Homeland Security

March 2011

ICSJWG Quarterly Newsletter

New Government Coordinating Council Sector Co-Chair

Amit Khosla, in his new role as Acting Deputy Director of the Control Systems Security Program (CSSP), has replaced Rick Lichtenfels as the new Government Coordinating Council (GCC) co-chair. Previously, Amit was the Acting Director of the International Affairs Program at the National Cyber Security Division (NCSD), Department of Homeland Security (DHS).

ICSJWG 2011 Spring Conference

Join your colleagues this May in Texas! The Industrial Control Systems Joint Working Group (ICSJWG) Spring Conference will be held at the Dallas/Addison Marriott Quorum by the Galleria Hotel on May 2-5, 2011, in Dallas, Texas.

The ICSJWG Spring Conference is open to all who are interested in learning more about cybersecurity issues facing critical infrastructure control systems. The ICSJWG conference is an excellent resource for government professionals (federal, state, local, tribal, and international), control systems vendors and systems integrators, research and development and academic professionals, and owners and operators (management, engineering, production, IT, etc.) to interface with peers and stay abreast of the latest initiatives impacting security for industrial control systems.

The ICSJWG conference agenda will be as follows:

- **Monday, May 2:** Afternoon and evening subgroup working meetings (subgroup members only)
- **Tuesday, May 3:** Keynote, plenary sessions, subgroup status and accomplishment presentations, followed by individual and panel presentations
- **Wednesday, May 4:** Individual and panel presentations
- **Thursday, May 5:** Eight (8) hour Intermediate Industrial Control Systems Cybersecurity Training (lecture only)

About the ICSJWG

The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.

For more information, visit http://www.us-cert.gov/control_systems/icsjwg/

Table of Contents

There is no cost to attend the ICSJWG conference or training. Travel, accommodations, meals, beverages, and any other expenses are the responsibility of conference participants and will NOT be covered by the ICSJWG or CSSP. Participants may book rooms at the conference hotel at a special rate of $122 when registering through the conference site or by calling Marriott reservations at (888) 236-2427 and asking for the conference room rate. Book early, a limited number of rooms have been set aside at the conference rate.

To learn more or to register for the ICSJWG Spring Conference visit: http://www.regonline.com/Register/Checkin.aspx?EventID=934568.

ICSJWG Subgroup Status

Below is an update on the progress of the ICSJWG subgroups. If you would like to become a member of any of the subgroups, send an email with your contact information to icsjwg@dhs.gov or contact the co-chairs directly.

- **Roadmap to Secure Industrial Control Systems Subgroup**
  GCC Co-Chair: Perry Pederson (Perry.Pederson@nrc.gov)
  SCC Co-Chair: Tim Roxey (Tim.Roxey@nerc.net)

  The co-chairs of the Roadmap to Secure Industrial Control Systems subgroup are finalizing an update to the subgroup's charter. Once completed, the draft will be posted to the Homeland Security Information Network (HSIN) portal and sent to subgroup members for feedback. After feedback has been received from subgroup members, it will be sent to ICSJWG leadership for final approval. The subgroup members are planning to have a final charter in place for the ICSJWG Spring Conference. They are also in the process of finalizing the Industrial Control Systems Cross-sector Roadmap document and expect to have a final copy to distribute at the conference.

- **Vendor Subgroup**
  GCC Co-Chair: Amit Khosla (Amit.Khosla@dhs.gov)
  SCC Co-Chair: Eric Cosman (ECCosman@dow.com)

  The Vendor subgroup is in the middle of revising their charter to bring it into alignment with the purpose of the group. Eric Cosman has provided a draft first revision, and the changes have been posted on the HSIN portal. Please review and provide any feedback in HSIN using track changes. In conjunction with the charter revision, members are working to find an appropriate name for the subgroup that will be more inclusive of non-vendors. If anyone has an idea for a new group name, please email icsjwg@dhs.gov.

  With respect to the ICSJWG Spring Conference, the Vendor subgroup plans to hold a plenary session at the conference. The vulnerability disclosure white paper that members have been working on for the past year is almost complete and will tentatively be the subject of the plenary session.

The Vendor subgroup would also like to know if there are any subgroup members who are participating in other vendor-related groups/organizations. Please email icsjwg@dhs.gov with the group name and if there are overlaps and/or divisions between the group's and Vendor subgroup's goals and objectives. The ICSJWG Vendor subgroup wants to ensure that it is not duplicating but combining efforts, wherever possible, with other mission-related groups.

One suggestion from this group was to have a subject matter expert come speak at the monthly meetings for about 15 minutes about topics related to industrial control systems cybersecurity. If anyone is interested in speaking at a future meeting, please send an email to icsjwg@dhs.gov.

- **Workforce Development Subgroup**
  GCC Co-Chair: VACANT
  SCC Co-Chair: VACANT

  The Workforce Development subgroup is on hold due to the resignation of both the GCC and SCC co-chairs. If anyone is interested in applying for either position, please send an email to icsjwg@dhs.gov. We are looking for subject matter experts who have the time and resources to dedicate to the position.

- **Research and Development Subgroup**
  GCC Co-Chair: Dr. Douglas Maughan (Douglas.Maughan@dhs.gov)
  SCC Co-Chair: David L Norton (DNORTO1@entergy.com)

  The Research and Development (R&D) subgroup has not met since the face-to-face meeting at the ICSJWG Fall 2010 Conference in Seattle. The ICSJWG R&D subgroup co-chairs would like to increase participation and have the subgroup members focus on the tasks outlined in the charter but have been unsuccessful in gathering interest. Members are planning to discuss strategy on how to attain the subgroup's future goals and objectives during the conference.

- **International Subgroup**
  GCC Co-Chair: Seán McGurk (cssp@dhs.gov)
  SCC Co-Chair: Graham Speake (graham.speake@us.yokogawa.com)

  The International subgroup will continue to serve as a registration point for industrial control systems professionals and will be informed of activities taking place in the ICSJWG community. While no actual meetings are currently planned, International members will be notified of all ICSJWG news and are welcome to attend ICSJWG events.

- **Information Sharing Subgroup**
  The ICSJWG Information sharing subgroup has been absolved with the roll-out of the HSIN portal. A new Standards subgroup is in the process of being created to replace the Information Sharing subgroup. Additional information on this new subgroup will be announced once the group has been created and co-chairs have been selected.

Homeland Security Information Network

HSIN is now fully developed and in use by ICSJWG subgroup members. Subgroup members can keep abreast of upcoming meetings through the calendars in HSIN. In addition, the "Alert Me" feature notifies users of changes to the portal, which eliminates the need for users to constantly log in to find out if updates have been made. Alerts can be sent immediately, daily, or weekly. To sign up for alerts, click on the "Alert Me" link on the left-hand side of the ICSJWG homepage and choose your delivery option.

ICSJWG subgroup members who still need access to HSIN can send an email to icsjwg@dhs.gov to request an account.

- **If you do not currently have a HSIN account**, please provide your name, company, contact information, critical infrastructure sector, and ICSJWG subgroup affiliations.

- **If you already have a HSIN account**, please provide your name, HSIN username, the email address that you used to sign up for your HSIN account, ICSJWG subgroup affiliation, and critical infrastructure sector.

At this time, DHS is not able to grant International subgroup members access to the HSIN portal. The owners of the HSIN portal are reviewing sharing agreements concerning information posted to the site. Until that process is complete, International subgroup user accounts will be on hold. ICSJWG Communications will contact all International subgroup members immediately once a solution is in place or if there is more information available.

Advanced Training Events Scheduled for 2011

CSSP is currently offering advanced cybersecurity training sessions at the Control Systems Analysis Center located in Idaho Falls, Idaho. These sessions will provide intensive hands-on training on protecting and securing control systems from cyber attacks, including a very realistic Red Team/Blue Team exercise that will be conducted within an actual control systems environment. It will also provide an opportunity for attendees to network and collaborate with other colleagues involved in operating and protecting control systems networks.

This event includes five days of intensive cybersecurity for industrial control systems training, and a Red Team/Blue Team hands-on exercise:

- **Day 1:** Welcome, overview of the DHS CSSP, a brief review of cybersecurity for industrial control systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.
- **Day 2:** Hands-on classroom training on Network Discovery, instruction for using Metasploit, and separating into Red and Blue Teams.
- **Day 3:** Hands-on classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.
- **Day 4:** A 12-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment and with maintaining operations to a batch-mixing plant and an electrical distribution Supervisory Control and Data Acquisition (SCADA) system.
- **Day 5:** Red Team/Blue Team lessons learned and roundtable discussion.

The following advanced training events have been scheduled for 2011:

- **April 11-15:** Industry Partners
- **May 14-18:** Industry Partners
- **May 23-27:** Israeli Partners
- **June 20-24:** Industry Partners
- **July 18-22:** Industry Partners
- **September 12-16:** International Partners
- **October 10-14:** Industry Partners
- **November 7-11:** Reserved
- **December 5-9:** Industry Partners

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant.

Additional offerings are being planned and will be announced once dates are finalized. As scheduled advanced training gets closer, an invitation along with a link to register for the course will be sent out and posted to the following website:
http://www.us-cert.gov/control_systems/cscalendar.html.

Please check back periodically, as this schedule is occasionally updated.

Register by clicking on the link provided on our webpage:
http://www.us-cert.gov/control_systems/cscalendar.html.

Registration is open approximately 2 months before the start of a class. Due to high demand, class size is limited to approximately 35 people with a maximum of 2 individuals per company per event. Classes fill quickly, so early registration is encouraged. Notification of cancellation is appreciated, with as much advance notice as possible so that others who wish to take the course can do so.

Industrial Control Systems Articles

ICSJWG is now accepting short articles of general interest pertaining to control systems security for the June quarterly newsletter. If you want to submit an article for the June newsletter, please email icsjwg@dhs.gov, and we will take your article into consideration for publishing. The deadline for submissions for the June newsletter is **May 27, 2011**.

Past ICSJWG newsletters are located on the CSSP website at
http://www.us-cert.gov/control_systems/icsjwg/index.html
and on HSIN at
https://cs.hsin.gov/C10/C1/ICSJWG/default.aspx?RootFolder=%2fC10%2fC1%2fICSJWG%2fDocument%20Library%2fICSJWG%20Newsletters&View=%7b7F0225B9%2d1943%2d4074%2dB349%2d32C32A4EB8E7%7d.

Thank you for contributing. The following articles were submitted by members of the ICSJWG for publication and distribution to the ICSJWG community. Article contents and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations. The advice and instructions provided in the articles should be confirmed and tested prior to implementation.

New Tricks for Old Dogs: Security Tool Review

By Bryan Owen, Cyber Security Manager, OSIsoft

With spring around the corner I decided to get a jump on some overdue decommissioning work in my test bed. Although well past their prime, these trusty machines were granted a final test before that long cold ride to the e-cycle yard.

First on the list is a 233Mhz Pentium II box sporting a 2GB system drive and 20GB drive for data. The final mission is data destruction. Since the machine is in surprisingly good working order it didn't feel right to put the drives under a drill press. "Darik's Boot and Nuke" a tool available @DBan.org was selected for the final test.

A self-contained boot disk approach is almost a necessity for this kind of work but it reminded me of Lofty Perch's "The First Mile: Client Side Security for Remote Access to Control Systems" (ICSJWG 2010 Fall Conference). Similarly, Boot and Nuke couldn't have been easier to use. Boot from CD and select "autonuke" to launch a nice DoD grade disk wipe. Success was reported after 3 hours. DBAN is a free software product that can be used at home or in a business at zero cost. More details are available on the SourceForge project site.

Next up is a machine being parted out because of an insatiable appetite for power supplies. The 2.8Ghz P4 is new enough to provide hardware No Execute (NX) so its final mission is in testing back ported platform defenses enabled by Microsoft's Enhanced Mitigation Experience Toolkit (EMET).

The bench test vulnerability is an old version of our database service as described in US CERT CIIN-08-337-01. Specifically, the test case verifies structured exception handler overwrite protection (SEHOP) added to a XP SP3 environment – the oldest platform supported by EMET.

The EMET GUI configuration experience is as simple as picking the target application and selecting a checkbox to opt in mitigations. I start the application and system load appears unchanged with EMET enabled. When the stress test exercises our bug, the operating system gracefully traps an application exception and logs an ERROR_STACK_BUFFER_OVERRUN code. The test is a success because without the added SEHOP protection the application would attempt to execute unchecked input data – ouch!

To reiterate, EMET is very easy to use and could be appropriate in the right situation (e.g., when no patch is available). Hopefully this example case peaks your interest in the rest of the toolkit. The export address filter shell code mitigation sounds especially intriguing and unique.

In the final tool test I dust off an old Cisco PIX 501 firewall to exercise a pre-release version of the latest PortalEdge package from Digital Bond. Syslog server logging capability is provided by the historian. The attack detection monitoring adds events emitted by popular firewall devices including the PIX.

The PIX PDM web interface is no good for configuration because of legacy browser and Java requirements. Vintage NSA Cisco router security guides direct me to the Center for Internet Security RAT tool as a good practice configuration benchmark. The PIX comes to life and to my surprise normal activity in the lab raises a few alerts:

- Attack Activity – Deny UDP reverse path check
- Suspicious Activity – Received ARP request collision
- Inbound Blocked – Inbound TCP connection denied

The attack alarm is really a configuration error. Source IP verification uses static routes as a white list and in this case a route to an NTP server was missing. Likewise, the suspicious ARP collision involved virtual machine traffic that I quickly compartmentalized to internal networks. Alarms on inbound and outbound traffic were the result of deliberate attempts.

Initial observations suggest the PortalEdge filters are useful because Syslog traffic can have a lot of 'white' noise. A more integrated test environment is needed to exercise the authenticated access categories and other potential CIP-005 monitoring scenarios.

Well the weekend is over for this geek. The PIX has redeemed itself as some good old 'junk' to mess with. I have no regrets for the other loyal machines now resting in peace – or in pieces!

Advanced Persistent Pen-Testers

By Andrew Ginter, CTO, Abterra Technologies, and Joel Langill, CSO, SCADAhacker

The recently-documented Night Dragon attacks were not examples of remarkable technology in action; they were remarkable because of their success, because they targeted control systems, and because of the "low tech" approach used in the attacks. All it took to compromise the control systems of large energy-industry firms, from China, was:

- the persistent application of technologies available for free on the Internet, and
- skills taught every day in penetration-testing courses all over the world.

Advanced threats are a fact of life for enterprise security teams. With the experience of Stuxnet and now Night Dragon, such threats need to be taken much more seriously by industrial security teams.

What Every Pen-Tester Knows

Penetration testing is one approach to security assessment. When you think you have secured a site thoroughly and when you have passed other kinds of assessments, security teams routinely bring in pen-testers. Pen-testers may be given different sorts of marching orders - different starting points, different objectives, different rules of engagement - but in general their goal is to "break" the security system and document how it was broken, so that the site's security can be improved. Many firms have their own internal pen-testers, and even those will bring in outside testers as "fresh eyes" periodically.

The kind of penetration testing which corresponds best to the Night Dragon accomplishments is "external, black box" testing. The tester is given no inside knowledge of the target, and starts from their own office, over the Internet. Their objective is to gain control of computers inside a trusted network and use those computers to extract valuable intellectual property.

Unlike the documented Night Dragon exploits, common wisdom among pen-testers is that the easiest way into a firm's network is not by attacking web servers with SQL-injection. Such attacks do "work," but increasingly firms host their web servers and associated databases at external providers with limited or no connectivity to the main business network.

Common wisdom among pen-testers is that social engineering is the easiest way into a business network. Do your homework, learn about a handful of individuals in the firm, understand what projects they are working on and who they correspond with, then fake a handful of emails. The emails persuade the targets to download malware or simply execute an attachment, because they think the download or attachment is coming from a trusted source. Anti-virus technology does not catch these executions, because they are custom malware. The exploits are crafted from source code toolkits downloaded from the web, which are customized, recompiled and re-packaged. The resulting executables are unique to this one target. There are no AV rules for the malware executables, because no AV vendor has ever seen this malware before.

That said, enterprise security teams at the biggest targets tend to be very aware of advanced threats and have invested heavily in measures to frustrate these attacks. External black-box testing of smaller firms succeeds more often than not. Such testing of the biggest targets has a low success rate. After all - the largest targets' own internal pen-testers have found and fixed all the easy approaches to breaking their security. When targeting large firms, many pen-testers will again do their homework and learn who their targets' smaller, trusted suppliers are. The testers then try this same approach on those suppliers, and start looking around inside the suppliers business networks for VPN connections to the real target, or for trusted laptops which might be carried into the real targets' networks from time to time.

The malware of choice in all these cases is not worms which propagate automatically, but as McAfee reported "remote administration tools." These are tools which first escalate privilege, and then reach out over the Internet to the attacker's servers, cloaking their communications as normal traffic - for example web accesses, instant messaging or voice-over-IP communications. Once connected, the tools give the attackers control of the machines on which they are installed. Attackers use these tools to slowly and silently learn about the target's networks and systems, and slowly spread to other computers on their way to their real objective.

What ICS Pen-Testers Know

Industrial control system penetration testers generally start by sitting down at a desktop on the target firm's business network. This provides a realistic scenario for either an insider who has compromised the network unintentionally, or an outsider who has gained credentials to masquerade as an insider in launching subsequent attacks by remote controller. ICS pen-testers know that while there may be specialized knowledge needed to crack the control system, testers with that knowledge generally succeed in their attacks. Even in the largest target firms, control system resources are comparatively much more poorly defended from business-network attacks than the enterprise network is defended from Internet attacks.

ICS pen-testers generally start with some reconnaissance of the machine they are given. They first escalate privilege on the machine and start looking at all the accounts on the machine for "most recently used" information about network connections, tools and documents. If they start on a machine that is at least occasionally used to access control system resources, this first step is often enough to reveal information about how to access the control system. If this first step fails, then more traditional network reconnaissance is undertaken, such as querying nearby network devices to try to find routers and firewalls leading to control system resources, or compromising nearby hosts or domain servers and repeating the inquiries there.

Once the connection to the control system is identified, things tend to move fast. Most control system firewalls are configured to allow all "business critical communications" to pass through. What this means in practice is that a large number of kinds of communications are allowed through the firewall. Many control system hosts still use default passwords. Security personnel argue that such usage is still "safe" because the accounts with default passwords have little privilege. The first thing pen-testers do once they are "in" with default passwords is escalate privilege.

Further, the hosts behind the firewall tend to be less thoroughly patched than hosts on the business networks, and even hosts on the largest business networks tend to be weeks or months behind on patching. Even if a site has a strong patch program, the sheer volume of testing required to certify patches for use on critical control systems or on the largest business networks means that patches take a long time to apply. All good pen-testers do their "homework" before going to site, and will come to site armed with exploits for the last few months' announced vulnerabilities, knowing that control system hosts will almost never be patched for the most recent exploits.

Once a control system host is compromised, again "remote administration" toolkits are installed and they provide a user experience similar to a remote desktop - the attacker can see the screens on the compromised computer and interact with those screens as if they were sitting at the computer. Once inside, pen-testers tend to look around for an engineering workstation. Such workstations generally contain a treasure-trove of information: high-level design documents, network diagrams, wiring diagrams, schema for ICS databases and master copies of PLC programming.

Looking Forward...

Again, the bad news is that penetration testers routinely report a high success rate for "black box" tests of control system networks from hosts inside a firm's business network. The probability of a remote assault on a control system succeeding is the product of the probability of penetrating the enterprise perimeter and the probability of penetrating the control system perimeter. Pen-testers generally report the latter probability is close to 1 in their experience. As a result, ICS security programs add little value to the fight against remote, advanced threats that leverage credentials gained from compromising trust relationships on the enterprise network. Worse, the skills used by these advanced adversaries are simple pen-testing skills taught routinely in enterprise and ICS pen-testing courses.

The good news is that at least at the biggest targets, remote "black box" attacks have a low success rate, due to a keen awareness of advanced threats at the enterprise level. This good news has to be tempered though: penetrating small to medium-sized businesses is much easier than the biggest targets. Further, pen-testers generally have a limited budget when testing a firm. Advanced threats with a bigger budget can be more persistent in their attacks, and therefore more successful.

The biggest thing asset owners can do to protect their control systems from advanced threats like Night Dragon is to improve the protection of their control systems from attackers on their business networks. By dramatically reducing the success rate of these attacks, both small and large firms will see their control systems become much harder to penetrate. Such improvements are not hard to achieve - unlike business networks where large amounts of information must routinely be exchanged with untrusted sources, where connections to never-before-seen websites are commonplace, and where there is a huge diversity of complex applications, control networks are predictable. Control networks may run applications which are unfamiliar to enterprise security personnel, but as a rule control networks are smaller, simpler, and easier to secure than are business networks, at least easier for those skilled in the art of securing control systems.

Any ICS pen-tester will tell you the first steps to better security are well-known:

- firm up the plant/business firewall - stop allowing so many connections,
- protect systems exposed through the plant firewall with up-to-the-second patches,
- stop using default passwords - even a password known by everyone at the site is not known by a remote attacker.

There are a host of next steps possible, from specialized deep-packet-inspection firewalls, to one-way communications hardware, to HIPS/whitelisting technologies. These first steps, though, are essential, and are still not widely practiced. Advanced threats are targeting control systems with the persistent application of well-known tools and techniques. You can make your systems much harder for such threats to penetrate.

Participation is Key!

Your participation and input is **critical** to the success of these subgroups and to the overall mission of the ICSJWG in coordinating cybersecurity efforts to secure industrial control systems across the nation's critical infrastructure. Please email the co-chairs or icsjwg@dhs.gov to get involved with one or more of the subgroups.

CSSP Contact Information

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to icsjwg@dhs.gov.

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at https://forms.us-cert.gov/report/.

Other important contact information:

Website Address: http://www.us-cert.gov/control_systems/
ICS-CERT Email: ics-cert@dhs.gov
Phone: 1-877-776-7585
CSSP Email: cssp@dhs.gov