http://articles.baltimoresun.com/2001-07-21/news/0107210195\\_1\\_fiber-pratt-st-internet-traffic](http://articles.baltimoresun.com/2001-07-21/news/0107210195_1_fiber-pratt-st-internet-traffic)

# A More Recent Physical Security Incident: ECMC

## Incident Recap

- Physical theft of two 200-lb safes from a locked room in our secured headquarters.
- Safes included DVDs containing PII data on 3.3 million student loan borrowers.
- Data recovered within 36 hours (although ECMC was not notified for nearly 1 month).
- Significant cost.
- Significant impact.

[www.ifap.ed.gov/presentations/attachments/50DontBeTomorrowsHeadlinesV1.ppt](http://www.ifap.ed.gov/presentations/attachments/50DontBeTomorrowsHeadlinesV1.ppt)

(Reportedly, the stolen safes were small consumer-sized units, and were wheeled out on rolling office chairs...)

# **This is Not Just a Domestic Problem**

- **“BT Mayfair phone exchange raided by network hardware thieves leaving customers cut off”, September 12<sup>th</sup>, 2008, <http://tinyurl.com/46mfsmf>**  
Thieves have broken into a BT phone exchange in London's plush Mayfair and stolen an estimated £2m worth of communications equipment. The theft led to BT business customers and home users in the area being cut off from their phone and broadband internet services. [...] They ripped out servers, routers and network cards, which can all fetch a high price on the black market.
- **‘Mysterious "Spy" Computer In [Iceland's] Parliament Works Differently Than Being Reported, Tech Expert Says,’ January 20<sup>th</sup>, 2011, <http://tinyurl.com/6ja62rq>**  
An unmarked computer found in a spare room of [Iceland's] parliament, and connected directly to parliament's internet system, was most certainly planted there [...] Any identifying serial numbers had been erased from the machine, nor were any fingerprints found, and its origins have not yet been traced. The police believed that the matter was the work of professionals.

# Suboceanic Cable Outages



---

## New cable cut compounds net woes

**A submarine cable in the Middle East has been snapped, adding to global net problems caused by breaks in two lines under the Mediterranean on Wednesday.**

The Falcon cable, owned by a firm which operates another damaged cable, led to a "critical" telecom breakdown, according to one local official.

The cause of the latest break has not been confirmed but a repair ship has been deployed, said owner Flag Telecom.

The earlier break disrupted service in Egypt, the Middle East and India.

"The situation is critical for us in terms of congestion," Omar Sultan, chief executive of Dubai's ISP DU, told The Associated Press, following the most recent break.

Wednesday's incident caused disruption to 70% of the nationwide internet network in Egypt on Wednesday, while India suffered up to 60% disruption.

<http://news.bbc.co.uk/2/hi/7222536.stm> , October 4th, 2008

# How Does This All Relate to BTOP/US-UCAN?

- The new BTOP US-UCAN network will serve a broader and potentially more sensitive mix of customers than the classic Abilene network or the current Internet2 Network.
- Quoting from the “Notice of Funds Availability” (NOFA) for BTOP Round 2, <http://tinyurl.com/yc5m7d5> at page 3797,

*“Community anchor institutions [“CAIs”] means schools, libraries, **medical and healthcare providers, public safety entities**, community colleges and other institutions of higher education, and other community support organizations and agencies that provide outreach, access, equipment, and support services to facilitate greater use of broadband service by **vulnerable populations**, including low-income, the unemployed, and the aged.”*

# IF Your Customers Include Health Care Facilities or Public Safety, Security Becomes More Important

- For example, natural disasters often can cause network outages. If you're servicing local health care facilities or public safety entities via that down network, local residents who are also affected by that natural disaster may no longer be able to reach emergency responders because of that network outage. **Thus, the US-UCAN backbone, and the aggregation networks connecting CAIs to it, may effectively become "life/safety critical" systems.**
- Similarly, health-related information and law-enforcement information running over the network may be quite sensitive. Presumably that information would always be protected by strong end-to-end encryption, but given the reality that even access to encrypted traffic can still potentially result in undesirable information disclosure (as a result of traffic analysis, etc.), well, everyone may need to be just a little more careful.

## Other Factors

- The BTOP program will result in a substantial amount of new physical facilities (fiber, colo space, network gear, servers, etc.); all those new assets that will also need physical protection.
- The US-UCAN network will be running at very high speeds, and very high speed gear tends to be very expensive. Very expensive assets deserve top notch physical protection.
- The BTOP program will service some difficult/tricky rural locations. That increases the likelihood that it may be hard to at least initially deploy a fully-redundant network architecture
- Federal oversight/review is a given, and the Federal Information Security Management Act (FISMA), includes a variety of physical security-related controls (see PE1-PE19, Appendix F, NIST Special Publication 800-53 Rev 3, <http://tinyurl.com/6awxb8d> ). Even if US-UCAN isn't technically subject to FISMA, federal agencies may still bring a "FISMA perspective" to any security review they do.

# Physical Security Areas From FISMA: PE1-PE19

- PE1 Physical and Environmental Protection Policy and Procedures
- PE2 Physical Access Authorizations
- PE3 Physical Access Control
- PE4 Access Control For Transmission Medium
- PE5 Access Control for Output Devices
- PE6 Monitoring Physical Access
- PE7 Visitor Control
- PE8 Access Records
- PE9 Power Equipment and Power Cabling
- PE10 Emergency Shutoff
- PE11 Emergency Power
- PE12 Emergency Lighting
- PE13 Fire Protection
- PE14 Temperature and Humidity Controls
- PE15 Water Damage Protection
- PE16 Delivery and Removal
- PE17 Alternate Work Site
- PE18 Location of Information System Components
- PE19 Information Leakage



# Why Should The Folks Here Today Care About This?

- A chain is only as strong as its weakest link (a cliché, but true).
- US-UCAN will likely be built in a way that's quite similar to how the Internet2 network was built: to ensure scalability, the backbone will likely rely on regional aggregators to provide connectivity to individual community anchor institutions [CAIs].
- Therefore, for the system *\*as a whole\** to be secure, we need:
  - the US-UCAN backbone to be secure, AND
  - the links between the backbone and regional aggregators to also be secure, AND
  - the links between the regional aggregators and the CAIs to also be secure.
- **Securing the network will thus require the participation and cooperation of regional aggregators. Many of those regional aggregators are present here in the audience today.**
- So what physical security vulnerabilities should you worry about?

## **II. Physical Security Vulnerabilities**

## 0) You Can't Worry About “Everything...”

- In the real world, we all have to “make our numbers,” and that usually means prioritizing and only spending money on security measures when it is necessary and cost effective for us to do so.
- **The risks that you or I perceive may be different than the risks that someone else sees under different circumstances.**
- For example, a military unit in the Mideast or Southern Asia might devote considerable attention to protecting facilities from attack by vehicle borne improvised explosive devices (VBIEDs).
- VBIEDs are generally considered to be a top military threat, particularly after the attack on the Marine Barracks in Beirut in 1983, and the Khobar Towers bombing in Saudi Arabia in 1996.

# Khobar Towers, Saudi Arabia

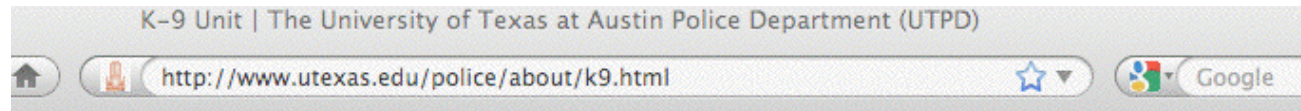


## But This Isn't The Mideast, Right?

- Here in the United States, higher education might largely discount VBIEDs as a threat, choosing to accept that risk rather than making investments in anti-VBIED technologies such as physical standoff zones, blast resistant glazing, vehicle inspection stations, etc.
- Bomb \*threats,\* however, can be quite common on campus – and quite disruptive. A growing number of campus police departments have decided to deploy local K-9 units to help clear buildings in response to campus bomb threats they may receive.
- These dogs and their handlers should be good friends with your campus system and networking staff, and routinely invited to walk/sweep campus data centers, labs, steam tunnels, etc.



# University of Texas Police Department K-9 Unit



## K-9 Unit

The K-9 Unit was created as a proactive measure to ensure the safety of students, faculty, staff and visitors to campus. Since September 11, 2001, UT Administrators have tried to provide for better public safety by changing procedures concerning how large gatherings are handled. The university felt that an explosive-detecting dog would be a valuable addition to the security of the campus since we are a venue for many large sporting events, concerts and other public gatherings.

The K-9 Unit enables UTPD to sweep for explosives before events begin and will help provide the public with a little more peace of mind.

Each canine and their handler completed five weeks of training at [Global Training Academy](#), a world recognized K-9 training facility in Somerset, Texas. Spike and Maatje are certified in explosive recognition and patrol.

### Officer Taylor and Spike



In February 2010, UTPD welcomed Spike to the department. Officer Jason Taylor serves as Spike's handler.

### Sgt. Stock and Maatje



In January 2005, UTPD welcomed its second canine, Maatje. Sgt. Robert Stock serves as Maatje's handler and joined UTPD in 2001.

# University of Wisconsin Police Department K-9 Unit

//www.uwpd.wisc.edu/field-services-k9-unit.htm



Google

## UWPD K-9 Unit

The University of Wisconsin Madison Police Department K-9 Unit started in May, 2002 by the efforts of K-9 Unit Coordinator Lieutenant Jason Whitney, management and the University Community. The Unit began with Czech Republic born German shepherd, Mosely. Mosely was trained in explosive detection and suspect tracking and worked with Special Events Lieutenant K-9 handler, Whitney. It is with respect that UW-Madison Police Department announced the death of Officer Mosely on March 3rd, 2010.



In October, 2003 the K-9 Unit expanded, adding a second Czech Republic born German shepherd, Rex. K-9 Rex is also trained in explosive detection and tracking and works 1st Shift Detective Bureau with his K-9 handler, Detective Shane Driscoll. Both Rex and Mosely had been trained with their handlers at Vohne Liche Kennels in Denver, Indiana. There are currently only three explosive detection K-9s in Dane county, two of them right here at UW-Madison PD.

The explosive detection K-9s respond to a variety of calls for service. The K-9s respond to bomb threats, suspicious packages and tracking suspects. The explosive K-9s can most frequently be seen prior to and during Badger sporting events. The K-9s also provide dignitary protection and clearing for other special events on campus and around the state. The explosive K-9s are available upon request statewide by law enforcement agencies for explosive detection and tracking.

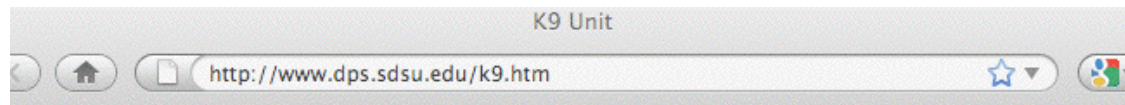


March 2007 brought another expansion to the Department's K-9 Unit. Born, raised and trained in Madison, WI, Casey is a Dutch Shepherd trained and certified in narcotics detection, agility and evidence recovery. K-9 Casey works 2nd shift patrol with her handler, Police Officer Cherise Caradine. K-9 Casey was trained by Madison Police Department Sergeant Christine Boyd, who coordinates and leads the Madison K-9 Unit and handled K-9 Arno

(1998-2006)



# San Diego State Police Department K-9 Unit



The goal of the SDSU Police K-9 program is to enhance the effectiveness of our police officers in searching for and apprehending violent criminals, locating evidence, narcotics and explosive devices. SDSU's K-9 teams train with other agencies within San Diego County and provide K-9 support to local, state and federal law enforcement agencies.

*Nemo* and *Brico* also provide an important community outreach function as the K-9 teams demonstrate their professionalism to community groups throughout the year.

The SDSU Police Department is grateful to both the SDSU Aztec Parent's Foundation and the San Diego Police Foundation for funding and helping expand the size and capabilities of the police department's K-9 Unit.

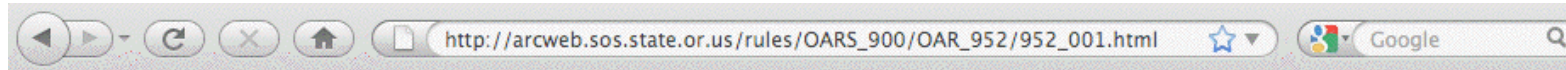




# 1) Fiber Cuts

- Regardless of how skeptical we may be of other physical security threats, one **very real** threat that I think we're all willing to acknowledge is that backhoes and other heavy equipment have an uncanny ability to find and accidentally cut buried fiber.
- You can help minimize the risk of unintentional damage to buried fiber by taking appropriate steps, including insuring that:
  - all buried facilities are well-documented as actually constructed
  - easily visible "buried cable" posts or signs are installed where appropriate or required
  - you (or your service agent) subscribe to your state's call-before-you-dig one-call utility notification center, insuring that you make timely response to all relevant locate-and-mark requests
  - any non-conductive/otherwise hard to locate facilities should be buried with a tracer wire or conductive marking tape (this may be a legal requirement in some states, e.g., OAR 952-001-0070)

# OAR 952-001-0070



## **Operators to Mark Underground Facilities or Notify Excavator that None Exist**

(1) Except as provided in section (3) of the rule, within two business days (48 hours) after the excavator notifies the Oregon Utility Notification Center of a proposed excavation, the operator or its designated agent shall:

(a) Mark with reasonable accuracy all of its locatable underground facilities within the area of proposed excavation. All marks shall indicate the name, initials or logo of the operator of the underground facilities, and the width of the facility if it is greater than two (2) inches;

(b) Provide marks to the excavator of the unlocatable underground facilities in the area of proposed excavation, using the best information available including as-constructed drawings or other facility records that are maintained by the facility operator; or

(c) Notify the excavator that the operator does not have any underground facilities in the area of the proposed excavation. Acceptable notifications must include locate request call back information and if done using an AVR (Automatic Voice Response) must have a repeat option and call back number to hear the information again.

(2) Operators of abandoned facilities shall mark said facilities to the standards of locatable facilities or unlocatable facilities.

(3) An operator shall mark any abandoned underground facility that is known to it with a capital letter "A" inside of a circle, using the appropriate operator color and identification.

(4) An operator of any out-of-service underground facility shall mark such facility in the same way it marks an underground facility that is in service.

(5) If an excavator uses offset marking, the excavator shall correctly measure the amount of offset, so that the excavator can reestablish the location of underground facilities where originally marked.

(6) If the excavator notifies the operator of underground facilities discovered during an excavation in response to an emergency, the operator of underground facilities shall comply with section (1) of this rule as soon as possible.

(7) Underground facilities shall be marked in accordance with the following designated color code:

(a) RED — Electric power lines, cables or conduit, and lighting cables.

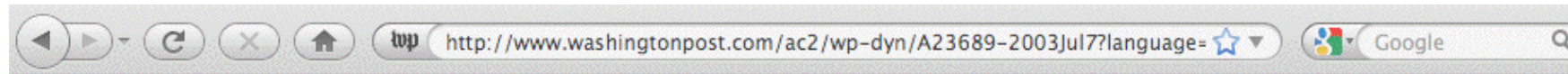
(b) YELLOW — Gas, oil, steam, petroleum, or other hazardous liquid or gaseous materials.

(c) ORANGE — Communications, cable TV, alarm or signal lines, cables or conduits.

# The Downside of Transparency

- At the same time we recognize and accept the need to be transparent about where fiber is located in an effort to avoid the problem of accidental fiber cuts, potential bad guys might also be interested in our fiber deployments. For example:
  - Are there critical choke points, such as bridges across major rivers or tunnels through large mountain ranges, where virtually all fiber follows a common path out of necessity?
  - Are there unmonitored access points (manholes, hand holes, fiber pedestals, etc.) where an attacker might be able to gain access to your fiber without being detected?
- Obviously you need to balance the need to provide enough information to avoid accidents, while simultaneously avoiding giving your enemies a “blueprint” for how to best attack you.

# Remember Sean Gorman's Dissertation?



washingtonpost.com

Advertisement

## Dissertation Could Be Security Threat

Student's Maps Illustrate Concerns About Public Information

By Laura Blumenfeld  
Washington Post Staff Writer  
Tuesday, July 8, 2003; Page A01

Sean Gorman's professor called his dissertation "tedious and unimportant." Gorman didn't talk about it when he went on dates because "it was so boring they'd start staring up at the ceiling." But since the Sept. 11, 2001, attacks, Gorman's work has become so compelling that companies want to seize it, government officials want to suppress it, and al Qaeda operatives -- if they could get their hands on it -- would find a terrorist treasure map.

Tinkering on a laptop, wearing a rumpled T-shirt and a soul patch goatee, this George Mason University graduate student has mapped every business and industrial sector in the American economy, layering on top the fiber-optic network that connects them.

He can click on a bank in Manhattan and see who has communication lines running into it and where. He can zoom in on Baltimore and find the choke point for trucking warehouses. He can drill into a cable trench between Kansas and Colorado and determine how to create the most havoc with a hedge clipper. Using mathematical formulas, he probes for critical links, trying to answer the question: "If I were Osama bin Laden, where would I want to attack?" In the background, he plays the Beastie Boys.

For this, Gorman has become part of an expanding field of researchers whose work is coming under scrutiny for national security reasons. His story illustrates new angles in the old tension between an open society and a secure society.

# Fiber Maps Are Still Widely Available...


Metro Fiber Maps: DC Metro Area, MD, DE | Telecom Ramblings

http://www.telecomramblings.com/metro-fiber-maps/dc-metro-area-md-

## Metro Fiber Maps: DC Metro Area, MD, DE

1 Comment [Tweet](#) 0

A collection of metro fiber maps for the Maryland, Delaware, and Washington DC metro area, including the major hubs in northern Virginia. Other Virginia metro areas will be found on the Virginia and the Carolinas page, a geographical division that seems to make more sense than the alternative.



Or, select a different region to view

Company	Maps	Lit/Dark	Comments
24/7 Fiber Network	<a href="#">Baltimore, Delmarva Peninsula</a>	dark	
Abovenet	<a href="#">Washington DC</a> , <a href="#">Northern Virginia</a> , <a href="#">Baltimore CBD</a> , <a href="#">Baltimore Metro</a> , <a href="#">Wilmington DE</a>	both	PDFs
Fibergate	<a href="#">DC Metro Area</a>	dark	Detailed fiber maps for many communities from this page
Fiberlight	<a href="#">Ashburn</a> , <a href="#">Culpeper VA</a> , <a href="#">DC Metro</a> , <a href="#">Herndon</a> , <a href="#">Baltimore</a>	both	PDFs and Interactive mapping
Fibertech	<a href="#">Montgomery County MD</a> , <a href="#">Wilmington DE</a>	both	Registration required
Intellifiber	<a href="#">DC Metro</a> , <a href="#">Baltimore</a> , <a href="#">Wilmington</a>	both	Google Earth format

# Architecting and Building for High Availability



- One way you can improve the physical security of your network is by adding redundancy, excess capacity, and resiliency to it.
- Your network should be architected and constructed so that there are no choke points or “single points of failure” -- loss of any single link or piece of gear should NOT result in an outage! Think, “We must always have redundant paths over diverse facilities!”
- Moreover, you must also have enough spare capacity on failover links so that if you do end up needing to actually use them, they won’t be congested (or you need a plan to selectively shed load until you’ve eliminated congestion).

# Obtaining High Availability Isn't Free

- Of course, the downside of all this is that high availability comes at a cost (as the saying goes, “you can get whatever level of availability you can afford to buy”).
- If you're building out fiber paths, the first path between two paths normally goes via the cheapest and most direct route. A diverse path (virtually by definition) will need to go via some longer/less desirable/more expensive-to-provision path.
- You also need to accept that you'll be buying capacity that you normally won't be using. (If you do end up relying on use of your “backup” link to have enough capacity to accommodate your production traffic requirement, what will you do if your primary link goes down? Each link should be able to **independently** carry all the traffic at your site)
- High availability also means that you'll need more hardware (e.g., at a minimum, more network interfaces for your routers, etc.)

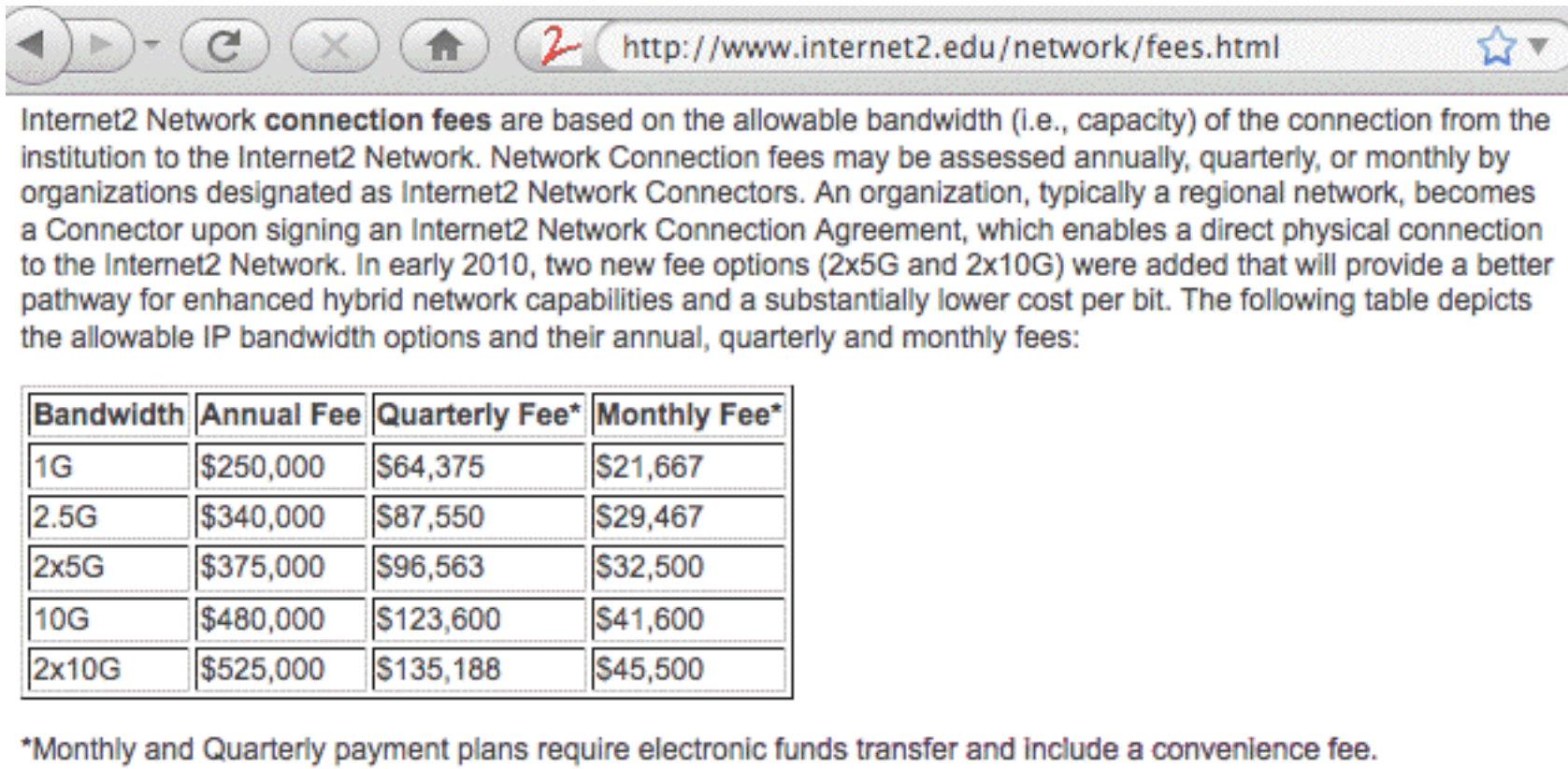


# All That Said, Many Internet2 Connectors Do Have Multiple Connections To Internet2

Internet2 IP Network	
 <a href="http://www.internet2.edu/network/ip/">http://www.internet2.edu/network/ip/</a> 	
Connector	Capacity
3ROX/Drexel	2x5G
CENIC	2x10G
CIC OmniPoP	2x10G
FLR/SoX	2x10G
GPN (Great Plains Network)	2x10G
Indiana GigaPoP	10G
KyRON	10G
LEARN (Lonestar Education and Research Network)	2x10G
LONI (Louisiana Optical Network Initiative)	10G
MAGPI	2x5G
MAX (Mid-Atlantic Crossroads)	2x5G
MCNC/SC Gigapop	2x10G
Merit Network, Inc.	2x10G
MREN (Metropolitan Research and Education Network)	10G
NOX (The Northern Crossroads)	2x10G
NYSERNet, Inc.	2x5G
Oregon Gigapop	2x5G
Pacific Northwest GigaPoP	10G
University of Memphis	10G
Utah/Montana	2x10G
Updated 12/31/10 – Next scheduled update 03/31/11	



# The Incremental Port Charge to Go From 1xN to 2xN On Internet2 Is Relatively Small



Internet2 Network **connection fees** are based on the allowable bandwidth (i.e., capacity) of the connection from the institution to the Internet2 Network. Network Connection fees may be assessed annually, quarterly, or monthly by organizations designated as Internet2 Network Connectors. An organization, typically a regional network, becomes a Connector upon signing an Internet2 Network Connection Agreement, which enables a direct physical connection to the Internet2 Network. In early 2010, two new fee options (2x5G and 2x10G) were added that will provide a better pathway for enhanced hybrid network capabilities and a substantially lower cost per bit. The following table depicts the allowable IP bandwidth options and their annual, quarterly and monthly fees:

Bandwidth	Annual Fee	Quarterly Fee*	Monthly Fee*
1G	\$250,000	\$64,375	\$21,667
2.5G	\$340,000	\$87,550	\$29,467
2x5G	\$375,000	\$96,563	\$32,500
10G	\$480,000	\$123,600	\$41,600
2x10G	\$525,000	\$135,188	\$45,500

\*Monthly and Quarterly payment plans require electronic funds transfer and include a convenience fee.

Note: 1x2.5Gbps → 2x5Gbps for (\$375K-\$340K=) just \$35K incremental!  
1x10Gbps → 2x10Gbps for (\$525K-\$480K=) just \$45K incremental!

# Diminishing Returns

- When you're thinking about how much you want to spend to insure that your network is "always available," you need to remain cognizant of the law of diminishing returns.
- The first backup/failover circuit you add will likely provide a substantial improvement in system availability, since if your main production circuit fails, that backup circuit will save your bacon. It likely represents an excellent bit of insurance for you to buy.
- If you're really risk averse or your service must absolutely remain available, a second backup/failover circuit might allow you to avoid an outage in the rare circumstances where both your primary and your secondary circuits simultaneously experience an outage – but, that \*should\* be a vanishingly rare event.
- But what of a third or fourth or n'th backup/failover circuit? You might only need that extra circuit one time in ten million, and the cost of eliminating an event that rare may be prohibitive.

# But An Example of How Sometimes Having Multiple Redundant Paths Can Pay Off Big Time: Public Safety Communications On August 1<sup>st</sup>, 2007 in St Paul

## The ARMER System as Implemented in the Twin City Metro Area

The ARMER backbone as implemented in the Twin Cities is composed of a large regional “umbrella” subsystem and two local subsystems that are integrated to operate as one.

The regional subsystem consisting of a number of towers throughout the nine county Twin City Metro area linked together by a redundant, dual-path microwave and fiber-optic system. (Note: The southern microwave loop of the ARMER system was inoperable on August 1 as some of the equipment was being relocated to accommodate Dakota County's transition on to the ARMER system. A second redundant pathway -- a critical fiber-optic link -- was actually carried under the collapsed bridge and was severed at the time of the collapse, but due to its alternate routing configuration, another fiber link -- a third level of redundancy -- the link destroyed in the collapse presented no communications problems.)

<http://www.srb.state.mn.us/pdf/I-35W%20Final%20Report.pdf>

# Hardware Sparing

- You also want to work to ensure that if an outage does occur due to a hardware failure, you can recover from it in a timely fashion.
- For example, are you continually monitoring your network and **maintaining adequate local spares?**
- Often, particularly in smaller secondary markets, more expensive spares are not stocked locally, they're shipped in from regional depots on an as-needed expedited basis.
- When multiple customers simultaneously suffer outages and all need replacement parts at the same time, or when same day courier service is disrupted due to a disaster, a lack of local spares could get ugly.

## 2) Network Confidentiality and Fiber Taps

- As the network begins to carry potentially sensitive health care related traffic or classified traffic from public safety agencies, traffic confidentiality will become more important.
- You may want to proactively and continually monitor your network links for any brief outages (windows which might be associated with the introduction of splitters or other unauthorized network elements). At the most basic, this can be done by sending/continually monitoring an ongoing “heartbeat” signal.
- More sophisticated units (as used to protect federal classified networks such as SIPRNet and JWICS), are also available if appropriate (see <http://www.networkintegritysystems.com/> )
- You may also want to periodically characterize your deployed fiber with an OTDR (optical time-domain reflectometer) to identify any “unexpected physical anomalies” which may have “developed.” (Macro bends may be enough for data interception)

# Network Integrity Monitoring



Network Integrity Systems develops PDS products to ensure superior protection and continuous availability of SIPRNet, JWICS and other classified networks transmitting national security information.

At the foundation of the product line is the INTERCEPTOR™ Optical Network Security System, an approved Alarmed Carrier Hardened Protected Distribution System (PDS) that can be easily installed on new or existing fiber optic cable systems.

Developed specifically for Information Assurance applications, and in part with Department of Defense funding, Interceptor is fully compliant with **NSTISSI 7003** and the corresponding **implementation guidelines of the various agencies and services**. It has been deployed since 2003 within the Intelligence community and in support of numerous facilities and installations across the Department of Defense, Department of Justice, Department of Homeland Security and all branches of the United States military.

---

**INTERCEPTOR**  
Alarmed Carrier Hardened PDS

**NSTISSI 7003 COMPLIANT**

---





# Physical Security Of All Optical Networks (AON)

To provide secure and reliable AONs, various security issues should be considered including physical security and information security. Physical security prevents unauthorized access to network resources. Information security, on the other hand, prevents unauthorized access to information, and assures confidentiality and integrity of the information. Currently, most of the research efforts on AONs security are geared

22

---

towards the physical security, and a little work has been done on the information security, in particular, the cryptographic needs of AONs. Accordingly, the following sections focus on the physical security of AONs.

## 3.5.1 Physical Security

Service disruption and tapping are the two most common threats to the physical security of AONs. The most commonly used AON components including optical fiber cables, combiners, splitters, multiplexers, demultiplexers, optical amplifiers, optical transmitters (or lasers), and optical receivers are susceptible to service disruption and tapping attacks.

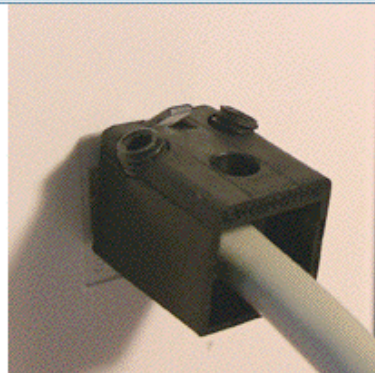
See National Communications Systems Technical Information Bulletin 00-7, "All-Optical Networks," [www.ncs.gov/library/tech\\_bulletins/2000/tib\\_00-7.pdf](http://www.ncs.gov/library/tech_bulletins/2000/tib_00-7.pdf)

# Live Open Ethernet Jacks/Ports

- It is amazing how often organizations will tolerate live open ethernet jacks/ports to which random people can plug in systems. Sometimes this even includes unlocked wiring closets, or publicly touchable routers, switches, or other network equipment.
- Most universities do not allow “free love” open wireless networks, so why would you allow anyone with an ethernet cable to have open access to your wired network? Some options to consider:
  - only heat up jacks on request, or at least disable jacks in hallways and empty offices by default
  - require authentication for most physical ethernet connections the same way you do for wireless connections
  - consider locking unused jacks and installed patch cables (e.g., see [www.rjlockdown.com](http://www.rjlockdown.com), but remember that Torx screwdriver bits are publicly available and recognize that jack plates can still be removed or patch cables cut and reterminated for access)




## The First and only Cat5 and Cat6 Jack Lock




They are sold in pairs that comes with a set of 3/32 Allen and T10 Torx set screws. Allen for low security and Torx for high security.

# \$8.99 to Defeat “Secure” Fasteners...



Click on image to zoom



## 100 Piece Security Bit Set **drillmaster**

ITEM # 91310 MANUFACTURER: DRILL MASTER

**Security bit set gives you full access to protected components**

Only: ~~\$9.99~~  
**Sale: \$8.99**

Qty:  [+ Add to Cart](#)  
[Add to Wishlist](#)

**Availability: In stock** **Shipping**

Leaves the warehouse in 1-2 business days. Economy Ground & Express Shipping available.  
(Exclusions may apply)

**Customer Rating:** ★★★★★ 11 Review(s) | [Add Your Review](#)

### Description of Drill Master 91310

This 100-piece set includes security bits that let you work with hex, hollow hex, Pozi, Torx, hollow-tip Torx, square and spline fasteners.

- Includes slotted and Phillips bits
- 1/4" hex shaft
- Rugged chrome vanadium construction
- Blow-molded case with individual compartments

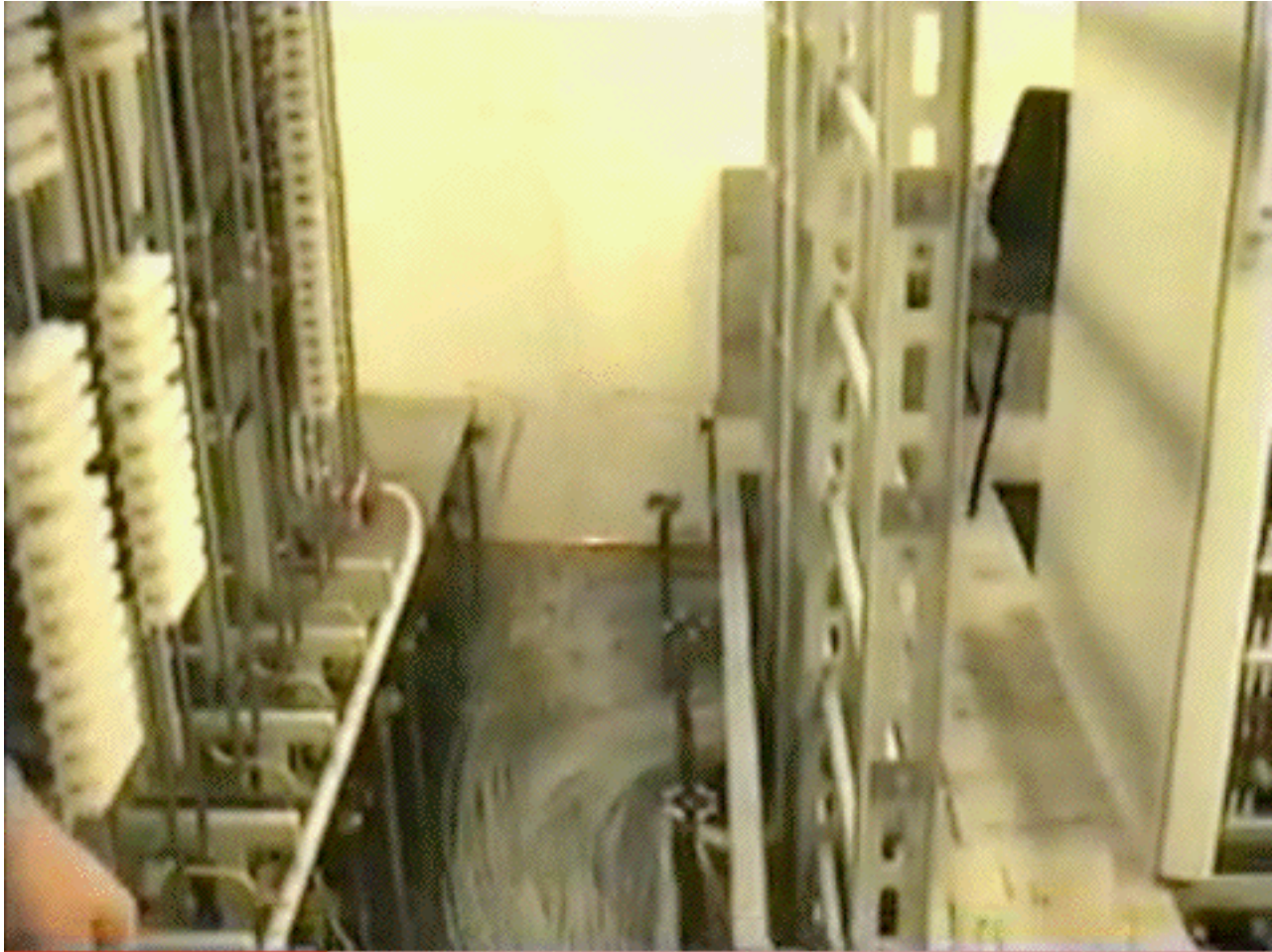
Hex end to 1/4" drive adapter, magnetic hex bit driver, hook hanging bit (Y- design), 1/4" hex to 1/4" socket drive bit and 1/4" hex wobble adapter -also includes 8 Phillips, 8 Pozi drive, 9 slotted, 4 spanner, 9 torque, 4 tri-wing, 9 hollow tip torque, 3 torque-set, 9 metric hex, 4 square, 10 SAE hex, 3 spline, 6 hollow metric hex, 6 hollow SAE hex and 3 clutch bits

### 3) The Security of Cabinets, Rooms and Buildings

- When we think about the physical security of networks, there's a temptation to think just about *the network*, e.g., the fiber and the ethernet themselves.
- In reality, every network also has numerous other physical facilities (cabinets, rooms, buildings, etc.) housing things such as key network equipment (optronics, routers, switches, etc.), as well as servers, critical staff, documentation, media, etc.
- Those facilities also need to be physically secure.
- Physical security can mean, among other things, that the facilities aren't likely to be damaged by a deluge or other natural disaster.



## A Flooded Data Center...



Video: [http://www.youtube.com/watch?v=ANU-oSE5\\_hU](http://www.youtube.com/watch?v=ANU-oSE5_hU)

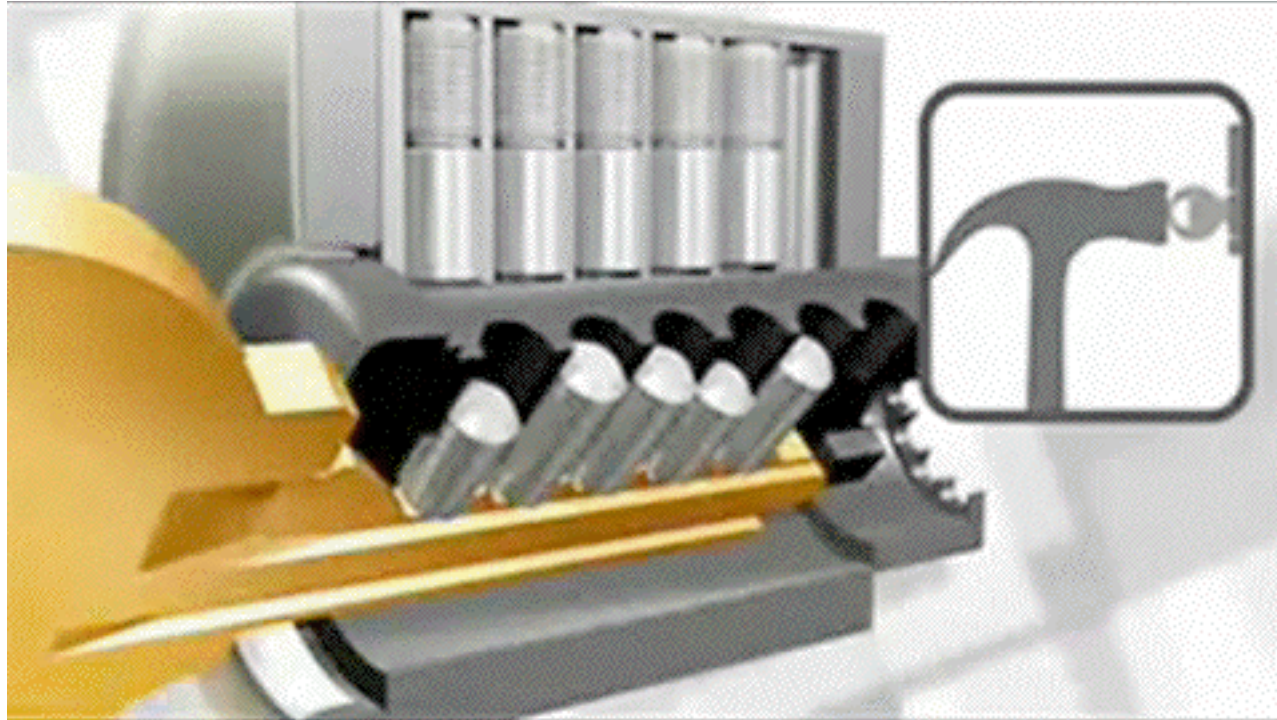
# Locks

- Once we get beyond things like protecting a site from flooding, physical security often focuses on access control via locks.
- Naturally, we all know that the locks on data equipment cabinets typically aren't very strong, and more often than not the keys for those cabinet are just left on top of the cabinet so they don't get "lost," cough, but because locks are used so many places related to computing and networking, let's talk a little about locks.

# Surreptitious Opening of Traditional Pin Tumbler Locks

- Even though traditional pin tumbler locks have well known limitations, they still form at least part of the physical security at most sites, including many computer or networking sites.
- If you think that traditional pin tumbler locks provide anything even \*remotely\* approaching reasonable security, I'd urge you to think again.
- In particular, you should learn about "bump keys."

## Video: How Lock Bumping Works



Video: <http://www.youtube.com/watch?v=7xkkS2p7SuQ>

## If Detection Isn't A Problem...

- If discovery of an intrusion isn't a problem, you should also know that many traditional locks can be drilled, pried, ground, frozen or otherwise defeated by brute force in just a matter of minutes.
- Thus, for any lock that “matters,” you should probably consult with a professional locksmith and have a high security lock (such as those made by Medeco) installed, reinforcing the door and the door jamb (including the strike plate area) at the same time.
- Don't forget to secure any exposed outward-swinging external door hinges, too!



# Hinges

[://www.statefarm.com/learning/be\\_safe/home/burglary/learning\\_besafe\\_atm\\_burg\\_hing.asp](http://www.statefarm.com/learning/be_safe/home/burglary/learning_besafe_atm_burg_hing.asp)

## Door Hinges and Home Security

### Door Hinges on Exterior Swinging Doors

Although most people don't give a second thought to the security options available in door hinges, there are door hinges available that can provide better security.

In some parts of the country, it is common to see doors swing out. When the door swings outward, the hinge pins are typically exposed on the outside of the house.

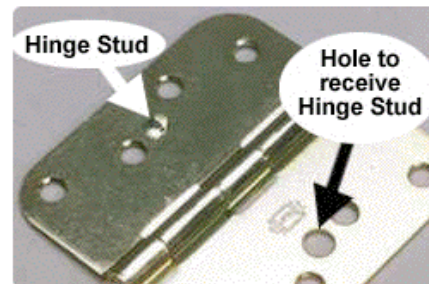
This could allow an intruder to tap the hinge pins up and out, and lift the door off its hinges, removing the door without unlocking it.

There are several door hinge designs available that make it more difficult to remove the hinge pins.



### Non-Removable Pins

On these hinges, the pins are held in place by a setscrew. If the door is in the open position, the setscrew is exposed and can be retracted, and the hinge pins removed. If the door is closed, the setscrew cannot be accessed.

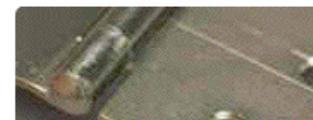


### Safety Studs

These hinges come in full mortised type only, meaning the hinge sits in routed-out insets in the door and frame. Studs extend from one hinge leaf and a hole is punched in the corresponding position on the opposite leaf. When the door is closed, the stud sits in the hole. If the hinge pin is removed, the door still cannot be taken off its hinges because the stud holds it in place.

### Fast-Riveted (Crimped) Pins

These hinges are designed so the hinge pin cannot be removed. The hinge pin is made longer than the hinge height, inserted into the hinge, and spun on the end to create a rivet-type end on the top and bottom of the pin.



# Padlocks

- Padlocks are widely used to secure network equipment. They are typically subject to all the issues associated with traditional pin tumbler locks, but they have additional issues of their own:
  - warded padlocks (see image at right) are trivial to open; they should **NEVER** be used
  - some padlocks are stamped with their “key code;” if you don’t remember to remove that code, it may be possible to use those numbers to create or find a key for that lock
  - the unshielded shackle of a padlock can often be cut with bolt cutters or a torch
  - even if you have a padlock that’s secure, it may be used in conjunction with a weak and easily defeated hasp or chain
- The ultimate? The Navy has approved the S&G 951 High Security Padlock, but at >\$1,000/lock, it might be, um, a little pricey



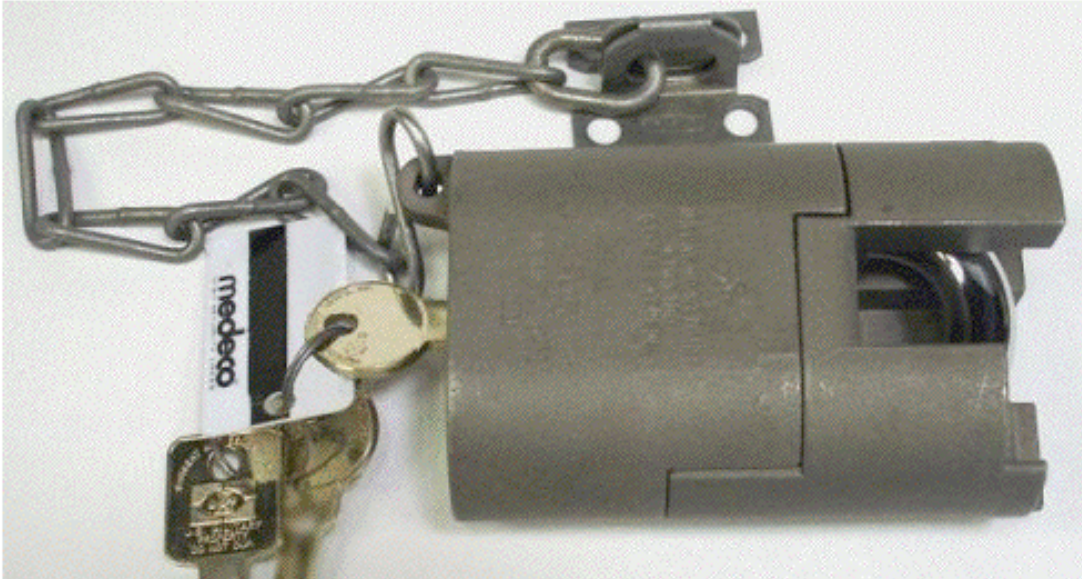
# A S&G 951 Padlock

DoD LOCK PROGRAM

http://www.dscp.dla.mil/gi/locks/

Google

## High Security Padlocks



- 5340-01-217-5068: S&G 951, Padlock, Key Operated. High Security Shrouded Shackle  
*For use by DoD personnel and active duty U.S. military **ONLY**.*
- 5340-01-449-4346: S&G 951, Padlock, Key Operated. High Security, Shrouded Shackle (with R1 key-way)  
*For use by all other Federal agencies and DoD contractors.*

(Different key-ways are intended for use by different audiences)

# Keys

- Key-related issues are another reason why traditional locks often provide mediocre security.
- In a university environment, it is routine for the same key to get issued to multiple people. When one of those keys get lost (or is not recovered when someone quits or is terminated), the locks that are opened by that key tend not to get rekeyed (typically, the cost of doing this would be prohibitive, and there are only a finite number of usable key combinations given physical constraints).
- Many sites also use master keys, allowing supervisors or custodial staff to have access to all offices on a given floor or in a particular building. If control over a master key is even temporarily lost (or an intruder can gain access to lock cylinders from multiple doors which all use the same master key), the intruder may be able to make a duplicate master and have the run of your facility.
- You really want to have a conversation with your lock & key person

# Part of A Keys Control Checklist from the USDA

## KEY CONTROL

1. Is a key-control system in effect? \_\_\_\_\_

2. Who is responsible for the key control system?

Name:

Phone#:

Email Address:

3. Are building entrance keys issued on a limited basis? \_\_\_\_\_


16

C:/USDA Checklists/USDA Physical Security Checklist

## USDA Physical Security Inspection Checklist

**DRAFT**

**YES NO**

4. Are master keys kept securely locked and issued on a strictly controlled basis?

\_\_\_\_\_

5. Can the key-control officer replace locks and keys at his discretion?

See: <http://www.usda.gov/da/physicalsecurity/physicalcheck.pdf>

# Alternatives to Locks and Keys

- Many facilities have moved to “key cards” (swipe cards, prox cards, etc.) as an alternative to traditional locks & keys
- Key cards offer distinct advantages over traditional locks and keys:
  - key cards can be integrated into user site IDs/badges
  - key card use can be tracked, while use of a key leaves no audit trail or record
  - key cards can be programmed to work only during particular days or particular periods of time, while keys work all the time
  - many key card systems can be configured to require “two factors” (e.g., you must use your key card AND enter a PIN code)
  - upon termination, a key card can be instantly canceled with no need to manually rekey the system, etc.
- Sometimes, though, key cards may offer only an illusion of security. For example, some may be easily brute forced using widely available tools.



## Some Prox Cards Tools

- Some resources mentioned in <http://www.mcafee.com/us/resources/white-papers/foundstone/wp-proxbrute.pdf>

-- Proxmark III: <http://www.proxmark3.com>

-- Proxpick: <http://www.proxpick.com/>

-- ProxClone: [http://proxclone.com/reader\\_cloner.html](http://proxclone.com/reader_cloner.html)

- Also worth a read:

“The RFID Hacking Underground,” Wired, May 2006

<http://www.wired.com/wired/archive/14.05/rfid.htm>

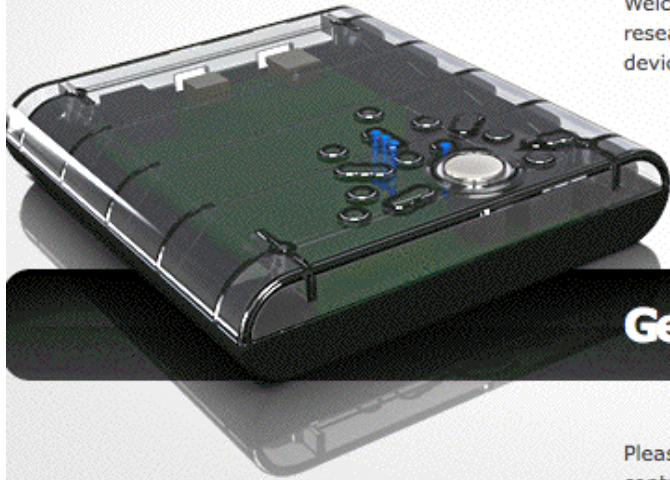
and

<http://rfidiot.org/>

# Proxmark3



Welcome to the Proxmark III online store. We offer the fastest way to get started researching RFID and Near Field Communication systems using the powerful Proxmark III device.



- Pre-programmed thoroughly tested boards
- Read & emulate any RFID tag
- Orders ship within 2 business days

**Get Yours Today!**

Please see the **FAQ** and **Terms of Sale**. Additional information can be obtained by contacting [sales@proxmark3.com](mailto:sales@proxmark3.com). This website requires that javascript be enabled to function correctly.

Enclosed Proxmark III	\$399	<a href="#">Add to Cart</a>
Naked Proxmark III - SOLD OUT	\$229	<a href="#">Add to Cart</a>
Low Frequency Antenna	\$59	<a href="#">Add to Cart</a>
High Frequency Antenna	\$59	<a href="#">Add to Cart</a>
Tag Bundle	\$12	<a href="#">Add to Cart</a>

# FWIW, Many Swipe-Style Cards Aren't Perfect Either



July 17, 2008

## After Security Breach, Harvard Unveils New IDs

### Encryption technology in new proximity ID Cards to strengthen security in FAS Buildings

By [Abby D. Phillip](#), CRIMSON STAFF WRITER

The Faculty of Arts and Sciences (FAS) announced last week that students, faculty, and staff will receive new identification cards that use contactless Smartcard technology when they return to campus this fall.

The upgrade comes less than a year after Theodore R. Pak '09 was caught creating duplicates of the Harvard University ID (HUID) cards belonging to University President Drew G. Faust, Assistant Dean of the College Paul J. McLoughlin II, and Dunster House Superintendent H. Joseph O'Connor.

Pak's hack revealed a significant security flaw in the more than 15-year-old swipe card system, as he was able to gain access to buildings and gates across campus with only knowledge of HUID numbers and a \$200 card reader bought from eBay.

Assistant Dean for Physical Resources Michael N. Lichten said that the Pak incident "was a motivator for us to move more quickly in putting the new system in place."

Prior to the Pak incident, HUID numbers were available to a number of individuals at the University including undergraduate User Assistants, Harvard University Dining Services workers, building managers, and freshman proctors. The University has since strictly restricted the access to these numbers, putting in place a number of protocols that limit how and when they can be displayed and accessed by members of the Harvard community.

The new cards are intended to bolster the security of FAS buildings by adding crucial encryption technology and more complex security procedures.

Lichten said that unlike the previous card system, which functioned directly on unencrypted HUID numbers, the new proximity cards will carry encrypted information that must match data saved by the security system on who is given access to each building.



# Biometrics

- Biometric systems use your physical characteristics to decide if you should or shouldn't be granted access to a facility or resource.
- Examples include:
  - fingerprint or hand geometry readers
  - iris and retina scanners
  - voice identification
  - facial recognition
  - signature recognition
- Nice discussion of biometric issues in GAO-03-1137T, "Challenges in Using Biometrics," <http://www.gao.gov/new.items/d031137t.pdf>
- Not a huge fan of biometric solutions.



# **Building Security:**

## **Piggy Backing/Tailgating/Social Engineering**

- Key cards or biometrics won't help if random individuals can gain access to a secure facility by piggy backing/tailgating behind an authorized user, or by manipulating basic social courtesies.
- A nice example of manipulating basic social courtesies, mentioned to me by a colleague recently: approach the door to a controlled area carrying what's obviously a heavy box. It takes a pretty heartless person to not help that person out by holding the door for them.
- Floor to ceiling turnstiles or mantraps (interlocking pairs of doors) can be used to help physically prevent these sort of phenomena.
- An attendant at the door can also ensure that everyone coming in "cards in" as may be required (but I know that this is something that many higher education sites have trouble enforcing).



## Single Entry Interlocking Door System

The TAP-100 Interlocking Door System is a fully programmable cylindrical portal which can be designed with metal detection, armored glass, and uni-directional or independent bi-directional electrical controls. The system can be integrated with any type of access control system.

### Characteristics

- Prevents piggybacking
- Small 32-1/4" diameter cylindrical portal
- Integrates with any access control system
- Optional bullet resistant glass
- Optional metal detection
- TAP-100EE: Integrated with emergency exit to allow automatic opening of curved doors and swing door simultaneously



# Building Security: Stay Behinds

- There's also the potential problem of “stay behind” visitors – if you're not continually escorting all visitors from entry to exit, or at least signing all visitors in and out, how do you know that all visitors who've \*entered\* your facility have \*left\* by the end of the day?
- An unescorted and forgotten visitor can be the “camel's nose” that defeats many of your physical access controls, potentially allowing anyone or everyone to gain access to your facilities.
- For example, a stay behind visitor can open an unalarmed external door from the inside, thereby allowing entry of additional people.
- Finding stay-behinds is easier if a building has motion sensor alarms deployed, or if the organization routinely uses security dogs to sweep sensitive buildings at closing time. Routinely lock all places where an unauthorized person might hide, out of sight, until the building empties (such as supply closets, unused offices, etc.)

# Walls, Ceilings, Floors, Roofs, Utility Tunnels, Etc.

- Sometimes you'll see a high security lock "protecting" a room with a hollow core door, externally accessible glass windows, sheetrock walls, a suspended ceiling, and maybe even a raised floor.
- In that sort of environment, an intruder can ignore the high security lock and just break the door or the window, or punch through the sheet rock walls, or climb in above the suspended ceiling or below the raised floor. (Embedded heavy gauge wire mesh can at least make that sort of through-the-wall or through-the-ceiling or floor entry more difficult)
- Similarly, have you secured your roof? Or could someone use an extension ladder to get to your roof, and then go through an unsecured roof hatch or skylight?
- What about any utility tunnels? Manholes are often one of the easiest-to-breach access points. Although locking manhole covers are available (e.g., see [www.securemanholes.com](http://www.securemanholes.com)), most manhole covers are simple cast iron units that provide no impediment to an intruder with a manhole cover lifter (or just a couple of bolts and some wire).

# Fencing

- University campuses aren't like industrial or government facilities, but if you can add a fenced perimeter around critical facilities, that fence will immediately add significantly to your site's physical security.
- Government and military folks (who do worry about things like VBIEDs) like a wire cable-reinforced perimeter fence that's ideally at least fifty feet away from the facility that's protected, built from 9 gauge (or heavier) chain link, seven feet or more tall, with an outward facing razor wire top guard plus a bottom rail, well anchored and backed up by things like interlocking precast concrete obstacles or large concrete planters.
- Dual fence designs are also popular.
- That may all be a bit much for university environments, but if you can deploy it, it's another layer of physical security.

# Exclusion Zones, Intrusion Detection & Landscaping

- Most fences (particular with proper signage) will at least serve to create a public exclusion zone in which an intruder can be readily identified and intercepted for questioning.
- Extensive lighting plus physical intrusion detection systems will help managing that exclusion zone.
- Any landscaping should not provide hiding spots for intruders.
- Any trees near or overhanging a security fence should also be trimmed or removed to prevent the tree from being used as a pathway over the fence.

## Example of a Fencing Failure

- “A fence approximately six feet high surrounds some of [the Kinshasa Nuclear Research Center] CREN-K. The fence is constructed of cement in some places and chain-link in others. The fence is not lit at night, has no razor-wire across the top, and is not monitored by video surveillance. There is also no cleared buffer zone between it and the surrounding vegetation. There are numerous holes in the fence, and large gaps where the fence was missing altogether. University of Kinshasa students frequently walk through the fence to cut across CREN-K, and subsistence farmers grow manioc on the facility next to the nuclear waste storage building. [...] No fence separates the nuclear waste storage building and the University of Kinshasa’s women’s dormitory. The two buildings sit approximately 300 meters apart, and one can walk freely from one to the other across the manioc field.”  
<http://tinyurl.com/68sgdds>

# Alarms and Guards

- Access control features such as locks and reinforced doors and walls can't keep a determined intruder out “forever” – virtually any facility can eventually be breached if the intruder has enough time and no interruptions.
- What access control features do give you is a window of time for guards to respond and deal with any intrusion attempt.
- The sooner your guards know that someone is attempting to break in, the more time they'll have to mobilize and deal with the attempted intrusion. Alarms buy you that response time.
- Again, just as was the case with locks, you should consider engaging an alarm professional to help you plan and deploy a suitable comprehensive alarm system (including things like area motion detectors, and perimeter integrity alarms with window-ajar and door-ajar sensors). You should also review response requirements with campus police and municipal law enforcement.



# Surveillance Video

- You can't be everywhere at once, so take advantage of surveillance cameras to increase your security leverage. Cameras have come way down in price, while quality has gone up (as has ease of installation). It should now be possible for you to affordably add surveillance video throughout all critical campus facilities.
- Surveillance video may deter issues from arising in the first place: if people know they're potentially being monitored, that alone may deter them from engaging in illegal activities.
- If illegal activities do occur, surveillance video can provide crucial evidence documenting what happened during the incident:  
(a) When did the incident occur? (b) How did the incident occur?  
(c) Who did it? (d) What did they take/what did they do?
- Consider using a redundant out-of-building digital video recorder to ensure that an in-building video recorder doesn't get stolen or compromised during a security incident.

## 4) Emergency Systems: Fire Detection & Suppression

- Electrical fires are one of the most destructive events an IT organization can run into, and fire suppression has become trickier since new inert gas (“Halon 1301”) installations have been banned due to ozone depletion concerns.
- Automatic water sprinkler systems (“dry pipe” systems) are the most common alternatives, but water sprinkler systems may not be effective when it comes to suppressing electrical fires occurring in machine rooms under raised floors.
- Non-Halon gaseous fire suppression systems (for example, carbon dioxide based systems) may be an alternative, but they represent serious potential risks for operators and other personnel who may need to be rapidly evacuated in the event of a fire. See the discussion of some Halon alternatives: <http://tinyurl.com/6agevle>
- Note: Regrettably, not all fires will take place in your well-fire-suppressed machine room...

# OSU's Thanksgiving 2010 Steam Tunnel Fire

- “Oregon State University resumes classes, though some phone and computer services still disabled from fire,” November 29<sup>th</sup>, 2010, <http://tinyurl.com/5sxxx3c> [emphasis added below]

Some Oregon State University buildings still had not regained telephone or computer data service Monday as the result of an electrical fire last week, but all classes resumed normally. The fire erupted early last Wednesday morning in wiring that runs through the university's steam tunnels, 6-to-8-foot-tall tunnels that run under most buildings on campus. Electrical wiring, telephone lines and **fiber optic cables** thread through the tunnels along with wrapped steam pipes that carry heat to buildings. Investigators are still trying to determine what caused an arc flash – a burst of electrically charged energy that burns at a temperature of 5,000 degrees or higher. The arc singed sections of wiring extending about a 100 feet from the flash point in three directions, said Vincent Martorello, director of facility services. The university gave its nearly 24,000 students early dismissal for the Thanksgiving break on Wednesday morning because the fire had disabled fire alarms in some buildings, Simmons said. The fire did not affect dormitories, **but it left five buildings Monday without computer data connections** and a dozen buildings without telephone service. Telephone service may not be fully restored until the end of the fall term, university officials said.



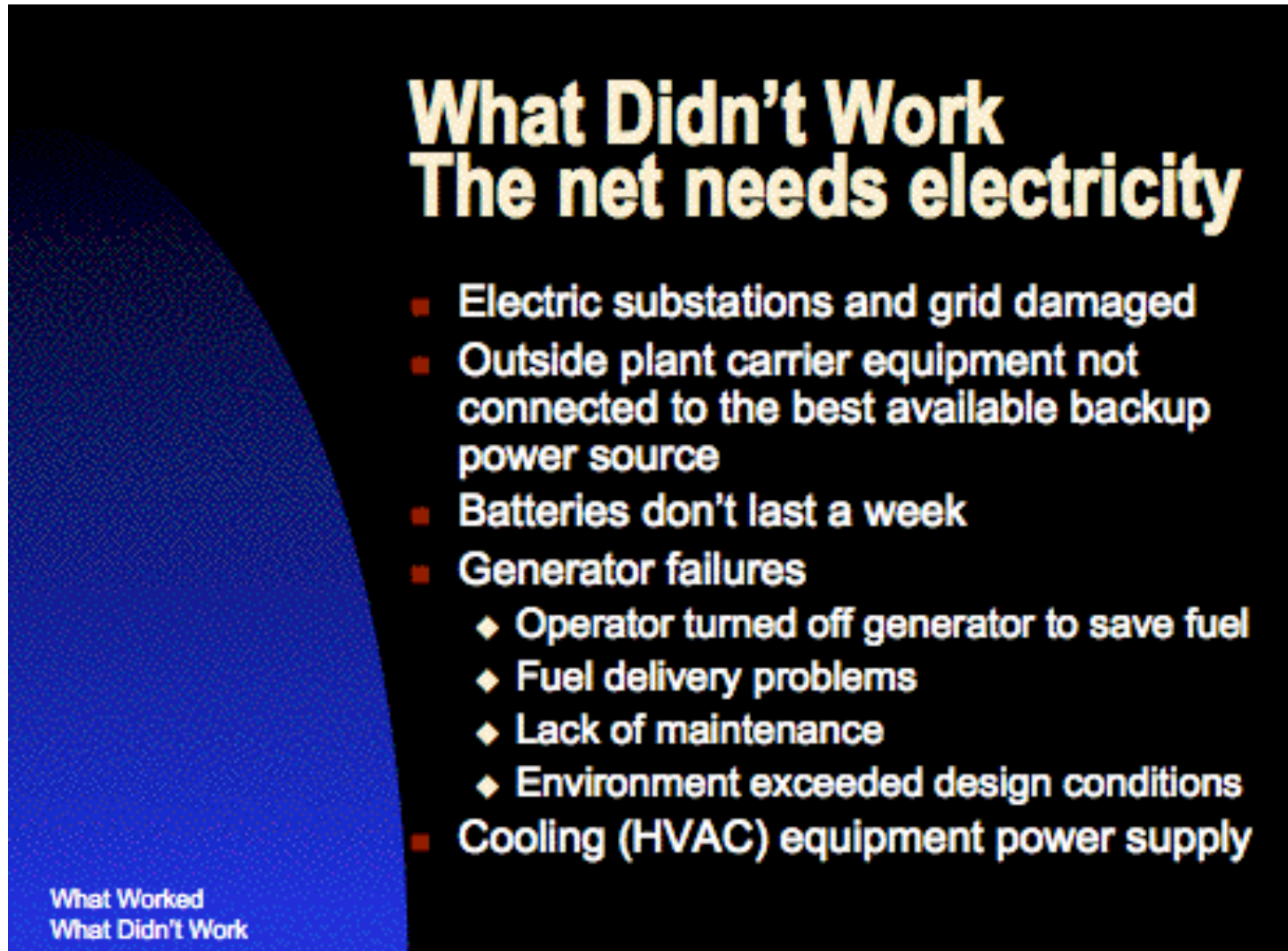
Source: <http://tinyurl.com/65mrh3w>

# Emergency Power and Cooling

- Often uninterruptible power supplies prove to be too small for the load they've been stretched to support. In those cases, even if you immediately began shutting down systems as soon as the power flipped to the UPS, you would not be able to cleanly take down all the covered equipment before running out of juice (and naturally most people don't want to begin powering things down until they're SURE that they're not facing just a brief outage). Check and figure out how long you can run with your actual load.
- UPS systems need to be backed up by diesel generators. Have you tested yours recently? How much fuel do you have available for it? In an emergency will you be able to get more? Are you sure?
- While most sites worry about emergency power, many forget to think about emergency cooling. If your machine room is going to overheat, even if you have juice, you won't be able to stay online. Spend some time thinking about your emergency cooling plan.



# An Example from 9/11



## What Didn't Work

### The net needs electricity

- Electric substations and grid damaged
- Outside plant carrier equipment not connected to the best available backup power source
- Batteries don't last a week
- Generator failures
  - ◆ Operator turned off generator to save fuel
  - ◆ Fuel delivery problems
  - ◆ Lack of maintenance
  - ◆ Environment exceeded design conditions
- Cooling (HVAC) equipment power supply

What Worked  
What Didn't Work

<http://www.nanog.org/meetings/nanog23/presentations/donelan.ppt>

# Network Operational Continuity in a Disaster

- Would your network continue to operate if your primary network operations center was hit by a major disaster, such as an earthquake?
- We can tease apart two issues here:
  - Will you have a functional NOC, post-disaster?
  - And will your remote network equipment continue to operate?
- These days, realistically speaking, you will likely want full replication of your NOC at an out-of-region location if you want to be able to continue to operate your network after a major disaster.
- That replicated NOC will need both trained and ready-to-go network engineers and NOC staff, as well as replicated servers and live current copies of all NOC databases. We recognize that this is a potentially expensive proposition, but one that we think deserves serious consideration.



# **Disaster Continuity for Remote Gear, Including Emergency Out-Of-Band Access**

- A major disaster, such as an earthquake, may also directly impact remote network equipment. Don't forget to plan for the emergency power, cooling and remote access needs of your remote networking sites (including fiber equipment huts).
- Every installation with active electronics needs, at a minimum, its own emergency power and cooling, particularly if primary power is coming from only a single utility feeder, or the utilities for a remote site are aerial rather than buried.
- It may also be worth spending some time thinking about how you will securely handle emergency out-of-band access to remote gear if in-band access gets interrupted due to a network outage.

## 5) Miscellaneous Items: Personnel Controls

- Personnel vetting and related controls are often viewed as a key part of physical security because on-site personnel enjoy unique physical access to site facilities.
- Historically universities have rarely done background checks on their employees, however, that practice has been evolving over time, particularly for system and networking staff members having effectively unlimited access to the University's infrastructure.
- As staffs are beefed up to support BTOP/US-UCAN activities, don't neglect personnel background checks in your eagerness to fill some of those hard-to-fill positions!
- Be sure to discuss any planned background checks with your Human Resources Department, since specific notice and consent requirements or other limitations may apply, and typically vary from state to state.

# ID Badges

- ID badges are another routine component of personnel security programs, and become necessary when an organization grows beyond a size where “everyone knows everyone” and “everyone knows what everyone should (or shouldn’t) be doing.”
- Ideally, ID badges would:
  - identify the person bearing the badge (“Sam Anderson”), and make it easy for third parties to verify that the right person has that badge (e.g., the picture on the badge matches its user)
  - give the person’s status (“employee”, “visitor”, etc.) and role (“senior network engineer”, “custodian”, etc.)
  - signal any atypical access (“machine room access allowed” or “must be accompanied at all times”)
  - include a magstripe or barcode that allows the credential to be easily verified against an authoritative database
  - be difficult to forge, resistant to unauthorized modifications, hard to accidentally damage, and cheap

# Credentials and A False Sense of Security

- While ID badges have the potential to improve security if properly used, sites need to be on guard against letting ID badges lull them into a false sense of security. Just because someone has an ID badge doesn't mean that they should be immune from being challenged if they're somewhere they shouldn't be, or doing something they shouldn't be doing.
- Credentials should also be challenged and verified if the person presenting them isn't known, or just "feels wrong" (trust your paranoia).
- For example, it has been reported that penetration testers have been routinely able to gain unauthorized access to sterile areas of airports and sensitive federal facilities by displaying bogus law enforcement credentials. Such access is particularly troubling when those individuals are allowed access with firearms or other weapons.

# An Example of Credential Abuse From the GAO

“Our undercover agents were 100 percent successful in penetrating 19 federal sites and 2 commercial airports. We were able to enter 18 of the 21 sites on the first attempt. The remaining 3 required a second visit before we were able to penetrate the sites.

At no time during the undercover visits were our agents’ bogus credentials or badges challenged by anyone. At the 21 sites that our undercover agents successfully penetrated, they could have carried in weapons, listening devices, explosives, chemical/biological agents, devices, and/or other such items/materials.

At each visit, our agents carried bogus badges and identification, declared themselves as armed law enforcement officers, and gained entry by avoiding screening. At least one agent always carried a valise.

Sixteen of the sites we visited contained the offices of cabinet secretaries or agency heads. At 15 of these sites, our undercover agents were able to stand immediately outside the suites of the cabinet secretary or agency head. In the 5 instances in which our agents attempted entry into such suites, they were successful. At 15 of the sites, our agents entered a rest room in the vicinity of these offices and could have left a valise containing weapons, explosives, and/or other such items/materials without being detected. Except for one agency, we made no attempt to determine whether any of the cabinet secretaries or agency heads were present at the time we visited their agencies.

At a federal courthouse, our agents were waved through a magnetometer but not screened. A briefcase that one of the agents carried was not checked. The agents were escorted to a gun box room, which they were permitted to enter alone. They were then instructed to lock their weapons, but no one supervised or observed the actual surrender of the agents’ weapons.

At the two airports we visited, our agents used tickets that had been issued in their undercover names for commercial flights. These agents declared themselves as armed law enforcement officers, displayed their spurious badges and identification, and were issued “law enforcement” boarding passes by the airline representative at the ticket counter. Our agents then presented themselves at the security checkpoints and were waved around the magnetometers. Neither the agents nor their valises were screened.”

Source: GAO/T-OSI-00-10, “Security Breaches at Federal Agencies and Airports,” May 25<sup>th</sup>, 2000, <http://ntl.bts.gov/lib/11000/11400/11410/os00010t.pdf>

## 6) “Information Leakage” (FISMA PE19)

- The final area of physical security we might consider is what FISMA PE19 calls “information leakage.”
- If we weren't talking about physical security today, when you hear the term “information leakage,” the first thoughts that would probably come to mind would probably include:
  - sniffing unencrypted network traffic
  - SQL injection attacks (potentially extracting PII or other confidential data in unanticipated ways)
  - malware (such as “banking trojans”) eavesdropping on user financial data
  - BGP route injection attacks (“BGP shunts”)
  - DNS poisoning
  - etc.

# Physical Surveillance Devices


- The physical analog to some of those network-based eavesdropping attacks would be physical surveillance devices, colloquially known as “bugs.”
- For some reason, while most people are all too willing to believe that hackers and malicious software exist and could spy on your online activity, they are often skeptical that there are physical surveillance devices that are an equal or greater threat.
- Put another way, some people think that **“physical surveillance devices are something that only the tin foil hat crowd tends to worry about. No one’s going to bother ‘bugging’ my computer or my office or my car.”**
- I’m happy that those folks are feeling so secure, but that sense of security may be unwarranted. Physical surveillance devices DO exist.



# Simple Example: A Hardware Keylogger

http://www.keycobra.com/wifi-keylogger.html

## New KeyDemon Wi-Fi Premium Keylogger <sup>new</sup>



**KeyDemon USB & PS2 Wifi Hardware Keyloggers** just released!

These **wireless wifi keylogger** is packed with state-of-the-art electronics: **two powerful processors**, a full **TCP/IP** stack, a **WLAN** transceiver, and **2 Gigabytes** of memory.

Besides standard [PS/2](#) and [USB keylogger](#) functionality, it features remote access over the Internet. This wireless keylogger will connect to a local **Wi-Fi Access Point**, and send **E-mails containing recorded keystroke data**. You can also connect to the keylogger at any time over TCP/IP and view the captured log. All this is a device less than 2 inches (5 cm) long!


### How the Wifi Keylogger work?

The main principle is very simple though: **just plug the keylogger in-between the keyboard and computer.**

**The KeyDemon Wi-Fi Premium Keylogger** incorporates a built-in WLAN transceiver and TCP/IP stack, meaning it can connect to the Internet through a Wi-Fi Access Point. To do that, you must provide it some basic data, such as the Network ID and password (just like any WLAN device).

Once connected to an Access Point, the keylogger will start sending E-mail reports with captured keystroke data to any recipient E-mail address you supply. This means you can keep track of what's happening on the monitored computer from any place throughout the world, just by checking your mailbox!

### New WiFi Keylogger




**USB Version**  
**Now Only \$179.95!**  
**(limited time only)**

[Buy Now](#)

30 Day Money Back  
Guarantee!

Invisible Keylogger Pro  
Software included FREE!



# Some More Hardware Logging Gear

<http://www.keelog.com/> Google

## KeyDemon Wi-Fi Premium



The world's first hardware keylogger with **built-in Wireless LAN** support! This keylogger connects to the Internet through an Access Point, and sends **captured keyboard data as E-mails**. With this **Wi-Fi hardware keylogger**, you can silently monitor a computer from anywhere in the world, just by checking your mailbox! Ultra stealthy, undetectable for software. [\[more...\]](#)

ver. **USB 2 GB** - \$149.00 | €104.00  
ver. **PS/2 2 GB** - \$139.00 | €97.00

## VideoGhost DVI / HDMI / VGA



Want to take key-logging to the next level? Grab entire screenshots with this **hardware video logger**! This **tiny framegrabber** hooks up to the **DVI, VGA, or HDMI** port of the graphics card, and silently records a **screenshot every few seconds**. You can later view all captured frames as **JPEGs**, by switching this video-recorder to a **2 Gigabyte USB flash drive**. Patent pending, edge cutting technology at an affordable price! [\[more...\]](#)



ver. **DVI 2 GB** - \$169.00 | €118.00  
ver. **HDMI 2 GB** - \$169.00 | €118.00  
ver. **VGA 2 GB** - \$169.00 | €118.00

# Eavesdropping

- Just as your computer may have a hardware “bug” attached to it, so, too, in some circumstances your data center or offices may be end up with a physical bug (surreptitious microphone or camera).
- While popular television shows frequently show these devices being easily detected, in reality, at least when professional quality equipment is used and installed by a skilled professional, it can be difficult to detect and neutralize those bugs (the process of locating and defeating bugs is normally referred to as “technical surveillance counter measures” or TSCM).
- If you remain skeptical that bugs are an real physical security issue, or that they can be difficult to detect and remove, I recommend you review the presentation: “Phone Talk,” [http://www.tscm.com/Phone\\_Lecture\\_2009/Phone\\_Lecture\\_Reston\\_VA-2009.htm](http://www.tscm.com/Phone_Lecture_2009/Phone_Lecture_Reston_VA-2009.htm) (167 slides)

# (Un)Trustworthy Hardware?

- “Information leakage” and “physical security problems” take on a profound new meaning if you can potentially end up with counterfeit hardware, or hardware made with counterfeit chips.
- I would encourage you to become familiar with the threat I’m referring to in this area – a nice briefing is the FBI PowerPoint deck entitled, “FBI Criminal Investigation – Cisco Routers,” as embedded in graphical form in “FBI Fears Chinese Hackers Have Back Door Into US Government and Military,” see <http://www.abovetopsecret.com/forum/thread350381/pg1>
- See also the excellent article “Dangerous Fakes,” [http://www.businessweek.com/magazine/content/08\\_41/b4103034193886.htm](http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm)
- Buying counterfeit products is one physical security risk, but other physical security risks are associated with disposing of surplus/no longer needed hardware on the other end of the cycle...

# Dumpster Diving and Surplus Equipment

- Historically, many crackers got their start by digging interesting computer and networking gear out of corporate dumpsters (a fine art normally known as “dumpster diving”).
- Today, there’s much more emphasis on recycling, and that’s laudable, but any storage media in surplus equipment needs to get wiped before that gear gets sold or otherwise disposed of, even if the system itself no longer boots/runs.
- Beware of amateur efforts at rendering hard drives unusable – staff members can easily hurt themselves while attempting to destroy surplus equipment with sledge hammers or other improvised tools (one particularly dangerous example involved amateur use of thermite!). Surprisingly, information may still sometimes be able to be recovered from a “destroyed” drive.
- Consider hiring a contractor to crush or shred your drives, or (if your volume is large), perhaps get your own crusher/shredder.





## Model 0300 Low/Medium Volume Hard Drive Shredder

### DESTROYS HARD DRIVES, OPTICAL MEDIA AND ASSORTED ELECTRONIC DEVICES

When it comes to the fast, safe, easy destruction of hard drives, nothing outperforms the Jackhammer™ Hard Drive Shredder from SEM.

Small footprint unit designed for low volume shredding, up to 500 laptop style drives per hour and 200 standard desktop style drives per hour. Single phase 120V power makes it ideal for office environment use. Designed with Operator Ease-of-use and safety in mind, **system features include:**

- Mailbox style feed opening
- Electrical limit switches to shut down machine when accessing cutting system or waste removal
- Easy access waste collection bin
- Integrated HEPA Filter
- Auto shut down when collection bin is full
- Illuminated controls to provide operator awareness of system status.
- Heavy duty casters for easy mobility



[see larger picture](#)

### Model 0300 Jackhammer Low/Medium Volume

MSRP:  
**\$29,609.00**

- ☒ Online Commercial:  
**\$21,250.00**
- ☐ GSA Contract:  
**\$18,950.00**

**1 Buy Now**

#### More Information

[View Datasheet \(PDF\)](#)  
[View Complete Catalog \(PDF\)](#)  
[View Video](#)



## Outputs: Confidential Documents

- Sensitive documents also need to be shredded, incinerated, or sequestered in a confidential document disposal container for approved disposal.
- Speaking of confidential document disposal containers, it is routine for these “wheelie” cans to live in mailrooms or corridor areas, locked to prevent casual browsing of discarded confidential documents, but often not living chained down.

Presumably the unauthorized removal of a full document disposal container full of confidential documents would be a disconcerting event, so please be careful and secure your wheelie cans of sensitive documents!

# All The Rest

- It isn't possible to go over everything that we really should talk about when it comes to IT physical security in only an hour, so please don't think that this is a comprehensive treatment –it's not. This talk is really just designed to “wet your whistle” when it comes to thinking about physical security.
- If you're not routinely talking about physical security at your site, or you don't have a formal physical security policy, you may want to think about having someone focus on this important area.
- Hopefully this talk will at least provide some starting points for that conversation.

# Thanks for the Chance to Talk!

- Are there any questions?